RSA NETWITNESS® SUITE

Logs and Network Documentation

for Version 11.1

RSA NETWITNESS® SUITE

Getting Started Guides

for Version 11.1

RSA NETWITNESS® SUITE

Hosts and Services Getting Started Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Hosts and Services Basics 9

What Is a Host 9

What Is a Host Type 9

What Is a Service 10

Setting Up a Host 11

Maintaining Hosts 12

Update Version Naming Convention 12

Maintaining Services 13

Services Implemented with the NetWitness Server 13

Running in Mixed Mode 15

Functionality Gaps Encountered During in Staggered Updates 15

Examples of Staggered Updates 16

Example 2. Multiple Decoders and Concentrators, Alternative 2 16

Example 3. Multiple Regions 17

Hosts and Services Procedures 18

Step 1. Deploy a Host 21

Step 2. Install a Service on a Host 22

Prerequisites 22

Procedure 22

Step 3. Review SSL Ports for Trusted Connections 23

Prerequisite 23

Encrypted SSL Ports 23

Step 4. Manage Access to a Service 25

Test a Trusted Connection 25

Apply Version Updates to a Host 28

Apply Updates from the Hosts View (Web Access) 29

Task 1. Populate Local Repo or Set Up an External Repo 29

Task 2. Apply Updates from the Hosts View to Each Host 29

Apply Updates from the Command Line (No Web Access) 31

Populate Local Update Repository 32

Set Up an External Repository with RSA and OS Updates 34

Create and Manage Host Groups 37
Create a Group 38
Change the Name of a Group 39
Add a Host to a Group 39
View the Hosts in a Group 39
Remove a Host from a Group 40
Delete a Group 41
Search for Hosts 41
Search for a Host 41
Find the Host that Runs a Service 41
Execute a Task From the Host Task List 43
Add and Delete a Filesystem Monitor 45
Configure the Filesystem Monitor 45
Delete a Filesystem Monitor 46
Reboot a Host 46
Shut Down and Restart a Host from the Hosts View 47
Shut Down and Restart a Host from the Host Task List 47
Set Host Built-In Clock 47
Set the Time on the Local Clock 48
Set Network Configuration 48
Specify the Network Address for a Host 49
Set Network Time Source 50
Specify the Network Clock Source 50
Set SNMP 51
Toggle SNMP Service on the Host 51
Set Syslog Forwarding 52
Set Up and Start Syslog Forwarding 52
Show Network Port Status 54
Display the Network Port Status 54
Show Serial Number 55
Show the Serial Number 55
Shut Down Host 56
Shut Down the Host 57
Stop and Start a Service on a Host 57
Stop a Service on a Host 57
Start a Service on a Host 58

Add, Replicate or Delete a Service User 59
Replication and Migration Considerations 60
Procedures 60
Add a Service User Role 63
Procedure 64
Change a Service User Password 65
Create and Manage Service Groups 66
Create a Group 67
Change the Name of a Group 68
Add a Service to a Group 68
View the Services in a Group 68
Remove a Service from a Group 68
Delete a Group 69
Duplicate or Replicate a Service Role 69
Duplicate a Service Role 70
Replicate a Role 70
Edit Core Service Configuration Files 71
Edit a Service Configuration File 71
Revert to a Backup Version of a Service Configuration File 72
Push a Configuration File to Other Services 72
Edit or Delete a Service 84
Procedures 84
Explore and Edit Service Property Tree 86
Procedures 86
Kill a Connection to a Service 87
End a Session on a Service 87
End an Active Query in a Session 88
Search for Services 89
Search for a Service 89
Filter Services by Type 89
Find the Services on a Host 91
Start, Stop or Restart a Service 92
Start a Service 92
Stop a Service 92
Restart a Service 93
View Service Details 93

Purpose of Each Service View 93
Access a Service View 93

Hosts and Services Views References 96

Hosts View 97
Workflow 97
What do you want to do? 98
Quick Look 98
Hosts Panel Toolbar 99
Groups Panel Toolbar 100
Services View 102
Workflow 102
What do you want to do? 103
Related Topics 103
Quick Look 103
Edit Service Dialog 107
Groups Panel Toolbar 109
Services Panel Toolbar 110
Services Config View 112
Topic 116
Features 118
Edit a Service Configuration File 119
Files Tab Toolbar 120
Services Explore View 122
The Node List 123
The Monitor Panel 124
Features 126
Services Logs View 128
Services Security View 130
Roles and Service Access 131
Features 132
Role Name Panel 132

Role Information and Permissions Panel 133
Service User Roles 134
Service User Permissions 135
Features 139
SDK Meta Role Permissions Options 139
Features 141
User List Panel 141
User Definition Panel 143
Services Stats View 146
Summary Stats Section 147
Gauges 151
Timelines 151
Historical Timelines 151
Chart Stats Tray 151
Components 152
Features 153
System View 156
Services Info Toolbar 157
Features 159
Host Task Selection List 160
Service Configuration Settings 162
Appliance Service Configuration Parameters 162
Archiver Service Configuration View 162
Broker Service Configuration Parameters 164
Aggregation Configuration Parameters 165
Concentrator Service Configuration Parameters 168
Core Service Logging Configuration Parameters 169
Core Service-to-Service Configuration Parameters 170

Core Service System Configuration Parameters 171
Decoder Service Configuration Parameters 173
Decoder and Log Decoder Configuration Parameters 174
Log Decoder Service Configuration View 178
Log Decoder Service Configuration Parameters 180
REST Interface Configuration Parameters 184
NetWitness Suite Core Service system.roles Modes 185

Troubleshooting Version Installations and Updates 186

Hosts and Services Basics

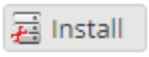
This guide gives administrators the standard procedures for adding and configuring hosts and services in NetWitness Suite. After introducing you to the basic purpose of hosts and services and how they function within in the NetWitness Suite network, this guide covers:

- The tasks you must complete to set up hosts and services in your network
- Additional procedures that you complete based on the long-term and daily, operational needs of your enterprise
- Reference topics that describe the user interface

What Is a Host

A host is the machine on which a service runs and a host can be a physical or virtual machine. See the "RSA NetWitness Suite Detailed Host Deployment Diagram" in the *RSA Netwitness Suite Deployment Guide* for an illustration of how host are deployed. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

What Is a Host Type

A host type assigns a service or services to a host when you install a host from the Hosts view. You choose a **Host Type** in the **Install Services** dialog which is displayed when select a host in the Hosts view and click 

(Install icon). The following table lists each host type and the service or services it installs. See the "RSA NetWitness Suite Detailed Host Deployment Diagram" in the *RSA Netwitness Suite Deployment Guide* for an illustration of how host are deployed. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Host Type	Services Installed
Archiver	Workbench and Archiver
Broker	Broker
Cloud Gateway	Cloud Gateway
Concentrator	Concentrator
Endpoint Hybrid	Log Decoder, Endpoint, and Concentrator

Host Type	Services Installed
Endpoint Log Hybrid	Log Collector, Log Decoder, Endpoint, and Concentrator
ESA Primary	Context Hub, Entity Behavior Analysis, and Event Stream Analysis
ESA Secondary	Entity Behavior Analysis and Event Stream Analysis
Log Collector	Log Collector
Log Decoder	Log Collector and Log Decoder
Log Hybrid	Log Collector, Log Decoder, and Concentrator
Malware Analysis	Malware Analysis and Broker
Packet Decoder	Decoder
Packet Hybrid	Concentrator and Decoder
Warehouse Connector	Warehouse Connector

What Is a Service

A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plugin to enable or disable, according to the function of the host.

You must configure the following Core services first:

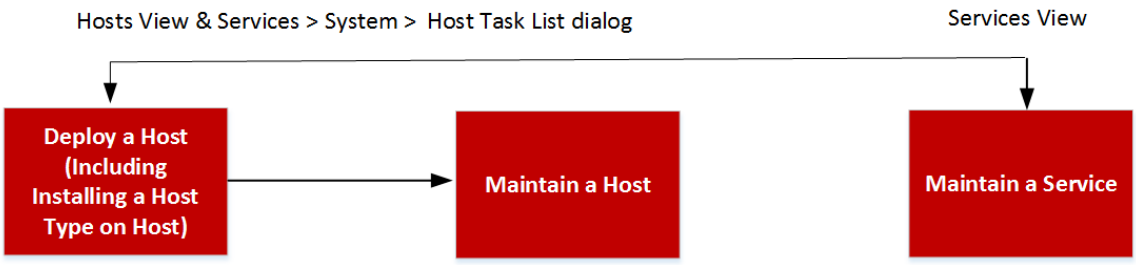
- Decoder
- Concentrator
- Broker
- Log Decoder

All the services are listed below and each service except the Log Collector has its own guide or shares a guide in the *Host and Services Configuration Guides*. The Log Collector has its own set of configuration guides to handle the configuration for all the supported event collection protocols. For Log Collector information, see *Log Collection Guides*.

- Archiver
- Broker
- Cloud Gateway

- Concentrator
- Context Hub
- Decoder (Packets)
- Endpoint
- Entity Behavior Analysis
- Event Stream Analysis
- Investigate
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Respond
- Warehouse Connector
- Workbench

You must configure hosts and services to communicate with the network and each other so they can perform their functions such as storing or capturing data.



Setting Up a Host

You use the Host view to add a host to NetWitness Suite. See Step 1. Deploy a Host for detailed instructions.

Maintaining Hosts

You use the main Host view to add, edit, delete, and perform other maintenance tasks for the hosts in your deployment. You use the Task List dialog to perform tasks relating to a host and its communications with the network. See Hosts and Services Procedures for detailed instructions.

After your initial implementation of NetWitness Suite, the major task you perform from the Host view is updating your NetWitness Suite deployment to a new version.

Update Version Naming Convention

You use the Hosts view to apply the latest version updates from your Local Update Repository (see the **Manage NetWitness Suite Updates** topic in *System Maintenance* for more information on your Local Update Repository). You must understand the update version naming convention to know which version you want to apply to the host. The naming convention is ***major-release.minor-release.service-pack.patch***. For example, if you choose 11.6.1.2, you would be applying the following version to the host.

- 11 = major release
- 6 = minor release
- 1 = service pack
- 2 = patch

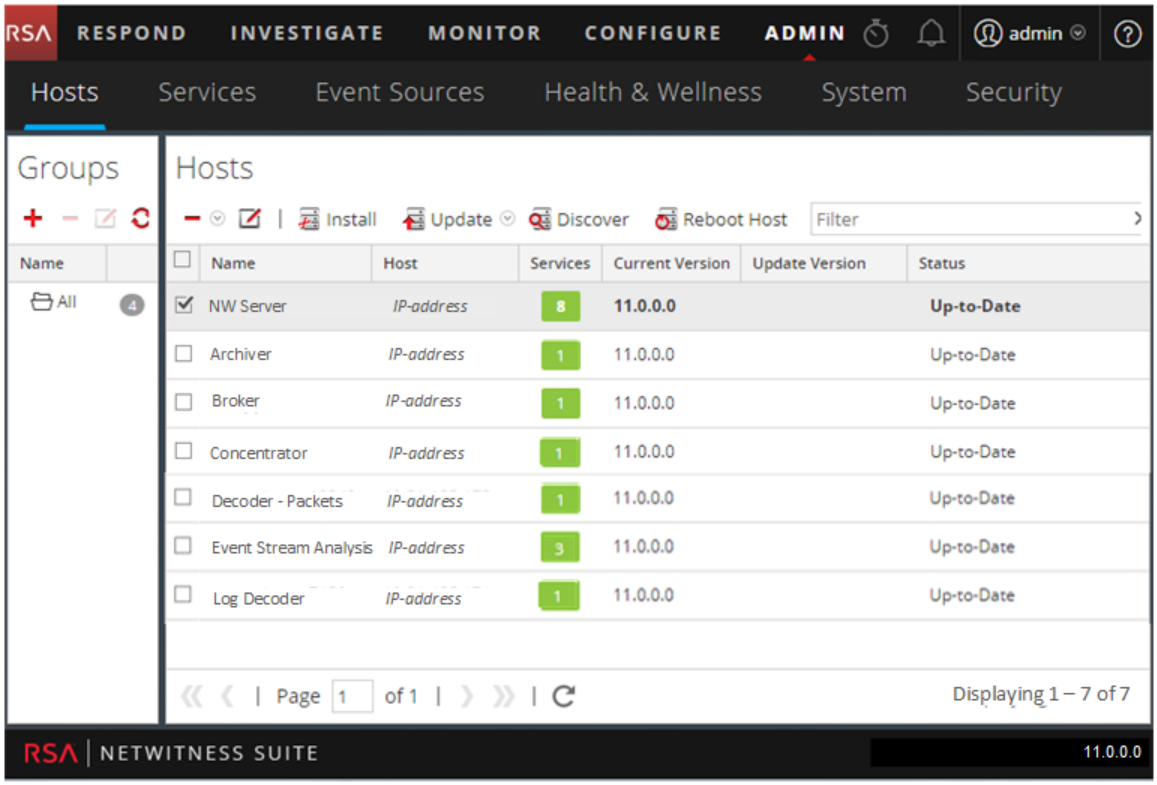
NetWitness Suite supports multiple versions in your deployment. The NetWitness Server (NW Server Host) is updated first and all other hosts must have the same or earlier version as the NW Server Host.

Note: You must update the NW Server Host first and that all other hosts have the same or earlier version as the NW Server Host.

In the following example of a multiple version deployment:

- Version updates currently available in your Local Update Repository are 11.0.2.0 and 11.0.1.0 for the Broker, LC/LD, and Log Decoder hosts.
- The NW Server Host and all the other hosts are currently updated to 11.0.2.0.

This means that you have the option to update the Broker, LC/LD, and Log Decoder hosts to 11.0.2.0 or 11.0.2.0.



Maintaining Services

You use the Services view to add, edit, delete, monitor, and perform other maintenance tasks for the services in your deployment. See Hosts and Services Procedures for detailed instructions.

Services Implemented with the NetWitness Server

The services in the following table are implemented when you deploy the NW Server to support:

- the expansion of physical and virtual deployment platforms and improvements to host and service maintenance.
- improvements to the Investigate and Respond functionality.

Caution: You do not need to configure these services to deploy NetWitness Suite. RSA recommends that you monitor the operating status of these services using Health-and-Wellness. Do not attempt to modify the parameters in the Explore view without contacting Customer Support (https://community.rsa.com/docs/DOC-1294).

Service	Purpose
Admin	The Administration Server (**Admin server**) is the back-end service for administrative tasks in the NetWitness Suite User Interface (UI). It abstracts authentication, global preferences management, and authorization support for the UI. The **Admin server** requires the **Config server** and the **Security server** to be online to perform its role.
Config	The Configuration Server (**Config server**) stores and manages configuration sets. A configuration set is any logical configuration group that is managed independently. The **Config server** facilitates the sharing of properties among services, provides configuration backup and restore facilities, and tracks changes to properties.
Integration	The Integration Server manages interactions with external systems. The service handles the following outbound or inbound channels. • REST API Gateway - gateway to external REST clients that assigns calls to the NetWitness Application Programming Interface (API). • Notifications Dispatcher - centralized dispatcher for all outbound notifications originating in the NetWitness deployment.
Investigate	The Investigate server is co-located on NW Server host with the **Admin server**, **Config server**, **Integration server, Orchestration server**, **Respond server**, and **Security server**. The Investigate server is co-located on NW Server host with the Admin server, Config server, Integration server, Orchestration server, Respond server, and Security server. See the *RSA NetWitness Suite Investigate and Malware Analysis User Guide* for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
Orchestration	The Investigate server is an internal, system management service that runs on the NW Server to provision, install, and configure all services in your NetWitness Suite deployment.
Respond	The Respond server is co-located on NW Server host with the **Admin server**, **Config server**, **Investigate server**, **Orchestration server**, and **Security server**. See the *RSA NetWitness Suite Respond Configuration Guide* for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Service	Purpose
Security	The NetWitness Suite Security Server (**Security server**) manages the security infrastructure of a NetWitness Suite deployment. It handles the following security-related concerns. • Users and the authentication accounts • Role Based Access Control (RBAC) • Deployment PKI infrastructure A NetWitness Suite deployment has users with authentication accounts. Independent of how you verify the identity of the analyst (for example, Active Directory), NetWitness Suite must maintain user state that is not provided by all authentication providers (for example, last login time, failed login attempts, and roles). The concept of a user is separate from the identify associated with the user and the **Security server** maintains these as separate User and Account entities. In addition to the out of the box local NetWitness accounts available to all NetWitness deployments, the server supports external authentication providers. The **Security server** also implements RBAC by managing Role and Permission entities. Permissions can be assigned to roles and roles to users. Together these enable a flexible authorization policy for the deployment. The server also manages generation of cryptographically secure tokens that encode the applicable authorization for a user. These tokens form the basis for deployment wide authorization.

Running in Mixed Mode

Mixed mode occurs when some services are updated to the latest version and some are still on older versions. This happens when you update the hosts in your deployment to the latest version in phases (or stagger the update).

Functionality Gaps Encountered During in Staggered Updates

If you stagger the update, you:

- May not have all the features operational until you update your entire deployment.
- Will not have service administrative features available until you update all the hosts in your deployment.
- May be without data capture for a period of time.

Examples of Staggered Updates

In the following examples, all the hosts are on 11.1.0.x and you want to stagger the host updates to version 11.1.1.0.

Example 1. Multiple Decoders and Concentrators, Alternative 1

In this example, the 11.1.0.x deployment includes 1 NW Server host, 2 Decoder hosts, 2 Concentrator hosts, 1 Archiver host, 1 Broker host, 1 Event Stream Analysis host, and 1 Malware Analysis host.

You must complete Phase 1 first and update the hosts in the order listed for Phase 1.

RSA recommends that you update the Phase 2 hosts in the order listed for Phase 1

Phase 1 - session 1

1. Update the Security Analytics Server host.
2. Update Event Stream Analysis host.
3. Update Malware Analysis host.
4. Broker or Concentrator host.

Phase 2 - session 2

1. Update 2 Decoder hosts.
2. Update 2 Concentrator hosts and Archiver host.

Phase 2 - session 3

1. Update all other hosts.

Example 2. Multiple Decoders and Concentrators, Alternative 2

In this example, the 11.1.0.x deployment includes 1 NW Server host, 2 Decoder hosts, 2 Concentrator hosts, 1 Broker host, 1 Event Stream Analysis host, and 1 Malware Analysis host. RSA recommends that you update the Phase 2 hosts the following sequence (you must complete Phase 1 first and update the hosts in the order listed).

Phase 1 - session 1

1. Update the Security Analytics Server host.
2. Update Event Stream Analysis host.
3. Update Malware Analysis host.
4. Update Broker host.

Phase 2 - session 2

1. Update 1 Decoder host and 1 Concentrator host.
   Time elapses during which NetWitness Suite processes a significant amount of data.

Phase 2 - session 3

1. Update 1 Decoder host, 1 Concentrator host, and the Broker host.
2. Log Decoders
   Update all Log Decoder hosts before you update Virtual Log Collectors
3. Update all other hosts.

Example 3. Multiple Regions

In this example, the 11.1.0.x deployment includes 1 NW Server host, 1 Event Stream Analysis host, 1 Malware Analysis host, 4 Decoder hosts, 4 Concentrator hosts, 2 Broker hosts, (2 sites, each with 2 Decoders, 2 Concentrators, and 1 Broker).

Phase 1 - Update Site 1

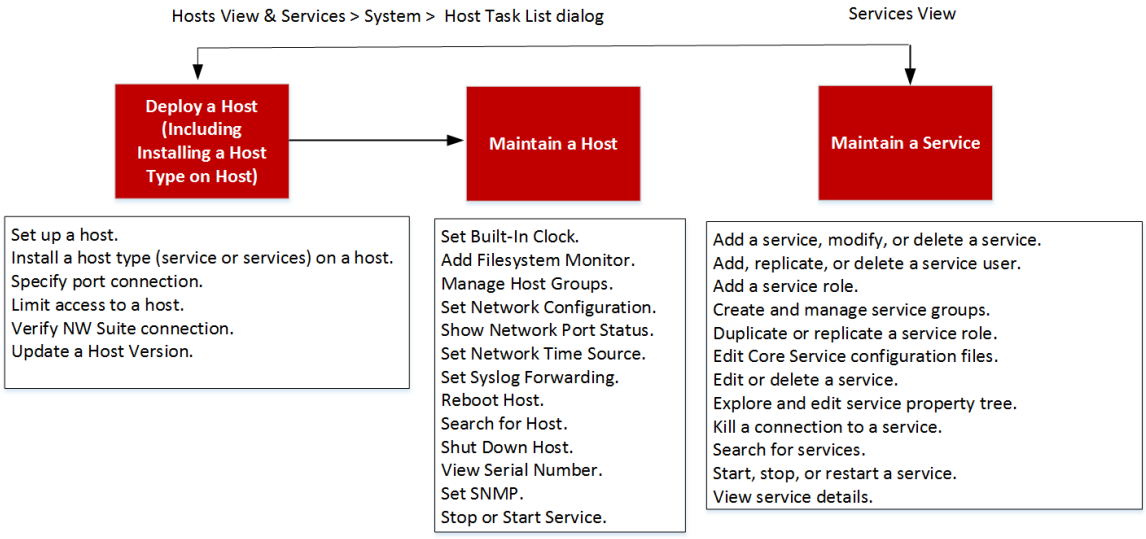
1. Update the NW Server host.
2. Update the Event Stream Analysis host.
3. Update the Malware Analysis host.
4. Update 1 Broker host, 2 Decoder hosts, and 2 Concentrator hosts.
5. Update all other hosts.

Phase 2 - Update Site 2

1. Update Broker hosts.
2. Update 2 Decoder hosts.
3. Update 2 Concentrator hosts.
4. Update all other hosts.

Hosts and Services Procedures

Every service requires a host. After you set up a host, you can assign services to and from this host to other hosts in your NetWitness Suite deployment.



High-Level Task	Description
Set Up a Host	Complete the following tasks in the order shown to set up a host. Step 1. Deploy a host. Step 2. Install a service on a host. Step 3. Review SSL Ports for Trusted Connections. Step 4. Manage access to a service.

High-Level Task	Description

Maintain a Host - Basics	The following maintenance tasks are not required and are shown in alphabetical order.
	• Apply version updates to a host.
	  • Populate Local Update Repository
	  • Set Up an External Repository with RSA and OS Updates
	• Create and manage host groups.
	• Search for hosts.
	• Set network configuration.
	• Set network time source.
	• Show network port status.
	• Show serial number.
	• Shut down a host.
	• Stop and start a service on a host.

High-Level Task	Description
Maintain a Host from the Host Task List Dialog	You use the Host Task List dialog to manage tasks that relate to a host and its communications with the network. Several service and host configuration options are available for Core hosts. • Execute a task from the Host Task List. • Add and delete a Filesystem monitor. • Reboot a host. • Set host built-in clock. • Set network configuration. • Set network time source. • Set SNMP. • Set Syslog forwarding. • Show network port status. • Show serial number. • Shut down host. • Stop and start a service on a host.

High-Level Task	Description
Maintain a Service	The following procedures describe how to maintain services. • Add, replicate or delete a service user. • Add a service user role. • Change a service user password. • Create and manage service groups. • Duplicate or replicate a service role. • Edit core service configuration files. • Edit or delete a service. • Explore and edit service property tree. • Kill a connection to a service. • Search for services. • Start, stop or restart a service. • View service details.

Step 1. Deploy a Host

1. Deploy a host.
   You can deploy a physical host (RSA Appliance), virtual host on-prem, a virtual in AWS, or a virtual host in Azure. See the following guides for instructions on how to deploy hosts.
   - *RSA NetWitness® Suite Physical Host Deployment Guide*
   - *RSA NetWitness® Suite Virtual Host Deployment Guide*
   - *RSA NetWitness® Suite AWS Deployment Guide*
   - *RSA NetWitness® Suite Azure Deployment Guide*
2. Go to **Administration** > **Hosts**.
   The **New Hosts** dialog is displayed with the hosts that you deployed.
3. Select the hosts that you want to enable.
   The **Enable** menu option becomes active.

4. Click **Enable**.

5. Select the host you enabled.
   The host is displayed in the Hosts view. At this point, you can install a service on the host.

Step 2. Install a Service on a Host

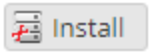
Each service is modeled as a plug-in to enable or disable according to the function of the host.

Prerequisites

Equipment, which can be physical or virtual, must be installed: NetWitness Server, Broker, Concentrator, Decoder, Log Decoder, Archiver, Warehouse, Malware Analysis server, or Event Stream Analysis server.

Procedure

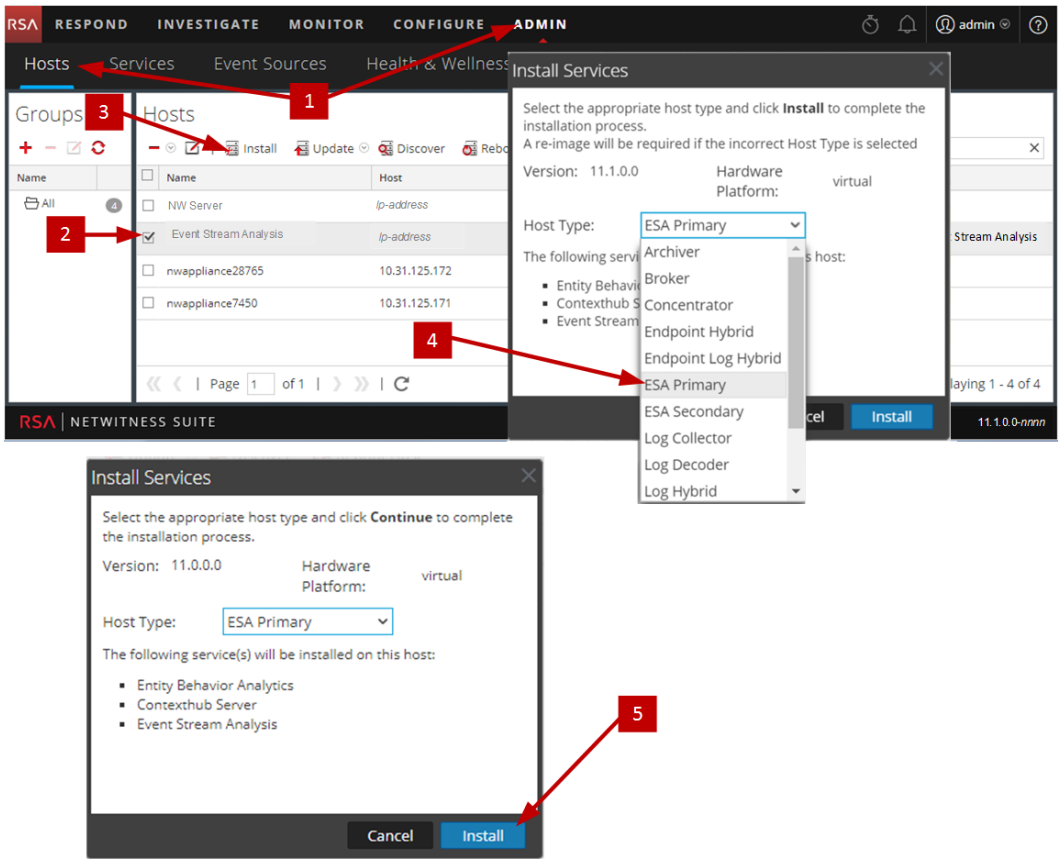
Perform the following steps to add a Service to a Host:

1. In NetWitness Suite, go to **ADMIN > Hosts**.
   The **Hosts** view is displayed.
2. Select the host on which you want to install the service (for example, **Event Stream Analysis**).
3. Click 

(Install Icon) in the toolbar.
   The **Install Services** dialog is displayed.
4. Select a service from the **Host Type** drop-down list (for example, **ESA Primary**).
   The

(Install command button) becomes active in **Install Services** dialog.

5. Click Install (Install command button).



Step 3. Review SSL Ports for Trusted Connections

To support trusted connections each core service has two ports, an unencrypted non-SSL port and an encrypted SSL port. Trusted connections require the encrypted SSL port.

Prerequisite

To establish a trusted connection, each NetWitness Suite Core service must be upgraded to 10.4 or later. Trusted connections are not backwards compatible with NetWitness Suite Core 10.3.x or earlier.

Encrypted SSL Ports

When you install or upgrade to 10.4 or later, trusted connections are established by default with two settings:

1. SSL is enabled.
2. The core service is connected to an encrypted SSL port.

Each NetWitness Suite Core service has two ports:

- Unencrypted **non-SSL port**
  Example: Archiver 50008
- Encrypted **SSL port**
  Example: Archiver 56008

The SSL port is the non-SSL port + 6000.

The following table lists all NetWitness Suite services with their respective ports and shows that each core service has two ports. All port numbers listed are TCP.

Service	Unencrypted Non-SSL Port	Encrypted SSL Port	Notes
Archiver	50008	56008	
Broker	50003	56003	
Cloud Gateway	N/A	N/A	
Concentrator	50005	56005	
Context Hub	N/A	50022	
Decoder (Packets)	50004	56004	
Endpoint	N/A	N/A	
Entity Behavior Analysis	N/A	N/A	
Event Stream Analysis	N/A	50030	
Investigate	N/A	N/A	Implemented with the NW Server.
Log Collector	50001	56001	

Service	Unencrypted Non-SSL Port	Encrypted SSL Port	Notes
Log Decoder	50002	56002	
Malware Analysis	N/A	60007	
Reporting Engine	N/A	N/A	Implemented with the NW Server.
Respond	N/A	N/A	Implemented with the NW Server.
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Step 4. Manage Access to a Service

In a trusted connection, a service explicitly trusts the NW Server to manage and authenticate users. With this trust, services in **ADMIN > Services** no longer require credentials to be defined for every NetWitness Suite Core service. Instead, users who have been authenticated by the server can access the service without entering another password.

Test a Trusted Connection

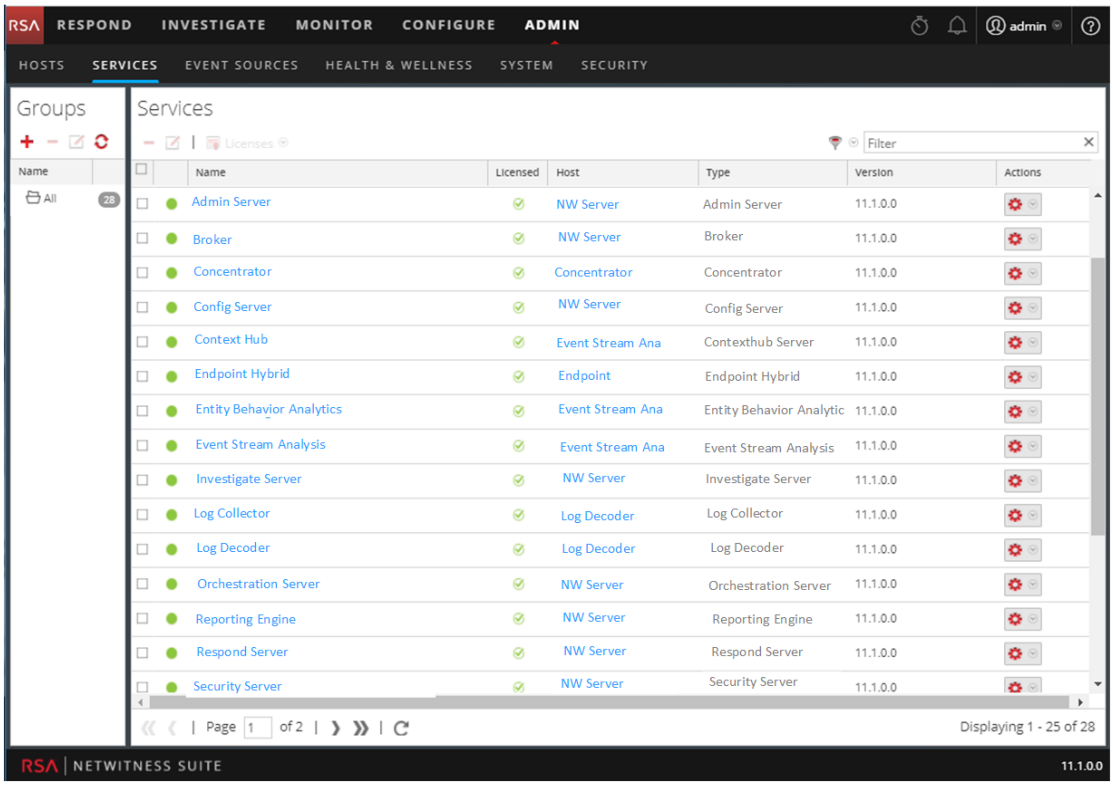
PREREQUISITES

1. A role must be assigned to the user.
   For details, see **Add a User and Assign a Role** topic in the *System Security and User Management Guide*.

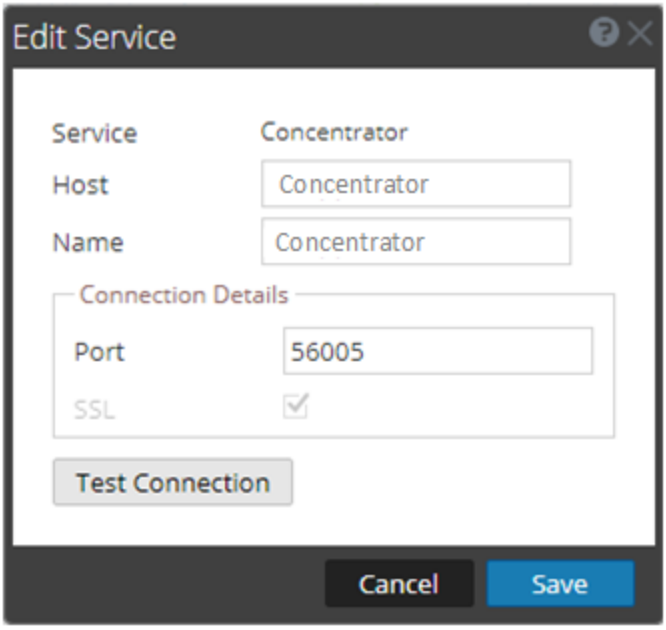
2. The user must:
   - Log on to NetWitness Suite to be authenticated by the server
   - Have access to the service

PROCEDURE

1. In NetWitness Suite, go to **ADMIN > Services**.
   The Services view is displayed.

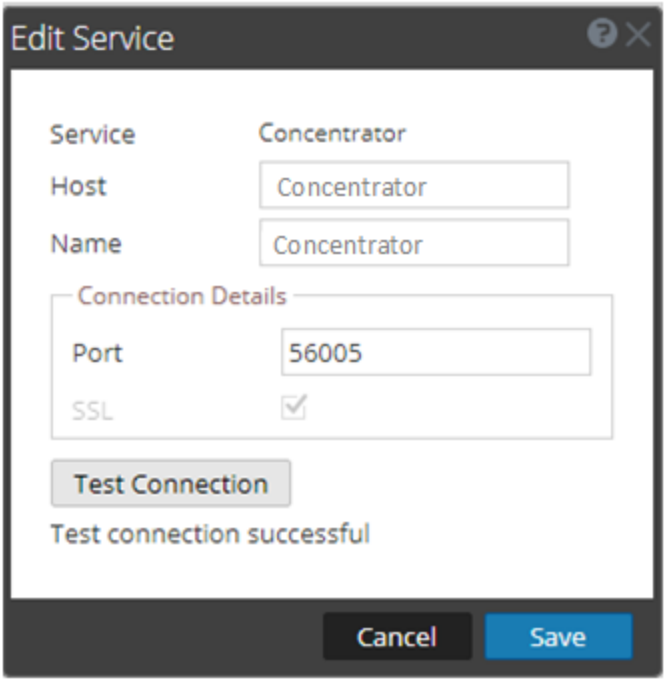


2. Select the service (for example, a Concentrator) to test and click .
   The **Edit Service** dialog is displayed.



3. If you did a fresh 11.0.0.0 install, the port is correct. No action is required in the **Port** field. Go to the next step.
   If you upgraded to 11.0.0.0 or have a mixed environment of a 11.0.0.0 server and 10.3 hosts, you must update the **Port** by deselecting and re-selecting **SSL**. Then, the **Port** number changes to the encrypted SSL port for the service.
4. Remove the **Username** to test the connection without credentials.

5. Click **Test Connection**.



The message **Test connection successful** confirms the trusted connection is established. The previously authenticated user can access the service without typing a username and password on the service.

6. Click **Save**.

Apply Version Updates to a Host

Complete the following tasks to update a host to a new version update.

There are two methods you can use to apply version updates to a host.

Note: If you have changed your location of the repo, refer to Set Up an External Repository with RSA and OS Updates for instructions.

- Apply updates from the Host view (Web Access)
- Apply update from the command line (No Web Access)

Apply Updates from the Hosts View (Web Access)

Task 1. Populate Local Repo or Set Up an External Repo

When you set up your NW Server, you select the Local Repo or an external repo. The Hosts view retrieves version updates from the repo you selected.

If you selected the Local Repo, you do not need to set it up, but you must make sure that it is populated with the latest version updates. See Populate Local Repository for instructions on how populate it with version update.

Note: If you selected an External Repo, you must set it up. See Set Up an External Repository with RSA and OS Updates for instructions on how to set up an external repo.

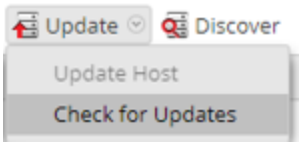
Task 2. Apply Updates from the Hosts View to Each Host

The Hosts view displays the software version updates available in your Local Update Repository and you choose and apply the updates you want from the Host view.

This procedure tells you how to update a host to a new version of NetWitness Suite.

Note: This topic uses NetWitness Suite 11.0.x.x to 11.1.0.0 as an example.

1. Log in to NetWitness Suite.
2. Go to **ADMIN > HOSTS**.
3. (Conditional) Check for the latest updates.

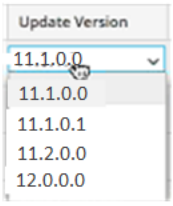


4. Select a host or hosts.

   You must update the NW Server to latest version first. You can update the other hosts in any sequence you prefer, but RSA recommends that you follow the guidelines in "Running in Mixed Mode" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for further information.

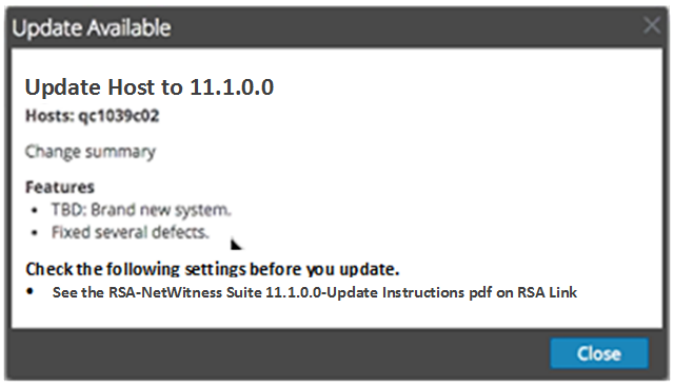
   Update Available is displayed in the **Status** column if you have an version update in your Local Update Repository for the selected hosts.

5. Select the version you want to apply from the **Update Version** column.



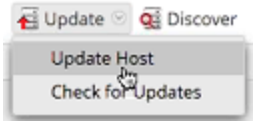
If you:

- Want to update more than one host to that version, after you update the NW Server host, select the checkbox to the left of the hosts. Only currently supported update versions are listed.
- Want to view a dialog with the major features in the update and information on the updates click the information icon ( ) to the right of the update version number. The following is an example of this dialog.

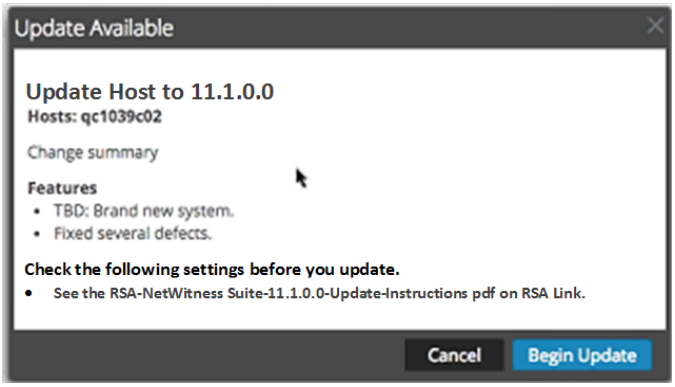


- Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show Update Available. By default, only supported updates for the selected host are displayed.

6. Click **Update > Update Host** from the toolbar.



A dialog is displayed with information on the selected update. Click **Begin Update**.



The **Status** column tells you what is happening in each of the following stages of the update:

- Stage 1 - **Downloading update packages** - downloads the repository artifacts to the NW Server applicable to the services on the host you chose.
- Stage 2 - **Configuring update packages** - configures update files in to correct format.
- Stage 3 - **Update in progress** - updates host to new version.

7. When you see **Update in progress**, refresh the browser.
   This may send you to the NetWitness Log In screen. If this happens, log in and navigate back to the Host view.
   After the host is updated, NetWitness Suite prompts you to **Reboot Host**.
8. Click **Reboot Host** from the toolbar.
   NetWitness Suite shows the status as **Rebooting...** until the host comes back online. After the host comes back online, the **Status** shows **Up-to-Date**. Contact Customer Care if the host does not come back online.

Note: If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates.

Apply Updates from the Command Line (No Web Access)

If your RSA NetWitness Suite deployment does not have Web access, complete the following procedure to apply a version update.

Note: In the following procedure, 11.1.0.0 is the version update used as an example in the code strings.

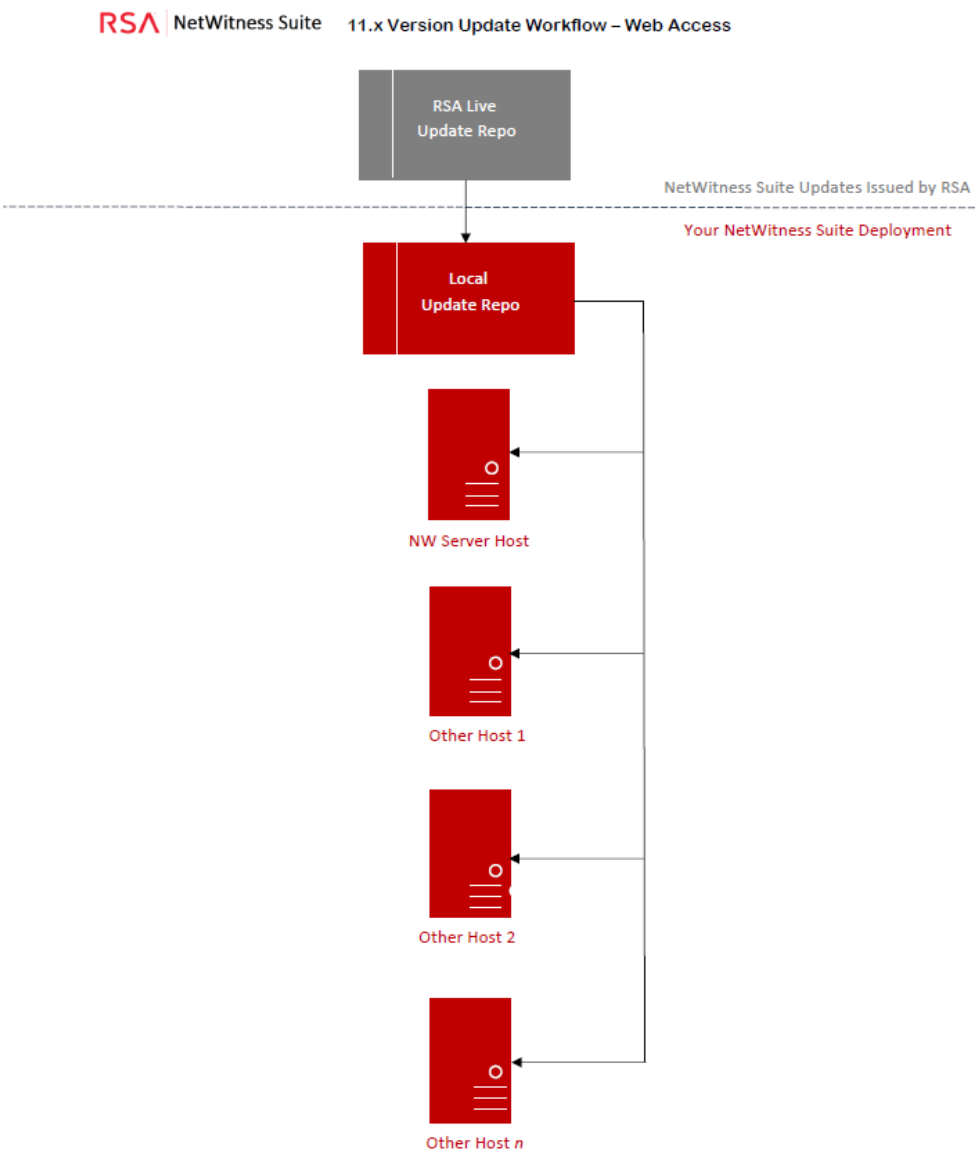
1. Download `.zip` update package for the version you want (for example, `netwitness-11.1.0.0.zip`) from RSA Link to a local directory.
2. SSH to the NW Server host.

3. Make a `tmp/upgrade/<version>` staging directory for the version you want (for example, `tmp/upgrade/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Unzip the package into the staging directory you created (for example, `tmp/upgrade/11.1.0.0`) .
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Initialize the update on the NW Server.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Apply the update to the NW Server.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Log in to NetWitnesss Suite and reboot the NW Server host in the Host View.
8. Apply update to each non-NW Server host.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   The update is complete when the polling is completed.
9. Log in to NetWitnesss Suite and reboot the host in the Host View.
   You can verify the version applied to the host with the following command:
   ```
   upgrade-cli-client --list
   ```

Populate Local Update Repository

NetWitness Suite sends version updates to the Local Update Repository from the Live Update Repository. Access to the Live Update Repository requires and uses the Live Account credentials configured under **ADMIN > SYSTEM > Live**. In addition, you must check the `Automatically download information about new updates every day` checkbox under **ADMIN > SYSTEM > Updates** to populate the Local Repo daily.

The following diagram illustrates how you obtain version updates if your NetWitness Suite deployment has Web Access.



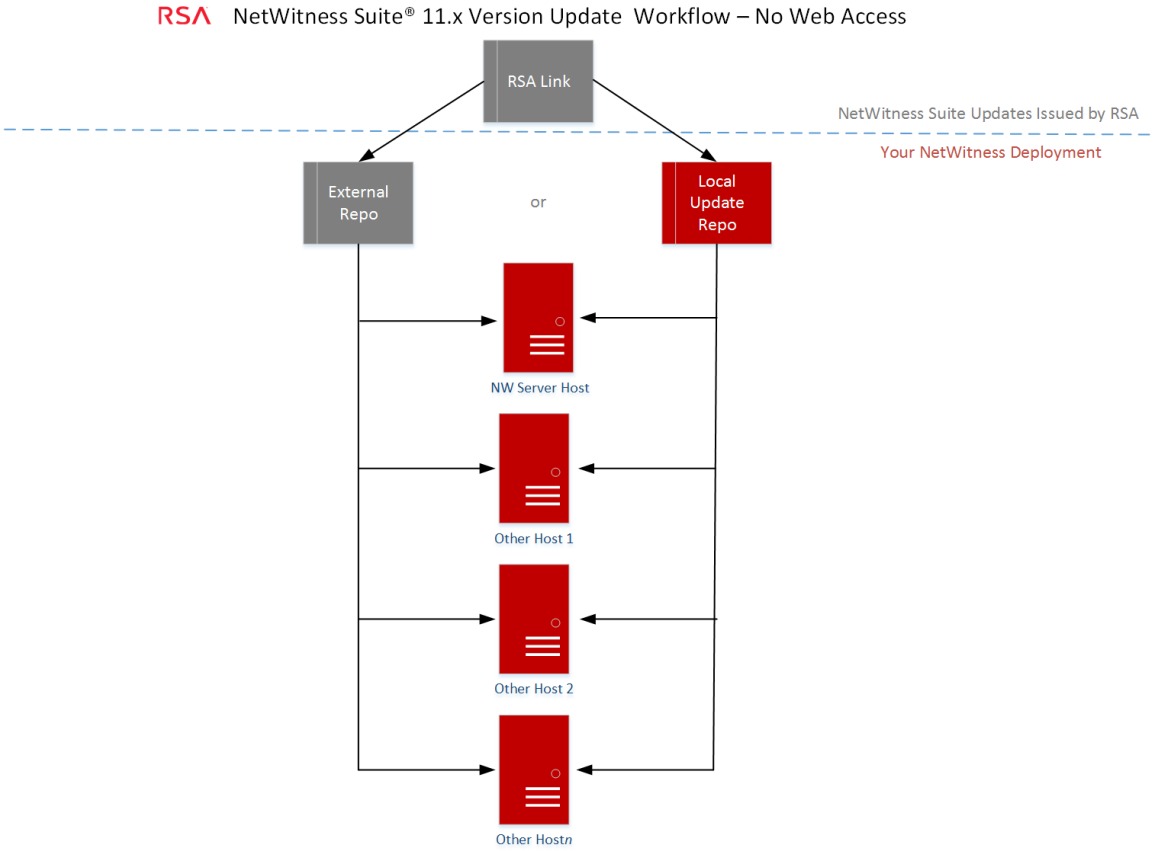
Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 7 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your NW Server Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository. Alternatively you can use an External Repo as described in "Set Up an External Repo."

To connect to the Live Update Repository, Navigate to the **ADMIN > SYSTEM** view, select **Live** in the options panel and ensure that credentials are configured (**Connection** light should be green). If it is not green, click **Sign In** and connect.

Note: If you need to use proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. Refer to "Configure Proxy forNetWitness Suite" in the *NetWitness Suite 1.1 System Configuration Guide*.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

See "Apply Updates from Command Line" if your NetWitness Suite deployment does not have Web Access.

The following diagram illustrates how you obtain version updates if your NetWitness Suite deployment does not have Web Access.



Set Up an External Repository with RSA and OS Updates

Note: In the following procedure, 11.1.0.0 is the version update used as an example in the code strings.

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step If you have an external repo and you want to override it.
   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/platform/netwitness/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
        See for the instructions.
   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/platform/netwitness/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
        The instructions are in the "Apply Updates from the Command Line" under topic.
2. Set up the external repo.
   a. Log in to the web server host
   b. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo`under `web-root` of the web server. For example, /var/netwitness is the web-root, submit the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
   e. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.

```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

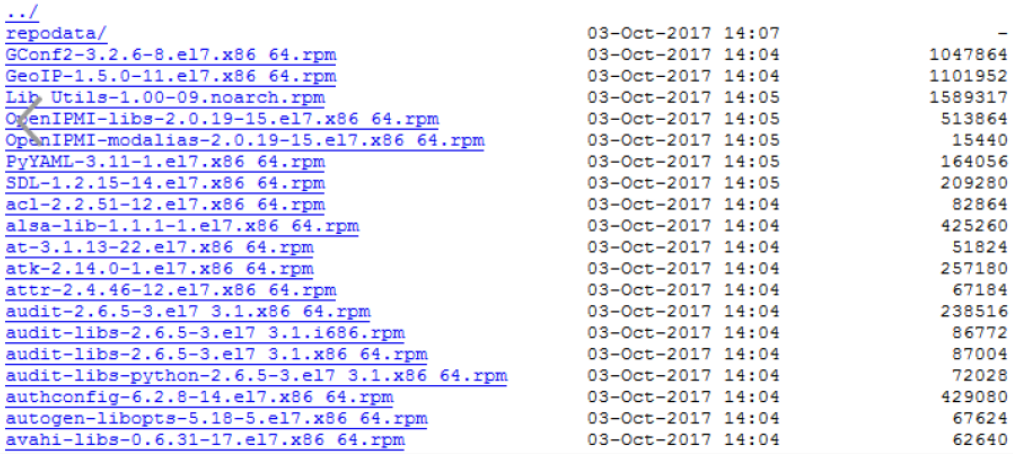
Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.

f. Unzip the:

1. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.

   ```
   unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
   ```

   The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.



../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

   ```
   unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
   ```

   The following example illustrates how the RSA version update file structure will

appear after you unzip the file.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

g. (Conditional - For Azure) Follow these steps for Azure update

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`

iv. `createrepo .`

h. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Create and Manage Host Groups

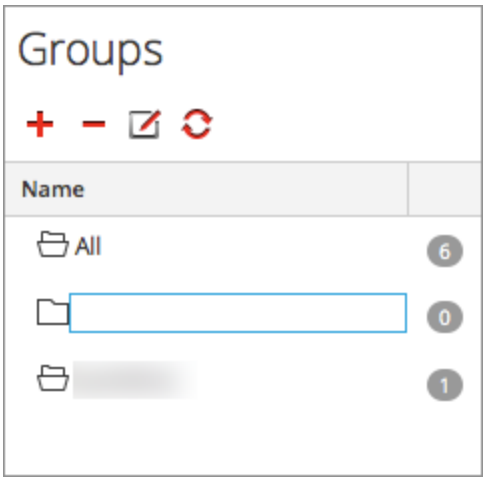
The Hosts view provides options for creating and managing groups of hosts. The Groups panel toolbar includes options for creating, editing, and deleting host groups. Once groups are created, you can drag individual hosts from the Hosts panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A host may belong to more than one group. Here are some examples of possible groupings:

- Group different host types to make it easier to configure and monitor all Brokers, Decoders, or Concentrators.
- Group hosts that are part of the same data flow; for example, a Broker, and all associated Concentrators and Decoders.
- Group hosts according to their geographic region and location within the region. If a major power outage occurs in a location, potentially affected hosts are easily identifiable.

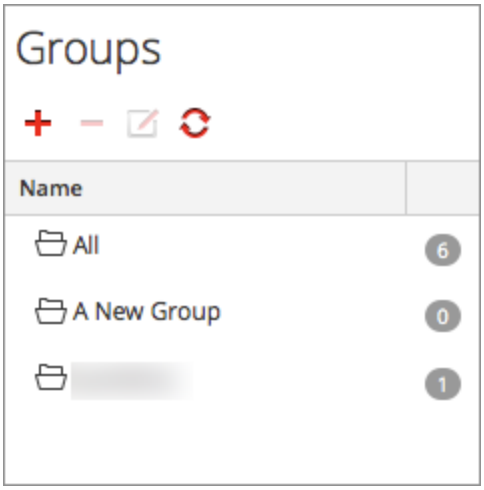
Create a Group

1. Select **ADMIN** > **Hosts**.
   The Hosts view is displayed.
2. In the **Groups** panel toolbar, click +.
   A field for the new group opens with a blinking cursor.



3. Type the name of the new group in the field (for example, **A New Group**) and press **Enter**.
   The group is created as a folder in the tree. The number next to the group indicates the

number of hosts in that group.



Change the Name of a Group

1. In the Hosts view **Groups** panel, double-click the group name or select the group and click .

   The name field opens with a blinking cursor.

2. Type the new name of the group and press **Enter**.

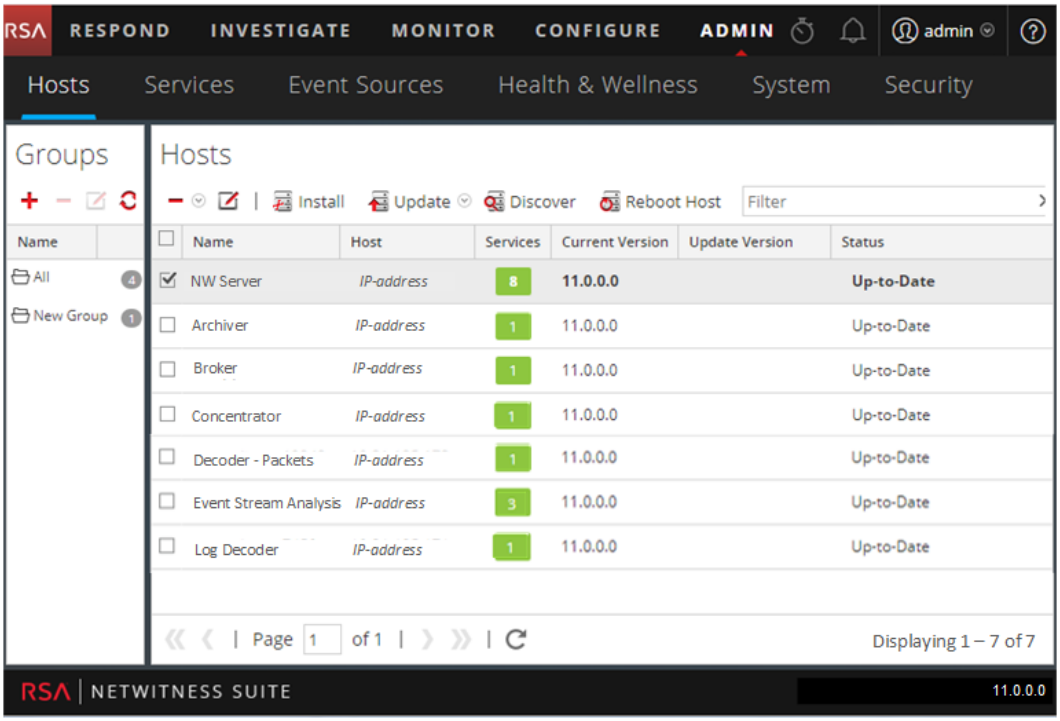
   The name field closes and the new group name is displayed in the tree.

Add a Host to a Group

In the Hosts view **Hosts** panel, select a host and drag the host to a group folder in the Groups panel.
The host is added to the group.

View the Hosts in a Group

To view the hosts in a group, click the group in the **Groups panel**.
The **Hosts panel** lists the hosts in that group.

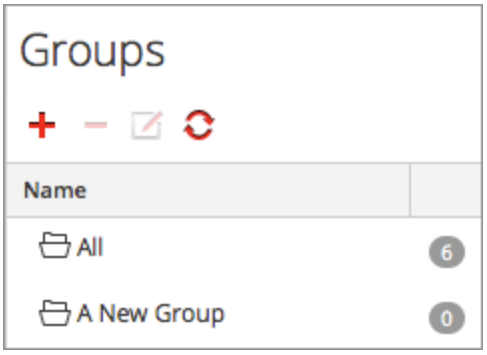


Remove a Host from a Group

1. In the Hosts view **Groups panel**, select the group that contains the host that you want to remove. The hosts in that group appear in the Hosts panel.
2. In the **Hosts panel**, select one or more hosts that you want to remove from the group, and in the toolbar, select > **Remove fromGroup**.

   The selected hosts are removed from the group, but are not removed from the NetWitness Suite user interface. The number of hosts in the group, which is listed near the group name, decreases by the number of hosts removed from the group. The **All** group contains the hosts that were removed from the group.

   In the following example, the host group called **A New Group** does not contain any hosts, since the host in that group was removed.



Delete a Group

1. In the Hosts view **Groups panel**, select the group that you want to delete.
2. Click .

   The selected group is removed from the Groups panel. The hosts that were in the group are not removed from the NetWitness Suite user interface. The **All** group contains the hosts from the deleted group.

Search for Hosts

You can search for hosts from a list of hosts in the Hosts view. The Hosts view enables you quickly filter the list of hosts by Name and Host. It is possible to have numerous NetWitness Suite hosts in use for various purposes. Instead of scrolling through the host list, you can quickly filter the host list to locate the hosts that you want to administer.

In the Services view, you can search for a service and quickly find the host that runs that service.

Search for a Host

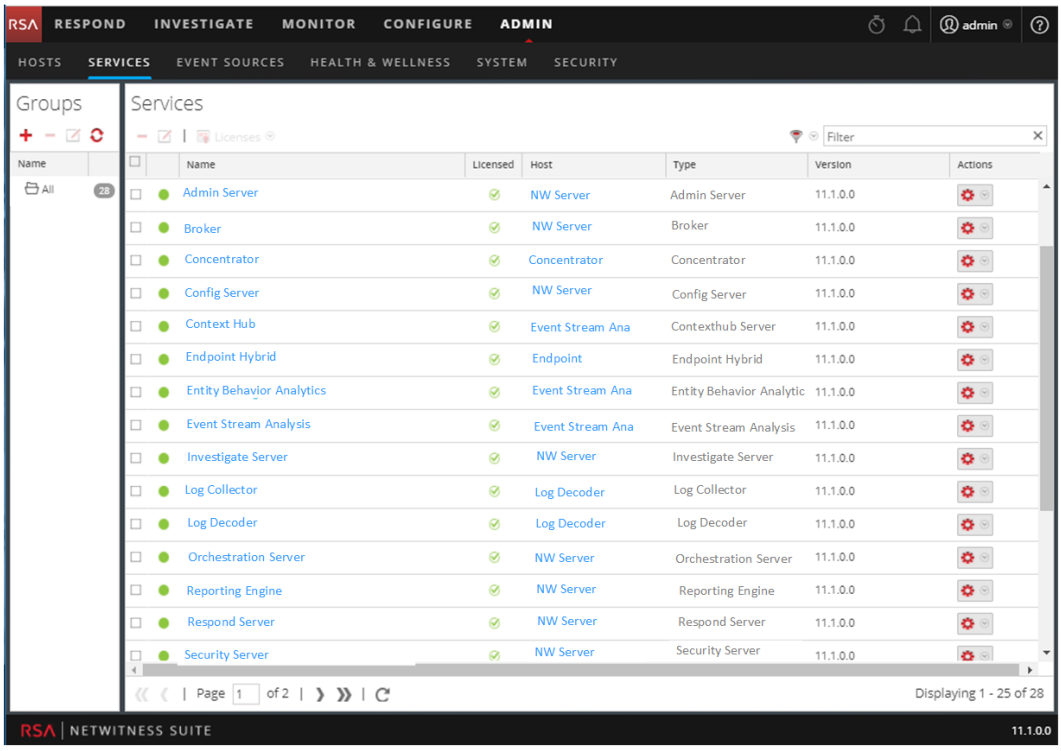
1. Select **ADMIN** > **Hosts**.
2. In the **Hosts Panel** toolbar, type a host **Name** or **Hostname** in the **Filter** field.

   The Hosts panel lists the hosts that match the names entered in the Filter field.

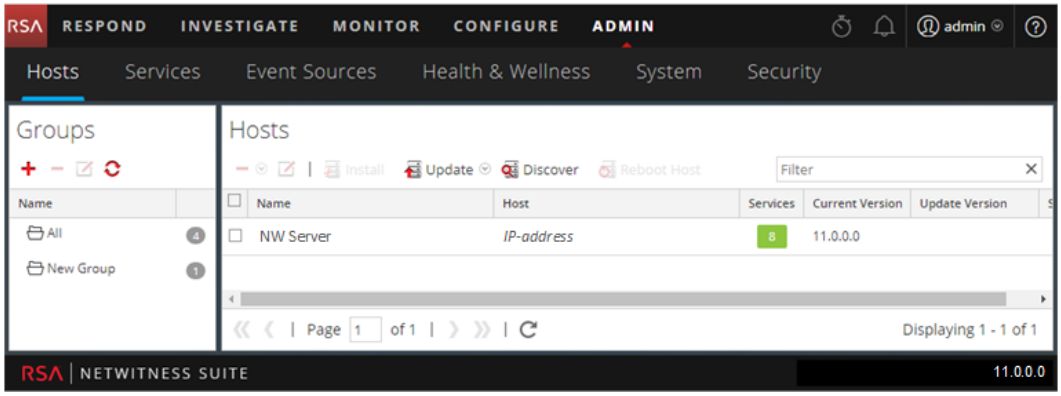
Find the Host that Runs a Service

1. Select **ADMIN** > **Services**.

2. In the Services view, select a service. The associated host is listed in the **Host** column for that service.



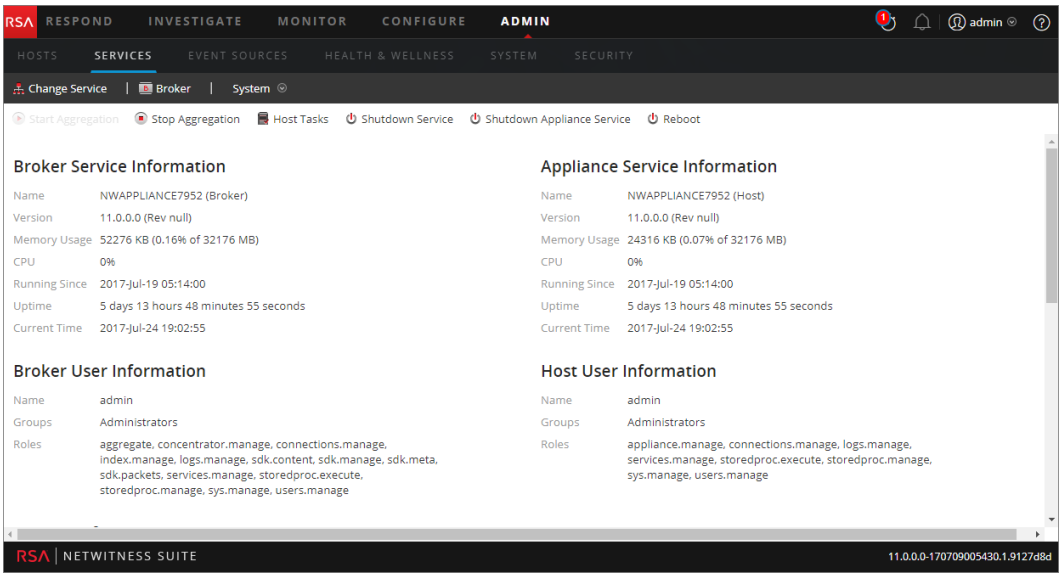
3. To administer the host in the Hosts view, click the link in the **Host** column for that service. The host associated with the selected service is displayed in the Hosts view.



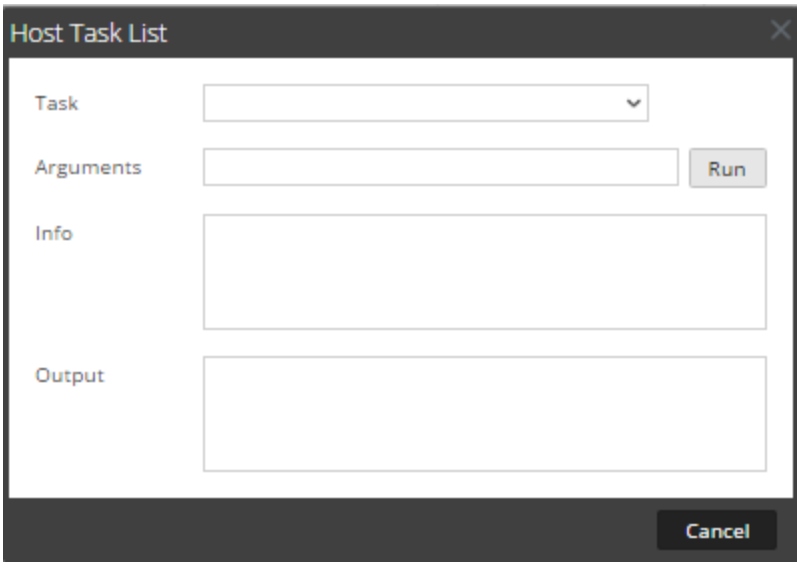
Execute a Task From the Host Task List

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View** > **System**.

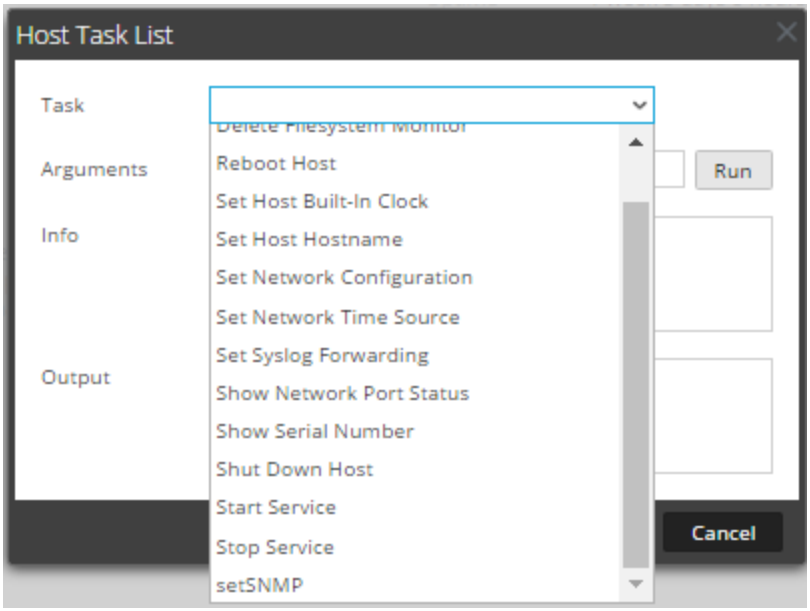
Note: The Admin, Config, Orchestration, Security, Investigate, and Respond services do have access to the System view. They only have access to the Explore view.
The System view for the service is displayed.



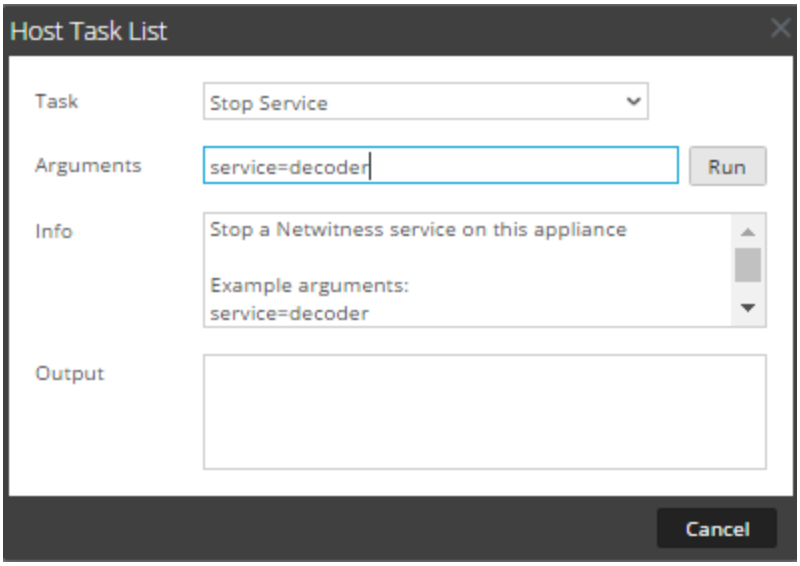
3. In the **Services System** view toolbar, click Host Tasks.



4. In the **Host Task List,** click in the **Task** field to display a drop-down list of tasks that run on a host.



5. Select a task; for example, click **Stop Service**.
   The task is displayed in the **Task** field and task description, example arguments, security roles, and parameters are displayed in the **Info** area.



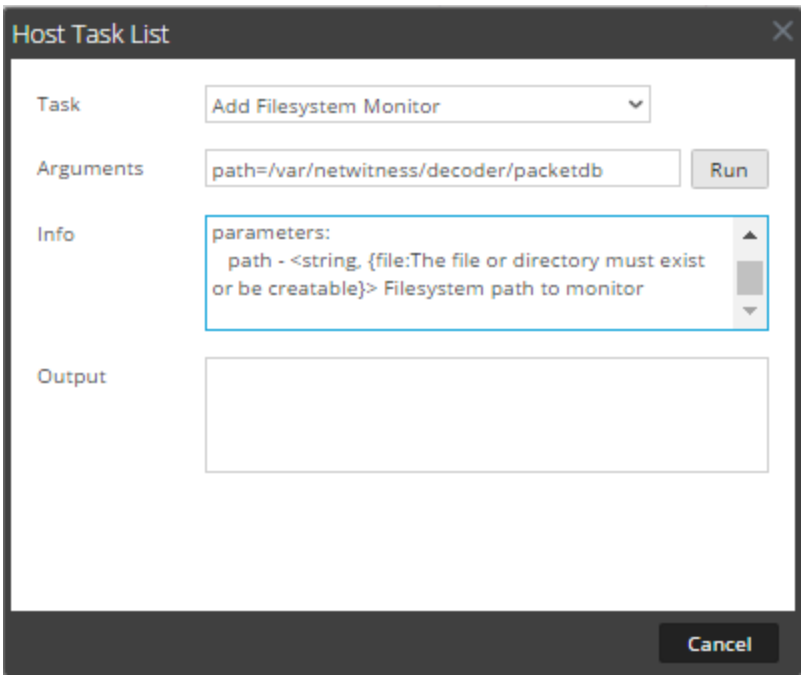
6. Type arguments if necessary and click **Run**.
   The command executes and the result is displayed in the **Output** section.

Add and Delete a Filesystem Monitor

When you want a service to monitor traffic on a specific file system, you can select the service and then specify the path. Security Analytics adds a filesystem monitor. Once a file system monitor is added to a service, the service continues to monitor traffic on that path until the file system monitor is deleted.

Configure the Filesystem Monitor

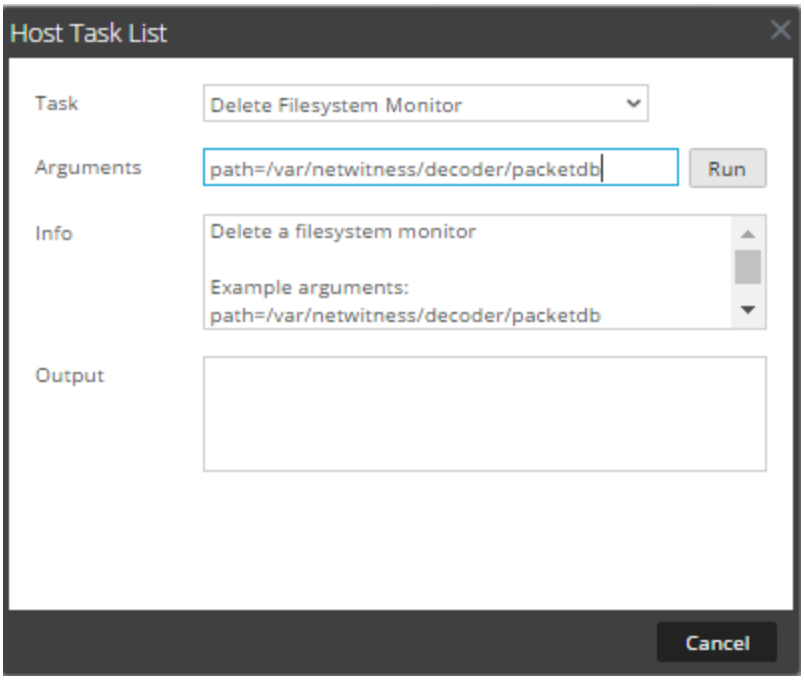
1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View** > **System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Add Filesystem Monitor**.
   In the **Info** area, a brief explanation of the task and the task arguments is displayed.
5. To identify the file system to monitor, type the path in the **Arguments** field. For example: **path=/var/netwitness/decoder/packetdb**



6. Click **Run**.
   The result is displayed in the **Output** area. The service begins to monitor the file system and continues to monitor it until you delete the filesystem monitor.

Delete a Filesystem Monitor

1. Navigate to the **Host Task List** dialog.
2. In the **Host Task List**, select **Delete Filesystem Monitor**.
   In the **Info** area, a brief explanation of the task and the task arguments is displayed.
3. To identify the filesystem to stop monitoring, type the path in the **Arguments** field. For example:
   path=/var/netwitness/decoder/packetdb



4. Click **Run**.
   The result is displayed in the **Output** area. The service stops monitoring the file system.

Reboot a Host

Under certain conditions it is necessary to reboot a host; for example, after installing a software upgrade. This procedure uses a Host Task List message to shut down and restart a host.

Security Analytics also offers other options for shutting down a host:

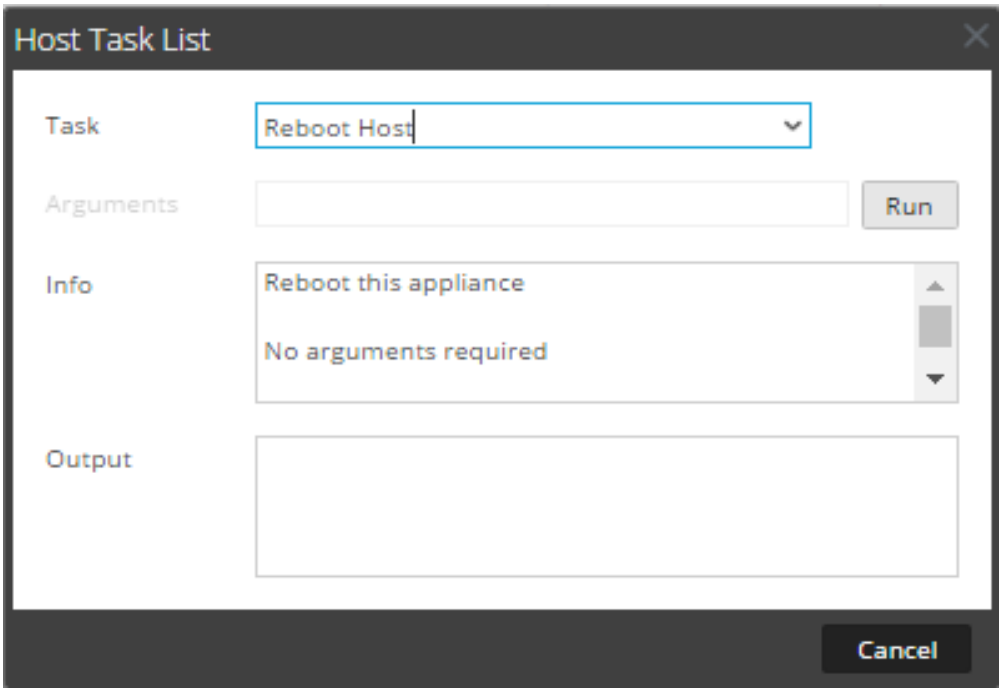
- To shut down and restart a host through an attached service, go to the Hosts view from a service in the Services view (see Search for Hosts) and then follow the *Shut Down and Restart a Host from the Hosts View* procedure below.
- To shut down the physical host without restarting, see Shut Down Host.

Shut Down and Restart a Host from the Hosts View

1. Select **ADMIN > Hosts**.
2. In the **Hosts** panel, select a host.
3. Select Reboot Host from the toolbar.

Shut Down and Restart a Host from the Host Task List

1. Select **ADMIN** > **Services**.
2. In the **Services** panel, select a service and click > **View** > **System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Reboot Host** in the **Task** field.
   No arguments are required.



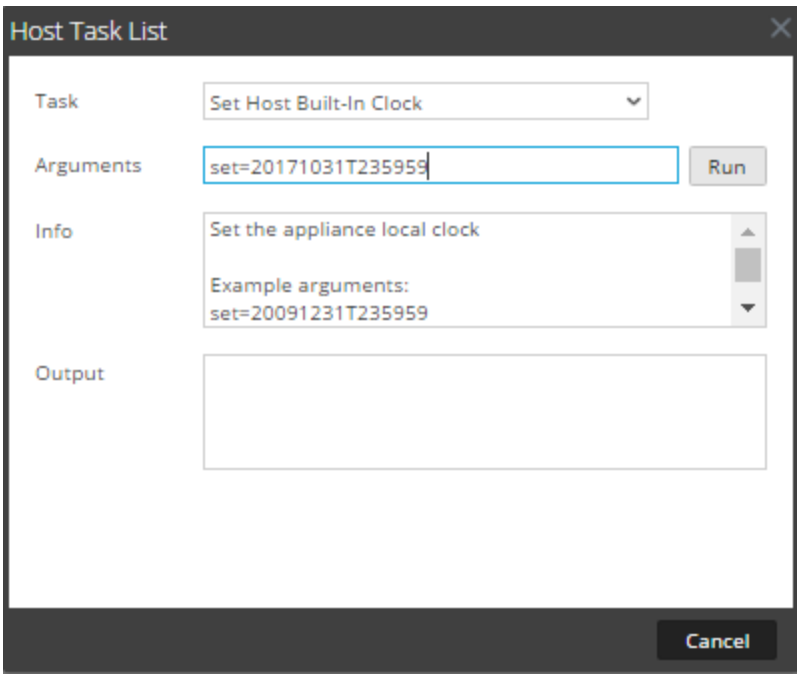
5. Click **Run**.
   The host is rebooted and the result is displayed in the **Output** area.

Set Host Built-In Clock

After a shutdown or battery failure, it may be necessary to set the local clock on a host. The Set Host Built-In Clock task resets the clock time.

Set the Time on the Local Clock

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and > **View** > **System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Set Host Built-In Clock**. Help for the task is displayed in the **Info** area.
5. Enter the date and time arguments in the **Arguments** field; for example, to specify October 31, 2017 at 11:59:59 PM, type:
   set=20171031T235959



6. Click **Run**.
   The clock is set to the specified time and a message is displayed in the **Output** area.

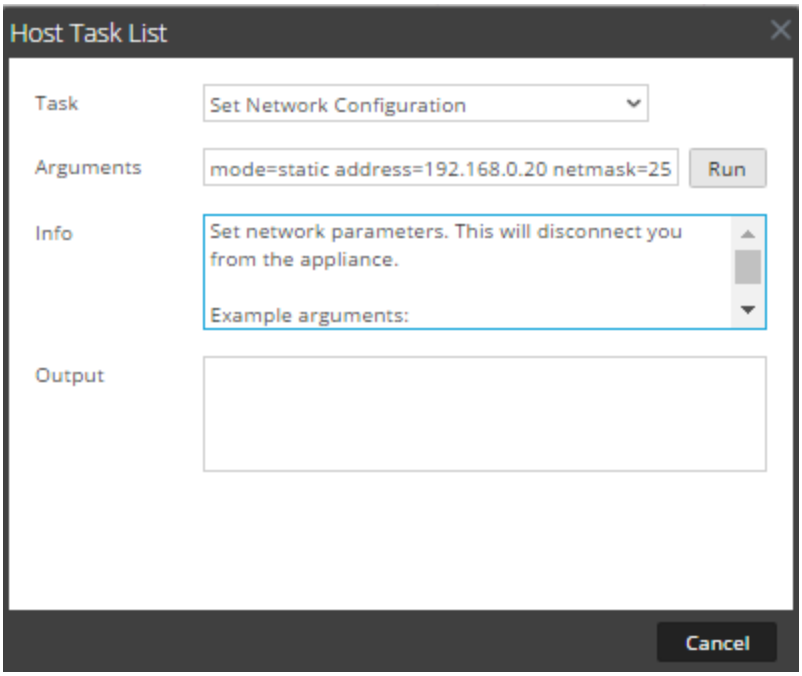
Set Network Configuration

When a configured Core host needs its address changed, you can set a new network address, subnet mask, and gateway for the host using the **Set Network Configuration** message in the **Host Task List**.

Caution: The change goes into effect immediately, and the host is disconnected from Security Analytics. You must then add the host to Security Analytics again using the new network address.

Specify the Network Address for a Host

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View System**.
   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, click **Set Network Configuration**.
   The task is displayed in the **Task** field and help is displayed in the **Info** area.
5. Enter the arguments in the **Arguments** field. For example:
   mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1



6. Click **Run.**
   The task executes and the result is displayed in the **Output** area. The host is disconnected from Security Analytics. You must add the host again with the new address.

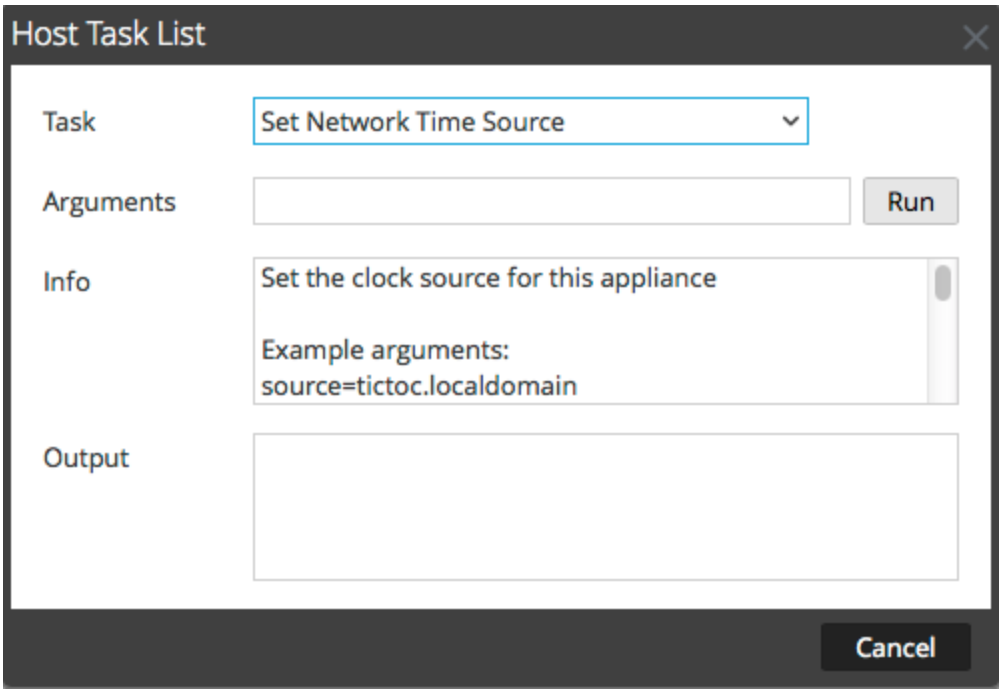
Note: If the mode is DHCP, there may be no way to determine the new address. You may have to connect to the host directly to determine the new address.

Set Network Time Source

When setting the clock source for a host, set the hostname or address of an NTP server to be the network clock source for the host. If the host is using a local clock source, you must specify **local** here to allow **Set the Local Clock Source** to be effective.

Specify the Network Clock Source

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click **View > System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Set Network Time Source**.



5. Do one of the following:
   - Type the hostname or address of the NTP server to serve as the clock source for this host; for example: **source=tictoc.localdomain**
   - If you want to use the host clock as a clock source, type: **source=local**
6. Click **Run**.
   The clock source is set and a message is displayed in the **Output** area.

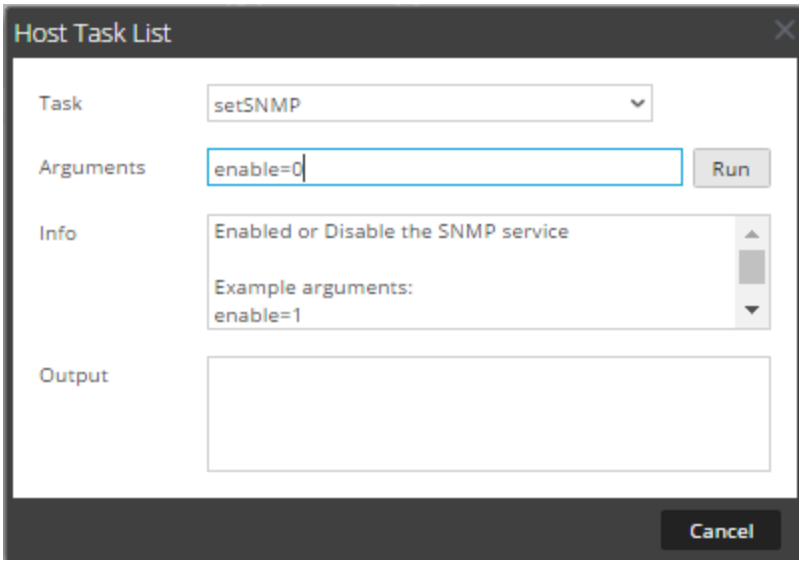
Note: If you specified a NTP clock source of **local**, the host clock serves as the clock source and the time is configured using Set Host Built-In Clock.

Set SNMP

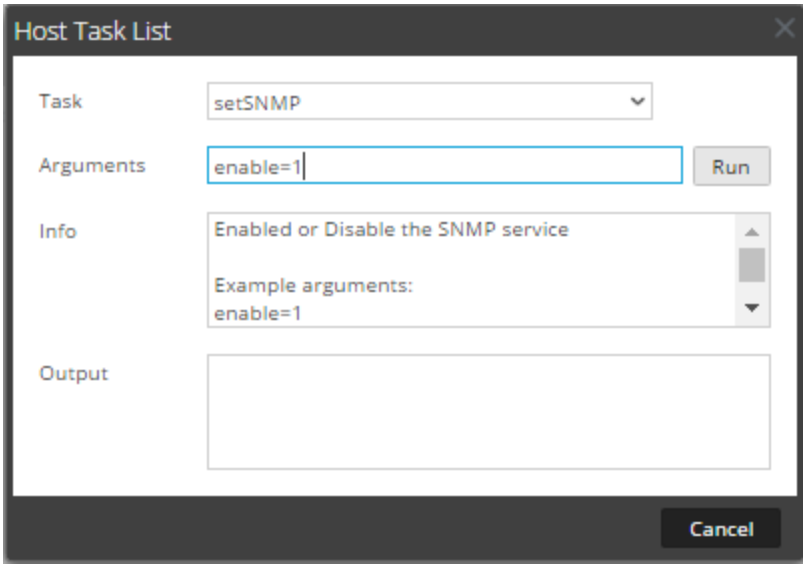
Set SNMP in the Host Task List enables or disables the SNMP service on a host. In order for a host to receive SNMP notifications, the SNMP service needs to be enabled. If you are not using SNMP for NetWitness Suite notifications, it is not necessary to enable the service.

Toggle SNMP Service on the Host

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View** > **System**.
   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **setSNMP**.
   In the **Info** area, a brief explanation of the task and the task arguments is displayed.
5. Do one of the following:
   - If you want to disable the service, type **enable=0** in the **Arguments** field.



- If you want to enable the service, type **enable=1** in the **Arguments** field.



6. Click **Run**.
   The result is displayed in the **Output** area.

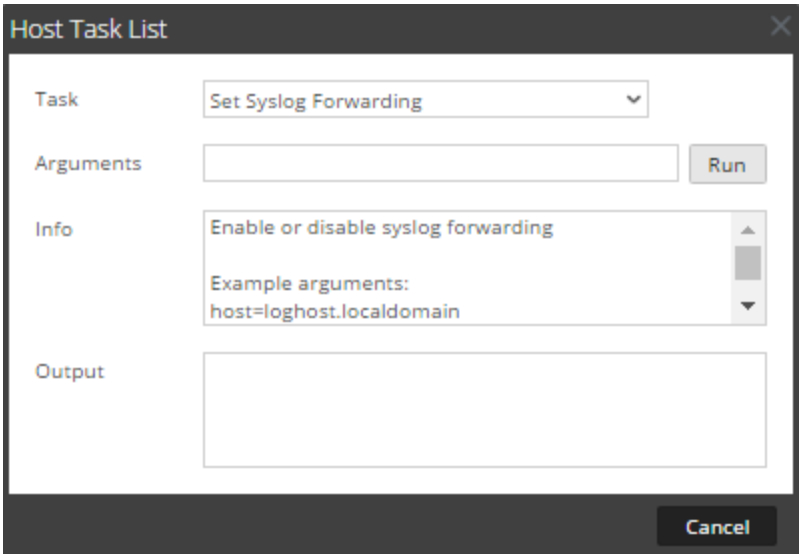
Set Syslog Forwarding

You can configure Syslog forwarding to forward the operating system logs of your NetWitness Suite Hosts to a remote syslog server. You can use the Set Syslog Forwarding task in the Host Task List to enable or disable syslog forwarding.

Set Up and Start Syslog Forwarding

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View** > **System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.

4. In the **Host Task List**, select **Set Syslog Forwarding**.
   In the **Info** area, a brief explanation of the task and the task arguments is displayed.



5. In the **Arguments** field, do any one of the following.
   - To enable syslog forwarding, specify any one of the following formats:
     - **host=<loghost>.<localdomain>** (for example, host=syslogserver.local).
     - **host=<loghost>.<localdomain>:<port>** (for example, host=syslogserver.local:514).
     - **host=<IP>** (for example, host=10.31.244.244).
     - **host=<IP>:<port>** (for example, host=10.31.244.244:514).
       The following table lists the parameters used to enable syslog forwarding and its descriptions.

Parameter	Description
loghost	The host name of the remote syslog server.
localdomain	The domain of the remote syslog server.
port	IP address of the remote syslog server.
IP	The port number on which the remote syslog server receives a syslog messages.

   - To disable syslog forwarding, type **host=disable**.
6. Click **Run**.
   The result is displayed in the **Output** area.

Once syslog forwarding is enabled or disabled, the `/etc/rsyslog.conf` file is updated automatically to enable or disable syslog forwarding to the remote syslog destination and the syslog service is restarted.

If you enable syslog forwarding, the logs from the configured service are forwarded to the defined syslog server and continues forwarding until disabled.

Note: You can now log in to the remote syslog server and verify if the messages are being received from the NetWitness Suite services configured for syslog forwarding.

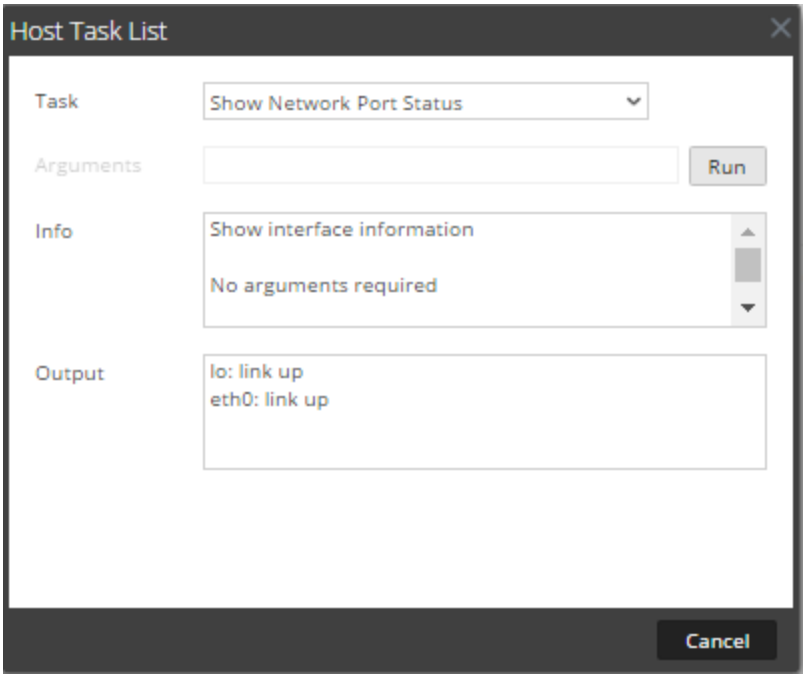
Show Network Port Status

The Show Network Port Status task in the Host Task List gives you the status of all configured ports on the host.

Display the Network Port Status

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and > **View**> **System**.
   The System view for the selected service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, click **Show Network Port Status**.
   The task is displayed in the **Task** field, and information about the task is displayed in the **Info** area.

5. To execute the task, click **Run**.
   The status for each port on the host is displayed in the **Output** area.



Show Serial Number

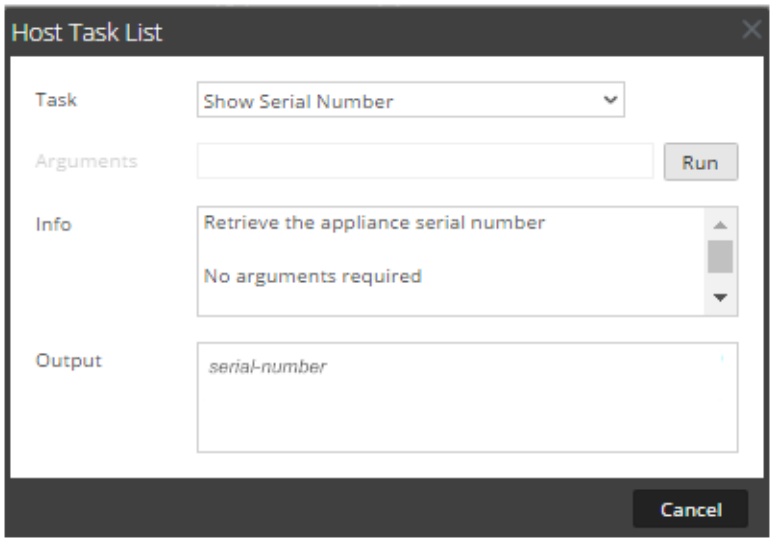
The Show Serial Number task in the Host Task List gives you the serial number of a host.

Show the Serial Number

1. Select **ADMIN > Services**.
2. In the **Services** grid, select a service and click > **View> System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Show Serial Number**.
   In the **Info** area, a brief explanation of the task and the task arguments is displayed.

5. No arguments are required for this task. Click **Run**.

   The serial number of the selected host is displayed in the **Output** area.



Shut Down Host

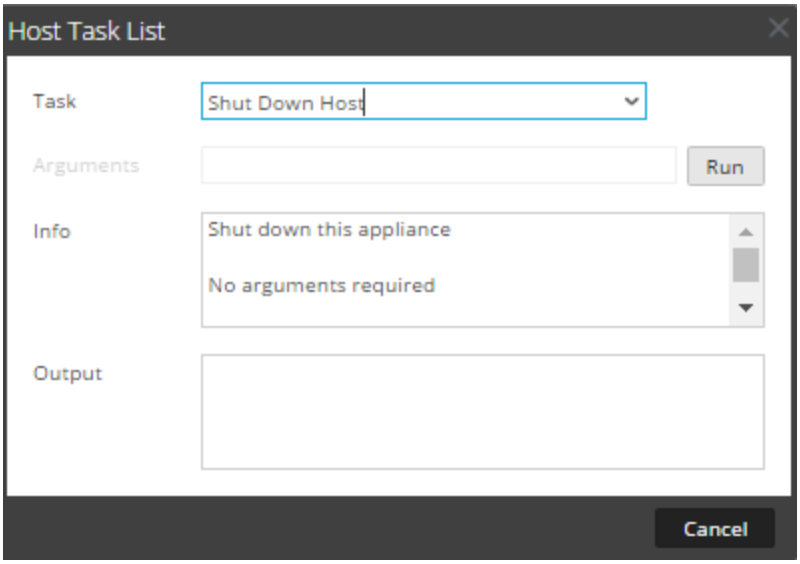
Under certain circumstances; for example, a hardware upgrade or an extended power outage that exceeds backup power capacity, it may be necessary to shut down a physical host. When you shut down a host, all services running on the host are stopped and the physical host turns off.

The physical host does not restart automatically; instead the power switch must be used to restart the host. Once the physical host restarts, the host and services are configured to restart automatically.

Reboot a Host to start and stop a host without shutting down the host.

Shut Down the Host

1. In the Host Task List dialog, select **Shut Down Host** in the **Task** field.



2. To execute the task, click **Run**.
   The host shuts down, and the host turns off.

Stop and Start a Service on a Host

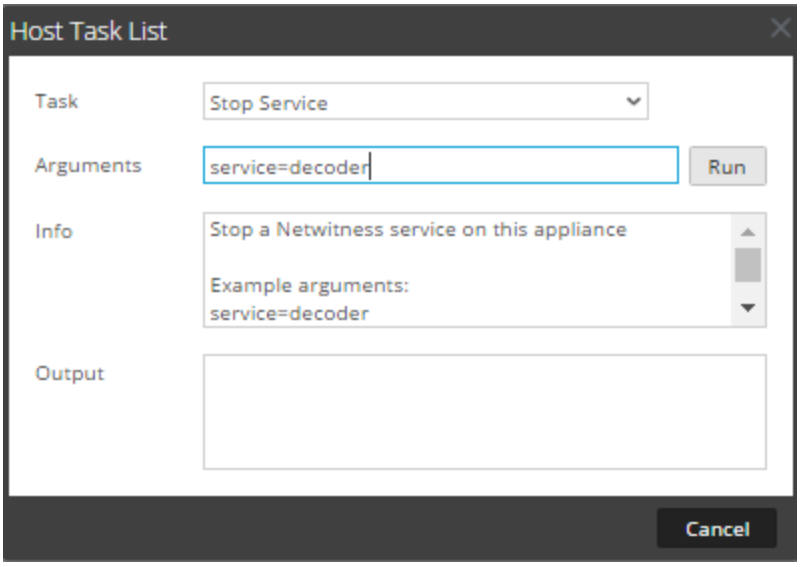
The Host Task List has two options for stopping and starting a service on a host. When you stop a service using the **Stop Service** message, all processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically. This is the same as the **Shutdown Service** option in the Services System view.

If a service does not restart automatically after being stopped, you can restart it manually using the **Start Service** message.

Stop a Service on a Host

1. Select **ADMIN** > **Services**.
2. In the **Services** grid, select a service and click > **View**> **System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, click **Stop Service**.
   The task is displayed in the **Task** field, and information about the task is displayed in the **info** area.

5. Specify the service (decoder, concentrator, broker, logdecoder, logcollector) to stop in the **Arguments** field; for example, **service=decoder**.

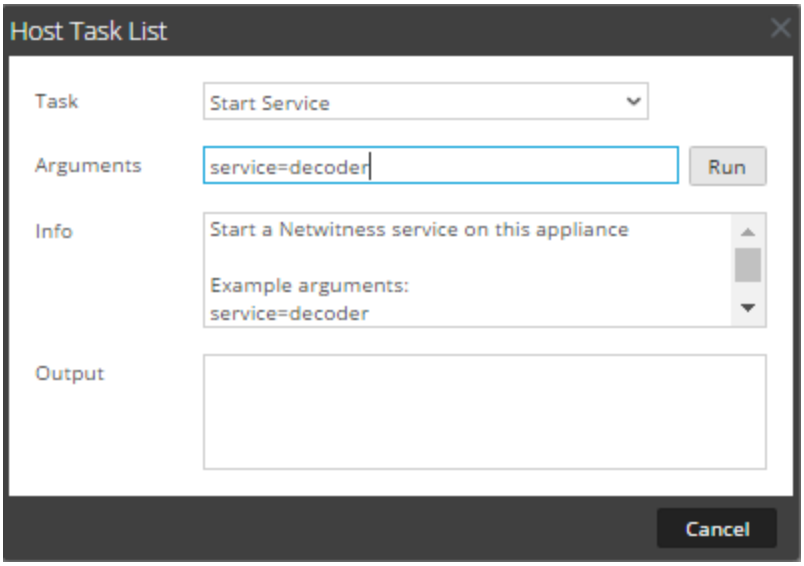


6. To execute the task, click **Run**.
   The service stops and the status is displayed in the **Output** area. All processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically.

Start a Service on a Host

1. In the **Host Task List**, select **Start Service** from the Task drop-down menu.
   The task is displayed in the **Task** field, and information about the task is displayed in the **info** area.
2. Specify the service (decoder, concentrator, broker, logdecoder, logcollector) to start in the **Arguments** field; for example,

service=decoder



3. To execute the task, click **Run**.
   The service starts and the status is displayed on the **Output** area.

Add, Replicate or Delete a Service User

You must add a user to a service for:

- Aggregation
- Accessing the service with the:
  - Thick client
  - REST API

Note: This topic does not apply to users who access services through the user interface on NetWitness Server. You must add those users to the system, not a service. For details, see the **Set Up a User** topic in *System Security and User Management*.

For each service user, you can:

- Configure user authentication and query handling properties for the service
- Make the user a member of a role, which has a set of permissions the user receives
- Replicate the user account to other services
- Change the service user password on selected services

Change a Service User Password provides instructions for changing the service user password across services.

Replication and Migration Considerations

When replicating a user from a NetWitness Suite 10.5 or later service to a NetWitness Suite 10.4 service, Query Timeout migrates to Query Level based on the closest level. For example, if a user has a Query Timeout of 15 minutes, the user gets a Query Level of 3 after the migration. If a user has a Query Timeout of 35 minutes, the user gets a Query Level of 2 after the migration. If a user has a Query Timeout of 45 minutes, the user gets a Query Level of 2 after the migration.

When migrating or replicating a user from a NetWitness Suite 10.4 service to a NetWitness Suite 10.5 or later service, Query Level migrates to Query Timeout based on the following definitions:

- Query Level 1 = 60 minutes
- Query Level 2 = 40 minutes
- Query Level 3 = 20 minutes

Procedures

ACCESS THE SECURITY VIEW

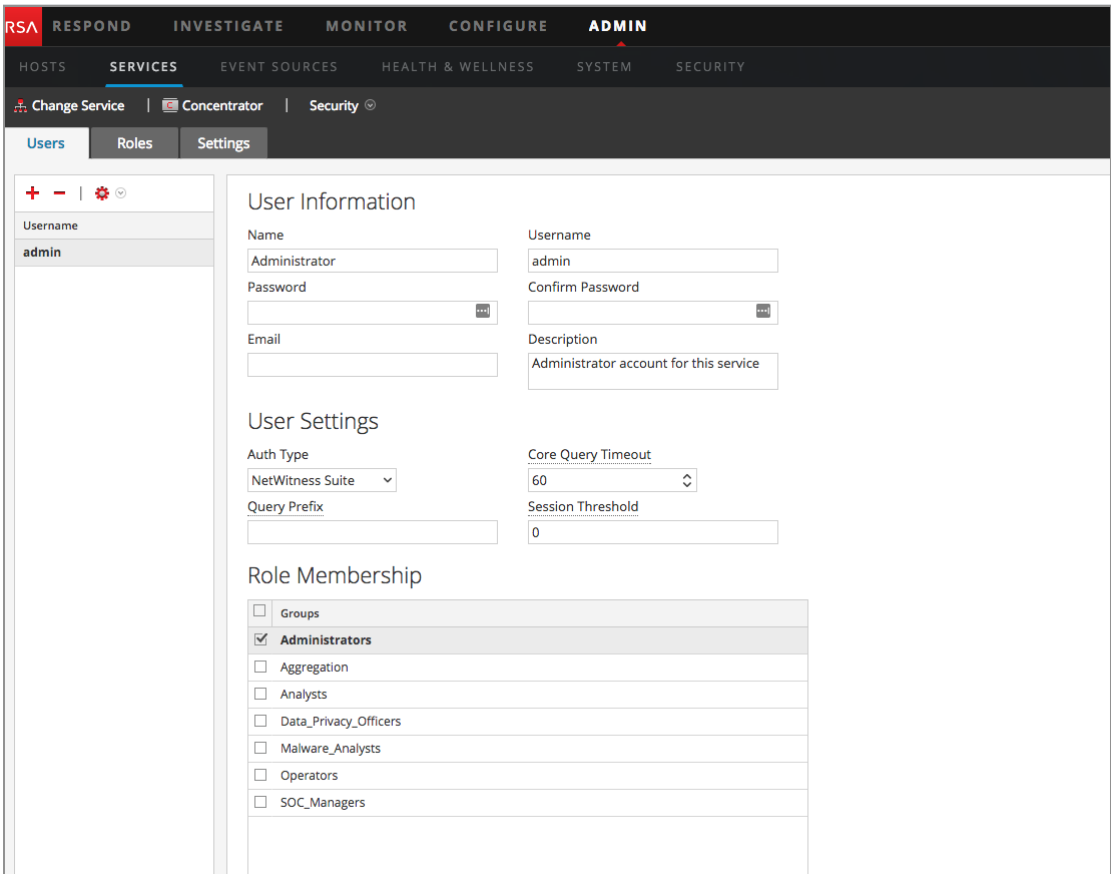
Each of the following procedures starts in the Services Security view.

To navigate to the Services Security view:

1. In NetWitness Suite, go to **ADMIN > Services**.

2. Select a service, then click > **View** > **Security**.

   The Security view for the selected service is displayed with the Users tab open.



Note: For NetWitness Suite 10.4 and earlier service versions, in the User Settings section, the **Query Level** field is displayed instead of **Core Query timeout**.

ADD A SERVICE USER

1. On the **Users** tab, click +.
2. Type the Username to access the service, then press **Enter**.

   The User Information section displays the Username and the rest of the fields are available for editing.
3. Type the password for logging on to the service in the **Password** and **Confirm Password** fields.
4. (Optional) Provide additional information:
   - **Name** for logging on to NetWitness Suite
   - **Email** address

- **Description** of the user

5. In the User Settings section, select the following information:
   - **Authentication Type**
     - If NetWitness Suite authenticates the user, select NetWitness.
     - If Active Directory or PAM is configured on NetWitness Server to authenticate the user, select External.

Note: In 10.4 and later, trusted connections make it unnecessary to configure external user accounts on the service. All external configuration is centralized on NetWitness Server.

   - **Core Query Timeout** is the maximum number of minutes a user can run a query on the service. This field applies to NetWitness Suite 10.5 and later service versions and does not appear for 10.4 and earlier versions.

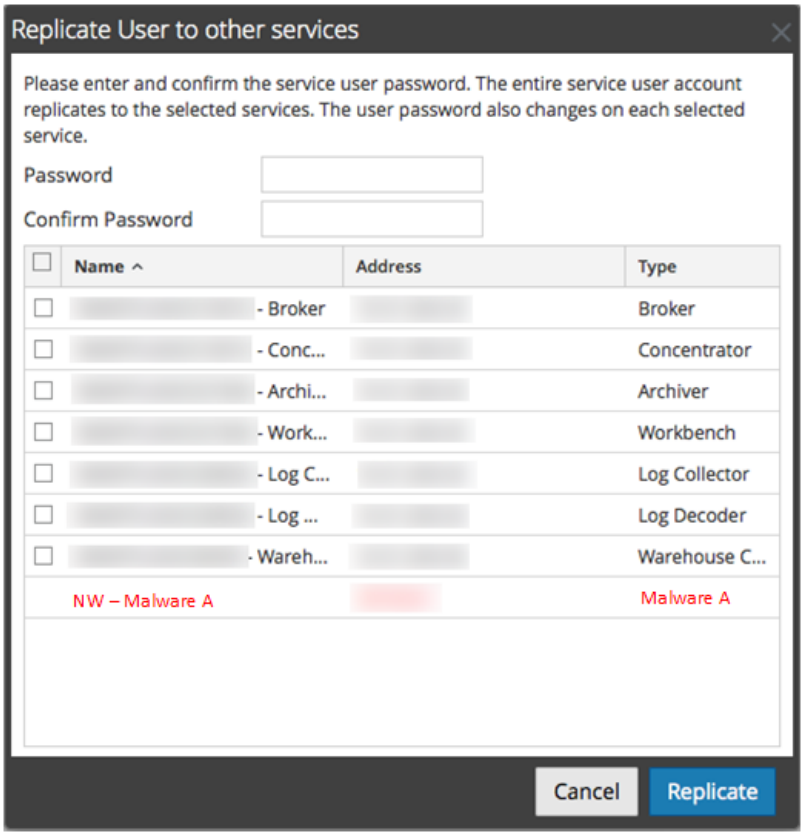
6. (Optional) Specify additional query criteria:
   - **Query Prefix** filters queries. Type a prefix to restrict results the user sees.
   - **Session Threshold** controls how the service scans meta values to determine session counts. Any meta value with a session count that is above the threshold stops its determination of the true session count.

7. In the **Role Membership** section, select each role to assign to the user. When a user is a member of a role on a service, the user has the permissions assigned to the role.
8. To activate the new service user, click **Apply**.

The user is added to the service immediately.

REPLICATE A USER TO OTHER SERVICES

1. In the Users tab, select a user and click > **Replicate**.
   The Replicate Users to Other Services dialog is displayed.



2. Enter the user's **password** and confirm the password.
3. Select each service to which you are replicating the user.
4. Click **Replicate**.

The user account is added to each selected service.

DELETE A SERVICE USER

1. On the **Users** tab, select the **Username** and click .

   NetWitness Suite requests confirmation that you want to delete the selected user.
2. To confirm, click **Yes**.

The user is deleted from the service immediately.

Add a Service User Role

There are pre-configured roles in NetWitness Suite that are installed on the server and on each service. You can also add custom roles. The following table lists the pre-configured system roles and their permissions.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to meta and session content
Analysts	Access to meta and session content but not to configurations
SOC_ Managers	Same access as Analysts plus additional permission to handle incidents
Malware_ Analysts	Access to malware events and to meta and session content
Data_Privacy_ Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).

You must add a service role when you have added a:

- **Service** user or users that requires a new set of permissions.
- **Custom role on NetWitness Server** because trusted connections require that the same custom role exists both on the server and on each service the custom role will access. The names must be identical. For example, if you add a Junior Analysts role on the server then you must add a Junior Analysts role on each service the role will access. For more information, see the **Add a Role and Assign Permissions** topic in *System Security and User Management*.

There is also a pre-configured **Aggregation** service role. Aggregation Role and Service User Roles and Permissions provide additional information.

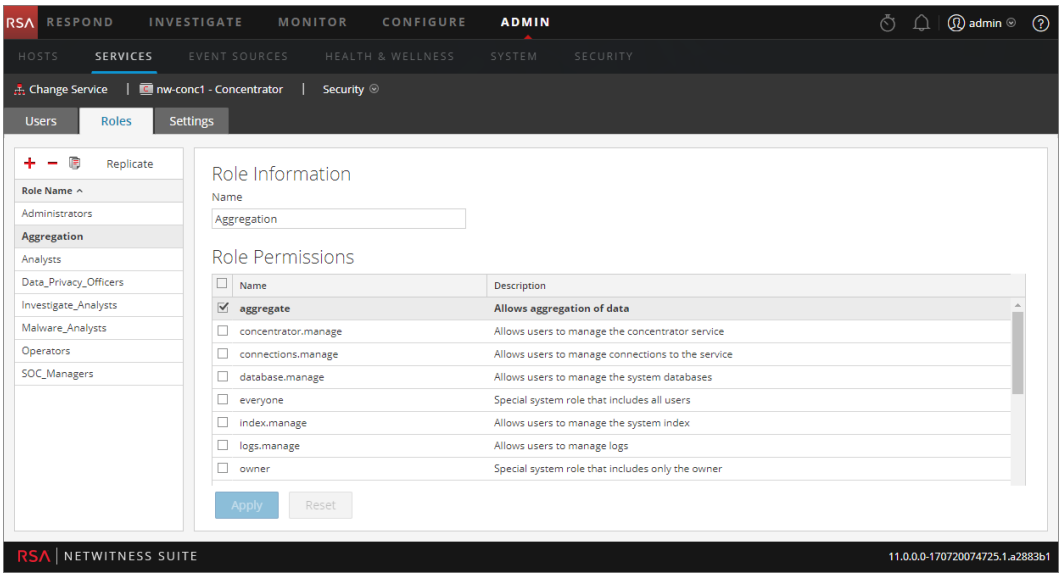
Procedure

To add a service user role and assign permissions to it:

1. In NetWitness Suite, go to **ADMIN > Services**.
2. Select a service, then **> View > Security**.
   The Security view for the selected service is displayed with the Users tab open.

3. Select the **Roles** tab and click +.

   The Services Security view is displayed and five pre-configured roles are already listed.



4. Click +, type the **Role Name** and press **Enter**.

   The Role Name is displayed above a list of **Role Permissions**.

5. Select each permission the role will have on the service.

6. Click **Apply**.

The role is added to the service immediately. You can add service users to it in the **Users** tab.

Change a Service User Password

This procedure allows Administrators to change the password of a service user and replicate the new password to all Core services with that user account defined. It replicates only the password change to the Core services selected and does not replicate the entire user account. Administrators can also change the password of the **admin** account on the Core services.

Note: The Change Password option does not apply to external users.

To change the password of a service user:

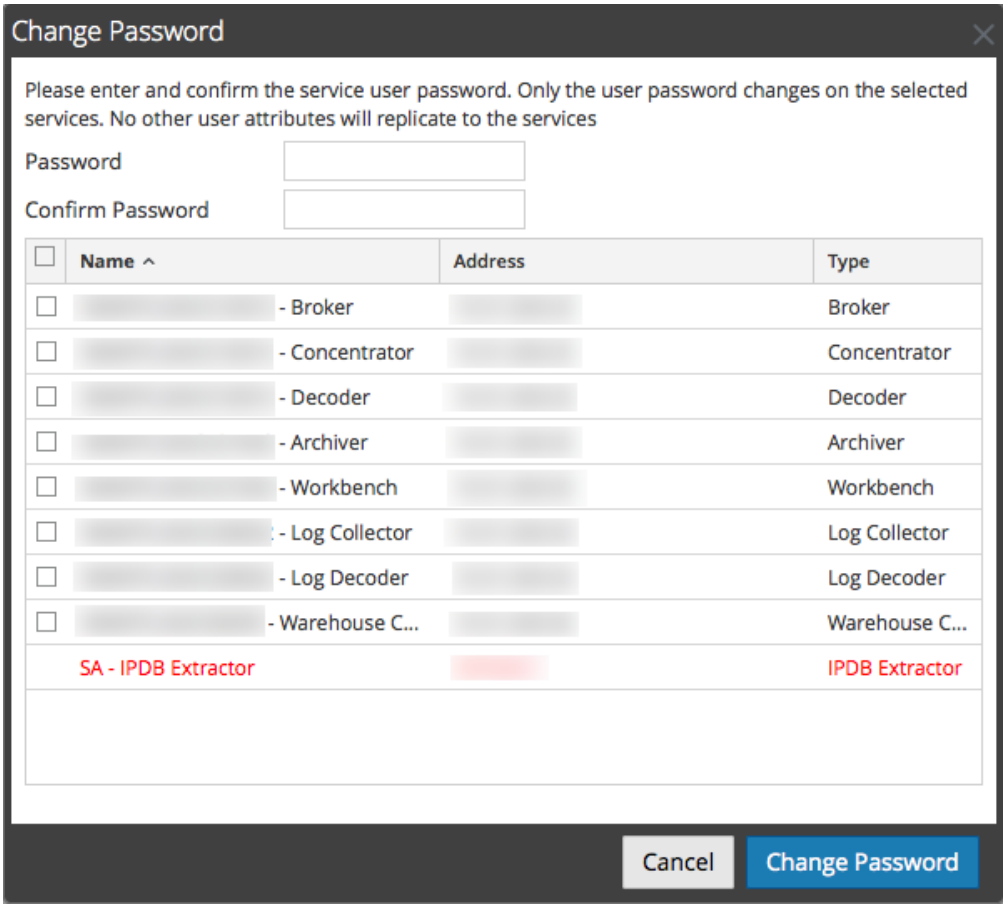
1. In NetWitness Suite, go to **ADMIN > Services**.

   The Administration Services view is displayed.

2. Select a service, then click **> View > Security**.

   The Security view for the selected services is displayed.

3. In the **Users** tab, select a user and select **Change Password** from the actions icon.
   The **Change Password** dialog is displayed.



4. Type a new password for the user and confirm the password.
5. Select the services where you want the user password to change.
6. Click **Change Password**.
   The status of the password change on the selected services is displayed.

Create and Manage Service Groups

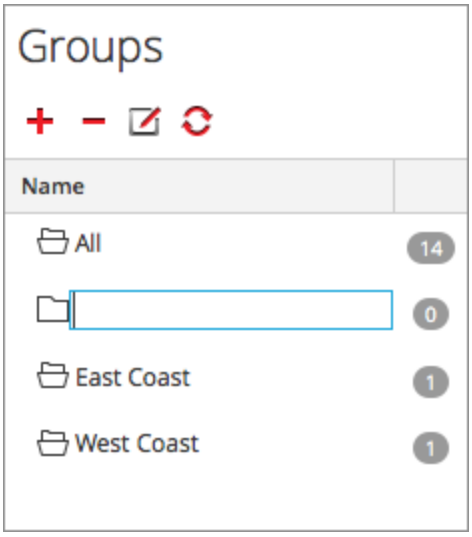
The Administration Services view provides options for creating and managing groups of services. The Services panel toolbar includes options for creating, editing, and deleting service groups. Once groups are created, you can drag individual services from the Services panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A service may belong to more than one group. Here are some examples of possible groupings.

- Group different service types to make it easier to configure and monitor all Brokers, Decoders, or Concentrators.
- Group services that are part of the same data flow; for example, a Broker, and all associated Concentrators and Decoders.
- Group services according to their geographic region and location within the region. If a major power outage occurs in a location, potentially affected services are easily identifiable.

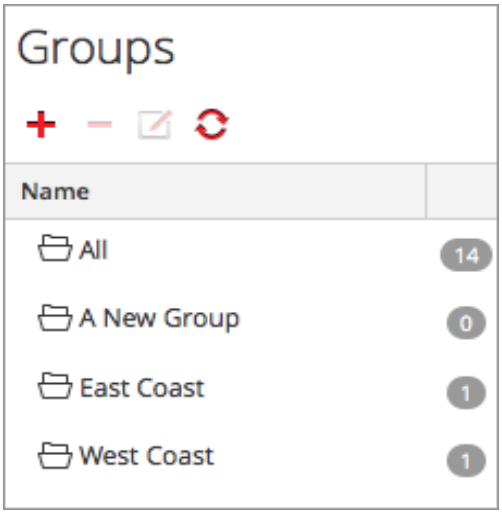
Create a Group

1. In NetWitness Suite, go to **ADMIN** > **Services**.
   The Administration Services view is displayed.
2. In the **Groups** panel toolbar, click +.
   A field for the new group opens with a blinking cursor.



3. Type the name of the new group in the field (for example, **A New Group**) and press **Enter**.
   The group is created as a folder in the tree. The number next to the group indicates the

number of services in that group.



Change the Name of a Group

1. In the **Services** view **Groups** panel, double-click the group name or select the group and click . The name field opens with a blinking cursor.
2. Type the new name of the group and press **Enter**.
   The name field closes and the new group name is displayed in the tree.

Add a Service to a Group

In the Services view **Services** panel, select a service and drag the service to a group folder in the groups panel; for example,**Log Collectors**.
The service is added to the group.

View the Services in a Group

To view the services in a group, click the group in the **Groups** panel.

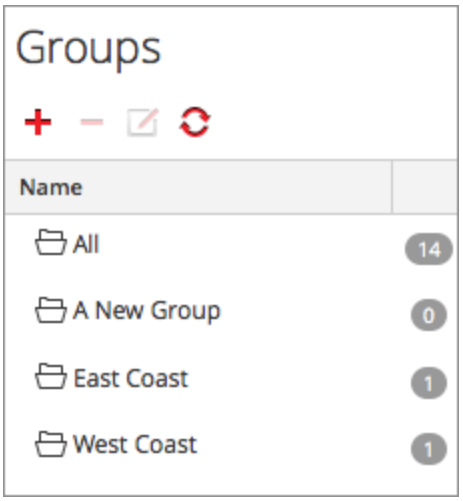
The **Services** panel lists the services in that group.

Remove a Service from a Group

1. In the Services view **Groups** panel, select the group that contains the service that you want to remove. The services in that group appear in the Services panel.
2. In the **Services** panel, select one or more services that you want to remove from the group, and in the toolbar, select > **Remove from Group**.
   The selected services are removed from the group, but are not removed from the NetWitness Suite user interface. The number of services in the group, which is listed near the group

name, decreases by the number of services removed from the group. The **All** group contains the services that were removed from the group.

In the following example, the service group called **A New Group** does not contain any services, since the service in that group was removed.



Delete a Group

1. In the Services view **Groups** panel, select the group that you want to delete.
2. Click −.

   The selected group is removed from the Groups panel. The services that were in the group are not removed from the NetWitness Suite user interface. The **All** group contains the services from the deleted group.

Duplicate or Replicate a Service Role

An efficient way to add a new service role is to duplicate a similar role, save it with a new name and revise the permissions that are already assigned. For example, you could duplicate the Analysts role. Then, save it as **JuniorAnalysts** and modify the permissions.

The quick way to add an existing role to other services is to replicate the role. For example, you could replicate the **JuniorAnalysts** role that exists on a broker to a concentrator and log decoder.

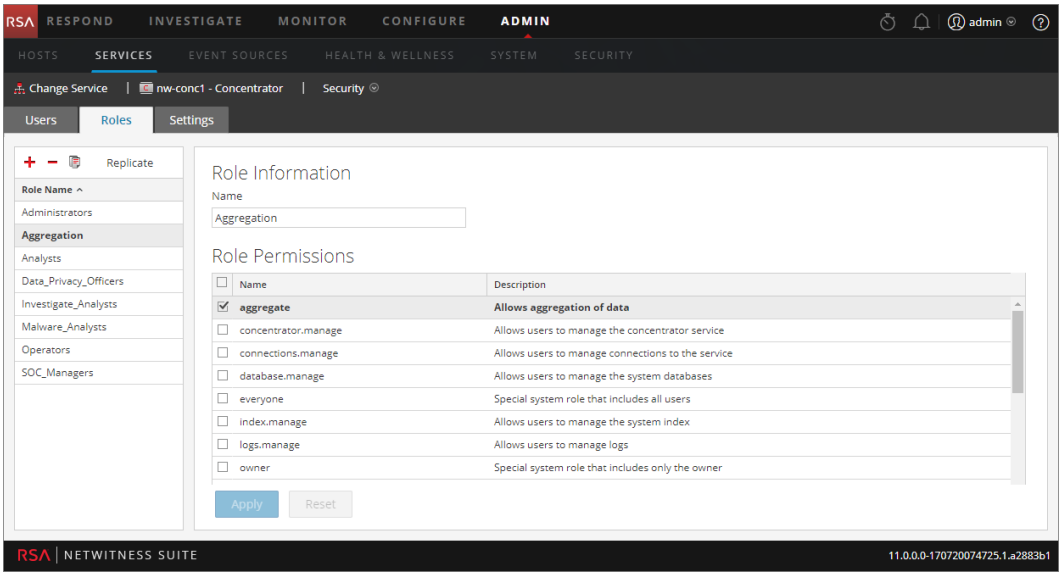
Each of the following procedures starts in the Services Security view.

To navigate to the Services Security view:

1. In NetWitness Suite, go to **ADMIN > Services**.
2. Select a service, then click **> View > Security**.
   The Security view for the selected service is displayed with the Users tab open.
3. Select the **Roles** tab.

Duplicate a Service Role

1. In the Roles tab, select the role you want to duplicate.



2. Click **Duplicate Role.**
3. Type a new name and click **Apply**.
4. Select the new role.
5. In the **Role Permissions** section, select or deselect permissions to modify what the new role can do.

The duplicated role is added to the service immediately.

Replicate a Role

1. In the **Roles** tab, select the role you want to replicate and click **Replicate**.
2. In the **Replicate Role to Other Services** dialog, select each service on which to add the role.
3. Click **Replicate**.

The replicated role is added to each selected service immediately.

Edit Core Service Configuration Files

The service configuration files--for Decoder, Log Decoder, Broker, Concentrator, Archiver, and Workbench services -- are editable as text files. In the Service Config view > Files tab, you can:

- View and edit a service configuration file that the NetWitness Suite system is currently using.
- Retrieve and restore the latest backup of the file you are editing.
- Push the open file to other services.
- Save changes made to a file.

The files available to edit vary depending upon the type of service being configured. The files that are common to all Core services are:

- The service index file.
- The netwitness file.
- The crash reporter file.
- The scheduler file.

In addition the Decoder has files that configure parsers, feed definitions, and a wireless LAN adapter.

Note: The default values in these configuration files are generally good for the most common situations; however, some editing is necessary for optional services, such as the crash reporter or scheduler. Only administrators with a good understanding of the networks and the factors that affect the way services collect and parse data should make changes to these files in the Files tab.

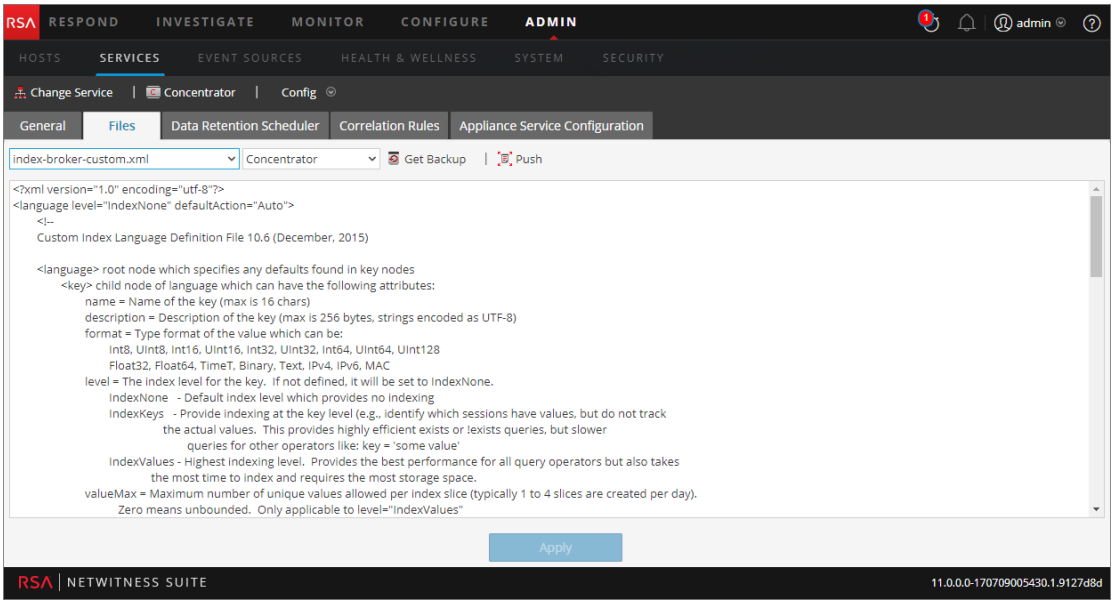
For more detail on service configuration parameters, see Service Configuration Settings.

Edit a Service Configuration File

To edit a file:

1. In NetWitness Suite, go to **ADMIN > Services**.
2. In the Services grid, select a service.
3. Select **> View > Config**.
   The Service Config view is displayed with the General tab open.
4. Click the **Files** tab.
   The selected service, such as Concentrator, appears in the drop-down list on the right.

5. (Optional) To edit a file for the host instead of the service, select **Host** in the drop-down list.
6. Choose a file from the **Please Select A File To Edit** drop-down list.
   The file content is displayed in edit mode.



7. Edit the file and click **Apply**.

The current file is overwritten and a backup file is created. The changes go into effect after the service is restarted.

Revert to a Backup Version of a Service Configuration File

After you make changes to a configuration file, save the file, and restart the service, a backup file is available. To revert to a backup of a configuration file:

1. Select a configuration file by completing steps 1-6 of the **Edit Service Configuration Files** procedure at the beginning of this topic.
2. Click Get Backup.
   The backup file opens in the text editor.
3. To revert to the backup version, click **Save**.

The changes go into effect after the service is restarted.

Push a Configuration File to Other Services

Once you have edited a service configuration file, you can push the same configuration to other services of the same type.

1. Select a configuration file by completing steps 1-6 of the **Edit a Service Configuration File** procedure at the beginning of this topic.
2. Click

. The Select Services dialog is displayed.
3. Select each service to push the configuration file on it.
   Each service must be the same type as the one you selected in the Services view.

   Caution: If you decide not to push the configuration file, click **Cancel**.
4. To push the configuration file to all selected services, click **OK**.

The configuration file is pushed to all selected services.

CONFIGURE THE TASK SCHEDULER

Scheduler File

You can edit the **scheduler** file that in the Service Config view > Files tab. This file configures the built-in task scheduler for a service. The task scheduler can automatically send messages at predefined intervals or specific times of the day.

Scheduler Task Syntax

A task line in the scheduler file consists of the following syntax, where **<Value>** has no spaces:

```
<ParamName>=<Value>
```

if **<Value>** has any spaces, this is the syntax:

```
<ParamName>="<Value>"
```

In each task line, these guidelines apply:

- Parameter **time** or one of the interval parameters (**seconds**, **minutes** or **hours**) is required.
- Escape special characters with a \ (backslash).

Task Line Parameters

The following task line parameters are accepted by the scheduler.

Syntax	Description
daysOfWeek: <string, optional, {enum-any:sun|mon|tue|wed|thu|fri|sat|all}>	The days of week to execute a task. The default value is **all**.
deleteOnFinish: <bool, optional>	Delete the task when it has successfully finished.

Syntax	Description
hours: <uint32, optional, {range:1 to 8760}>	The number of hours between executions.
logOutput: <string, optional>	Output the response to log using the specified module name.
minutes: <uint32, optional, {range:1 to 525948}>	The number of minutes between executions.
msg: <string>	The message to send the node.
params: <string, optional>	The parameters for the message.
pathname: <string>	The path of the node that receives the message.
seconds: <uint32, optional, {range:1 to 31556926}>	The number of seconds between executions.
time: <string>	The time of execution in HH::MM:SS format (local time of this server).
timesToRun: <uint32, optional>	How many times to run since service start, **0** = means unlimited (default).

Messages

The following are the message strings to use in the Task Scheduler **msg** parameter.

Message	Description
addInter	Add a task to run at a defined interval. For example, this message runs the **/index save** command every 6 hours: addInter hours=6 pathname=/index msg=save

Message	Description
addMil	Add a task to run at a specific time of day or even day(s) of the week. For example, this message runs the **/index save** command at 1AM every business day: addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri
delSched	Deletes an existing scheduled task. The **id** parameter of the task must be retrieved from the print message.
print	Prints all scheduled tasks.
replace	Assign all scheduled tasks in one message, deleting any existing tasks.
save	Tell a node to save

Sample Task Line

The following example task line in the scheduler file downloads the feeds package file (**feeds.zip**) to the selected Decoder every 120 minutes from the feeds host server:

```
minutes=120 pathname=/parsers msg=feed params="type\=wget
file\=http://feedshost/nwlive/feeds.zip"
```

EDIT A SERVICE INDEX FILE

This topic provides important information and guidelines for configuring service custom index files, which are editable in the Service Config view > Files tab.

The index file, along with other configuration files, controls operation of each Core service. Accessing the index file through the Service Config view in NetWitness Suite opens the file in a text editor, where you can edit the file.

Note: Only Administrators with a thorough and comprehensive understanding of Core service configuration are qualified to make changes to an index file, which is one of the central configuration files for the appliance service. Changes made should be consistent across all Core services. Invalid entries or a misconfigured file can prevent the system from starting and can require the assistance of RSA Support to bring the system back into a working state.

These are the index files:

- `index-broker.xml`, and `index-brokereustom.xml`
- `index-concentrator.xml`, and `index-concentrator ɛustom.xml`

- index-decoder.xml, and index-decodereustom.xml
- index-logdecoder.xml, and index-logdecodereustom.xml
- index-archiver.xml, and index-archiver custom.xml
- index-workbench.xml, and index-workbench custom.xml

Index and Custom Index Files

All customer-specific index changes are made in **index-<service>-custom.xml**. This file overrides any settings in index-<service>.xml, which is solely controlled by RSA.

Note: Customers using NetWitness Suite versions prior to 10.1 had to customize index files by editing and saving the index file, and this method relied on NetWitness Suite creating a backup of the current index file upon restart of the service. Using this process, the current file is overwritten and a backup file is created. The toolbar option provides a way to revert to a backup version of the index file.
During software upgrades, index-<service>.xml is not preserved, as it is overwritten by any changes made by the RSA content team. However, a backup is made in the same directory and named index-<service>.xml.rpm_pre_save. The index-<service>.xml.rpm_pre_save file can be referenced if needed to create the customer-specific **index-<service>-custom.xml** file, which needs to be done only once. Going forward, the new system allows RSA to make index changes without modifying existing customer specific changes.

The custom index file, **index-<service>-custom.xml,** allows creation of custom definitions or overrides of your own language keys that are not overwritten during the upgrade process.

- Keys that are defined in index-<service>-custom.xml replace the definitions found in index-<service>.xml.
- Keys that are added to index-<service>eustom.xml and not found in index-<service>.xml are added to the language as a new key.

Some common applications for editing the index file are:

- To add new custom meta keys to add new fields to the NetWitness Suite user interface.
- To configure protected meta keys as part of a data privacy solution as described in the *Data Privacy Management* guide.
- To adjust the NetWitness Suite Core database query performance as described in the *NetWitness Suite Core Database Tuning Guide*.

Note: For NetWitness Suite 10.1 and above, there is no need to edit the Broker custom index file, except for data privacy deployment scenarios and system roles. The Broker automatically merges the keys of all aggregate services to create a comprehensive language. The fallback language defined in `index-broker.xml` and **`indexbroker-custom.xml`** is used if there are no services or if all services are offline.

Caution: Never set the index level to `IndexKeys` or `IndexValues` on a Decoder if you have a Concentrator or Archiver aggregating from the Decoder. The index partition size is too small to support any indexing beyond the default `time` meta key.

ENABLE CRASH REPORTER SERVICE

The Crash Reporter is an optional service for NetWitness Suite services. When activated for any of the core services, the Crash Reporter automatically generates a package of information to be used for diagnosing and solving the problem that resulted in the service failure. The package is automatically sent to RSA for analysis. The results are forwarded to RSA support for any further action.

The information package sent to RSA does not contain captured data. This information package consists of the following information:

- Stack trace
- Logs
- Configuration settings
- Software version
- CPU information
- Installed RPMs
- Disk geometry

The Crash Reporter crash analysis can be activated for any Core product.

The crashreporter.cfg File

One of the files available for editing in the Service Config view > Files tab is **crashreporter.cfg**, the Crash Reporter Client Server configuration file.

This file is used by the script that checks, updates, and builds crash reports on the host. The list of products to monitor can include Decoders, Concentrators, hosts, and Brokers.

This table lists the settings for the **crashreporter.cfg** file.

Setting	Description
applicationlist=decoder, concentrator, host	Define the list of products to monitor.
sitedir=/var/crashreporter	Location of the site directory for the report.
webdir=/usr/share/crashreporter/Web	Location of the web directory.
devdir=/var/crashreporter/Dev	Location of the development directory.
datadir=/var/crashreporter/data	Location of the directory storing data files.
perldir=/usr/share/crashreporter/perl	Location of the perl files.
bindir=/usr/share/crashreporter/bin	Location of the binary executables.
libdir=/usr/share/crashreporter/lib	Location of the binary libraries.
cfgdir=/etc/crashreporter	Location of the configuration files.
logdir=/var/log/crashreporter	Location of the log files.
scriptdir=/usr/share/crashreporter/scripts	Location of the directory containing scripts.
workdir=/var/crashreporter/work	Location of the process work directory.
sqldir=/var/crashreporter/sql	Location where created sql files are placed.

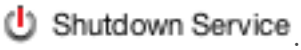
Setting	Description
reportdir=/var/crashreporter/reports	Location where temporary reports are created.
packagedir=/var/crashreporter/packages	Location of the created package files.
gdbconfig=/etc/crashreporter/crashreporter.gdb	Location of the gdb configuration file.
corewaittime=30	Define the number of seconds to wait after finding a core in order to determine if the core is still being written.
cyclewaittime=10	Define the number of minutes to wait between search cycles
deletecores=1	Specify if the core files should be deleted after report. 0 = No 1 = Yes **NOTE:** Until the core file is deleted, it is reported each time crashreporter is restarted.

Setting	Description
deletereportdir=1	Specify if the report directory should be deleted after the report. Useful in order to view core reports on box. 0 = No 1 = Yes **NOTE:** If not deleted, the directory will be included in each subsequent package.
debug=1	Specify whether debugging messages are turned on or off in the **crashreporter** logging output. 0 = No 1 = Yes
posturl=https://www.netwitnesslive.com/crash...ter/submit.php	Define the webserver post url.
postpackages=0	Specify if the packages should be posted to the webserver. 0 = No 1 = Yes

Setting	Description
deletepackages=1	Specify if packages should be deleted after they are posted to webserver. 0 = No 1 = Yes

Configure the Crash Reporter Service

To configure the Crash Reporter service:

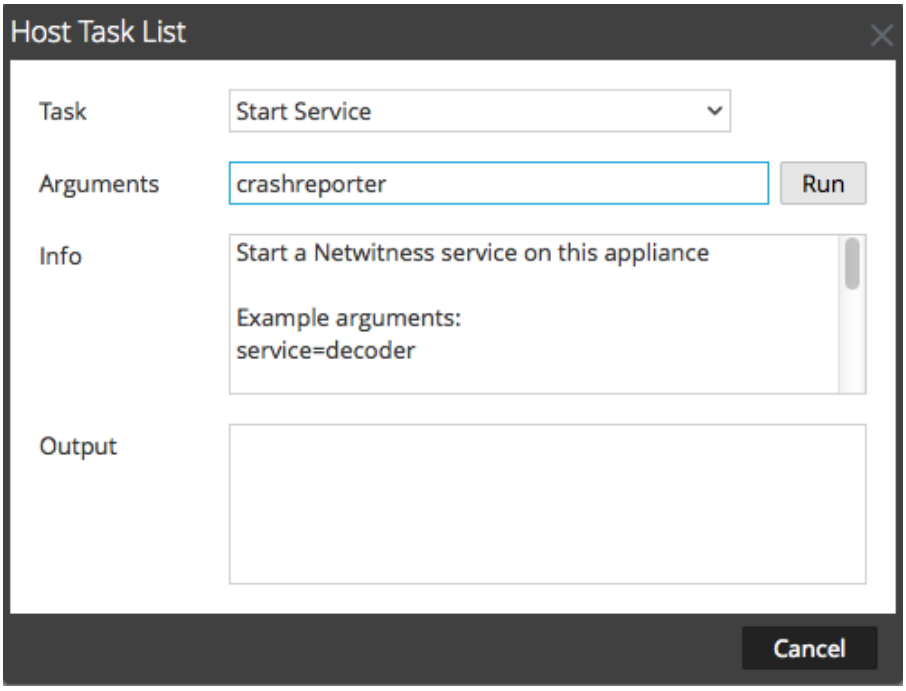
1. Select **ADMIN > Services**.
2. Select a service then click **> View > Config**.
3. Select the **Files** tab.
4. Edit **crashreporter.cfg**.
5. Click **Save**.
6. To display the Service System view, select **Config > System**.
7. To restart the service, click  .
   The service shuts down and restarts.

Start and Stop the Crash Reporter Service

To start the Crash Reporter Service:

1. Select **ADMIN > Services**.
2. Select a service and click **> View > System**.
3. In the toolbar, click .
   The Host Task List is displayed.
4. In the Task drop-down list, select **Start Service**.

5. In the Arguments field, type **crashreporter**, then click **Run**.



The Crash Reporter service is activated and remains active until you stop it.

To stop the Crash Reporter service, select **Stop Service** from the Task drop-down list.

MAINTAIN THE TABLE MAP FILES

The table mapping file provided by RSA, `table-map.xml`, is a very significant part of the Log Decoder. It is a meta definition file which also maps the keys used in a log parser to the keys in the metadb.

Do not edit the `table-map.xml` file. If you want to make changes to the table-map, make them in the `table-map-custom.xml` file. The latest `table-map.xml` file is available on Live and RSA updates it as required. If you make changes to the `table-map.xml` file, they can be overwritten during an upgrade of service or content.

In the `table-map.xml`, some meta keys are set to `Transient` and some are set to `None`. To store and index a specific meta key, the key must be set to `None`. To make changes to the mapping, you need to create a copy of the file named `table-map-custom.xml` on the Log Decoder and set the meta keys to `None`.

For meta key indexing:

- When a key is marked as `None` in the `table-map.xml` file in the Log Decoder, it is indexed.
- When a key is marked as `Transient` in the **`table-map.xml`** file in the Log Decoder, it is not indexed. To index the key, copy the entry to the `table-map-custom.xml` file and change the keyword `flags="Transient"` to `flags="None"`.

- If a key does not exist in the `table-map.xml` file, add an entry to the `table-map-custom.xml` file in the Log Decoder.

Caution: Do not update the `table-map.xml` file because an upgrade can overwrite it. Add all of the changes that you want to make to the **`table-map-custom.xml`** file.

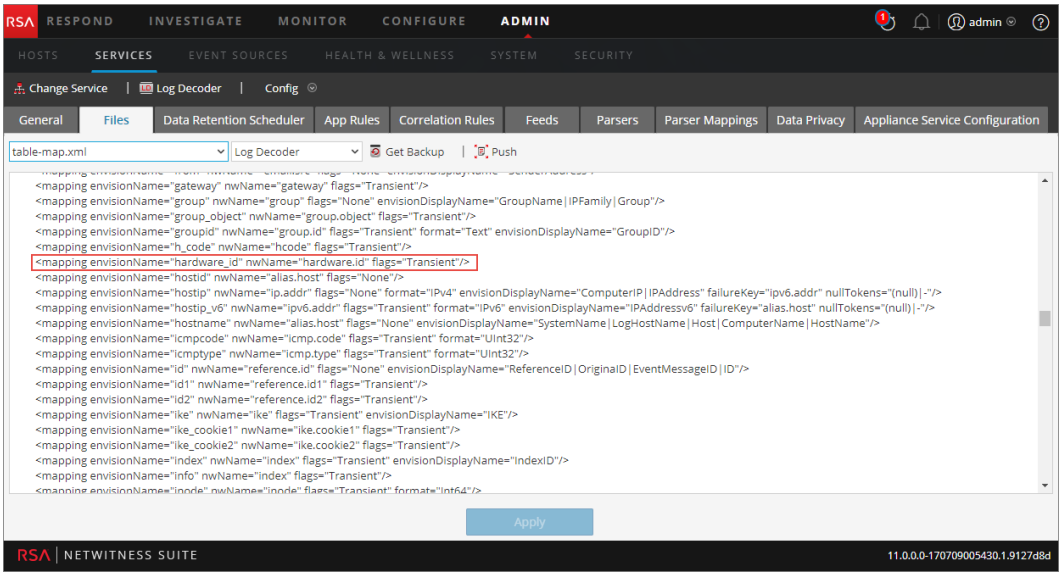
Prerequisites

If you do not have a `table-map-custom.xml` file on the Log Decoder, create a copy of `table-map.xml` and rename it to `table-map-custom.xml`.

Procedure

To verify and update the table mapping file:

1. Go to **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder and click > **View** > **Config**.
3. Click the **Files** tab and select the **`table-map.xml`** file.



4. Verify that the flags keywords are set correctly to either `Transient` or `None`.
5. If you need to change an entry, do not change the `table-map.xml` file. Instead, copy the entry, select the `table-map-custom.xml` file, find the entry in the `table-map-custom.xml` file and change the flags keyword from `Transient` to `None`.
   For example, the following entry for the `hardware.id` meta key in the `table-map.xml` file is not indexed and the flags keyword shows as `Transient`:
   `<mapping envisionName="hardware_id" nwName="hardware.id" flags="Transient"/>`
   To index the `hardware.id` meta key, change the flags keyword from `Transient` to `None`

in the `table-map-custom.xml`:

```
<mapping envisionName="hardware_id" nwName="hardware.id"
flags="None"/>
```

6. If an entry does not exist in the `table-map.xml` file, add an entry to the `table-map-custom.xml` file.
7. After making your changes to the `table-map-custom.xml` file, click **Apply**.

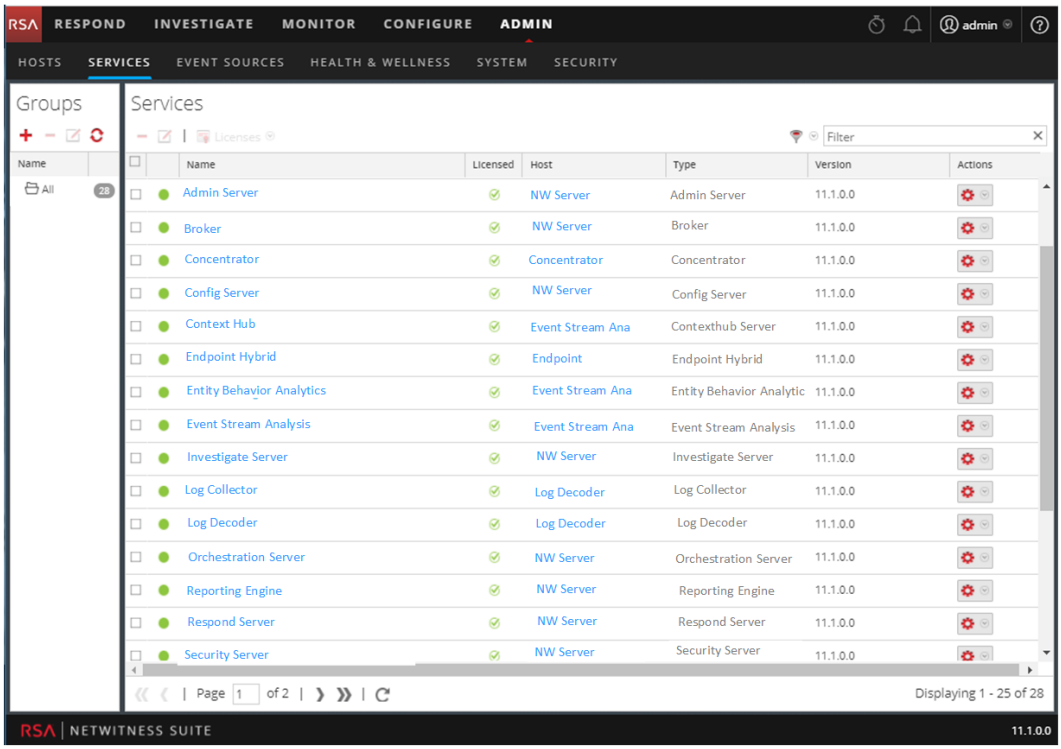
Caution: Before changing the table mapping files, carefully consider the effect of changing the index from `Transient` to `None` since it can impact the available storage and performance of the Log Decoder. For this reason, only certain meta keys are indexed out of the box. Use the `table-map-custom.xml` file for different use cases.

Edit or Delete a Service

You can edit service settings, such as changing the host name or port number, or delete a service that you no longer need.

Each of the following procedures starts in the Services view.

To navigate to the Services view, in NetWitness Suite, go to **ADMIN > Services**.

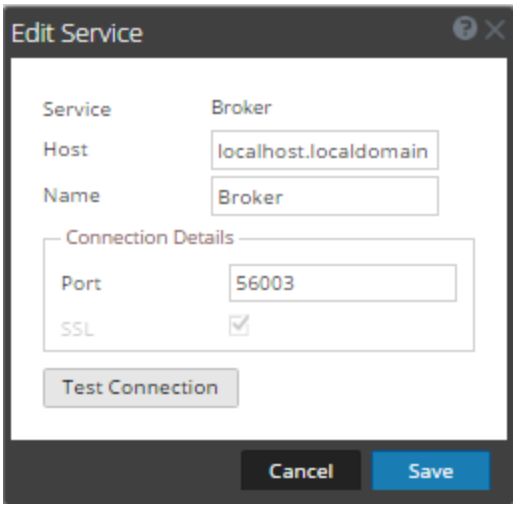


Procedures

EDIT A SERVICE

1. In the Services view, select a service and click or > **Edit**.

   The **Edit Service** dialog is displayed. It shows only the fields that apply to the selected service.



2. Edit the service details by changing any of the following fields:
   - **Name**
   - **Port** - Each core service has two ports, SSL and non-SSL. For trusted connections, you must use the SSL port.
   - **SSL** - For trusted connections, you must use SSL.
   - **Username** and **Password** - Use these credentials to test the connection to a service.
     a. If you use a trusted connection, delete the username.
        If you do not use a trusted connection, type a username and password.
     b. Click **Test Connection**.
3. (Optional) If the service requires a license select Entitle Service. This option is displayed only for services that require a license.
4. Click **Save**.

The changes take effect immediately.

DELETE A SERVICE

1. In the Services view, select one or more services and click or > **Delete**.
2. A dialog requests confirmation. To delete the service, click **Yes**.

The deleted service is no longer available to NetWitness Suite modules.

Explore and Edit Service Property Tree

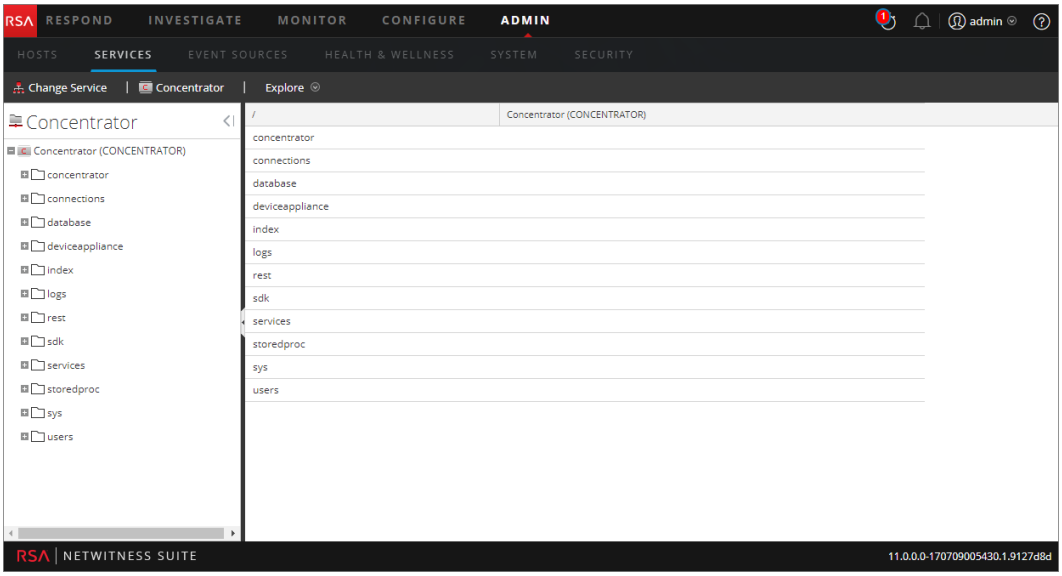
You have advanced access and control of service functionality in the Services Explore view, which consists of two parts. The Node list displays service functionality in a tree structure of folders. The Monitor panel displays properties of the folder or file selected in the Nodes list.

Each of the following procedures starts in the Explore view.

To navigate to the Explore view:

1. In NetWitness Suite, go to **ADMIN > Services**.
2. Select a service, then select **> View > Explore**.

   The Explore view is displayed. The Node list is on the left and the Monitor panel is on the right.



Procedures

DISPLAY OR EDIT A SERVICE PROPERTY

To display a service property:

1. Right-click a file in the Node list or Monitor panel.
2. Click **Properties**.

To edit the value of a service property:

1. In the **Monitor** panel, select an editable property value.
2. Type a new value.

SEND A MESSAGE TO A NODE

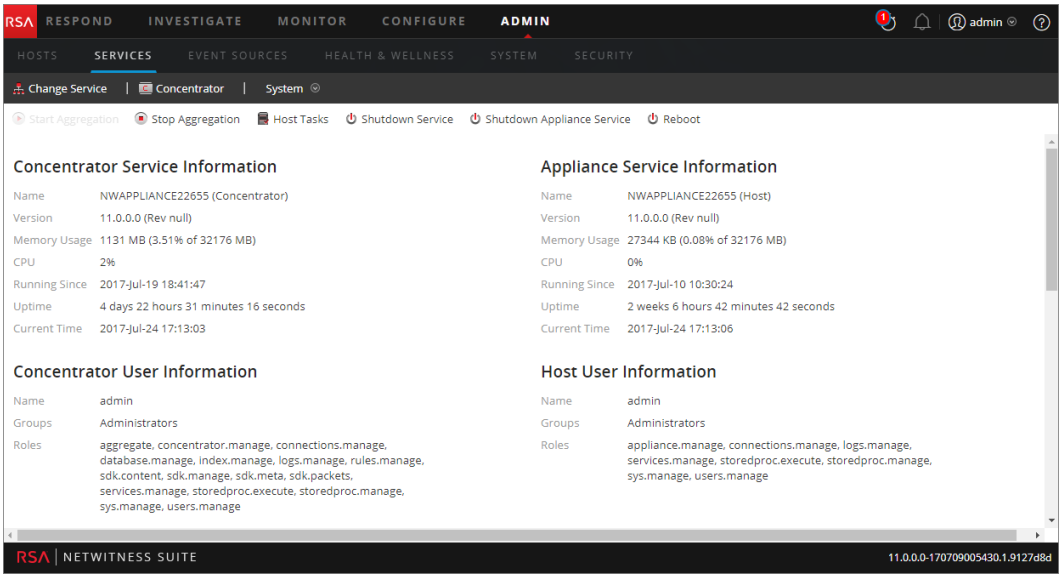
1. In the Properties Dialog select a **message type**. Options vary according to the file selected in the Node list.
   A description of the selected message type is displayed in the **Message Help** field.
2. (Optional) If the message requires them, type the **Parameters**.
3. Click **Send**.
   The value or format is displayed in the **Response Output** field.

Kill a Connection to a Service

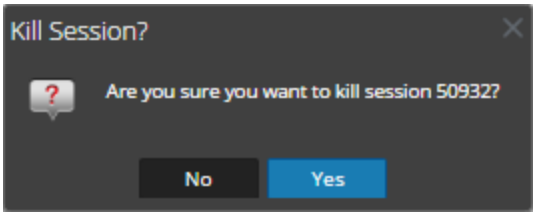
You can view sessions that are running on a service in the Service System view. From within the list of sessions, you can end the session and end active queries in a session.

End a Session on a Service

1. In NetWitness Suite, go to **ADMIN > Services**.
   The Admin Services view is displayed.
2. Select a service, and select **> View > System**.
   The Service System view is displayed.



3. In the **Session Information**grid at the bottom, click a ***session-number***.
   The following confirmation dialog is displayed.

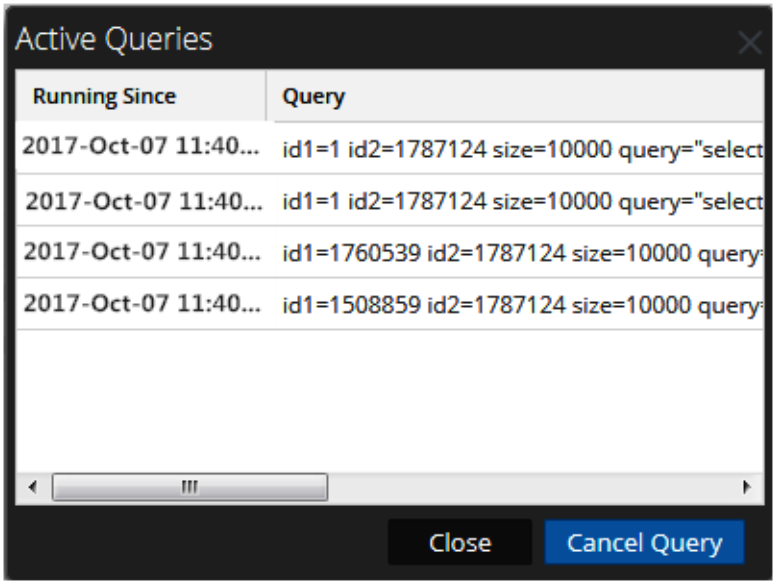


4. Click **Yes**.

The session ends and is removed from the grid.

End an Active Query in a Session

1. Scroll down to the **Sessions** grid.
2. In the **Active Queries** column, click a non-zero count of active queries for a session. You cannot click on it if there are 0 active queries.
   The Active Queries dialog is displayed.



3. Select a query and click **Cancel Query**.
   The query stops and the Active Queries column is updated.

Search for Services

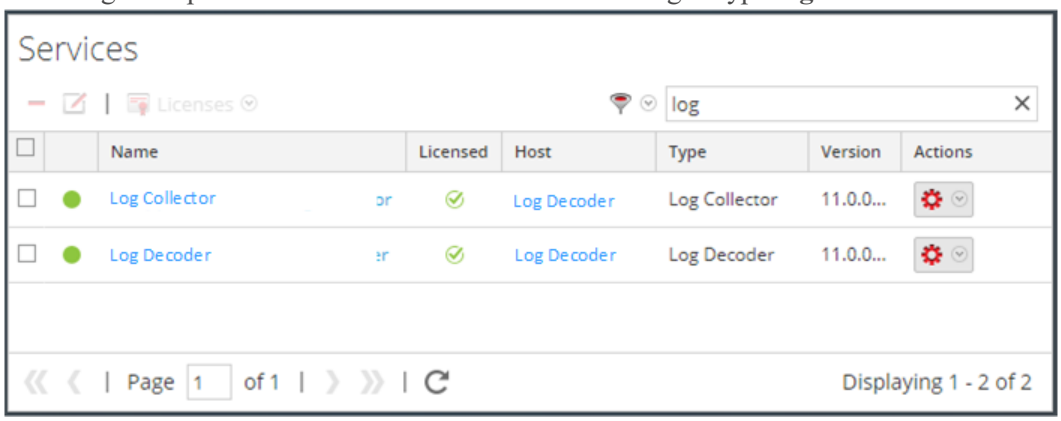
You can search for services from the list of services in the Services view. The Services view enables you quickly filter the list of services by Name, Host, and Service Type. You can use the Filter drop-down menu and the Filter field separately or at the same time to filter the Services view.

In addition to being able to locate the services for a host in the Services view, you can also quickly find the services that run on a host in the Hosts view.

Search for a Service

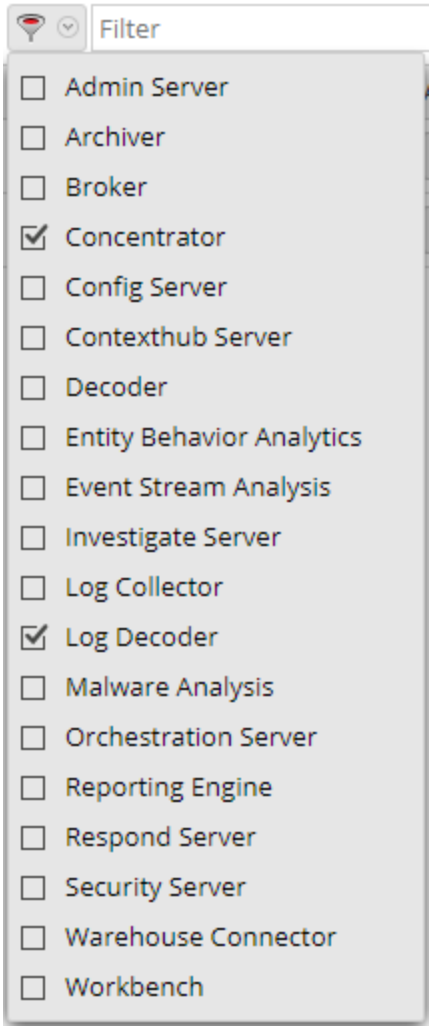
1. In NetWitness Suite, go to **ADMIN> Services**.
2. In the **Services** panel toolbar, type a service **Name** or **Host** in the **Filter** field.

   The Services panel lists the services that match the names entered in the Filter field. The following example shows the search results after starting to type **log** in the filter field.

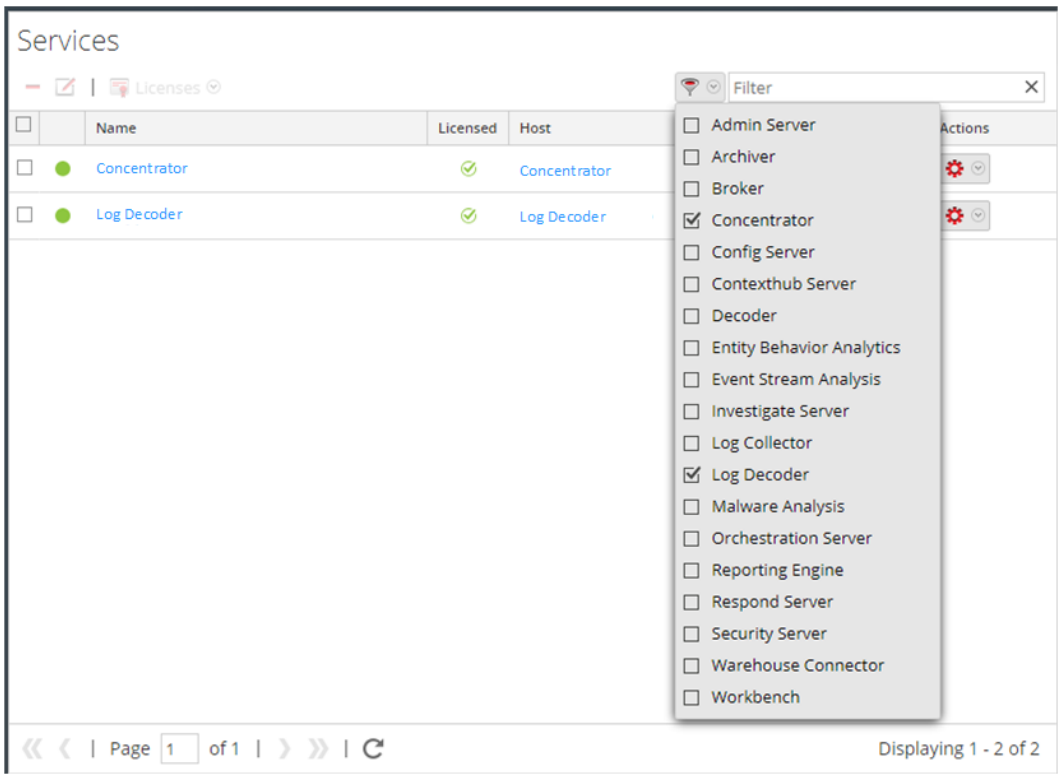
   

Filter Services by Type

1. In NetWitness Suite, go to **ADMIN > Services**.
2. In the Services view, click and select the service types that you would like to appear in the Services view.



The selected service types appear in the Services view. The following example shows the Services view filtered for Concentrator and Log Decoder.

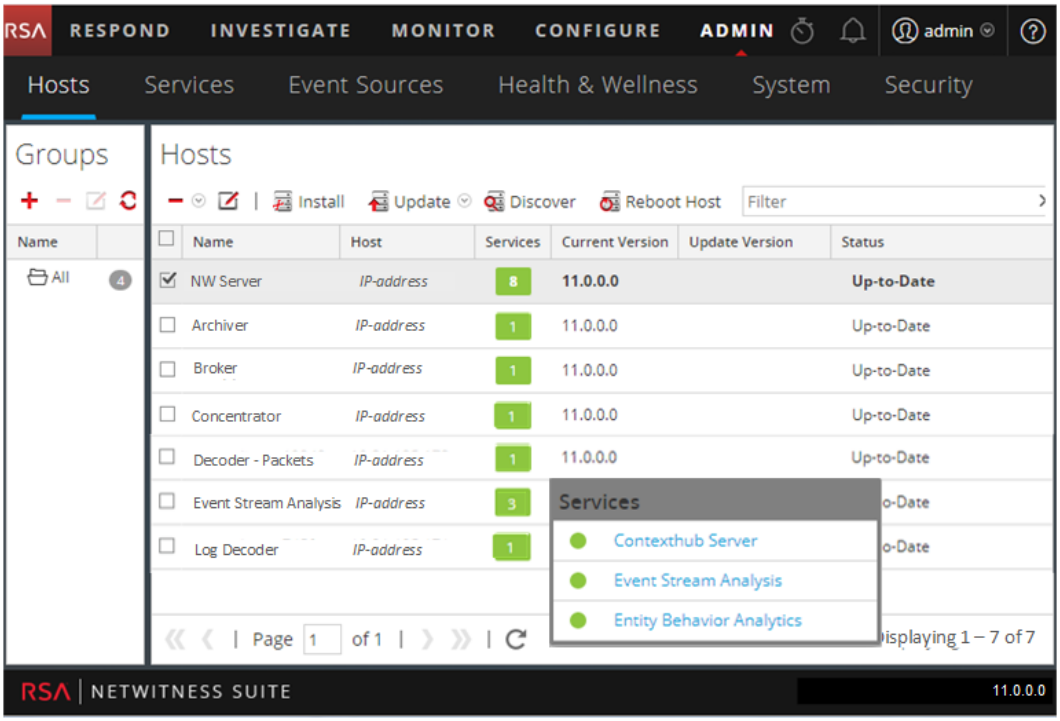


Find the Services on a Host

In addition to being able to locate the services for a host in the Services view, you can also quickly find the services that run on a host in the Hosts view.

1. In NetWitness Suite, go to **ADMIN > Hosts**.
2. In the Hosts view, select a host and click the box that contains a number (the number of services) in the **Services** column.
   A list of the services on the selected host is displayed.

In the following example, a list of three services on the selected host are listed after clicking the box containing the number 3.



3. You can click the service links to view the services in the Services view.

Start, Stop or Restart a Service

These procedures apply to core services only.

Each of the following procedures starts in the Services view. In NetWitness Suite, go to **ADMIN > Services**.

Start a Service

Select a service and click > **Start**.

Stop a Service

When you stop a service, all of its processes stop and active users are disconnected from it.

To stop a service:

1. Select a service and click > **Stop**.
2. A dialog requests confirmation. To stop the service, click **Yes**.

Restart a Service

Occasionally, you have to restart a service for changes to take effect. When you change a parameter that requires a restart, NetWitness Suite displays a message.

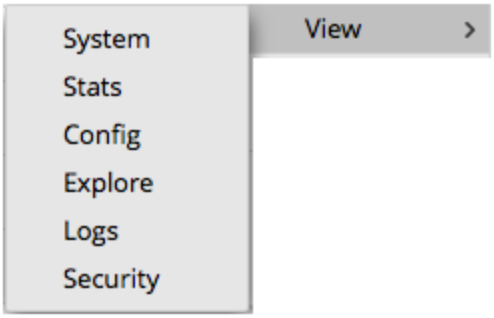
To restart a service:

1. Select a service and click > **Restart**.
2. A dialog requests confirmation. To stop the service, click **Yes**.

The service stops, then restarts automatically.

View Service Details

You can view and edit information about services using options in the View menu for a service.



Purpose of Each Service View

Each view displays a functional piece of a service and is described in detail in its own section:

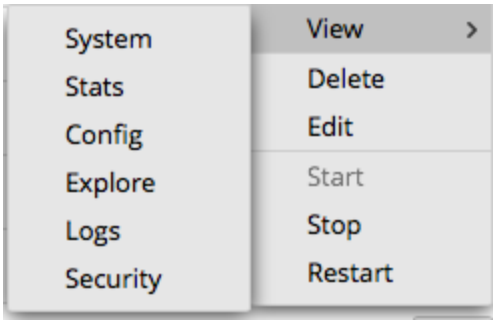
- System View shows a summary of service, appliance service, host user, license, and session information.
- Services Stats View provides a way to monitor service operations and status.
- Services Config View is for configuring all aspects of a service.
- Services Explore View is for viewing and editing host and service configurations.
- System Logging Panel shows service logs that you can search.
- Services Security View is a way to add Security Analytics Core user accounts for aggregation, thick client users, and REST API users.

Access a Service View

To access a view for a service:

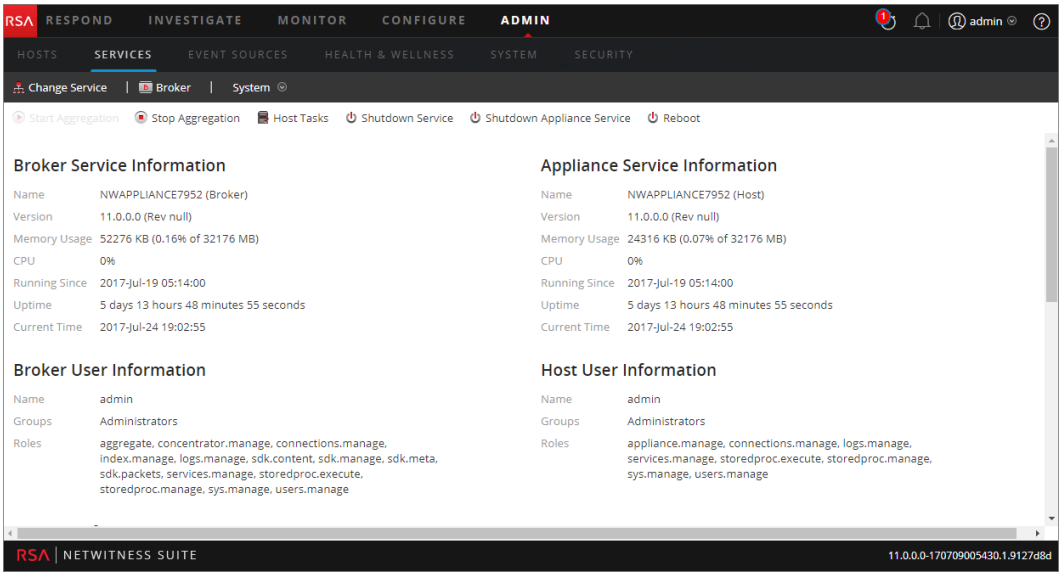
1. In NetWitness Suite, go to **ADMIN > Services**.
2. Select a service and click **> View**.

   The View menu is displayed.



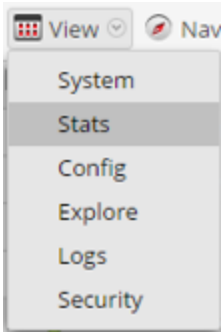
3. From the options on the left, select a view.

   This is a System view for a Broker.



4. Use the toolbar to navigate:

   a. Click **Change Service** to select another service.
      The **Administrate Service** dialog is displayed.
   b. Select the checkbox to the left of the service that you want.
   c. Select the view that you want for the service you selected in the View drop-down menu.



The new view (for example Stats) is displayed for the service you selected.

Hosts and Services Views References

This topic is a reference for features in the NetWitness Suite ADMIN user interface.

This topic describes features available in the NetWitness Suite Admin user interface. The Admin module pulls NetWitness Suite Admin activities into a single view to monitor and manage hosts (appliances), services, tasks, and security.

Topics

- Hosts View
- Services View
- Services Config View
- Services Explore View
- Services Logs View
- Services Security View
- Services Stats View

Hosts View

You set up and maintain the physical or virtual machine on which NetWitness Suite services run in the **Hosts** view.

Important: See Troubleshooting Version Installations and Updates for help on resolving errors you receive during version installation and update.

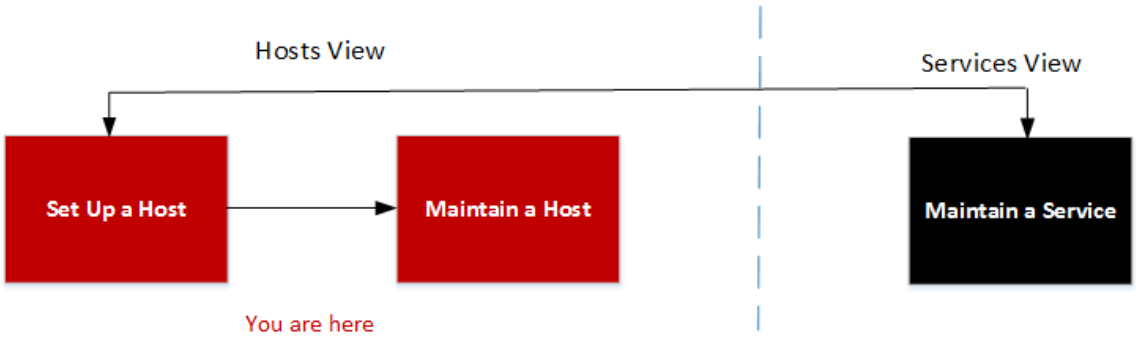
A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plug-in to enable or disable, according to the function of the host. You must configure the following Core services first:

Core	Other	Other	Other
Decoder	Log Decoder	Context Hub	Reporting Engine
Concentrator	Archiver	Log Collector	Warehouse Connector
Broker	Event Stream Analysis	Malware Analysis	Workbench

You must configure hosts and services to communicate with the network and each other so they can perform their functions such as storing or capturing data.

Workflow

This workflow shows the procedures you complete to set up a host, maintain a host, and update the host with new NetWitness Suite versions. Setting up a host is the first task in this workflow. The hosts with core services are set up out of the box. After that, you can set up additional hosts to enhance your NetWitness Suite deployment. The other two tasks, maintaining a host and updating versions for a host, are performed when required and do not have a specific order of completion.

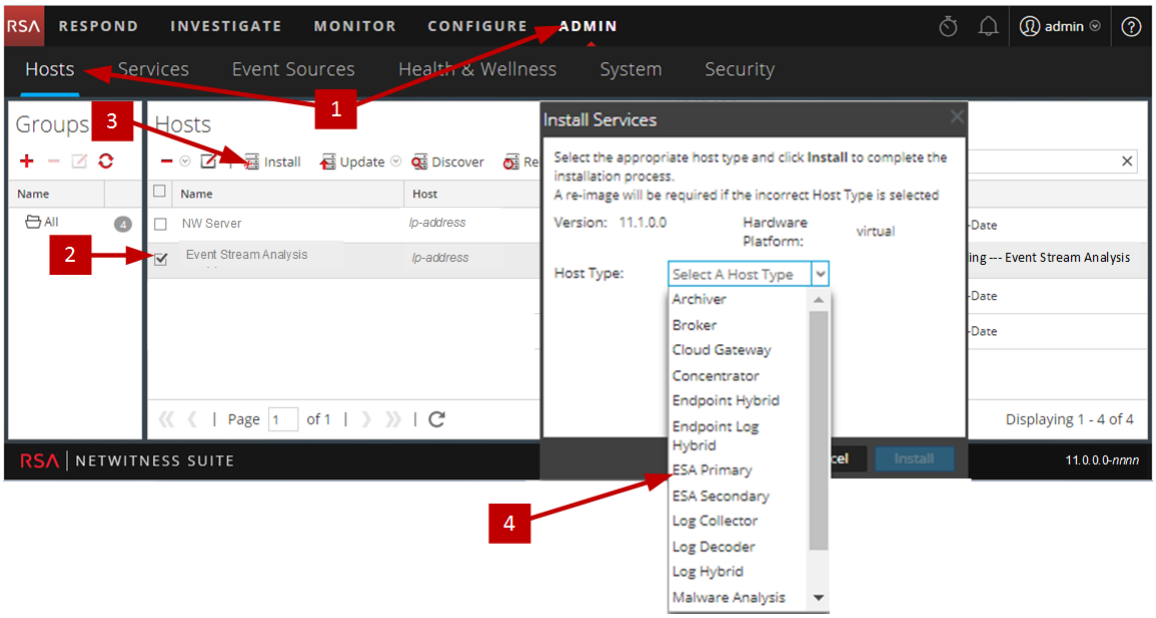


What do you want to do?

See Hosts and Services Procedures for detailed instructions of the following tasks.

Role	I want to ...
Administrator	Setup up a host.
Administrator	Maintain a host.
Administrator	Apply version updates to a host.

Quick Look



The following example shows you how to set up a host.

1. Select ADMIN > Hosts.
2. Select the host you deployed (for example, **Event Stream Analysis**).
3. Click Install (Install icon).
4. Select the host type to install from the **Install Services** dialog (for example, **ESA Primary**). This host type installs the Entity behavior Analytics, Context Hub, and Event Stream Analysis services on this host.

Hosts Panel Toolbar

The Hosts view toolbar contains the tools that you use to maintain the hosts in your NetWitness Suite deployment.

In NetWitness Suite, go to **Admin** > **Hosts** to access the Hosts view. The Hosts panel toolbar is at the top of the Hosts grid in the Hosts view.

Features

The following table describes the features of the Hosts panel toolbar.

Features	Description
	Remove From Group: If the host is part of a host group, you can remove the host from the group.
	Open the Edit Host dialog in which you edits a host or service identification and basic communication settings. This dialog has the same features as the Add Host dialog. Related procedure: Step 1. Deploy a Host
Install	Opens the **Install Services** dialog from which you can install a service on a deployed host. Related procedures: Step 2. Install a Service on a Host
Update	• **Update** - Updates the host or hosts you have selected with the version you select in the **Update Version** column. • **Check for Updates** - Checks the Local Update Repo for the latest updates available from RSA. Related procedure: Apply Version Updates to a Host
Discover	Most of the time, the Discovery function completes automatically and you do not need to click the Discover button. For a fresh installation, click Discover to access the Provision dialog box so you can complete the provisioning phase. After the provisioning phase, NetWitness Suite automatically discovers services running on the host and you do not need to click Discover. For a fresh installation, click **Discover** to access the **Provision** dialog box so you can complete the provisioning phase. After the provisioning phase, NetWitness Suite automatically discovers services running on the host.

Features	Description
Reboot Host	Restart the host.
Filter	Filter hosts by Name or Host.

Groups Panel Toolbar

The Groups panel toolbar provides options for managing groups of hosts. Use the toolbar to create, edit, and delete groups. After you create a group, you can drag individual hosts from the Hosts panel into that group.

Use groups may to organize hosts by function, geography, project, or any other organization principle that is useful. A host may belong to more than one group.

In NetWitness Suite, go to **ADMIN > Hosts**. The Groups panel toolbar is at the top of the Groups grid in the Hosts view.

The Groups panel provides a way to create logical groups of hosts. Once hosts are grouped, it is easier to perform operations on multiple hosts by interacting with each host in a group rather than individual hosts from an non-grouped list.

Note: In NetWitness Live, groups can subscribe to resources while individual hosts can not.

The Groups panel consists of a grid populated with a list of defined host groups and the Groups Panel Toolbar.

Column	Description
	Displays a new row in the Group grid in which you enter the name of a new group.
	Asks for confirmation that you want to delete the group or host. You can confirm or cancel the deletion.
	Opens the name field in a row of the Group grid so that you can type a new name for an existing group.

Column	Description
	Refreshes the selected group.
Name	The name of the host group. Click the group name in the Groups panel to list the hosts in that group on the Hosts panel.
<Blank>	Indicates the number of hosts in the group. Click the number of hosts in the group on Groups panel to list the hosts in that group on the Hosts panel.

Services View

You set up and maintain the NetWitness Suite services run in the **Services** view. With the Services view, you can:

- Quickly search for and locate a specific service or type of service, such as Log Decoder or Warehouse Connector
- Use shortcuts to get to administration tasks
- Add, edit, and remove services
- Manage licensing and view the license status of a service (licensed or unlicensed)
- Sort Services by Name and Host
- Filter services by Type and by Name and Host
- Start, stop, and restart services

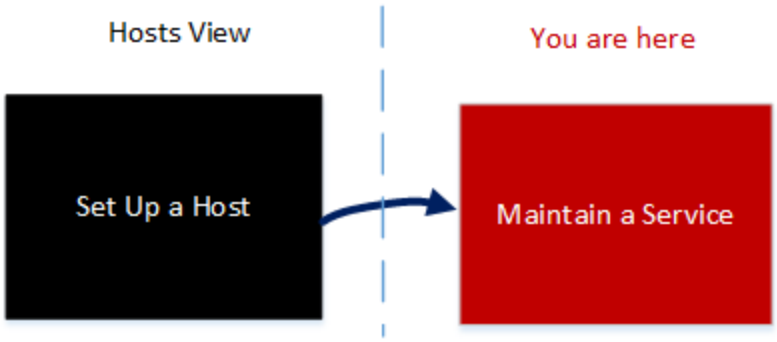
A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plug-in to enable or disable, according to the function of the host. You must configure the following Core services first:

Core	Other	Other	Other
Decoder	Archiver	IPDB Extractor	Warehouse Connector
Concentrator	Event Stream Analysis	Log Collector	Workbench
Broker	Context Hub	Malware Analysis	
Log Decoder	Incident Management	Reporting Engine	

You must configure hosts and services to communicate with the network and each other so they can perform their functions such as storing or capturing data.

Workflow

This workflow shows the procedures you complete to set up and maintain a service. Adding a service to a host is the first task in this workflow. The hosts with core services are set up out of the box. After that, you can set up additional services on hosts to enhance your NetWitness Suite deployment.



What do you want to do?

See Hosts and Services Procedures for detailed instructions of the following tasks.

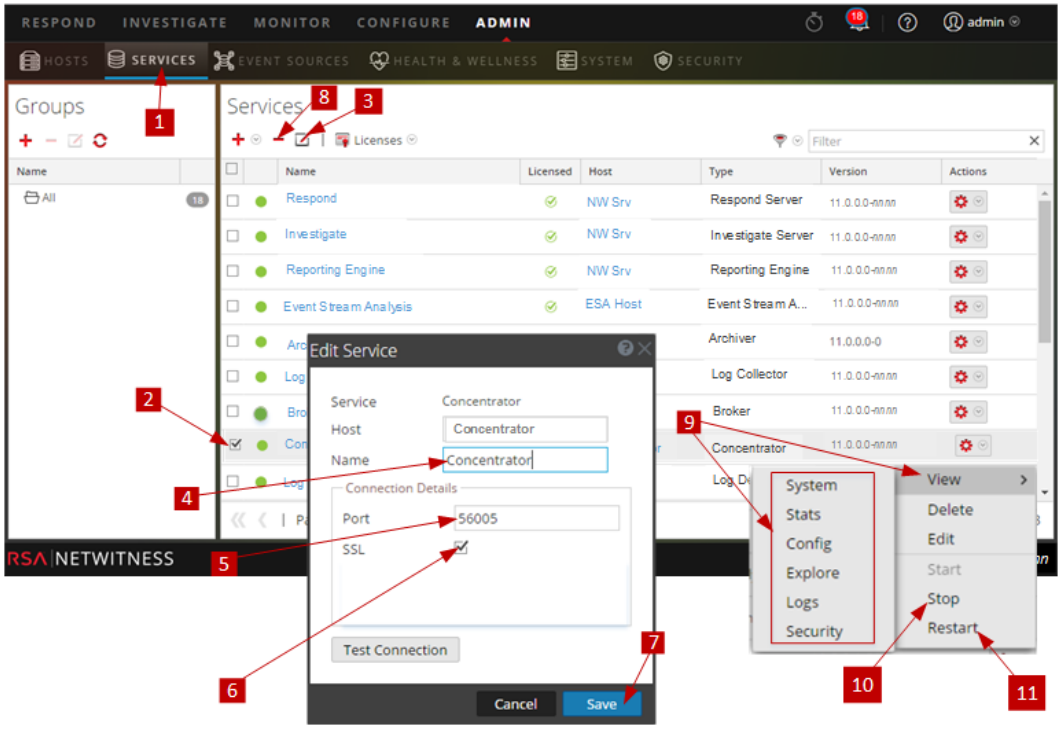
Role	I want to ...
Administrator	Maintain a service.
Administrator	Set up a host.

Related Topics

- Best Practices
- Troubleshoot Host Updates

Quick Look

The following example shows you how to maintain a service.



Select a Service.

1	Go to **ADMIN** > **Services** view.
2	Click the checkbox to the left of the service you want to select.

Edit the Service Name and Connection.

3	Click (Alternatively, select Edit from the (Action drop-down menu).
4	Edit the **Host** name.
5	Edit the service **Name**.
6	Edit the **Port** number.
7	Deselect or select SSL communication connection.
8	Click **Test Connection** .

Delete a Service.

9	**Select a Service** and click the delete icon.

View Service Statistics and Configure Parameters

10 Perform the following steps to view service statistics and configure a service parameters.

a. **Select a Service** and click the actions icon.

b. Click **View** and select:

- **System** to:
  - View current high-level information about the service and its host.
  - Access the System View toolbar.
- **Stats** to view detailed service statistics.
- **Config** to view and configure service parameters.
- **Explore** to view and configure service parameters in the NetWitness Suite Explore view.
- **Logs** to view log messages issued by the service.

10 **Select a Service**, click the actions icon, and click **Stop** a service that is running.

11 **Select a Service**, click the actions icon, and click **Restart** to restart a stopped service.

Topics

See the following RSA NetWitness Suite guides for detailed information on individual services. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Archiver Configuration Guide

Broker and Concentrator Configuration Guide

Cloud Behavioral Analytics Gateway Configuration Guide

Context Hub Configuration Guide

Decoder and Log Decoder Configuration Guide

Endpoint Insights Configuration Guide

Event Stream Analysis (ESA) Configuration Guide

Investigate and Malware Analysis User Guide

Log Collection Configuration Guide

Malware Analysis Configuration Guide

Reporting Engine User Guide

Respond Configuration Guide

Workbench Configuration Guide

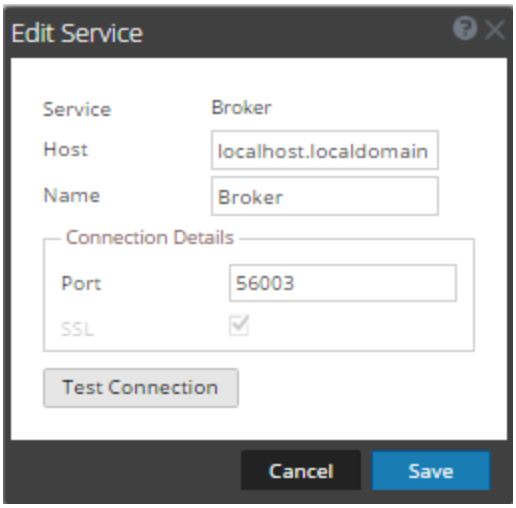
Warehouse Connector Configuration Guide

Edit Service Dialog

This topic introduces the Edit Service dialog accessible from the ADMIN Services view (ADMIN > Services).

NetWitness Suite services are automatically discovered in NetWitness Suite.

You can use the Edit Service dialog to modify services. To access the Edit Service dialog, go to **ADMIN > Services** and select **Edit** ( ) in the **Services** panel toolbar.



Procedures related to services are described in Hosts and Services Procedures.

Features

This table describes the features of the Add Service or Edit Service dialogs.

Field or Option	Description
Service	Displays the service type. You can add the following services: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.
Host	Specifies the host on which the service resides.

Field or Option	Description
Name	Specifies the name used to identify the service; for example, **Broker**. An understandable naming convention can make administrative tasks easier. Some administrators find it convenient to use the hostname or IP address (specified in the **Host** field) for the **Name** as well.
Port	Specifies the port used to communicate with this service. The default port based on the selected service type in the **Service** field is autofilled here. If you select **SSL** below, this port becomes an SSL port. If you do not select **SSL**, it becomes a non-SSL port. You can customize this port by opening a firewall for the port that you add. For information on ports, see the **Network Architecture and Ports** topic in the *Deployment Guide*.
SSL	Indicates that NetWitness Suite uses SSL for communications with this service.
Username	Specifies the user name used to log in to this service. The default username is **admin**.
Password	Specifies the password used to log in to this service. The default password is **netwitness**.
Entitle Service	(Optional) Assigns licenses from the local license server (LLS) to selected services. For more information, see the **View Current Entitlements** topic in the *Licensing Guide*.
Test Connection	Clicking this button tests the connection of a service that you are adding.
Cancel	Clicking this button closes the Add Service or Edit Service dialog. If you do not save the service before closing the dialog, the service is not added or edited.
Save	Clicking this button saves the new service.

Groups Panel Toolbar

This topic introduces the features and options in **ADMIN > Services** view > **Groups** panel toolbar.

The Groups panel toolbar provides options for managing groups of services. The toolbar includes options for creating, editing, and deleting groups. Once groups are created, you can drag individual services from the Services panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A service may belong to more than one group.

To access the Services view, in **NetWitness Suite**, go to **ADMIN > Services.** The Groups panel toolbar is at the top of the Groups grid in the Services view.

Features

This table describes toolbar features.

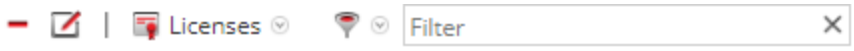
Option	Description
+	Displays a new row in the Group grid in which you enter the name of a new group.
−	Asks for confirmation that you want to delete the group or service. You can confirm or cancel the deletion.
✎	Opens the name field in a row of the Group grid so that you can type a new name for an existing group.
↻	Refreshes the selected group.

Services Panel Toolbar

This topic introduces the options in Service panel toolbar for adding, removing, editing, and licensing services. You can also filter the services listed in the Services Panel.

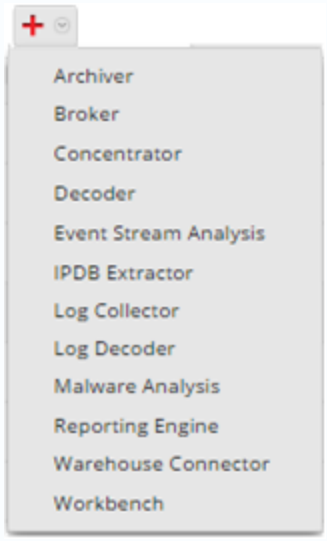
The Services panel toolbar has options for adding, removing, editing, and licensing services. You can filter the listed services based on and one or more service types, service name, and host.

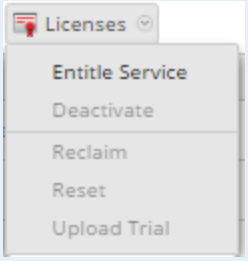
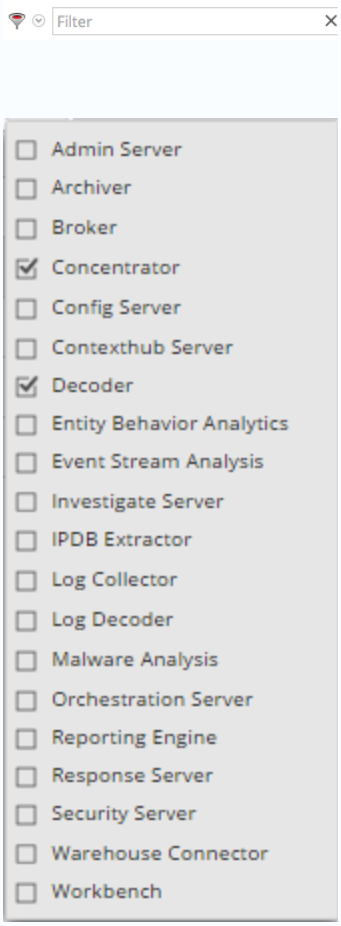
To access the Administration Services view, in **NetWitness Suite**, go to **ADMIN > Services.** The Services panel toolbar is at the top of the Services grid in the Services view.



Features

The table describes the features of the Services panel toolbar.

Feature	Description
	Adds a service for this instance of RSA NetWitness Suite to manage (see Step 2. Install a Service on a Host).
	Deletes a service from this instance of NetWitness Suite (see Edit or Delete a Service).
	Edits service identification and basic communication settings.

Feature	Description
	• Entitle Service: Assigns licenses from the local license server (LLS) to selected services (see the **Overview Tab** topic in the *Licensing Guide*). • Deactivate: Not used in NetWitness Suite 10.6. • Reclaim: Reclaims a deactivated license from LLS for the selected service. • Reset: Not used in NetWitness Suite 10.6. • Upload Trial: Not used in NetWitness Suite 10.6.
	Filters the services listed in Services view. In the Filter drop-down menu, you can filter the services by one or more selected service types. In this example, when you select Concentrator and Decoder, only the Concentrator and Decoder services appear in the Services view. In the Filter field, you can filter the services by Name and Host. You can use the Filter drop-down menu and the Filter field at the same time to filter the services listed in the Services view.

Services Config View

This topic introduces the features and functions of the Services Config view.

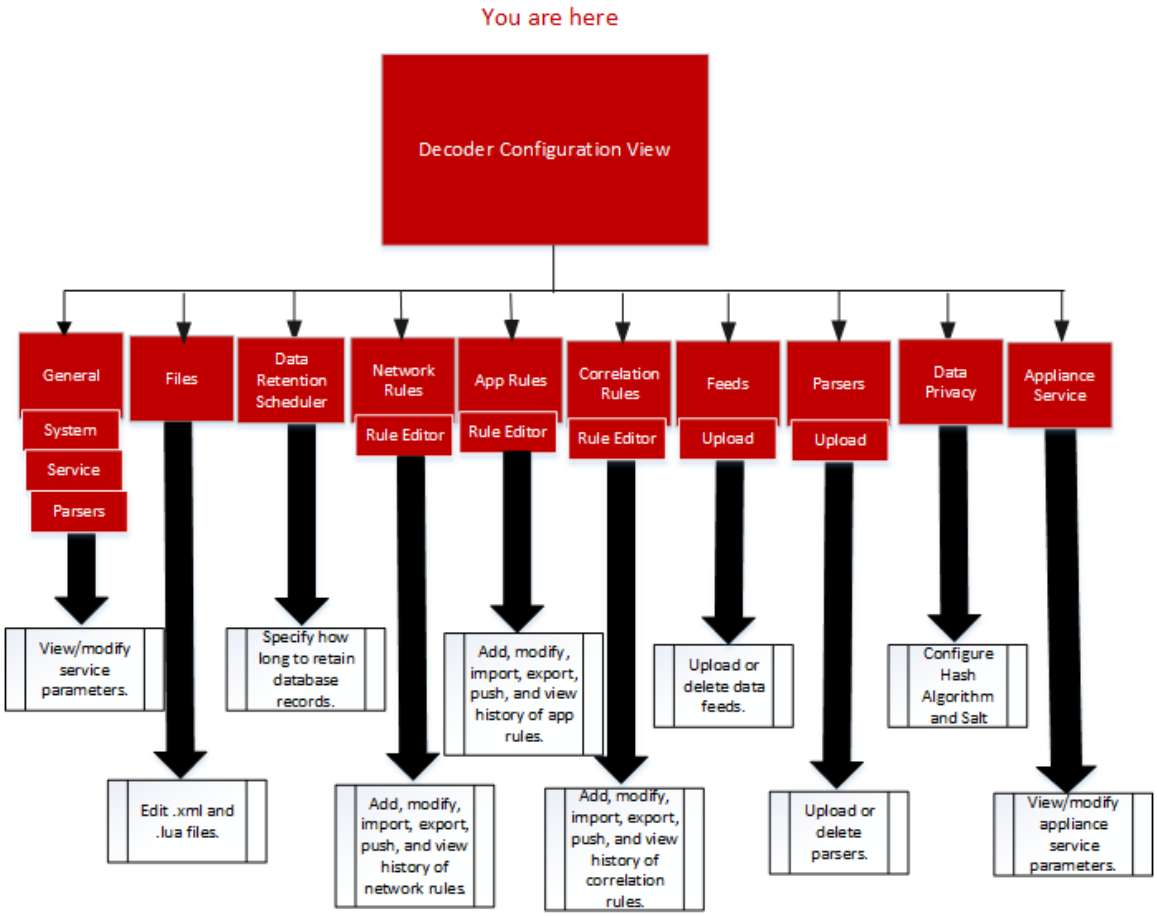
The Services Config view is one of the views available from the **Services** > Actions ( ) menu. It provides a user interface for configuring all aspects of a Core service or NetWitness Suite service.

The configuration options in the Services Config view are organized as tabs, with each tab providing a view of a set of related parameters. Unlike the Services Explore view, which offers direct access to all configuration files for a service, these tabs present the most commonly modified parameters of service configuration in a user-friendly view.

Due to configuration requirements for different services; each type of service has variations in available tabs and configuration parameters in this view. Individual topics describe configuration parameters that are specific to a host (Brokers and Concentrators, Decoders and Log Decoders) or service (for example, Reporting Engine, IPDB Extractor, Log Collector, and Warehouse Connector).

Workflows

The following workflow shows the configuration tasks for the Decoder service as an example of this view. See the Configuration Guides individual services (for example for the *RSA NetWitness® SuiteBroker and Concentrator Configuration Guide*) for details on their **ADMIN > Services > Config** Views.

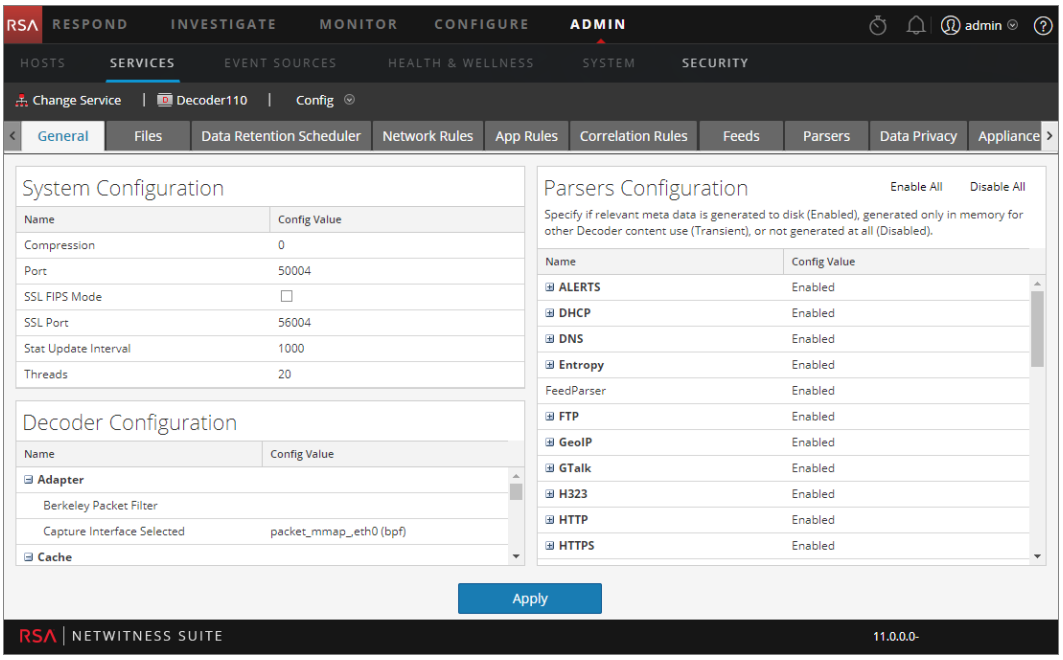


To access the Services Config view:

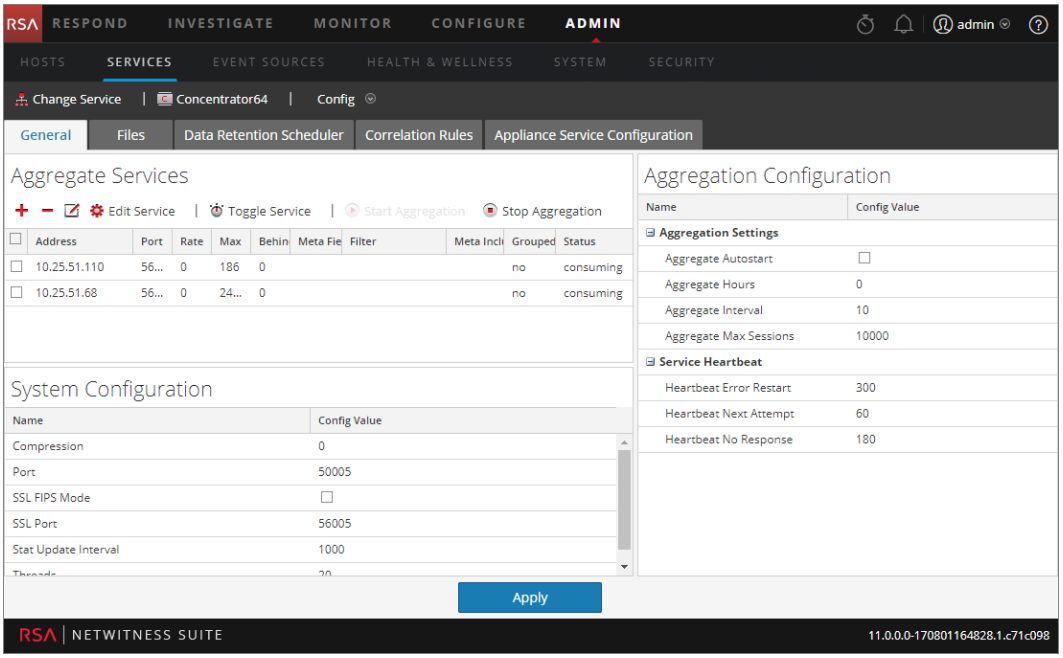
1. In **NetWitness Suite**, go to **ADMIN > Services**.
   The Administration Services view is displayed.
2. Select a service and select **>View > Config**.
   Services Config view for the selected service is displayed.

Quick Look

This is an example of the Services Config view for a Decoder.



This is an example of the Services Config view for a Concentrator.



Topics

- Topic
- Features
- Edit a Service Configuration File

Appliance Service Configuration Tab

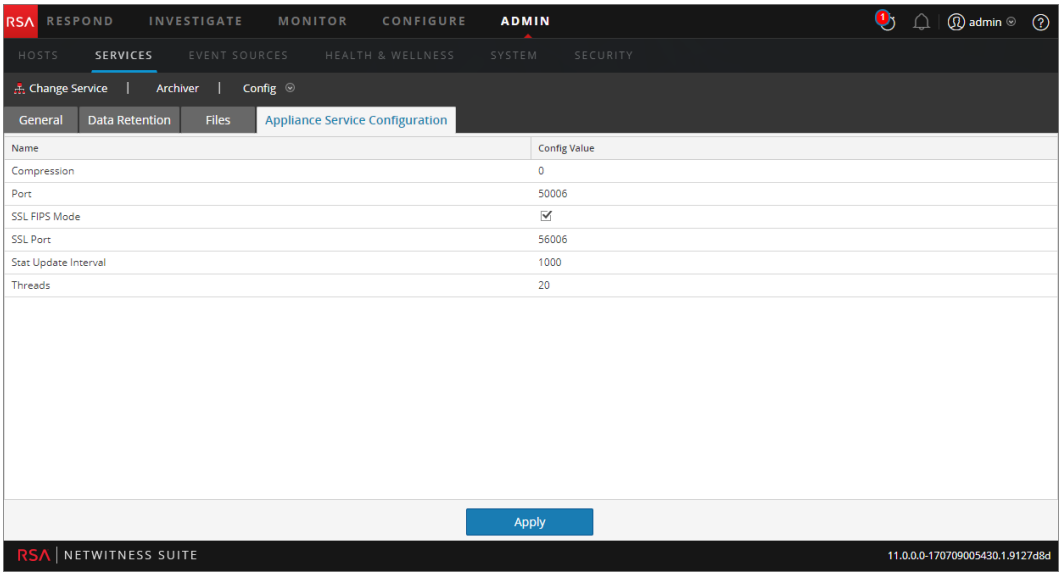
This topic lists and describes the available the configuration parameters for the NetWitness Suite Core Appliance service. The NetWitness Suite Core Appliance service provides hardware monitoring on legacy NetWitness hardware.

The Configuration view for the Archiver, Broker, Concentrator, IPDB Extractor, Decoder, Log Collector, or Log Decoder service has an Appliance Service Configuration tab.

To access the Appliance Service Configuration tab:

1. In **NetWitness Suite**, go to **ADMIN > Services**.
   The Administration Services view is displayed.
2. Select a service and select **>View > Config**.
   Services Config view for the Archiver service is displayed.
3. Click the **Appliance Service Configuration** tab.

This is an example of the Appliance Service Configuration tab for an Archiver.



Name	Description of Configuration Value	When Changes Take Effect
Compression	Compresses a message when it reaches the positive number (in bytes) that you specify.	The next time you connect to this service.
Port	Unencrypted listening port. **0** indicates that the port is disabled.	Upon restart of the service.
SSL FIPS Mode	One of the parameters you need to enable or disable Federal Information Processing Standards (FIPS). Refer to "Activate or Deactivate FIPS" in the RSA NetWitness® Suite System Maintenance Guide for detailed instructions.	Upon restart of the service.
SSL Port	SSL (Secure Sockets Layer) listening port. **0** indicates that the port is disabled. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.	Upon restart of the service.
Stat Update Interval	How often (in milliseconds) the system updates statistic nodes for monitoring Health and Wellness.	Immediately.
Threads	Threads in thread pool required to used to handle requests. The **Threads** parameter works with the **Polling Interval** parameter for event and log threads.	Immediately.

Topic

Appliance Service Configuration Parameters

Data Retention Scheduler Tab

This topic describes the configurable options in the Data Retention Scheduler tab for Decoder, Log Decoder, and Concentrator.

In the Data Retention Scheduler tab, you can define the criteria for removing database records from primary storage on Decoder, Log Decoder, and Concentrator services, and schedule the timing for checking the threshold.

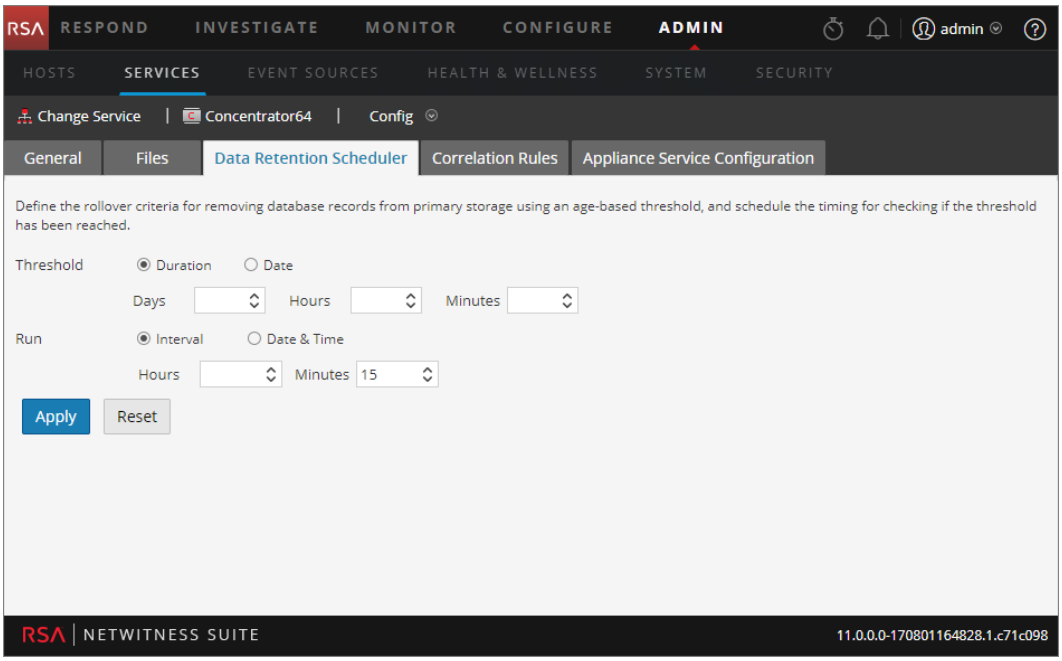
For information on the Data Retention tab for Archiver, see the **Data Retention Tab - Archiver** topic in the *Archiver Configuration Guide*.

Note: If additional customization is necessary, it can be done using the Scheduler under the Files tab in the Services Config view. For example, if more storage is available to save the RAW data versus the meta, it may make more sense to use Capacity as the threshold and to set different thresholds per database (meta versus packet).

To access the Data Retention Scheduler tab:

1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a Decoder, Log Decoder, or Concentrator, and then select **> View > Config**.
3. In the **Services Config** view for the service, click the **Data Retention Scheduler** tab.

The following figure illustrates the parameters in the Data Retention Scheduler tab for a Concentrator.



Features

The Data Retention Scheduler tab has sections to specify Threshold settings and Run settings. The following table lists the parameters supported for data retention configuration.

Parameter	Description
Threshold	The threshold is based on the age of the data, the amount of time the data has been stored or the date on which the data was stored. The date is from the database file, not from the actual session time. • **Duration**: The duration of time that data can be stored before removal. Specifies the number of days (365 maximum), hours (24 maximum), and minutes (60 maximum) that have elapsed since the time stamp on the data. • **Date**: The removal of data based on the date of the timestamp. Specifies the monthly date and time in the **Calendar** and **Time** fields.
Run	The schedule for running the job that checks rollover criteria. • **Interval**: Schedule the database check to occur at a regular interval. Specifies the **Hours** and **Minutes** between the scheduled checks. • **Date and Time**: Schedule the database check to occur at a regular day and time. Specifies the day from the drop-down list and the system clock time in `hh:mm:ss` format. Possible values for day are **Everyday**, **Weekdays**, **Weekends**, and **Custom**, where **Custom** allows you to select one or more specific days of the week.
Apply	Overwrites any previous schedule for this service and applies the new settings immediately. **Caution:** Once these settings have been applied and the threshold is met, the old data will be deleted from the database and no longer accessible.
Reset	Resets the schedule to the last applied state.

Files Tab

This topic describes the service configuration files that are visible in the Services Config view > Files tab.

The Files tab in the Services Config view is the user interface for editing service configuration files—Decoders, Log Decoders, Brokers, Archivers, and Concentrators—as text files.

The files available to edit vary depending upon the type of service being configured. The files that are common to all Core services are:

- The service index file.
- The netwitness file.
- The crash reporter file.
- The scheduler file.
- The feed definitions file.

In addition, the Decoder has files that configure parsers, feed definitions, and a wireless LAN adapter.

Note: The default values in these configuration files are generally good for the most common situations; however, some editing is necessary for optional services, such as the crash reporter or scheduler. Only administrators with a good understanding of the networks and the factors that affect the way services collect and parse data should make changes to these files in the Files Tab.

More detail on the service configuration parameters is available in the Service Configuration Settings.

To access the Files tab:

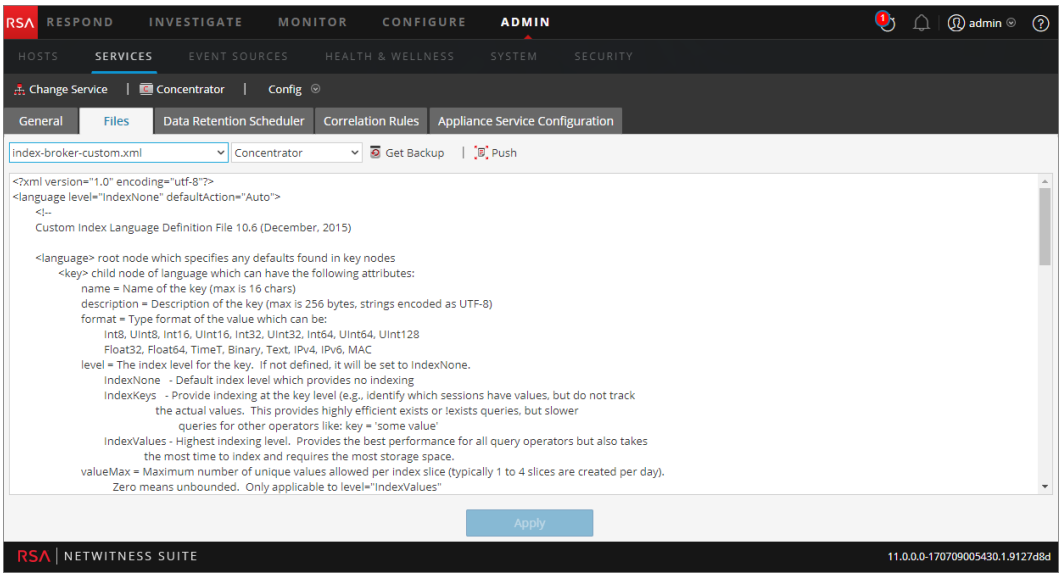
1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a service and select **> View > Config**.

   The Services Config view is displayed with the **General** tab open.
3. Click the **Files** tab.

Role	I want to ...
Administrator	Edit a Service Configuration file.

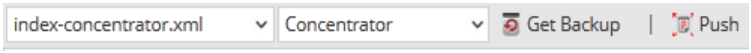
Edit a Service Configuration File

This is an example of the Files tab.

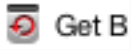
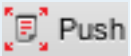


Files Tab Toolbar

The Files tab has a toolbar and an edit window. This is an example of the toolbar.



These are the features of the Files tab toolbar.

Feature	Description
File drop-down list	Displays a list of files that the system is currently using. When you select a file, the text of the file is displayed in the text edit window. In the text window, you can edit the file and save the changes, or create alternate files to use.
Service / Host drop-down list	Displays the service type and host. You can open a file from either the service or the host for editing.
	Retrieves the latest backup of the current file, which can prove useful when you have made changes and want to go back to the previous version of the file. The backup does not replace the current file unless you click **Save**.
	Displays a dialog in which you can select services of the same type and push the currently viewed file to the services.

Feature	Description
Apply	Overwrites the current file, creates a backup file.

Services Explore View

This topic introduces the features of NetWitness Suite Services Explore view, a powerful and flexible user interface for viewing and editing host and service configurations.

The Services Explore View offers advanced access and control of all NetWitness Suite hosts and services. All services expose their functionality through a tree-like series of nodes, similar to the Windows Explorer view of your file system. Here you can:

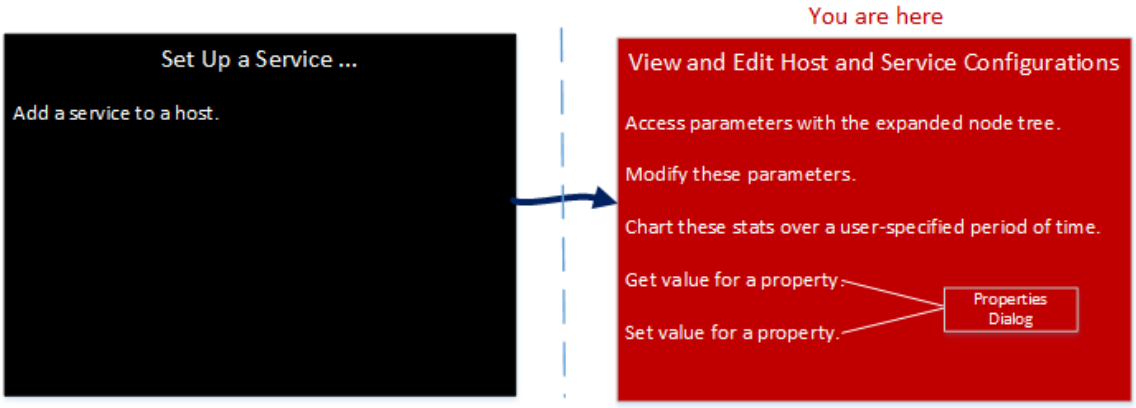
- View a directory tree showing common files for all selected services.
- Navigate down through the directory to a file.
- Open the same file for each service, and display the contents side by side.
- Select an entry in the file and edit the value.
- Apply a property value from one service to other services.

The Services Explore View can also display a Properties dialog, a simple interface for viewing properties of any node in the system and sending messages to the node, shown in the figure below.

Caution: A good understanding of the nodes and parameters is required when editing in this view. Incorrect settings can cause performance problems.

Workflow

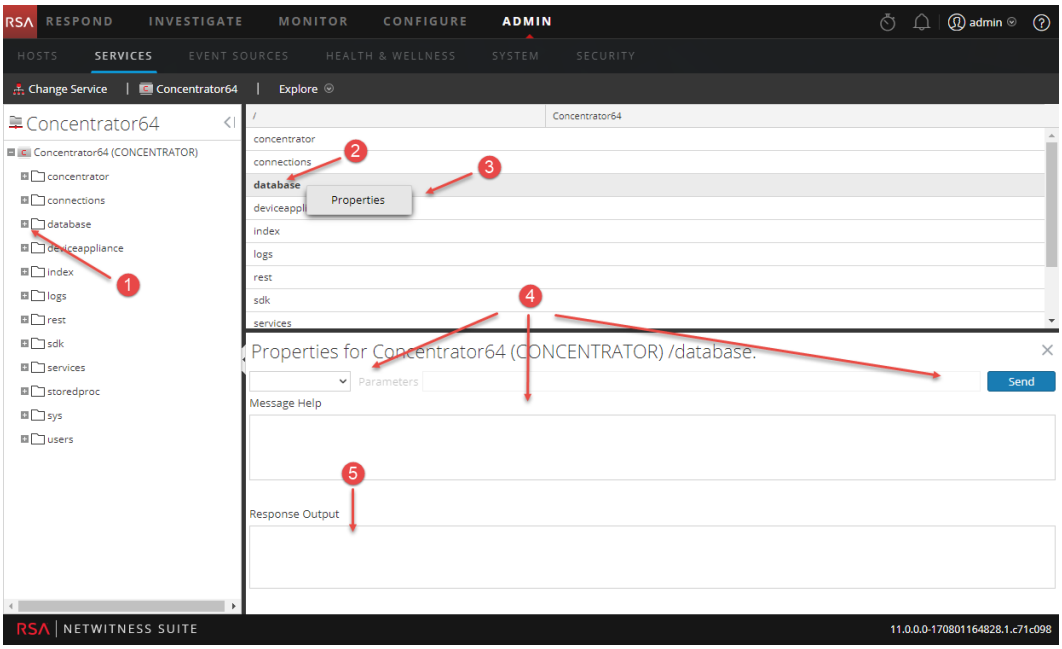
This workflow shows the tasks you perform from the Explore view.



Quick Look

To access the Services Explore view:

1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a service and select > **View** > **Explore**.



1	Expand the node to display its parameter categories.
2	Click a property (for example, **meta.dir**) to select it.
3	Right-click a node or category and click **Properties** to display the Properties dialog.
4	Perform an operation on a node or category: a. Select a command from the drop-down list. b. Enter a command string (if required). c. Click **Send**.
5	Review the output.

Features

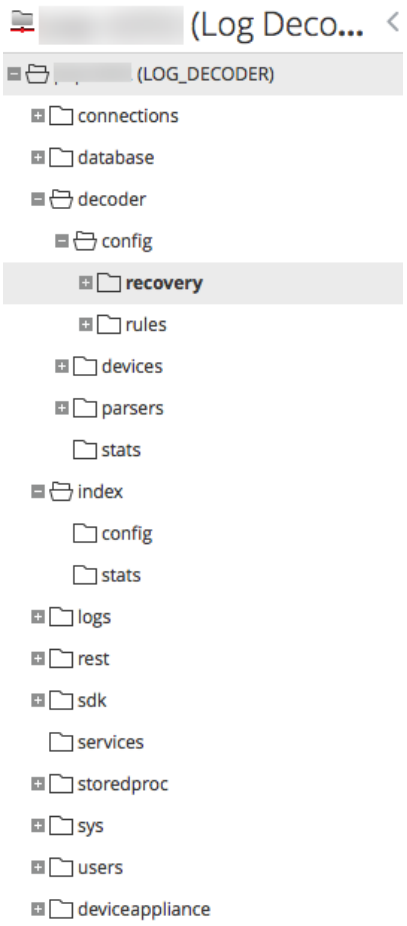
The **Services Explore View** has two main panels:

- The Node list
- The Monitor panel

You can access the Properties of any file by right-clicking the file and selecting Properties.

The Node List

The Node list displays the services as a tree-like series of nodes and folders. The levels in the Node list expand and collapse to display the full hierarchy.



Each root folder is named based on the functionality it exposes. For instance, the **/connections** folder shows all connected IP addresses. Underneath each **IP/Port** are two folders, **sessions** and **stats**.

- The **sessions** folder displays all authenticated user sessions originating from the IP/Port.
- The **stats** folder displays values, such as the number of messages sent/received, bytes sent/received, and others, set by the service. These are not editable.

Selecting any folder in the tree view displays its children in the **Monitor** panel. Every node in the tree is actively monitored, so when a statistic or configuration node changes value, it is immediately reflected in the tree and monitor panel.

The Monitor Panel

The **Monitor** panel displays properties and values for a selected node (such as **index**) and a child folder (such as **config**). There are two ways to edit values:

- Clicking the value and typing a new value
- Sending a **set** message in the Properties dialog

/Index/Config	(Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

Topics

- Features
- Log Decoder Service Configuration Parameters

Properties Dialog

This topic explains how to send messages to a system node in the Services Explore view > Properties dialog.

The Properties dialog opens below the Monitor panel when you select Properties from the context menu. The Properties dialog provides a user-friendly messaging tool for communication with system nodes. This is useful for getting and setting values for a property for multiple services.

All nodes support the help message, which contains:

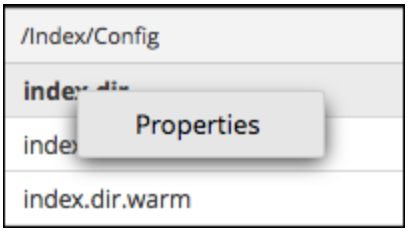
- A description of the node.
- The list of supported messages with a corresponding description.
- Security roles needed to access the messages.

The available messages vary according to the service and root folder. Many of these messages are also accessible as options with a NetWitness Suite dashboard or view.

To access the Properties dialog:

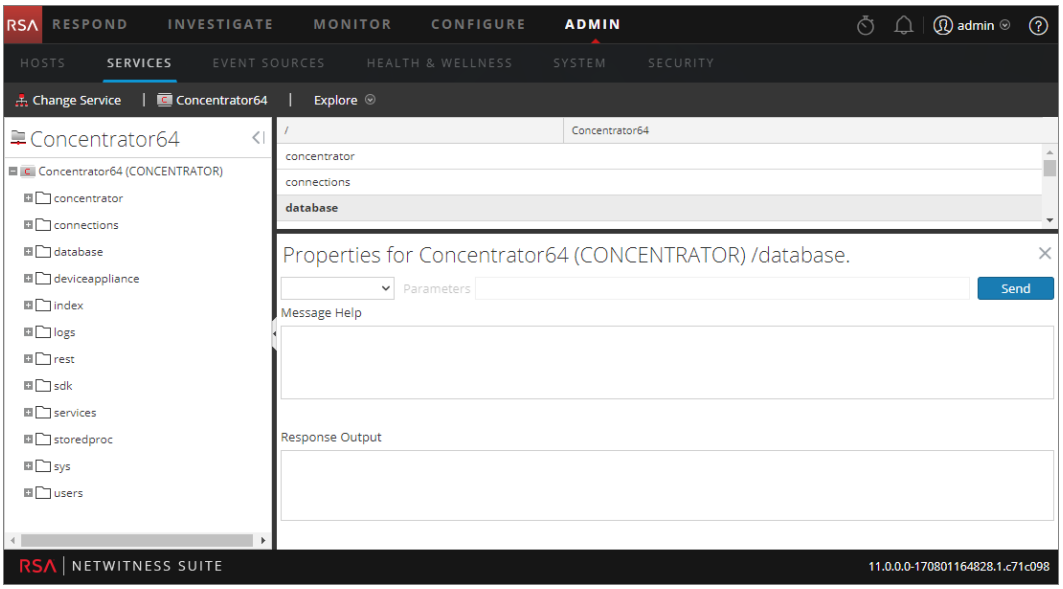
1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a service and select **> View > Explore**.
3. In the **Node** list, select a file.

4. In the **Monitor** panel, right-click a property and select **Properties**.



The Properties dialog is displayed. You can also right-click any file in the Node list to display the Properties dialog.

The following example shows the Properties dialog with help for a message (**info**) displayed.



Features

The Properties dialog has the following features.

Feature	Description
Message drop-down list	Lists all available messages for the current node. Select a message to send the node.
Parameters input field	Type the message parameters in this field.
Send button	Sends the message to the node.
Message Help	Displays help text for the current message.

Feature	Description
Response Output	Displays the response to a message or output from a message.

Services Logs View

This topic introduces the Services Logs view.

The Services Logs view provides the ability to view and search the logs for a specific service. The Services Logs view is identical to the System Logging Panel with two exceptions:

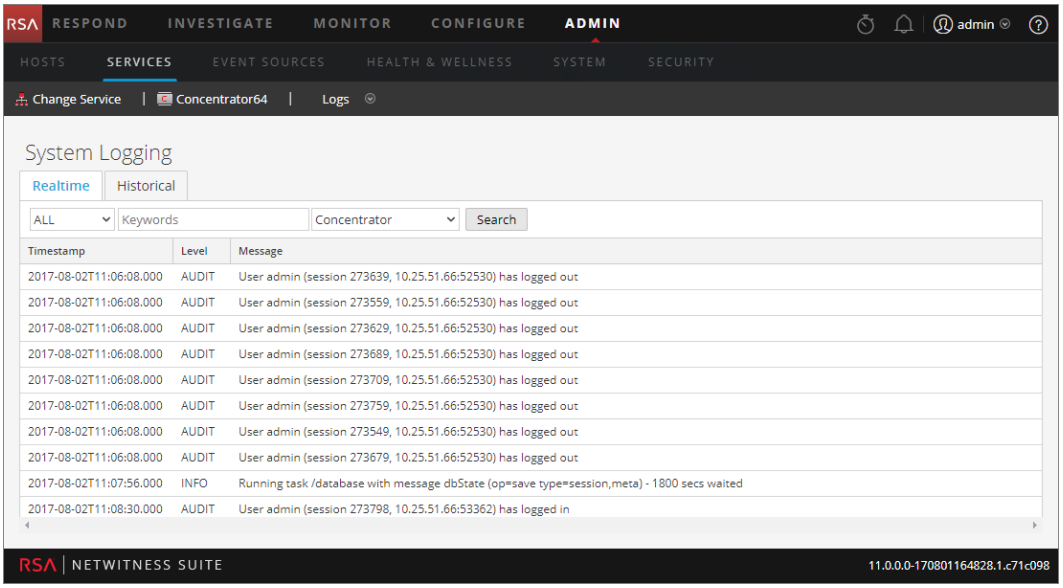
- The Services Logs view has an additional filter to select messages for the service or host.
- The System Logging panel has an additional tab for Settings.

Refer to System Logging Panel for a complete description of NetWitness Suite logging features.

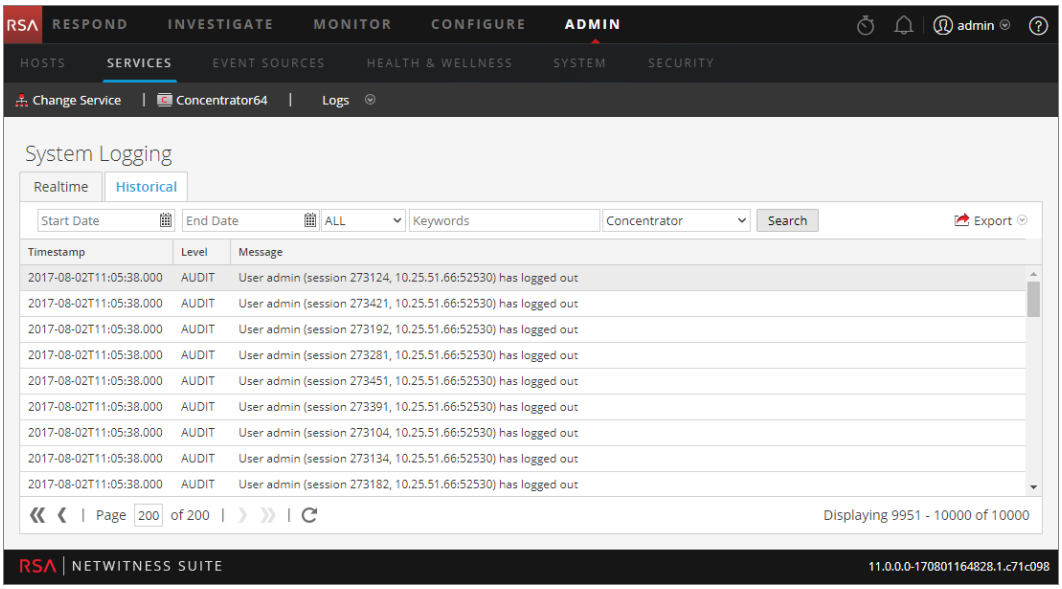
To view a service log:

1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a service and select **>View > Logs**.

The following figure shows the Services Logs view Realtime tab.



The following figure shows the Services Logs view Historical tab.



Features

The System Logging Panel has the following tabs, and the logging functions are described as part of system maintenance (see **Monitor Health and Wellness of Security Analytics** in the *System Maintenance* guide).

Feature	Description
Realtime tab	This is the monitor mode of the service log.
Historical tab	This is a searchable view of the service log.

Services Security View

This topic provides an overview of service security management in the Services Security view.

In NetWitness Suite, each service has a separate configuration of users, roles, and role permissions, which are managed in the Services Security view.

To access service information and perform service operations through NetWitness Suite, a user must belong to a role that has permissions on that service. For 10.4 or later NetWitness Suite Core services that utilize trusted connections, it is no longer necessary to create NetWitness Suite Core user accounts for users that log on through the web client. You only need to create NetWitness Suite Core user accounts for aggregation, thick client users, and REST API users.

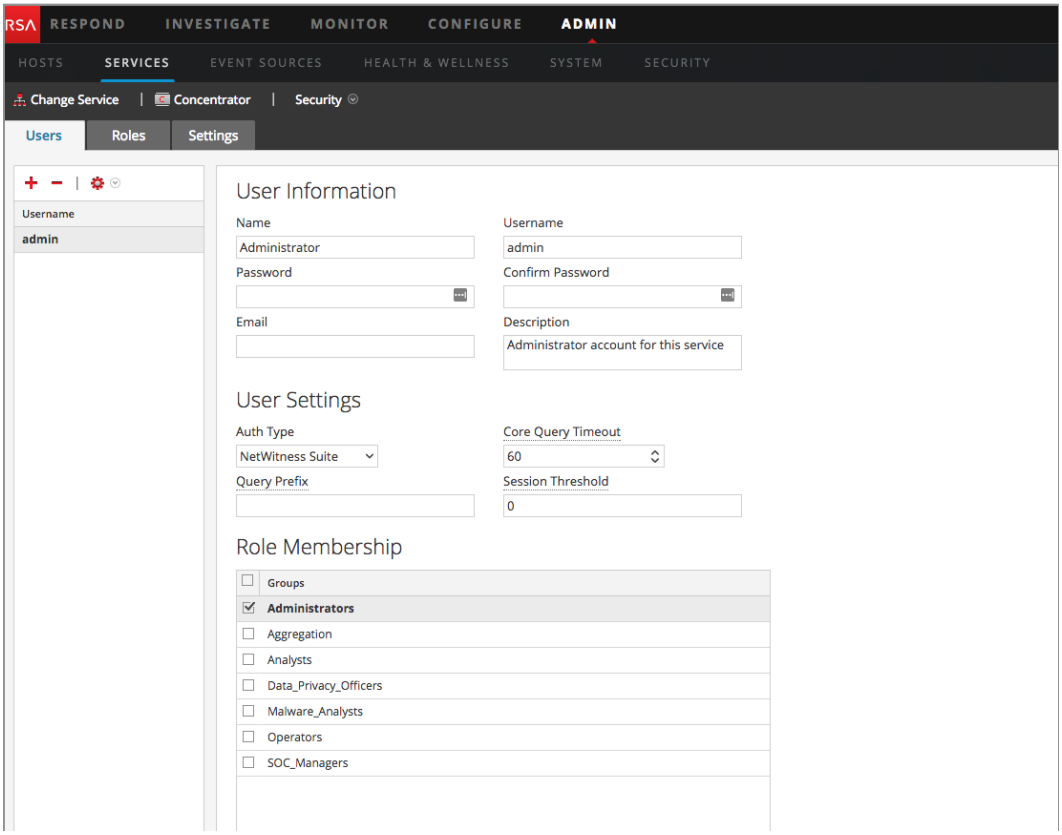
Note: Only the default admin user in NetWitness Suite is created by default on all services. As a prerequisite to managing service security, the default admin user account must be present in the NetWitness Suite Administration > Services view. For every other user, you must configure access to each particular service through NetWitness Suite.

Procedures related to this tab are described in Hosts and Services Procedures.

To access the Services Security view:

1. In **NetWitness Suite**, go to **ADMIN > Services.**
2. Select a service and select > **View > Security**.

   The Services Security view for the selected service is displayed.



Features

The Services Security view has three tabs, Users tab, Roles tab, and Settings tab.

Roles and Service Access

Primary considerations in configuring service security are defining the roles and assigning users to the roles. The Service Security view separates these two functions into the Users tab and the Roles tab.

- In the Roles tab, you can create roles and assign permissions to the roles for a selected service.
- In the Users tab, you can add a user, edit user settings, change the user password, and edit the role membership of the user for a selected service. Although you select a single service in the Services Security view, you can apply the settings for one service to other services.

Topics

- Roles Tab
- Service User Roles and Permissions
- Aggregation Role
- Settings Tab
- Users Tab

Roles Tab

This topic introduces the features of the Services Security View > Roles Tab.

The **Roles** tab enables you to create roles and assign permissions. Each role can have different permissions for different services. For example, the Analysts role can have different role permissions based on the selected service.

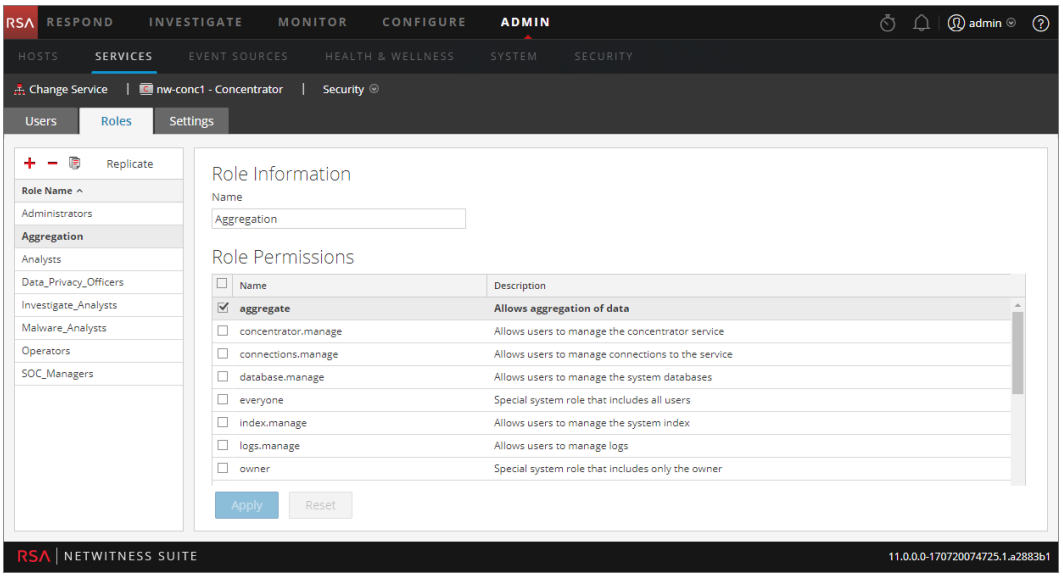
Before you can add users to roles, you need to define user roles, usually by function, and assign permissions to the roles.

Procedures related to this tab are described in Hosts and Services Procedures.

To display the **Services Security View > Roles** tab:

1. In **NetWitness Suite**, go to **ADMIN > Services.**
2. Select a service to which you want to add a user, and select **> View > Security**.
3. Select the **Roles** tab.

The following figure shows the Roles tab in the Services Security view.



Features

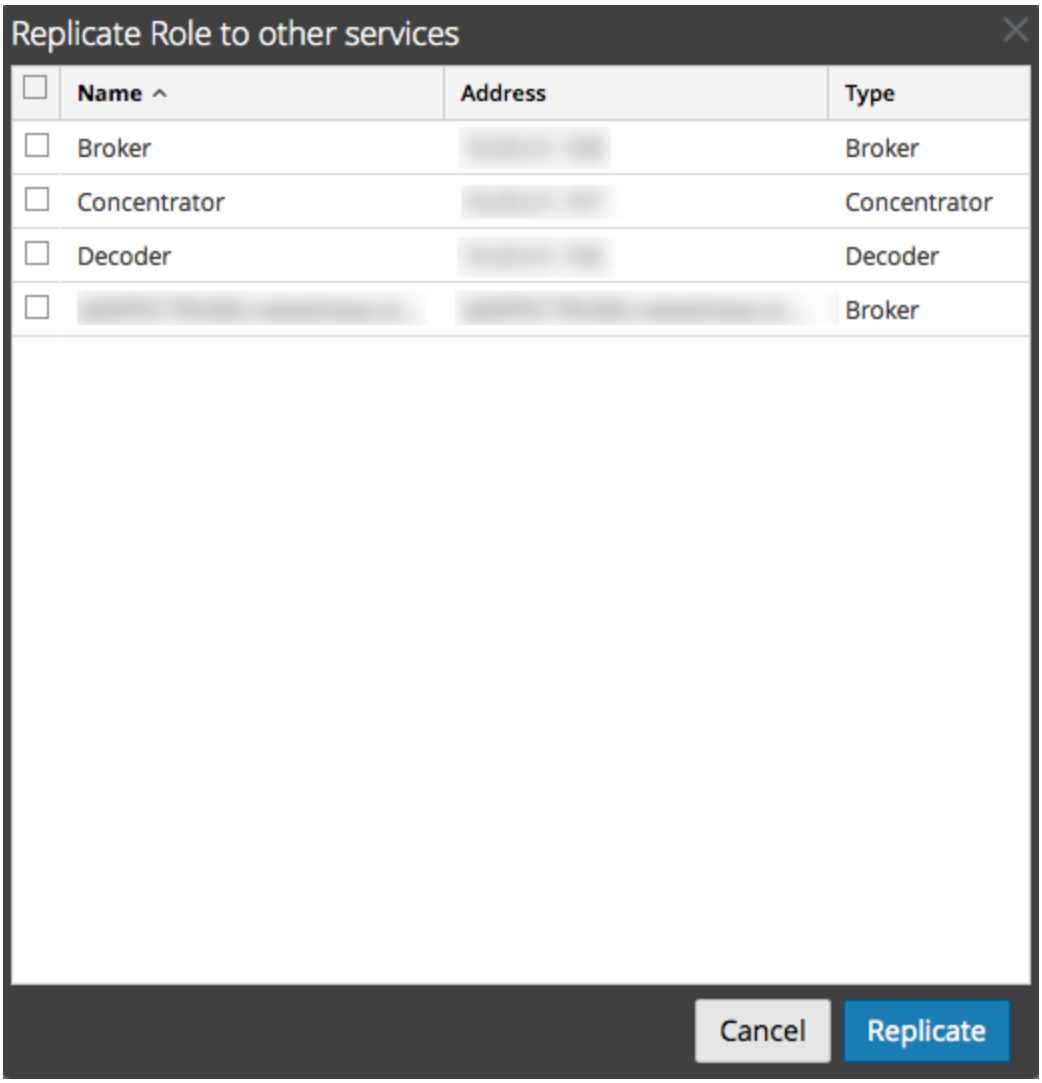
The Roles tab has a **Role Name** panel on the left. Selecting a role name shows the **Role Information** panel for the selected role on the right.

Role Name Panel

The **Role Name** panel has the following features.

Feature	Description
	Adds a new group to the current service.
	Deletes the selected group from the current service.
	Copies a role and its assigned permissions to a new role. The name of the new role must be unique. For example, you can copy the **Analysts** role and create another role with a new name, such as **Analyst_Managers**.
Replicate	Pushes a role and its assigned permissions to other services. After you select a role and click **Replicate**, the **Replicate Role to other services** dialog is displayed. In the dialog, you can select the services where you want to replicate the role.

The following figure shows the **Replicate Role to other services** dialog.



Role Information and Permissions Panel

The **Role Information and Permissions** panel defines role permissions.

There are two buttons:

- The **Apply** button saves the changes made in the Role Permissions panel and they become effective immediately.
- If you have not saved changes in the Role Permissions panel, the **Reset** button resets all fields and settings to their values before editing.

Service User Roles and Permissions

This topic describes the pre-configured service user roles and permissions.

The Services Security view Roles tab enables you to create service user roles and assign permissions. You can also use the pre-configured roles included with NetWitness Suite to assign user permissions.

Service User Roles

NetWitness Suite has the following pre-configured service user roles.

Role	Assigned Permissions	Personnel/Account
Administrators	All permissions	NetWitness Suite System Administrator
Aggregation	aggregate sdk.content sdk.meta sdk.packets	You can use this role to create an Aggregation account. This role provides the minimum permissions necessary to perform aggregation of data. It is only available on NetWitness Suite 10.5 and later services.
Analysts, Malware_ Analysts, and SOC_ Managers	sdk.meta sdk.content sdk.packets storedproc.execute	Users can use specific applications, run queries and view content for purposes of analysis.
Data_Privacy_ Officers	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	Data Privacy Officer Data Privacy Officers have the dpo.manage permission on Decoders and Log Decoders.

Role	Assigned Permissions	Personnel/Account
Operators	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	Operators are responsible for the daily operation of the services.

Service User Permissions

There are many permissions that you can assign a service role in NetWitness Suite. Users can have different permissions on each service, depending on their role assignments and the permissions selected for each role. This table describes the permissions that you can assign to a role.

Permission	Definition
sys.manage	Allows the user to edit the service configuration settings.
services.manage	Allows the user to manage connections to other services.
connections.manage	Allows the user to manage connections to the service.
users.manage	Allows the user to create individual users and user roles and specify user permissions.
aggregate	Allows the user to perform aggregation of data.

Permission	Definition
sdk.meta	Allows the user to run queries in the Investigation and Reporting applications and to view the metadata returned by the query.
sdk.content	Allows the user to access raw packets and logs from any client application (Investigations and Reporting).
sdk.packets	Allows users to access raw packets and logs from any client application.
appliance.manage	Allows the user to manage the appliance (host) tasks. This permission is required by the Appliance service.
decoder. manage	Allows the user to edit the configuration settings for the Decoder service.
concentrator.manage	Allows the user to edit the configuration settings for the Concentrator/Broker service.
logs.manage	Allows the user to view the service logs and edit the logging configuration settings for the specified service.
parsers.manage	Allows the user to manage all attributes under the parsers node.
rules.manage	Allows the user to add and delete all rules.
database.manage	Allows the user to set database locations, sizes, and the various configuration settings for the session, meta and/or packet/log databases.
index.manage	Allows the user to manage all index-related attributes.
sdk.manage	Allows the user to view and set all SDK configuration items.
storedproc.execute	Allows the user to execute a Lua stored procedure.
storedproc.manage	Allows the user to manage Lua stored procedures.
archiver.manage	Allows the user to modify the Archiver configuration.

Permission	Definition
dpo.manage	Allows the user to manage the transform configuration and the applicable keys.

Aggregation Role

This topic describes the Aggregation role and permissions that allow service users to perform aggregation.

The Aggregation role is a service user role intended only for aggregation of data. It has the minimum role permissions required to do aggregation:

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

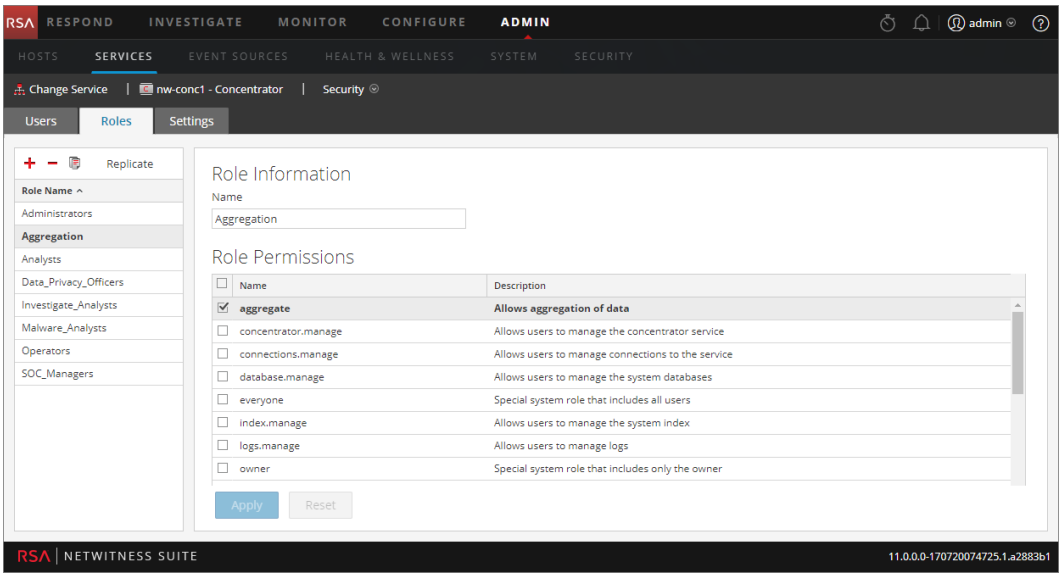
The Aggregation role is available only on NetWitness Suite 10.5 and later services and it can be used for an aggregation account. Members of this role or service users with these permissions can perform aggregation on Decoders, Concentrators, Archivers, and Brokers. The **aggregate** permission allows service users to perform aggregation of sessions and metadata along with raw packets and logs.

You can still use the decoder.manage, concentrator.manage, and archiver.manage permissions, but the Aggregation role permissions allow aggregation only and prevent the other available operations.

You access the service roles from the ADMIN > Services (select a service) > Actions > View > Security > Roles tab.

Procedures related to roles are described in Hosts and Services Procedures. Service User Roles and Permissions provides detailed information on the pre-configured roles.

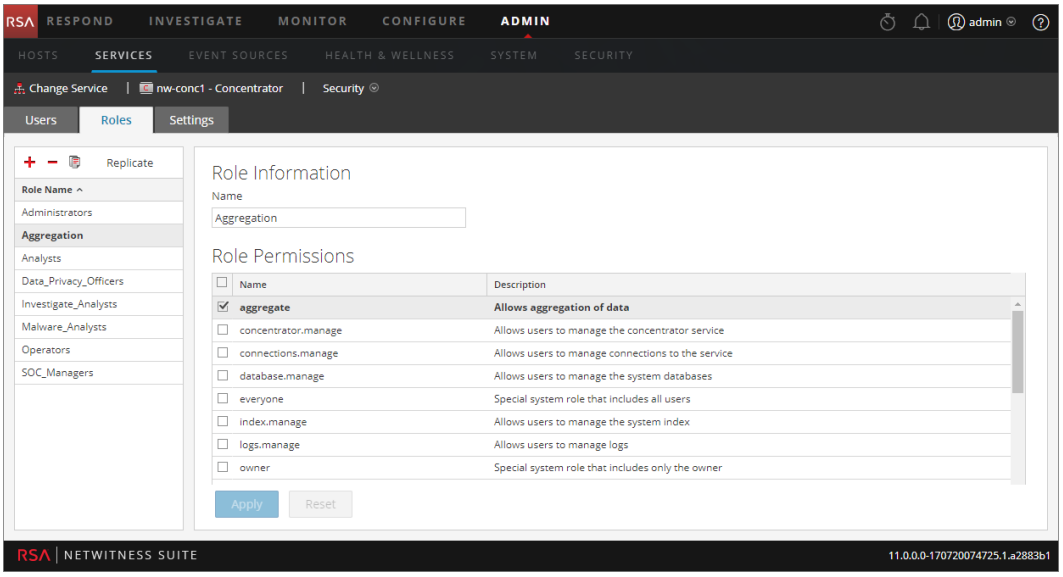
The following figure shows the permissions in the Aggregation role.



Settings Tab

This topic describes the features of the Services Security view > Settings tab.

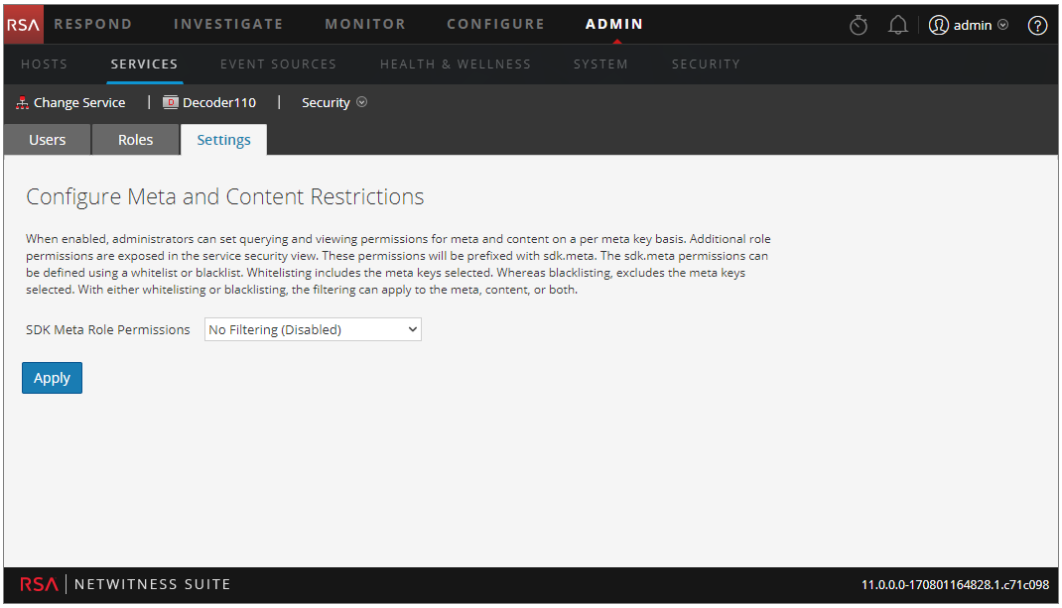
In the Services Security view Settings tab, Administrators can enable and configure system roles that define permissions on a per meta key basis for individual Brokers, Concentrators, Decoders, and Log Decoders. Configuring this feature adds configurable meta keys to the Services Security view > Roles tab so that individual meta keys can be applied to specific roles on a specific service. The following figure illustrates this.



This configuration is generally part of a data privacy plan implemented to ensure that specific types of content consumed or aggregated by a service are kept secure by limiting visibility of the meta data and content to privileged users (see *Data Privacy Management*).

To display the tab:

1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. In the **Services** grid, select a Decoder or Log Decoder service, click **> View > Security,** and click the **Settings** tab.



Features

The tab includes two features.

Feature	Description
SDK Meta Role Permissions field	Provides option for disabling or configuring meta key and content restrictions. The filtering options are described.
Apply button	Applies the selected configuration immediately. If not disabled, the meta keys are added to the Roles tab so they can be applied to specific roles.

SDK Meta Role Permissions Options

The following table lists the filtering options available in the SDK Meta Role Permissions selection list, and the numeric values used to disable (0) and the types of filtering (1 through 6).

Note: There is no need to know the numeric value unless configuring meta and content visibility manually in the system.roles node.

system.roles Node Value	Settings Tab Option	Description
0	No Filtering (Disabled)	System roles that define permissions on a per meta key basis are disabled.
1	Whitelist meta and content	Meta and content for the specified SDK meta roles are white listed, or visible to users assigned the system role.
2	Whitelist only meta	Meta for the specified SDK meta roles is white listed, or visible to users assigned the system role.
3	Whitelist only content	Content for the specified SDK meta roles is white listed, or visible to users assigned the system role.
4	Blacklist meta and content	Meta and content for the specified SDK meta roles are black listed, or not visible to users assigned the system role.
5	Blacklist only meta	Meta for the specified SDK meta roles is black listed, or not visible to users assigned the system role.
6	Blacklist only content	Content for the specified SDK meta roles is black listed, or not visible to users assigned the system role.

Users Tab

This topic explains the features of the Services Security view > Users tab.

In the Services Security view, the Users tab enables you to configure the following for a service:

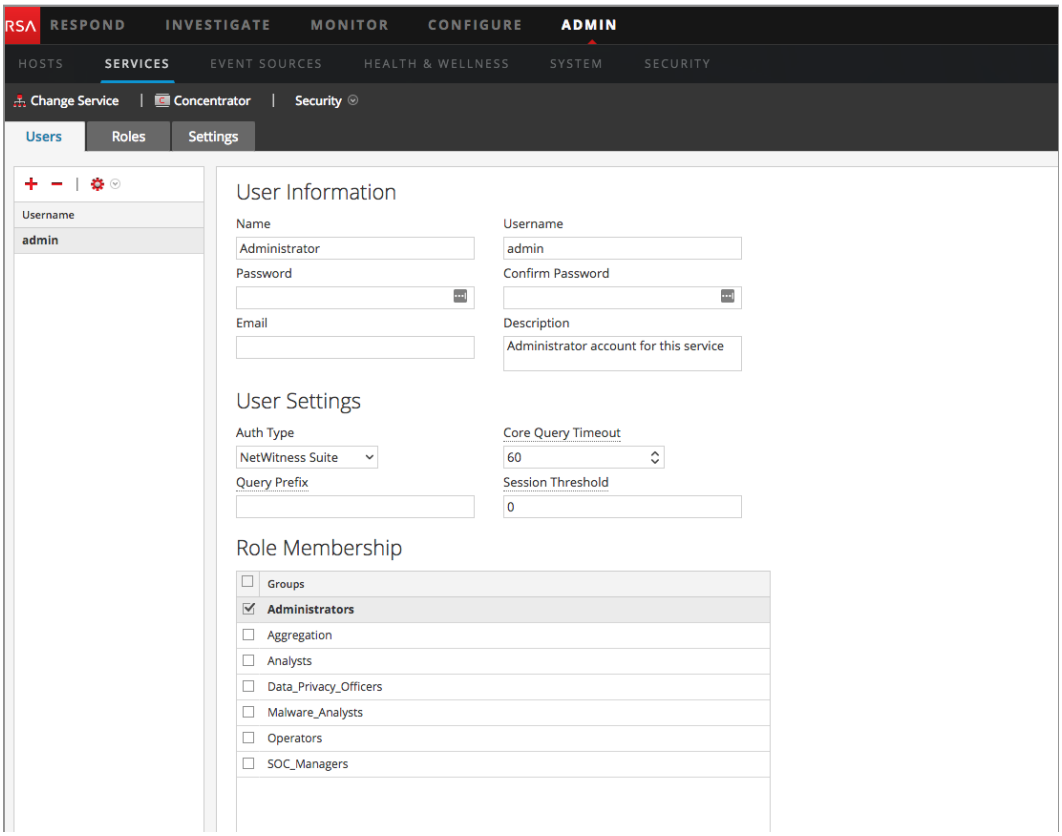
- Add user accounts.
- Change service user passwords.
- Configure user authentication properties and query handling properties for the service.
- Specify the user role membership, which specifies the roles that the user belongs to on the selected service.

Note: For 10.4 or later NetWitness Suite Core services that utilize trusted connections, it is no longer necessary to create NetWitness Suite Core user accounts for users that log on through the web client. You only need to create NetWitness Suite Core user accounts for aggregation, thick client users, and REST API users.

Procedures related to this tab are described in Hosts and Services Procedures.

To access the Services Security view > Users tab:

1. In **NetWitness Suite**, go to **ADMIN > Services.**
2. Select a service to which you want to add a user, and select **> View > Security**.



Features

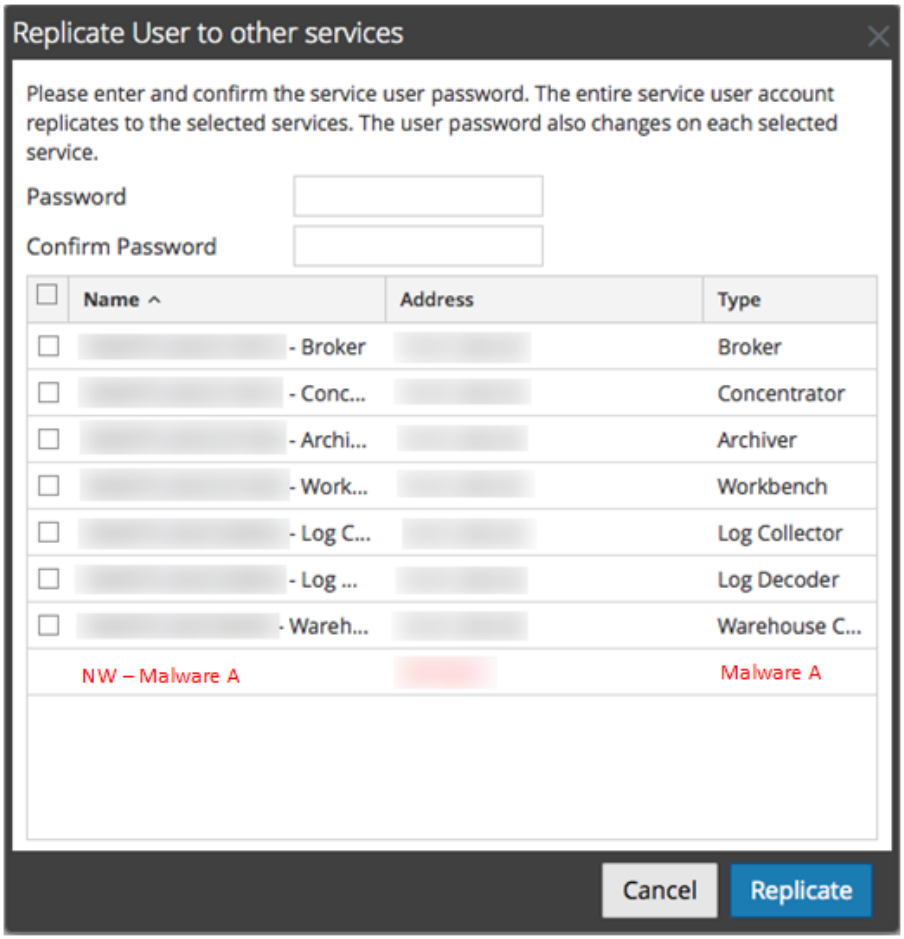
The Users tab has a User List panel on the left. Selecting a username makes the User Definition panel on the right available.

User List Panel

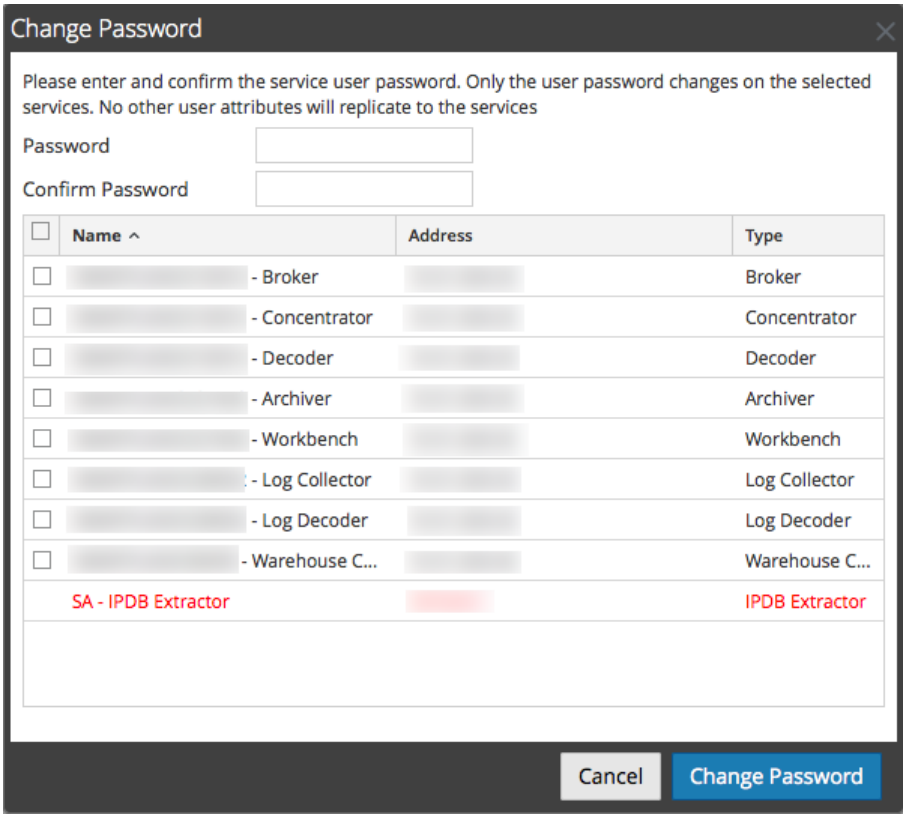
The User List panel has the following features.

Feature	Description
+	Adds a new user to the current service.
−	Deletes the selected users from the service.
⚙	Performs one of the following actions on the selected service user account: • **Replicate:** Replicates the entire service user account to selected services. • **Change Password:** Changes the password of a service user and replicates the new password to Core services with that user account defined. The Change Password option replicates only the password change to the Core services selected and does not replicate the entire user account.
Username	The user names for all user accounts that access the service. The username must be one used to log on to NetWitness Suite.

The following figure shows the **Replicate User to other services** dialog.



The following figure shows the **Change Password** dialog.



User Definition Panel

The User Definition panel has three sections:

- User Information identifies the user as created in the Administration Security view.
- User Settings define parameters that apply to this user's access to the service.
- Role Membership defines user roles to which the user belongs.

There are two buttons:

- The **Save** button saves the changes made in the User Definition panel, and they become effective immediately.
- If you have not saved changes in the User Definition panel, the **Reset** button resets all fields and settings to their values before editing.

User Information

The User Information section has the following features.

Field	Description
Name	The name of the user.
Username	The username that this user enters to log on to the service. This is the NetWitness Suite username generated when the administrator added the user and the associated credentials in the **Administration Security** view (Administration > Security).
Password (and **Confirm Password**)	The password that the user enters to log on to the service. This is the NetWitness Suite password generated when the administrator added the user and the associated credentials in the **Administration Security** view. The NetWitness Suite account password and the service password must match in order to allow the user to connect to the service through NetWitness Suite.
Email	(Optional) The user's email address.
Description	(Optional) A general description field to describe this user.

User Settings

The User Settings section has the following features.

Field	Description
Auth Type	The authentication scheme for this user. The product line supports internal and external authentication. • **Netwitness** specifies internal authentication, and is enabled by default. In this mode, all users must authenticate with the user account and passwords that are generated when the administrator uses the NetWitness Suite Administration Security view (Administration > Security) to create the user and their associated credentials. • **External** specifies that authentication is enabled through the host interface with PAM (Pluggable Authentication Modules). For more information, see the **Configure PAM Login Capability** topic in the *System Security and User Management* guide.

Field	Description
Query Prefix	(Optional) Always append the query syntax to all queries by this user. For example, adding the query prefix **email != 'ceo@company.com'** prevents those email results from showing up in the sessions.
SA Core Query Timeout	**Note:** This field applies to NetWitness Suite 10.5 and later service versions and does not appear for 10.4 and earlier service versions. NetWitness Suite 10.4 and earlier services use Query Level instead of SA Core Query Timeout. Specifies the maximum number of minutes a user can run a query on the service. If this value is set to zero (0), the query timeout is not enforced for the user on the service. When replicating a user from a NetWitness Suite 10.5 or later service to a NetWitness Suite 10.4 service, Query Timeout migrates to Query Level based on the closest level. For example, if a user has a Query Timeout of 15 minutes, the user gets a Query Level of 3 after the migration. If a user has a Query Timeout of 35 minutes, the user gets a Query Level of 2 after the migration. If a user has a Query Timeout of 45 minutes, the user gets a Query Level of 2 after the migration.
Session Threshold	(Optional) Controls the behavior of the application when scanning meta values to determine session counts. Any meta value with a session count that is above the set threshold stops its determination of the true session count when the threshold is reached. If a threshold is set for a session, the Navigation view shows that the threshold was reached and the percentage of query time used to reach the threshold.

Role Membership

The Role Membership section shows the roles that a user is a member of for the selected service.

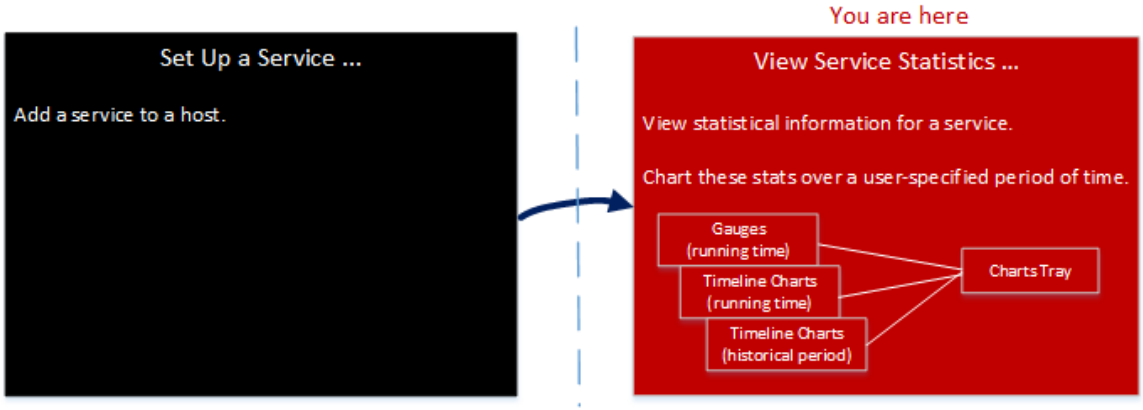
Services Stats View

This topic describes the features available in NetWitness Suite Services Stats view.

The Services Stats view provides a way to monitor the status and operations of a service. This view displays key statistics, service system information, and host system information for a service. In addition, more than 80 statistics are available for viewing as gauges and in timeline charts. In historical timeline charts, only statistics for session size, sessions, and packets are viewable.

Workflow

This workflow shows the tasks you perform from the Stats view.

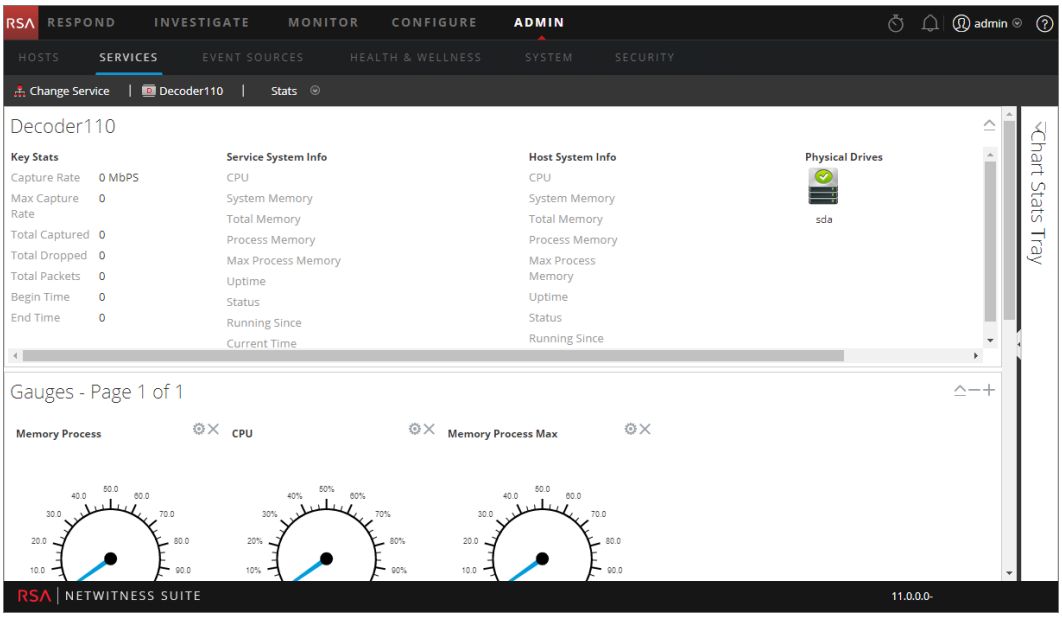


In the Stats view, you can customize the monitored statistics for individual services.

The following example shows you how to use the Stats view for a Decoder. The Stats view for all the services provide you with the same information for each service.

To access the Service Stats view:

1. In **NetWitness Suite** , go to **ADMIN > Services**.
   The Services view is displayed.
2. Select a service and select **> View > Stats**.



Features

Although different statistics are available for different types of services, certain elements are common to the Services Stats view for any Core service:

- Summary Stats section
- Gauges section
- Timelines section
- Historical Timelines section
- Chart Stats Tray

Summary Stats Section

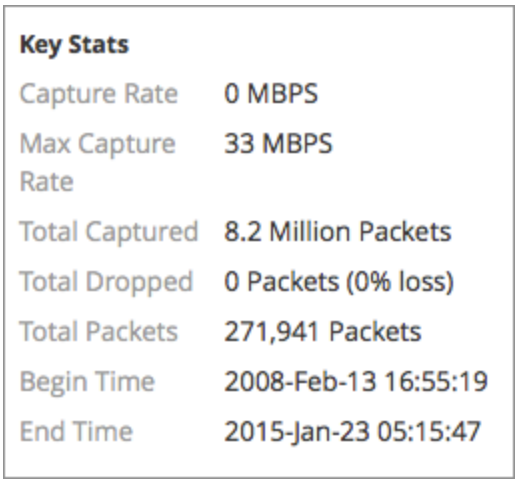
The Summary Stats section is at the top of the default view, and has no editable fields.

There are five panels in the Summary Stats section. The **Key Stats** panel displays different statistics for different types of services. The remaining panels in the Summary Stats section are the same for all types of services.

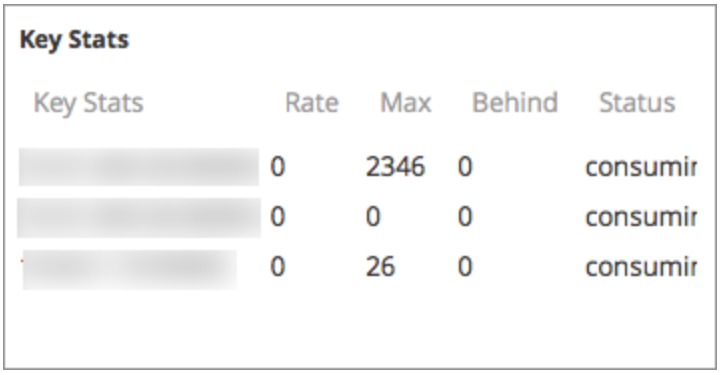
Key Stats

The Key Stats panel displays different statistics for different types of services.

- For a Decoder or Log Decoder, key statistics include capture statistics, such as capture rate, total packets or logs captured, total packets or logs dropped, the data capture begin time and end time.

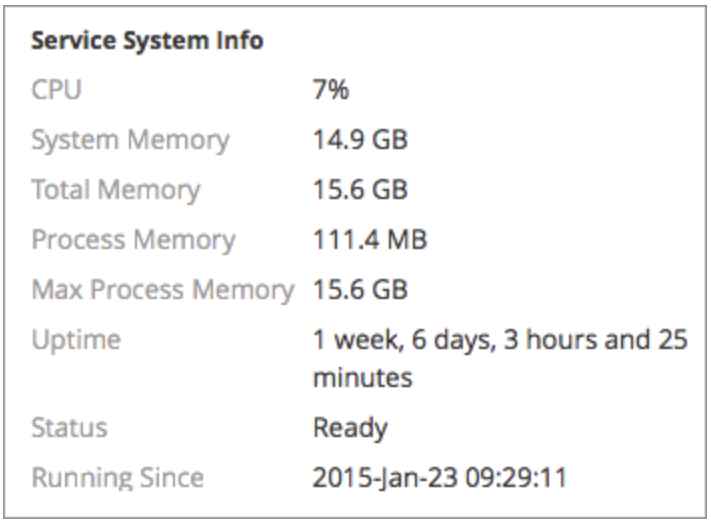


- A Broker or Concentrator aggregates data from multiple services. Therefore, the key statistics for all aggregate services are presented in a grid. The columns in the grid provide the service name, the capture rate, the maximum capture rate, the number of session behind (that need to be aggregated), and the service status.



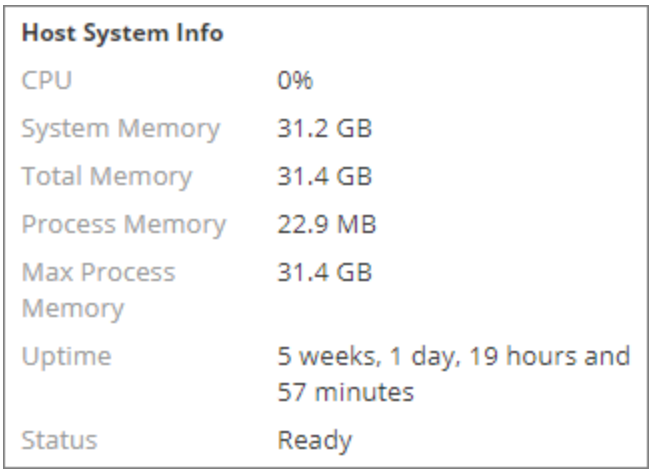
Service System Info

The Service System Info panel includes the percentage of CPU used by the service, the memory usage statistics (system, total, process, and maximum process), service uptime, status, running since time, and the current time.



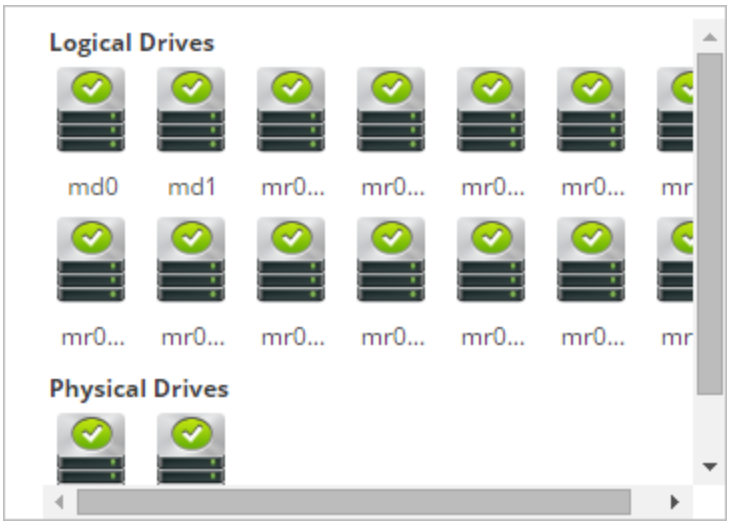
Service System Info	
CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	111.4 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 25 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

Host System Info includes percentage of CPU used by the host, the memory usage statistics (system, total, process, and maximum), host uptime, status, running since time, and the current time.



Host System Info	
CPU	0%
System Memory	31.2 GB
Total Memory	31.4 GB
Process Memory	22.9 MB
Max Process Memory	31.4 GB
Uptime	5 weeks, 1 day, 19 hours and 57 minutes
Status	Ready

Logical Drives and **Physical Drives** are shown with an icon for the drive name and state. Drive types used in the names and the drive status options are listed below.



Drive Types and Status

Drive Type	Description	Comment	Status Options
sd	SCSI block device	Directly connected SAS, SATA MegaRAID volumes	OK (green) FAIL (red)
ld	MegaRAID Logical Volume	Defined in BIOS or with MegaCLI tool	OK (green) DEGRADED (yellow) BUILDING (yellow) FAIL (red)
pd	MegaRAID Physical Disks	Not directly exposed to Linux	OK (green) FAIL (red)
md	Linux software RAID Volume		OK (green) DEGRADED (yellow) BUILDING (yellow) FAIL (red)

Gauges

The Gauges section in the Stats View presents statistics in the form of analog gauges. See Features for details on configuring gauges.

Timelines

Timeline charts display the selected statistics in a running timeline with focus on the current time. This is the same for all types of services, and only the display name of the timeline is editable. See Timeline Charts for details on configuring timelines.

Historical Timelines

Historical timeline charts display statistics for session size, sessions, and packets in a historical timeline. This is the same for all types of services, and has an editable display name, begin date, and end date. See Timeline Charts for details on configuring timelines.

Note: Historical Timeline charts is being deprecated for Log Collector, Virtual Log Collector (VLC) and Windows Legacy Collector services.

Chart Stats Tray

The Chart Stats Tray lists all available statistics for the selected service type. Different services have different statistics to monitor. See Components for a detailed description.

Topics

- Components
- Features
- Timeline Charts

Chart Stats Tray

This topic describes the Chart Stats Tray in the Services Stats view.

In the Services Stats view, the Chart Stats Tray provides a way to customize the monitored statistics for individual services. The Chart Stats Tray lists all available statistics for the service. The number of statistics varies according to the type of service being monitored. Any statistic in the Chart Stats Tray can be displayed in a gauge or a timeline chart. Only statistics for session size, sessions, and packets are viewable in historical timeline charts.

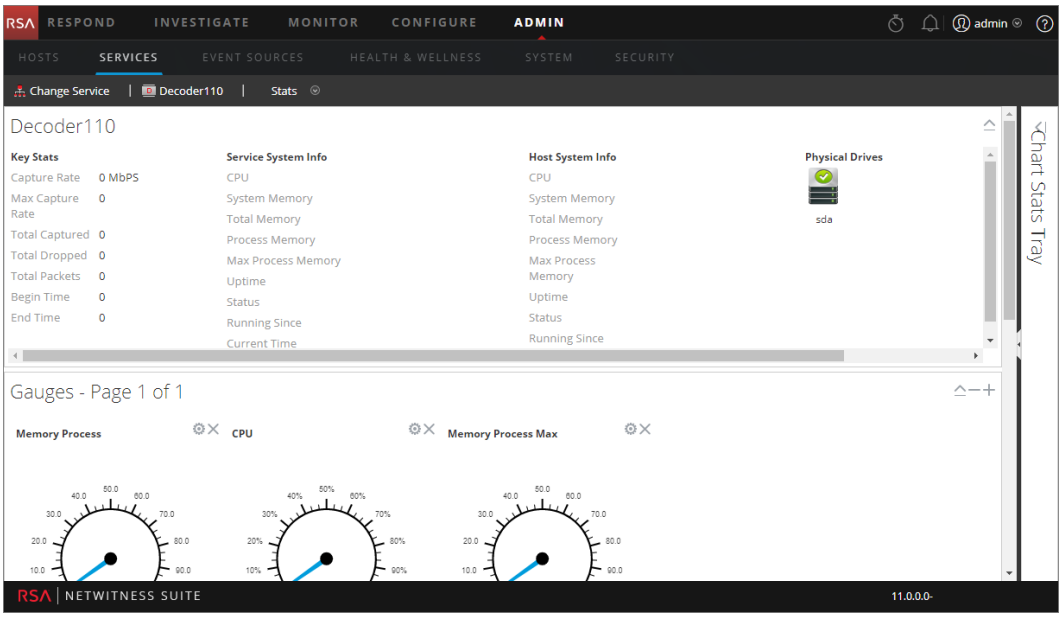
To access the Services Stats view:

1. In the **NetWitness Suite**menu, select **ADMIN > Services**.
   The Administration Services view is displayed.
2. Select a service and select **> View > Stats.**

The Chart Stats Tray is on the right side.

3. If the tray is collapsed, click <| to view the list of available statistics.

The following example shows the Services Stats view for a Decoder. The Chart Stats Tray is collapsed.



Components

The Chart Stats Tray has different statistics for different types of services. In the example above, 111 statistics are available for the Decoder. The following table describes features of the Chart Stat Tray.

Feature	Description
<|	Click to expand the panel horizontally.
|>	Click to collapse the panel horizontally.
Search	Type a search term in the field and press **RETURN**. Statistics that match are displayed with the matching word highlighted.
«	Click to go to the first page.
‹	Click to go to the previous page.

Feature	Description
ge 5 of 2	Type a page number in the Page field.
›	Click to go to the next page.
»	Click to go to the last page.
↻	Click to refresh the view.
s 1 - 12 of	Displays the range of statistics being displayed. The total number statistics varies by service type.

Gauges

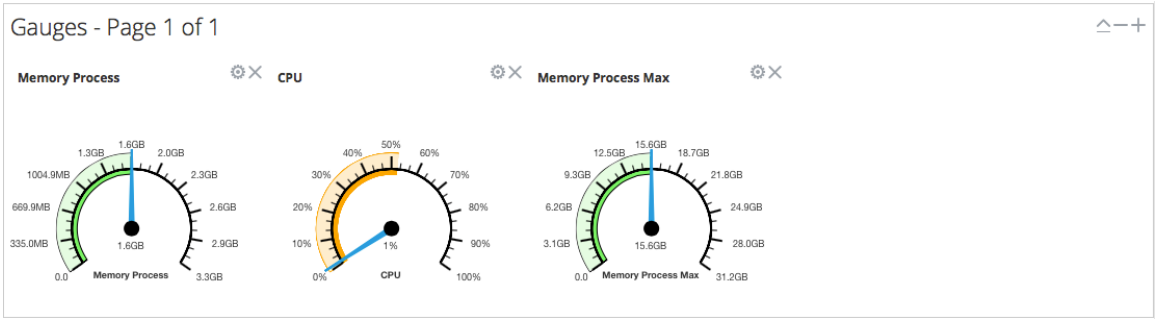
This topic introduces the features of the Gauges section in the Services Stats view.

The Gauges section of the Services Stats view presents statistics in the form of an analog gauge. You can drag any statistic available in the Chart Stats Tray to the Gauges section. The properties of each individual gauge are editable; all gauges have an editable title and some have additional editable properties.

To access the Services Stats view:

1. In the **NetWitness Suite**menu, select **ADMIN > Services**
   The Administration Services view is displayed.
2. Select a service and select **> View > Stats**.
   The Services Stats view includes the Gauges section.

The following figure shows the default gauges in the Services Stats view for a Log Decoder.



Features

The default gauges show these statistics:

- Process memory use
- CPU use
- Maximum process memory used

The controls in the Gauges title bar and in each gauge are the standard dashlet controls.

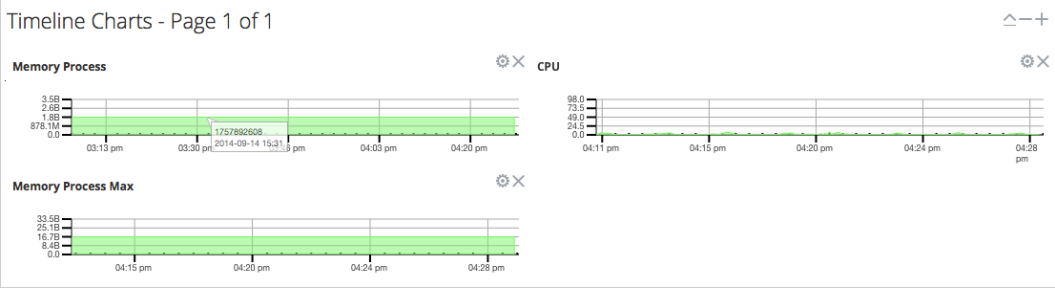
- In the Gauges title bar, you can collapse and expand the section and page forward or back.
- In each gauge, you can edit properties ( ) and delete ( ) the gauge.

Timeline Charts

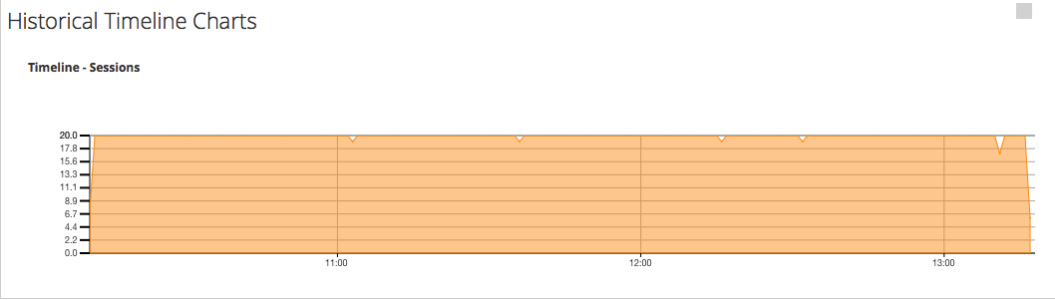
This topic describes the features of the timeline charts in the Services Stats view.

Timeline charts display statistics in a running timeline. The Services Stats view includes two types of timelines: current time and historical. You can drag any statistic available in the Chart Stats Tray to the Timeline Charts section. Only statistics for session size, sessions, and packets are viewable in historical timeline charts. The properties of an individual timeline chart are editable; all timeline charts have an editable title and some have additional editable properties.

The following figure is an example of a current timeline showing the value and timestamp of a data point.



The following figure is an example of a historical timeline chart.



The default current timeline charts show these statistics:

- Memory Process
- CPU

- Memory Process Max

The historical time charts show these statistics:

- Sessions
- Packets
- Session Size

The controls in the Timeline Charts title bar and in each timeline are the standard dashlet controls.

- In the Timeline Charts title bar, you can collapse and expand the section and page forward or back.
- In each timeline, you can edit Properties ( ) and delete ( ) the timeline.
- Hovering over a data point in the chart, displays the value and timestamp for the selected point.

System View

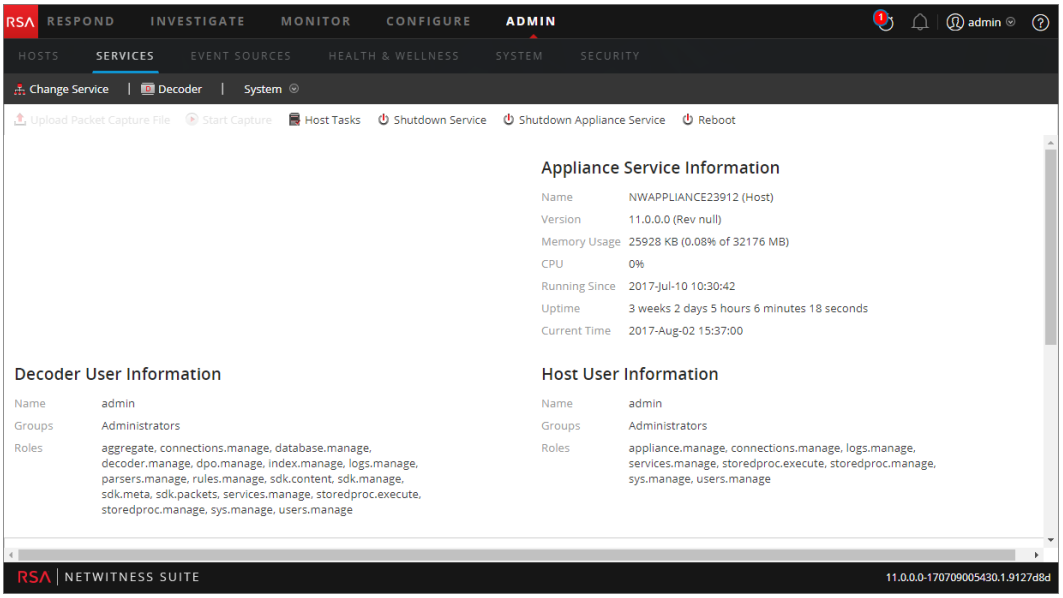
This topic introduces features in the System view using the Decoder and Log Decoder as an example. See the Configuration Guides individual services (for example for the *RSA NetWitness® SuiteBroker and Concentrator Configuration Guide*) for details on their **ADMIN > Services > System** Views.

A Log Decoder is a special type of Decoder, and is configured and managed in a similar way to a Decoder. Therefore, most of the information in this section refers to both types of Decoders. Differences for Log Decoders are noted.

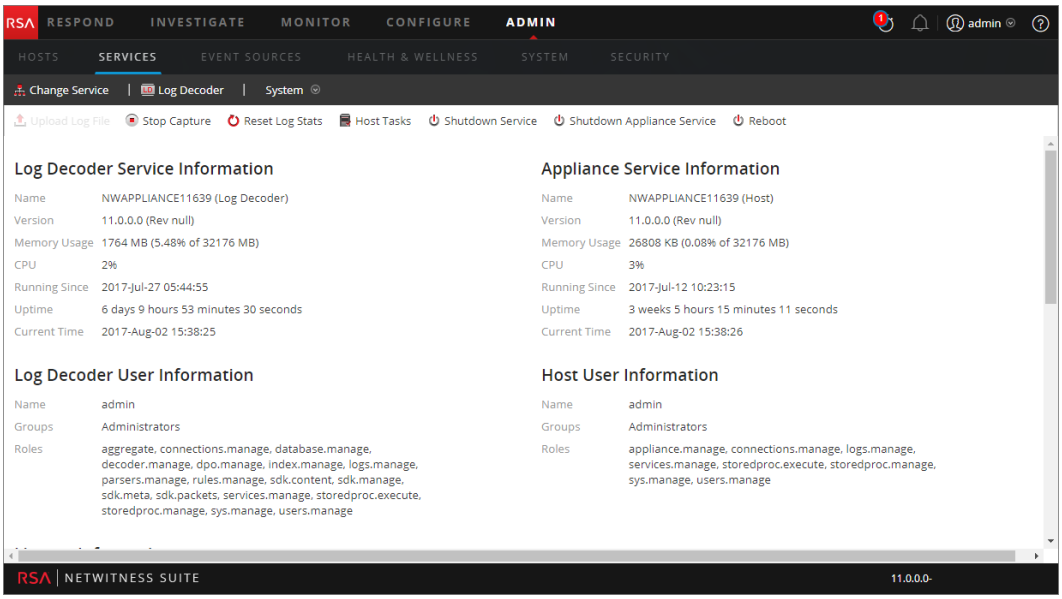
To access the Services System view for a Decoder:

1. In **NetWitness Suite** , go to **ADMIN > Services**.
   The Services view is displayed.
2. Select a service and select **> View> System**.

The following figure shows an example of the Services System view for a Decoder.



The following figure shows the Services System view for a Log Decoder.



Features

Services Info Toolbar

The following toolbars show the options specific to Log Decoders and Decoders.

In addition to the common options in the Services System view toolbar, you can start and stop capture of packets or logs. The upload file options are different for the standard Decoder (packet capture file) and the Log Decoder (log file).

Action	Description
Upload Packet Capture File	Displays a dialog that provides a way to select a packet capture (.pcap) file for upload to the selected Decoder. For more information, see the **Upload Packet Capture File** topic in the *Decoder and Log Decoder Configuration Guide*. **Note:** This option does not apply to Log Decoders.
Upload Log File	Displays a dialog that provides a way to select a log (.log) file for upload to the selected Log Decoder. For more information, see the **Upload Log File to a Log Decoder** topic in the *Decoder and Log Decoder Configuration Guide*.

Action	Description
Start/Stop Capture	Starts packet capture on the selected Decoder. When packet capture is in progress, the option in the toolbar changes to Stop Capture, and the option to upload a file is unavailable.

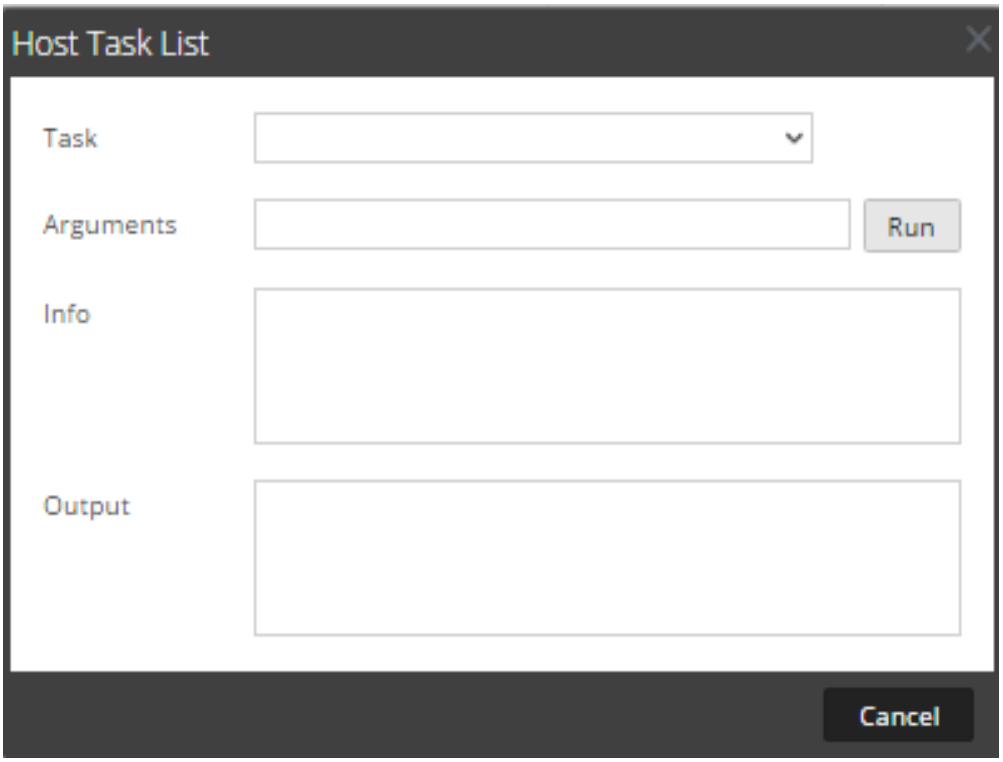
Host Task List Dialog

This topic introduces the Services System view > Host Task List dialog.

In the RSA NetWitness Suite Services System view, you can use the Host Tasks option to manage tasks that relate to a host and its communications with the network. Several service and host configuration options are available for Core services.

To access the Host Tasks dialog:

1. In **NetWitness Suite** , select **ADMIN >Services**.
2. Select a service and select > **View> System**.
   The System View for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
   The Host Task List dialog is displayed. The **Task** list offers a list of supported messages for the associated host.



Features

The table below describes the dialog features.

Field	Description
Task	An entry field in which you type or select a message for a Core host. When you click in this field a drop-down list of available host tasks is displayed.
Arguments	An entry field in which you enter the arguments, if any, for the message.
Run	Executes the task and arguments in the entry fields.
Info	Information about the message purpose and syntax.
Output	The output or result of an executed task.
Cancel	Closes the Host Task list dialog.

Host Task Selection List

These tasks are displayed as a drop-down list in the Task field. The available options are regulated by the security role required to execute the option.

Task	Description
Add Filesystem Monitor	Starts monitoring the storage services attached to the specified filesystem (see Add and Delete a Filesystem Monitor.
Delete Filesystem Monitor	Stops monitoring the storage services attached to the specified filesystem.
Reboot Host	Shuts down and restarts the host (see Reboot a Host).
Set Host Built-in Clock	Sets the host local clock (see Set Host Built-In Clock).
Set Host Hostname	This method of changing the hostname is deprecated in NetWitness Suite 10.6; replaced by the procedure described in Hosts and Services Procedures

Task	Description
Set Network Configuration	Sets network address parameters (see Set Network Configuration).
Set Network Time Source	Sets the clock source for this host (see Set Network Time Source).
Set Syslog Forwarding	Enables or disables syslog forwarding from a remote server to the selected service (see Set Syslog Forwarding).
Show Network Port Status	Shows the network interface information for a host (see Show Network Port Status).
Show Serial Number	Gets the host serial number (see Show Serial Number).
Shut Down Host	Shuts down the physical host and the host remains off (see Shut Down Host).
Start Service	Starts a service on this host (see Start, Stop or Restart a Service).
Stop Service	Stops a service on this host.
setSNMP	Enables or disables the SNMP service on a host (see Set SNMP).

Service Configuration Settings

This topic introduces the available service configuration settings for RSA NetWitness Suite Core services.

NetWitness Suite Core services include Brokers, Concentrators, Decoders, Log Decoders, Archivers, and the Appliance service. The service configuration parameters listed in these tables constitute all viewable and configurable parameters. Some parameters are configurable in various parts of the NetWitness Suite user interface and others are viewable or configurable only on the Services Explore view.

Appliance Service Configuration Parameters

This topic lists and describes the available the configuration parameters for the NetWitness Suite Core Appliance service.

The NetWitness Suite Core Appliance service provides hardware monitoring on legacy NetWitness hardware.

This table describes the Appliance Configuration parameters.

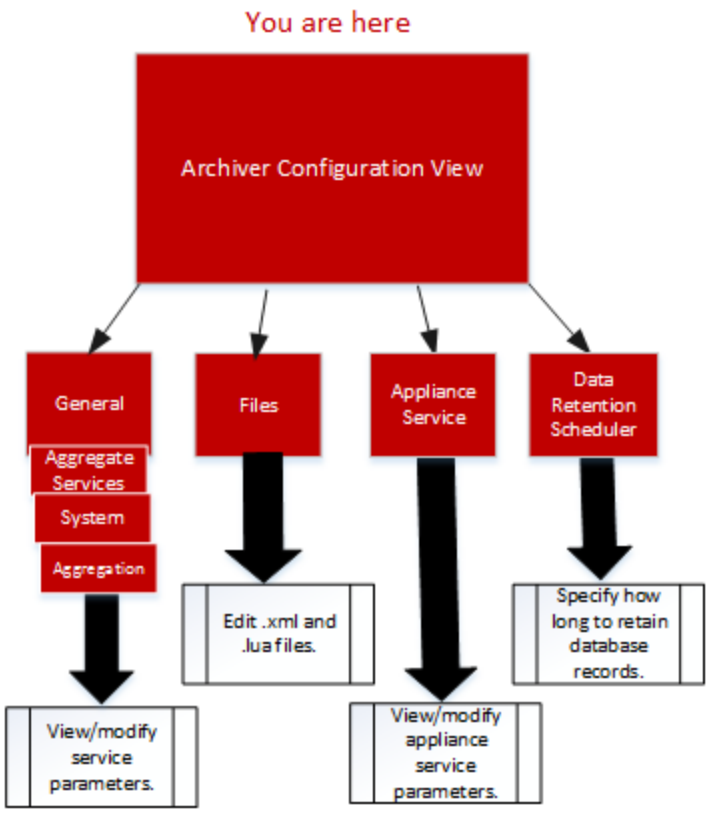
Appliance Parameter Field	Description
Logs	/logs/config, see Core Service Logging Configuration Parameters
REST	/rest/config, see REST Interface Configuration Parameters
Services	/services/<service name>/config, see Core Service-to-Service Configuration Parameters
System	/sys/config, see Core Service System Configuration Parameters

Archiver Service Configuration View

This topic lists and describes the available configuration settings for NetWitness Suite Archivers.

Workflow

The following workflow show the configuration tasks for the Archiver service.



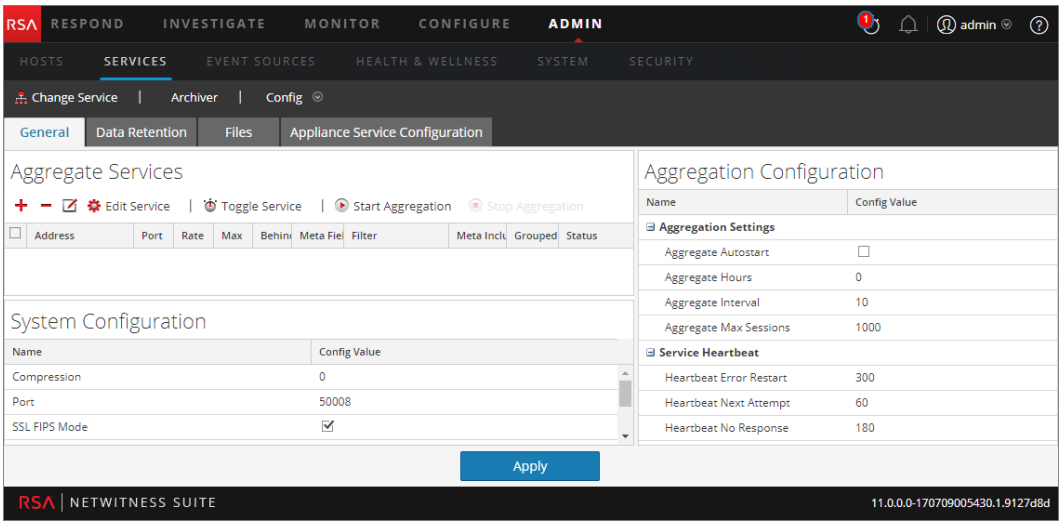
Role	I want to ...
Administrator	Configure Meta Filters for Aggregation. Refer to "(Optional) Configure Meta Filters for Aggregation" in the *RSA NetWitness Suite Archiver Configuration Guide* for instructions.
Administrator	Configure Group Aggregation. Refer to "Configure Group Aggregation" in the *RSA NetWitness Suite Deployment Guide* for instructions.

Quick Look

To access the Services Config view:

1. In **NetWitness Suite**, select **ADMIN > Services**.
   The Admin Services view is displayed.
2. Select an Archiver service and select **>View > Config**.
   Services Config view for the Archiver service is displayed.

This is an example of the Services Config view for an Archiver.



Broker Service Configuration Parameters

This topic lists and describes the configuration parameters for NetWitness Suite Brokers.

This table lists and describes the Broker configuration parameters.

Broker Parameter Field	Description
Broker	/broker/config refer to Aggregation Configuration Parameters
aggregate.interval.behind	Minimum number of milliseconds before another round of aggregation is requested when the broker is behind. Change takes effect immediately.
Database	/database/config refer to the **Database Configuration Nodes** topic in the *NetWitness SuiteCore Services Database Tuning Guide*
Index	/index/config
index.dir	The directory where the broker device mapping files are stored. Change takes effect on service restart.
language.filename	The index language specification (XML) that is loaded on startup. Change requires service restart.
Logs	/logs/config refer to Core Service Logging Configuration Parameters

Broker Parameter Field	Description
REST	/rest/config refer to REST Interface Configuration Parameters
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *NetWitness Suite Core Services Database Tuning Guide* and NetWitness Suite Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration Parameters
System	/sys/config refer to Core Service System Configuration Parameters

Aggregation Configuration Parameters

This topic lists and describes the available configuration parameters that are common to services that perform aggregation, such as NetWitness Suite Concentrators and Archivers.

This table lists and describes the parameters that control aggregation on an aggregating service.

Configuration Path	/concentrator/config or /archiver/config
aggregate.autostart	Automatically restarts aggregation after a service restart, if enabled. Change takes effect immediately.
aggregate.buffer.size	Displays the size of the buffer (default unit is KB) used per round of aggregation. Larger buffers may improve aggregation performance but could impact query performance. Change takes effect after aggregation restart.
aggregate.crc	If enabled, all aggregation streams will be CRC validated. Change takes effect immediately.
aggregate.hours	Displays the maximum number of hours behind a service will be allowed to start aggregation. Change takes effect immediately.
aggregate.interval	Lists the minimum number of milliseconds before another round of aggregation is requested. Change takes effect immediately.

Configuration Path	/concentrator/config or /archiver/config
aggregate.meta.page.factor	Lists the allocated number meta pages per session used for aggregation. Change takes effect on service restart.
aggregate.meta.perpage	Lists the allocated number of meta stored on one page of data. Change takes effect on service restart.
aggregate.precache	Determines if the concentrator will precache the next round of aggregation for upstream services. Can improve aggregation performance but could impact query performance. Change takes effect immediately.
aggregate.sessions.max	Lists the number of sessions to aggregate on each round. Change takes effect after aggregation restart.
aggregate.sessions.perpage	Lists the number of sessions stored on one page of data. Change takes effect on service restart.
aggregate.time.window	Displays the maximum +/- time window, in seconds, that all services must be inside before another round of aggregation is requested. Zero turns off time window. Change takes effect immediately.
consume.mode	Determines if the concentrator can only aggregate locally or over a network, based on licensing restrictions. Change takes effect on service restart.
export.enabled	Allows export of session data, if enabled. Change takes effect on service restart.
export.expire.minutes	Lists the number of minutes before export cache files are expired and flushed. Change takes effect immediately.
export.format	Determines the file format used during data export. Change takes effect on service restart.

Configuration Path	/concentrator/config or /archiver/config
export.local.path	Displays the local location to cache exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
export.meta.fields	Determines which meta fields are exported. Comma list of fields. Star means all fields. Star plus field list means all fields BUT listed fields. Just field list says just include those fields. Change takes effect immediately.
export.remote.path	Displays the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.rollup	Determines the rollup interval for export files. Change takes effect on service restart.
export.session.max	Displays the maximum sessions per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.size.max	Displays the maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.usage.max	Displays the maximum percentage of cache space used before stopping aggregation. Zero is no limit. Change takes effect immediately.
heartbeat.error	Lists the number of seconds to wait after a service error before attempting a service reconnect. Change takes effect immediately.
heartbeat.interval	Lists the number of milliseconds between heartbeat service checks. Change takes effect immediately.

Configuration Path	/concentrator/config or /archiver/config
heartbeat.next.attempt	Lists the number of seconds to wait before attempting a service reconnect. Change takes effect immediately.
heartbeat.no.response	Lists the number of seconds to wait before taking unresponsive service offline. Change takes effect immediately.

Concentrator Service Configuration Parameters

This topic lists and describes the available configuration parameters for NetWitness Suite Concentrators.

This table lists and describes the Concentrator configuration parameters .

Concentrator Parameter Field	Description
Concentrator	/concentrator/config refer to Aggregation Configuration Parameters
Database	/database/config refer to the **Database Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*
Index	/index/config refer to the **Index Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration Parameters
REST	/rest/config refer to REST Interface Configuration Parameters
SDK	sdk/config refer to the **SDK Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*and NetWitness Suite Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration Parameters
System	/sys/config refer to Core Service System Configuration Parameters

Core Service Logging Configuration Parameters

This topic lists and describes the logging configuration parameters for all NetWitness Suite Core services.

Logging configuration is the same on all NetWitness Suite Core services.

The following table describes the logging configuration parameters:

Logs Configuration Folder	/logs/config
log.dir	Displays the directory where the log database is stored. Optional assigned max size (=#) is in MBs. Change takes effect on service restart.
log.levels	Controls what types of log messages are stored (comma separated). Module specific settings are defined like this: <Module>=[debug|info|audit|warning|failure|all|none]. Change takes effect immediately.
log.snmp.agent	Sets a remote SNMP Trap Receiving agent.
snmp.trap.version	Sets the SNMP version to be used for gets and traps (2c or 3).
snmpv3.engine.boots	Displays the SNMPv3 engine boots count. This field auto-increments on startup and should not normally need to be set by the user.
snmpv3.engine.id	Sets the SNMPv3 engine ID, which is 10-64 hexadecimal digit number optionally preceded by 0x. You can add suffix values at the end of the engine ID for each of the SA Core services running on the same host. For example, if the generated Engine ID for the SA Core host is 0x1234512345, you can set the Engine ID for the Decoder service as 0x123451234501 and set 0x123451234504 for the Appliance service.

Logs Configuration Folder	/logs/config
snmpv3.trap.auth.local.key	Sets the SNMPv3 Trap Authentication Local Key, which is a 16 or 20 hexadecimal digit number (depending on which authentication protocol is used) preceded by 0x. For MD5, the key is 16 hexadecimal digits, while SHA uses 20 hexadecimal digits. You can use any desired algorithm to generate the local keys. It is recommended that a generation method involving randomness be used as opposed to selecting key values manually.
snmpv3.trap.auth.protocol	Displays the SNMPv3 Trap Authentication Protocol (none, MD5 or SHA).
snmpv3.trap.priv.local.key	Sets the SNMPv3 Trap Privacy Local Key, which is a 16 hexadecimal digit number preceded by 0x.
snmpv3.trap.priv.protocol	Displays the SNMPv3 Trap Privacy Protocol (none or AES).
snmpv3.trap.security.level	Displays the SNMPv3 Trap Security Level, which indicates whether authentication and privacy are used or not. Possible values are noAuthNoPriv, authNoPriv or authPriv.
snmpv3.trap.security.name	Sets the SNMPv3 Trap Security Name used during SNMPv3 trap authentication.
syslog.size.max	Displays the maximum size of a log sent to syslog (some syslog daemons have issues with very large messages). Zero means no limit. Change takes effect immediately.

Core Service-to-Service Configuration Parameters

This topic lists and describes the configuration parameters that control how a Core service connects to another Core service. For example, when a Concentrator connects to a decoder, the parameters of that connection are controlled by these settings.

Whenever a Core service establishes a connection to another Core service, the service that acts as the **client** creates a new sub-folder in the /services folder of the configuration tree. The name of the sub-folder corresponds to the name of the service and has the form `host:port`. For example, the service connection folder for a Concentrator connection to a Decoder could be `/services/reston-va-decoder:50004`. Inside each service connection folder, there is a `config` sub-folder that holds configurable parameters.

The following table describes the Service Configuration parameters:

Services	/services/host:port/config
allow.nonssl.to.ssl	Allows a non-SSL connection to connect to a SSL service, when set to true. Otherwise, if false, non-secure to secure connections will be denied. Change takes effect immediately.
compression	Displays a config node that determines if data is compressed before sending. A positive value determines the number of bytes that need to be sent before it will be compressed. Zero means no compression.
crc.checksum	Displays a config node that determines if data streams are validated with a CRC checksum. A positive value determines the number of bytes that need to be sent before it will be CRC validated. Zero means no CRC validation.
ssl	Displays a config node that enables or disables SSL encryption on the connection.

Core Service System Configuration Parameters

This topic lists and describes the configuration parameters that are common to all NetWitness Suite Core services.

The following table lists and describes the System configuration parameters:

System Configuration Folder	/sys/config
compression	Displays the minimum amount of bytes before a message is compressed, when set to a positive value. Zero means no compression for any message. Change takes effect on subsequent connections.
crc.checksum	Displays the minimum bytes before a message is sent over the network with a CRC checksum (to be validated by the client), when set to a positive value. Zero means no CRC checksum validation with any message. Change takes effect on subsequent connections.
drives	Displays drives to monitor for usage stats. Change takes effect on service restart.
port	Displays the port this service will listen on. Change takes effect on service restart.
scheduler	Displays the folder for scheduled tasks.
service.name.override	Displays an optional service name used by upstream services for aggregation in lieu of hostname.
ssl	Encrypts all traffic using SSL, if enabled. Change takes effect on service restart.
stat.compression	Compresses stats as they are written to the database, if enabled. Change takes effect on service restart.
stat.dir	Displays the directory where the historical stats database is stored (separate multiple dirs with semicolon). Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.

System Configuration Folder	/sys/config
stat.exclude	Lists stat pathnames to be excluded from the stat database. The following wildcards are permitted: ? match any single character, * match zero or more characters to delimiter /, ** match zero or more characters including delimiter. Change takes effect immediately.
stat.interval	Determines how often (in milliseconds) statistic nodes are updated in the system. Change takes effect immediately.
threads	Lists the number of threads in the thread pool to handle incoming requests. Change takes effect immediately.

Decoder Service Configuration Parameters

This topic lists and describes the available configuration parameters for NetWitness Suite Decoders.

This table lists and describes the Decoder configuration parameters.

Decoder Parameter Field	Description
Decoder	/decoder/config refer to Decoder and Log Decoder Configuration Parameters
Database	/database/config refer to the **Database Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*
Index	/index/config refer to the **Index Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration Parameters
REST	/rest/config refer to REST Interface Configuration Parameters

Decoder Parameter Field	Description
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*and NetWitness Suite Core Service system.roles Modes
System	/sys/config refer to Core Service System Configuration Parameters

Decoder and Log Decoder Configuration Parameters

This topic lists and describes the configuration parameters that are identical on both packet decoder and log decoder services.

Decoder Configuration Settings

This table lists and describes the Decoder and Log Decoder shared configuration parameters.

Decoder Configuration Path	/decoder/config
aggregate.buffer.size	Displays the size of the buffer (default unit is KB) used per round of aggregation. Larger buffers may improve aggregation performance but could impact capture performance. Change takes effect after capture restart.
aggregate.precache	Determines if the decoder will precache the next round of aggregation for upstream services. Can improve aggregation performance but could impact capture performance. Change takes effect immediately.
assembler.pool.ratio	Displays the percentage of pool pages that assembler manages and uses for the assembly process. Change takes effect on service restart.
assembler.session.flush	Flushes sessions when they are complete (1) or flushes sessions when they are parsed (2). Change takes effect on service restart.

Decoder Configuration Path	/decoder/config
assembler.session.pool	Lists the number of entries in the session pool. Change takes effect on service restart.
assembler.size.max	Lists the maximum size that a session will obtain. A setting of 0 removes the session size limit. Change takes effect immediately.
assembler.size.min	Lists the minimum size that a session must be before persisting. Change takes effect immediately.
assembler.timeout.packet	Lists the number of seconds before packets are timed out. Change takes effect immediately.
assembler.timeout.session	Lists the number of seconds before sessions are timed out. Change takes effect immediately.
assembler.voting.weights	Displays the weights used to determine which session stream is marked client and server. Change takes effect immediately.
capture.autostart	Determines if capture begins automatically when the service starts. Change takes effect on service restart.
capture.buffer.size	Displays capture memory buffer allocation size (default unit is MB). Change takes effect on service restart.

Decoder Configuration Path	/decoder/config
capture.device.params	Displays capture service specific parameters. Change takes effect on service restart. The parameters understood by this field are specific to the currently selected capture device. If any of the parameters are not recognized by the current capture device, they are ignored. On Log Decoders, there is only the Log Events capture device. It accepts some optional parameters. • **use-envision-time**: If this is set to 1, the time meta for each event will be imported from the Log Collector stream. If this is 0 or not set, the imported event time will be stored in the event.time meta. • **port**: This parameter can be set to a numeric value to override the default syslog port listener, 514.
capture.selected	Displays current capture service and interface. Change takes effect immediately.
export.expire.minutes	Lists the number of minutes before export cache files are expired and flushed. Change takes effect immediately.
export.packet.enabled	Allows export of packet data, if enabled. Change takes effect on service restart.
export.packet.local.path	Displays the local location to cache packet exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
export.packet.max	Displays the maximum packets per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.

Decoder Configuration Path	/decoder/config
export.packet.remote.path	Lists the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.packet.size.max	Displays the packet maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.rollup	Determines the rollup interval for export files. Change takes effect on service restart.
export.session.enabled	Allows export of session data, if enabled. Change takes effect on service restart.
export.session.format	Determines the file format used during session export. Change takes effect on service restart.
export.session.local.path	Displays the local location to cache session exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
export.session.max	Displays the maximum sessions per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.session.meta.fields	Determines which meta fields are exported. Comma list of fields. Star means all fields. Star plus field list means all fields BUT listed fields. Just field list says just include those fields. Change takes effect immediately.
export.session.remote.path	Displays the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.session.size.max	Lists the session maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.

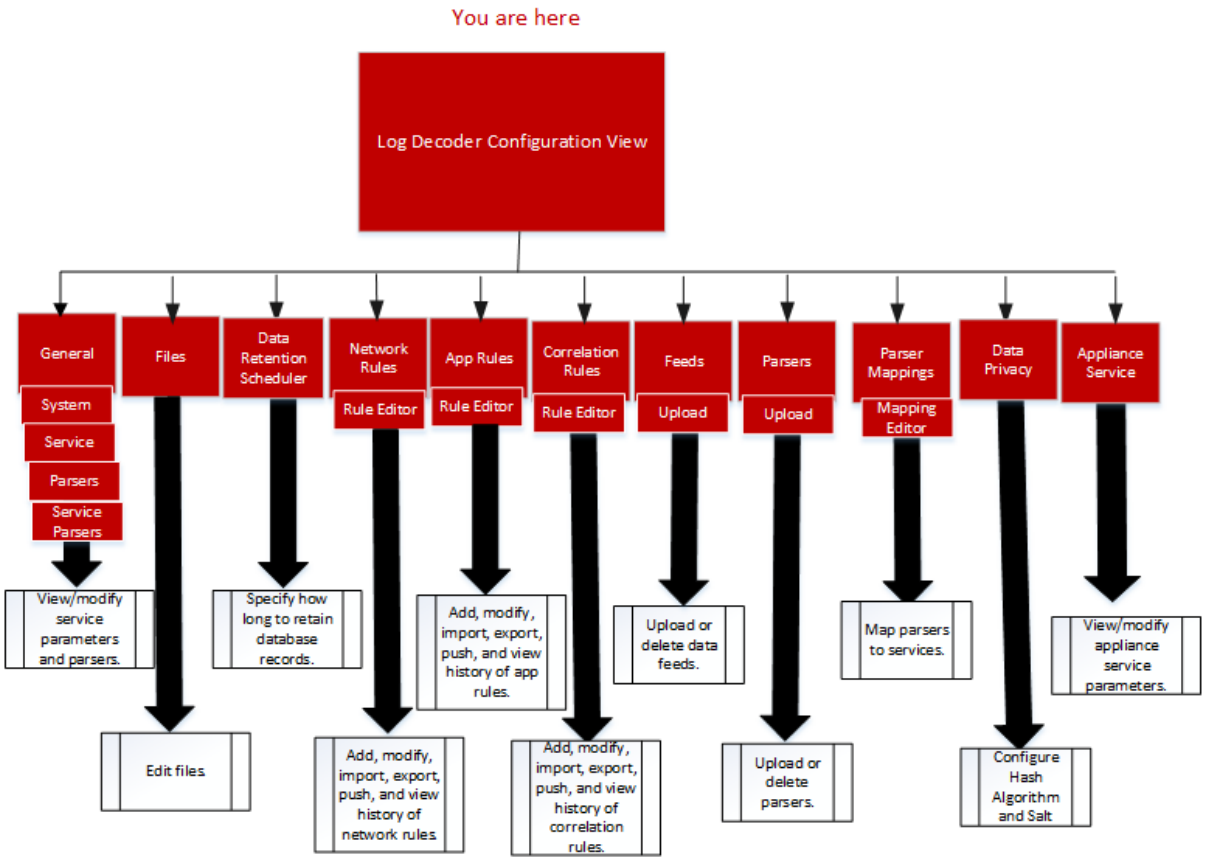
Decoder Configuration Path	/decoder/config
export.usage.max	Lists the session maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
parse.threads	Lists the number of parse threads to use for session parsing. Zero means let server decide. Change takes effect on service restart.
pool.packet.page.size	Displays the size of a packet page (default is KB). Change takes effect on service restart.
pool.packet.pages	Lists the number of packet pages decoder will allocate and use. Change takes effect on service restart.
pool.session.page.size	Displays the size of a session page (default is KB). Change takes effect on service restart.
pool.session.pages	Lists the number of session pages decoder will allocate and use. Change takes effect on service restart.

Log Decoder Service Configuration View

This topic lists and describes the configuration settings for NetWitness Suite Concentrators.

Workflow

The following workflow show the configuration tasks for the Log Decoder service.



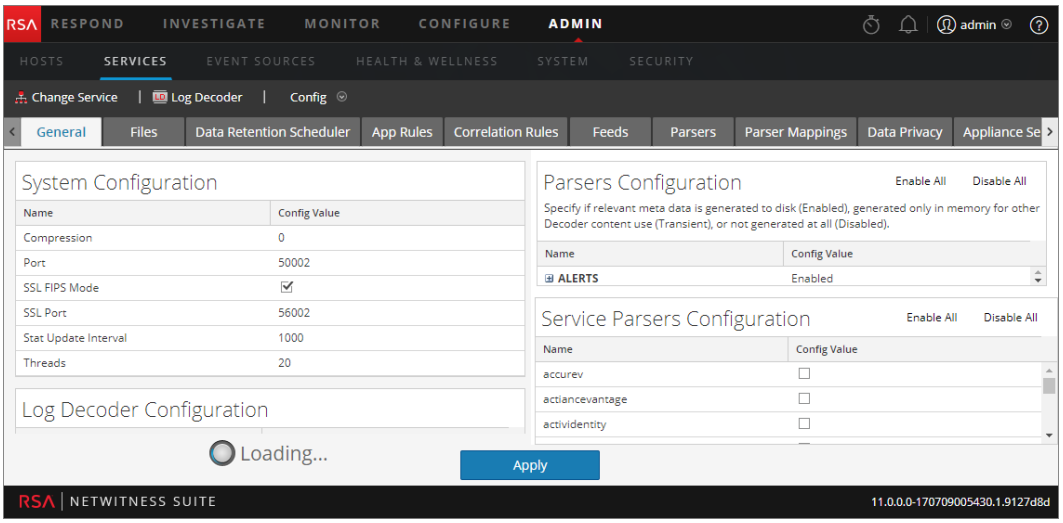
Role	I want to ...
Administrator	Configure Group Aggregation.

Quick Look

To access the Services Config view:

1. In **NetWitness Suite**, select **ADMIN > Services**.
   The Admin Services view is displayed.
2. Select a Log Decoder service and select **>View > Config**.
   Services Config view for the Log Decoder service is displayed.

This is an example of the Services Config view for a Log Decoder.



Topics

Log Collector Configuration Parameters Interface

Log Decoder Service Configuration Parameters

This topic lists and describes the available configuration parameters for RSA NetWitness Suite Log Decoders.

Log Decoder Configuration Settings

This table lists and describes the Log Decoder configuration settings.

Log Decoder Setting Field	Description
Database	/database/config refer to the **Database Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*.
Decoder	/decoder/config refer to Decoder and Log Decoder Configuration Parameters
Index	/index/config refer to the **Index Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*.
Logs	/logs/config refer to Core Service Logging Configuration.
REST	/rest/config refer to REST Interface Configuration

Log Decoder Setting Field	Description
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *NetWitness Suite Core Database Tuning Guide*and Core Service system.role Modes.
System	/sys/config refer to Core Service System Configuration.

Log Tokenizer Configuration Settings

The log decoder has a set of configuration items that control how the automatic log tokenizer creates meta items from unparsed logs. The log tokenizer is implemented as a set of built-in parsers that each scan for a subset of recognizable tokens. The functionality of each of these native parsers is shown in the table below. These word items form a full-text index when they are fed to the indexing engine on the Concentrator and Archiver. By manipulating the parsers.disabled configuration entry, you can control which Log Tokenizers are enabled.

Parser Name	Description	Configuration Parameters
Log Tokens	Scans for runs of consecutive characters to produce 'word' meta items.	token.device.types, token.char.classes, token.max.length, token.min.length, token.unicode
IPSCAN	Scans for text that appears to be an IPv4 address to produce 'ip.addr' meta items.	token.device.types
IPV6SCAN	Scans for text that appears to be an IPv6 address to produce 'ipv6' meta items.	token.device.types

Parser Name	Description	Configuration Parameters
URLSCAN	Scans for text that appears to be a URI to produce 'alias.host', 'filename', 'username', and 'password' meta items.	token.device.types
DOMAINSCAN	Scans for text that appears to be a domain name to produce 'alias.host', 'tld', 'cctld', and 'sld' meta items.	token.device.types
EMAILSCAN	Scans for text that appears to be an email address to produce 'email' and 'username' meta items.	token.device.types
SYSLOGTIMESTAMPSCAN	Scans for text that appears to be syslog-format timestamps. Syslog is missing the year and time zone. When such text is located, it is normalized into UTC time to create 'event.time' meta items.	token.device.types
INTERNETTIMESTAMPSCAN	Scans for text that appears to be RFC 3339-format timestamps to create 'event.time' meta items.	token.device.types

These are the Log Tokenizer configuration parameters.

Log Decoder Parser Setting Field	Description
token.device.types	The set of device types that will be scanned for raw text tokens. By default, this is set to `unknown`, which means only logs that were not parsed will be scanned for raw text. You can add additional log types here to enrich parsed logs with text token information. If this field is empty, then log tokenization is disabled.
token.char.classes	This field controls the type of tokens that are generated. It can be any combination of the values `alpha`, `digit`, `space`, and `punct`. The default value is `alpha`. • **alpha**: Tokens may contain alphabetic characters • **digit**: Tokens may contain numbers • **space**: Tokens may contain spaces and tabs • **punct**: Tokens may contain punctuation marks
token.max.length	This field puts a limit on the length of the tokens. The default value is 5 characters. The maximum length setting allows the Log Decoder to limit the space needed to store the word metas. Using longer tokens requires more meta database space, but may provide slightly faster raw text searches. Using shorter tokens causes the text query resolver to have to perform more reads from the raw logs during searches, but it has the effect of using much less space in the metadb and index.
token.min.length	This is the minimum length of a searchable text token. The minimum token length will correspond to the minimum number of characters a user may type into the search box in order to locate results. The recommended value is the default, 3.

Log Decoder Parser Setting Field	Description
token.unicode	This boolean setting controls whether unicode classification rules are applied when classifying characters according to the token.char.classes setting. If this is set to true, each log is treated as a sequence of UTF-8 encoded code points and then classification is performed after the UTF-8 decoding is performed. If this is set to false, then then each log is treated as ASCII characters and only ASCII character classification is done. Unicode character classification requires more CPU resources on the Log Decoder. If you do not need non-English text indexing, you can disable this setting to reduce CPU utilization on the Log Decoder. The default is enabled.

REST Interface Configuration Parameters

This topic lists and describes the available configuration parameters for the REST interface built in to all NetWitness Suite Core Services.

Settings

The following table lists and describes the REST configuration parameters:

REST Configuration Path	/rest/config
cache.dir	Displays the host directory to use for temporarily creating and storing files. Change takes effect on service restart.
cache.size	Displays the total maximum size (default unit is MB) of all files in the cache directory before the oldest are deleted. Change takes effect on service restart.
enabled	Switches to enable or disable REST services, 1 is on, 0 is off. Change takes effect on service restart.

REST Configuration Path	/rest/config
port	Displays the port the REST service will listen on. Change takes effect on service restart.
ssl	Encrypts all REST traffic using SSL, if enabled. The default 'system' means use setting from /sys/config/ssl. Change takes effect on service restart.

NetWitness Suite Core Service system.roles Modes

All NetWitness Suite Core services offer role-based authorization modes. This topic describes the modes that are available, and how they are configured within every service.

The configuration node `/sdk/config/system.roles` sets querying and viewing permissions for meta and content on a per key basis. This parameter supports the data privacy management function and when enabled using one of the non-zero values helps a data privacy officer to control access to specific meta keys and content. This parameter is configurable in the NetWitness Suite user interface (see the **Data Privacy Tab** topic in the *Data Privacy Management* guide for details). When the value is edited, change takes effect immediately.

Zero means that service permissions based on SDK meta keys are disabled.

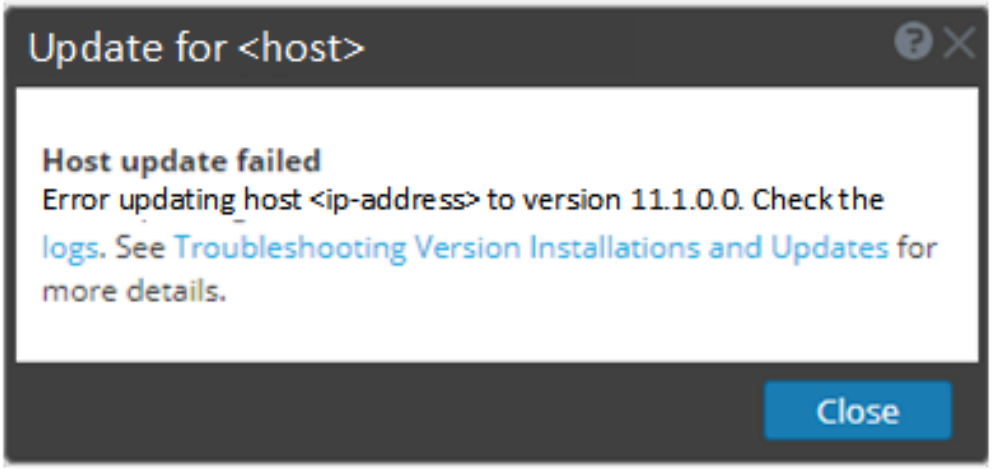
- 0 - disabled

When one of the non-zero values is specified, the data privacy officer can select a meta key to whitelist or blacklist the display of the associated meta, content, or both, for a specific user role on a service.

- 1 - whitelist meta and content filtered
- 2 - whitelist meta filtered
- 3 - whitelist content filtered
- 4 - blacklist meta and content filtered
- 5 - blacklist meta filtered
- 6 - blacklist content filtered

Troubleshooting Version Installations and Updates

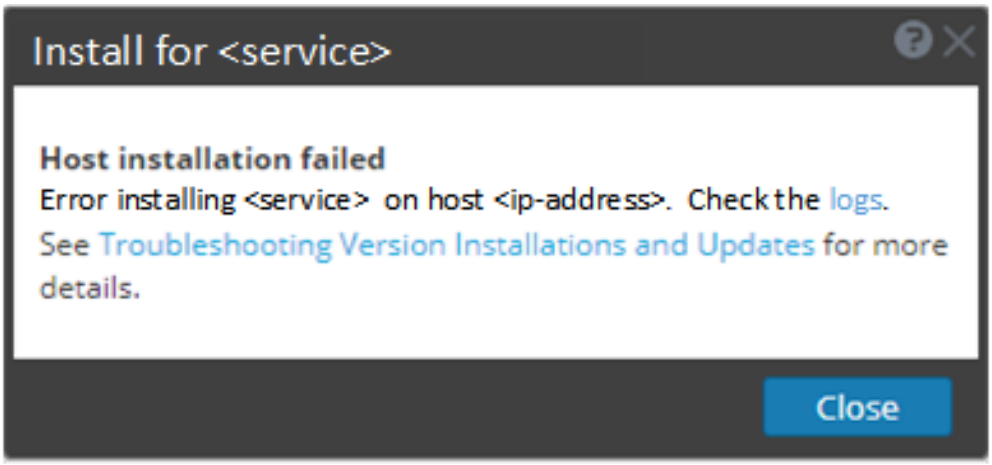
This section describes the error messages displayed in the **Hosts** view when it encounters problems updating host versions and installing services on hosts in the **Hosts** view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.

Solution	1. **Try to apply the version update to the host again**.
	Often this is all you need to do.
	2. If you still cannot apply the new version update:
	a. Monitor the following logs on NW Server as it progresses (for example, use submit the `tail -f` command string from the command line'):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error will appear in one or more of these logs.
	b. Try to resolve the issue and reapply the version update.

- Cause 1 - `deploy_admin` password has expired.
  Solution - Reset your `deploy_admin` password .
  Complete the following steps to resolve Cause 1.
  1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
  2. Select the `deploy_admin` and click **Reset Password**.
  3. (Conitional) If NetWitness Suite does not allow you to expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
     a. Reset `deploy_admin` to use a new password.
     b. On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`
- Cause 2 -The `deploy_admin` password was changed on NW Server host but not changed on non-NW Server hosts.
  Complete the following step to resolve Cause 2.
  - On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.
    `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Problem	When you select a host and click **Install** the install service process fails.

Solution	1. **Try to install the service again.**.
	Often this is all you need to do.
	2. If you still cannot install the service:
	a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error will appear in one or more of these logs.
	b. Try to resolve the issue and reinstall the service.
	• Cause 1 - Entered the wrong`deploy_admin` password in the nwsetup-tui.
	Solution - Retrieve your `deploy_admin` password.
	Complete the following steps to resolve Cause 1.
	1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
	2. Select the `deploy_admin` and click **Reset Password**.
	3. (Conitional) If NetWitness Suite does not allow you to expired

`deploy_admin` password in the **Reset Password** dialog, complete the following steps.

a. SSH to the NW Server host.
`security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name platform.deployment.password -quiet`

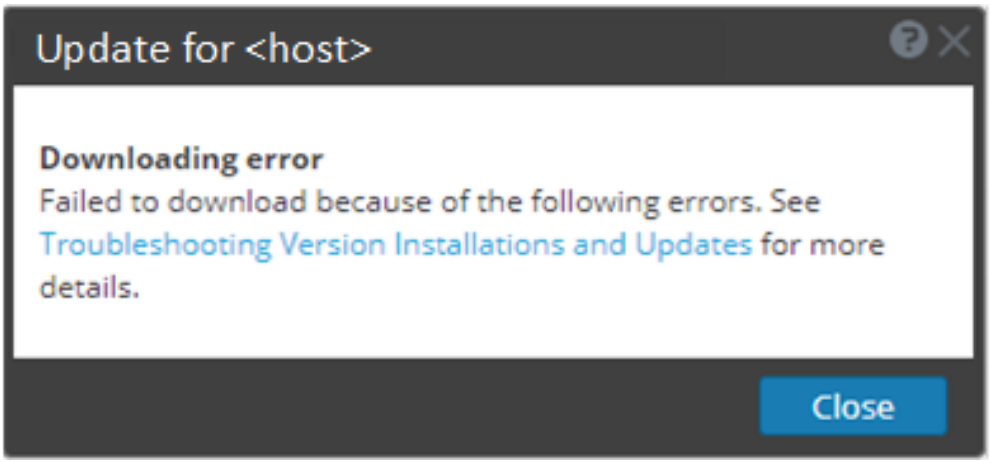
b. SSH to the host that failed installation/orchestration.

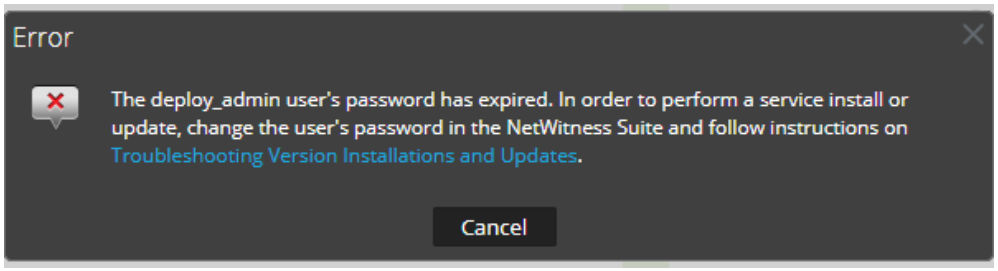
c. Run the nwsetup-tui again using correct `deploy_admin` password.

- Cause 2 -The `deploy_admin` password has expired.
  Complete the following step to resolve Cause 2.

  1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
  2. Select the `deploy_admin` and click **Reset Password**.
  3. (Conditional) If NetWitness Suite allows you enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
     a. Enter the expired `deploy_admin` password.
     b. Uncheck the Force password change on next login checkbox.
     c. Click **Save**.
  4. (Conditional) If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the Reset Password dialog, complete the following steps.
     a. Reset `deploy_admin` to use a new password.
     b. On all the NW Server host and all other hosts on 11.x, run the following command using the new `deploy_admin` password.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`
     c. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Problem	When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete.
Cause	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
Solution	1. Try to download it again. 2. If the download still fails, try to download it outside of NetWitness Suite as described in Apply Updates from the Command Line (No Web Access). 3. If you still cannot download the update file, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Cause	The `deploy_admin` user password has expired.
Solution	Reset your `deploy_admin` password password. 1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab. 2. Select the **deploy_admin** and click **Reset Password**. • If NetWitness Suite allows you to enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps. a. Enter the expired `deploy_admin` password. b. Uncheck the **Force password change on next login** checkbox. c. Click **Save** • If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the **Reset Password** dialog. a. On the NW Server host and all other hosts on 11.x , run the following command using the new `deploy_admin` password. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

RSA NETWITNESS® SUITE

Getting Started Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Getting Started with NetWitness Suite **6**

Overview 6

Architecture 6

Core Versus Downstream Components 9

Logging in to NetWitness Suite **11**

Log Off NetWitness Suite 12

Changing Your Password **13**

Identify Your Role **15**

NetWitness Suite Basic Navigation **16**

Accessing Main Views 17

Secondary Menus 17

Additional Options 17

Main Views 18

MONITOR 19

MONITOR Menu 19

RESPOND 20

RESPOND Menu 20

INVESTIGATE 23

INVESTIGATE Menu 23

CONFIGURE 28

CONFIGURE Menu 28

ADMIN 30

ADMIN Menu 31

Setting up Your Default View by SOC Role **33**

Setting Your Default View 35

Basic Troubleshooting Tips for User Setup 37

Setting User Preferences **38**

View Your User Preferences (Respond and some Investigate views) 38

View Your User Preferences (Most views except Respond and some Investigate views) 40

Set the Time Zone and Date and Time Format 40
Select the Default NetWitness Suite Starting Location 41
Select the Default Investigate View 41
Choose the Appearance of NetWitness Suite 41
Enable or Disable System Notifications for Your User Account 43
Enable or Disable Context Menus for Your User Account 43

Managing Dashboards 45

Dashboard Basics 45
Dashboard Title 45
Dashboard Selection List 45
Dashboard Toolbar 46
The Default Dashboard 47
Selecting a Preconfigured Dashboard 48
Enabling or Disabling Dashboards 48
Enabling a Dashboard 49
Disabling a Dashboard 51
Setting a Dashboard as a Favorite 51
Creating Custom Dashboards 52
Working with Dashlets 53
Add a Dashlet 55
Edit Dashlet Properties 56
Rearrange a Dashlet 59
Maximize a Single Dashlet 59
Delete a Dashlet 60
Importing and Exporting Dashboards 60
Import a Dashboard 60
Export a Dashboard 61
Copying a Dashboard 61
Sharing a Dashboard 62

Managing Jobs 63

Display the Jobs Tray 63
View Your Jobs in the Profile View > Jobs Panel 64
Pause and Resume Scheduled Execution of a Recurring Job 65
Cancel a Job 65
Delete a Job 65

Download a Job 66

Viewing and Deleting Notifications 67

View Notifications 67

View All Notifications 67

Delete Notification Records 68

Viewing Help in the Application 69

View Inline Help 69

View Tooltips 69

View Online Help 69

Finding Documents on RSA Link 70

Locate NetWitness Suite Documentation 70

Locate RSA Content 70

Locate RSA Supported Event Sources 71

Locate Hardware Setup Guides 71

Find Documents Using NetWitness Navigator 71

Follow Content for Updates 71

Send Your Feedback to RSA 72

NetWitness Suite Getting Started References 73

User Preferences 74

What do you want to do? 74

Related Topics 74

User Preferences (Respond and some Investigate views) 75

Preferences 77

Notifications Panel and Notifications Tray 79

What do you want to do? 79

Jobs Panel and Jobs Tray 82

What do you want to do? 82

Getting Started with NetWitness Suite

Overview

RSA NetWitness Suite is a powerful threat detection suite that enables Security Operation Centers (SOCs) to quickly locate, prioritize, and triage threats. NetWitness Suite helps you to isolate and remediate known threats as well as those that were previously unknown. It provides deep insight into packets, logs, and endpoints that provide you with an unparalleled view into your enterprise or business.

NetWitness Suite is more powerful than ever, but it is easier for Tier 1 Analysts to use because it automates the process of identifying and prioritizing suspicious threats. NetWitness Suite In addition, Tier 2 and Tier 3 analysts can hunt for and locate threats using new analysis tools along with views of metadata and raw data available in prior releases of NetWitness Suite.

Architecture

RSA NetWitness Suite is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. NetWitness Suite allows administrators to collect three types of data from the network infrastructure, packet data, log data, and endpoint data. If NetWitness Endpoint 4.4, 4.4.0.0, or later is installed and configured, endpoint event data is also collected. The key aspects of the architecture are:

- **Distributed Data Collection**. The **Decoder** ingests packet data while the **Log Decoder** ingests log data. Decoders parse and reconstructs all collected network traffic from Layers 2 - 7, or log and event data from hundreds of devices and event sources, including NetWitness Endpoint data (if installed and configured). The **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting. The **Broker** aggregates data captured by other devices and event sources. Brokers aggregate data from configured Concentrators; Concentrators aggregate data from Decoders. Therefore, a Broker bridges the multiple real-time data stores held in the various Decoder/Concentrator pairs throughout the infrastructure.
- **Real-time Alerting**. The NetWitness Suite **Event Stream Analysis (ESA)** service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators. ESA uses an advanced Event Processing Language (EPL) that allows analysts to express filtering, aggregation, joins, pattern recognition and correlation across multiple disparate event streams. Event Stream Analysis helps to perform powerful incident detection and alerting.
- **Real-time Analytics** (Automatic analysis of events) The RSA Automated Threat Detection

functionality includes preconfigured ESA analytics modules for detecting Command and Control traffic.

- **NetWitness Server**. The NetWitness Server provides Reporting, Investigation, Administration, and other aspects of the user interface.
- **Capacity**. NetWitness Suite has a modular-capacity architecture enabled with direct-attached capacity (DACs) or storage area networks (SANs), that adapts to the organization's short-term investigation and longer-term analytic and data-retention needs.

The NetWitness Suite provides large deployment flexibility. You can design its architecture using as many as multiple dozens of physical hosts or a single physical host, based on the particulars of the customer's performance and security-related requirements. In addition, the entire NetWitness Suite system has been optimized to run on virtualized infrastructure.

The System Architecture comprises these major components: Decoders, Brokers, Concentrators, Archivers, ESA, and Warehouse Connectors. NetWitness Suite components can be used together as a system or can be used individually.

- In a security information and event management (SIEM) implementation, the base configuration requires these components: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA), and the NetWitness Server.
- In a forensics implementation, the base configuration requires these components: Decoder, Concentrator, Broker, ESA, Malware Analysis, and Endpoint Hybrid or Endpoint Log Hybrid. The Response-Server service is also required and is used to prioritize alerts.

The table provides a synopsis of each major component:

System Component	Description
Decoder / Log Decoder	• NetWitness Suite collects packet, log, and endpoint data. • Packet data, that is, network packets, are collected using the Decoder through the network tap or span port, which is typically determined to be an egress point on an organization's network. • A Log Decoder can collect four different log types - Syslog, ODBC, Windows eventing, and flat files. • Windows eventing refers to the Windows 2008 collection methodology and flat files can be obtained via SFTP. • Both types of Decoders ingest raw transactional data that is enriched, closed out, and aggregated to other NetWitness Suite components. • The process for ingesting and parsing transactional data is a dynamic and open framework.
Endpoint Hybrid or Endpoint Log Hybrid	• Collects and manages endpoint data from hosts. • Generates metadata for investigation, analysis, alerting, and reporting. • Collects logs from Windows hosts, and all other event sources that are supported for the Log collection in the NetWitness Suite.
Concentrator	• Provides index and query capability to NetWitness Collections. • Can optionally forward data to ESA.
Broker	• Distributes NetWitness Collection access across many Concentrators or Archivers, making the entire NetWitness Suite enterprise appear as a single collection.

System Component	Description
Archiver	• The Archiver service enables long-term log archiving by indexing and compressing log data and sending it to archiving storage. • The archiving storage is optimized for long-term data retention, and compliance reporting. • Archiver stores raw logs and log metadata from Log Decoders for long term-retention, and it uses Direct-Attached Capacity (DAC) for storage. **Note:** Raw packets and packet metadata are not stored in the Archiver.
Event Stream Analysis (ESA)	• The Event Stream Analysis service provides event stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators. • ESA uses advanced Event Processing Language that allows users to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams. • ESA helps to perform powerful incident detection and alerting. • The RSA Automated Threat Detection functionality includes preconfigured ESA analytics modules for detecting Command and Control traffic.

Core Versus Downstream Components

In NetWitness Suite, the Core services ingest and parse data, generate metadata, and aggregate generated metadata with the raw data. The Core services are Decoder, Log Decoder, Concentrator, and Broker. Downstream systems use data stored on Core services for analytics; therefore, the operations of downstream services are dependent on Core services. The downstream systems are Archiver, ESA, Malware Analysis, Investigate, and Reporting.

Although the Core services can operate and provide a good analytics solution without the downstream systems, the downstream components provide additional analytics. ESA provides real-time correlation across sessions and events as well as between different types of events, such as log, packet, and endpoint data. Investigate provides the ability to drill into data, examine events and files, and reconstruct events in a safe environment. The Malware Analysis service provides real-time, automated inspection for malicious activity in network sessions and associated files.

Logging in to NetWitness Suite

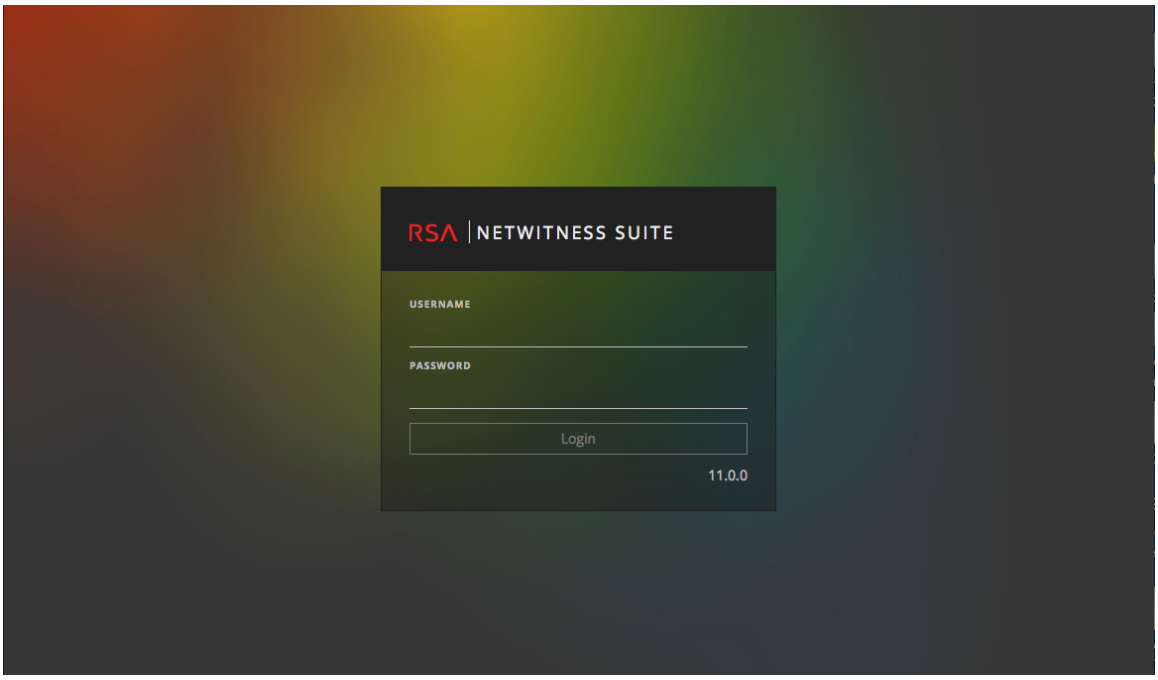
Logging in to NetWitness Suite can vary based on your environment. You may have an internal user account or an external user account. Internal user accounts are local to the NetWitness Suite and internal users can log in to NetWitness Suite and receive role-based permissions. External user accounts authenticate outside of the NetWitness Suite and are mapped to NetWitness Suite roles. If you are an external user and you cannot access NetWitness Suite or view the information that you need, contact your System Administrator. Your Administrator can assign the appropriate roles to your account.

1. Use an icon provided by your Administrator, or type the following in your web browser:

   `https://<hostname or IP address>/login`

   Where `<hostname or IP address>` is the hostname or IP address of your NetWitness server.

   The login screen is displayed.



2. Type your username and password, and then click **Login**.

   If your login is successful, you will be logged in to the landing page specified in your user preferences.

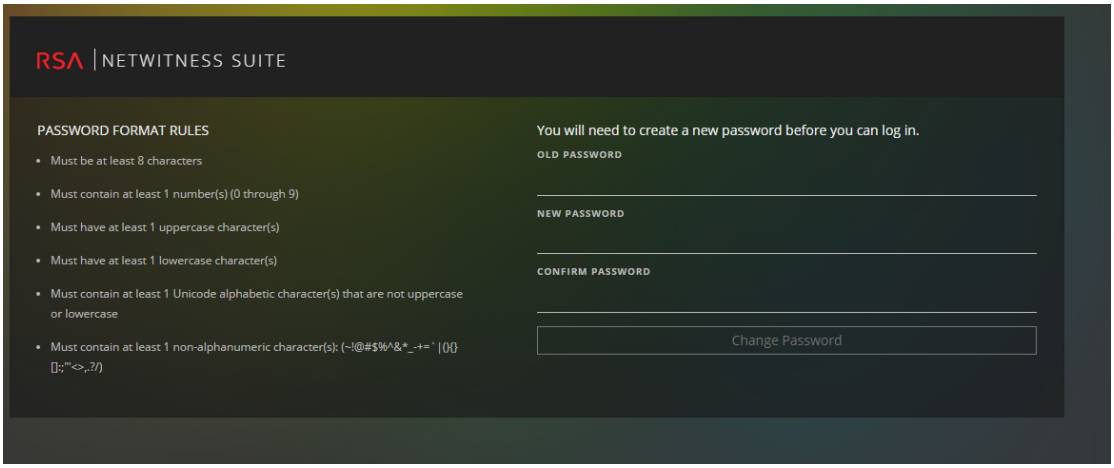
Note: NetWitness Suite supports modern (or current) versions of the latest browsers.

If you are locked out:

If you try too many times to log in with an incorrect username or password, your account will lock. Contact your Administrator to unlock your account.

If you have a new account or your account is expired:

1. In the dialog to create a new password, enter your old password, type a new password, and confirm it. Password format rules (as defined by your system administrator) are provided on the left and your new password must conform to the indicated format rules.



2. Click **Change Password**.

If you do not have the appropriate access to NetWitness Suite:

If you are able to log in successfully, but you are not able to view the information that you need, it is possible that you need a user role assigned to your user account. Contact your Administrator for assistance.

Log Off NetWitness Suite

To log off from the Respond and some Investigate views:

1. In the main menu bar, select .
2. In the User Preferences, click **Sign Out**.

To log off from the other views:

In the main menu bar, select > **Sign Out**.

Changing Your Password

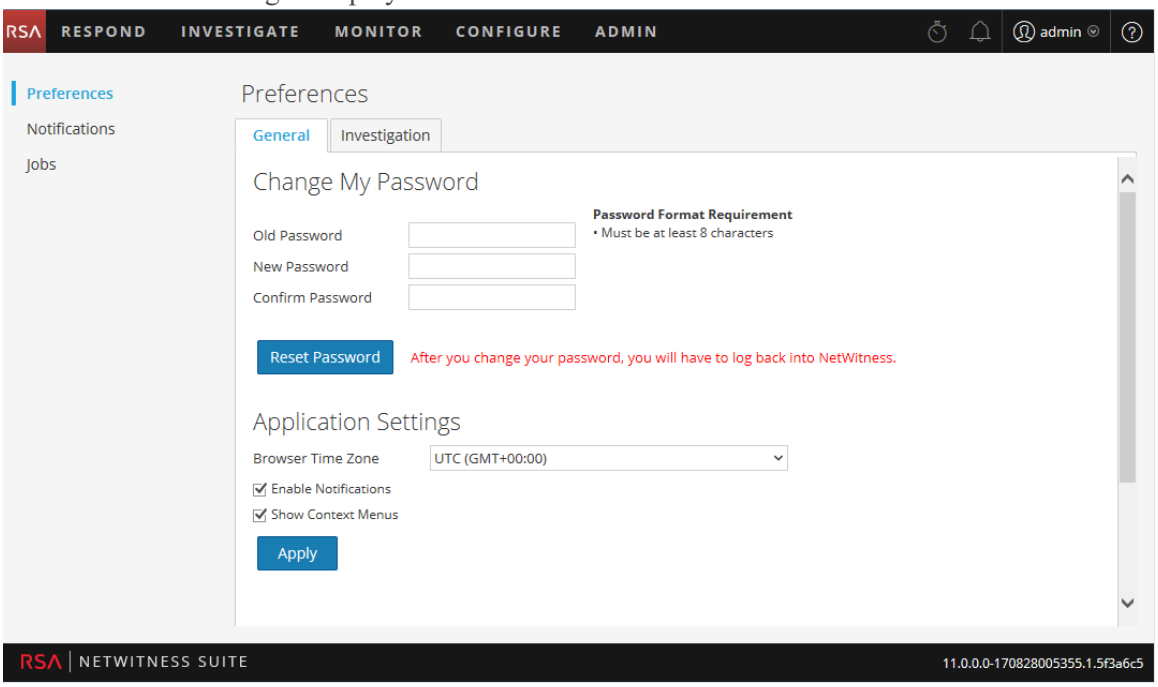
You can change the password that you use for NetWitness Suite authentication at any time in your user preferences. Your Administrator defines the appropriate password strength requirements for your NetWitness Suite password, such as minimum password length and minimum number of uppercase, lowercase, decimal, non-Latin alphabetic, and special characters. These requirements are then displayed when changing your password.

Note: When a Core service uses a trusted connection, you do not enter a password so no update is required for Core service accounts.

To change your password:

1. Do one of the following:
   - For most views, such as Investigate, Monitor, Configure, or Admin, select > **Profile**.
   - In the Respond and some Investigate views (Event Analysis, Hosts, and Files), select and in the User Preferences dialog click **Change my password**.

   The Preferences dialog is displayed.



2. In the **Change My Password** section, enter the password that you used to authenticate to NetWitness Suite in the **Old Password** field.
3. In the **New Password** field, enter the password that you want to use for the next login.
4. In the **Confirm Password** field, retype the new password.

5. Click **Reset Password**.
   You will be logged out of NetWitness Suite for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Suite.

Identify Your Role

The roles listed here are the typical roles or functions of a Security Operations Center (SOC). Determine the role or roles that you perform in the SOC. You can use these functions as a guide to decide how to set up and navigate NetWitness Suite so that you can efficiently perform your job tasks.

SOC Team

SOC Manager (SOC Management and Reporting)

- Manage SOC Readiness
- Respond to Incidents
- Respond to Data Breaches

Data Privacy Officer

Monitor and protect privacy and sensitive information

Incident Reponder (T1 Analyst)

- Respond to Incidents
- Remediate incidents

Threat Hunter (T2/T3 Analyst)

- Hunt for threats
- Conduct forensic analysis
- Recommend issues for remediation
- Remediate issues

Content Expert (Threat Intelligence)

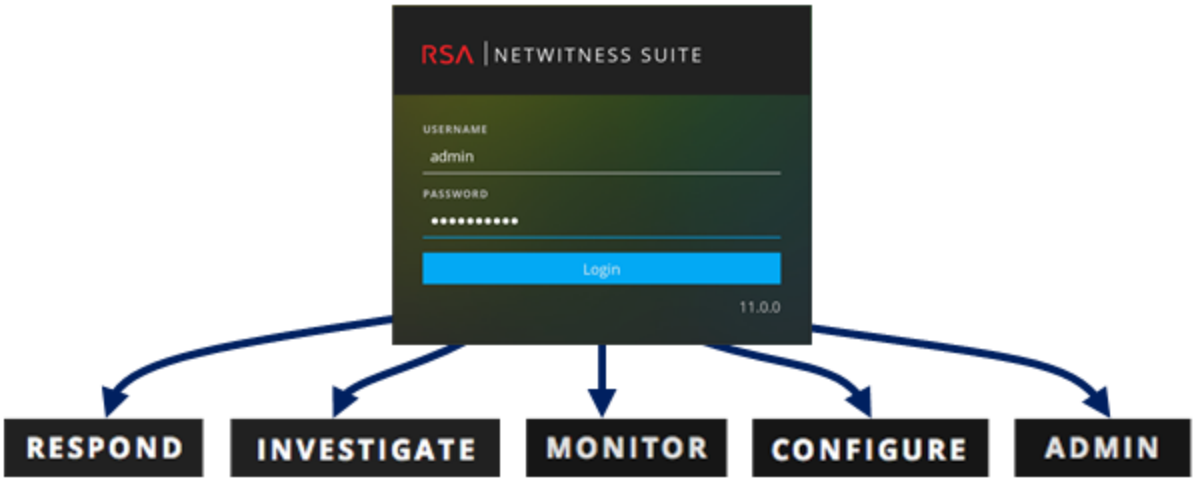
- Investigate new threat intelligence
- Evaluate and create new feeds
- Create correlation rules to flag indicators of compromise

System Administrator

- Install and configure equipment and software.
- Manage user access
- Monitor and fine tune performance
- Backup and restore data
- Manage storage and archives
- Update software
- Create reports for regulatory compliance

NetWitness Suite Basic Navigation

The NetWitness Suite application is divided into five main functional areas, known as views, that are based on typical Security Operation Center (SOC) roles.



- **RESPOND**: This view is for Incident Responders, who can view a list of prioritized incidents to triage. These incidents come from sources such as ESA rules, NetWitness Endpoint, or ESA Analytics modules for Automated Threat Detection. You can also view all of the alerts received by NetWitness Suite here.
  For legacy 10.6 users, this view was known as the Incident Management view. The Alerts List in the Respond view replaces the ESA 10.6 Alerts > Summary view.
- **INVESTIGATE**: This view is primarily for advanced Threat Hunters, who prefer to manually hunt for threats using NetWitness Suite metadata, raw event data, and event reconstruction and analysis. Incident Responders also use this view to get details about events associated with an incident being investigated. Both Threat Hunters and Incident Responders can use the forensic event reconstruction and event analysis features in this view.
- **MONITOR**: This view is for all users. You can view dashboards and reports on different areas of interest depending on your user permissions. NetWitness Suite opens to this view by default.
  For legacy 10.6 users, this is the Dashboard view.
- **CONFIGURE**: This view is for Threat Intel (content) personnel, who configure data sources and inputs to NetWitness Suite. Threat Intel personnel use this area to download and manage Live content. They can also create and manage incident and ESA rules.
  For legacy 10.6 users, this view contains Live, Incidents > Configure, and Alerts > Configure from the previous version.

- **ADMIN**: This view is for System Administrators, who set up and maintain the overall application.

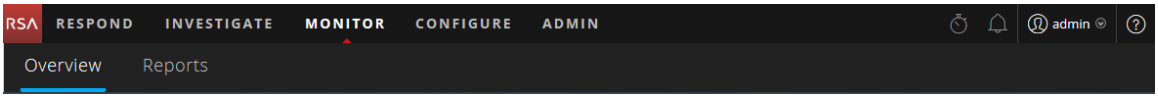
  For legacy 10.6 users, this is the Administration view less the sections added to the Configure view.

Accessing Main Views

The options that open each of the main views are listed at the top of the browser window. With the appropriate permissions, you can access any of these views at the top of every browser window at any time.

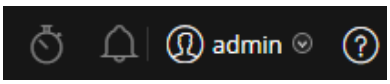
Secondary Menus

Some views have secondary menus with additional views that you can select, which vary according to the tasks that you can complete. The following example shows the MONITOR menu.

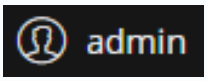
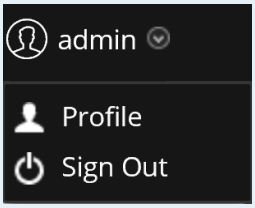


Additional Options

In addition to the main views, there are additional options at the top of the browser window that are common to the entire application.



The following table describes these common options:

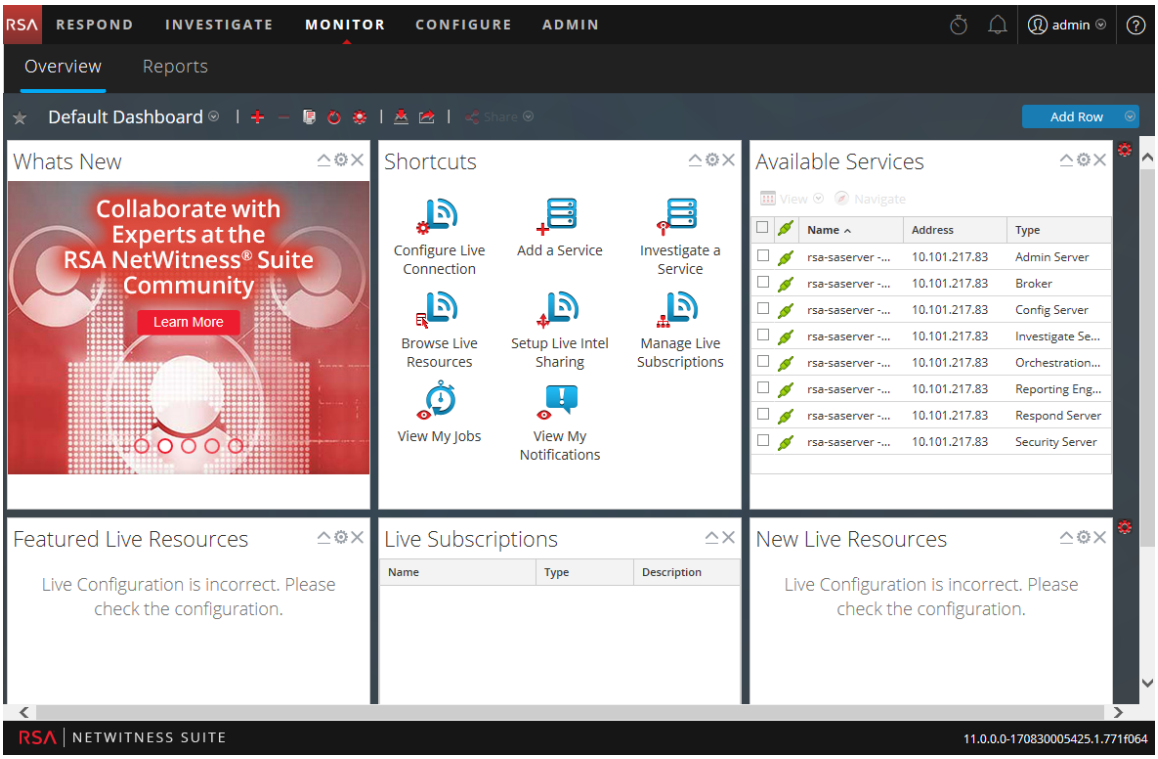
Common Option	Name	Description
	Jobs	In the INVESTIGATE, MONITOR, CONFIGURE, and ADMIN views, click this icon to view and manage your jobs in the Jobs tray. Jobs are on-demand or scheduled tasks that take some time to complete in the NetWitness Suite application.
	Notifications	Click this icon to view notifications from the application.
	User Preferences	Click this icon to view your available user preference options. You can manage your user preferences and log out of NetWitness Suite.
	User Profile	Click your user profile to view the available options. You can manage your user preferences, change your password, and log out of NetWitness Suite.
	Help	Click this icon to view NetWitness Suite help topics.

Main Views

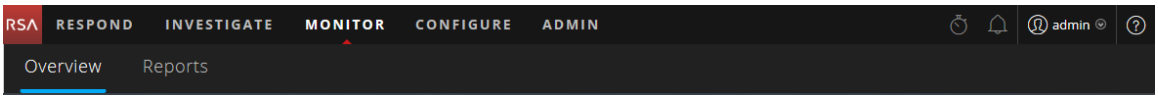
The following sections explain the main views.

MONITOR

The MONITOR view contains the NetWitness Suite dashboard. Monitor offers preconfigured dashboards and reports that you can use or you can create your own.



MONITOR Menu



The MONITOR menu has the following options:

- **Overview**: The Overview view enables you to view and manage your dashboards. You can select the following preconfigured dashboards:
  - Default
  - Identity
  - Investigation
  - Operations - File Analysis
  - Operations - Logs
  - Operations - Network

- Operations - Protocol Analysis
- Overview
- RSA SecurID
- Threat - Hunting
- Threat - Intrusion
- Threat - Malware Indicators

For legacy 10.6 users, this was the Dashboard view.

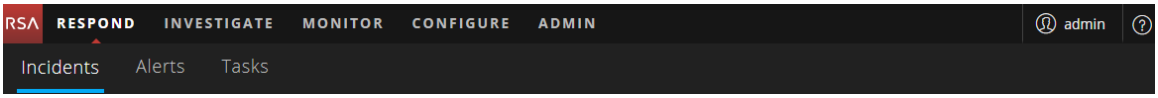
- **Reports**: The Reports view enables you to view and manage reports relevant to your SOC role according to your assigned permissions.

What can I do here?	Path	Show me how
Select a Dashboard	MONITOR > Overview	See Setting Up a Dashboard.
Create a Dashboard	MONITOR > Overview	See Setting Up a Dashboard.
Manage Dashboards	MONITOR > Overview	See Setting Up a Dashboard.
View a Report	MONITOR > Reports > View	See the *Reporting Guide*.
Manage Reports	MONITOR > Reports > Manage	See the *Reporting Guide*.

RESPOND

The Respond view presents analysts with a queue of incidents in severity order. When you take an incident from the queue, you receive relevant supporting data to help you investigate the incident. From there, you can determine the incident scope and escalate or remediate it as appropriate.

RESPOND Menu

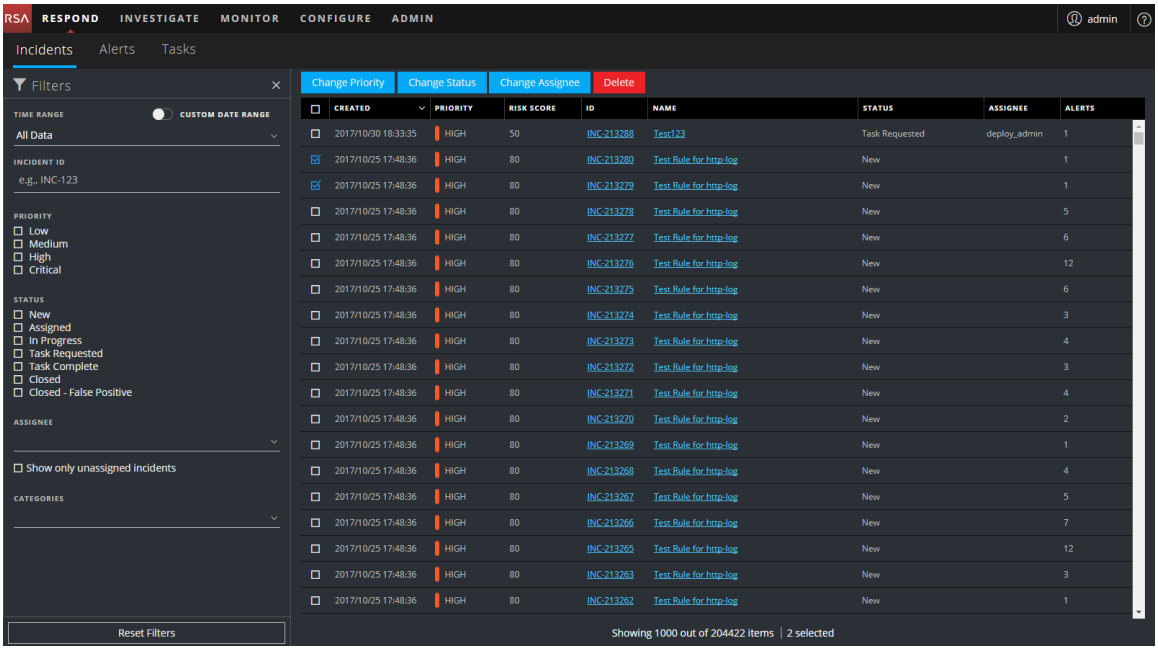


The RESPOND menu has the following options:

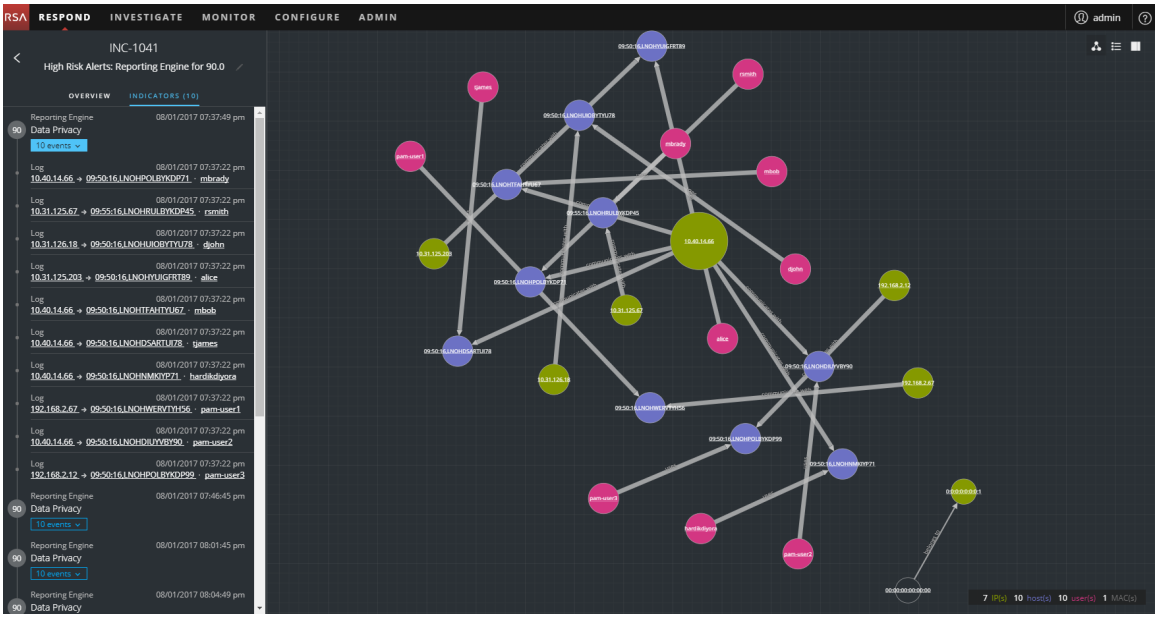
- **Incidents**: The Incidents List view contains a list of all incidents with basic information. The Incident Details view provides extensive details about the incident.

- **Alerts**: The Alerts List and Alert Details views provide information about all of the threat alerts and indicators received byNetWitness Suite in one location.
- **Tasks**: The Tasks List view enables you to create tasks and track them to completion.

The following figure shows the Respond view - Incident List view.

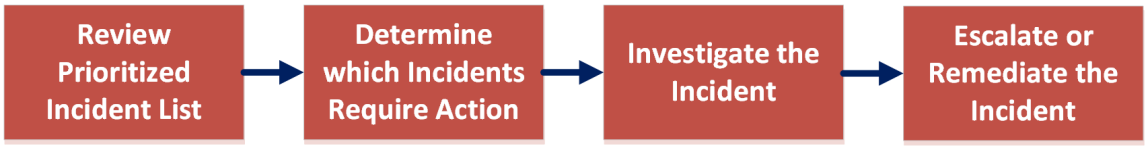


The following figure shows an example of the Respond view - Incident Details view.



When using NetWitness Suite as your case management tool, you can also case manage incidents from this view. New incidents appear at the top of the incident queue in priority order and incidents in progress are below the new incidents.

The following figure shows a high-level Respond view workflow.



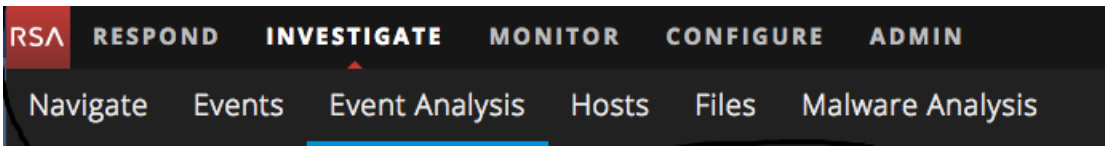
In the Respond view, analysts look at the prioritized list of incidents and determine which incidents require action. They click an incident for a clear picture of the incident with supporting details and they can investigate the incident further. Analysts can then determine how to respond to the threat, by escalating or remediating it.

What can I do here?	Path	Show me how
View prioritized incident lists	RESPOND > Incidents (Incident List view)	See the *NetWitness Respond User Guide*.
Determine which incidents require action (Triage an incident)	RESPOND > Incidents (Incident Details view)	See the *NetWitness Respond User Guide*.
Investigate the incident	RESPOND > Incidents (Incident Details view)	See the *NetWitness Respond User Guide*. (You can also pivot to the Investigate view.)
Escalate or Remediate the Incident	RESPOND > Incidents (Incident Details view) and RESPOND > Tasks (Tasks List view)	See the *NetWitness Respond User Guide*.
Review Alerts	RESPOND > Alerts (Alerts List and Alert Details views)	See the *NetWitness Respond User Guide*.

INVESTIGATE

The Investigate view presents six different views into a set of data, allowing analysts to see metadata, endpoint data, logs, events, and potential indicators of compromise. In addition to investigating data on a specific service, you can pivot into Investigate from Respond, the Monitor view, an entry in a report generated by the Reporting Engine, or a properly configured third-party application. You can begin your investigation in any of the six Investigate views, then continue the investigation in another Investigate view; the manner in which you proceed is determined by the question that needs to be answered. If you find an event that needs a response, you can create an incident in Respond where an incident responder will take further action. The *NetWitness Investigate User Guide* provides detailed information.

INVESTIGATE Menu



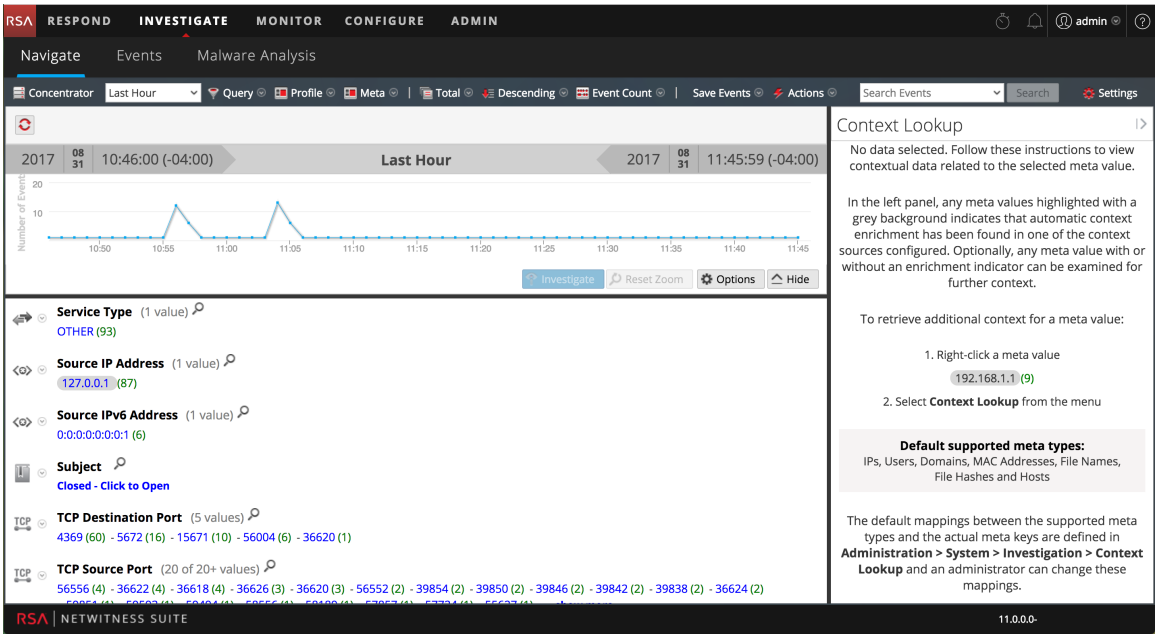
The INVESTIGATE menu has the following options:

- **Navigate**: The Navigate view provides a list of meta keys and meta values with a focus on metadata. You can drill into the data, open a selected event in the Events view or the Event Analysis view, view a reconstruction of an event, search for events, look up additional context from the Context Hub service, and configure Navigate view preferences.
- **Events**: The Events view provides a list of events with a focus on raw data. You can browse a simple list of events, a detailed list, and a log list. You can search for events, open a selected event in the Event Analysis view, view a reconstruction of the event, conduct event analysis, and configure Events view preferences.
- **Event Analysis**: The Event Analysis view provides a list of events with focus on metadata and raw data. You can view a reconstruction that offers helpful cues to identify points of interest in a reconstruction, jump to the Hosts view, pivot to standalone Endpoint, look up data in Live, and do external lookups.
- **Hosts view**: (Version 11.1 and later) The Hosts view lists all hosts with a NetWitness Endpoint Insights Agent running. For every host, you can view processes, drivers, DLLs, files (executables), services, and autoruns that are running, and information related to logged-in users. From the Hosts view, you can go to the Navigate and Event Analysis views.
- **Files view**: (Version 11.1 and later) The Files view lists all unique files found in your deployment and their associated properties. For each file, you can view details such as file

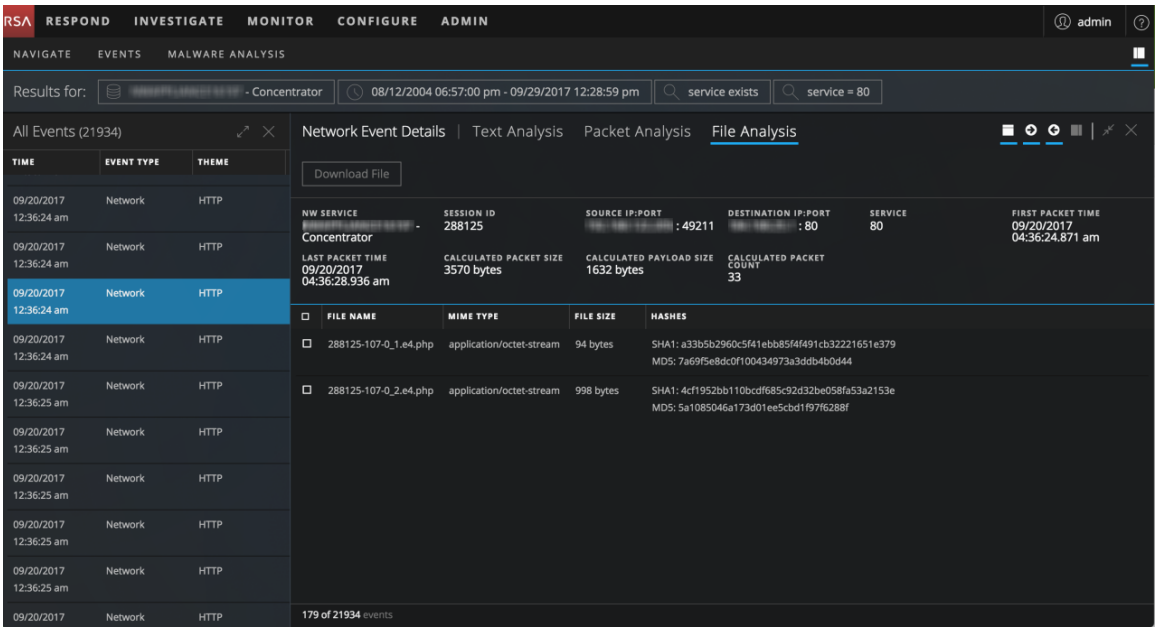
size, entropy, format, company name, signature, and checksum. From the Files view, you can go to the Navigate and Event Analysis views.

- **Malware Analysis**: Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows PE, PDF, and MS Office) to assess the likelihood that a file is malicious. Using Malware Analysis, you can prioritize the massive number of files captured in order to focus analysis efforts on the files that are most likely to be malicious.

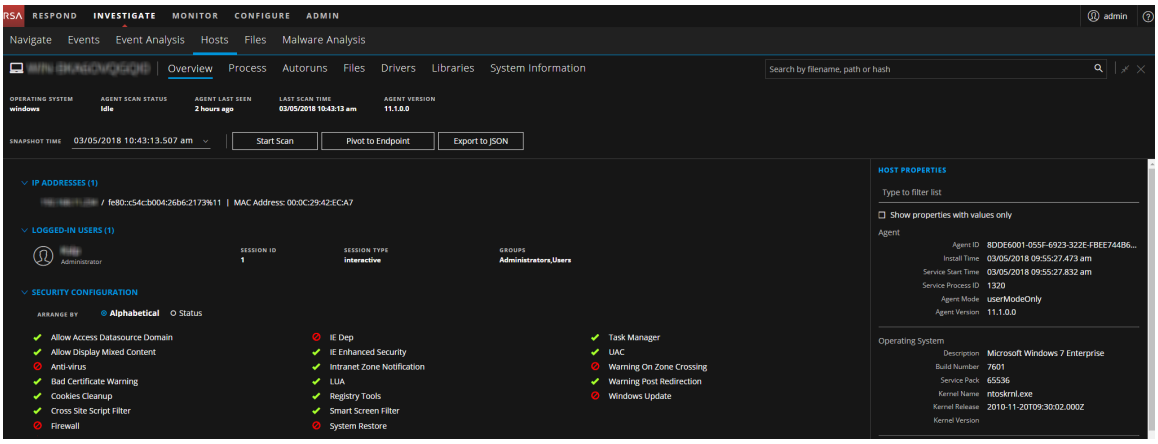
The following figure shows the Investigate view - Navigate view.



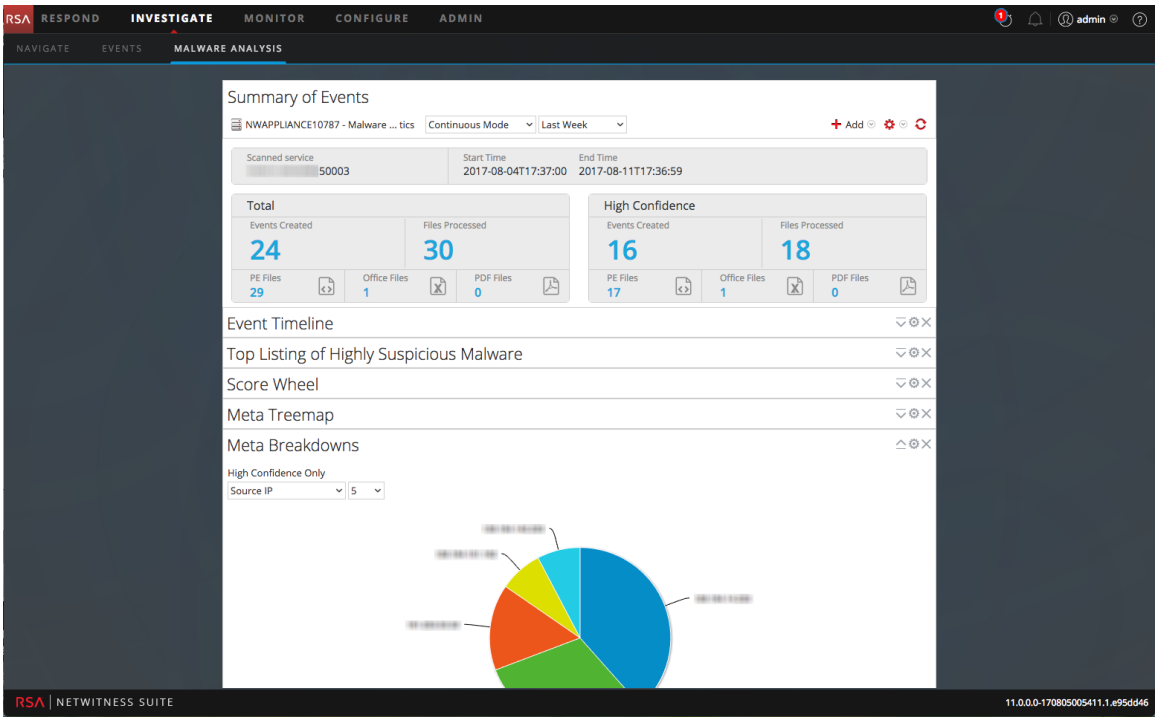
The following figure shows the Investigate view - Event Analysis view.



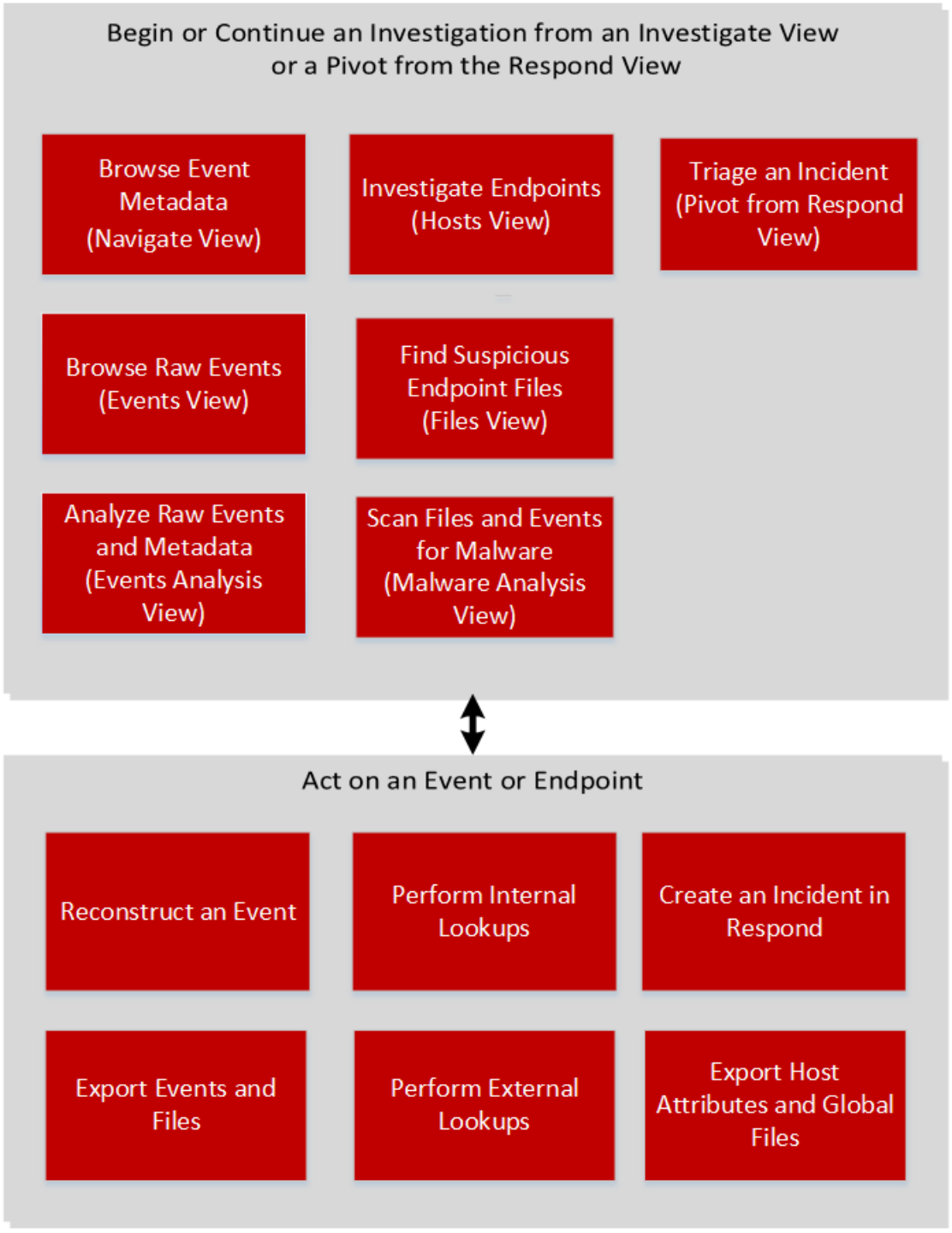
The following figure shows the Hosts view - Host Details view.



The following figure shows the Malware Analysis Summary of Events.



The following figure shows a high-level workflow of the Investigate view.

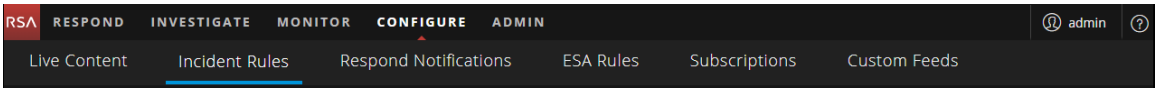

Begin or Continue an Investigation from an Investigate View or a Pivot from the Respond View
Browse Event Metadata (Navigate View)
Investigate Endpoints (Hosts View)
Triage an Incident (Pivot from Respond View)
Browse Raw Events (Events View)
Find Suspicious Endpoint Files (Files View)
Analyze Raw Events and Metadata (Events Analysis View)
Scan Files and Events for Malware (Malware Analysis View)
Act on an Event or Endpoint
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files

What can I do here?	Path	Show me how
Browse Event Metadata	Navigate view	See "Investigating Metadata in the Navigate View" in the *NetWitness Investigate User Guide*.
Browse Raw Events	Events view	See "Examining Raw Events in the Events View" in the *NetWitness Investigate User Guide*.
Analyze Raw Events and Metadata	Event Analysis view	See "Examining Metadata and Raw Events in the Event Analysis View" in the *NetWitness Investigate User Guide*.
Investigate Endpoints	Hosts view	See "Investigating Hosts and Files" in the *NetWitness Investigate User Guide*.
Find Suspicious Endpoint Files	Files view	See "Investigating Hosts and Files" in the *NetWitness Investigate User Guide*
Scan Files and Events for Malware	Malware Analysis view	See "Conducting Malware Analysis" in the *NetWitness Investigate User Guide*

CONFIGURE

The Configure view enables Threat Intel (content) personnel to configure data sources and inputs to NetWitness Suite in one convenient location.

CONFIGURE Menu



The CONFIGURE menu has the following options:

- **Live Content**: (Live Services) The Live Content view enables you to search for and subscribe to Live Services resources. Live Services is the component of the NetWitness Suite that manages communication and synchronization between NetWitness Suite services and a library of Live content available to RSA NetWitness Suite customers. You can view, search, deploy, and subscribe to content from the RSA Live Content Management System (CMS) to

NetWitness Suite services and software. When you subscribe to a resource, you agree to receive updates on a regular basis from RSA Live Services.
For Legacy 10.6 users, this was Live > Search.

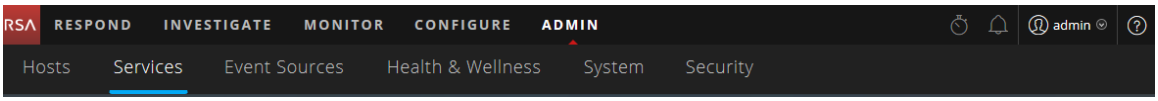
- **Incident Rules**: The Incident Rules view enables you to create incident rules with various criteria to automatically create incidents. You can view prioritized incidents in the Respond view.
  For Legacy 10.6 users, this was Incidents > Configure. In 11.1 and later, Aggregation Rules are known as Incident Rules.
- **Respond Notifications**: The Respond Notifications view enables you to automatically send email notifications to SOC Managers and the Analysts assigned to the incidents when incidents are created or updated.
- **ESA Rules**: The ESA Rules view enables you to manage the Event Stream Analysis (ESA) rules that specify criteria for problem behavior or threatening events in your network. When ESA detects a threat that matches the rule criteria, it generates an alert.
  You can create ESA rules yourself or download them from Live Services. The Rule Library shows all ESA rules created or downloaded. To activate rules, you have to add them to a deployment. Deployments map rules from your rule library to the appropriate ESA services.
  For Legacy 10.6 users, this was Alerts > Configure.
- **Subscriptions**: (Live Services) The Subscriptions view enables you manage the Live content that you subscribed to in the Live Content view. To set up Live Services on NetWitness Suite, you configure the connection and synchronization between the CMS server and NetWitness Suite.
  For Legacy 10.6 users, this was Live > Configure.
- **Custom Feeds**: (Live Services) The Custom Feeds view streamlines the task of creating and managing custom feeds, as well as populating the feeds to selected Decoders and Log Decoders. You can set up and maintain custom and identity feeds.
  NetWitness Suite uses feeds to create metadata based on externally defined metadata values. A feed is a list of data that is compared to sessions as they are captured or processed. For each match, additional metadata is created.
  You can create custom feeds to provide extra metadata extraction, for example, to accommodate custom network applications.
  For Legacy 10.6 users, this was Live > Feeds.

What can I do here?	Path	Show me how
Create a Live Services account.	RSA Live Registration Portal: https://cms.netwitness.com/registration/	See the *Live Services Management Guide*.
Find and deploy Live Services resources.	CONFIGURE > Live Content	See the *Live Services Management Guide*.
Create incidents automatically.	CONFIGURE > Incident Rules	See the *NetWitness Respond Configuration Guide*.
Configure Respond notifications.	CONFIGURE > Respond Notifications	See the *NetWitness Respond Configuration Guide*.
Configure alerts.	CONFIGURE > ESA Rules	See the *Alerting with ESA Correlation Rules User Guide*.
Set up Live Services Services on NetWitness Suite	CONFIGURE > Subscription	See the *Live Services Management Guide*.
Set up and maintain custom and identity feeds.	CONFIGURE > Custom Feeds	See the *Live Services Management Guide*.

ADMIN

In the Admin view, Administrators can manage network hosts and services; monitor the health and Wellness of NetWitness Suite; and manage system-level security. They can also configure global system resources and manage event sources.

ADMIN Menu



The ADMIN menu has the following options:

- **Hosts**: The Hosts view is where you set up and maintain hosts. A host is the machine on which services run and a host can be a physical or virtual machine.
- **Services**: The Services view enables you to manage services, manage service users and roles, maintain service configuration files, and explore and edit service properties. A service performs a unique function, such as a Decoder service, which captures network data in packet form.
- **Event Sources**: The Event Sources view enables you to manage event sources and configure alerting policies for them. Organizations typically monitor event sources in groups based on the criticality of the event sources. You can create monitoring policies for each event source group and order them based on priority.
- **Health & Wellness**: The Health & Wellness view enables you to monitor the health of the NetWitness Suite hosts and services in your network environment.
- **System**: The System view enables you to set global NetWitness Suite configurations. You can configure global audit logging, email, system logging, jobs, RSA Live Services, URL integration, Investigation, Event Stream Analysis (ESA), ESA Analytics, and advanced performance settings. In addition, you can manage NetWitness Suite versions and configure the local licensing server.
- **Security**: The Administration Security view provides the capability to manage user accounts, manage user roles, map external groups to NetWitness Suite roles, and modify other security-related system parameters. These apply to the NetWitness Suite system and are used in conjunction with the security settings for individual services.

What can I do here?	Path	Show me how
Manage hosts.	ADMIN > Hosts	See the *Host and Services Getting Started Guide*.
Manage services including managing service user access and security.	ADMIN > Services	See the *Host and Services Getting Started Guide*.

What can I do here?	Path	Show me how
Manage event sources and configure alerting policies for them.	ADMIN > Event Sources	See the *Event Source Management Guide*.
Set up and monitor alarms for the hosts and services in your NetWitness Suite domain.	ADMIN > Health & Wellness > Alarm	See the *System Maintenance Guide*.
Monitor statistics for the NetWitness Suite hosts and the services running on the hosts.	ADMIN > Health & Wellness > Monitoring	See the *System Maintenance Guide*.
Create and apply policies to your hosts and services to help you maintain the health and wellness of your NetWitness Suite domain.	ADMIN > Health & Wellness > Policies	See the *System Maintenance Guide*.
Set global configurations for NetWitness Suite.	ADMIN > System	See the *System Configuration Guide*.
Configure Global Audit Logging.	ADMIN > Systen > Global Auditing	See the *System Configuration Guide*.
Set up system security.	ADMIN > Security	See the *System Security and User Management Guide*.
Manage system users with roles and permissions.	ADMIN > Security	See the *System Security and User Management Guide*.

Setting up Your Default View by SOC Role

After logging in to NetWitness Suite, you can make navigating the application easier by setting up your default view based on your Security Operations (SOC) role. You set your default view, also known as a landing page, in your user preferences.

The following figure shows the main NetWitness Suite views.

- **Respond**: This view is for Incident Responders, who can view a list of incidents to triage and alerts. For legacy 10.6 users, this view was known as the Incident Management view and the Respond > Alerts view replaces the ESA 10.6 Alerts > Summary view .
  Respond is the default opening view. If you do not have permission to see the Respond view, you will have Monitor as your default view.
- **Investigate**: This view is for Threat Hunters, who investigate and hunt for advanced threats.
- **Monitor**: This view is for all users and it is the classic view for previous application versions. You can view dashboards and reports on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard.
- **Configure**: This view is for Threat Intel (content) personnel, who configure data sources and inputs to NetWitness Suite. Threat Intel personnel use this area to download and manage Live content. They can also create and manage incident and ESA rules.
  For legacy 10.6 users, this view was Live, Incidents > Configure, and Alerts > Configure.
- **Admin**: This view is for System Administrators, who set up and maintain the overall application.

You can select any of the main NetWitness Suite views as your default view. In addition to the main views, NetWitness Suite has predefined dashboards that you can select in the Monitor view depending on the tasks you perform:

- Default Dashboard
- Identity Dashboard
- Operations - Logs Dashboard
- Operations - Network Dashboard
- Overview Dashboard

- Threat - Indicators Dashboard
- Threat - Intrusion Dashboard

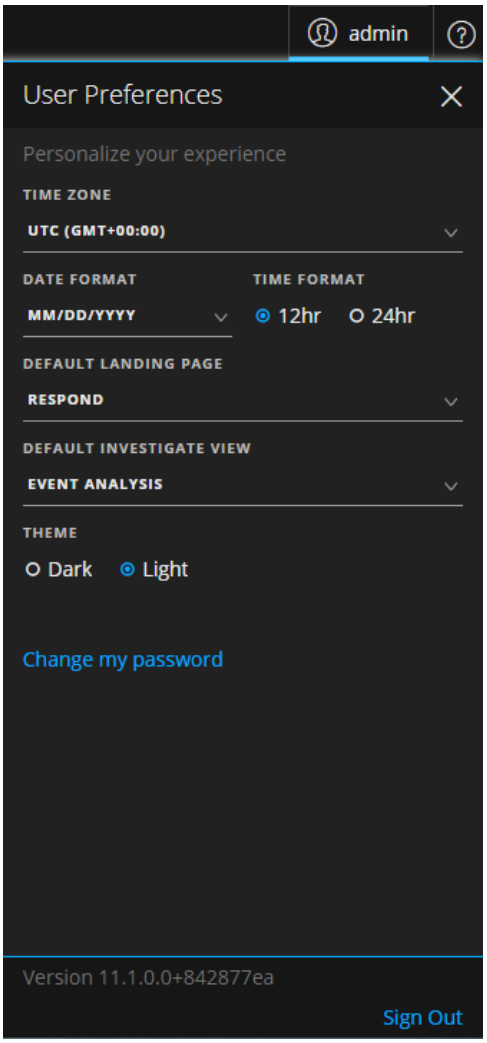
The following table shows typical SOC roles and the available views you can select as your landing page in your user preferences based on your SOC role. If you have more than one role, select the view that is most appropriate for you to start with when you log in to NetWitness Suite.

SOC Roles	Role Description	Consider this Default Landing Page
Incident Responder (Tier 1 Analyst)	Addresses incidents and alerts queued for them to review and mitigate	**RESPOND**
Threat Hunter (Tier 2/Tier 3 Analyst)	Investigates and hunts for advanced threats	**INVESTIGATE**
SOC Manager (SOC Management and Reporting)	Manages SOC readiness and responds to incidents and data breaches.	**MONITOR** (Dashboard is in the MONITOR view.) When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard.)
Content Expert (Threat Intelligence)	Configures data sources and inputs to NetWitness Suite.	**MONITOR** or **CONFIGURE** (Dashboard is in the MONITOR view. When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard. If you choose MONITOR as your default view, you can navigate to the CONFIGURE view from the main menu.)

SOC Roles	Role Description	Consider this Default Landing Page
Data Privacy Officer (DPO)	Similar to an Administrator, but a DPO monitors and protects privacy-sensitive information.	**MONITOR** (Dashboard is in the MONITOR view. When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard.)
System Administrator	Focuses on the configuration and stability of the overall application. Manages user access.	**ADMIN**

Setting Your Default View

1. (Respond view and some Investigate views) On the main menu bar, select .
   The User Preferences dialog shows your current preferences.



2. In the **Default Landing Page** field, select the default view that you would like to see when you log in to NetWitness Suite. Use the above table to make your selection based on your SOC role. For example, if you are an Incident Responder, you can select **Respond** and if you are a Threat Hunter, you can select **Investigate**.
   Your preferences become effective immediately. You can change your default landing page at any time. For information on other preferences, see Setting User Preferences.
3. To verify that you can see the correct default view, click **Sign Out** to log out and then log back in to NetWitness Suite.

Basic Troubleshooting Tips for User Setup

The following table provides basic troubleshooting tips that may be helpful for user setup in NetWitness Suite.

Problem	Troubleshooting Tip
When I log in to NetWitness Suite, I see the wrong default view.	Verify that the correct default view is set in the Default Landing Page field in your user preferences. If you select the MONITOR view, you can select the predefined dashboard that is most appropriate for your SOC role. You can also import or create your own dashboard.
I see the correct view, but the metadata does not load.	Try using another browser. For example, if you are using Safari, try using Firefox or Chrome.
I am using Internet Explorer 10 and I get the following error: `The page can't be displayed.`	NetWitness Suite supports modern (or current) versions of the latest browsers. Try installing a newer browser version. If you cannot upgrade your browser, you can try enabling the TLS 1.2 protocol in your browser: Navigate to **Internet options > Advanced > Settings > Security**. In addition to your other protocols, ensure that the TLS 1.2 protocol is enabled. Click **Apply**. Reload the page.
When I log in, I cannot see anything.	See your Administrator, you may need a user role assigned to your account or additional troubleshooting.
I can't see where to change my default landing page.	Go to the User Preferences in the Respond view or see your Administrator.

Setting User Preferences

You can view and manage your NetWitness Suite global application preferences from your user profile. Your global preference options vary depending on whether you access them from the Respond view or other views, such as Monitor, Configure, Admin, and Investigate.
You can:

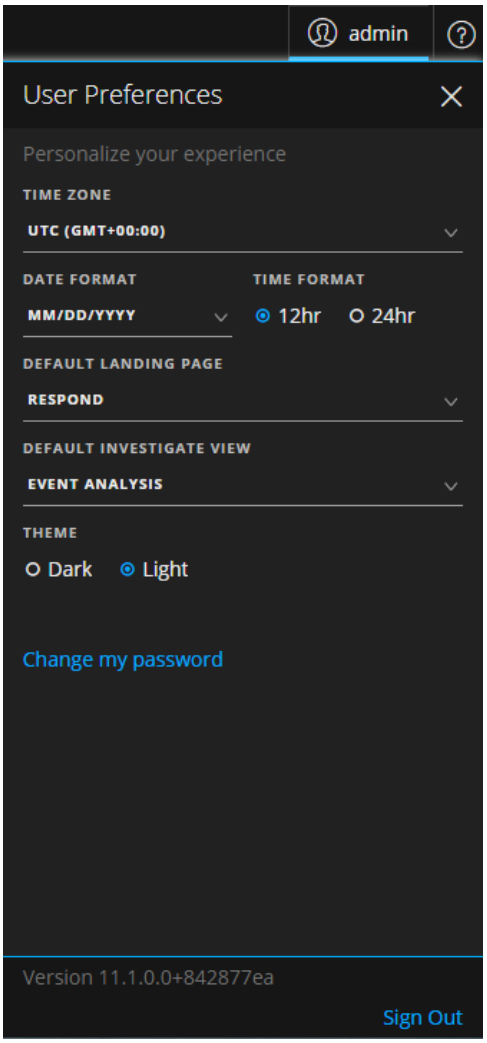
- Set the application time zone
- Set the application date and time format *
- Select your default NetWitness Suite starting location*
- Select your default Investigate view*
- Choose a dark or light theme for the application*
- Change your password (See Changing Your Password for more information.)
- Enable or disable notifications**
- Enable or disable context menus**

* You can make this change from the **User Preferences** dialog accessible from Respond and some Investigate views: Event Analysis, Hosts, and Files.

** You can make this change from the **Preferences** dialog accessible from most views except Respond and some Investigate views: Event Analysis, Hosts, and Files.

View Your User Preferences (Respond and some Investigate views)

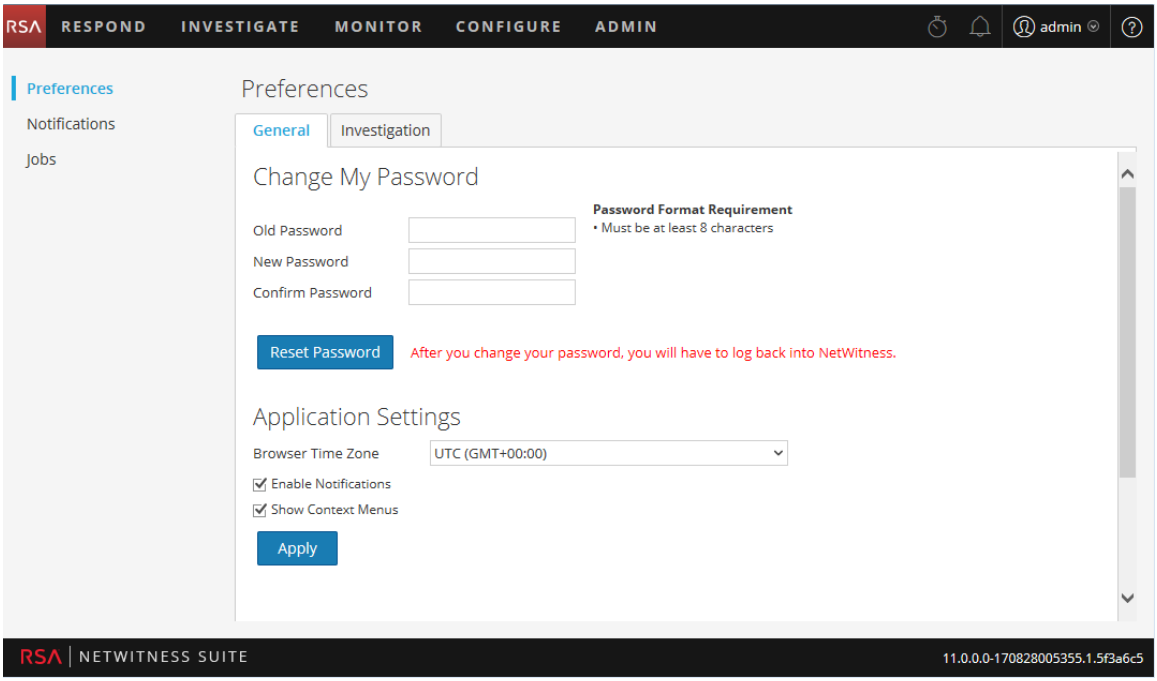
In the upper left corner of the NetWitness Suite browser window, select .
The User Preferences dialog shows your current preferences when accessed through the Respond view and the following Investigate views: Event Analysis, Hosts, and Files.



Any selections that you make become effective immediately.

View Your User Preferences (Most views except Respond and some Investigate views)

For most of the following views: Investigate, Monitor, Configure, and Admin: In the upper left corner of the NetWitness Suite browser window, select > **Profile**.
The Preferences dialog shows your current preferences.



Set the Time Zone and Date and Time Format

You can change the time zone and the format of the date and time for your location.

Note: You can only change the date and time preferences for your location from the Respond and some Investigate views: Event Analysis, Hosts, and Files.

1. In the User Preferences dialog, select your localization preferences:
   a. **Time Zone**: Set the time zone to use in the NetWitness Suite.
   b. **(Respond and some Investigate views) Date Format**: Set the format for the order of the display of the month (MM), day (DD), and year (YYYY). For example, the MM/DD/YYYY format shows the date as 05/11/2017.
   c. **(Respond and some Investigate views) Time Format**: Set the time as 12-hour or 24-hour time. For example, 2:00 PM in 12-hour time is 14:00 in 24-hour time.

   Changes in the Respond view become effective immediately.

2. **(Most views except Respond and some Investigate views)** Click **Apply**.
   Your preferences become effective immediately.

Note: When Daylight Saving Time (DST) starts or ends, if the selected time zone for the currently logged in user observes DST, the UI automatically updates to reflect the correct time.

Select the Default NetWitness Suite Starting Location

1. **(Respond and some Investigate views)** Open the User Preferences dialog.
2. In the **Default Landing Page** field, select the opening view that you would like to see when you log in to NetWitness Suite. You can choose Respond, Investigate, Monitor, Configure, and Admin according to your user role. For example, you can choose Respond to go directly to the relevant section of the application for Incident Responders. See Setting up Your Default View by SOC Role to help you select the appropriate default view.
   This selection sets the default view for the entire application. Changes become effective immediately.

Select the Default Investigate View

1. **(Respond and some Investigate views)** Open the User Preferences Dialog.
2. In the **Default Investigate View** field, select the default landing page when you log in to NetWitness Suite and navigate to Investigate. You can choose Navigate, Events, Event Analysis, Hosts, Files, or Malware Analysis as the default Investigate view. For example, you can choose Events for the default Investigate view to go directly to the Events page to view the events generated for a service. See Setting up Your Default View by SOC Role to help you select the appropriate default view.

Note: After you have applied the change in the drop-down, sometimes it takes few seconds for the changes to come in effect.

Choose the Appearance of NetWitness Suite

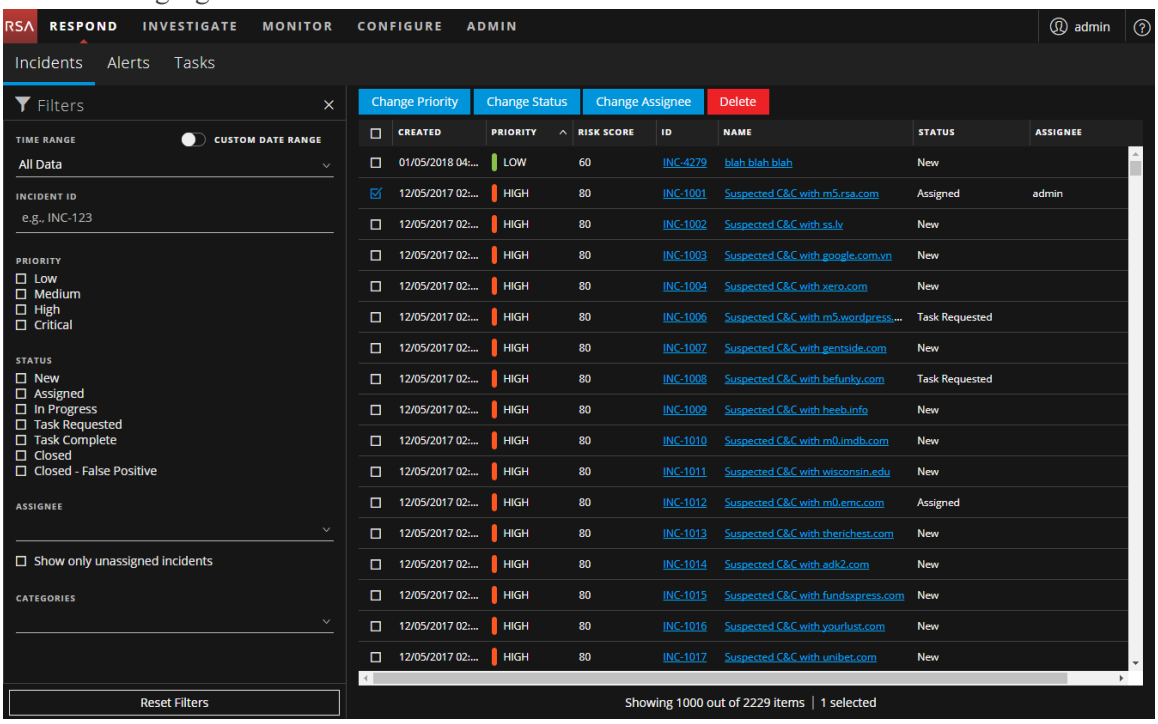
This option is only available for NetWitness Suite versions 11.1 and later.

You can choose a dark theme or a light theme for your application, depending on your personal preference. When you change the theme, the Respond view and some Investigate views change to the light or dark theme. Your selection only changes how NetWitness Suite appears to you, not other users.

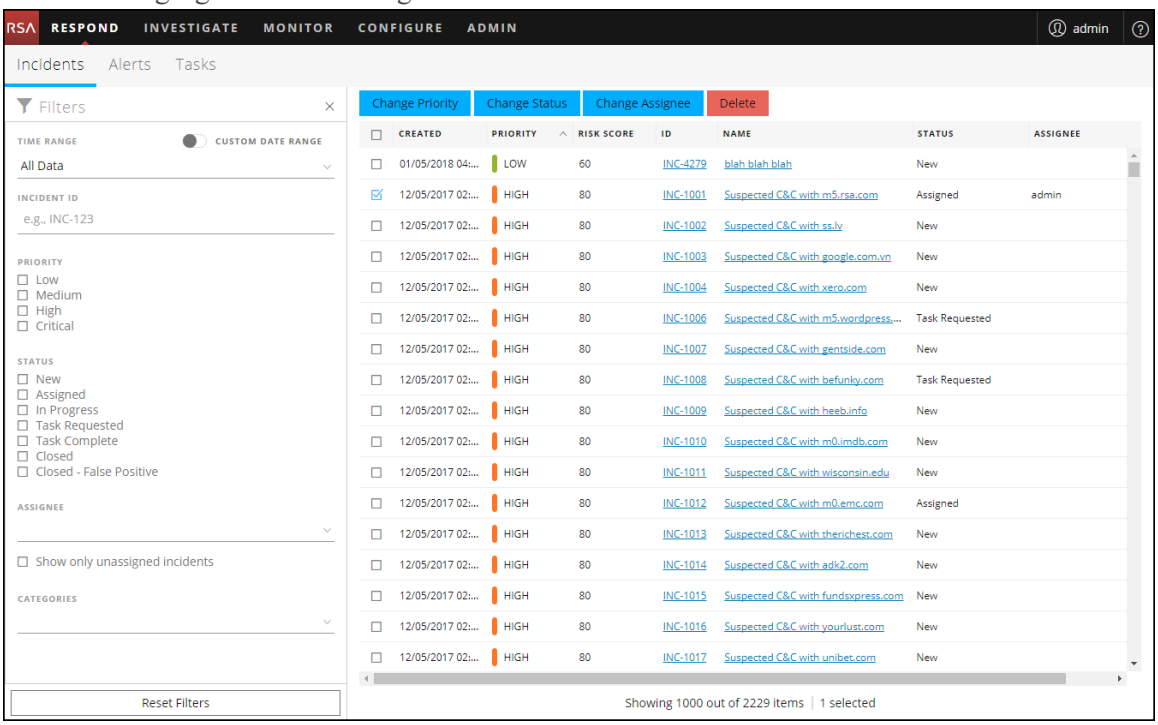
1. **(Respond and some Investigate views)** Open the User Preferences dialog.
2. Under **THEME**, select one of the following options:
   - **Dark**: The dark theme is best for darker environments or when you do not need as much contrast.
   - **Light**: The light theme is best for lighter environments, when you need more contrast, or when you are projecting the application for others to view. Since some views are not affected by the theme changes, you may want to choose the light theme for a more cohesive viewing experience.

Changes become effective immediately.

The following figure shows the dark theme.



The following figure shows the light theme.



Enable or Disable System Notifications for Your User Account

(Most views except Respond and some Investigate views) By default, NetWitness Suite system notifications are enabled when a new user account is created. You can disable and enable these notifications at any time.

1. In the Preferences dialog:
   - To enable notifications for your user account, select the **Enable Notifications** checkbox.
   - To disable notifications, clear the **Enable Notifications** checkbox.
2. Click **Apply**.

   Your preference becomes effective immediately.

Enable or Disable Context Menus for Your User Account

(Most views except Respond and some Investigate views) By default, context menus are enabled when a new user account is created. Context menus provide additional functions for specific views when you right-click a view.

1. In the Preferences dialog:
   - To enable context menus for your user account, select the **Enable Context Menus** checkbox.
   - To disable context menus, clear the **Enable Context Menus** checkbox.
2. Click **Apply**.
   Your preference becomes effective immediately.

Note: Settings available on the Investigate tab in the Preferences dialog are documented in the *NetWitness Investigate User Guide*.

Managing Dashboards

A dashboard is a group of dashlets that give you the ability to view in one space, the key snapshots of the various components that you consider important. In NetWitness Suite, you can compose dashboards to obtain high-level information and metrics that portray the overall picture of a NetWitness Suite deployment, displaying only the information that is most relevant to the day-to-day operations.

By default, the NetWitness Suite default dashboard is displayed when you log in to NetWitness Suite, and it is populated with a few useful dashlets to get you started with your own customizations. The dashboards for all NetWitness Suite components are available to add to the default NetWitness Suite dashboard or a custom NetWitness Suite dashboard.

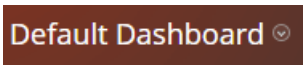
You can view dashboards and reports on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard. The dashboards help you to quickly and easily view reports. You can configure your dashboards to display the information that supports your workflow. This topic explains the high-level tasks that can be done when you are setting up a dashboard.

Dashboard Basics

If the Monitor view is your default landing page following logging in to NetWitness Suite you will always see either the default dashboard or the currently configured dashboard immediately after completing the login process. To return to the dashboard from another NetWitness Suite component, go to **MONITOR** > **Overview**.

Dashboard Title

The dashboard title reflects the currently active dashboard; for example, Default Dashboard.



Dashboard Selection List

You can access preconfigured and custom dashboards on the dashboard selection list. When you select a dashboard, its title is displayed below the NetWitness Suite toolbar.

A dashboard has:

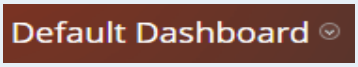
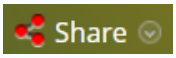
- The dashboard toolbar
- The dashboard title and the dashboard selection list.

Dashboard Toolbar

The dashboard toolbar is available next to the title of the selected dashboard. The dashboard toolbar allows various operations on dashboards and dashlets.

Note: The Copy, Delete, Import, Export, Share, and Add Row options are disabled for preconfigured dashboards.

Option	Description
	Sets the selected dashboard as the Favorite.

Option	Description
	Displays the list of available dashboards from which you can make a selection.
	Displays the Create a Dashboard dialog, where you define or add a custom dashboard.
	Deletes a custom dashboard. The default dashboard cannot be deleted.
	Allows you to copy a dashboard.
	Displays the Manage Dashlet dialog.
	Exports a dashboard as a .zip file.
	Imports a dashboard as .zip or.cfg file.
	Allows you to share a dashboard with another user.
	Enables user to add rows and columns to the dashboard based on the requirement. Click the icon in a row to add a dashlet.

The Default Dashboard

The default dashboard is configured to display specific dashlets in specific positions. The default dashboard serves as an example of dashboard composition and a starting point for customization.

- You can customize the information on the default dashboard by editing, adding, moving, maximizing, and deleting dashlets.
- After modifying the default dashboard, you can restore the default dashboard ( ) to its original layout.
- The default dashboard cannot be deleted or shared.

Selecting a Preconfigured Dashboard

On installation of NetWitness Suite Suite, the following preconfigured dashboards are automatically activated and are available to you:

- Default
- Identity
- Investigation
- Operations - File Analysis
- Operations - Logs
- Operations - Network
- Operations - Protocol Analysis
- Overview
- RSA SecurID
- Threat - Hunting
- Threat - Intrusion
- Threat - Malware Indicators

You cannot perform the following actions on a preconfigured dashboard:

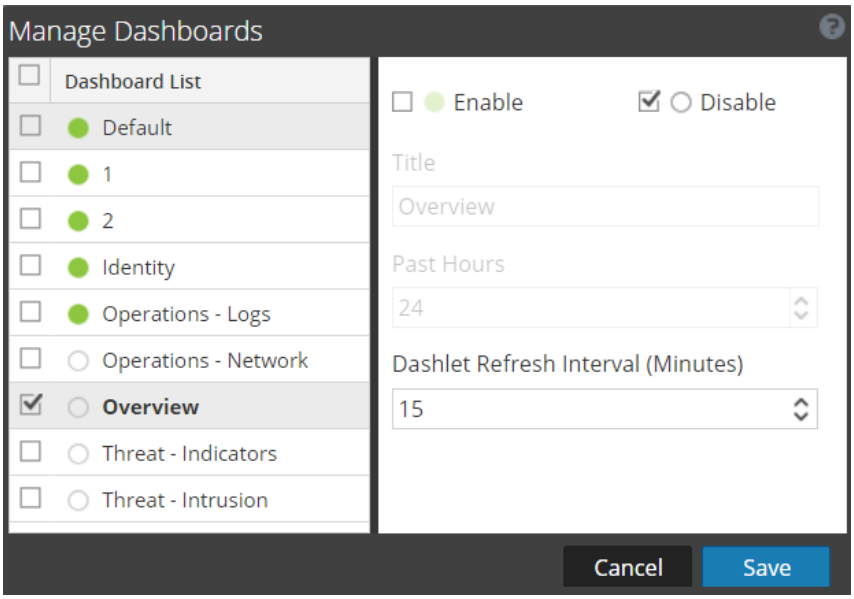
- Edit a dashboard
- Export a dashboard
- Share a dashboard
- Delete a dashboard

For more information on each Preconfigured dashboard, see the Dashboards Catalog in the RSA Content space on RSA Link.

Enabling or Disabling Dashboards

When you enable or disable a dashboard, all the dashlets within the dashboard are enabled or disabled along with the associated charts, unless they are used in any other dashboard.

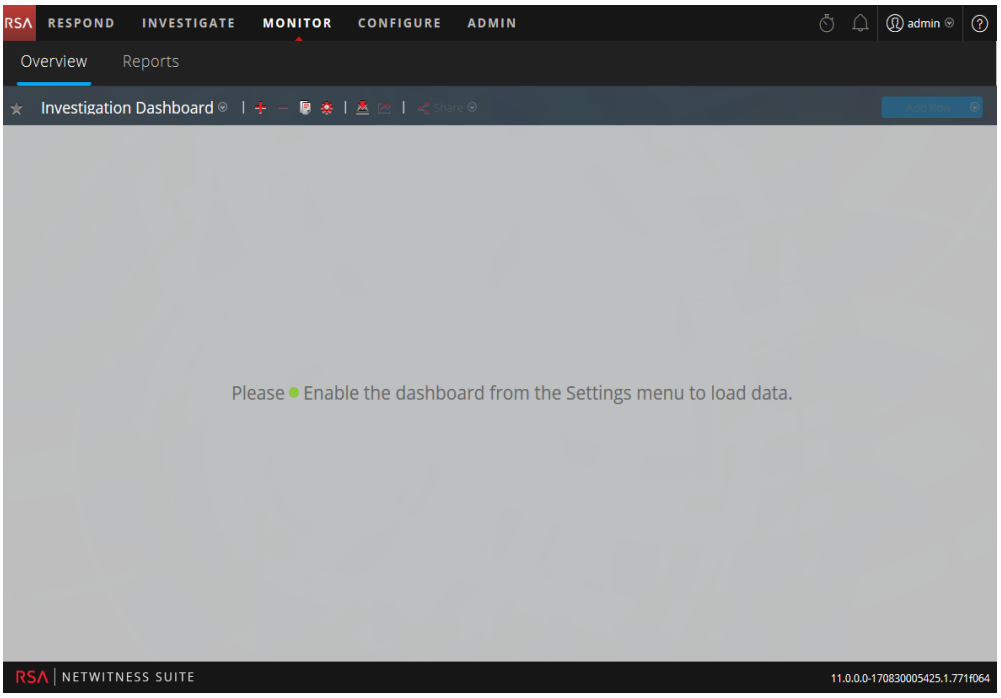
NetWitness Suite modules can display only those dashlets presented in the Manage Dashlet dialog. The main dashboard offers all NetWitness Suite dashlets. This is an example of currently available dashlets.



Name	Description
Dashboard List	Displays a list of the default, preconfigured, and custom dashboards.
Enable	Displays if the selected dashlet is enabled.
Disable	Displays if the selected dashlet is disabled.
Title	Displays the title of the selected dashlet and you can also rename the dashaboard.
Past Hours	Displays the time for which the data is collected.
Dashlet Refresh Intervals (Minutes)	Displays the refresh interval time of a dashlet.

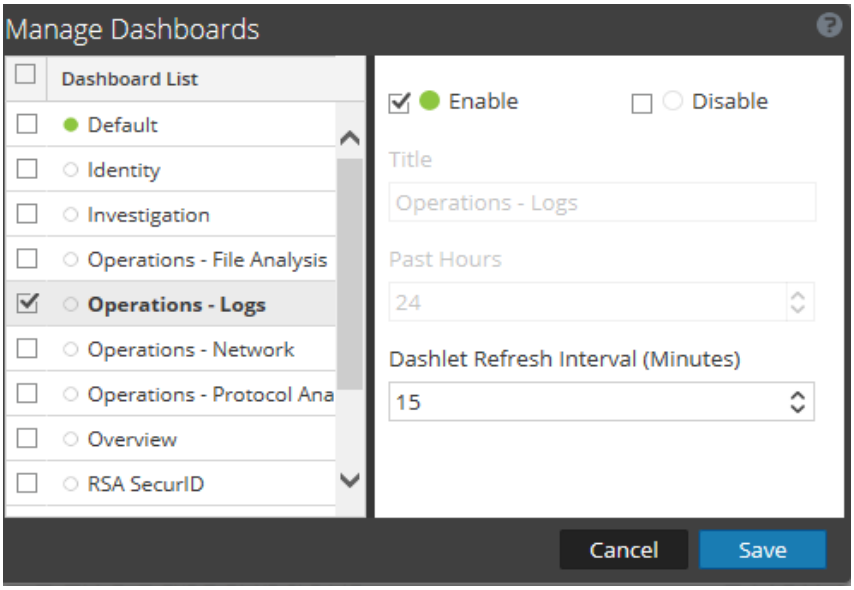
Enabling a Dashboard

If you select a dashboard that is not enabled, a masked screen is displayed.



To enable one or more dashboard(s):

1. Navigate to the dashboard to be enabled.
2. In the dashboard toolbar, click .
3. Select the **Manage Dashboard** option.
   The Manage Dashboards dialog is displayed.



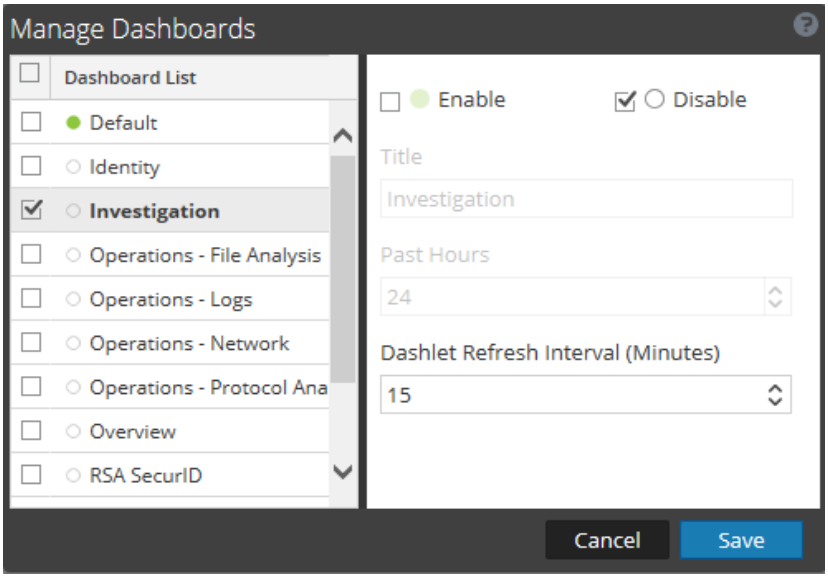
4. From the dashboard list, select the dashboard(s) to be enabled.

5. Click the **Enable** checkbox.
6. Click **Save**.

Disabling a Dashboard

To disable one or more dashboard(s):

1. Navigate to the dashboard to be disabled.
2. In the dashboard toolbar, click .
3. Select the **Manage Dashboard** option.
   The Manage Dashboards dialog is displayed.



4. From the dashboard list, select the dashboard(s) to be disabled.
5. Click the **Disable** checkbox.
6. Click **Save**.

Setting a Dashboard as a Favorite

To customize the views in NetWitness Suite, you can set a preconfigured or custom dashboard as a Favorite. The NetWitness Suite dashboard, as the name suggests, offers all NetWitness Suite dashlets. The Favorite dialog sets a specific dashboard as your favorite dashboard and will be listed as favorite every time you log in to NetWitness Suite.

1. Navigate to any dashboard.
2. In the dashboard toolbar, click

.

If the favorite icon is red in color, it indicates that selected dashboard is set as a Favorite and is listed on top above the line.

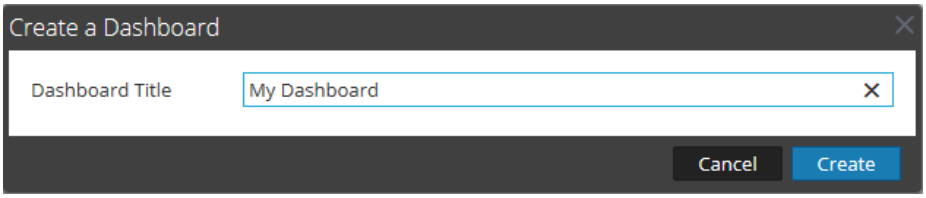
Creating Custom Dashboards

You can create custom dashboards to serve a particular purpose; for example, to represent a specific geographical or functional area of the network. Each custom dashboard is appended to the dashboard selection list.

To create a custom dashboard:

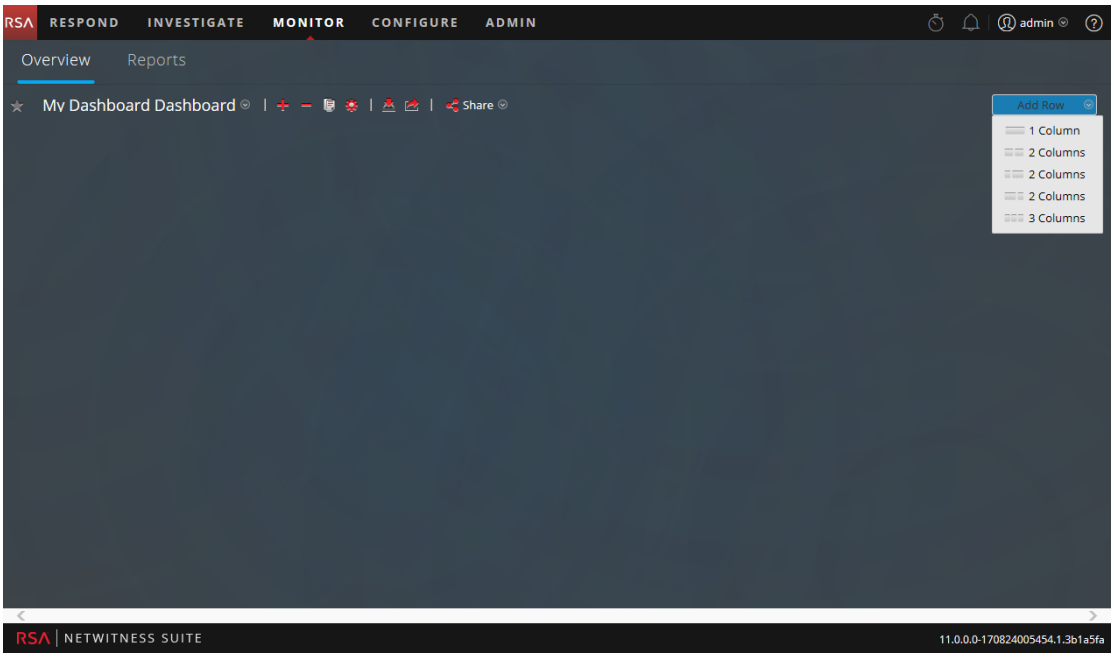
1. In the dashboard toolbar, click .

   The Create a Dashboard dialog is displayed.



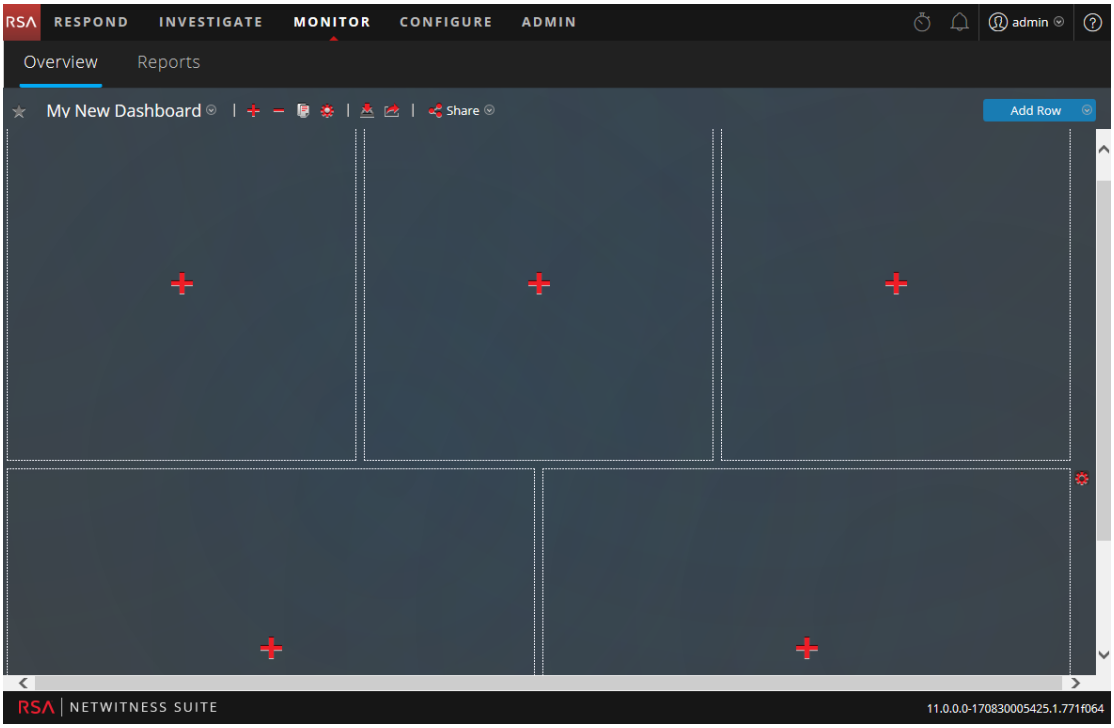
2. Enter a title for the new dashboard and click **Create**.

   The new dashboard is displayed as a blank screen.



3. Add rows to the dashboard, which can contain one or more columns, using the **Add Row** ( ) control on the right side of the screen. Just click on the desired column

configuration in the drop-down list to add one row to the dashboard with the selected number of columns. Repeat the process to add more rows.



4. You can now add any desired dashlets to the dashboard by click the in an empty placeholder in a row. For complete details on adding and managing dashlets, see Working with Dashlets.

Once custom dashboards are created, you can:

- Switch between dashboards by selecting an option from the dashboard selection list
- Delete any custom dashboard
- Import or export a dashboard

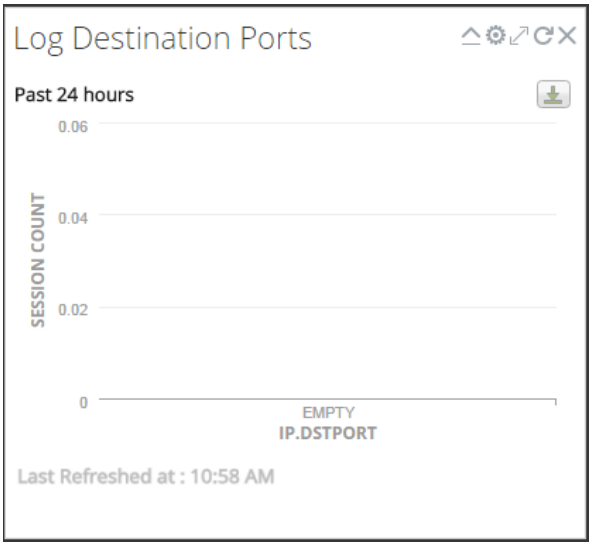
Each dashboard has:

- The dashboard toolbar
- The dashboard title and the dashboard selection list
- Zero or more dashlets

Working with Dashlets

NetWitness Suite uses dashlets to display focused subsets of system information, services, jobs, resources, subscriptions, rules, and other information.

The controls for a dashlet are in the title bar. All dashlets use a common set of controls, and only those that apply to the particular dashlet appear in the title bar of the dashlet.



The following table displays the description of each icon on the dashlet.

Icon	Name	Description
	Collapse vertically	Collapses the dashlet vertically so that only the title is visible.
	Expand vertically	Expands the dashlet to its original size.
	Reload	Reloads the dashlet.
	Settings	Displays configurable settings for the dashlet.
	Maximize	In some dashlets with content that does not fit horizontally within the width of the dashlet, maximizes a chart or a dashlet to full screen.
	Delete	Deletes the dashlet from the dashboard.
Last Refreshed at		Displays the time at which the data is polled from the related chart.

Icon	Name	Description
View More		When clicked, navigates to the corresponding dashboard which is linked to the main dashlet and displays more details. If you have not linked the dashboard to an existing dashlet, this link with not be available on the dashlet. To configure this option, click , and in the Dashboard Link field select a related dashboard view more details of the specific dashlet. **Note:** This feature is only available for the realtime chart dashlet and the preconfigured dashboards in NetWitness Suite 11.0 or later.

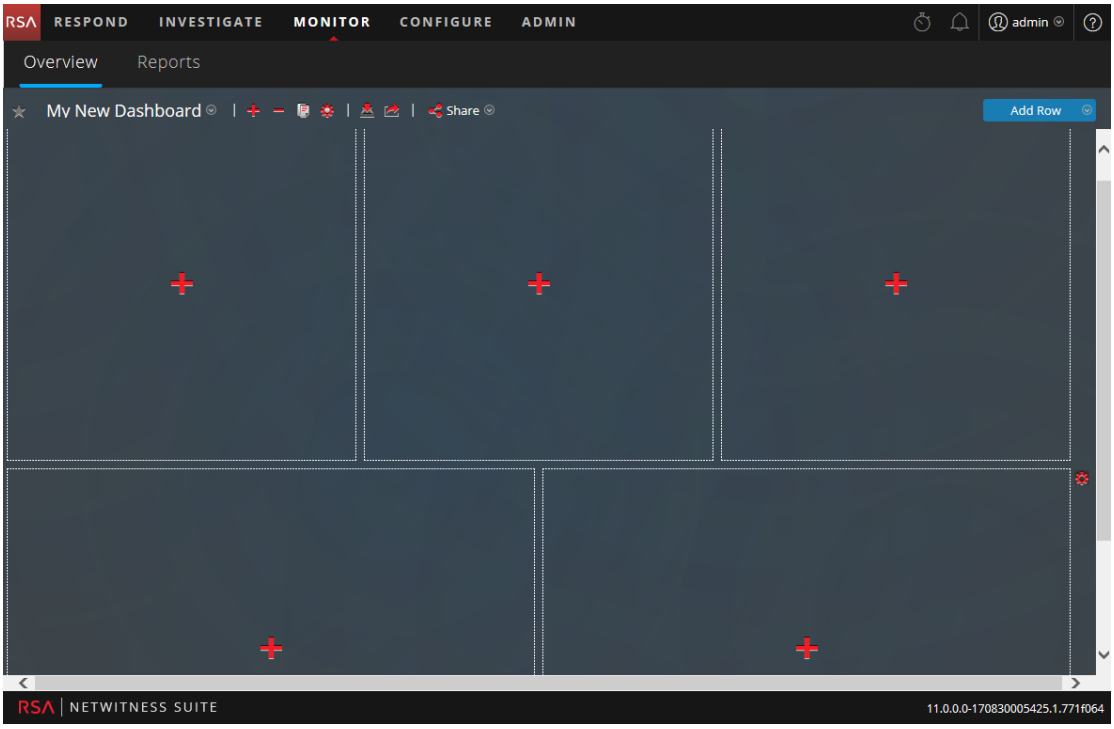
You can add dashlets to the default dashboard or construct a custom dashboard with your own useful set of dashlets to make your workflow more efficient.

Add a Dashlet

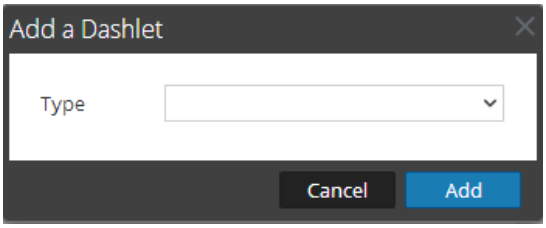
To customize the views in NetWitness Suite, you can add dashlets to a default dashboard or create custom dashboards. However, you cannot add dashlets to preconfigured dashboards.

To add a dashlet:

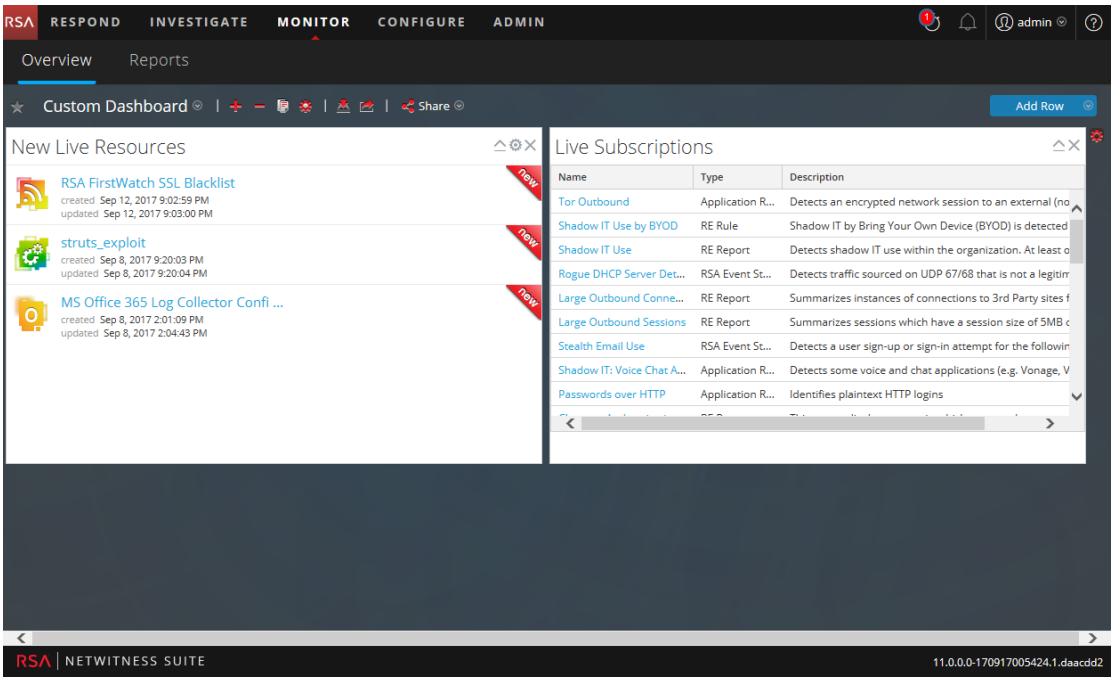
1. Navigate to any dashboard or create a new dashboard.



2. Click on the placeholder where you want to add the dashlet.
   The Add a Dashlet dialog is displayed.



3. Click on the Dashlet **Type** selection list to view the available dashlets, and select the type of dashlet you want to add. Depending on the type of dashlet you are adding, some configurable fields will be displayed in the **Add a Dashlet** dialog.
4. Type a title for the dashlet. The title can include letters, numbers, special characters, and spaces.
5. If there are additional configurable fields for the dashlet, set appropriate values.
6. When all required fields have been configured, click **Add**.
   The dashlet is added to the dashboard in the selected placeholder and is automatically saved.



Edit Dashlet Properties

All preconfigured dashlets are read-only and their properties cannot be edited. Other dashlets are editable and allow users to customize some aspect of the data displayed in the dashlet. A dashlet with editable properties has a settings ( ) option that displays all the editing options.

After the dashlets are added, you can drag and drop them and they can be swapped.

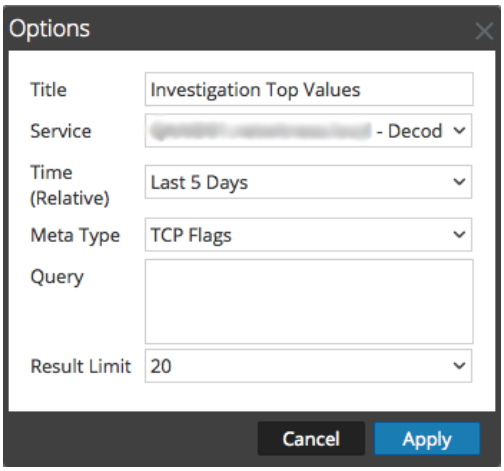
A dashlet without editable properties, such as the Live Subscriptions dashlet, does not display the settings option in the title bar. Many dashlets have an editable title where you can edit the following properties:

- Dashlet display title.
- Type of services to monitor; for example, you can monitor only Decoders, or you can monitor Decoders and Concentrators.

Other dashlets have parameters that you define to specify the kind and amount of information you want to see in the dashlet. For example, a Realtime Chart Dashlet has the settings option.

1. To display and modify the options for a dashlet, click settings ( ) in the dashlet title bar.

   The **Options** dialog is displayed.

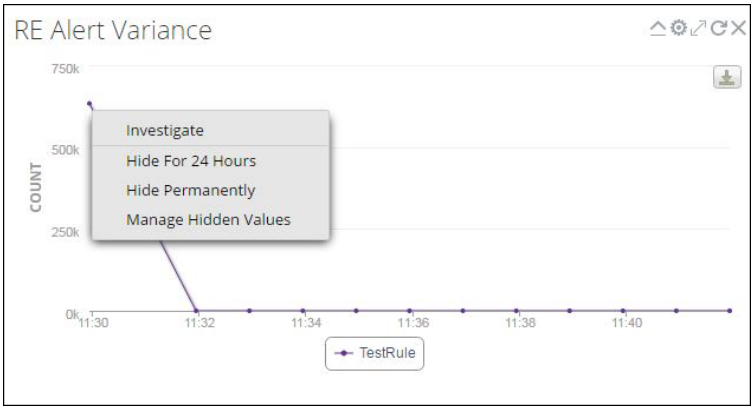


2. Edit any of the displayed properties. For example, in an Investigation Top Values dashlet, you can edit the Result Limit from 20 to 40.
3. Click **Apply**.

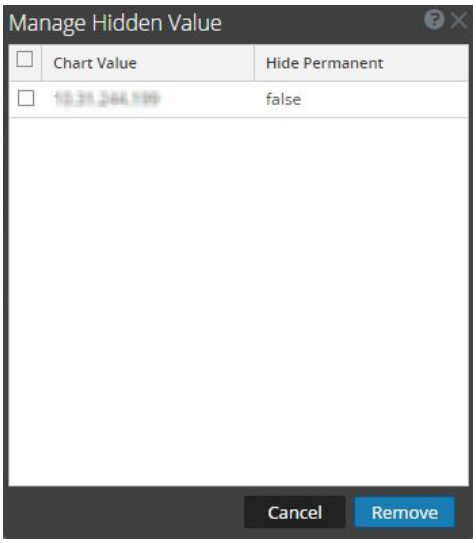
Some dashlets have configuration options to tailor the appearance or the contents of the dashlet. The following options are available for RE Top Alerts, RE Alert Variance, and RE Realtime Charts dashlets on left-click:

- **Hide For 24 Hours**: This option allows you to hide the selected value for the next 24 hours. After 24 hours, the data will automatically be displayed on the dashlet, if the value is configured and listed on top.
- **Hide Permanently**: This option allows you to hide the selected value permanently until you

add it back using the Manage Hidden Values option.



- **Manage Hidden Values**: This option displays a list of all the hidden values. You can select the checkbox for a value and click **Remove** to view the data back on the chart.



Note: The options to Hide for 24 Hours, Hide Permanently, and Manage Hidden Values are not available for Geomap charts.

Note: When you edit a value in a preconfigured dashboard, it is a user-specific change. The changes made to a preconfigured dashboard will be applicable only to your dashboard and cannot be viewed by other users who use the same preconfigured dashboard. For example, if you hide a value in an overview dashboard, the change will be applicable only to your dashboard. If another user views the same overview dashboard, the value will still be displayed. The same applies to a custom dashboard. When you hide a value in the custom dashboard and share the same dashboard with another user, the values will still be displayed even though the dashboard is shared.

For more information on available dashlets, see the Dashboards Catalog in the RSA Content space on RSA Link.

Rearrange a Dashlet

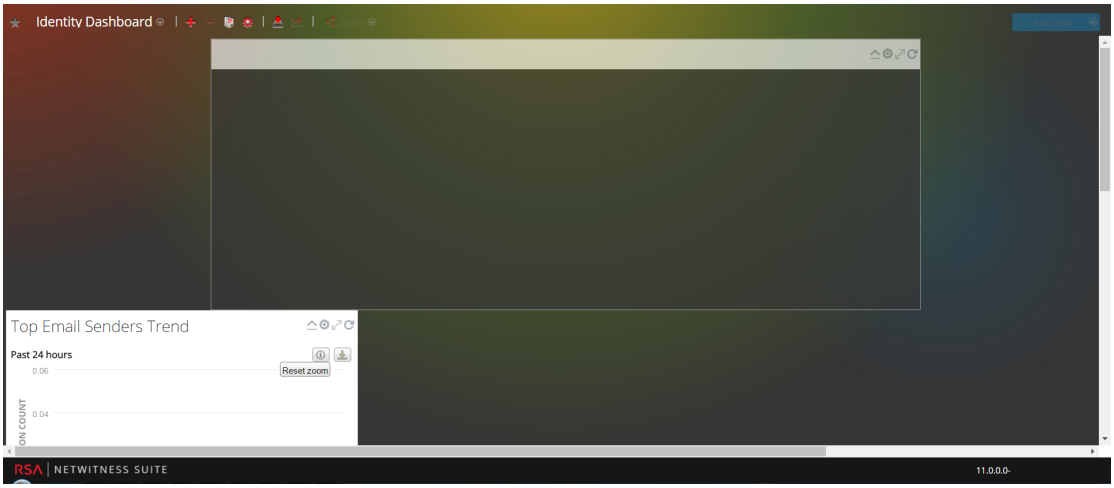
You can arrange dashlets according to your preference by dragging and dropping them into a different order on the dashboard.

1. To move a dashlet, hover in the header of the dashlet that you want to move.

   The directional cursor appears over the dashlet. Click and hold in the header of the dashlet that you want to move.

2. Continue to hold the left mouse button and drag the window toward the new location.

   The figure below shows a dashlet as it is being re-arranged.



3. Release the mouse button when the dashlet is in the desired location.

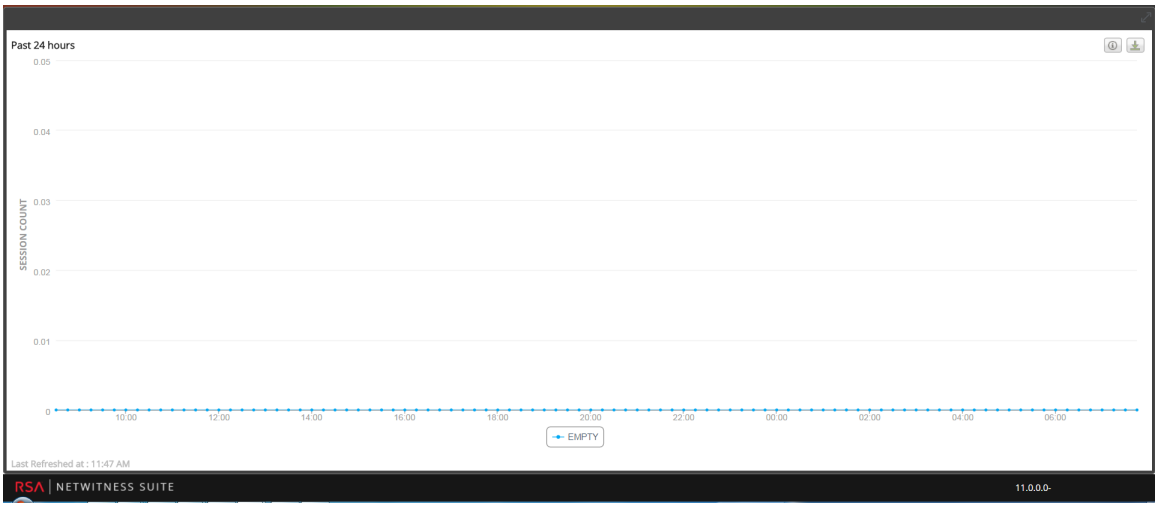
   The dashlet that currently occupies that position moves down.

Maximize a Single Dashlet

This section explains how to open a dashlet on the entire area of the main NetWitness Suitedashboard with the same dashlet title. Dashlets that have a lot of columns or charts, for example some Reporting dashlets, are easier to view when maximized so that the entire contents is visible without scrolling.

To maximize a dashlet, click the maximize control icon in the dashlet title bar: . The dashlet is displayed on full screen.

To minimize a dashlet, click the same control icon in the dashlet title bar: . The dashlet is restored to previous size.



Delete a Dashlet

1. Click ✕ in the dashlet title bar:

   A confirmation pop-up is displayed to confirm if you want to delete the dashlet.

2. Click **Yes**, if you want to delete. The dashlet is removed from the dashboard.

   Click **No**, if you do not want to delete.

Note: After you remove the dashlet, the empty space is replaced by a placeholder where you can add another dashlet using the above Add a Dashlet procedure.

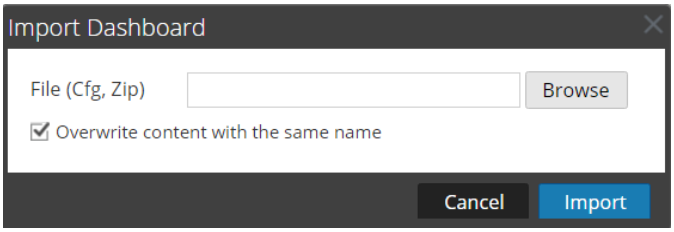
Importing and Exporting Dashboards

The ability to customize dashboards to changing circumstances and conditions could result in a large number of dashboards that are not needed on a daily basis. Rather than reinvent the wheel each time you want to recreate a particular custom dashboard, you can export your dashboards that are not currently in use. When you are ready to use a previously exported dashboard, import the dashboard into NetWitness Suite.

Import a Dashboard

1. In the dashboard toolbar, select **Import Dashboard** .

   The **Import Dashboard** dialog is displayed.



2. Browse to the dashboard file in the **Import Dashboard** dialog. You can import .cfg and .zip files.
3. Click **Import Dashboard**.
   The dashboard is displayed in NetWitness Suite

Note: If you import a dashboard from Security Analytics 10.6. x into NetWitness Suite11.x, the dashboard and the associated rules and charts must be imported separately. But when you import a dashboard from NetWitness Suite11.x into NetWitness Suite, the dashboard and all the rules and charts associated with it, gets imported in .zip format.

Export a Dashboard

Note: When you export a Reporter Realtime dashboard, the corresponding Reporting Engine contents also gets exported

Exported dashboards are designed to work within the same NetWitness Suite instance. It is also possible to share your custom dashboards with other users in your organization, provided they have equivalent permissions.

To export a dashboard, you must have the dashboard open to access the Export Dashboard option under the Edit drop-down menu in the dashboard toolbar.

1. Navigate to the dashboard that you want to export. All existing dashboards appear in the drop-down **Dashboard Selection List** in the currently displayed dashboard.
2. Click Export Dashboard ( ) in the dashboard toolbar.
   The exported file is saved in the .zip format.

Note: The Export feature is not applicable for preconfigured dashboards.

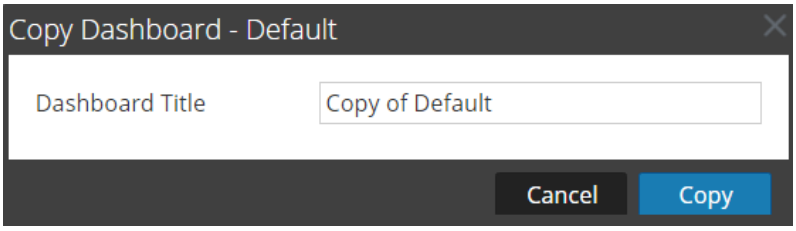
Copying a Dashboard

To customize the views in NetWitness Suite, you can copy dashboards to the NetWitness dashboard or a custom dashboard. The NetWitness Suite dashboard, as the name suggests, offers all NetWitness Suite dashlets. The Copy Dashboard dialog creates a duplicate dashboard, which can be customized. When you copy a dashboard, the default name will be prefixed with Copy of. For example, if the name of the original dashboard is XYZ, the default title of the copied dashboard will be Copy of XYZ.

To copy a dashboard:

1. Navigate to any dashboard
2. In the dashboard toolbar, click .
   The Copy Dashboard - Default dialog is displayed. The following screenshot is an example

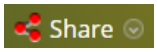
of copying a dashboard.



3. Enter the Dashboard Title.
4. Click **Copy**.

Sharing a Dashboard

In NetWitness Suite, as an Administrator you can share dashboards for viewing purposes with other roles such as Administrators, Analysts, Operators and so on. When you share a dashlet, the users can only view the dashboard, make dashboard as favorite, copy the dashboard, and export the dashboard. In case of other roles such as Analysts, Operators and so on, you can share the dashboard only with similar roles. For example, an analyst will be able to share a dashboard with other analysts only.

1. Navigate to any dashboard.
2. In the dashboard toolbar, click 

and select the checkbox of the role with whom you want to share the dashboard.

Note: If you do not want to share the dashboard, clear the checkbox of the role.

Managing Jobs

Inevitably, there are tasks, on-demand or scheduled, in NetWitness Suite that take a few minutes to be completed. The NetWitness Suite jobs system lets you begin a long-running task and continue using other parts of NetWitness Suite while the job is running. Not only can you monitor the progress of the task, but you can also receive notifications when the task has completed and whether the result was a success or failure.

While you are working in NetWitness Suite, you can open a quick view of your jobs from the NetWitness Suite toolbar. You can look anytime, but when a job status has changed, the Jobs icon ( ) is flagged with the number of running jobs. Once all jobs are completed, that number disappears.

You can also see the jobs in these two views.

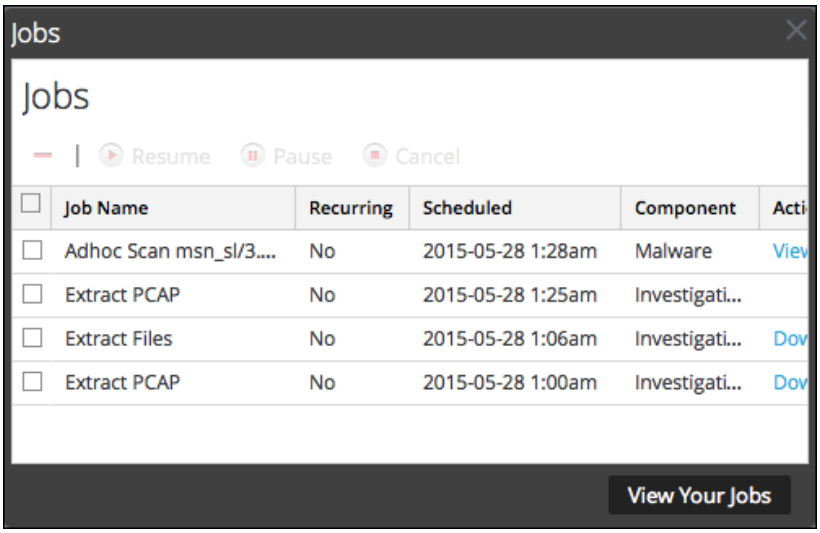
- In the Profile view, you see the same jobs in a full panel. These are only your jobs.
- In the System view, users with administrative privileges can view and manage all jobs for all users in a single jobs panel.

The structure of the jobs panel is the same in all views.

Display the Jobs Tray

In the NetWitness Suite toolbar, click the Jobs icon: .

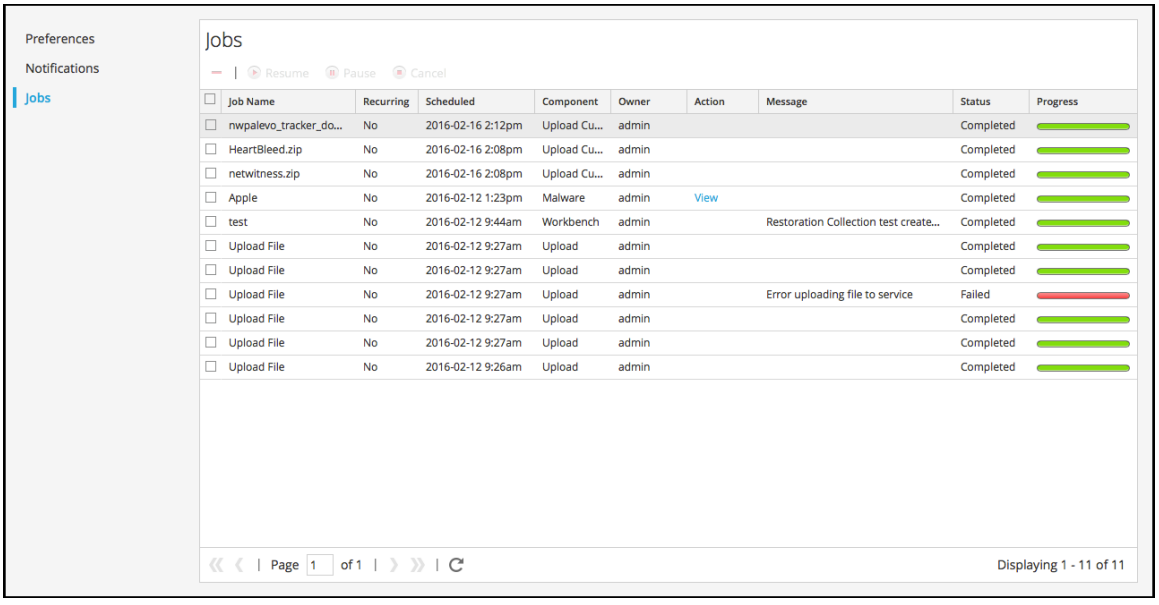
The Jobs Tray is displayed.



The Jobs Tray lists all jobs that you own, recurring and non-recurring, using a subset of the columns available in the Jobs panel. Otherwise the Jobs Tray and the Profile view > Jobs panel are the same. In the Administration System view, the Jobs panel lists information about all NetWitness Suite jobs for all users.

View Your Jobs in the Profile View > Jobs Panel

To see a larger view of your jobs, click **View Your Jobs**.
The Profile view > Jobs panel is displayed.



Pause and Resume Scheduled Execution of a Recurring Job

The Pause and Resume options apply only to recurring jobs. You can pause a recurring job that is running; however, it has no effect on that execution. The next execution (assuming the job is still paused) is skipped.

1. To stop the next execution of a recurring job, in any **Jobs panel**, select the job, and click **Pause**.

   The next execution of the job is skipped, and the schedule is paused until you click Resume.

2. To restart execution of paused recurring jobs, select the job and click **Resume**.

   The next execution of the job occurs as scheduled, and the schedule for the job resumes.

Cancel a Job

To cancel jobs that are executing or in the queue to execute:

1. In the **Jobs Tray** or either **Jobs** panel, select one or more jobs.
2. Click **Cancel**.

   A confirmation dialog is displayed.

3. Click **Yes**.

   The jobs are canceled, and the entries remain in the grid with a status of **canceled**.

   If you cancel a recurring job, it cancels that execution of the job. The next time the job is scheduled to run, it executes normally.

Delete a Job

Caution: When you delete a job, the job is instantly deleted from the grid. No confirmation dialog is offered. If you delete a recurring job, all future executions are removed as well.

Users can delete their own jobs before, during, or after execution. Users with the ADMIN role can delete any job. To delete jobs:

1. Select one or more jobs.
2. Click **Delete**.
3. The jobs are deleted from the grid.

Download a Job

When a job has the Download status in the Action column, you can download the result of the job. If you are working in the Investigation Module and extract the packet data for a session as a PCAP file or extract the payload files (for example, Word documents and images) from a session, a file is created. To download the file to your local system, click **Download**.

Viewing and Deleting Notifications

While you are working in NetWitness Suite, you can view recent system notifications without leaving the module in which you are working. You can open a quick view of notifications from the NetWitness Suite toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged.

Examples of notifications include:

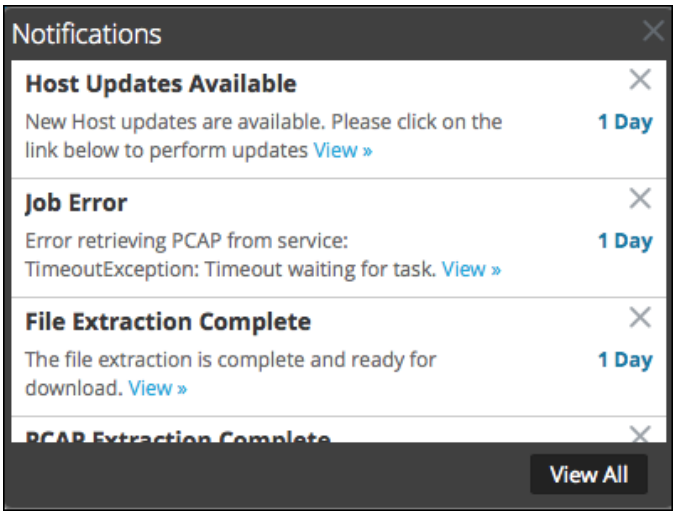
- A host upgrade completed.
- A parser push to decoders completed.
- A newer software version is available.

You can see all notifications in a full Notifications panel in these two views.

- In the Profile view, you see only your notifications.
- In the System view, users with administrative privileges can view and manage all notifications for all users in a single panel.

View Notifications

To display the Notifications tray, click the Notifications icon ( ).

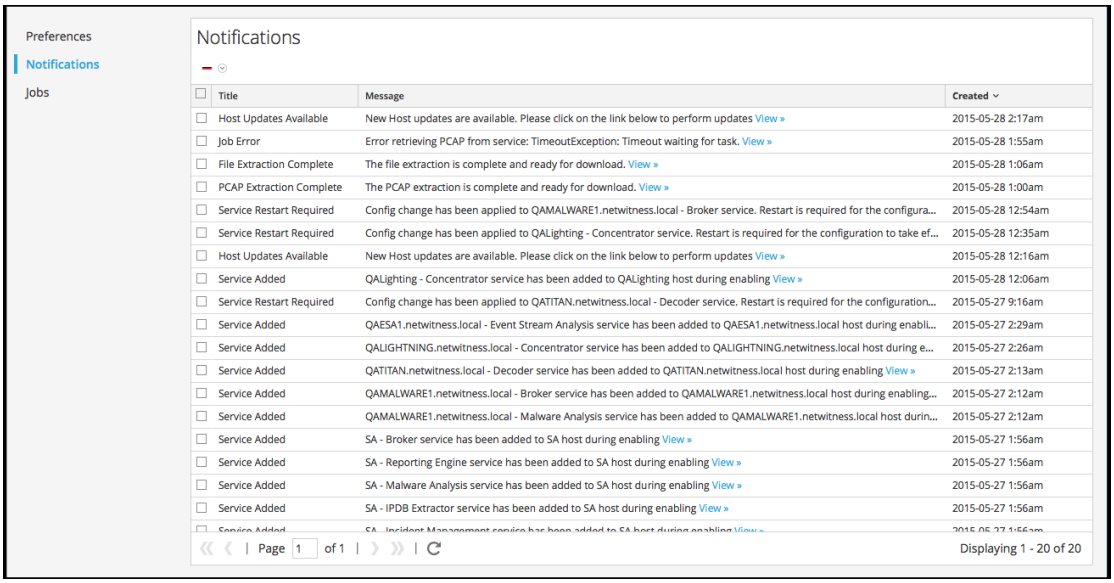


View All Notifications

To view all notifications, do one of the following:

1. Go to **Profile**, then in the options panel of the Profile view, select **Notifications.**
2. Go to **ADMIN > System**, then in the options panel of the System view, select **Notifications**.
3. Click to open the Notifications tray, then click **View All** in the Notifications tray.

   The Notifications panel is displayed. Here all notifications are displayed, and the format is different from the format of the Notifications Tray.



Delete Notification Records

To delete notification records:

1. In the **Profile Notifications** table, select the notifications that you want to delete.
2. Click .

   The selected notifications are deleted from this table and from the Notifications Tray.

Viewing Help in the Application

There are different ways available to get help while using NetWitness Suite.You can use inline help, tooltips, and online help links.

View Inline Help

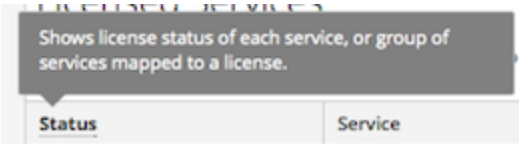
Inline help provides additional information about what to do in sections or fields that you are currently viewing in the NetWitness Suite user interface. To display inline help, hover over . The inline help shows a brief description of the element.

Inline help example:

View Tooltips

Tooltips are a quick way for you to see a description of the text or additional information about an action, field, or parameter. Tooltips appear as underlined text. To display the tooltip and see a brief description of the term, hover over the underlined text.

Tooltip example:

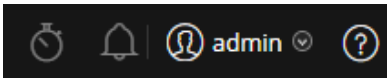


View Online Help

Online help links take you outside of NetWitness Suite to the RSA Link online documentation. This site has a complete documentation set for NetWitness Suite, and the links take you directly to the topic that describes the part of the user interface currently in view.

To view the online help topic for the current location, click in the NetWitness Suite toobar or in a dialog. The relevant help topic is displayed in a separate browser window. The topic describes the features and functions of the current view or dialog. From that topic, you can quickly navigate to the related procedures.

The following figure is an example of the online help icon in the NetWitness Suite toobar.



Finding Documents on RSA Link

The RSA NetWitness® Suite documentation is located on RSA Link, the RSA support portal and community. RSA Link brings all of your RSA resources together in one place. It includes advisories, product documentation, knowledge base articles, downloads, and training. To view a *Guided Tour of RSA Link*, see https://community.rsa.com/videos/21554.

Locate NetWitness Suite Documentation

NetWitness Suite Logs and Packets documentation is at the following link:
https://community.rsa.com/docs/DOC-40370

To navigate to NetWitness Suite Logs and Packets documentation:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **RSA NETWITNESS LOGS AND PACKETS**.

To navigate to NetWitness Endpoint 4.x documentation:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **RSA NETWITNESS ENDPOINT**.

Locate RSA Content

RSA Content is at the following link:
https://community.rsa.com/community/products/netwitness/rsa-content

To navigate to RSA Content:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **RSA CONTENT**.

Locate RSA Supported Event Sources

RSA Supported Event Sources are at the following link:
https://community.rsa.com/community/products/netwitness/parser-network/event-sources

To navigate to RSA Supported Event Sources:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **EVENT SOURCE CONFIGURATION**.

Locate Hardware Setup Guides

The Hardware Setup Guides are at the following link:
https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **HARDWARE SETUP GUIDES**..

Find Documents Using NetWitness Navigator

You can search for desired RSA NetWitness Suite documentation in RSA Link using the NetWitness Navigator tool.

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. Under PRODUCT RESOURCES (right side of page) click **RSA NetWitness Navigator**.
3. Select desired search criteria from the available options. When searching for documentation, you should select **User Documentation** as the Content Type. Also, the Cost option is ignored for user documentation.
4. Click **VIEW RESULTS** to view a list of matching documents.
5. Click **RESET OPTIONS** to clear your previous search options.

Follow Content for Updates

You can follow pages or documents to be notified of changes.

1. Log in to RSA Link.
2. Navigate to a page or a document and in the top right corner select either **Follow** or **Actions** > **Follow**.

Send Your Feedback to RSA

Your feedback is very important to us and helps us to provide a better experience for our customers. Please send your suggestions to sahelpfeedback@rsa.com.

NetWitness Suite Getting Started References

The following section contains user interface reference information related to getting started with the NetWitness Suite application.

- User Preferences
- Notifications Panel and Notifications Tray
- Jobs Panel and Jobs Tray

User Preferences

To adjust NetWitness Suite to best fit your environment and work practices, you can set your own global application preferences. You can:

- Set the application time zone
- Set the date and time formats
- Select your default NetWitness Suite starting location
- Select your default Investigate view
- Choose a dark or light theme for the application
- Change your password
- Enable notifications
- Enable context menus
- Change Investigate preferences - Described in the *NetWitness Investigate User Guide*.

Your global preference options vary depending on whether you access them from the Respond view or other views, such as Investigate, Monitor, Configure, and Admin. There are two global user preferences dialogs accessible from the main menu bar:

- **User Preferences** dialog: Accessible from Respond and the following Investigate views: Event Analysis, Hosts, and Files.
- **Preferences** dialog: Accessible from most other views.

What do you want to do?

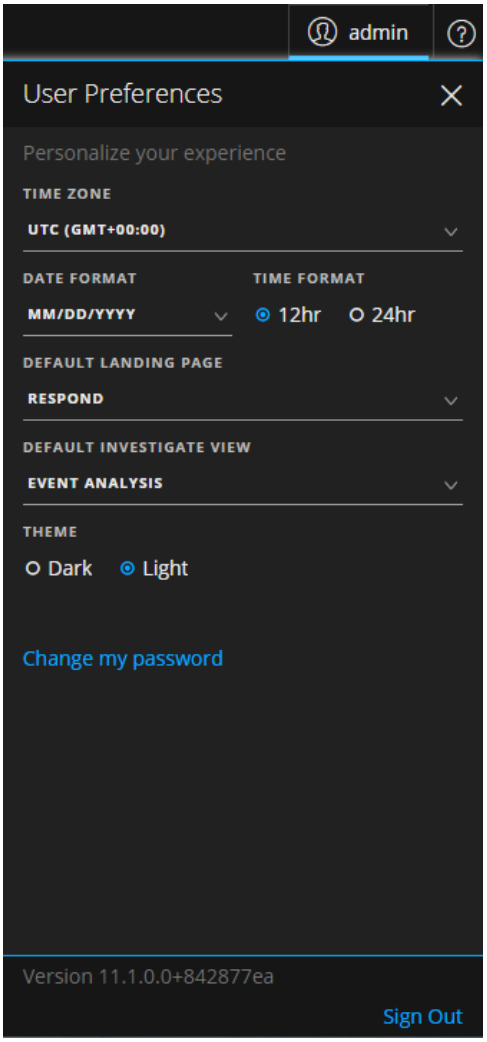
Role	I want to ...	Show me how
All	Change my Password	Change My Password
All	Choose my Default Landing Page	Setting up Your Default View by SOC Role
All	Set my User Preferences	Setting User Preferences

Related Topics

- NetWitness Suite Basic Navigation

User Preferences (Respond and some Investigate views)

To access your user preferences, click .
The User Preferences dialog shows your current preferences and the NetWitness Suite version.



The following table describes the global application preference options that you can access from the User Preferences dialog.

Option	Description
Time Zone	Sets the time zone to use in NetWitness Suite.
Date Format	Sets the format for the order of the display of the month (MM), day (DD), and year (YYYY). For example, the MM/DD/YYYY format shows the date as 05/11/2017.

Option	Description
Time Format	Sets the time as 12-hour or 24-hour time. For example, 2:00 PM in 12-hour time is 14:00 in 24-hour time.
Default Landing Page	Enables you to select the default view when you log in to NetWitness Suite. You can choose Respond, Investigate, Monitor, Configure, and Admin according to your user role. For example, you can choose Respond to go directly to the relevant section of the application for Incident Responders. This selection sets the default view for the entire application.
Default Investigate View	(This option applies to NetWitness Suite 11.1 and later.) Select the default landing page for the Investigate view. You can choose Navigate, Events, Event Analysis, Hosts, Files, or Malware Analysis as the default Investigate view. For example, you can choose Events for the default Investigate view to go directly to the Events page to view the events generated for a service.
Theme	(This option applies to NetWitness Suite 11.1 and later.) Changes the appearance of the Respond view and some Investigate views that you see in the application. You can choose between light and dark themes: • **Dark**: The dark theme is best for darker environments or when you do not need as much contrast. • **Light**: The light theme is best for lighter environments, when you need more contrast, or when you are projecting the application for others to view. Since some views are not affected by the theme changes, you may want to choose the light theme for a more cohesive viewing experience. Your selection only changes how NetWitness Suite appears to you, not other users.
Change my password	Opens the Preferences dialog where you can change your password.
Version	Shows the NetWitness Suite version.
Sign Out	Enables you to log out of NetWitness Suite.

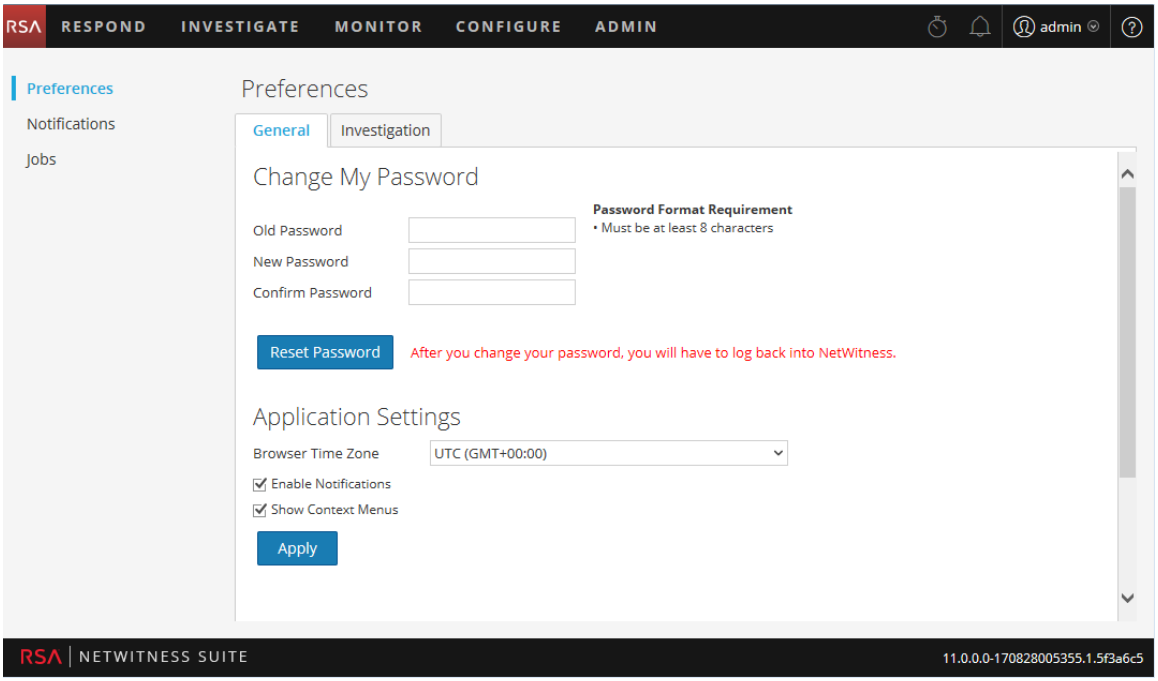
Any selections that you make become effective immediately.

Preferences

To access additional global user preferences, do one of the following:

- For most views, such as Investigate, Monitor, Configure, or Admin, go to > **Profile**.
- In the Respond and some Investigate views (Event Analysis, Hosts, and Files), select and in the User Preferences dialog click **Change my password**.

The Preferences dialog shows your current preferences.



The following tables describe the global application preference options that you can access from the Preferences dialog.

Change My Password

This section enables you to change your password. Your Administrator defines the appropriate password strength requirements for your NetWitness Suite password, such as minimum password length and minimum number of uppercase, lowercase, decimal, non-Latin alphabetic, and special characters. These requirements are then displayed when changing your password.

The following tables describes the options in the Change My Password section.

Option	Description
Old Password	Enter the password that you used to log in to NetWitness Suite.

Option	Description
New Password	Enter the password that you want to use for the next login.
Confirm Password	Retype the new password.
Reset Password	Updates your user profile with the new password. You will be logged out of NetWitness Suite for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Suite. The password change is applied to your system login and to all NetWitness Suite services on which your account has been added.

If you changed your password, you will be logged out of NetWitness Suite for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Suite.

Application Settings

The following tables describes the options in the Application Settings section.

Option	Description
Browser Time Zone	Sets the time zone to use in NetWitness Suite. Your time zone preference is displayed on the toolbar.
Enable Notifications	This checkbox enables and disables notifications for your user account. By default, NetWitness Suite system notifications are enabled when a new user account is created.
Enable Context Menus	This checkbox enables and disables context menus for your user account. By default, context menus are enabled when a new user account is created. Context menus provide additional functions for specific views when you right-click in a view.
Apply	Updates your preferences and applies the changes immediately.

Notifications Panel and Notifications Tray

NetWitness Suite provides system notifications to advise users about certain actions or conditions.

- A host upgrade completed.
- A parser push to decoders completed.
- A service went down (critical log of a certain type).
- A visualization completed.
- A report completed.
- A newer software version is available.

While you are working in NetWitness Suite, you can view recent system notifications without leaving the module in which you are working. You can open a quick view of notifications from the NetWitness Suite toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged.

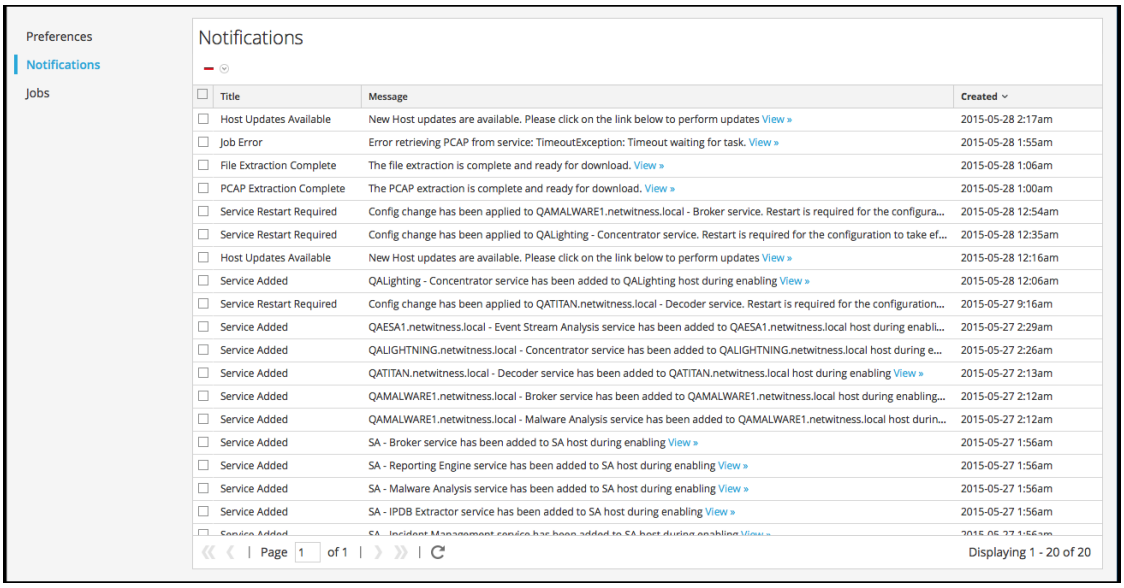
When you are viewing notifications in the Notifications tray, only recent notifications are displayed. You can view all notifications in a table format in the Profile view or in the System view. Procedures for viewing notifications are provided in Viewing and Deleting Notifications.

What do you want to do?

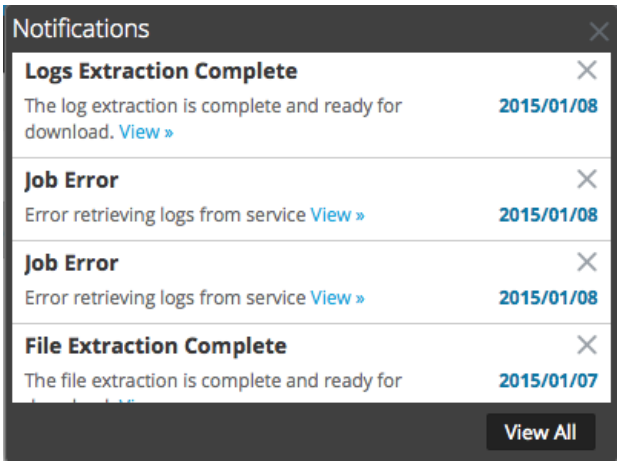
Role	I want to ...	Show me how
All	View all notifications	Viewing and Deleting Notifications
All	Delete notifications	Viewing and Deleting Notifications

To access the Notifications panel, do one of the following:

- Go to **Profile**, then in the options panel of the Profile view, select **Notifications.**
- Go to **ADMIN > System**, then in the options panel of the System view, select **Notifications**.



- Click , then click **View All** in the Notifications tray.



The Notifications panel and tray has a toolbar and a table. The Notification tray is a subset of the information in the Notifications panel. The following table describes the Notifications panel features.

Feature	Description
	Displays a drop-down menu where you can delete the selected notification records or all the notification records in the **Notifications** table and in the Notifications Tray.
Title	The title of the notification, for example, **File Extraction Complete**.
Message	The entire message, for example, **The file extraction is complete and ready for download.**
View	Some messages include a link that displays a view where you can take action. For example, if there is a file to download, clicking this link opens the Jobs panel, the view where you can download the file.
Created	The date and time the notification was created. In the Notifications Tray, this column is the number of days since the notification was created.
View All	Displays the Profile View Notifications table.

Jobs Panel and Jobs Tray

Jobs are started by various NetWitness Suite modules; for example, the Live module can download CMS resources, the Administration module can upload a feed to a service, and the Investigation module can analyze and reconstruct packets in packet capture files.

In the Administration System view, users in the ADMIN group can manage all NetWitness Suite jobs in the Jobs panel. Other non-administrative users can view their own jobs in the Profile view.

In addition, while working in NetWitness Suite, you can open a quick view of your jobs from the NetWitness Suite toolbar. When a job status has changed, the Jobs icon ( ) is flagged with the number of running jobs. Once all jobs are completed, that number disappears.

In the Jobs panel, you can:

- View and sort the jobs
- Pause or resume a job
- Cancel a job
- Delete a job
- Download a job

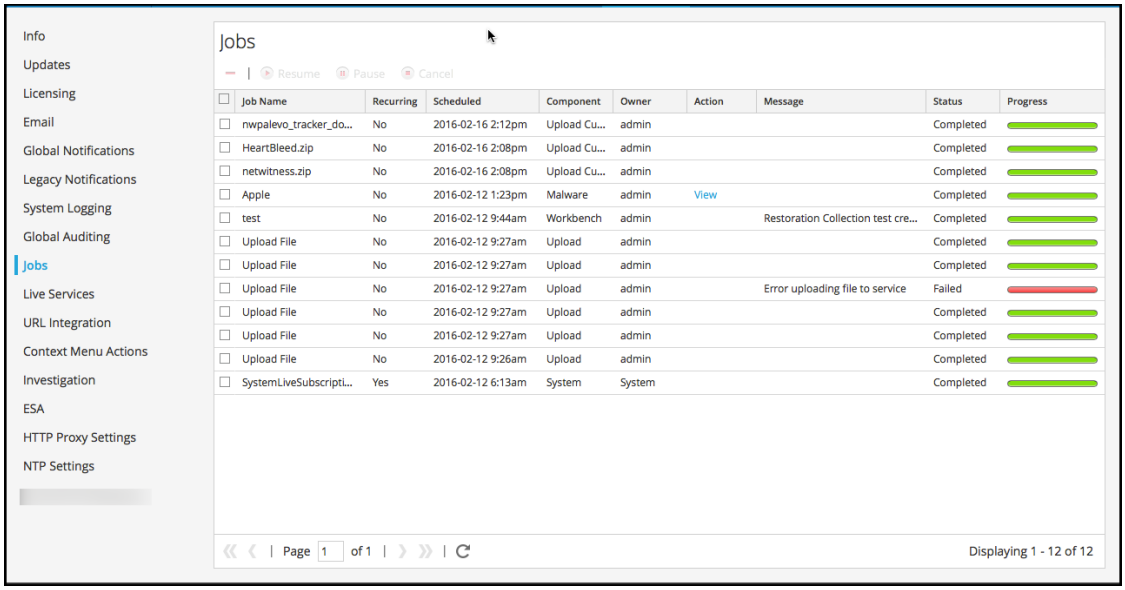
The structure of the jobs panel is the same in all views.

What do you want to do?

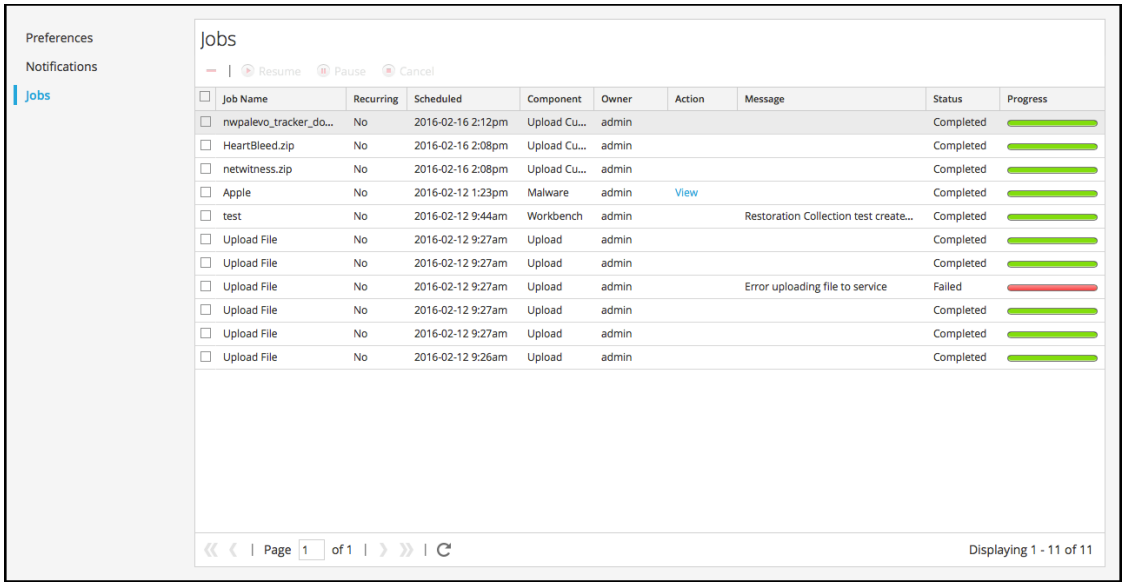
Role	I want to ...	Show me how
All	Pause and Resume a Scheduled Job	Managing Jobs
All	Cancel or Delete a Job	Managing Jobs
	Download a Job	Managing Jobs

To access the Jobs panel, do one of the following:

- Go to **ADMIN > System**, and in the options panel, select **Jobs**.

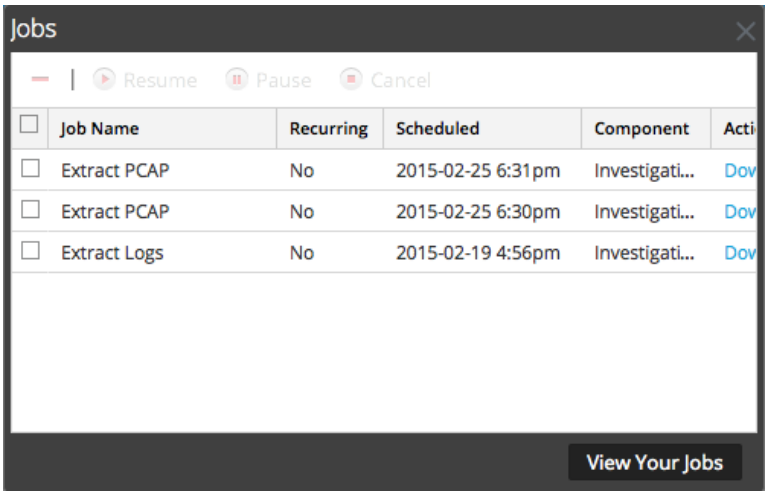


- Go to **Profile**, and in the options panel, select **Jobs**.



The Jobs panel organizes information about jobs into a grid. The columns present a job progress bar, the job name, an indication that the job is recurring or not recurring, the NetWitness Suite module that is controlling the job, the owner of the job, the status, any associated message, and a download button to allow downloading of a job's packet capture files or payload files.

To display the Jobs tray, click the **Jobs** icon .



The Jobs tray lists all jobs that you own, recurring and non-recurring, using a subset of the columns available in the **Jobs** panel. Otherwise the Jobs tray and the Profile View > Jobs panel are the same. In the Administration System view, the Jobs panel lists information about all NetWitness Suite jobs for all users.

The following table describes the options in the Jobs panel.

Feature	Description
Resu	The Resume option applies only to recurring jobs that have been paused. When you resume a paused job, the next execution of the job executes as scheduled.
Paus	The Pause option applies only to recurring jobs. When you pause a recurring job that is running, it has no effect on that execution. The next execution (assuming the job is still paused) is skipped.
Cancel	Cancels a recurring or non-recurring job. You can cancel a job while it is running. If you cancel a recurring job, it cancels that execution of the job. The next time the job is scheduled to run, it executes normally.
	Deletes a recurring or non-recurring job from the **Jobs** panel. When you delete a job, the job is instantly deleted from the Jobs panel. No confirmation dialog is offered. If you delete a recurring job, all future executions are removed as well.

The following table describes the Jobs tray and Jobs panel features.

Feature	Description
Selection box	Click in this box to select one or more jobs.
Progress	Shows the percentage complete for a job.
Job Name	Displays the name of the job; for example, **Extract Files** or **Upgrade Service**.
Recurring	Indicates whether the job is recurring or non-recurring. **Yes** = recurring, **No** = non-recurring.
Component	Indicates the component in which the job originated; for example, **Investigation** or **Administration**.
Owner	Indicates the owner of the job. The owner of the job is not included in the default **Jobs Tray**, because only the current user's jobs are displayed here. The column is available to add.
Status	Indicates the status of the job. Common values for status are **Paused**, **Running**, **Canceled**, **Failed**, **Completed**, and other status values are possible.
Message	Displays additional information about the job; for example, **Extracting files** or **No sessions found.**
Action	Views job in the Investigation Malware Analysis view, or downloads job files for the job to the default **Downloads** directory on the local system. Only successfully completed jobs have the **View** link in the **Action** column. Only jobs that create a file have the **Download** link in the **Action** column.
View Your Jobs	Displays jobs in the **Profile View > Jobs panel.**
Scheduled	Indicates the date and time at which the job was scheduled to begin.

RSA NETWITNESS® SUITE

Planning and Setup Guides

for Version 11.1

RSA NETWITNESS® SUITE

AWS Deployment Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2018

Contents

AWS Deployment Overview 5

AWS Environment Recommendations 5

Abbreviations and Other Terminology Used in this Guide 5

AWS Deployment Scenarios 9

Full NetWitness Suite Stack VPC Visibility 9

Hybrid Deployment - Decoder and Log Decoder 11

Hybrid Deployment - Decoder, Log Decoder, and Concentrator 12

Prerequisites 12

Supported Services 12

AWS Deployment 14

Rules 14

Checklist 14

Establish AWS Environment 15

Find NetWitness Suite AMIs 15

Launch an Instance and Configure a Host 16

Installation Tasks 20

Configure Hosts (Instances) in NetWitness Suite 35

Configure Packet Capture 35

Integrate Gigamon GigaVUE with the Packet Decoder 35

Integrate f5® BIG-IP with the Packet Decoder 37

AWS Instance Configuration Recommendations 40

Archiver 41

Broker 42

Concentrator - Log Stream 43

Packet Stream Solutions 44

Concentrator - Gigamon Solution 44

Concentrator - f5 BIG-IP Solution 44

Decoder - Gigamon Solution 45

Decoder - f5 BIG-IP Solution 45

ESA and Context Hub on Mongo Database 47

Log Collector (Syslog, Netflow, and File Collection Protocols) 48

Log Decoder 49
NetWitness Server, Reporting Engine, Respond and Health & Wellness 50
NetWitness Endpoint Hybrid 51

AWS Deployment Overview

Before you can deploy RSA NetWitness® Suite in the Amazon Web Services (AWS) you need to:

- Understand the requirements of your enterprise.
- Know the scope of a NetWitness Suite deployment.

When you are ready to begin deployment:

- Make sure that you have a NetWitness Suite "Throughput" license.
- For packet capture in AWS, you can purchase either of the following Third-Party solutions. If you engage one of these third-parties, they will assign an account representative and a professional services engineer to you who will work closely with RSA Support.
  - Gigamon® GigVUE
  - f5BIG-IP

AWS Environment Recommendations

AWS instances have the same functionality as the NetWitness Suite hardware hosts. RSA recommends that you perform the following tasks when you set up your AWS environment.

- Based on the resource requirements of the different components, follow best practices to use the system and dedicated storage Elastic Block Store (EBS) Volumes appropriately.
- Make sure that compute capacity provides a write speed of 10% greater than the required sustained capture and ingest rate for the deployment.
- Build Concentrator directory for index database on the Provisioned IOPS SSD.

Abbreviations and Other Terminology Used in this Guide

Abbreviations	Description
AMI	Amazon Machine Image
AWS	Amazon Web Services
BYOL	Bring your own licensing

Abbreviations	Description
CPU	Central Processing Unit
Dedicated Instance	AWS Dedicated Instances run in a VPC on hardware that is dedicated to a single customer. Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances may share hardware with other instances from the same AWS account that are not Dedicated instances. Refer to the AWS "Amazon EC2 Dedicated Instance" documentation (https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/) for more information on dedicated instances.
EBS Optimization	An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance. For more information on EBS-optimized instances, see the AWS "Amazon EBS–Optimized Instances" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html).
EBS Volume	Elastic Block Store (EBS) volume is a highly available and reliable storage volume that you can attach to any running instance that is in the same Availability Zone. For more information on EBS Volumes, see the AWS "Amazon EBS Volumes" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html) .
EC2 instance	Virtual server in AWS Elastic Compute Cloud (EC2) for running applications on the AWS infrastructure. See also **Instance**.

Abbreviations	Description
Enhanced Networking Enabled	Enhanced networking provides higher bandwidth, higher packet-per-second performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the virtual machine network interface (VIF) driver. For more information on enhanced networking, see the AWS "How do I enable and configure enhanced networking on my EC2 instances" documentation (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/).
EPS	Events Per Second
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigbit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
HDD	Hard Disk Drive
Instance	A virtual host in the AWS (that is, virtual machine or server in the AWS infrastructure on which you run services or applications). See also **EC2 Instance**.
Instance Type	Specifies the required CPU and RAM for an instance. For more information on the instance types, see the AWS "Amazon EC2 Instance Types" documentation (https://aws.amazon.com/ec2/instance-types/).
IOPS	Input/Output Operations Per Second

Abbreviations	Description
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
On-Premise	On-premise hosts are installed and run on computers on the premises (in the building) of the organization using the hosts, rather than in the AWS.
PPS	Packets Per Second
RAM	Random Access Memory (also known as memory)
Security Group	Set of firewall rules. For more information, see the "Network Architecture and Ports" documentation on RSA Link (https://community.rsa.com/docs/) for a comprehensive list of the ports you must set up for all NetWitness Suite components.
SSD	Solid-State Drive
Tag	A meaningful identifier for AWS instance.
Tap Vendor	Network Tapping Vendor
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
VM	Virtual Machine
VPC	Virtual Public Cloud
vRAM	Virtual Random Access Memory (also known as virtual memory)

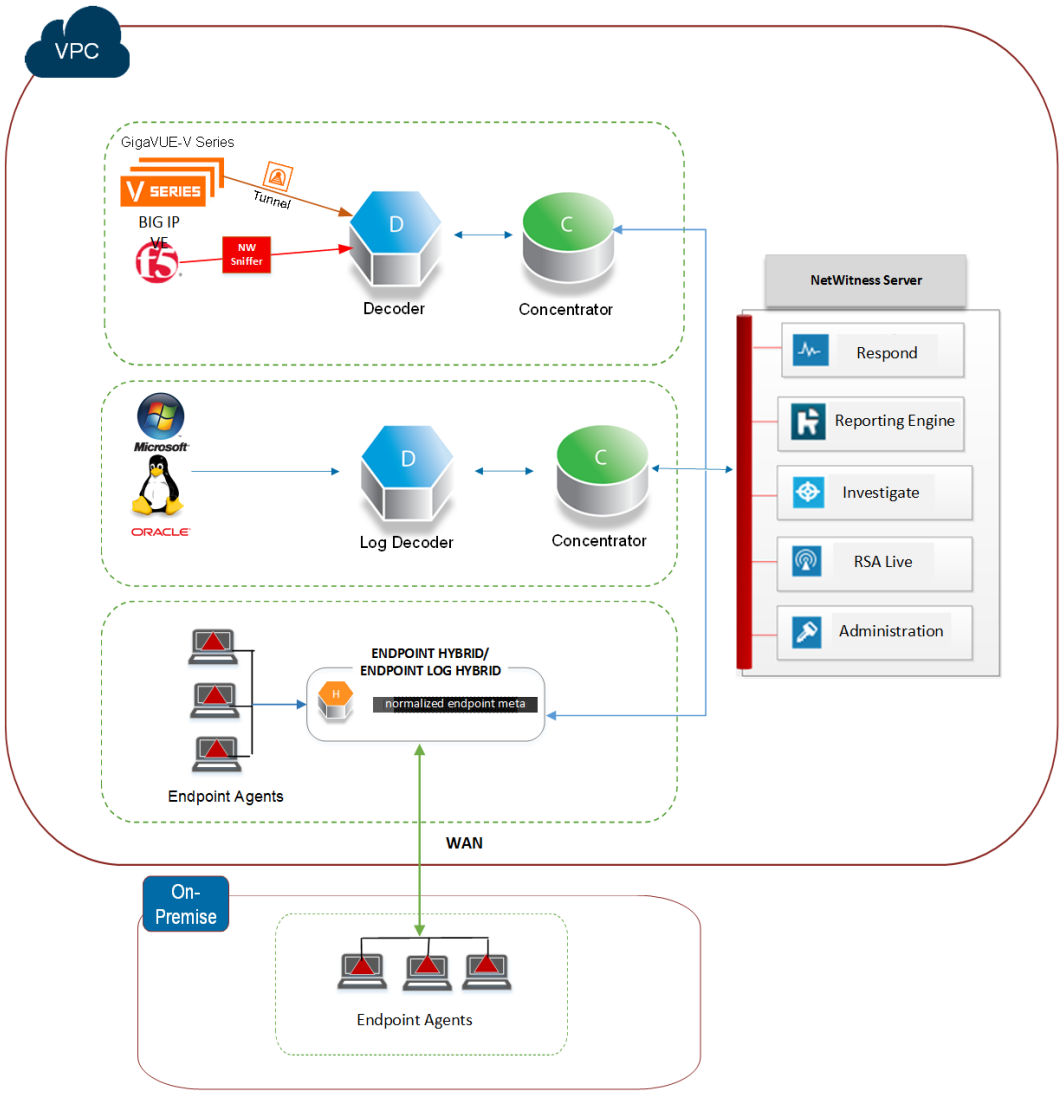
AWS Deployment Scenarios

The following diagrams illustrate some common AWS deployment scenarios. In the diagrams, the:

- **GigaVUE Series** (Gigamon® Solution) is an agent-based solution that uses **Tunneling** (implemented by the NetWitness Suite administrator) to facilitate packet data capture in AWS.
- **BIG-IP** (f5® Solution) is a load balancing solution that uses a Packet Decoder acting as a sniffer (customized by the NetWitness Suite administrator) to facilitate packet capture in AWS.
- **Decoder** collects packet data. The **Decoder** captures, parses, and reconstructs all network traffic from Layers 2 – 7.
- **Log Decoder** collects logs. The **Log Decoder** collects log events from hundreds of devices and event sources.
- **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while facilitating reporting and alerting.
- **Endpoint Hybrid** - collects endpoint data. The Endpoint Hybrid comprises of Endpoint Server, Log Decoder, and Concentrator. For more information, see *NetWitness Endpoint Insights Configuration Guide*.
- NetWitness Server hosts **Respond**, **Reporting**, **Investigate**, **Live Content Management**, **Administration** and other aspects of the user interface.

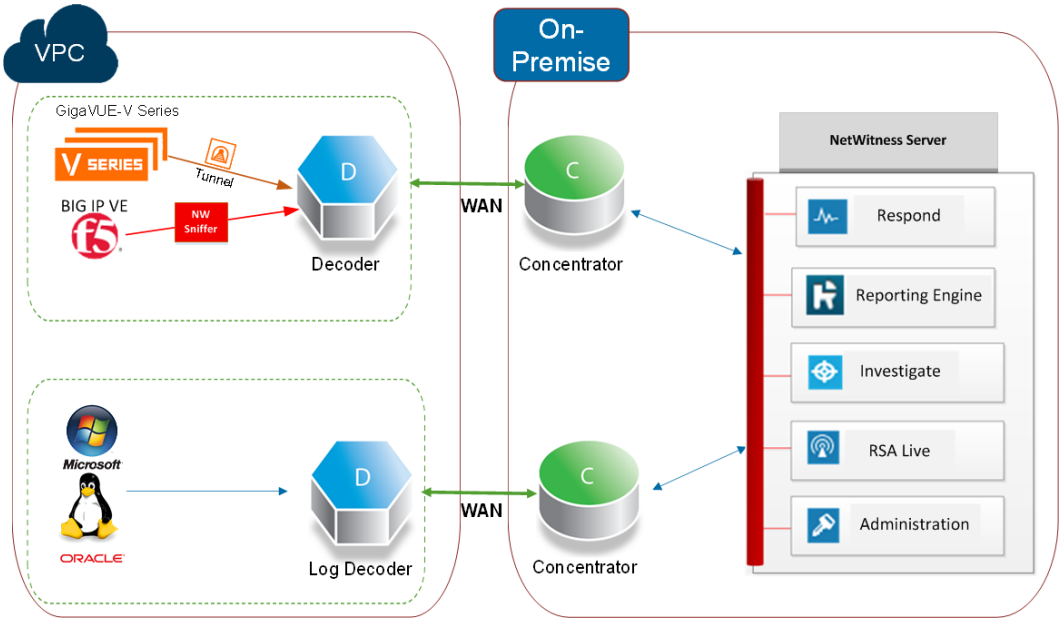
Full NetWitness Suite Stack VPC Visibility

This diagram shows all NetWitness Suite components (full stack) deployed in AWS.


VPC
GigaVUE-V Series
V SERIES
BIG IP
VE
Tunnel
NW Sniffer
D
Decoder
C
Concentrator
NetWitness Server
Respond
Reporting Engine
Investigate
RSA Live
Administration
Microsoft
ORACLE
D
Log Decoder
C
Concentrator
ENDPOINT HYBRID/
ENDPOINT LOG HYBRID
H
normalized endpoint meta
Endpoint Agents
WAN
On-Premise
Endpoint Agents

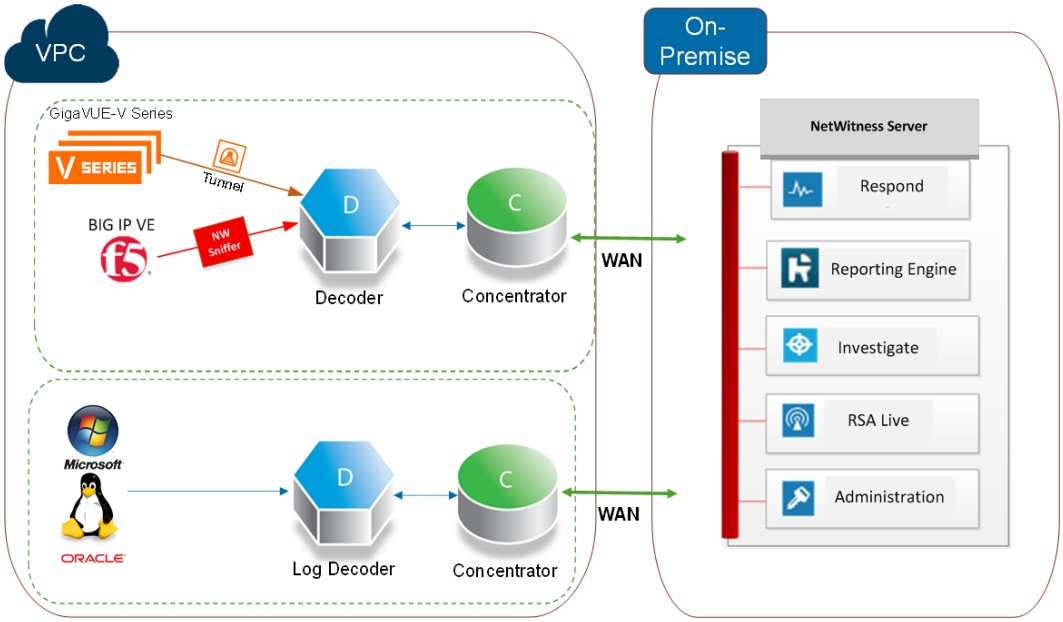
Hybrid Deployment - Decoder and Log Decoder

This diagram shows the Decoder, and Log Decoder deployed in AWS with all other NetWitness Suite components deployed on your premises.



Hybrid Deployment - Decoder, Log Decoder, and Concentrator

This diagram shows the Decoder, Log Decoder, and the Concentrator deployed in AWS with all other NetWitness Suite components deployed on your premises.



Prerequisites

You need the following items before you begin the integration process:

- Access to AWS console
- Network rout-able (and proper AWS Security Groups) for the containers to transfer data to the NetWitness Suite Decoder.

Supported Services

RSA provides the following NetWitness Suite services.

- NetWitness Server
- Archiver
- Broker
- Concentrator
- Event Stream Analysis

- Log Decoder
- Decoder
- Remote Log Collector
- Endpoint Server

AWS Deployment

This topic contains the rules and high-level tasks you must follow to deploy RSA NetWitness® Suite components in the AWS.

Rules

You must adhere to the following rules when deploying NetWitness Suite in AWS.

- SSH to the NetWitness Suite instance at least once after deployment to initialize the system.
- Before you enable the out-of-the-box (OOTB) dashboards, set the default data source in Reporting Engine configuration page.
- If you reboot the Packet Decoder instance, the tunnel is not retained. Create the tunnel on Packet Decoder again and restart the decoder service.
- Always use private IP addresses when you provision AWS NetWitness Suite instances.

Note: If you assign a public IP to the Netwitness Server Host, update the /etc/nginx/conf.d/nginx.conf configuration file as follows:

```
location /nwrpmrepo
{
alias /var/lib/netwitness/common/repo;
index index.html index.htm;
allow <Subnet-Gateway>/Subnet mask ;
#example
# allow 10.0.0.1/25;
deny all;
autoindex on;
}
```

Checklist

Step	Description	√
1	Establish AWS Environment	
2	Find NetWitness Suite AMIs	
3	Launch an Instance and Configure a Host	
4	Configure Hosts (Instances) in NetWitness Suite	

Step	Description	√
5	Configure Packet Capture	

Establish AWS Environment

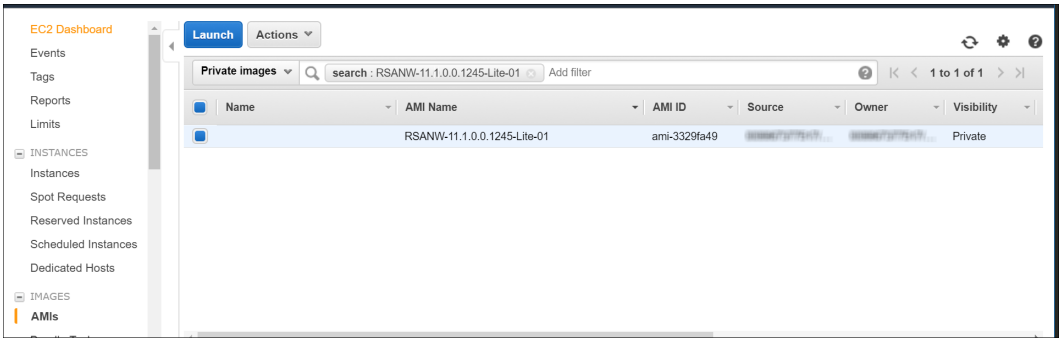
1. Make sure that you have an AWS environment with the capacity to meet or exceed the NetWitness Suite performance guidelines described in AWS Instance Configuration Recommendations.
2. Go to Find NetWitness Suite AMIs.

Find NetWitness Suite AMIs

Search for NW- AMI files within the Public/Shared/Community repository. Use "RSANW" for a key word to search for the AMI files.

Note: Refer to the AWS **Finding Shared AMIs** documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html) for additional instructions.

1. Open the Amazon EC2 console (New Subscriber Account) at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose AMIs.
3. In the first filter, choose Public images.
4. Type "RSANW" in the search field to find the NetWitness Suite AMIs.



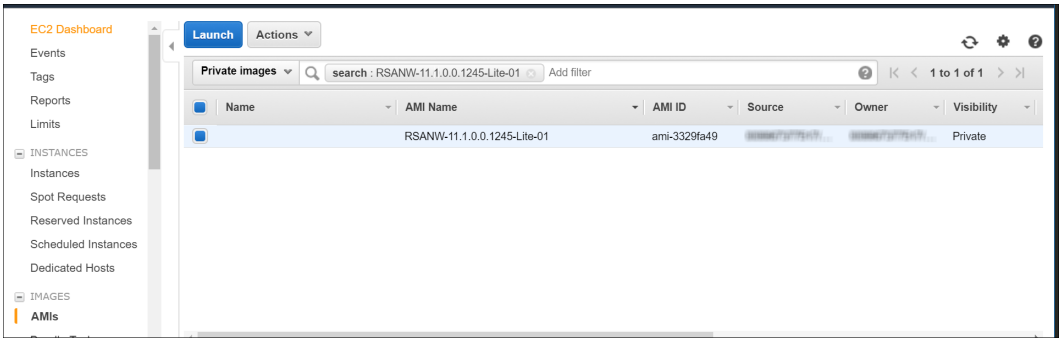
Note: Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) to obtain access to the **RSANW-11.1.0.0.1245-Full-01**.

5. Go to Launch an Instance and Configure a Host.

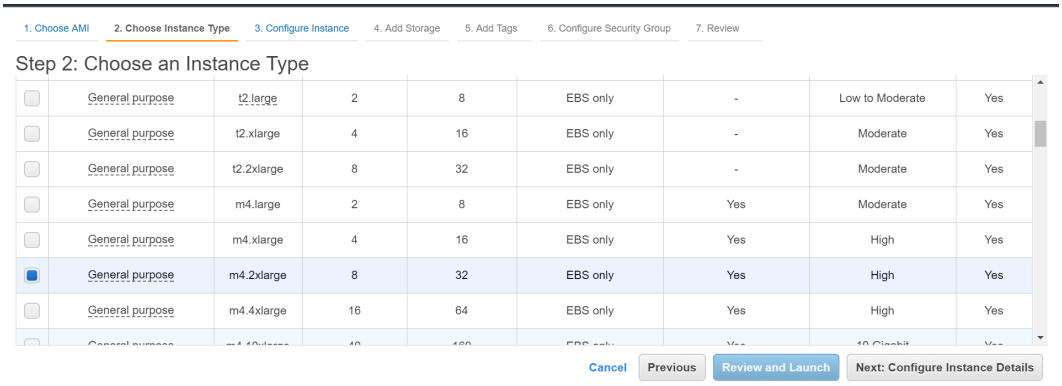
Launch an Instance and Configure a Host

Note: Refer to the AWS "Launching an Instance" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html) for additional instructions.

1. Select an instance from the grid (for example, **RSA-NW-Concentrator-11.1.0.0-01**) and click **Launch**.



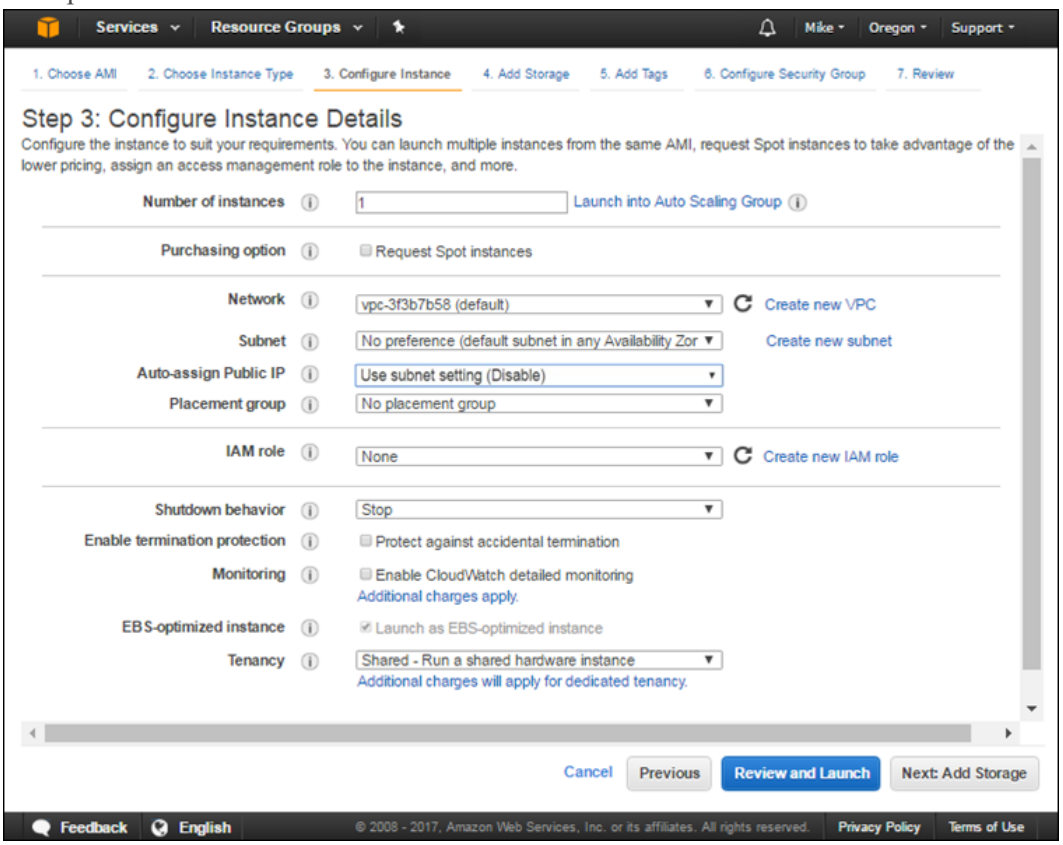
2. Choose the RAM and CPUs by selecting instance type.
   Refer to AWS Instance Configuration Recommendations for guidelines on how to configure the EC2 Instance based on the requirements of the NetWitness Suite component (that is, service) for which you are launching an instance. The following example has the **m4.2xlarge** instance type selected with **8** CPUs and **32** GB of RAM.



3. Click **Next: Configure Instance Details** at the bottom right of the **Step 2: Choose an Instance Type** page.

   The **Step 3. Configure Instance Details** page is displayed.

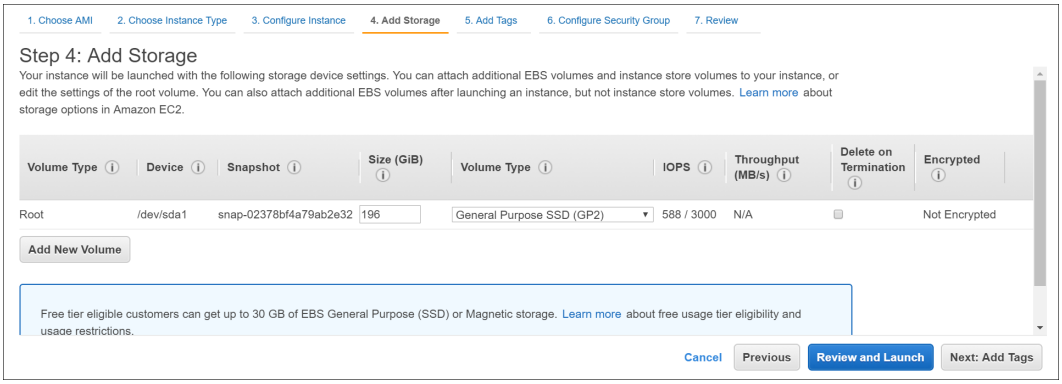
   For NetWitness Suite, the subnet and VPC are defaulted to the values in the following example.



4. Click **Next: Add Storage** at the bottom right of the **Step 3: Configure Instance Details** page.

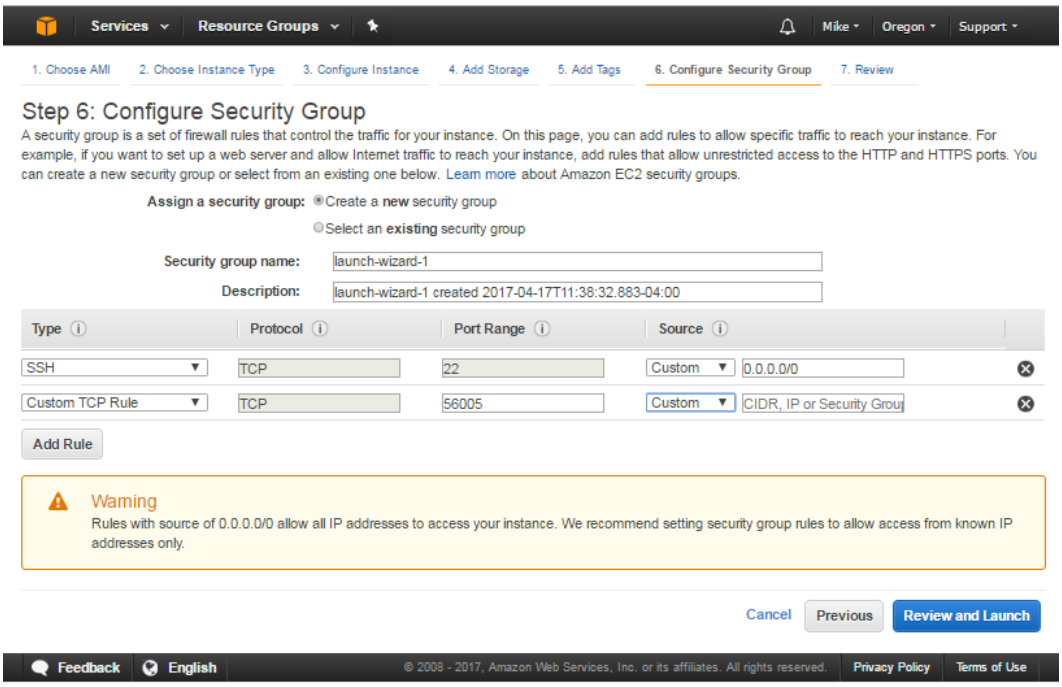
   The **Step 4. Add Storage** page is displayed.

Refer to AWS Instance Configuration Recommendations for guidelines on how to configure storage based on based on the requirements of the NetWitness Suite component (that is, service) for which you are launching an instance.



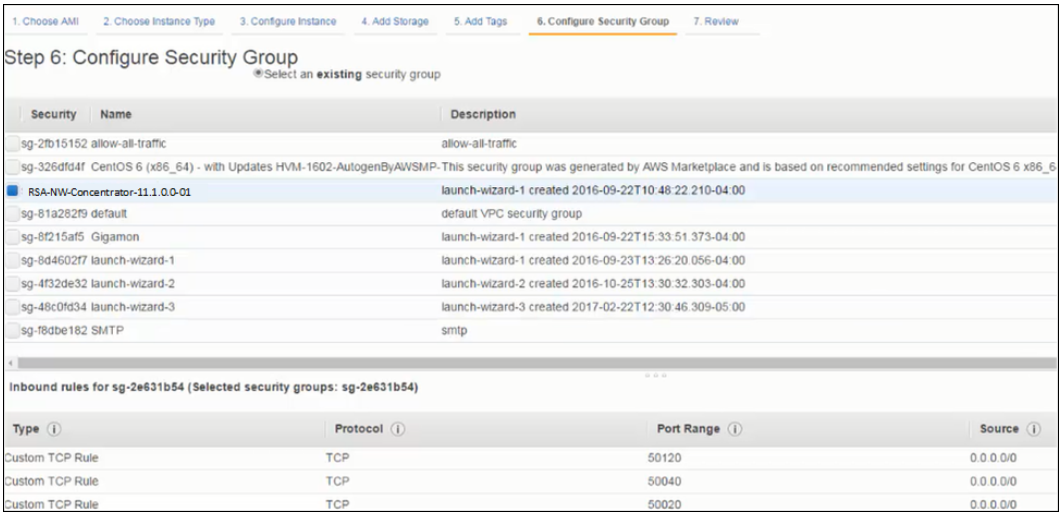
5. Click **Next: Add Tags** at the bottom right of the **Step 4: Add Storage** page.
   The **Step 5. Add Tags** page is displayed. Enter the name of your Instance.
6. Click **Next: Configure Security Group** at the bottom right of the **Step 5: Add Tags** page.
   The **Step 6. Configure Security Group** page is displayed.
   a. Select the "Create a **new** security group" radio button.
   b. Create a rule that opens all the firewall for the NetWitness Suite component.
      You must configure the security group correctly to configure the instance (host) from the NetWitness Suite) User Interface and SSH to it.

      Note: See the "Network Architecture and Ports" documentation in RSA Link (https://community.rsa.com/docs/DOC-83050) for a comprehensive list of the ports you must set up for all NetWitness Suite components..



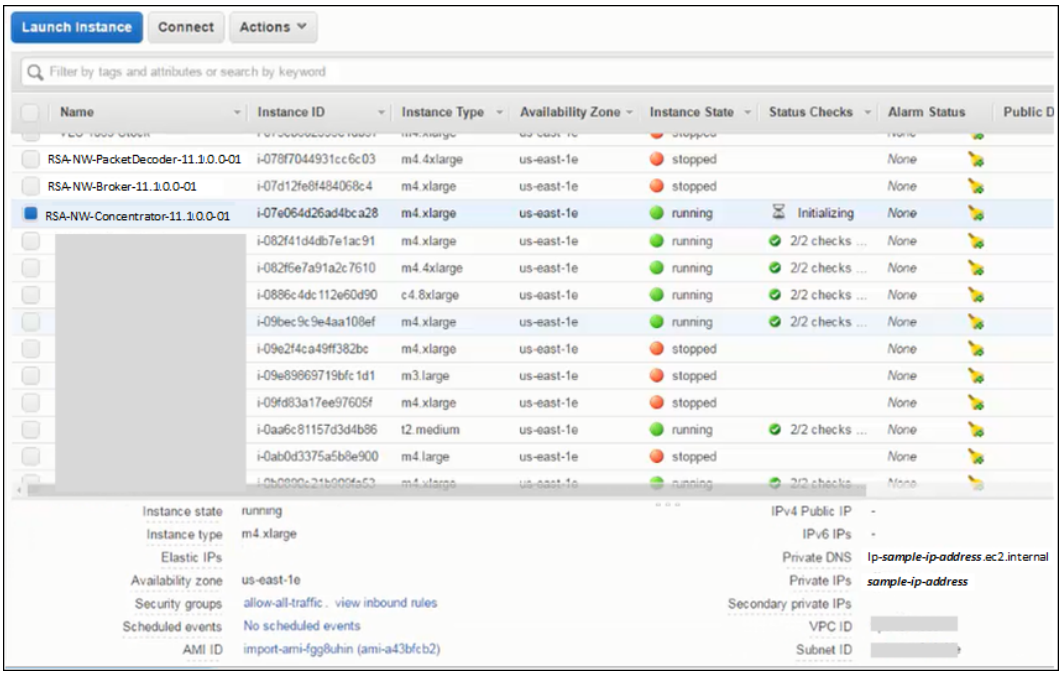
Note: After you configure a Security Group, you can change it at any time.

7. Click **Review and Launch** at the bottom right of the **Step 6: Configure Security Group** page.
   The **Step 7. Review Instance Launch** page is displayed.
8. Click **Launch** at the bottom right of the **Step 7. Review Instance Launch** page.
   The **Select an existing key pair or create a new key pair** dialog is displayed.
9. Choose **Proceed without key pair**.
10. Click **Launch Instance**.
    AWS displays the following information as it builds the Instance.



11. Click **View Instances**.
12. Select **Instances** in the left navigation panel to review all instances that AWS is initializing (for example, the **NW-Concentrator**) .

The IP Address for the new **RSA-NW-Concentrator-11.1.0.0-01** host is ***sample-ip-address***.



13. SSH to newly-created instance using the default NetWitness Suite credentials.
14. Go to Configure Hosts (Instances) in NetWitness Suite.

Installation Tasks

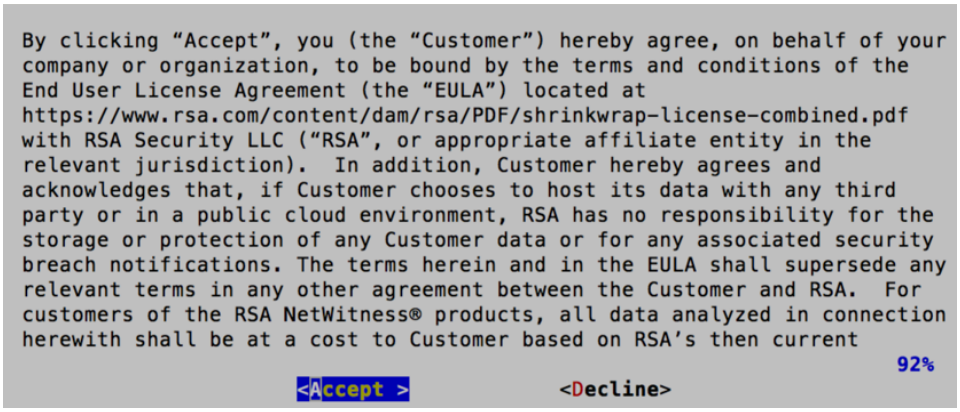
Task 1 - Install 11.1.0.0 on the NetWitness Server (NW Server) Host

Note: You can perform this task for RSANW-11.1.0.0.1245-Full-01 instance.

1. Run the `nwsetup-tui` command to set up the host.

This initiates the Setup program and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console you use access the host.
3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see the "Post Installation Tasks" topic in the *Physical Host Installation Guide*.
If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

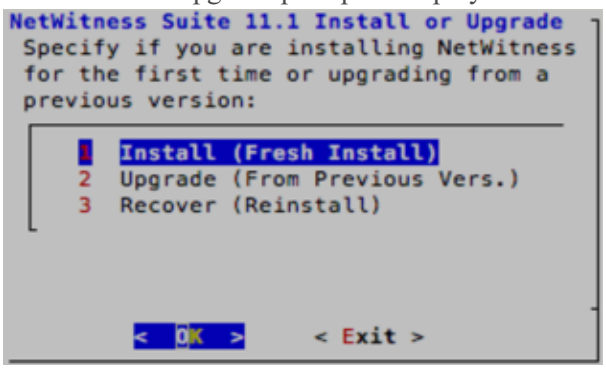


2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

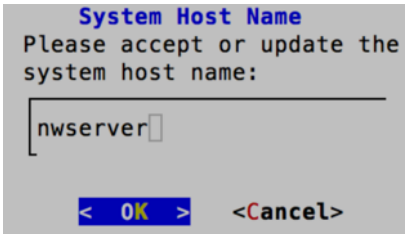
3. Tab to **Yes** and press **Enter**.
   Choose **No** if you already installed 11.1.0.0 on the NW Server.

   Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

The Install or Upgrade prompt is displayed.



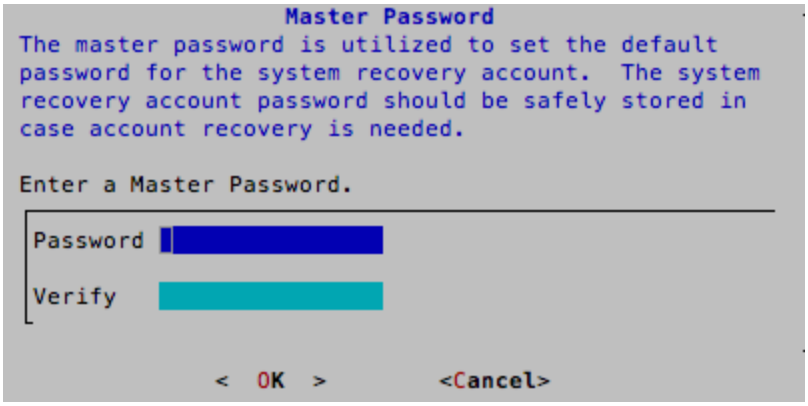
4. Press **Enter** (Install is selected by default).
   The "Host Name" prompt is displayed.



5. Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.
   The "Master Password prompt" is displayed.
   The following list of characters are supported for Master Password and Deployment Password:

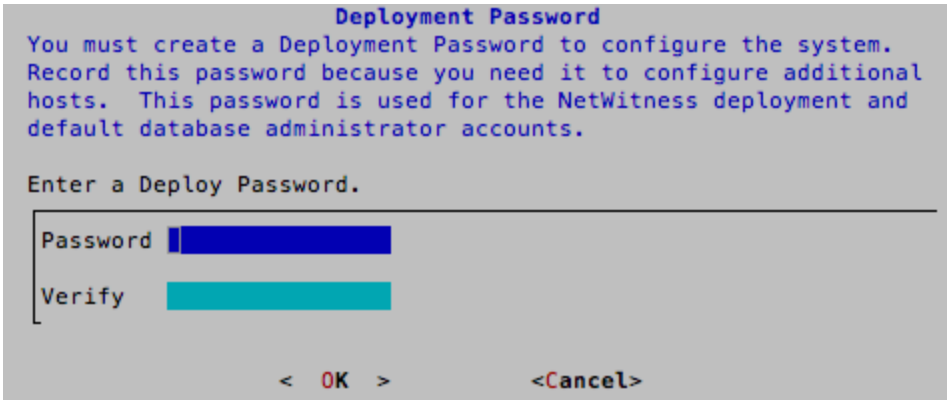
   - Symbols : ! @ # % ^ + ,
   - Numbers :0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z
     No ambiguous characters are supported for Master Password and Deployment Password

(for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -.



6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

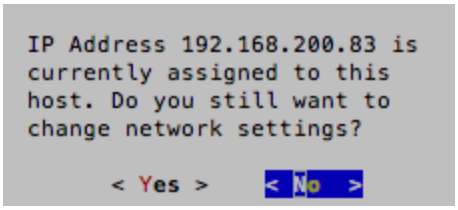
   The "Deployment Password" prompt is displayed.



7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   If:

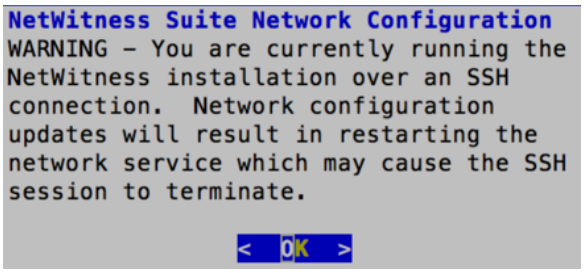
- The Setup program finds a valid IP address for this host, the following prompt is displayed.



  Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** if you want to change the IP configuration found on the host.

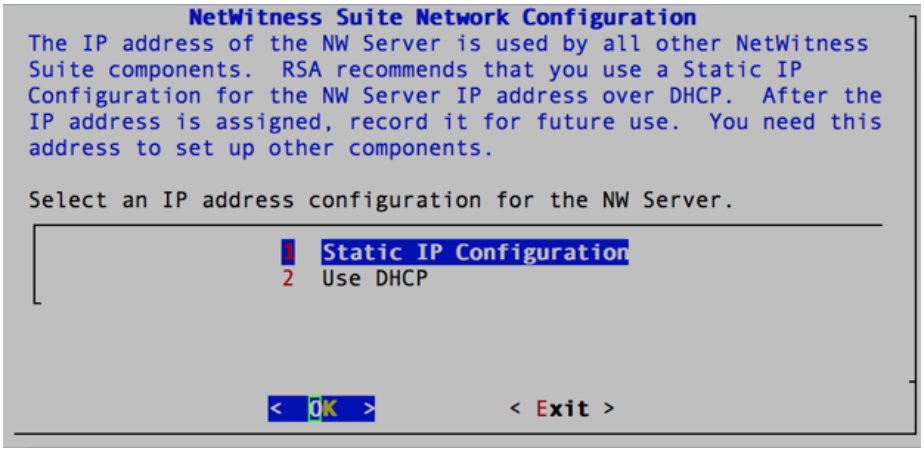
- If you are using an SSH connection, the following warning is displayed.

Note: If you connect directly from the host console, the following warning will not be displayed.



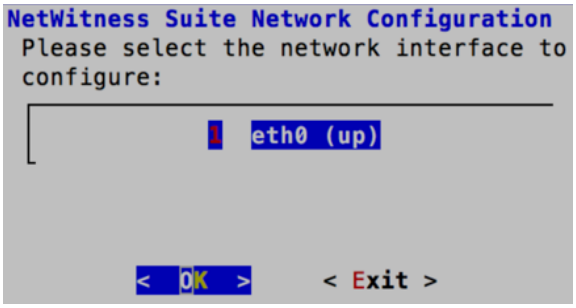
Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 12 to and complete the installation.
- If The Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the Network Configuration prompt is displayed.

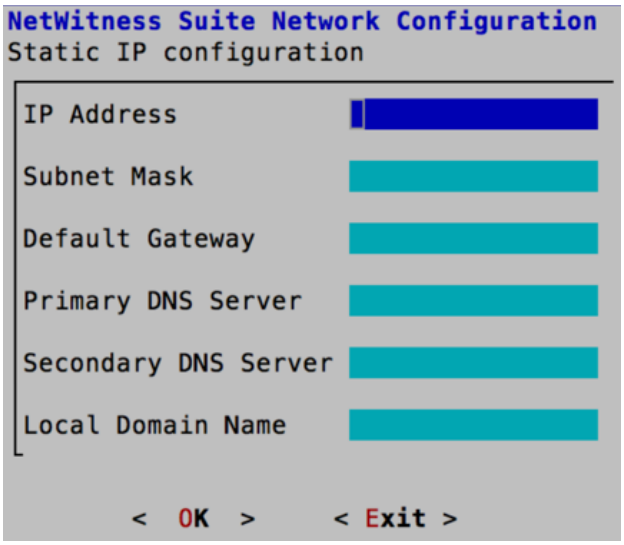


8. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

The Network Configuration prompt is displayed.



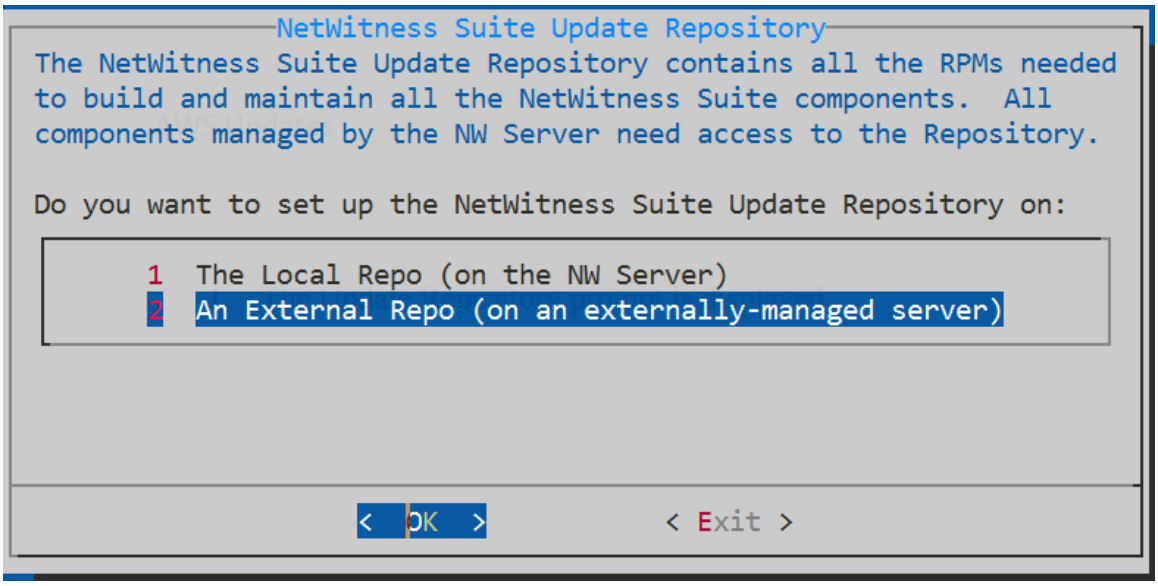
9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.
   The Static IP Configuration prompt is displayed.



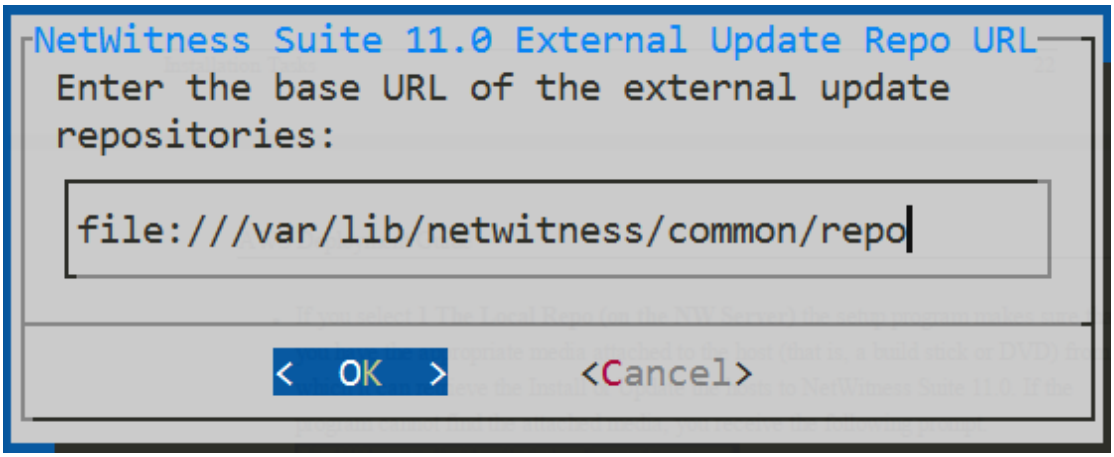
10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.
    If you do not complete all the required fields, an All fields are required error message is displayed (**Primary DNS Server**, **Secondary DNS Server**, and **Local Domain Name** fields are not required.)
    If you use the wrong syntax or character length for any of the fields, an Invalid *field-name* error message is displayed.

Caution: If you select DNS Server, make sure that the DNS Server is correct and the host can access it before proceeding with the install.

The Update Repository prompt is displayed.

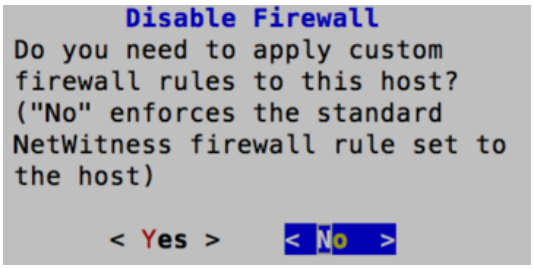


11. If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.

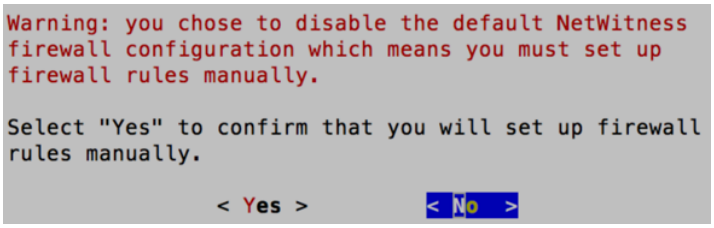


Enter the base URL of the NetWitness Suite external repo and click OK. The Start Install prompt is displayed.

12. Apply the standard firewall configuration, press **Enter**.
    - Disable the standard configuration, tab to **Yes** and press **Enter**.
      The Disable firewall prompt is displayed.



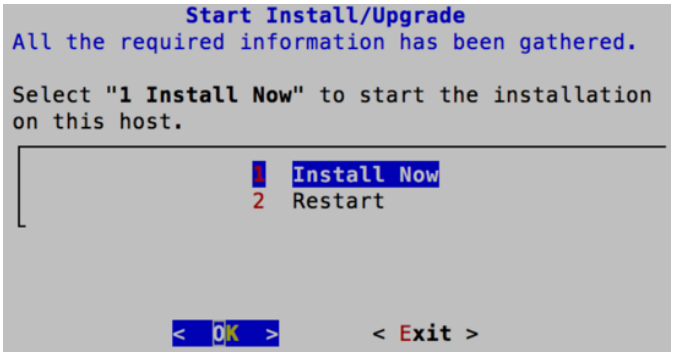
The disable firewall configuration confirmation prompt is displayed.



Tab to **Yes** and press **Enter** to confirm (press **Enter** to use standard firewall configuration).

13. Press **Enter** to install 11.1.0.0 on the NW Server.

    The Start Install prompt is displayed.



When "Installation complete" is displayed, you have installed the 11.1.0.0 NW Server on this host.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

Task 2 - Install 11.1.0.0 on Other Component Hosts

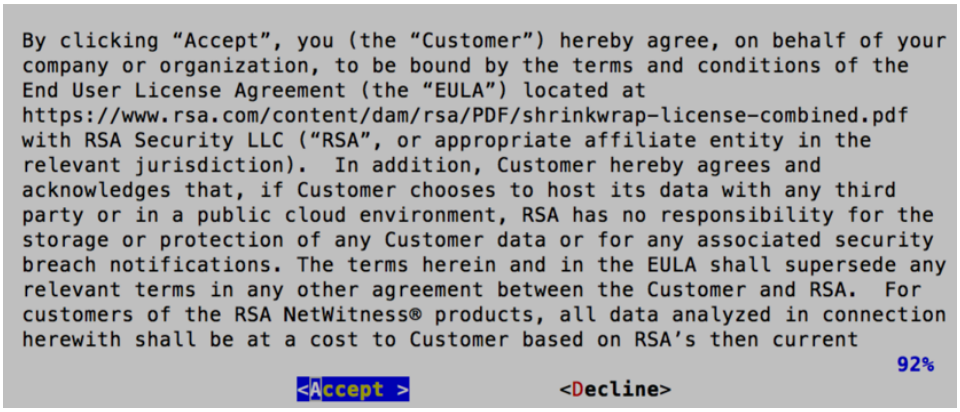
Note: You can perform this task for RSANW-11.1.0.0.1245-Lite-01 instance.

1. Run the `nwsetup-tui` command to set up the host.

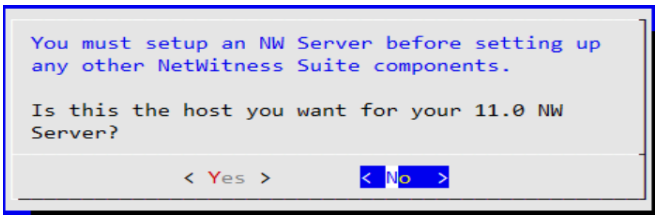
This initiates the Setup program and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console you use access the host.
3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see the "Post Installation Tasks" topic in the *Physical Host Installation Guide*..
If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

2. Tab to **Accept** and press **Enter**.



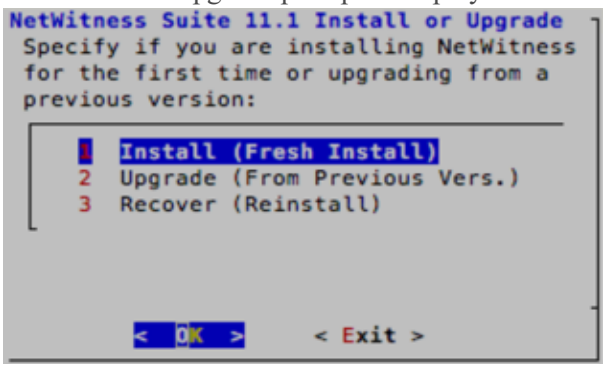
3. The "Is this the NW Server" prompt is displayed.



Tab to **No** and press **Enter**.

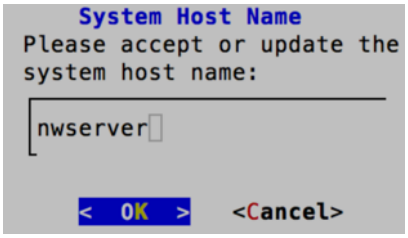
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

4. The Install or Upgrade prompt is displayed.



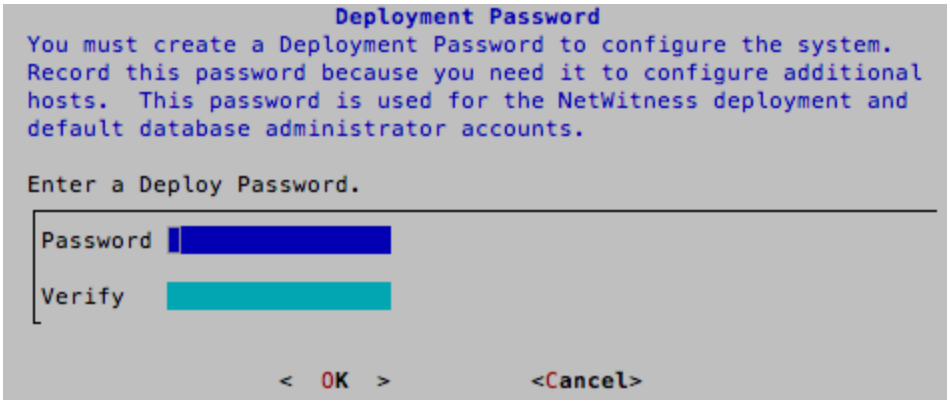
Press **Enter** (Install is selected by default).

5. The "Host Name" prompt is displayed.



Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

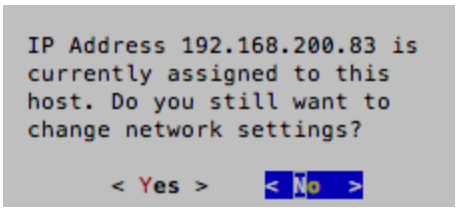
6. The "Deployment Password" prompt is displayed.



Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

7. If:

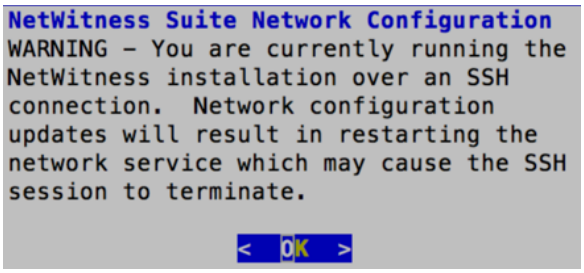
The Setup program finds a valid IP address for this host, the following prompt is displayed.



Press **Enter** if you want to use this IP and avoid changing your network settings.

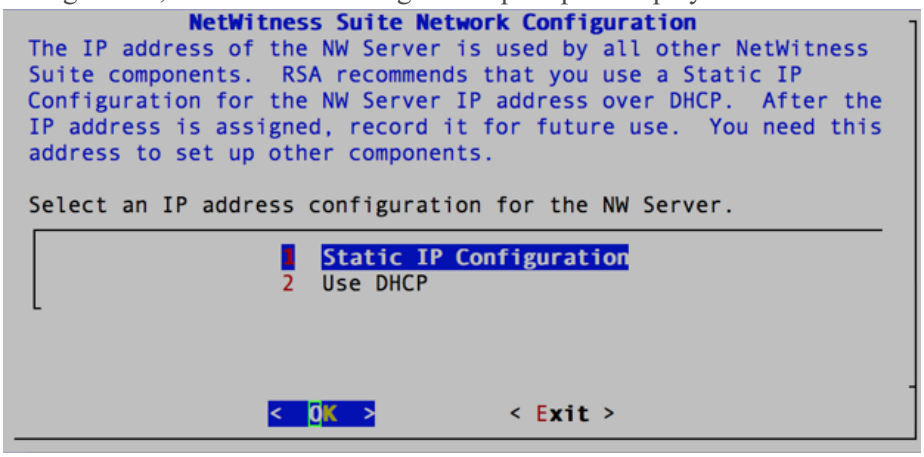
Tab to **Yes** and press **Enter** If you want to change the IP configuration found on the host.

You are using an SSH connection, the following warning is displayed.



Press **Enter** to close warning prompt. The Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 12 to and complete the installation.

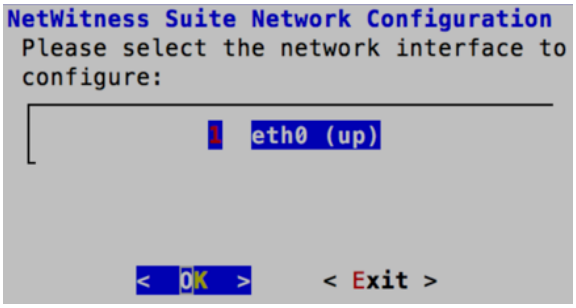
The Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the Network Configuration prompt is displayed.



Tab to **OK** and press **Enter** to use **Static IP**.

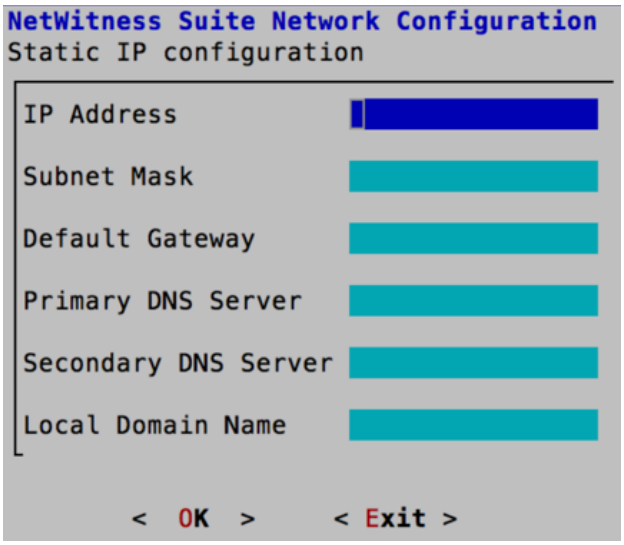
If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

8. The Network Configuration prompt is displayed.



Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.

9. The Static IP Configuration prompt is displayed.

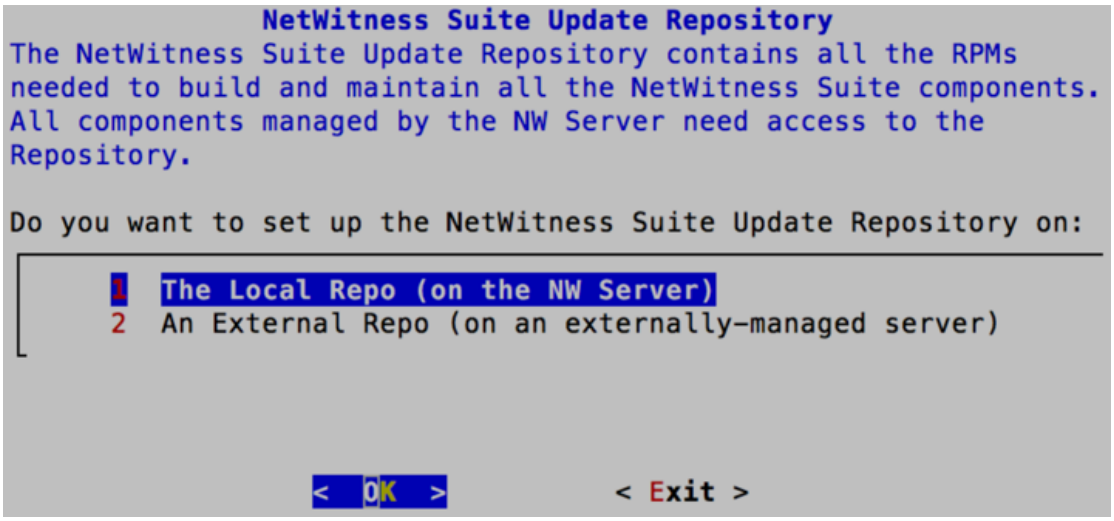


Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

10. If you do not complete all the required fields, an All fields are required error message is displayed (**Primary DNS Server**, **Secondary DNS Server**, and **Local Domain Name** fields are not required.)
    If you use the wrong syntax or character length for any of the fields, an Invalid *field-name* error message is displayed.

    Caution: If you select DNS Server, make sure that the DNS Server is correct and the host can access it before proceeding with the install.

11. The Update Repository prompt is displayed.

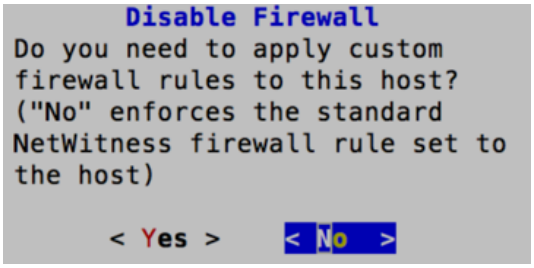


Press **Enter** to choose the **Local Repo** on the NW Server.

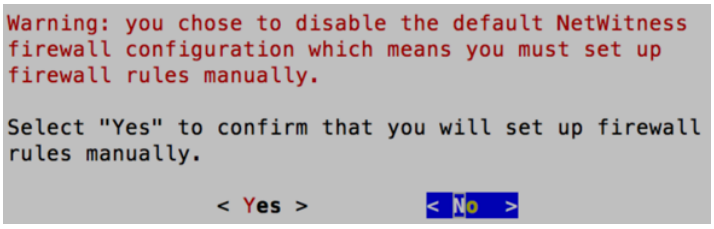
12. To:

    - Apply the standard firewall configuration, press **Enter**.
    - Disable the standard configuration, tab to **Yes** and press **Enter**.

      The Disable firewall prompt is displayed.

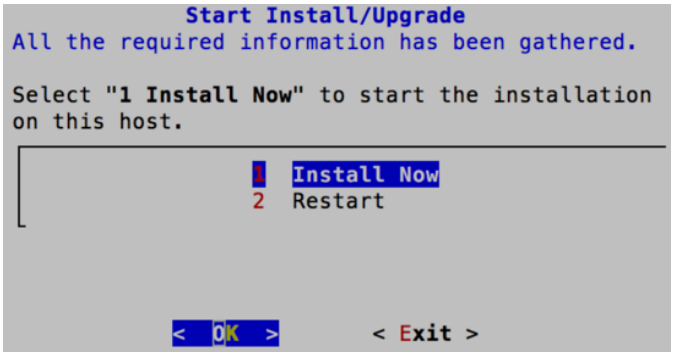


      The disable firewall configuration confirmation prompt is displayed.



      Tab to **Yes** and press **Enter** to confirm (press **Enter** to use standard firewall configuration).

13. The Start Install prompt is displayed.



    Press **Enter** to install 11.1 on the NW Server.

    When "Installation complete" is displayed, you have installed the 11.1.0.0 NW Server on this host.

    Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

Configure Hosts (Instances) in NetWitness Suite

Configure individual hosts and services as described in RSA NetWitness® Suite *Host and Services Configuration Guide*. This guide also describes the procedures for applying updates and preparing for version upgrades.

Note: After you successfully launch an instance, AWS assigns a default hostname to it. See the "Change the Name and Hostname of a Host" documentation in RSA Link (https://community.rsa.com) for instructions on changing a hostname.

Configure Packet Capture

You can integrate any of the following Third-Party solutions with the Packet Decoder to capture packets in the AWS cloud:

- Gigamon® GigaVUE
- f5® BIG-IP

Integrate Gigamon GigaVUE with the Packet Decoder

There are two main tasks to configure the Gigamon® third-party Tap vendor packet capture solution:

Task 1. Integrate the Gigamon® solution.

Task 2. Configure a tunnel on Packet Decoder.

Task 1. Integrate the Gigamon Solution

Gigamon® Visibility Platform on AWS will be available through the AWS Marketplace and activated by a BYOL license. A thirty-day free trial is also available.

For more information on the Gigamon® solution refer to the "Gigamon® Visibility Platform for AWS Data Sheet" (https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigamon-visibility-platform-for-aws-4095.pdf).

For deployment details refer to the "Gigamon® Visibility Platform for AWS Getting Started Guide" (https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-visibility-platform-for-aws-getting-started-guide-4111.pdf).

After the “Monitoring Session” is deployed within the Gigamon GigaVUE-FM, you can configure the Packet Decoder Tunnel.

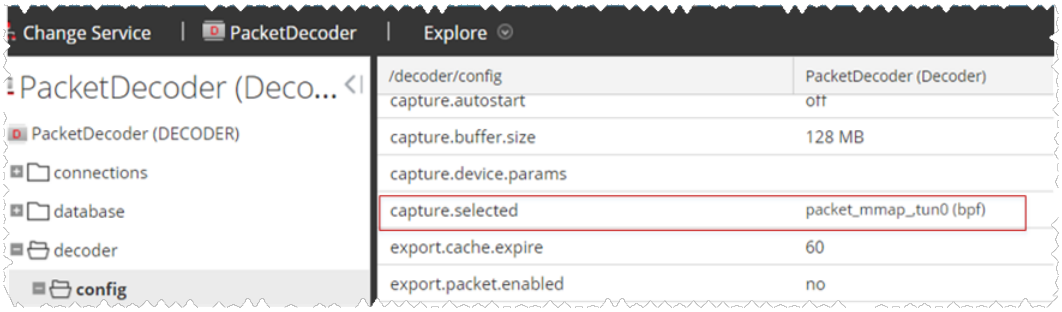
Task 2. Configure Tunnel on the Packet Decoder

1. SSH to the Decoder.
2. Submit the following command strings.

```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_
VSERIES_NODE_TUNNEL_INTERFACE> ttl 255

$ sudo ip link set tun0 up mtu <MTU-SIZE>

$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the
list of interfaces)

$ sudo lsmod | grep gre ( to make sure if the below kernel modules
are running:

ip_gre 18245 0

ip_tunnel 25216 1)

If they are not running then execute the below commands to enable the
modules

$ sudo modprobe act_mirred

$ sudo modprobe ip_gre
```

3. Create a firewall rule in the Packet Decoder to allow traffic through the tunnel.
   a. Open the `iptables` file.
      `vi /etc/sysconfig/iptables`
   b. Append the line `-A INPUT -p gre -j ACCEPT` before the `commit` statement
   c. Restart `iptables` by executing the following commands.
      `service iptables restart`
4. Set the interface in the Packet Decoder.
   a. Log in NetWitness Suite, select the `decoder/config` node in Explorer view for the Packet Decoder service.

b. Set the `capture.selected = packet_mmap_,tun0`.



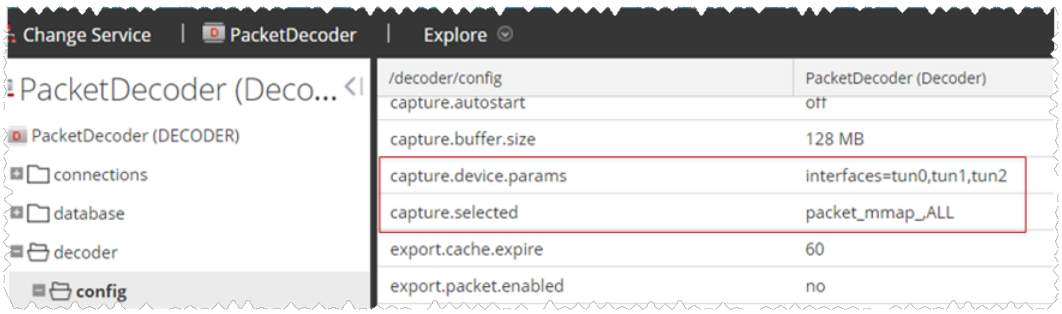
5. (Conditional) - If you have multiple tunnels on the Packet Decoder.

   a. Restart Decoder service after you create the tunnel in Packet Decoder.

   b. Log in to NetWitness Suite, select the `decoder/config` node in Explorer view for the Packet Decoder service, and set the following parameters.

   capture.device.params = interfaces=tun0,tun1,tun2

   capture.selected = packet_mmap_,All



6. Restart decoder service.

   ```
   $ sudo restart nwdecoder
   ```

   The user should be all set to capture the network traffic in Decoder.

Complete the following steps to create a new project and get your project key.

Integrate f5® BIG-IP with the Packet Decoder

IG-IP Virtual Edition (VE) is an inline virtual server and load balancer. A common use case would be for the f5® box to be a virtual web server that presents a single IP address / host name that manages requests to a pool of web servers in the cloud.

All traffic to RSA NetWitness® Suite flows through the f5® BIG-IP VE virtual server.

The virtual server functions of the BIG-IP clone all traffic to a designated computer by re-writing mac addresses and loading them into a subnet shared with the destination sniffer. This guide describes how to set up the Decoder as the sniffer.

f5® BIG-IP VE Deployment Information

f5® BIG-IP VE on AWS will be available through the AWS Marketplace and activated by a BYOL license. A thirty-day free trial is also available.

For more information on this solution refer to the f5® BIG-IP DNS Data Sheet (https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf).

Task 1: Set Up a BIG-IP VE Virtual Server Instance

Set up a BIG-IP VE Virtual Server Instance according to the instructions in the "BIG-IP Virtual Edition 12.1.0 and Amazon Web Services: Multi-NIC Manual" (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-multi-nic-setup-amazon-ec2-12-1-0.html). Complete all the steps through the last steps, "Creating a virtual server."

This virtual server performs packet capture. You may need to create multiple virtual servers to depending on your volume.

As part of creating the virtual server, you must have at least one server in your NetWitness Suite domain to handle the traffic routed by the virtual server (for example, you can create another instance in AWS to host the internal server).

Task 2: Create a Clone Pool

1. Make sure that your Decoder has a network interface on the same subnet as one of the network interfaces on the BIG-IP VE instance.
   The clone pool sends packets to the Decoder by rewriting MAC addresses and sending them out a network interface. MAC address rewriting can be used to route packets to another subnet.
2. Set up the clone pool within the BIG-IP VE virtual server according to the instructions in "K13392: Configuring the BIG-IP system to send traffic to an intrusion detection system (11.x - 13.x)" article (https://support.f5.com/kb/en-us/solutions/public/13000/300/sol13392.html).
   This document explains how to create the clone pool, and how to make an existing virtual server copy traffic to the clone pool. In this case, we will place the Decoder instance in the clone pool.

Guidelines

The following guidelines will help you to configure packet capture correctly using BIG-IP VE.

- The Decoder instance must have its own IP address on one of the same subnets as BIG-IP VE. BIG-IP uses that IP address to identify the Decoder as being part of the clone pool.

- When adding the Decoder instance to the clone pool, BIG-IP asks for a port number in addition to the IP address. This port number does not matter for the cloned traffic. The Decoder will receive all the cloned traffic, regardless of what port number was used here.
- By default, the AWS subnet shared by the Decoder and BIG-IP VE will not allow the cloned traffic to travel from the BIG-IP VE interface to the Decoder interface. You must disable the **`source/dest. check`** on both the Decoder and BIG-IP VE network interfaces in AWS.
- The Decoder instance must have a single network interface, eth0, by default. The Decoder captures traffic on this interface, but it may also receive administrative traffic on this interface. RSA recommends using network rules to filter out ssh and nwdecoder traffic from the capture stream. These are ports 22 (ssh) and 50004/56004 (nwdecoder).

Troubleshooting Tips

There are areas to troubleshoot if packets are not being accepted by the Decoder.

- Make sure that the BIG-IP VE is sending the packets out of the correct interface.
  The BIG-IP VE instance contains tcpdump. Use it to verify the cloned packets are being sent out the expected interface. If they are not, there is a problem in the setup of the clone pool or the virtual server.
- Make sure that the Decoder is receiving packets.
  The Decoder has `tcpdump` installed on it. Use it to verify that the Decoder is receiving packets. If the Decoder is not capturing packets, make sure that
  - The AWS **`source/dest. check`** is turned off.
  - The Decoder is on the same subnet as the interface the BIG-IP VE is using to clone packets.

AWS Instance Configuration Recommendations

Note: These recommendations can be used as a baseline for 11.1.0.0 and adjusted as needed.

Note: For a description of terms and abbreviations used in this topic, refer to Abbreviations and Other Terminology Used in this Guide.

This topic contains the minimum AWS instance configuration settings recommended for the RSA NetWitness® Suite virtual stack components.

- EC2 Instance:
  - Minimum instance type - **m4-2xlarge** is the minimum instance type required for any NetWitness Suite component AMI so that it can function.
  - Instance type adjustments -you must adjust instance types according to your ingestion rate, content and parsers, dashboard reports, scheduled reports, investigations, and active users.
  - Recommended settings - the recommended settings in the SA component instance tables below were calculated under the following conditions.
    - Ingestion rates of 15,000 EPS and 1.5 Gbps were used.
    - All the components were integrated.
    - The Log stream includes a Log Decoder, Concentrator, and Archiver.
    - The Packet stream includes a Packet Decoder and Concentrator.
    - The Endpoint Hybrid stream includes a Endpoint Server, Concentrator and Log Decoder.
    - Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
    - The background load includes reports, charts, alerts, investigation, and respond.
- EBS Volumes (Storage)

  Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance on how to increase the number of volumes based on your storage requirements using the RSA Sizing & Scoping Calculator.

  Note: The Concentrator index volume must be allocated on Provisioned IOPS SSD.

  - Index
  - Meta

- Session
- Packet

Archiver

EC2 Instance			
EPS	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
5,000	m4.xlarge No of CPU: 4 Memory: 16 GB	No	Yes
10,000	m4.2xlarge No of CPU: 8 Memory: 32 GB	No	Yes
15,000	m4.4xlarge No of CPU: 16 Memory: 64 GB	No	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
archiver	/dev/sdg	Throughput Optimized HDD	240 MB/s
workbench	/dev/sdh	Throughput Optimized HDD	N/A

Broker

EC2 Instance		
Instance Type	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
m4.xlarge No of CPU: 4 Memory: 16 GB	No	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
broker	/dev/sdg	General Purpose SSD	N/A

Concentrator - Log Stream

EC2 Instance			
EPS	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
5,000	m4.xlarge No of CPU: 4 Memory: 16 GB	No	Yes
10,000	m4.2xlarge No of CPU: 8 Memory: 32 GB	No	Yes
15,000	m4.4xlarge No of CPU: 16 Memory: 64 GB	No	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index	/dev/sdg	Provisioned IOPS	10,000
session, metadb	/dev/sdh	Throughput Optimized HDD	240 MB/s

Packet Stream Solutions

Concentrator - Gigamon Solution

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
500 Mbps	c4.4xlarge No of CPU: 16 Memory: 30 GB	No	Yes
1,000 Mbps	c4.8xlarge No of CPU: 36 Memory: 60 GB	No	Yes
1.5 Gbps	m4.10xlarge No of CPU: 40 Memory: 160 GB	No	Yes

Concentrator - f5 BIG-IP Solution

To be updated when f5 BIG-IP performance testing is complete.

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
230 Mbps	m4.4xlarge No. of CPU: 16 Memory: 64 GB	No	No

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index	/dev/sdg	Provisioned IOPS	15,000
session, metadb	/dev/sdh	Throughput Optimized HDD	240 MB/s

Decoder - Gigamon Solution

EC2 Instance			
Mbps/Gbps	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
500 Mbps	c4.2xlarge No of CPU: 8 Memory: 15 GB	Yes	Yes
1000 Mbps	c4.4xlarge No of CPU: 16 Memory: 30 GB	Yes	Yes
1.5 Gbps	c4.8xlarge No of CPU: 36 Memory: 60 GB	Yes	Yes

Decoder - f5 BIG-IP Solution

To be updated when f5 BIG-IP performance testing is complete.

EC2 Instance			
Mbps/Gbps	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
230 Mbps	m4.4xlarge No. of CPU: 16 Memory: 64 GB	No	No

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session,meta	/dev/sdg	Throughput Optimized HDD	240 MB/s
packet	/dev/sdh	Throughput Optimized HDD	240 MB/s

ESA and Context Hub on Mongo Database

	EC2 Instance		
EPS	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
9,000	m4.2xlarge No of CPU: 8 Memory: 32 GB	No	Yes
18,000	r4.2xlarge No of CPU: 8 Memory: 61 GB	No	Yes
30,000 Aggregation Rate	r4.4xlarge No of CPU: 16 Memory: 122 GB	No	Yes

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
apps (/opt/rsa)	/dev/sdg	General Purpose SSD	N/A

Log Collector (Syslog, Netflow, and File Collection Protocols)

EC2 Instance			
EPS	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
30,000 NON SSL	c4.2xlarge No of CPU: 8 Memory: 15 GB	No	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
logcollector	/dev/sdg	General Purpose SSD	N/A

Log Decoder

EC2 Instance			
EPS	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
5,000	c4.2xlarge No of CPU: 8 Memory: 15 GB	Yes	Yes
10,000	c4.4xlarge No of CPU: 16 Memory :30 GB	Yes	Yes
15,000	c4.8xlarge No of CPU: 36 Memory: 60GB	Yes	Yes

EBS Volumes (Storage)l			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session,meta	/dev/sdg	Throughput Optimized HDD	240 MB/s
packet	/dev/sdh	Throughput Optimized HDD	240 MB/s

NetWitness Server, Reporting Engine, Respond and Health & Wellness

EC2 Instance		
Instance Type	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
m4.2xlarge No of CPU: 8 Memory: 32 GB	No	Yes
m4.4xlarge No of CPU: 16 Memory: 64 GB	No	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
uax,ipdb	/dev/sdg	General Purpose SSD	N/A
redb,rehome	/dev/sdh	General Purpose SSD	N/A

NetWitness Endpoint Hybrid

	EC2 Instance		
Agents	**Instance Type**	**Enhanced Networking Enabled**	**Tenancy Type - Dedicated - Run a Dedicated Instance**
15,000 agents	m4.10xlarge No of CPU: 40 Memory: 160 GB RAM	Yes	Yes

EBS Volumes (Storage)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Throughput**
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session,meta (Log Decoder)	/dev/sdg	Throughput Optimized HDD	240 MB/s
packet (Log Decoder)	/dev/sdh	Throughput Optimized HDD	240 MB/s
index (Concentrator)	/dev/sdi	Provisioned IOPS	10,000
session,meta (Concentrator)	/dev/sdj	Throughput Optimized HDD	240 MB/s
mongoDB	/dev/sdl	Throughput Optimized HDD	240 MB/s

RSA NETWITNESS® SUITE

Azure Deployment Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2018

Contents

Deployment Overview **5**

Azure Environment Recommendations 5

Abbreviations and Other Terminology Used in this Guide 5

Azure Deployment Scenarios 7

Full NetWitness Suite Stack Azure Visibility 7

Hybrid Deployment - Log Decoder 8

Supported Services 8

VM Configuration Recommendations **10**

Deployment Rules and Checklist **12**

Rules 12

Checklist 12

Step 1. Deploy NW Server Host in Azure 13

Task 1. - Upload NW Server VHDs 13

Task 2. - Create NW Server Image 16

Task 3. Create Virtual Machine (VM) 18

Step 2. Deploy Component Core Services in Azure 26

Step 3. Configure Host VMs in NetWitness Suite 31

Deployment Overview

Before you can deploy RSA NetWitness® Suite in Azure you need to:

- Understand the requirements of your enterprise.
- Know the scope of a NetWitness Suite deployment.

When you are ready to begin the deployment:

- Make sure that you have a NetWitness Suite "Throughput" license.
- Use Chrome for your browser (Internet Explorer is not supported).

Azure Environment Recommendations

Azure instances have the same functionality as the NetWitness Suite hardware hosts. RSA recommends that you perform the following tasks when you set up your Azure environment.

- Based on the resource requirements of the different components, follow best practices to use the system and dedicated storage appropriately.
- Build Concentrator directory for index database on SSD.

Abbreviations and Other Terminology Used in this Guide

Abbreviations	Description
Azure	Azure is Microsoft's public cloud computing platform. It provides a range of cloud services, including those for compute, analytics, storage and networking. You can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud.
BYOL	Bring your own licensing
CPU	Central Processing Unit
EPS	Events Per Second
GB	Gigabyte. 1GB = 1,000,000,000 bytes

Abbreviations	Description
Gb	Gigbit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
HDD	Hard Disk Drive
IOPS	Input/Output Operations Per Second
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
On-Premise	On-premise hosts are installed and run on computers on the premises (in the building) of the organization using the hosts, rather than in the Azure.
RAM	Random Access Memory (also known as memory)
Security	Set of firewall rules. Refer to Deployment: Network Architecture and Ports (https://community.rsa.com/docs/DOC-83050) for a comprehensive list of the ports you must set up for all NetWitness Suite components.
SSD	Solid-State Drive
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
VHD	Virtual Hard Disk
VM	Virtual Machine
vRAM	Virtual Random Access Memory. This is the memory for a virtual machine.

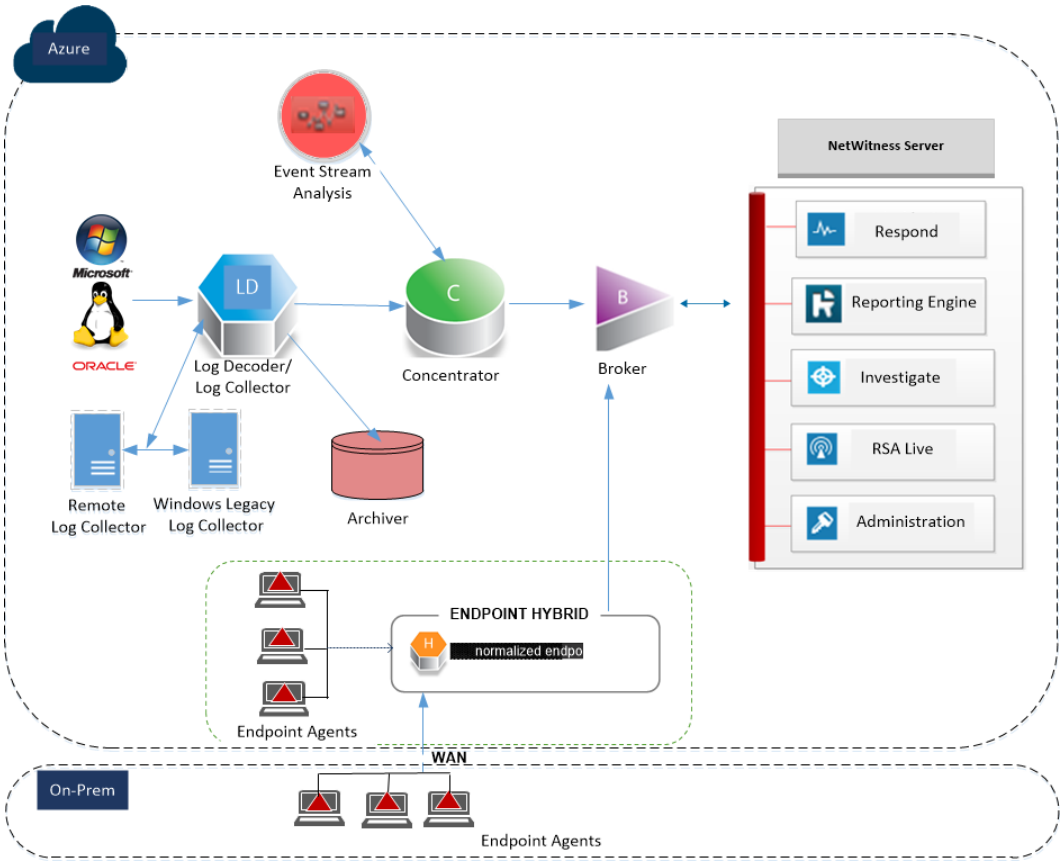
Azure Deployment Scenarios

The following diagrams illustrate some common Azure deployment scenarios. In the diagrams, the:

- **Log Decoder** receives logs collected by the Log Collector. The Log Collector collects log events from hundreds of devices and event sources.
- **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while facilitating reporting and alerting.
- **Endpoint Hybrid** is used for collection of endpoint data. The Endpoint Hybrid comprises of and Endpoint Server, Log Decoder, and a Concentrator.
- NetWitness Server hosts **Respond**, **Reporting Engine**, **Investigate**, **RSA Live**, **Administration**, **Endpoint Hybrid/Log Hybrid** and other aspects of the user interface.

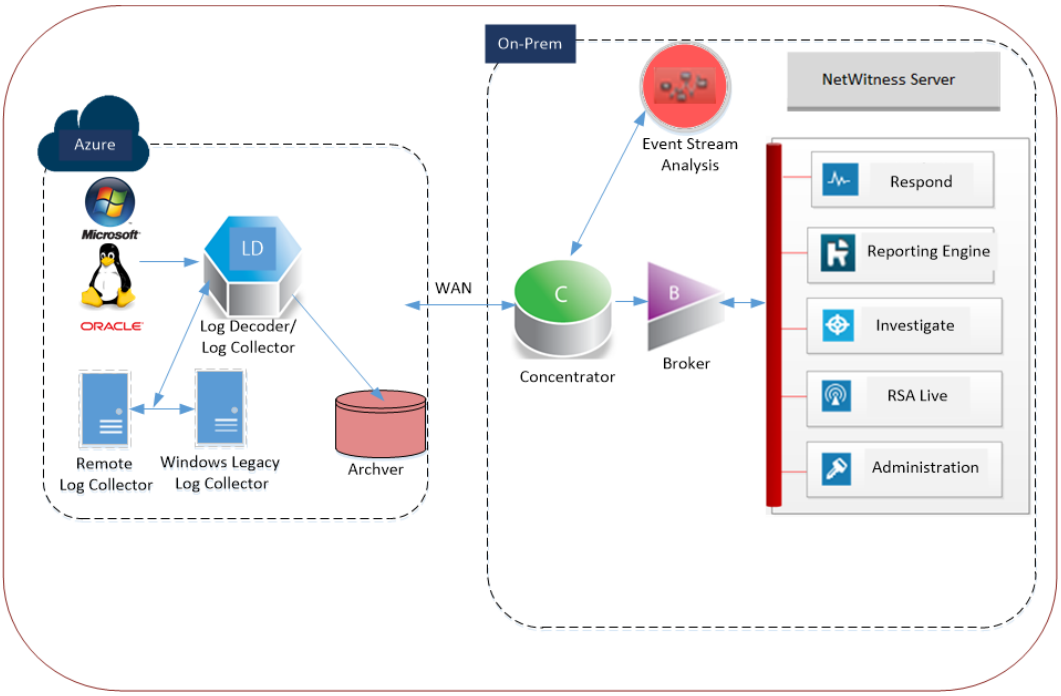
Full NetWitness Suite Stack Azure Visibility

This diagram shows all NetWitness Suite components (full stack) deployed in Azure.



Hybrid Deployment - Log Decoder

This diagram shows the Log Decoder and Archiver deployed in Azure with all other NetWitness Suite components deployed on your premises.



Supported Services

RSA provides the following NetWitness Suite services.

- NetWitness Server
- Admin Server
- Config Server
- Investigate Server
- Orchestration Server
- Reporting Engine
- Respond Server
- Security Server
- Archiver
- Broker

- Concentrator
- Event Stream Analysis
- Log Decoder
- Remote Log Collector
- Endpoint Server

VM Configuration Recommendations

Note: These recommendations were qualified for RSA Security Analytics 10.6.4. These recommendations can be used as a baseline for 11.1.0.0 and adjusted as needed.

Note: For a description of terms and abbreviations used in this topic, refer to Deployment Overview.

This topic contains the minimum Azure VM configuration settings recommended for the NetWitness Suite (NW) virtual stack components.

- VM:
  - The recommended settings in the NetWitness Suite component VM tables below were calculated under the following conditions.
    - Ingestion rates of 15,000 EPS were used.
    - All the components were integrated.
    - The Log stream included a Log Decoder, Concentrator, and Archiver.
    - Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
    - The background load included reports, charts, alerts, investigation, and incident management.
- VHD (Storage)
  Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance on how to increase the number of volumes based on your the storage requirements using the RSA Sizing & Scoping Calculator.

  Note: For higher EPS rates, the Concentrator index volume must be allocated SSDs.

VM Sizing			
Component	**EPS**	**Compute**	**VM Size**
Archiver	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2

VM Sizing			
Component	**EPS**	**Compute**	**VM Size**
Broker	15,000	No of CPU: 4 Memory: 14 GB	Standard DS3 v2
Concentrator	15,000	No of CPU: 16 Memory: 112 GB	Standard DS14 v2
ESA and Context Hub	15,000	No of CPU: 20 Memory: 140 GB	Standard D15 v2
Log Collector	15,000 NON SSL	No of CPU: 8 Memory: 16 GB	Standard F8
Log Decoder	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2
NW Server*	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2

*Reporting Engine, Respond, and Health & Wellness can be co-located on NetWitness Server host.

Deployment Rules and Checklist

This topic contains the rules and high-level tasks provides you must follow to deploy RSA NetWitness® Suite components in the Azure.

Rules

You must adhere to the following rules when deploying NetWitness Suite in Azure.

- Always use private IP addresses when you provision Azure NetWitness SuiteVMs.
- Before you enable the out-of-the-box (OOTB) dashboards, set the default data source in Reporting Engine configuration page.

Checklist

Step	Description	√
1.	Step 1. Deploy NW Server Host in Azure	
2.	Step 2. Deploy Component Core Services in Azure	
3.	Step 3. Configure Host VMs in NetWitness Suite	

Step 1. Deploy NW Server Host in Azure

Complete the following tasks to deploy a NetWitness Server (NW Server) on a virtual machine (VM) in the Azure Cloud environment.

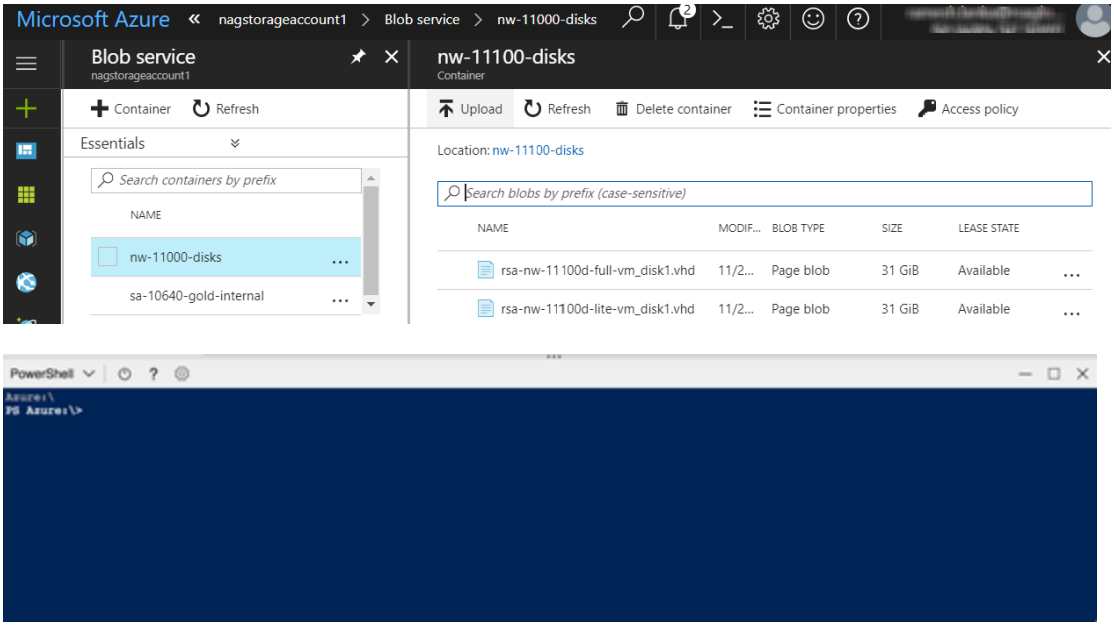
Note: It is not mandatory to deploy the SA Server in the Azure Cloud environment to deploy other components (see Azure Deployment Scenarios).

- Task 1. - Upload NW Server VHDs
- Task 2. - Create NW Server Image
- Task 3. - Create Virtual Machine (VM)

Task 1. - Upload NW Server VHDs

Complete the following steps to upload NW Server VHDs to Azure.

1. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) to open a support case requesting the NW Server VHDs. A valid throughput license will be required.
2. Customer Support will update the case with VHD URI's.
3. Via the Azure Portal, open the Powershell CLI.



- You'll need a storage account, blob service and container setup. This is where the VHD's will be copied to. After these are in place, you can execute the following command within the Azure Portal Powershell CLI. Follow these steps to copy the blob to azure container:

a. Run this command from Powershell to install AzureRM: `Install-Module -Name AzureRM –AllowClobber`

b. Execute this command to verify the installation process has been successfully done: `Import-Module -Name AzureRM`

c. If you find any error regarding execution policy then execute this command: - `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned` (then repeat step 2)

d. Login using this command: `Login-AzureRmAccount`

e. Select the Subscription: `Select-AzureRmSubscription -SubscriptionId <subscriptionid>`

f. Create a target context: `$targetStorageContext = (Get-AzureRmStorageAccount -ResourceGroupName <resource-group-name> -Name <storage-account-name>).Context`

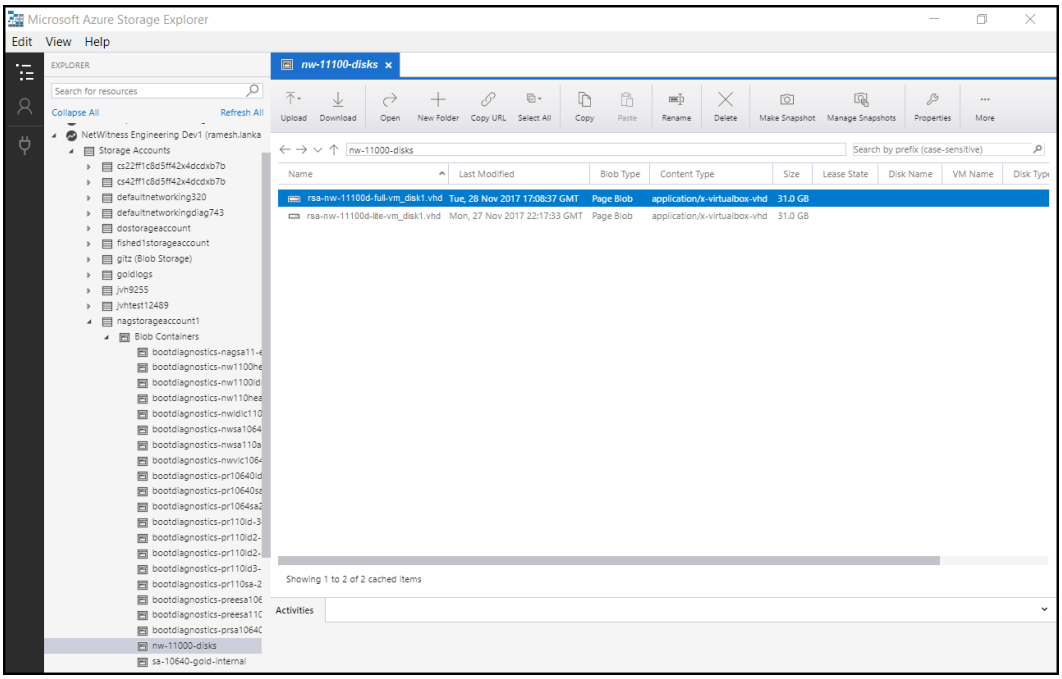
g. Start the copy: `Start-AzureStorageBlobCopy -AbsoluteUri "<SAS-URL>" -DestContainer <container-name> -DestBlob <destination-blob-name> -DestContext $targetStorageContext`

h. You can get the Blob copy status by executing this command: `Get-AzureStorageBlobCopyState -Blob "< destination-blob-name>" -Container "<container-name> " –Context $targetStorageContext`

4. Once the VHD's are successfully copied. You'll need to create an image and VM.

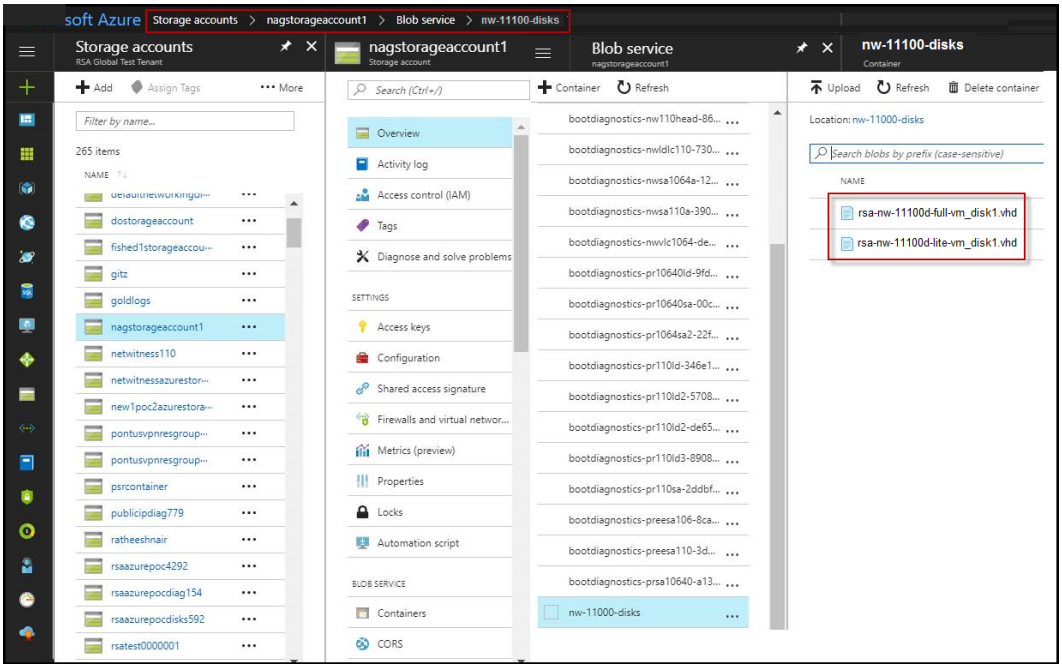
5. Verify that all the NW Server VHDs are uploaded into the Azure Cloud.

Note: Alternatively, you can use the Microsoft Azure Storage Explorer windows utility (http://storageexplorer.com/) to verify that all the VHDs from the following location subscription exist. This utility helps you manage the contents your storage.



a. Log in to the Azure portal (https://portal.azure.com).

b. In the right panel, click **Storage accounts** > **netwitnessazurestorage1** > **Blob service** > **nwazurevhdstore**.

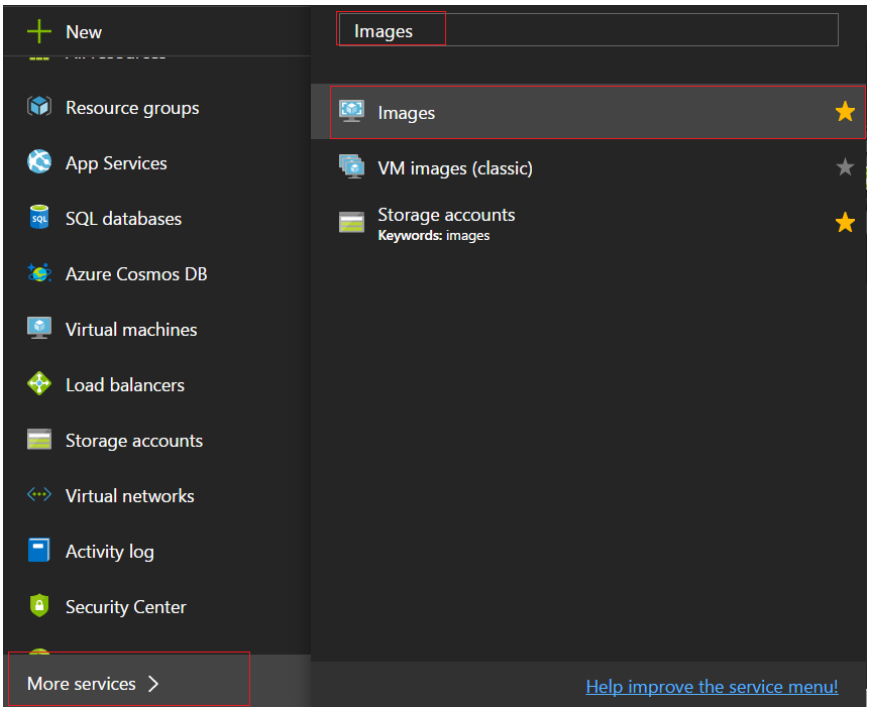


6. (Optional) In the Azure Explorer, go to the **NetWitness** group > **Storage Accounts** > **netwitnessazurestorage1**) > **Blob Containers** > **nwazurevhdstore**). The following screen shot shows you an example of the contents of a storage container.

Task 2. - Create NW Server Image

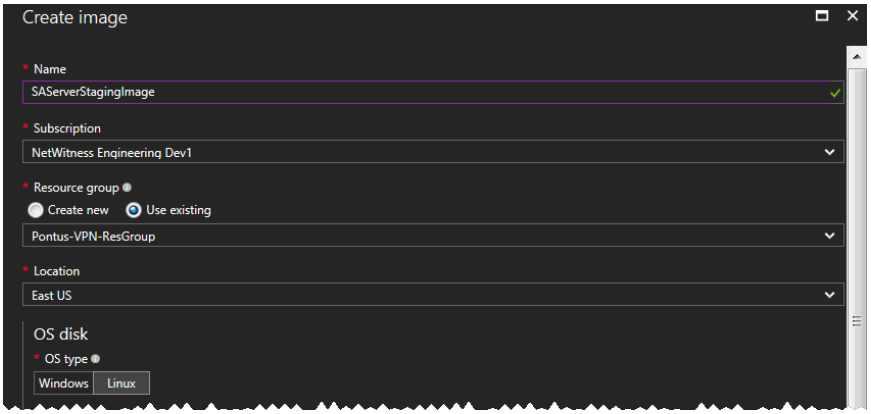
Complete the following steps to create an NW Server image in Azure from upload VHDs.

1. Log in to https://portal.azure.com.
2. In the left panel, click **More Services** and filter by Images.
3. Click **Images**.



4. Create and configure the Image.
   a. Click **Add**.
   b. Enter an Image Name, select the correct Resource Group, select a valid Location, and set the OS Disk to Linux.

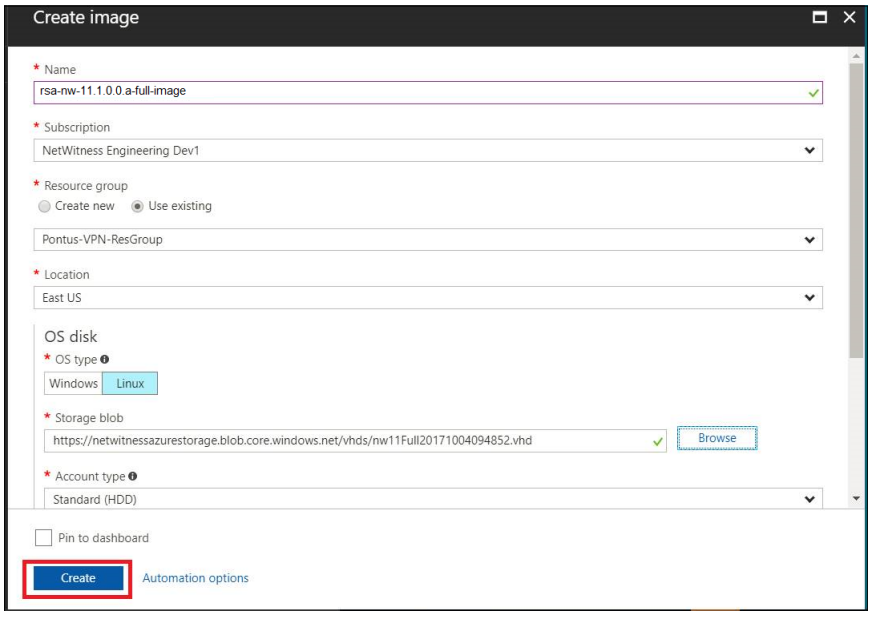
In the **Storage blob**, browse to where VHDs are uploaded.



c. Select **https://netwitnessazurestorage.blob.core.windows.net/nwvhdstore/SA-Server-11.0.0.0-03-Gold-disk1.vhd** in the **OS disk Storage blob** field.

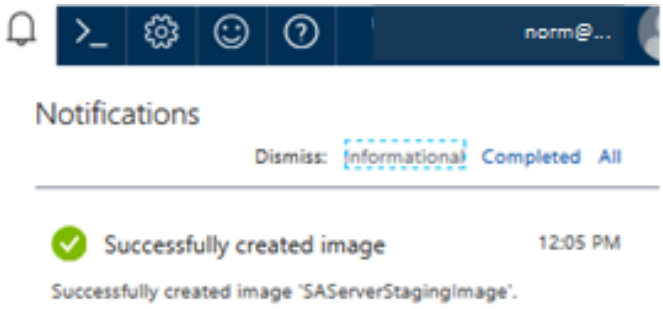
d. Make sure that **Standard (HDD)** is selected for **Account Type**.

The following screen shot illustrates a completed **Create Image** view.



e. Click **Create** to create the Image.

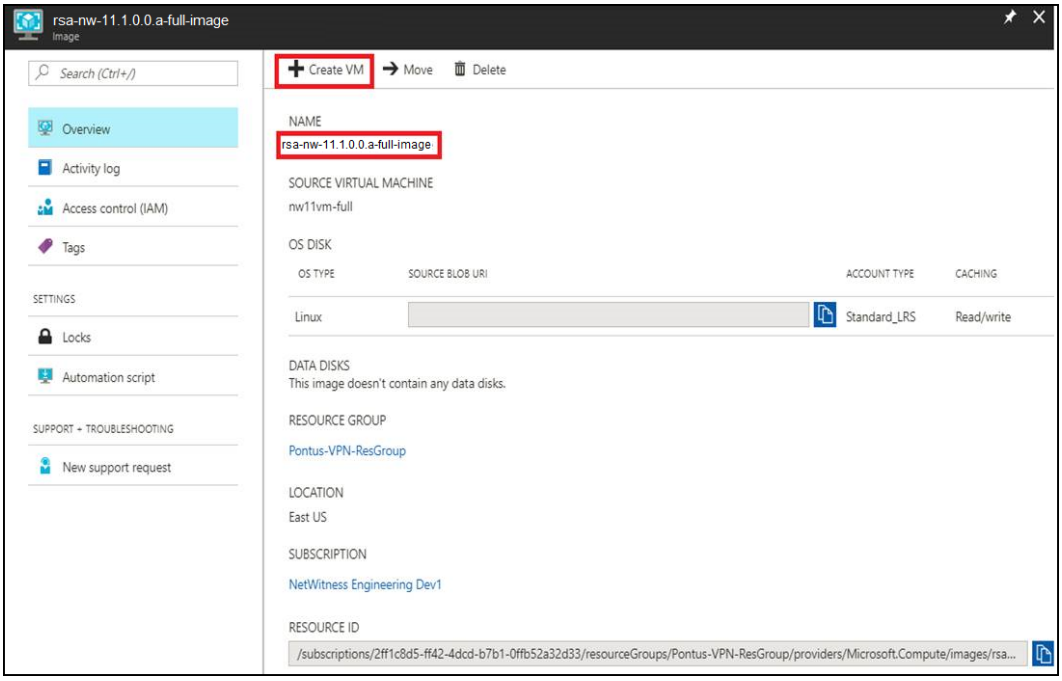
The following confirmation is displayed when the image is created.



Task 3. Create Virtual Machine (VM)

Complete the following steps to create a VM in Azure using the SA Server image.

1. Go to **Images** and click **Create VM**.



The **1 Basics - Configure basic settings** section is in focus.

2. Define values for all of the fields.

   a. In the **Name** field, enter a user-defined name (for example, **NWServer1100**).

   b. In the **VM disk type** field, select **HDD** from the drop-down list.

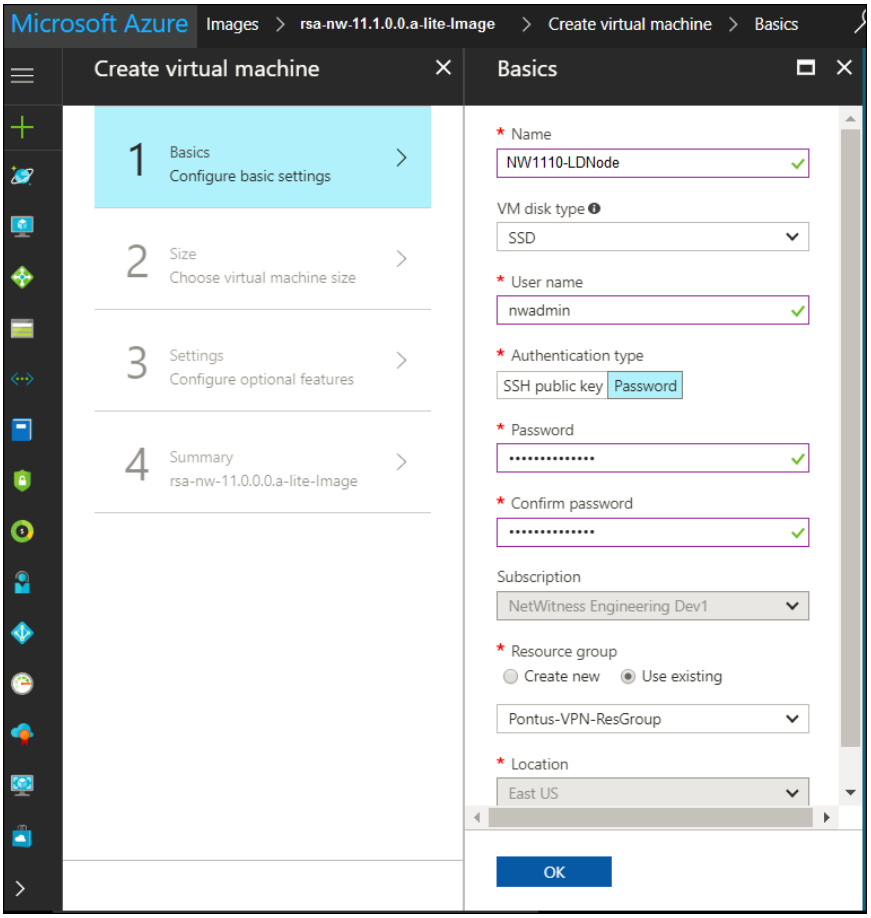
   Caution: The username and password that you define is used to login to the system as a non-administrator user. Do not use the root user (the login does not have superuser permissions). You must change the root password the first time that you log in to the VM by executing the `su passwd root` command. This is a critical step and should not be missed. You cannot use `root` for a username (Azure-specific).

   c. In the **User name** field, enter a valid username.

   d. In the **Authentication type** field, click **Password** and enter a strong password that is a combination of lowercase, uppercase, numeral and a symbol (for example, **Password@123**).

   e. Make sure that the values selected in the **Subscription**, **Resource group and Location** fields are correct.

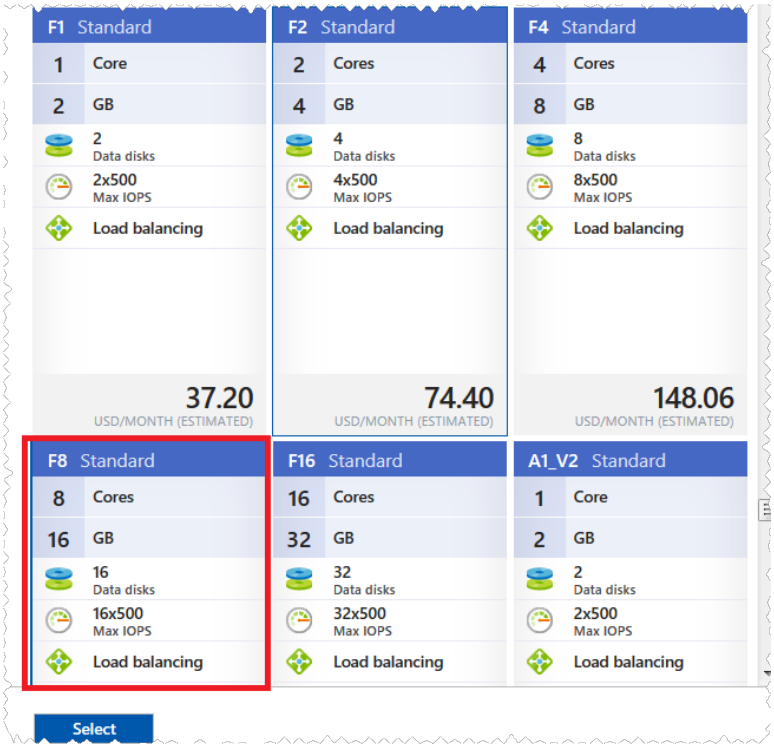
   f. Click **OK**.



The **2 Size - Choose virtual machine size** section is in focus.

3. Click ***size-required-based-on-capacity*** (for example, **F8 Standard**), and click **Select**.

Note: Sizing is based upon the capacity requirements of your enterprize (see VM Configuration Recommendations for RSA VM size recommendations based on log capture rates. The minimum size RSA recommends for the SA Server is **F8 Standard**.



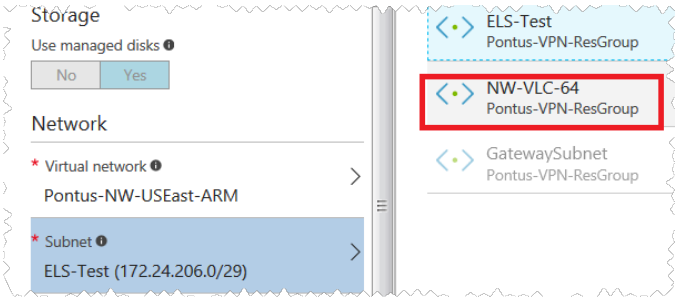
The **3 Settings – Configure optional features** section is in focus.

4. Click and define the fields.

   a. In the **Storage** field, make sure that **Use manage disks** is set to **Yes**.

   b. In the **Network** field, select:

   - A valid **Virtual network** and **Subnet**.



   - **None** for the **Public IP address**.

     RSA recommends **None** for the **Public IP address** (this is not mandatory). You can

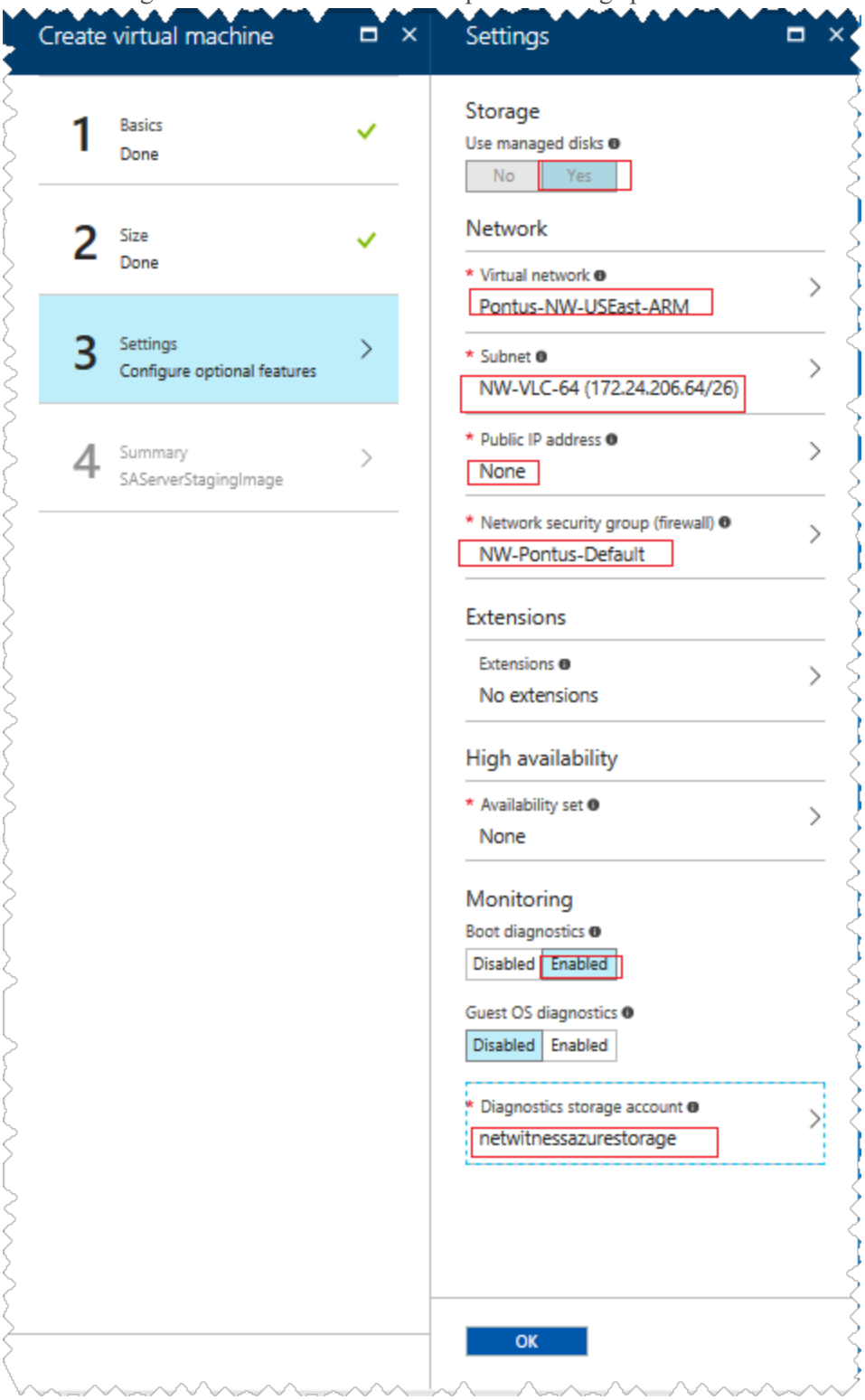
assign a public IP address, but it countermands Best Practices to assign a public IP to something that is based in the Azure cloud.

- A valid **Network security group**.
  For information on Network security groups, see the Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg).

c. In the Monitoring field, select:

- **Enabled** for **Boot Diagnostics**
- **Enabled** for **Guest OS diagnostics**
- a valid **Diagnostics storage account**

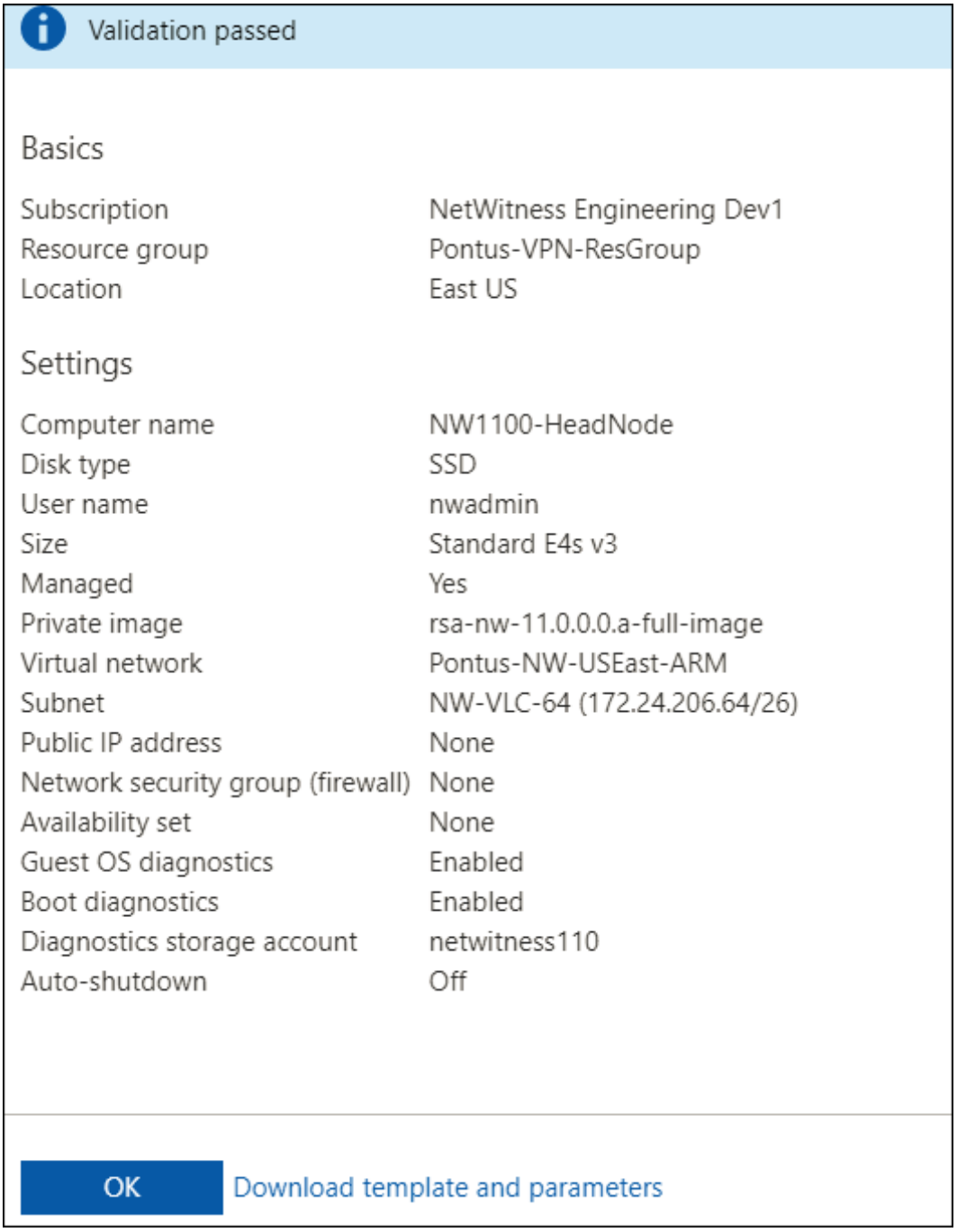
The following screen shot illustrates a completed Settings panel.



d. Click **OK**.

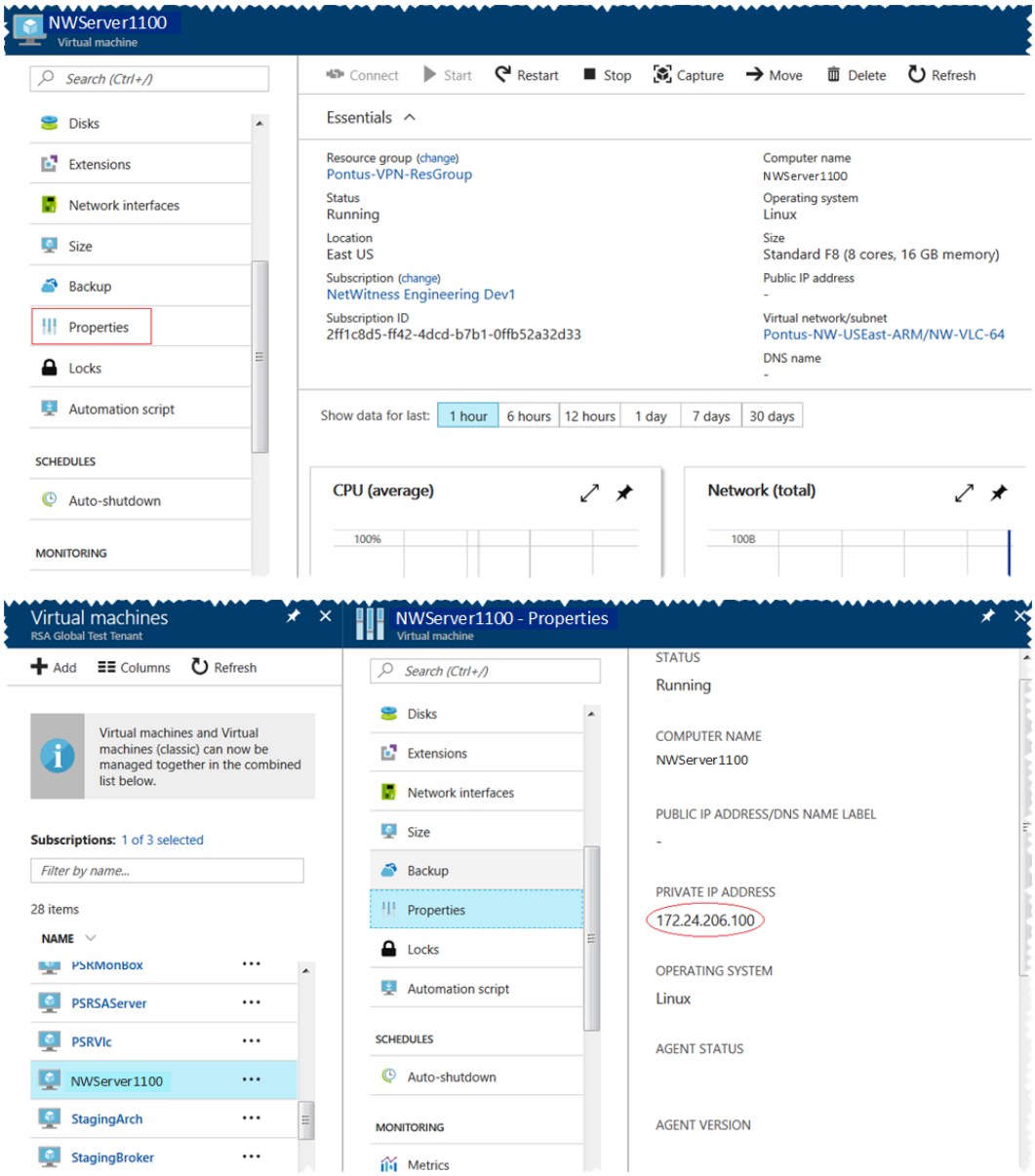
The **4 Summary – SAServerStagingImage** section is in focus.

5. Verify that the Validation passed, and click **OK**.



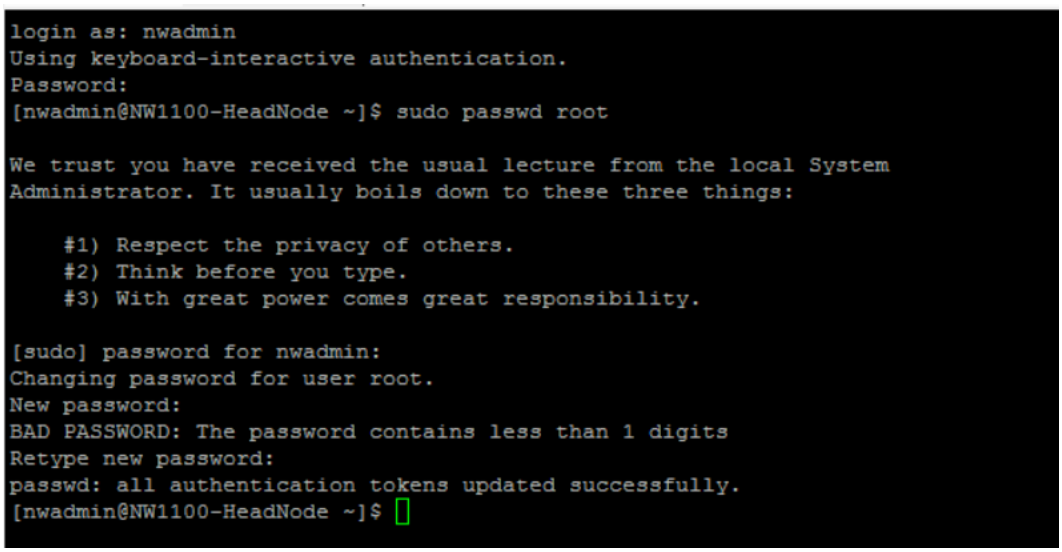
You know that the NW Server VM Deployment is successful when you see the VM status as **Running**.

6. Click **Properties** to view the **IP Address** details.



7. SSH to the VM using the username that you specified in Step 2d of Task 3 and reset the **root** password. Use the `su passwd root` command string to reset the root password as shown

in the following screen shot.



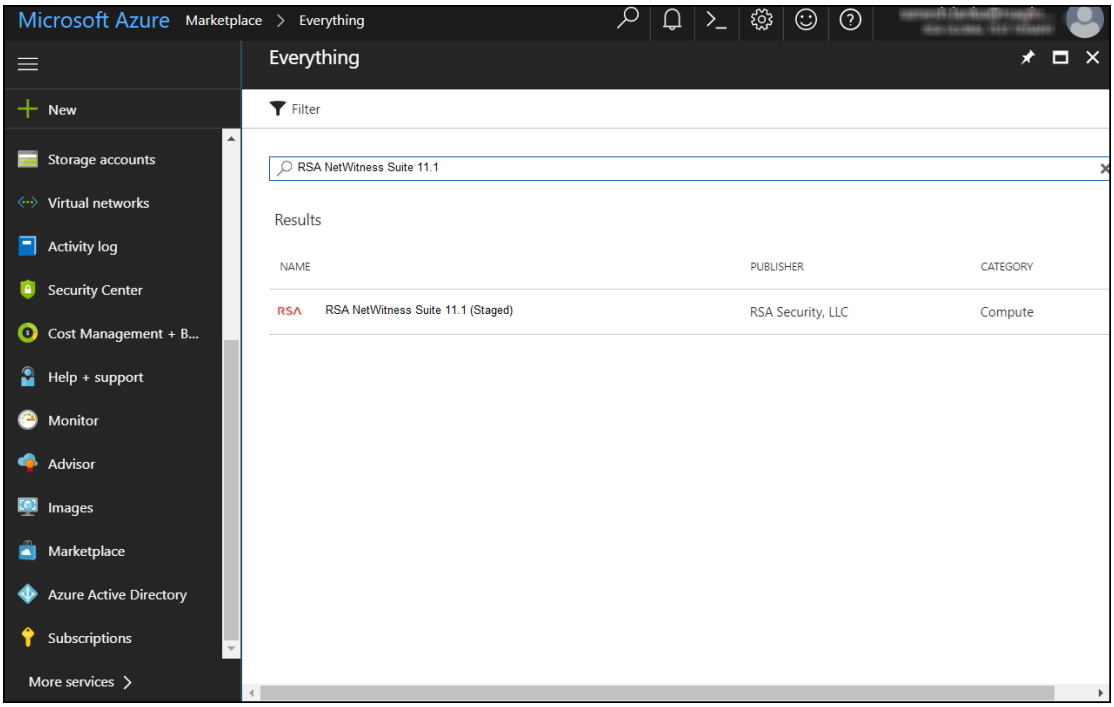
8. Close the current SSH session and open a new SSH session with **root** as the username and the password created in the previous step.

> **Note:** Step 8 is a critical, one-time step for a new deployment. If you do not complete this step, the Security Analytics User Interface will not load.

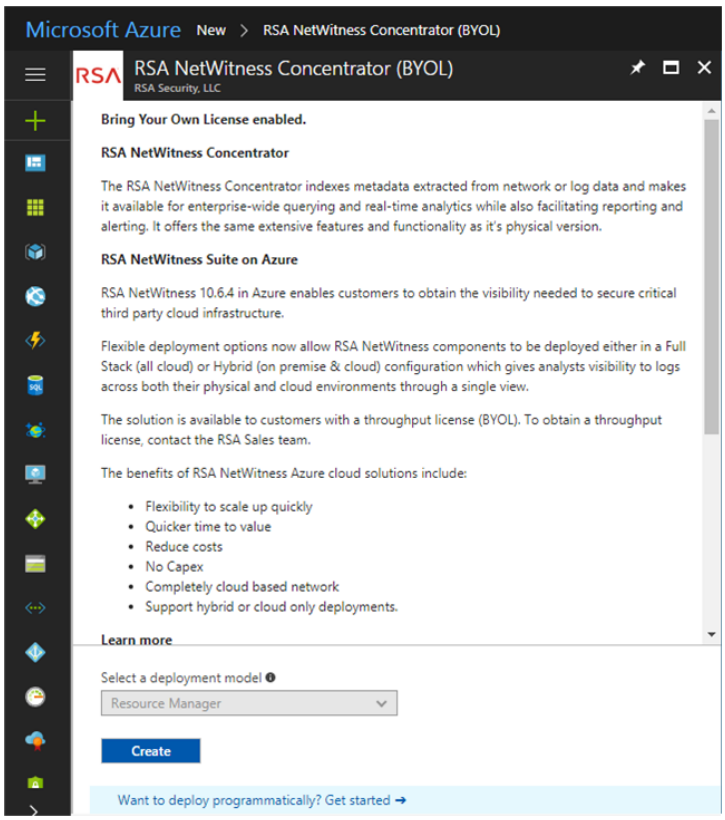
Step 2. Deploy Component Core Services in Azure

Complete the following procedure to configure core RSA NetWitness® Suite component services on a virtual machines (VMs) in the Azure Cloud environment.

1. Go to azuremarketplace.microsoft.com and sign in with your credentials.
2. Search for RSA.



3. Click RSA NetWitness® Suite core service (for example, **RSA NetWitness Concentrator**) and click **Create**.



The **Create virtual machine** wizard is displayed with the **1 Basics** section is in focus.

4. Complete Basics.

   a. Specify a VM **Name** (for example, **Concentrator**).

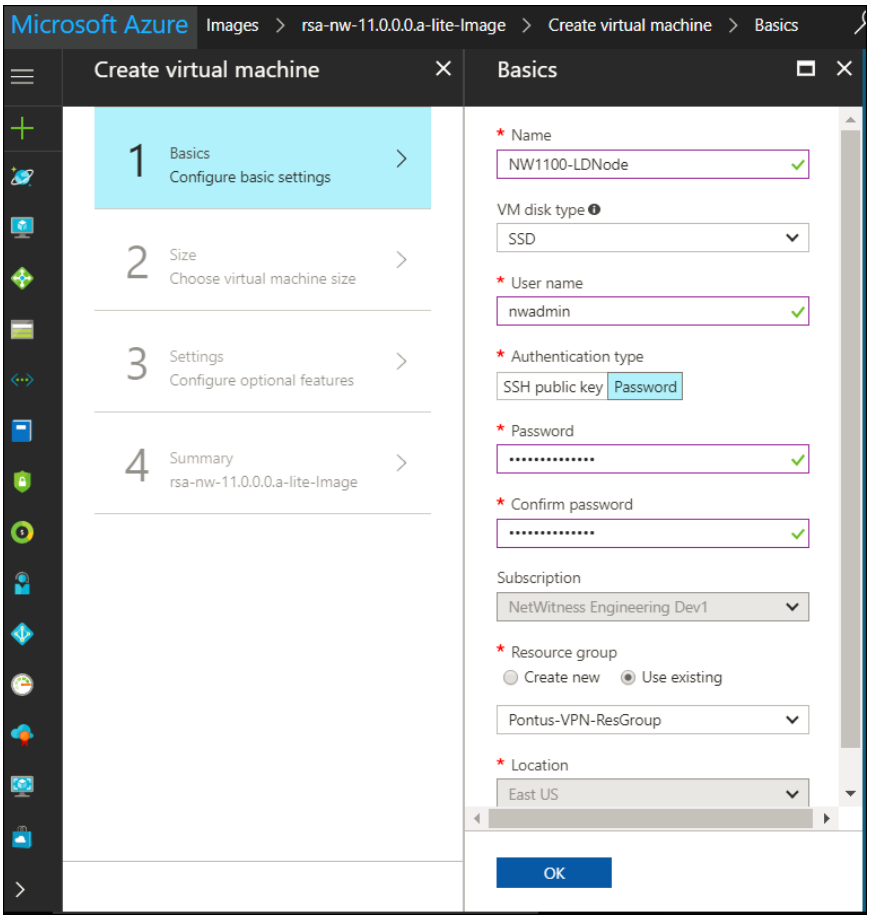
   b. Select **SSD** for the **VM disk type**of the Concentrator. Select HDD for all other components.

      Solid State Disk (SSD) performs better than a Hard Drive (HDD).

   c. Select **Password** for **Authentication type**.

   d. Enter your credentials (that is **User name** and **Password**) and **Confirm Password**.

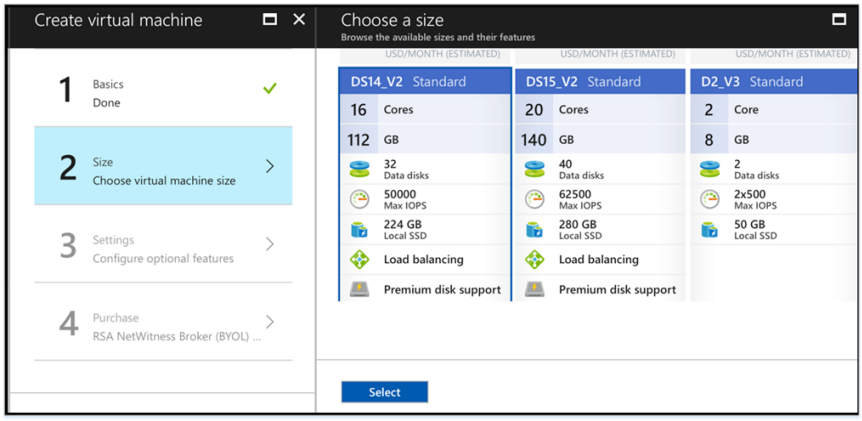
   e. Click **OK**.



Azure validates your **Basic** specifications and the **2 Size** section is in focus.

5. Click on the appropriate VM size (for example, **Standard DS14 v2** for the Concentrator) for the service and click **Select** for a VM **Size**.

   See VM Configuration Recommendations for the VM sizes RSA recommends for each service.



Azure validates your **Size** specifications and the **3 Settings** section is in focus.

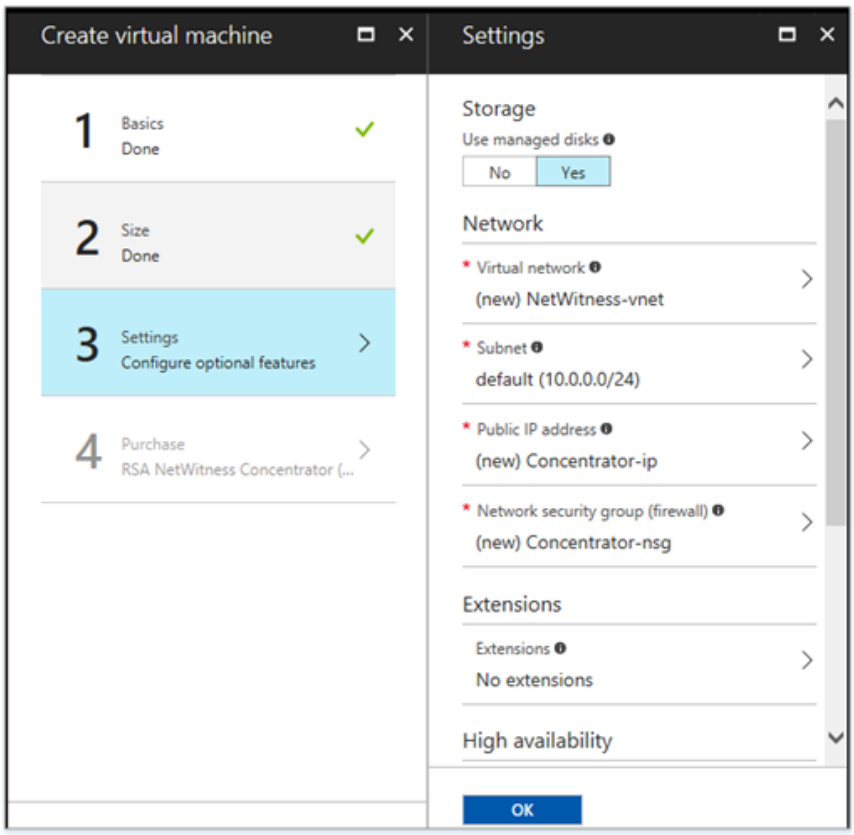
6. Specify **Settings**.

   a. In the **Storage** field, make sure **Use manage disks** is set to **Yes** .

   b. Under **Network**:

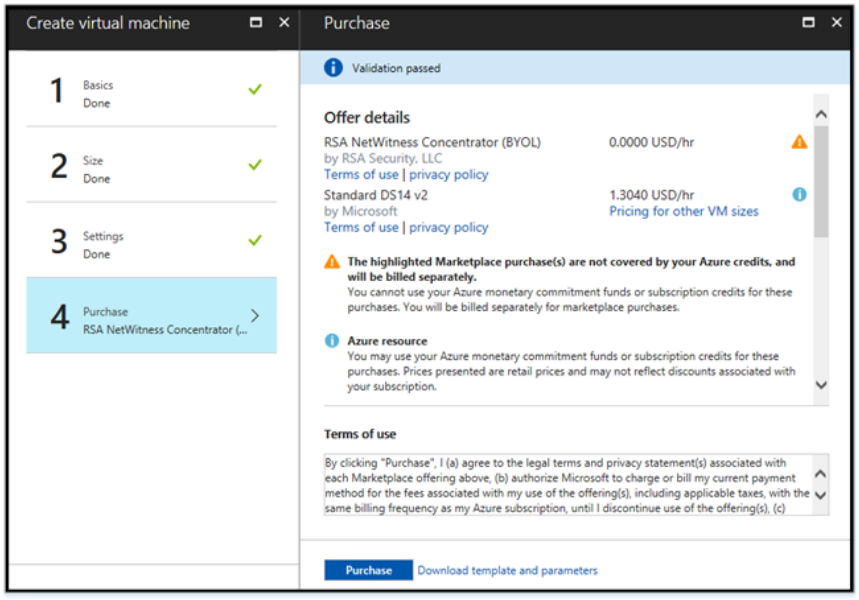
   - Adjust **Virtual network**, **Subnet** and **Public IP address** according to the requirements of your network.
   - Specify a valid **Network security group**.

     For information on Network security groups, see the Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg). Refer to Deployment: Network Architecture and Ports (https://community.rsa.com/docs/DOC-83050) for a comprehensive list of the ports you must set up for all RSA NetWitness® Suite components.



   c. Click **OK**.

Azure validates your VM and the **4 Purchase** section is in focus.



7. Click **Purchase** to create the core RSA Security Analytics component service (for example, **Concentrator**) VM in Azure.
8. Configure the host VM in RSA NetWitness® Suite 11.1.0.0.

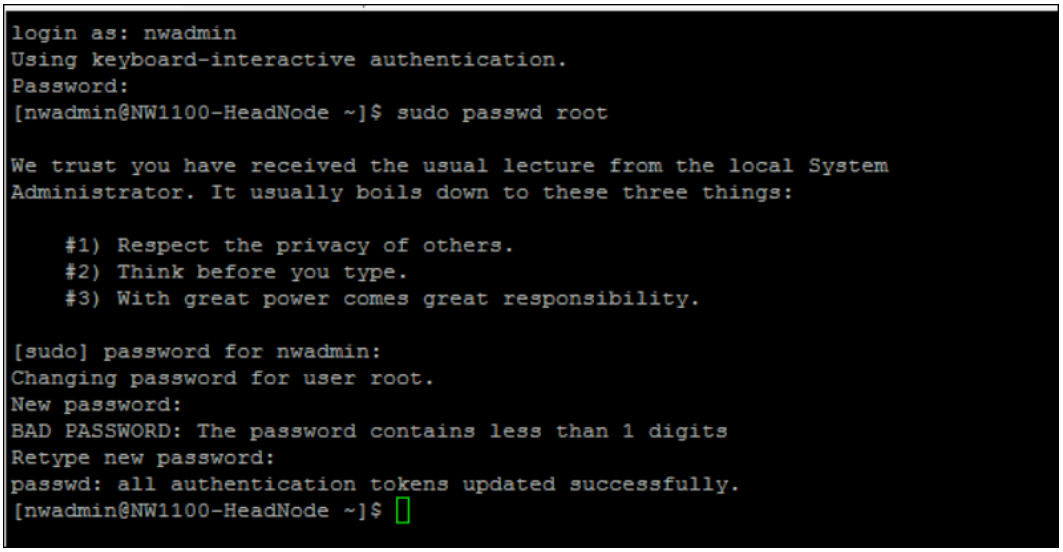
   See Step 3. Configure Host VMs in NetWitness Suite for instructions.
9. Repeat steps 1 through 8 inclusive for the rest of the core RSA NetWitness component services.

Step 3. Configure Host VMs in NetWitness Suite

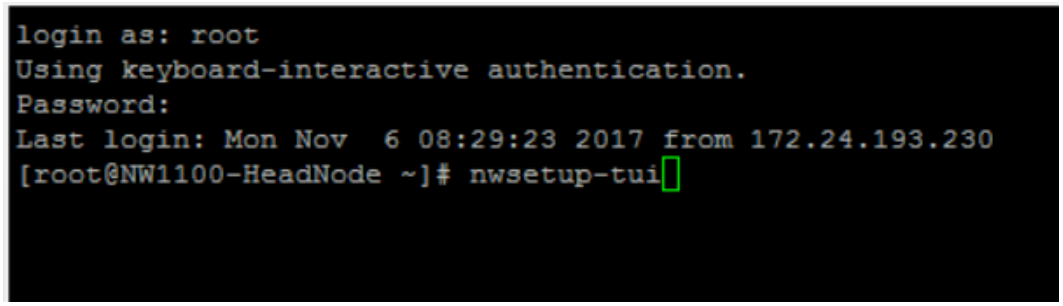
Configure individual hosts and services as described in RSA NetWitness® Suite *Host and Services Configuration Guide*. This guide also describes the procedures for applying updates and preparing for version upgrades.

Note: After you successfully create a VM, Azure assigns a default hostname to it. Refer to "Change the Name and Hostname of a Host" see *Edit a Host* (https://community.rsa.com/docs/DOC-84841) in the RSA NetWitness® Suite help for instructions on changing a hostname.

1. SSH to the host using the credentials you specified in the **1 Basics** section of the **Create VM** wizard when you created the VM in Azure (in item 4d of Step 2. Deploy Component Core Services in Azure).
2. Reset the password for **root**.

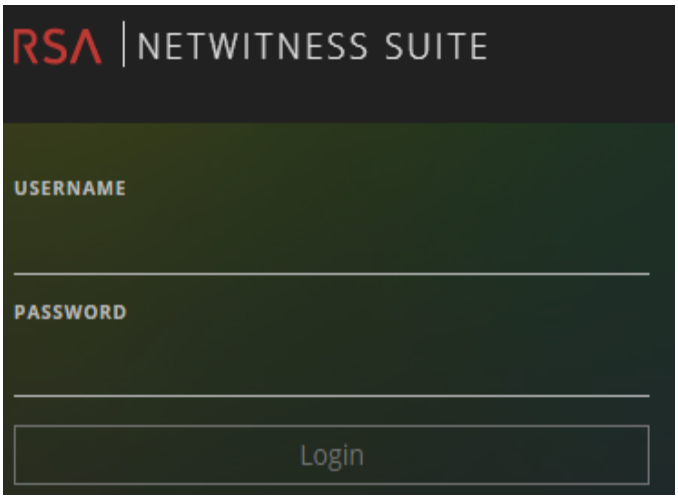


3. SSH to the host using **root** for username and the password created in the previous step and provide NetWitness Suite an IP for provisioning.



Refer to the Installation Tasks section and the Configure Hosts (Instances) section in the *AWS Deployment Guide for RSA NetWitness 11.1*.

4. Log in to RSA NetWitness Suite.



5. Go to **Administration** > **Hosts**.

   The **New Hosts** dialog is displayed with the host VMs that you created in Azure.

6. Select the hosts that you want to enable.

   The **Enable** menu option becomes active.

7. Click **Enable**.

8. Select the host you enabled.

9. Click Install and select the component you deployed in Azure (for example, Event Stream Analysis). For more information, see the *Hosts and Services Getting Started Guide for Version 11.1*.

RSA NETWITNESS® SUITE

Deployment Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Suite Deployment **5**

Basic Deployment Process 6

Process 6

NetWitness Suite High-Level Deployment Diagram 7

RSA NetWitness Suite Detailed Host Deployment Diagram 8

Deployment: Network Architecture and Ports **10**

NetWitness Suite Network Architecture Diagram 10

Comprehensive List of NetWitness Suite Host and Service Ports 11

NW Server Host 11

Archiver Host 12

Broker Host 13

Concentrator Host 14

Endpoint Hybrid or Endpoint Log Hybrid 14

Event Stream Analysis (ESA) Host 16

Log Collector Host 17

Log Decoder Host 18

Log Hybrid Host 20

Malware Host 21

Packet Decoder Host 22

Packet Hybrid Host 23

NetWitness Endpoint Insights Architecture 24

NetWitness Endpoint Insights 11.1 24

NetWitness Endpoint Insights 11.1 with Log Decoder 24

NetWitness Endpoint 4.4 Integration with NetWitness Endpoint Insights 11.1 25

Site Requirements and Safety **26**

Intended Application Uses 26

Service 26

Safety Information 26

Site Selection 26

Equipment Handling Practices 26

Power and Electrical Warnings 27

Rack Mount Warnings 27
Cooling and Air Flow 27
Antenna Placement 27

Configure Group Aggregation 28

RSA Group Aggregation Deployment Recommendations 28
Advantages of Using Group Aggregation 28
Configure Group Aggregation 30
Prerequisites 30
Set up Group Aggregation 32

NetWitness Suite Deployment

This guide describes the basic requirements of a NetWitness Suite deployment and outlines optional scenarios to address needs of your enterprise. Even in small networks, planning can ensure that all goes smoothly when you are ready to bring the hosts online.

Note: This document refers to several additional documents available on RSA Link. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

There are many factors you must consider before you deploy NetWitness Suite. The following items are just some of these factors. You need to estimate growth and storage requirements when you consider these factors.

- The size of your enterprise (that is, the number of locations and people that will use NetWitness Suite.
- The volume of packets and logs you need to process.
- The performance each NetWitness Suite user role needs to do their jobs effectively.
- The prevention of downtime (that is, how to avoid a single point of failure).
- The environment in which you plan to run NetWitness Suite
  - RSA Appliances (software running on hardware supplied by RSA)
    See the *RSA NetWitness® Suite Physical Host Installation Guide* for detailed instructions on how to deploy RSA Appliances.
  - Software Only provided by RSA:
    - On-Premises (On-Prem) Virtual Hosts
      See the *RSA NetWitness® SuiteVirtual Host Installation Guide* for detailed instructions on how to deploy on-prem virtual hosts.
    - VCloud:
      - Amazon Web Services (AWS)
        See the *RSA NetWitness® SuiteAWS Deployment Guide* for detailed instructions on how to deploy virtual hosts in AWS.
      - Azure
        See the *RSA NetWitness® SuiteAzure Deployment Guide* for detailed instructions on how to deploy virtual hosts in Azure.

Basic Deployment Process

Before you can deploy NetWitness Suite you need to:

- Consider the requirements of your enterprise and understand the deployment process.
- Have a high-level picture of the complexity and scope of a NetWitness Suite deployment.

Process

The components and topology of a NetWitness Suite network can vary greatly between installations, and should be carefully planned before the process begins. Initial planning includes:

- Consideration of site requirements and safety requirements.
- Review of the network architecture and port usage.
- Support of group aggregation on Archivers and Concentrators, and virtual hosts.

When ready to begin deployment, the general sequence is:

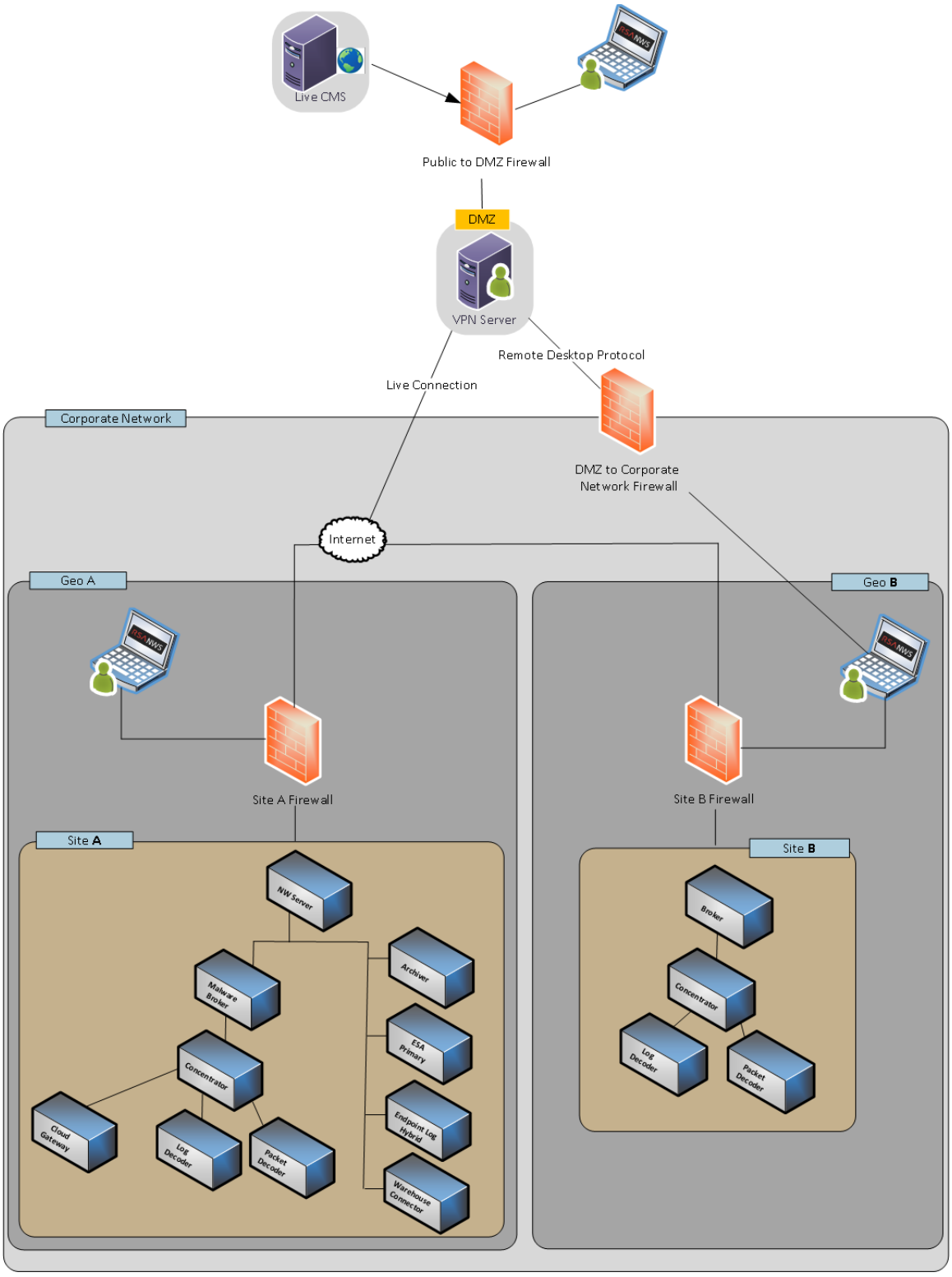
- For RSA Appliances:
  1. Install appliances and connect to the network as described in the RSA NetWitness® Suite Hardware Setup Guides and the *RSA NetWitness® Suite Physical Host Installation Guide*.
  2. Set up licensing for NetWitness Suite as described in the *RSA NetWitness® Suite Licensing Guide*.
  3. Configure individual appliances and services as described in *RSA NetWitness® Suite Host and Services Getting Started Guide*. This guide also describes the procedures for applying updates and preparing for version upgrades.
- For On-Prem virtual hosts, follow the instructions in the *RSA NetWitness® Suite Virtual Host Setup Guide*.
- For AWS, follow the instructions in the *RSA NetWitness® Suite AWS Deployment Guide*.
- For Azure, follow the instructions in the *RSA NetWitness® Suite Azure Deployment Guide*.

When updating hosts and services, follow recommended guidelines under the "Running in Mixed Mode" topic in the *RSA NetWitness Suite Host and Services Getting Started Guide*.

You should also become familiar with Hosts, Host Types, and Services as they are used in the context of NetWitness Suite also described in the *RSA NetWitness Suite Host and Services Getting Started Guide*.

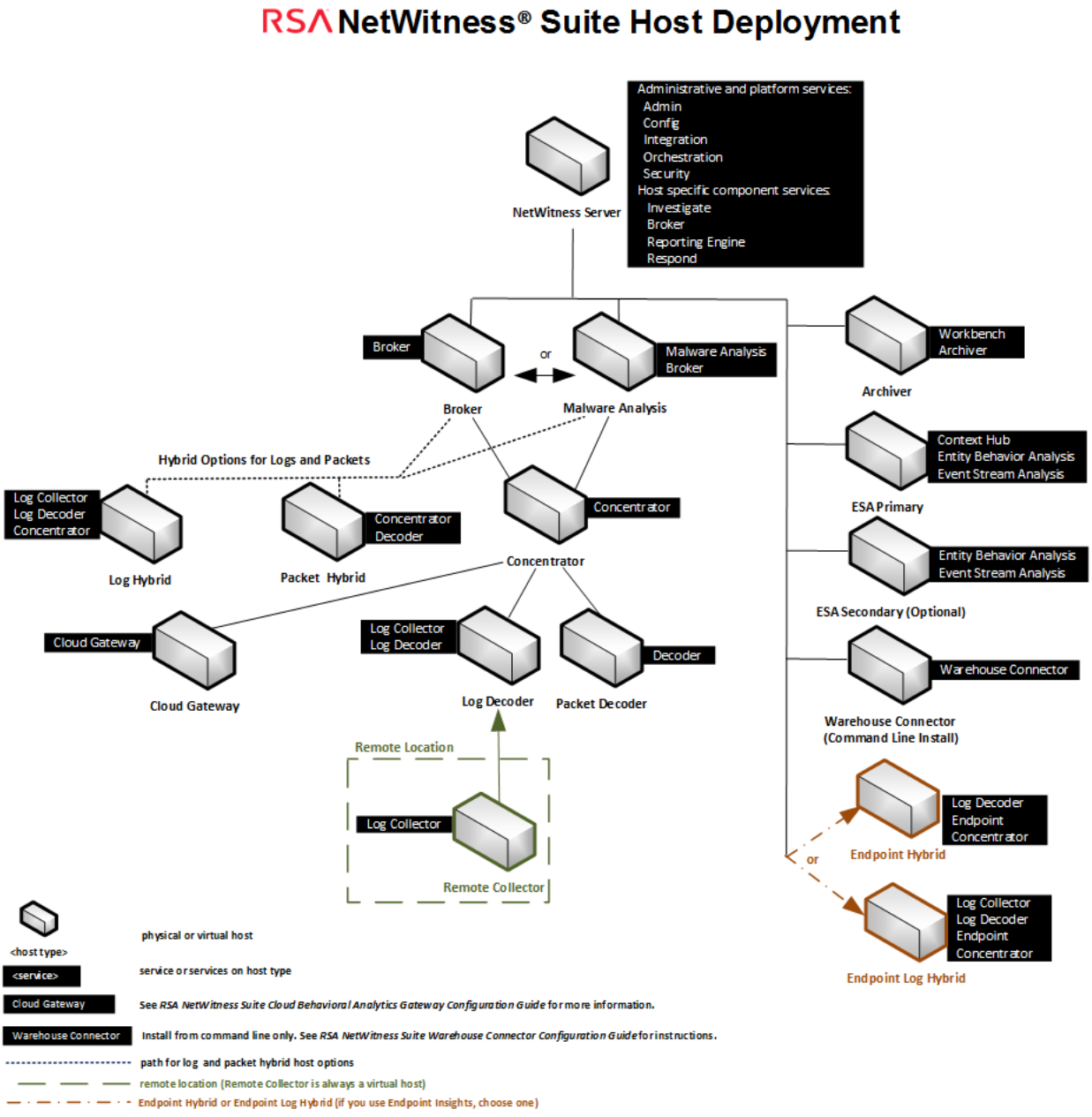
NetWitness Suite High-Level Deployment Diagram

The following diagram illustrates a basic, multi-site NetWitness Suite Deployment.



RSA NetWitness Suite Detailed Host Deployment Diagram

The following diagram is an example of a NetWitness Suite deployment hosted on physical or virtual machines. For instructions on how to install NetWitness Suite see the *Physical Host Installation Guide*, *Virtual Host Installation Guide*, *AWS Deployment Guide*, or *Azure Deployment Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.



Deployment: Network Architecture and Ports

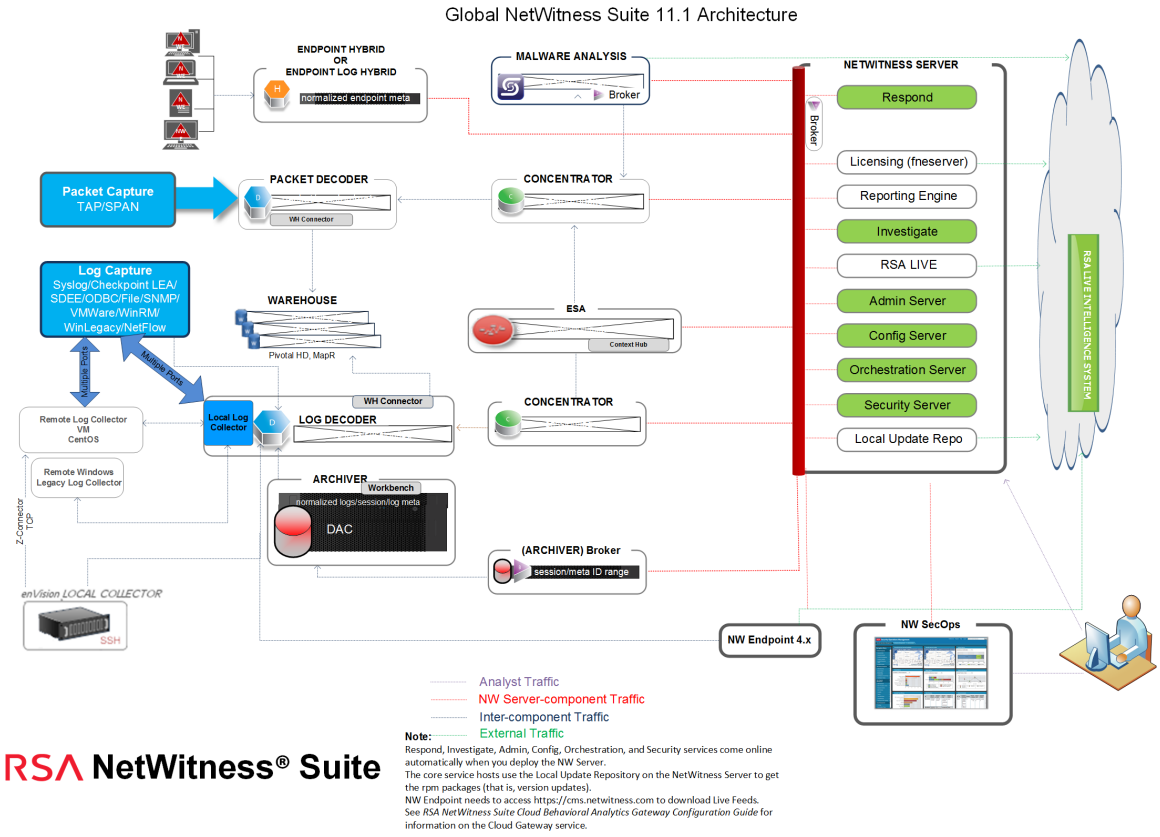
Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness Suite deployment to communicate with each other.

See NetWitness Endpoint Insights Architecture at the end of this topic for individual Endpoint Architectural diagrams.

NetWitness Suite Network Architecture Diagram

The following diagram illustrates the NetWitness Suite network architecture including all of its component products.

Note: NetWitness Suite core hosts must be able to communicate with the NetWitness Server (Primary Server in a multiple server deployment) through UDP port 123 for Network Time Protocol (NTP) time synchronization.



Comprehensive List of NetWitness Suite Host and Service Ports

Note: 1.) For ports used in event collection through the NetWitness Logs, see the "The Basics" in the *RSA NetWitness Suite Log Collection Deployment Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

This section contains the port specifications for the following hosts.

NW Server Host

Archiver Host

Broker Host

Concentrator Host

Endpoint Hybrid/Endpoint Log Hybrid Host

Event Stream Analysis Host

Log Collector Host

Log Decoder Host

Log Hybrid Host

Malware Host

Packet Decoder Host

Packet Hybrid Host

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	NW Server	TCP 443, 80	nginx - NetWitness UI
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
NW Hosts	NW Server	TCP 15671	RabbitMQ Management UI
Admin Workstation	NW Server	TCP 22	SSH
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Server	NW Server	TCP 50003, 50103, 56003	Broker Ports
NW Server	NW Server	TCP 5671	RabbitMQ-amqp
NW Server	NW Server	UDP 50514	Audit Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	NW Server	TCP 7000, 7003, 7009, 7010	Launch Ports
NW Server	NW Server	TCP 50006, 50106, 56006	NetWitness Appliance Ports
NW Hosts	NW Server	UDP 123	NTP
NW Hosts	NW Server	TCP 27017	MongoDB
NW Server	NW Server	UDP 123	NTP
NW Server	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations
NW Server	NW Endpoint	TCP 443, 9443	For NW Endpoint 4.x integrations

Archiver Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Archiver	TCP 15671	RabbitMQ Management UI
Admin Workstation	Archiver	TCP 22	SSH
NW Server	Archiver	TCP 56008 (SSL), 50008 (Non-SSL), 50108 (REST)	Archiver Application Ports
NW Server	Archiver	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Archiver	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.

Source Host	Destination Host	Destination Ports	Comments
NW Server	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Non-SSL), 50107 (REST), UDP 514	Workbench Application Ports
Archiver	Archiver	UDP 50514	Audit Data
Archiver	Archiver	UDP 123	NTP
Archiver	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Broker Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 15671	RabbitMQ Management UI
Admin Workstation	Broker	TCP 22	SSH
NW Server	Broker	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
NW Server	Broker	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Broker	Broker	UDP 50514	Audit Data
Broker	Broker	UDP 123	NTP
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Concentrator Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Concentrator	TCP 15671	RabbitMQ Management UI
Admin Workstation	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW Server	Concentrator	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Concentrator	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Concentrator	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations
Concentrator	Concentrator	UDP 50514	Audit Data
Concentrator	Concentrator	UDP 123	NTP

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint 11.1 Agent	Endpoint Hybrid or Endpoint Log Hybrid	TCP 443	NGINX HTTPS

Source Host	Destination Host	Destination Ports	Comments
Endpoint 11.1 Agent	Log Decoder or Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Server	Log Decoder (External)	TCP 50102, 56202, 50202	To forward meta to an external Log Decoder
NW Server	Endpoint Hybrid or Endpoint Log Hybrid	TCP 7050	UI web traffic
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5672	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

Endpoint Hybrid or Endpoint Log Hybrid with NetWitness Endpoint 4.4

Source Host	Destination Host	Destination Ports	Comments
NW Console Server (4.4.0.2 or later)	Endpoint Hybrid	TCP 443	NGINX HTTPS
Meta Service	Log Decoder	TCP 50102, 56202, 50202	NGINX HTTPS To forward meta to a Log Decoder Endpoint Hybrid or Endpoint Log Hybrid with NWE 4.4

Event Stream Analysis (ESA) Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI
Admin Workstation	ESA	TCP 22	SSH
NW Server, ESA Secondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 50030 (SSL)	ESA Application Port
NW Server	ESA	TCP 50035 (SSL)	ESA Application Port
NW Server	ESA	TCP 50036 (SSL)	ESA Application Port
NW Server	ESA	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
ESA	cms.netwitness.com	TCP 443	Live
ESA	NFS Server	TCP 111 2049 UDP 111 2049	NTP
ESA	Active Directory	636 (SSL)/389 (Non-SSL)	
NW Server	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Non-SSL)	
ESA Primary	ESA Primary	TCP 7007	Launch Port

Source Host	Destination Host	Destination Ports	Comments
ESA Primary	ESA Primary	UDP 50514	Audit Data
ESA Primary	ESA Primary	UDP 123	NTP

Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Collector	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.	
Log Event Sources	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Log Collection Ports
Log Event Sources	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Log Collection FTP/S Ports
NW Server	Log Collector	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Log Collector	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Collector	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Collector	Log Collector	UDP 50514	Audit Data
Log Collector	Log Collector	UDP 123	NTP
Log Collector	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC installations

Log Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Log Event Sources	See *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.	

Source Host	Destination Host	Destination Ports	Comments
Log Event Sources	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Decoder	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Decoder	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Decoder	Log Decoder	UDP 50514	Audit Data
Log Decoder	Log Decoder	UDP 123	NTP
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.	
Log Event Sources	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Log Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
Admin Workstation	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malware Application Ports
NW Server	Malware	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Malware	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Malware	TCP 5432	Postgresql
NW Server	Malware	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports

Source Host	Destination Host	Destination Ports	Comments
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	Malware	UDP 50514	Audit Data
Malware	Malware	UDP 123	NTP
Malware	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Packet Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Decoder	TCP 22	SSH
NW Server	Packet Decoder	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Decoder	Packet Decoder	UDP 50514	Audit Data
Packet Decoder	Packet Decoder	UDP 123	NTP

Source Host	Destination Host	Destination Ports	Comments
Packet Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

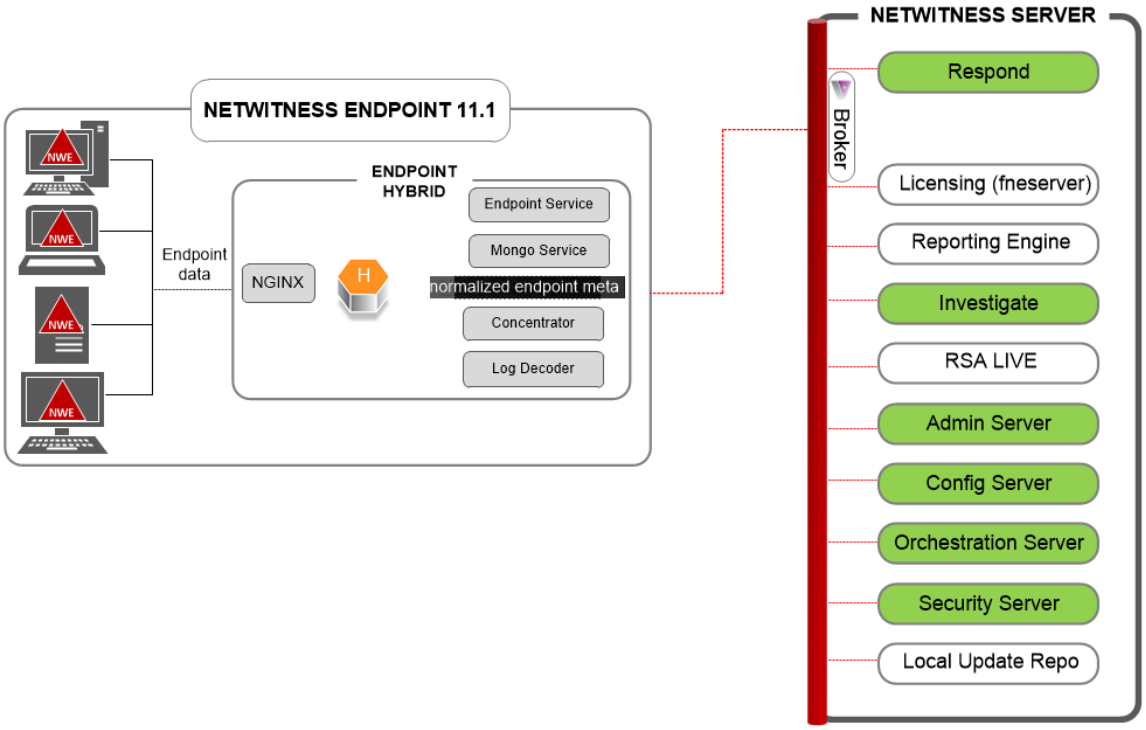
Packet Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Hybrid	TCP 22	SSH
NW Server	Packet Hybrid	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Packet Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Hybrid	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

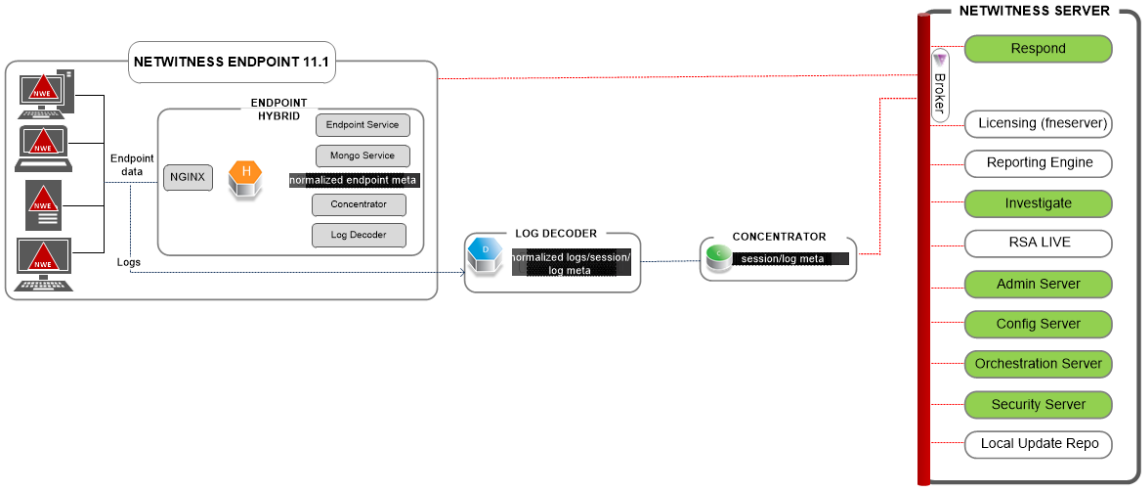
NetWitness Endpoint Insights Architecture

The following diagrams illustrate the NetWitness Endpoint Insights network architecture.

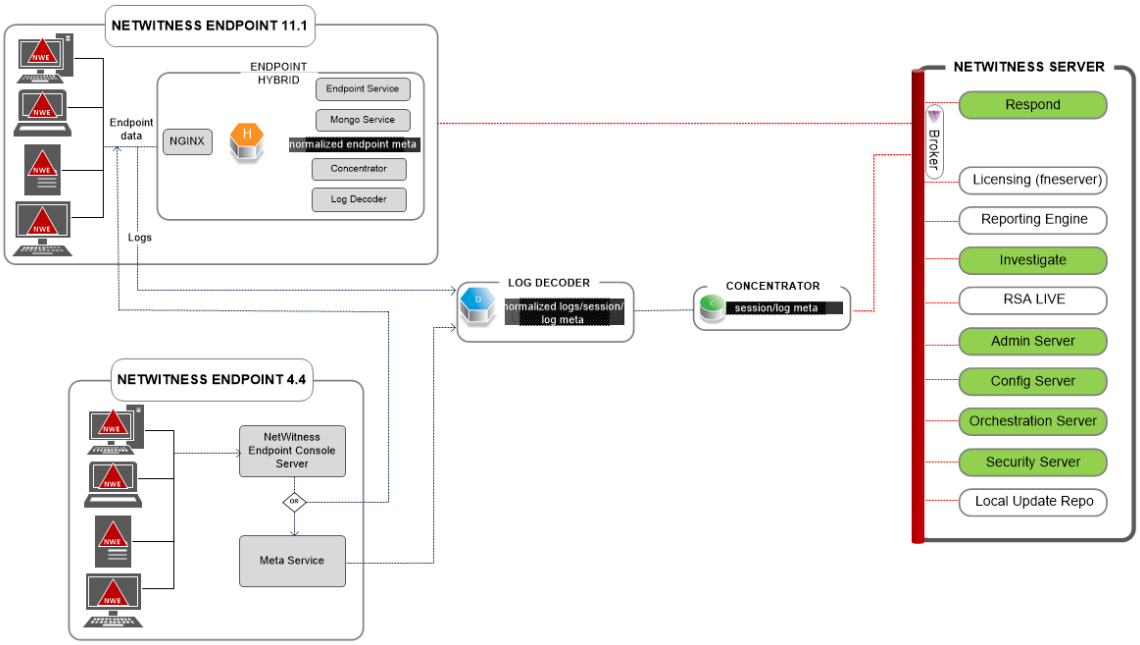
NetWitness Endpoint Insights 11.1



NetWitness Endpoint Insights 11.1 with Log Decoder



NetWitness Endpoint 4.4 Integration with NetWitness Endpoint Insights 11.1



For more information on the services running on Endpoint Hybrid, see *RSA NetWitness Endpoint Insights Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Site Requirements and Safety

Make sure that you read this topic thoroughly and observe all warnings and precautions prior to installing or maintaining your RSA devices.

Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE) that may be installed in offices, schools, computer rooms, and similar indoor commercial type locations. This device is not intended for any connection to an outdoor type cable.

Service

There are no user-serviceable components inside of this device. Please contact Customer Care in the event of a malfunction. In a fault condition, high temperatures may arise inside the system causing an alarm signal. In the event of the alarm signal, immediately disconnect the device from the power source and contact Customer Care. Further operation of the device will be unsafe and may cause personal injury or property damage.

Safety Information

Site Selection

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean, dry, and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat, including direct sunlight and radiators.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cords, because they serve as the product′s main power disconnect.

Equipment Handling Practices

Reduce the risk of personal injury or equipment damage by:

- Conforming to local occupational health and safety requirements when moving and lifting equipment.
- Using mechanical assistance or other suitable assistance when moving and lifting equipment.
- Reducing the weight for easier handling by removing any easily detachable components.

Power and Electrical Warnings

Caution: The power button, indicated by the standby power marking, DOES NOT completely turn off the system AC power; 5V standby power is active whenever the system is plugged in. To remove power from system, you must unplug the AC power cord(s) from the wall outlet.

- Do not attempt to modify or use an AC power cord if it is not the exact type required. A separate AC cord is required for each system power supply.
- This product contains no user-serviceable parts. Do not open the system.
- When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing it from the server.

Rack Mount Warnings

- The equipment rack must be anchored to an unmovable support to prevent it from tipping when a server or piece of equipment is extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.
- Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Extend only one piece of equipment from the rack at a time.
- To avoid risk of potential electric shock, a proper safety ground must be implemented for the rack and each piece of equipment installed in it.

Cooling and Air Flow

Installation of the equipment should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Antenna Placement

This equipment should be installed and operated with a minimum distance of 7cm between the radiator and your body. The antennas used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Configure Group Aggregation

You use Group Aggregation to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them. You can configure multiple Archiver services or Concentrator services to efficiently aggregate from multiple Log Decoder services to improve query performance on the data:

- Stored in the Archiver.
- Processed through the Concentrator.

RSA Group Aggregation Deployment Recommendations

RSA recommends the following deployment for Group Aggregation.

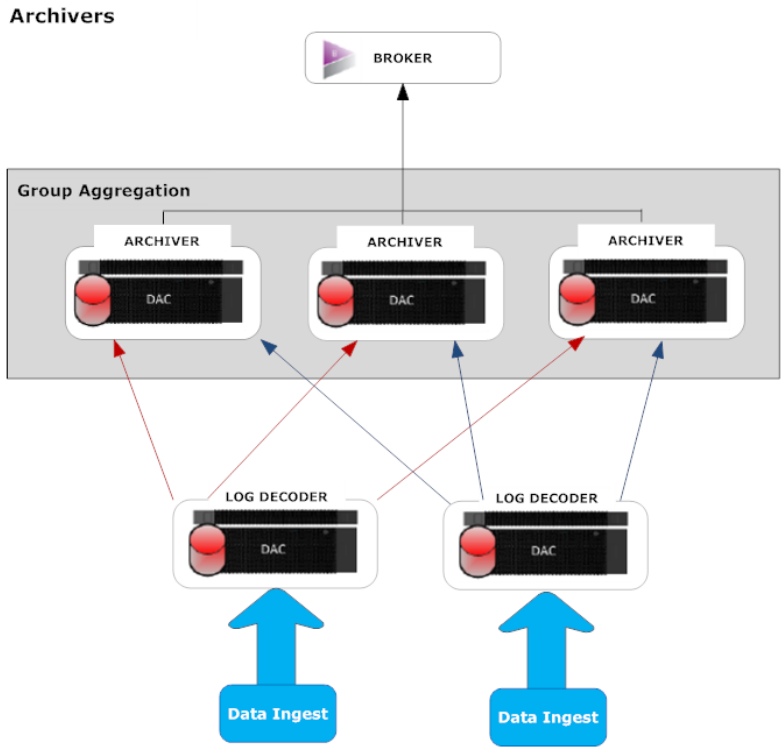
- 1 - 2 Log Decoders
- 3 - 5 Archivers or Concentrators

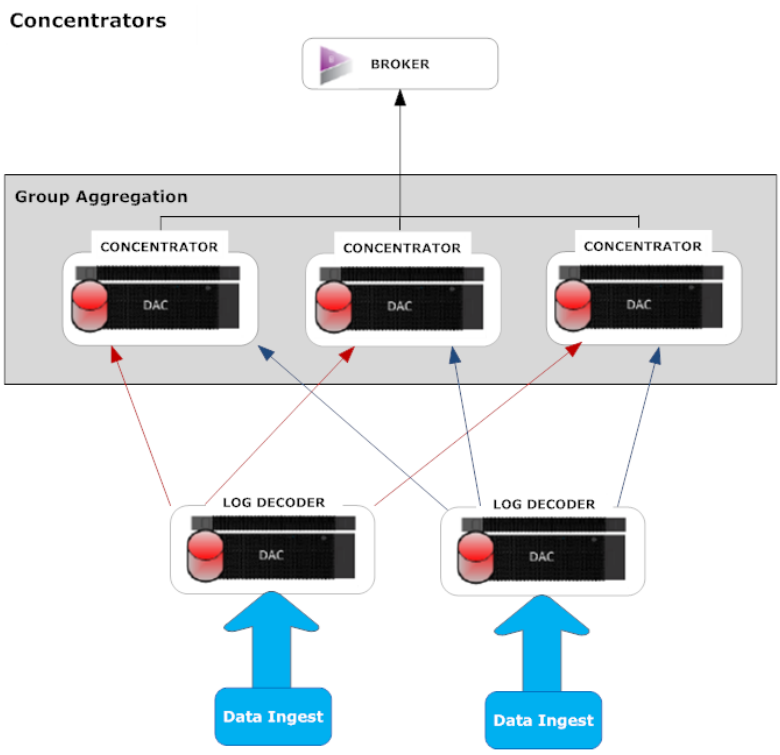
Advantages of Using Group Aggregation

Group Aggregation:

- Increases the speed of RSA NetWitness® Suite queries.
- Improves the performance of aggregate queries (Count and Sum) on the environment.
- Enhances investigation service performance.
- Gives you the option of storing data for a longer duration for investigation purposes.

The following diagram illustrates Group Aggregation.


Archivers
BROKER
Group Aggregation
ARCHIVER
DAC
ARCHIVER
DAC
ARCHIVER
DAC
LOG DECODER
DAC
LOG DECODER
DAC
Data Ingest
Data Ingest


Concentrators
BROKER
Group Aggregation
CONCENTRATOR
DAC
CONCENTRATOR
DAC
CONCENTRATOR
DAC
LOG DECODER
DAC
LOG DECODER
DAC
Data Ingest
Data Ingest

You can have any number of Archivers or Concentrators grouped together and form an aggregation group. The Archiver or Concentrator services in the group divide all the aggregated session between them based on the number of sessions defined in the Aggregate Max Sessions parameter.

For example, in an aggregation group containing two Archiver services or two Concentrator services with the Aggregate Max Sessions parameter set to 10000 the services would divide the session between themselves as illustrated in the following table.

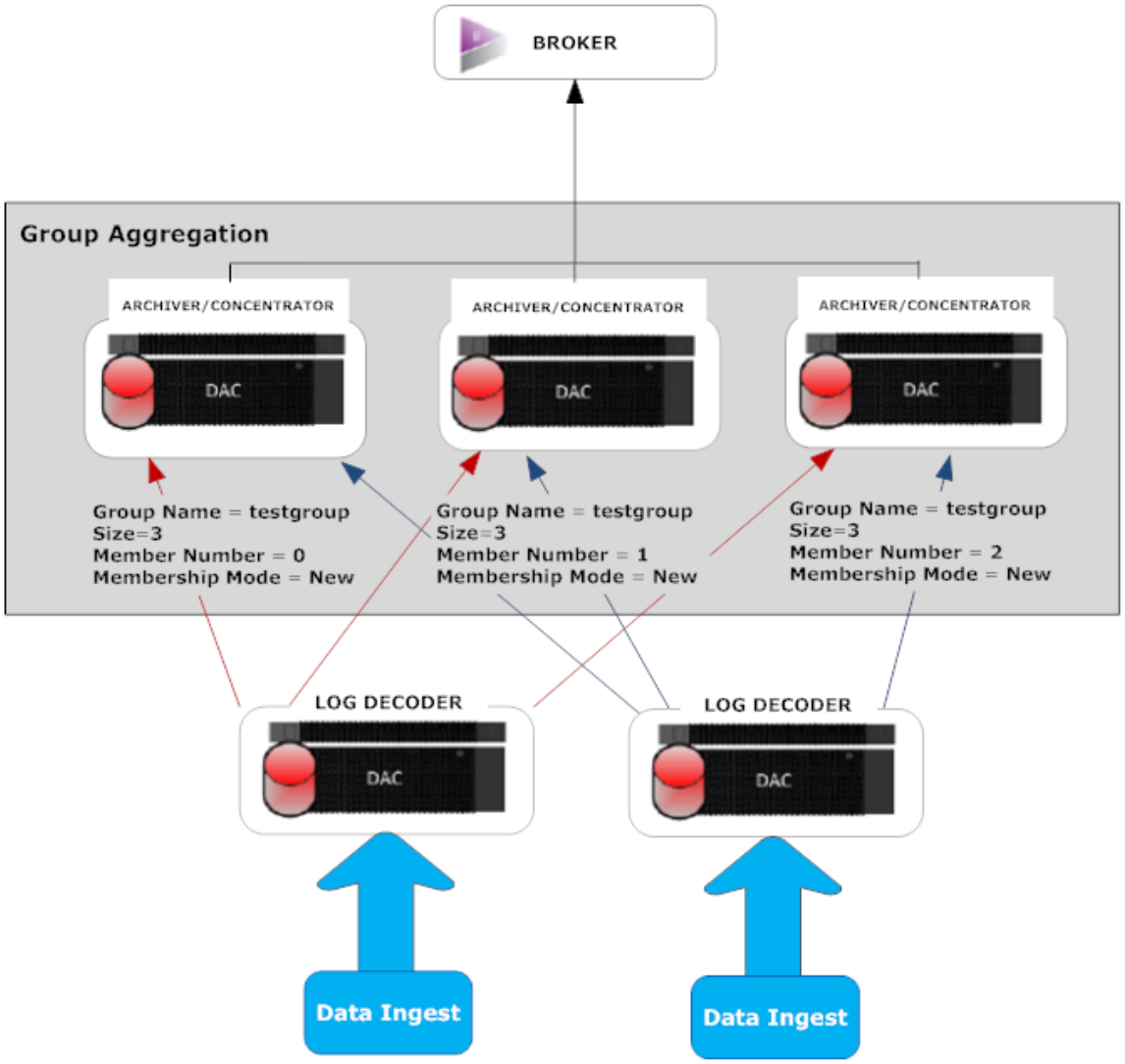
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

Configure Group Aggregation

Complete this procedure to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.

Prerequisites

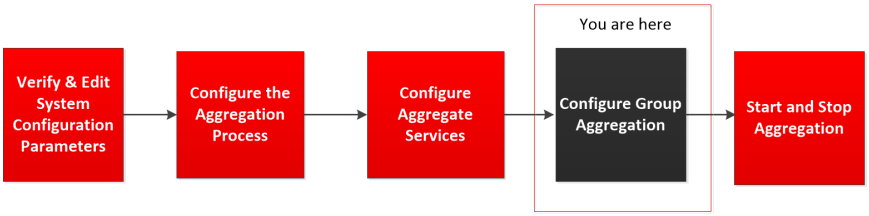
Plan the network design for group aggregation. The following figure is an example of a group aggregation setup.



Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

Parameter	Description
Group Name	It determines the group to which the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All Archiver or Concentrators services in the group should have the same group name.
Size	It determines the number of Archiver or Concentrator services in the aggregation group.

Member Number	It determines the position of the Archiver or Concentrator in the aggregation group. For a group of size N, member number from 0 to N-1 must be set on each of the Archiver or Concentrators services in the aggregation group. For example: If the size of the aggregation group is 2, the member number of one of the Archiver or Concentrator service should be set to 0 and the member number of the other Archiver or Concentrator should be set to 1.
Membership Mode	There are two membership modes: New and Replace. New: Adding a new Archiver or Concentrator service as a member to the existing aggregation group or creating an aggregation group. The Archiver or Concentrator service does not aggregate any existing sessions from the service as other members of the group would have already aggregated all the sessions on the service. This Archiver or Concentrator service will only aggregate new sessions as they appear on the service. Replace: Replacing an existing aggregation group member. The Archiver or Concentrator will begin aggregation from the oldest session available on the service it is aggregating from. **Note:** This parameter has an effect only when no sessions have been aggregated from the service. After some sessions are aggregated, this parameter has no effect.



Set up Group Aggregation

Complete the following procedure to set up group aggregation.

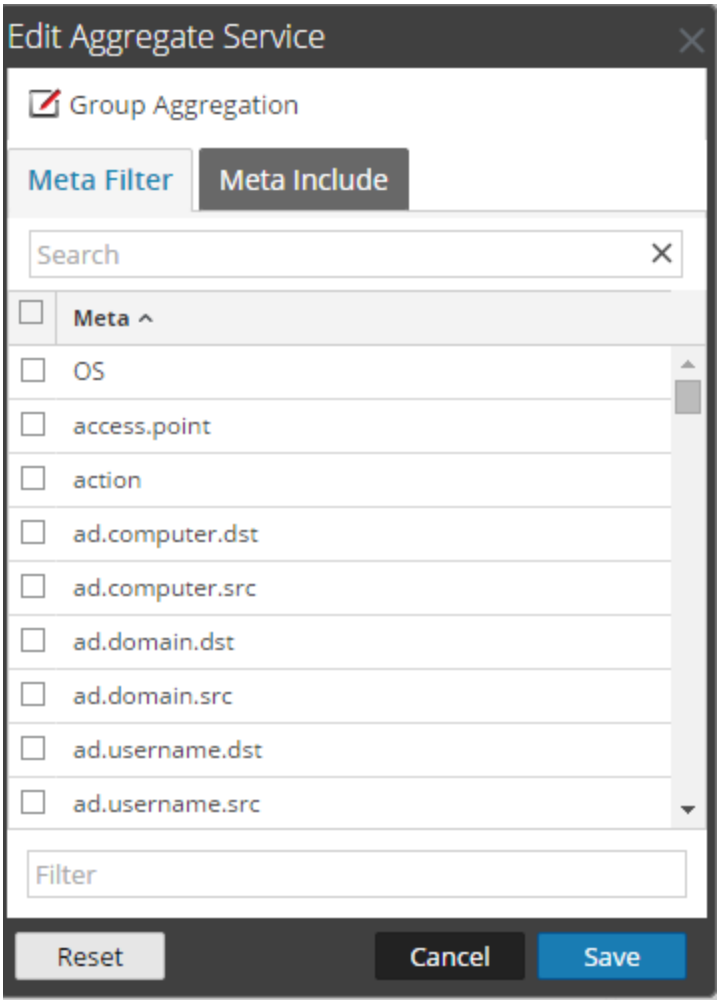
1. Configure multiple Archiver or Concentrator services in your environment. Make sure that you add the same Log Decoder as data source to all the services.
2. Perform the following on all the Archiver or Concentrator services that you want to be part of aggregation group:
   a. In the **main menu**, select **ADMIN > Services**.

b. Select the Archiver or Concentrator service, and in the **Actions** column, select **View > Config**.
The Device Config view of the Archiver or Concentrator is displayed.

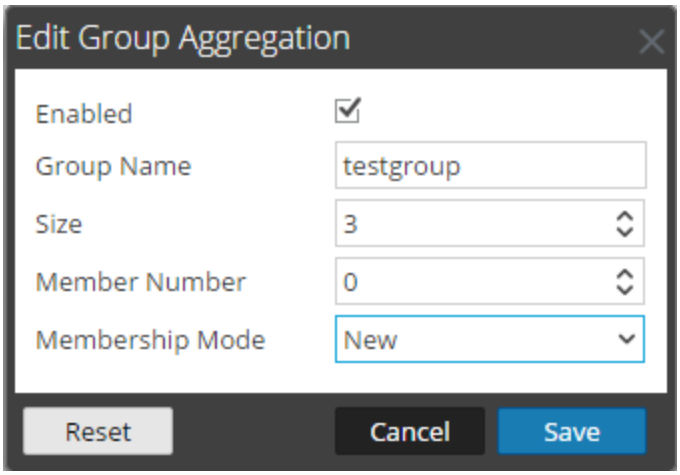
c. Under **Aggregate Services** section, select the Log Decoder device.

d. Click Toggle Service to change the status of the Log Decoder to offline if it is online.

e. Click .
The **Edit Aggregate Service** dialog is displayed.



f. Click Group Aggregation.
The **Edit Group Aggregation** dialog is displayed.



g. Select the **Enabled** checkbox and set the following parameters:

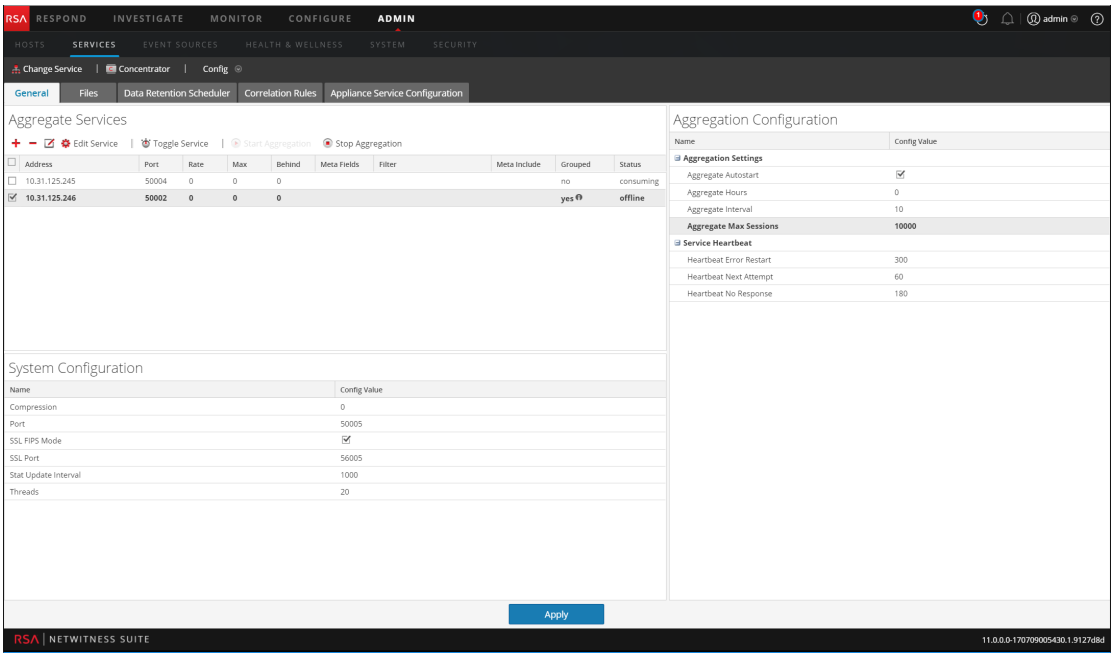
   In the **Group Name** field, type the group name.
   In the **Size** field, select the number of Archiver or Concentrator services in the aggregation group.
   In the **Member Number** field, select the position of the Archiver or Concentrator in the aggregation group.
   In the **Membership Mode** drop-down menu, select the mode.

h. Click **Save**.

i. In the Device Config View page, click **Apply**.

j. Perform **Step b** to **Step i** on all other Archiver or Concentrator services that need to be part of group aggregation.

3. In the **Aggregation Configuration** section, set the **Aggregate Max Sessions** parameter set to **10000**.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Config
General
Files
Data Retention Scheduler
Correlation Rules
Appliance Service Configuration
Aggregate Services
Edit Service
Toggle Service
Start Aggregation
Stop Aggregation
Address
Port
Rate
Max
Behind
Meta Fields
Filter
Meta Include
Grouped
Status
10.31.125.245
50004
0
0
0
no
consuming
10.31.125.246
50002
0
0
0
yes
offline
Aggregation Configuration
Name
Config Value
Aggregation Settings
Aggregate Autostart
Aggregate Hours
0
Aggregate Interval
10
Aggregate Max Sessions
10000
Service Heartbeat
Heartbeat Error Restart
300
Heartbeat Next Attempt
60
Heartbeat No Response
180
System Configuration
Name
Config Value
Compression
0
Port
50005
SSL FIPS Mode
SSL Port
56005
Stat Update Interval
1000
Threads
20
Apply
RSA | NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

RSA NETWITNESS® SUITE

User Guides

for Version 11.1.0.0

RSA NETWITNESS® SUITE

Alerting with ESA Correlation Rules User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Getting Started with ESA **9**

Best Practices 9

Understand Event Stream Analysis Rule Types 9

Best Practices for Writing Rules 11

Best Practices for Working with RSA Live Rules 12

Best Practices for Deploying Rules 12

Best Practices for System Health 13

Troubleshoot ESA 13

Troubleshoot ESA Services 14

Troubleshoot RSA Live Rules for ESA 15

Troubleshoot Deployments 16

Troubleshoot Rules 17

Steps to Troubleshoot Memory Issues with an ESA Service Offline 17

View Memory Metrics for Rules 23

Prerequisites 23

Procedures 24

How ESA Generates Alerts **27**

Sensitive Data 27

How ESA Treats Sensitive Data from Core Services 27

Advanced EPL Rule 28

Enrichment Source 28

ESA Rule Types **29**

Starter Pack Rules 29

Trial Rules Mode 29

Role Permissions 30

Practice with Starter Pack Rules 31

Rule Library 31

Procedure 32

Work with Trial Rules **35**

Deploy Rules as Trial Rules 35

Procedure 35
View Memory Metrics for Rules Using Trial Mode 37
Prerequisites 38
Procedures 38

Add Rules to the Rule Library 41

Download Configurable RSA Live ESA Rules 41
Prerequisites 42
Procedure 42
Customize an RSA Live ESA Rule 43
Add a Rule Builder Rule 44
Step 1. Name and Describe the Rule 45
Step 2. Build a Rule Statement 46
To Add a Whitelist 48
To Add a Blacklist 49
Example: Blacklist 49
Example: Ignoring Case, Strict Pattern Matching, and Using The Is Not Null Operator 50
Example Results 55
Example: Grouping the Rule Results 56
Example: Working with Numeric Operators 58
Step 3. Add Conditions to a Rule Statement 59
Add an Advanced EPL Rule 61
Prerequisites 61
Procedure 62
Event Processing Language (EPL) 63
ESA Annotations 64
To Use Identifiers with Alert Notification Suppression: 65
Sample Advanced EPL Rules 67
EPL #1: 67
EPL #2: 68

EPL #3: 69
EPL #4: Using NamedWindows and match recognize 70
EPL #5: Using Every @RSAAlert(oneInSeconds=0, identifiers={"user_src"}) 71
EPL #6: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"}) 71
EPL #7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"}) 72
EPL #8: using groupwin , time_length_batch and unique 73
EPL #9: using groupwin , time_length_batch and unique 73
EPL #10: using groupwin , time_length_batch and unique 74
EPL #11: @RSAAlert(oneInSeconds=0) 75
Working with Rules 75
Edit, Duplicate or Delete a Rule 76
Edit a Rule 76
Duplicate a Rule 76
Delete a Rule 76
Filter or Search for Rules 77
Filter 77
Search 78
Import or Export Rules 78
Import ESA Rules 78
Export 79
Choose How to be Notified of Alerts 81
Notification Methods 82
Add Notification Method to a Rule 83
Prerequisites 84
Procedure 84
Add a Data Enrichment Source 87
Sample Rule with Enrichment 88
Configure a Database Connection 90

Procedure 91
Enrichment Sources 93
Configure a Database as Enrichment Source 93
Configure In-Memory Table as an Enrichment Source 95
Configure an Ad hoc In-Memory Table 96
Add a Recurring in-Memory Table 99
Workflow 101
Configure an In-Memory Table Using an EPL Query 102
Step 1: Create Your Rule 103
Step 2: Create the Enrichment 106
Step 3: Add the Enrichment to the Rule 106
Configure Warehouse Analytics as an Enrichment Source 108
Configure Context Hub List as an Enrichment Source 109
Add an Enrichment to a Rule 113
Procedure 113
Deploy Rules to Run on ESA 115
How Deployment Works 115
Deployment Steps 116
Step 1. Add a Deployment 116
Step 2. Add an ESA Service 117
Step 3. Add and Deploy Rules 118
Additional Deployment Procedures 120
Delete ESA Service in a Deployment 120
Edit or Delete Rule in a Deployment 120
Edit a Rule 121
Delete a Rule 121
Edit or Delete a Deployment 121
Show Updates to a Deployment 122
View ESA Stats and Alerts 125
View Stats for ESA Service 125
Procedures 125

View a Summary of Alerts 126

ESA Alert References 129

New Advanced EPL Rule Tab 130
What do you want to do? 130
Related Topics 130
Advanced EPL Rule 130
Build a Statement Dialog 134
What do you want to do? 134
Related Topics 134
Build a Statement Dialog 134
Deploy ESA Rules Dialog 139
What do you want to do? 139
Related Topics 139
Deploy ESA Rules Dialog 139
Deploy ESA Services Dialog 141
What do you want to do? 141
Related Topics 141
Deploy ESA Services Dialog 141
Rule Builder Tab 143
What do you want to do? 143
Related Topics 143
Rule Builder 144
Rules Tab 150
What do you want to do? 150
Related Topics 150
Rule Builder 151
Rules Tab Options Panel 152
Rules Section 152
Deployments Section 153
Rule Library Panel 154
Rule Library Toolbar 155
Rule Library List 155
Deployment Panel 157

ESA Services 157
ESA Rules 158
Rule Syntax Dialog 160
Rule Syntax Dialog 160
Services Tab 162
What do you want to do? 162
Related Topics 162
Services 162
Deployed Rule Stats Panel 164
Settings Tab 166
What do you want to do? 166
Related Topics 166
Settings 166
Meta Key References 167
Enrichment Sources 167
Database Connections 168
Updates to the Deployment Dialog 170
What do you want to do? 170
Related Topics 170
Deployment Dialog 170

Getting Started with ESA

This topic covers quick start topics for RSA NetWitness® Suite Event Stream Analysis (ESA) to help you get started in using ESA. The following topics are designed to assist you in working with ESA Correlation Rules.

- Best Practices helps you to understand how to best set up, deploy, and create rules.
- Troubleshoot ESA helps you to troubleshoot different aspects of ESA, including rule writing and deployment.
- View Memory Metrics for Rules helps you to work with memory metrics to understand memory usage for ESA services.

There are two ESA services that can run on an ESA host:

- Event Stream Analysis (ESA Correlation rules)
- Event Stream Analytics Server (ESA Analytics)

The first service is the Event Stream Analysis service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live. This user guide covers alerting using ESA Correlation Rules. For information on configuring ESA Correlation Rules, see the "Configure ESA Correlation Rules" section of the *ESA Configuration Guide*.

The second service is the ESA Analytics service, which is used for Automated Threat Detection. Because the ESA Analytics service uses preconfigured ESA Analytics modules for Automated Threat Detection, you do not have to create or download rules to use it. For information on the ESA Analytics service, see the *Automated Threat Detection Configuration Guide* and the "Configure ESA Analytics" section of the *ESA Configuration Guide*.

Best Practices

Best practices provide guidelines to help you write and manage rules, deploy rules, and maintain system health for your ESA services.

Understand Event Stream Analysis Rule Types

The Event Stream Analysis service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators. However, when working with Event Stream Analysis, you should be aware of the factors that affect resource usage in order to create effective rules.

Each event that is received by ESA is evaluated to determine if it may trigger a rule. There are three types of rules that can be deployed in order to determine what the ESA engine should do with the incoming event. Each of these rule types have different impacts on system resource utilization. All three rule types may be created via the Rule Builder, Advanced EPL rules, or downloaded via RSA Live. The table below lists the rule type and the impact this rule may have on system resources.

Rule Type	Description
Simple Filter Rule	This rule has no correlation to other events. At ingestion time, this rule is evaluated against a set of conditions, and if those conditions are met an alert is generated. If no conditions match, the event is quickly released by the engine to free up memory usage. These rules do not take up memory since the events are not retained beyond the initial evaluation. The memory resource usage does not increase as more simple filter rules are deployed. However, if the filter condition is too generic, it is possible that this rule can generate too many alerts, which will strain the system resources for the storage and retrieval of these alerts. For example, you might write a rule to generate an alert when HTTP network activity arrives over a non-standard HTTP port.
Event Window Rule	This rule evaluates a set of events over a time period for specific conditions. At ingestion time, the rule is evaluated against a set of conditions. If those conditions are met, the event is retained in memory for a specific amount of time. After the specified time passes, the events are removed from the time window if the number of events collected does not meet the threshold to trigger an alert. The memory consumption of such rules are highly dependent on the incoming event rate (traffic), the amount of data per event, and the time length specified in the event window. Each matching event is retained in memory until the time window has passed, so the longer the time window, the greater the potential volume. For example, you might write a rule that generates an alert if a user fails to log into any system five times within a ten minute time frame.

Rule Type	Description
Followed By Rule	This rule evaluates a chain of incoming events to determine if the sequence of events matches a particular condition. At ingestion time, the rule is evaluated against a set of conditions. If the conditions are met, one of two actions occurs: • If this is the first event of the sequence, a new event thread is started, and the event is retained as the head of the sequence. • If the event belongs to an existing event thread, it is added to that sequence. In both cases, the event is retained in memory. The amount of resource usage is particularly sensitive to the customer environment for this type of rule. If the filter condition generates many event threads, resources are consumed for each new thread (in addition to the event). Additionally, if the end of the event thread is never met (i.e., an alert is never generated), then the entire event is saved in memory indefinitely. For example, you might write a rule to generate an alert when a user fails to log in to a server, then performs a successful login, and then creates a new account.

In addition to the memory usage discussed above, alert generation also consumes system resources. Each alert that is generated must be stored for retrieval and must also be processed by NetWitness Respond. This process uses disk space for storage, requires database memory to be consumed, and increases CPU utilization running queries.

When writing and deploying rules, you should be aware that each of these actions "cost" you system resources. The sections below are designed to help you keep your usage at a healthy level and monitor for problems if systems are becoming overloaded.

Best Practices for Writing Rules

These are general guidelines for writing rules.

- **Create alerts for actionable events.** The purpose of an alert should be to notify you of an event that requires immediate and specific action. For events that do not require action, or only require you to have awareness of the event, you can create a report.
- **Configure new rules as trial rules so you can observe how they react in your environment**. If you deploy new rules as trial rules, they will be disabled if the configured memory threshold is exceeded. You can also use the memory snapshot feature to see how much memory was being used when a trial rule was disabled. For more details, see Work with Trial Rules.

- **Configure Alert notifications only after your rule testing and tuning is complete**. This can help ensure you do not get flooded with notifications if a rule behaves differently than you expect.
- **Rules need to be specific so that you limit resource usage**. Use the following guidelines to limit usage:
  - Make the filters on the rule exclude all but the necessary events for the rule to fire accurately.
  - Make the size of your windows (window time for correlation) as small as possible.
  - Limit the events that you include in the window: For example, if you only want to see IDS events, ensure that you only include those events in your time window.
- **Rules need to be tuned to an alert level that is manageable**. If you are flooded with alerts, then the purpose and utility of an alert is lost. For example, maybe you want to know about encrypted traffic to other countries. But, you could limit the list to countries that are known risks. This limits the volume of alerts to a level you can manage.

Best Practices for Working with RSA Live Rules

These are guidelines for RSA Live Rules.

- **Deploy RSA Live rules in small batches**. Not every rule is suited to every environment. The best way to ensure your RSA Live rules are successful is to deploy them in small batches so you can test them in your environment. If you deploy small batches, it's much easier to tell if a particular rule has an issue.
- **Read the rule descriptions provided with RSA Live rules**. ESA rules are not “one size fits all.” Not all rules will work in your environment. The rule descriptions tell you which parameters you will need to modify to successfully deploy a rule in your environment.
- **Set your parameters**. RSA Live rules have parameters that need to be modified. If you do not modify your parameters, the rule may not work or it may exhaust your memory.
- **Deploy new rules as trial rules so you can observe how they react in your environment.** If you deploy new rules as trial rules, they will be disabled if the configured memory threshold is exceeded. For more details, see Work with Trial Rules.

Best Practices for Deploying Rules

These are general guidelines for deploying rules.

- **Deploy rules in small batches so you can observe how they react in your environment.** Not all environments are the same, and a rule will need to be tuned for memory usage, alert volume, and effective detection of events.
- **Test rules before you configure alert notifications**. Configure Alert notifications only after your rule testing and tuning is complete. This can help ensure you do not get flooded with alerts if a rule behaves differently than you expect.
- **Monitor system health as a part of your deployment process**. When you deploy rules, monitor your system's health as a part of your deployment process. You can view total memory utilization for your ESA in the Health and Wellness tab. For more information, see "Viewing Health and Wellness statistics" in Troubleshoot ESA.

Best Practices for System Health

These are general guidelines for system health.

- **Set up new rules as trial rules**. A common issue is that new rules may cause memory issues. To prevent this, you can set up new rules as trial rules. If the configured memory threshold is met, all trial rules are disabled to prevent the system from running out of memory. For more information about trial rules, see Work with Trial Rules.
- **Set up thresholds in the Health & Wellness module to alert you if memory usage is too high**. There are metrics in the Health & Wellness module that track memory usage. You can set up alerts and notifications to send you an email if those thresholds are crossed. For more information about the memory statistics you can view, see "Viewing Health and Wellness statistics" in Troubleshoot ESA.
- **Monitor memory metrics for each rule in the Health & Wellness module**. For each rule, you can view the estimated memory usage in the Health & Wellness module. You can use this information to ensure that rules do not use too much memory. For more information about the memory statistics you can view, see "Viewing Health and Wellness statistics" in Troubleshoot ESA.

Troubleshoot ESA

This section describes common issues that may occur while using ESA, and it suggests common solutions to these problems.

Troubleshoot ESA Services

Problem	Possible Causes	Solutions
On the NetWitness Suite Dashboard, the ESA service appears in red to indicate it is offline. In the **CONFIGURE** > **ESA Rules** view, the following message appears: "The Service is either offline or not reachable."	Several	When an ESA service is offline, there are many possible causes. However, a common issue is that you have created a rule that uses excessive memory and causes the ESA service to fail. To troubleshoot this problem, see Steps to Troubleshoot Memory Issues with an ESA Service Offline. Other common causes might be that your firewall is blocking the connection between the ESA and NetWitness Suite, or the ESA service machine may be down.
		To bring up ESA Services: From **ADMIN** > **Services**, select the actions icon for your ESA service, and choose **start**. If your ESA service is stopping and restarting in a loop, you may need to call Customer Support to get the services to start.
After a recent upgrade, the ESA service appears in red on the NetWitness Suite Dashboard to indicate it is offline. In the **CONFIGURE** > **ESA Rules** view, the following message appears: "The Service is either offline or not reachable."	Configuration issues	If your system has been recently upgraded, you may have made a configuration error. Under **ADMIN** > **Services**, select your ESA service, and click **Edit Service**. On the Edit Service field, click Test Connection. If the connections fails, you likely have a configuration error. Attempt to fix your configuration error, and try again.

Problem	Possible Causes	Solutions
The ESA appears to be running slowly.	Configuration issues	You may be able to improve performance by modifying the buffer (the default value is *1048576 bytes*), or setting the TCP setting to TCPNoDelay to prevent a delay in receiving TPC acknowledgments (Acks). You can modify these settings (*readBufferSize* and *tcpNoDelay*) by going to */Workflow/Source/nextgenAggregation* in the Explore view.

Troubleshoot RSA Live Rules for ESA

Problem	Possible Causes	Solutions
I imported a group of rules from RSA Live, and now my ESA service is crashing. Why?	You may not have configured the parameters for the RSA Live rule to tune it for your environment.	Each rule in RSA Live has a description that includes the parameters you must configure and prerequisites for your environment. Review this description to see if the rule is appropriate for your environment. To ensure that you deploy rules safely in your environment, configure new rules as trial rules to test them in your environment. Trial rules add a safeguard for testing new rules. For details on this, see Deploy Rules as Trial Rules.

Problem	Possible Causes	Solutions
I imported a group of rules from RSA Live, and while the rules deployed without errors, they were later disabled.	Not all RSA Live rules are meant for every environment. You may not have the correct meta in your ESA for the rule to run.	You can verify that a rule was disabled by going to **CONFIGURE > ESA Rules > Services > Deployed Rule Stats**. If the rule is disabled, the green icon does not display next to the rule. If a rule deployed correctly but was disabled, check the logs for exceptions related to the rule. Specifically, check to see if the rules were disabled due to missing meta. To do this, go to **ADMIN** > **Services**, select your ESA service and then > **View** > **Logs**. Then, search for a message similar to the following: "Property named '<meta_name>' is not valid in any stream" For example, you might see: `Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream` If a similar message displays, you may need to add a custom meta key to the Log Decoder or Concentrator. To do this, follow these instructions: "Create Custom Meta Keys Using Custom Feed " in the *Decoder and Log Decoder Configuration Guide*.

Troubleshoot Deployments

Problem	Possible Causes	Solutions
I created a rule, and I checked the syntax. The rule looked fine. When I went to deploy the rule, I got an error. Why?	You may not have the correct meta to deploy the rule.	Check the Meta key references. You may not have the correct meta to deploy the rule.

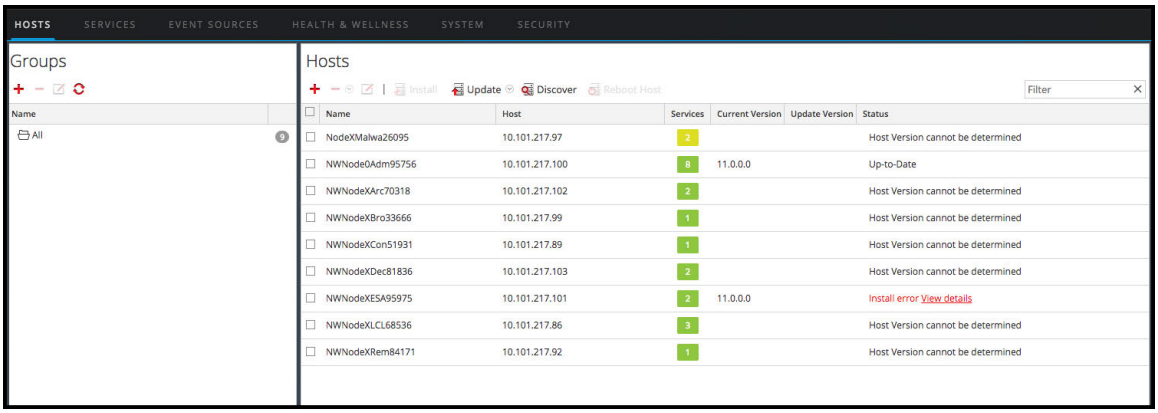
Troubleshoot Rules

Problem	Possible Causes	Solutions
I created a custom rule (via the Rule Builder or Advanced EPL), and my rule is not firing. Why?	You may have connectivity issues.	Check the 'Offered Rate' statistic on the **CONFIGURE** > **ESA Rules** > **Services** tab. If the offered rate is zero, then the ESA service is not receiving data from Concentrators. Validate the Concentrator connectivity. Go to **ADMIN** > **Services**, select your ESA, and then **View** > **Config**. Ensure the concentrator is enabled. Select the concentrator and click on **test connection**. If the offered rate is not zero, the meta key name and type used in the rule likely doesn't match the meta key present in events. Check to see if the meta key name and type used in the rule is valid by searching for the meta key name in **CONFIGURE** > **ESA Rules** > **Settings** tab (Meta key references search).
	There may be a problem with the rule.	**If a specific rule is not firing**, go to **CONFIGURE** > **ESA Rules** > **Services** to see if the rule was disabled. In the **Deployed Rule Stats** section, a rule that is disabled displays a clear enabled button (instead of the green enabled button). You can also check Events Matched field. Go to **CONFIGURE** > **ESA Rules** > **Services**. From there, you can see the number of events that were matched in the **Events Matched** column. If no events matched, check the logic of your rule for errors. For example, check the syntax for uppercase and lowercase errors, and check the time window. If the rule still doesn't fire, consider simplifying the logic of the rule to see if it fires when there is less complexity.

Steps to Troubleshoot Memory Issues with an ESA Service Offline

Step 1: Verify that your Host Is Running

The first step to troubleshooting is to ensure that your host is running. To do this, go to **ADMIN**> **HOSTS**. If the host is down, the system parameters will not display (updating host information can sometimes be delayed), the **Services** display in red, and the **Updates** field displays an error message.



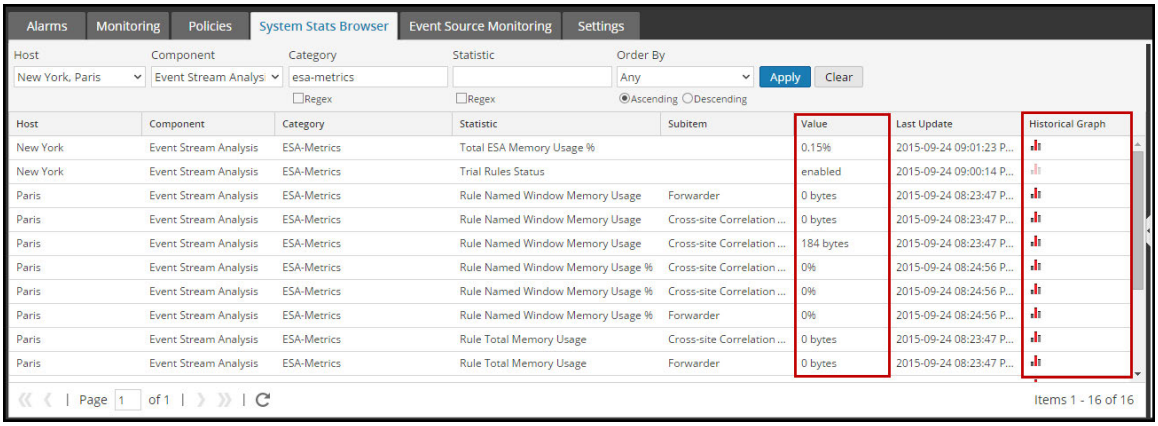
If your host is down, contact your NetWitness Suite Administrator to restart it. Otherwise, go to Step 2.

Step 2: View Detailed Statistics in Health & Wellness

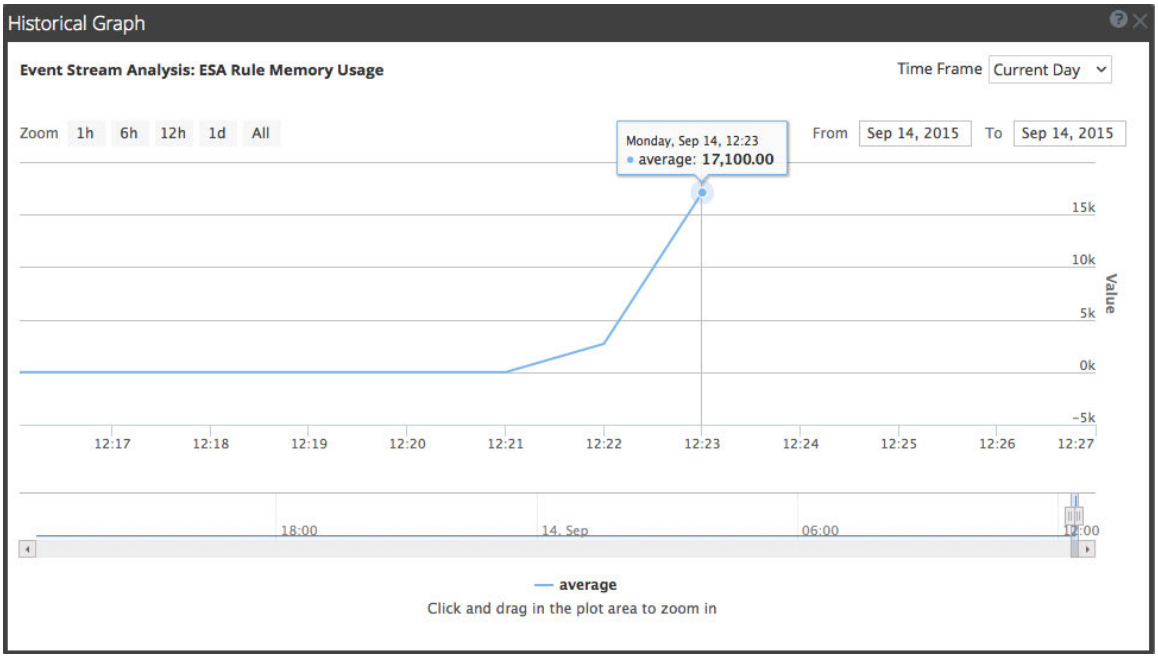
Once you are sure your ESA service is down, you can go to Health & Wellness to see where potential issues are occurring. The most common problem is that your ESA service is exceeding memory thresholds, which causes it to stop or fail.

1. Go to **ADMIN** > **Health & Wellness** > **Alarms** to see if the ESA triggered any alarms. Look for the following alarms:
   - ESA Overall Memory Utilization > 85%
   - ESA Overall Memory Utilization > 95%
   - ESA Service Stopped
2. Go to **ADMIN** > **Health & Wellness** > **System Stats Browser** to see the memory metrics for each rule's performance. To view the metrics, enter the following:

Host	Component	Category
<your host>	Event Stream Analysis	esa-metrics



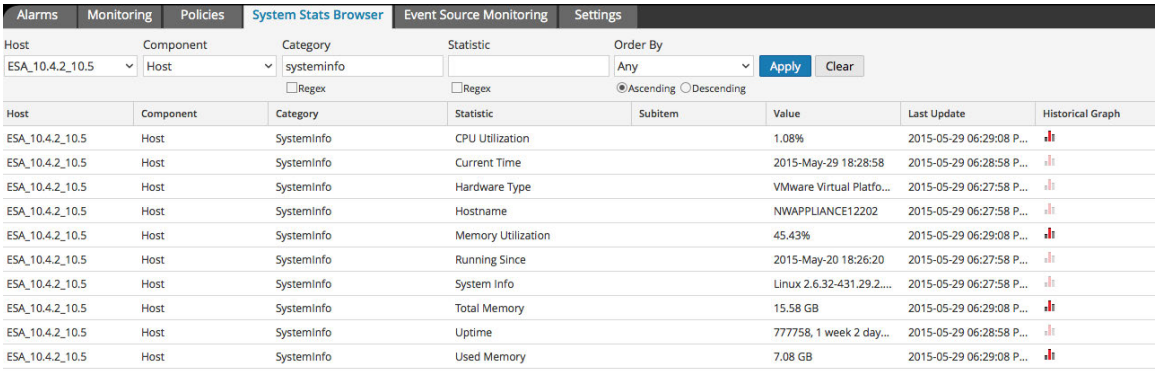
The memory for each rule is displayed in the **Value** column, and the value is displayed in bytes. You can view a historical view of memory usage in the **Historical Graph** column.



3. Go to **ADMIN** > **Health & Wellness** > **System Stats Browser** to see details of your ESA performance. Select your host, and use the following filters to view the following statistics:

Host	Component	Category	Statistic	Example
<your host>	Host	SystemInfo	CPU Utilization	1.08%
<your host>	Host	SystemInfo	Memory Utilization	45.43%
<your host>	Host	SystemInfo	Used Memory	7.08 GB
<your host>	Host	SystemInfo	Total Memory	15.58 GB
<your host>	Host	SystemInfo	Uptime	77758, 1 week, 2 day...
<your host>	Event Stream Analysis	ProcessInfo	Memory Utilization	7.07 GB

Host	Component	Category	Statistic	Example
<your host>	Event Stream Analysis	ProcessInfo	CPU Utilization	0.2%
<your host>	Event Stream Analysis	JVM.Memory	all	Committed Heap Memory Usage 8.0 GB
<your host>	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %	4.64%



If you are having a problem with memory or CPU utilization, continue to step 3.

Step 3: Bring up your ESA Services

1. From **ADMIN** > **Services**, select the actions icon for your ESA service and choose **start**.
2. Return to the ESA Service to troubleshoot which rules have created memory issues.

If your ESA service is stopping and restarting in a loop, you may need to call Customer Support to get the services to start.

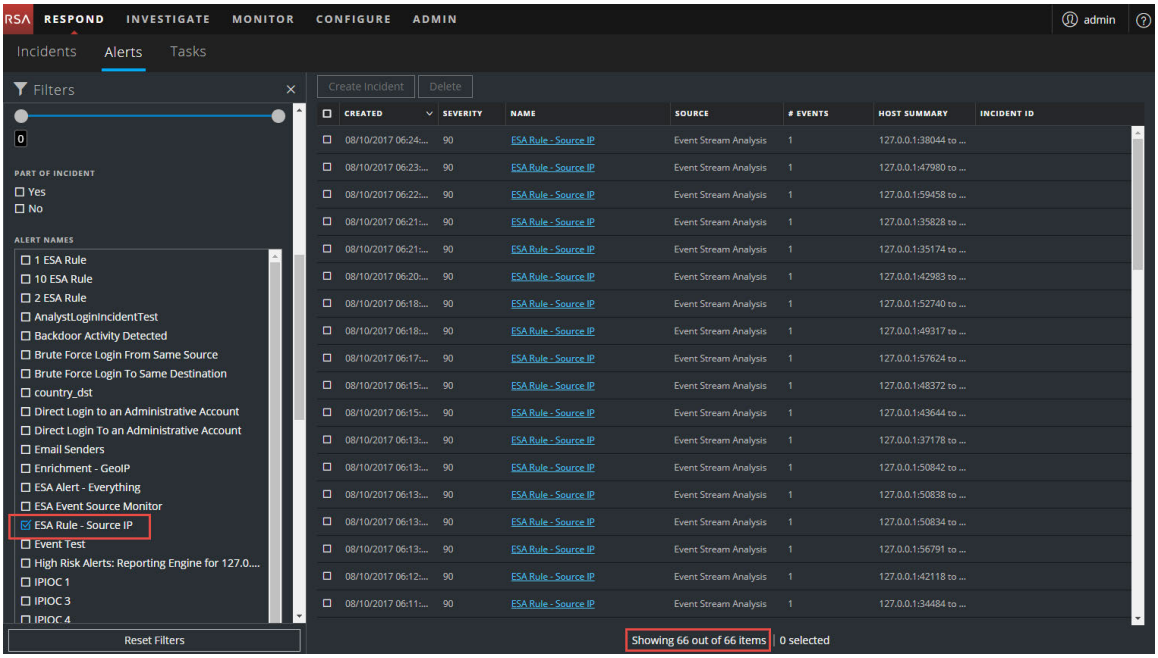
If you are able to start your ESA service without a shutdown, continue to step 4.

Step 4: Check the Alerts and Events Volume

Once you are able to restart your ESA service without an immediate shutdown, you can review the stats for your rules to see which rules are consuming too many resources. Sometimes, ESA services fail because a rule is generating too many alerts or a rule is matching too many events. Check for both of these issues if you have determined that memory usage is causing your ESA service to shut down.

View Alert Summaries

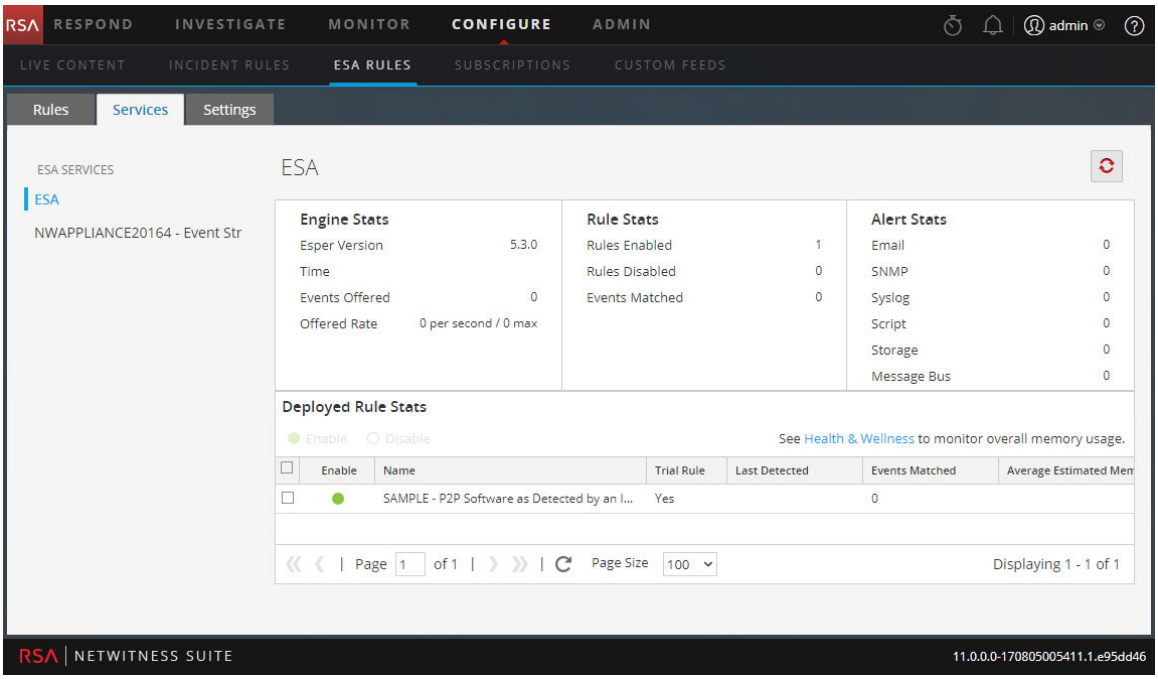
Rules that generate a high volume of alerts can overwhelm the system and cause it to fail or restart. To view the alert summaries, go to **RESPOND > Alerts**. In the **Filters** panel on the left, in the **ALERT NAMES** section, select the alert name for the rule. The number of alerts with that name appears at the bottom of the Alerts list results. If the number is significantly high for a particular rule, you need to disable the rule and rewrite it to be more efficient.



To clear your filter, click **Reset Filters**.

View Events Matched

Sometimes a rule matches too many events, which can use up excessive memory. This typically occurs if you create a large event window where a great number of events accumulates without triggering an alert. These are a problem because each event is stored in memory while the rule waits for the alert to trigger. To check for this issue, go to **CONFIGURE** > **ESA Rules** > **Services.** From there, you can see the number of events that were matched in the **Events Matched** column. If there was a high number of events matched for a given rule, you can investigate the rule further to see if you can make it more efficient.



Step 5: Disable and Repair the Rule that Caused Issues

Once you have determined the rules that need to be rewritten, disable them and rewrite rules so that they don't generate such a high volume of alerts or events. For pointers on how to write more efficient rules, see Best Practices.

Disable Rules

1. To disable rules, go to **CONFIGURE** > **ESA Rules** > **Services**, and select the rules you want to disable in the **Deployed Rules Stats** field.
2. Select **Disable** to disable the rules.

Edit Rules

1. To repair the rules, go to **CONFIGURE** > **ESA Rules** > **Rules** > **Rule Library**. Select the rule to edit, and click the actions icon .
2. Select **Edit**.
3. Edit the rule to be more efficient. For instructions on creating rules, see Add Rules to the Rule Library
4. Once you are satisfied with your rule, you can save the rule as a trial rule to ensure that any memory issues do not affect ESA services performance. To do this, follow the steps listed in Work with Trial Rules.

Enable Rules

1. To enable rules, go to CONFIGURE > **ESA Rules** > **Services**, and select the rules you want to enable in the **Deployed Rules Stats** field.
2. Select **Enable** to enable the rules.

(Optional) Check the ESA Log Files for More Information

Once you verify that your services are down and some potential causes for the system going down, check to see if the service is stopping and restarting in a loop. To do this, go to the ESA logs. From the **ADMIN** > **Services** view, select your ESA service, and then select > **View** > **Logs**.

If you cannot access the ESA logs from the NetWitness Suite interface, you can use SSH to get in the system and go to:`opt/rsa/esa/logs/esa.log`.

View Memory Metrics for Rules

This topic tells ESA rule writers how to view memory metrics for rules. You can see estimated memory usage for each rule running on a server, and you can use this information to modify your rule statements and conditions if they use too much memory.

Rules can sometimes consume more memory than you expect, causing your ESA to slow down or stop. To see approximately how much memory a rule is using, you can configure memory metrics. Memory metrics allow you to view an estimated memory usage for each rule in the Health & Wellness System Stats browser (so you will need permissions to access this module). You can use this information to modify your rules to be more efficient.

At a high level, you will need to complete the following steps to use the memory metrics to troubleshoot memory usage for rules:

1. Ensure that the memory metrics feature is enabled (via Explorer > CEP > Metrics > EnableStats). The Memory Metrics feature is enabled by default.
2. Ensure you have the correct permissions to view the Health & Wellness module. For information on roles and permissions, see Role Permissions.
3. View the memory statistics in Health & Wellness.
4. (Recommended) Configure Health & Wellness ESA policies to send an email if memory thresholds are exceeded. See "Manage Policies" in the *System Maintenance Guide* for instructions on sending email notifications.
5. Use the memory metrics data to modify rules to be more efficient, if necessary.

Prerequisites

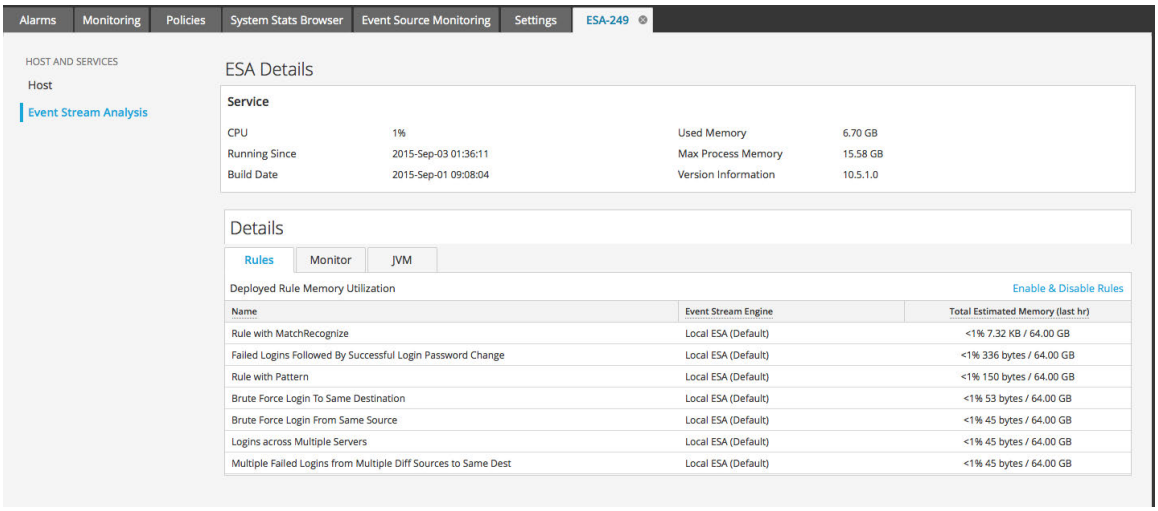
The following are requirements for using memory metrics:

- Memory Metrics feature is enabled (via **Explorer** > **CEP** > **Metrics** > **EnableStats**).
- The user must have the appropriate permissions to view Health & Wellness statistics.
- (Recommended) Configure the ESA Health & Wellness policy to send an email when memory thresholds are exceeded.

Procedures

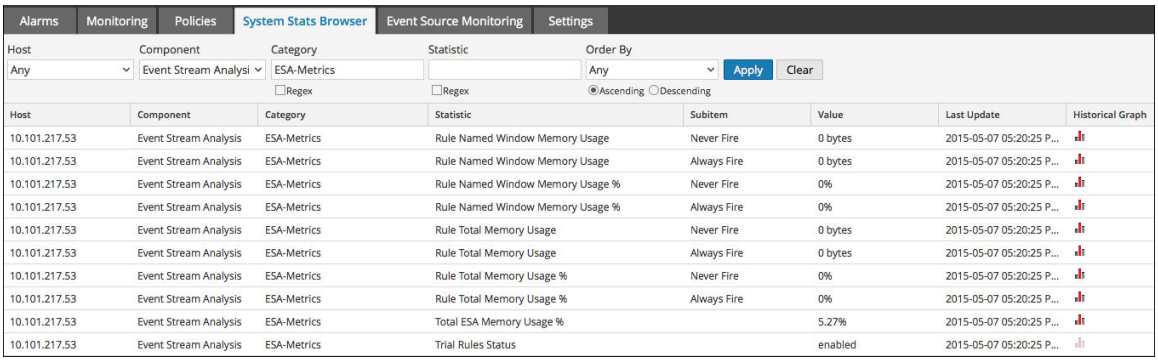
View Memory Metrics in the Health & Wellness System Monitoring Module

1. Go to **ADMIN** > **Health & Wellness** > **Monitoring**
2. View the details for your ESA service.
3. Click the **Rules** tab.
4. You can view the average memory usage for each rule for the previous hour.



View Memory Metrics in the Health & Wellness System Stats Browser

1. Go to **ADMIN** > **Health & Wellness** > **System Stats Browser**.
2. For component, select **Event Stream Analysis**. For category, enter **ESA-Metrics**.



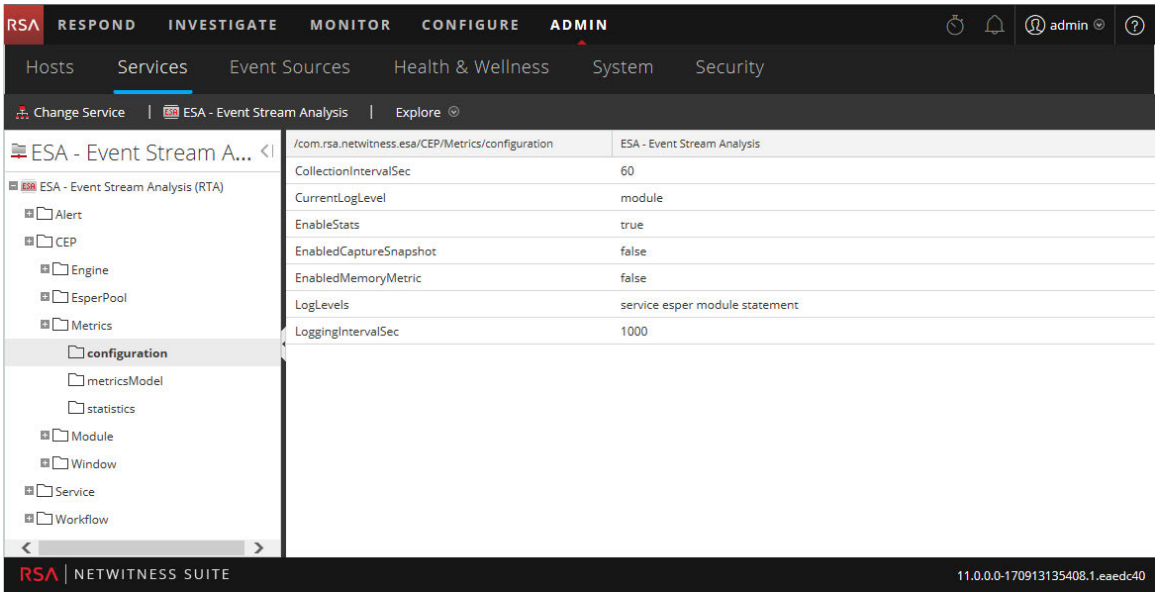
The name of the rule is displayed in the **Subitem** field, and the memory usage is displayed in the **Value** column.

3. To view the historical memory usage for the rule, click on the **Historical Graph** icon.

Note: The **Last Update** field reflects when Health & Wellness polls ESA. However, the Memory Metrics is not synchronized with the Health & Wellness polling. For example, if the memory threshold is exceeded on 10/10/15 at 12 p.m., but Health & Wellness polls at 10/10/15 at 12:10 p.m., the **Last Update** field will display a timestamp of 10/10/15 12:10 p.m.

Enable or Disable the Memory Metrics Feature

1. Go to **ADMIN** > **Services**and select your ESA.
2. Once you've selected your ESA, click **Actions** > **View**> **Explore**, and navigate to **CEP** > **Metrics** > **Configuration** as shown below.



3. Change the field EnabledStats to **true** or **false** depending on whether you want to enable or disable the memory metrics feature.

How ESA Generates Alerts

This topic provides a brief description of how an Event Stream Analysis (ESA) service runs rules to generate alerts. The Event Stream Analysis (ESA) service runs rules that specify criteria for problem behavior or threatening events in your network. When ESA detects a threat that matches rule criteria, it generates an alert.

To generate alerts, ESA performs the following functions:

1. Gathers data
2. Runs ESA rules against the data
3. Captures events that meet rule criteria
4. Generates alerts for those captured events

You can use the Alerts module to gain visibility into your network and to detect problems in it.

Sensitive Data

This topic explains how ESA treats sensitive data, such as usernames or IP address, that it receives from Core services. The Data Privacy Officer (DPO) role can identify meta keys that contain sensitive data and should display obfuscated data. ESA will not display or store sensitive meta. Consequently, ESA will not pass sensitive data to NetWitness Respond.

Optionally, ESA can add an obfuscated version of the sensitive data to an event. For example, the DPO identifies user_dst as sensitive. ESA can add an obfuscated version, such as user_dst_hash, to an event. The obfuscated meta is not sensitive, so ESA will display and store it the same way as any other non-sensitive meta.

For more information on the strategy and benefits of obfuscating data, see the *Data Privacy Management Guide*.

This topic explains the following:

- How ESA treats sensitive data it receives from Core services
- How to prevent sensitive data leaks in an Advanced EPL rule

How ESA Treats Sensitive Data from Core Services

When ESA receives sensitive data from Core services, ESA passes on only the obfuscated version of the data. ESA does not store or show sensitive data.

The following features are impacted:

- Outputs – ESA does not forward sensitive data to outputs, which include alerts, notifications and MongoDB storage.
- Advanced EPL rules – If an EPL statement creates an alias for a sensitive meta key, sensitive data will leak. This topic illustrates how this happens so you can avoid it.
- Enrichments – If a sensitive meta key is used in the join condition, sensitive data will leak. This topic illustrates how this happens so you can avoid it.

Advanced EPL Rule

If an EPL query statement renames a sensitive meta key, the data will not be protected.

ESA identifies a sensitive meta key by the name:

ip_src is the sensitive meta key.
ip_src_hash is the non-sensitive, obfuscated version.

To support data privacy, the sensitive meta key must not be renamed in an EPL query. If a sensitive meta key is renamed, the data will no longer be protected.

For example, in a rule such as select ip_src as ip_alias..., ip_alias contains the sensitive data but it is not protected because ESA only knows about ip_src, not ip_alias. In this case, IP addresses would not be obfuscated. Real values would be displayed.

Enrichment Source

When a sensitive meta key is used in a join condition, sensitive data can be displayed.

The enrichment database, which is the other part of the join condition, has one column that matches the sensitive meta key. This cross reference is to actual values not obscured values. Consequently, actual values are displayed.

In the following example, both parts of the join condition are highlighted.

- ip_src contains sensitive data.
- ipv4 will be added to the alert and exposed as non-sensitive data

Because the ipv4 value is the same as the ip_src value, ipv4 contains and displays sensitive data.

ESA Rule Types

This topic describes each type of ESA rule, when to use them and the permissions each role has with them. The following table lists each type, describes it, and explains when to use it.

Rule Type	Description	When to Use
Rule Builder	In the rule builder, you define rule criteria in an easy-to-use interface.	Use the rule builder to create your first rules. You choose many of the rule conditions from lists.
Advanced EPL	With the Event Processing Language (EPL), you define rule criteria by writing a query.	Use advanced EPL rules to define rule criteria in the EPL syntax.
RSA Live ESA	RSA Live has a catalog of ESA rules that you can download and modify to run in your network.	Download RSA Live ESA rules to leverage rules that are already built. Modify the configurable parameters to customize to meet your requirements.

Starter Pack Rules

A few sample Rule Builder rules come with NetWitness Suite and appear in the Rule Library. Use starter pack rules to get comfortable working with rules before creating your own. You can safely edit and deploy these sample rules.

Trial Rules Mode

For any type of rule, you can select the Trial Rule setting as an additional safeguard. Trial rules get disabled if they exceed a memory threshold the administrator sets. Run a rule in trial mode to monitor memory usage and to disable the rule automatically if it uses more memory than the threshold allows.

Role Permissions

This topic lists all ESA permissions and shows which permissions are assigned to each pre-configured NetWitness Suite role. User access is restricted based on roles and permissions assigned to roles.

- Administrators
- Operators
- Analyst
- Security Operations Center (SOC) Managers
- Malware Analysts (MA)
- Data Privacy Officer

There are four permissions for ESA:

1. Access Alerting Module – Is required for any permission
2. View Rules – Allows view-only permission for rules in the Rule Library
3. View Alerts – Allows view-only permission for alerts ESA generates
4. Manage Rules – Allows you to view, create, edit and delete rules

The following table lists permissions for ESA and the roles to which they are assigned. Use this table to see how each role can work with rules and alerts.

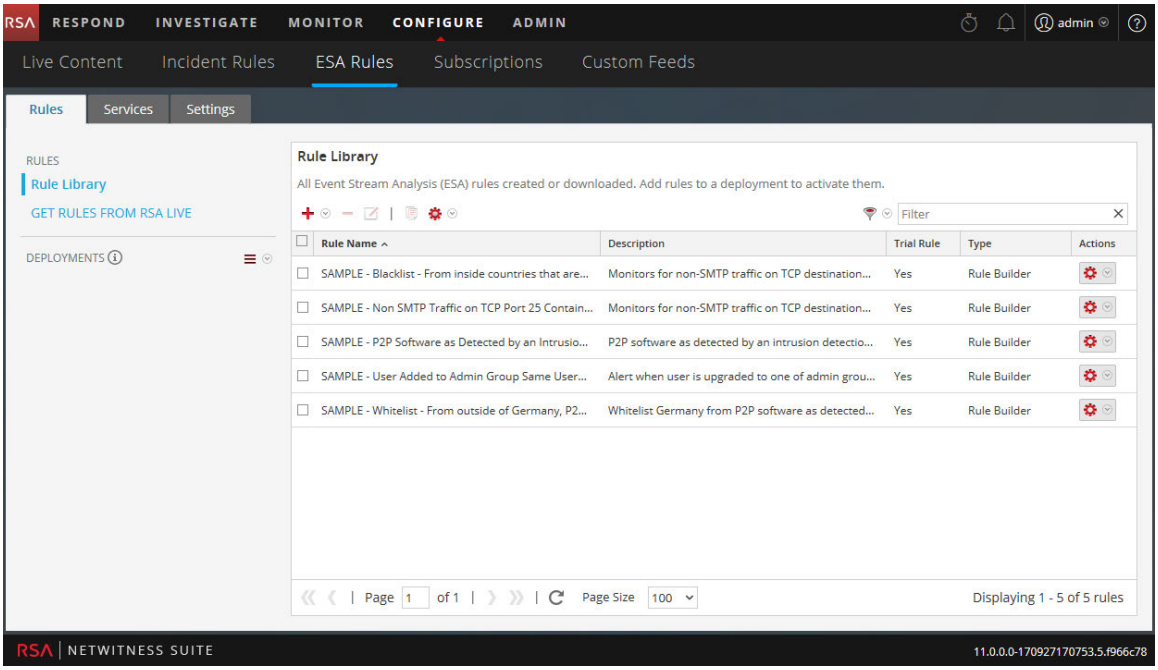
Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Alerting Module	Yes	Yes	Yes	Yes		Yes
View Rules	Yes	Yes		Yes		Yes
View Alerts	Yes		Yes	Yes		Yes
Manage Rules	Yes	Yes		Yes		Yes

For more information on roles and permissions, see the *System Security and User Management Guide*.

Practice with Starter Pack Rules

NetWitness Suite comes with starter pack rules so analysts can become familiar with how rules look before you create your own rules. Use the starter pack rules to become familiar with the Rule Builder and to practice editing and deploying a rule.

Starter pack rules are installed in the Rule Library, which will contain every rule you download or create. The following figure shows sample rules in the Rule Library.



These are the available starter pack rules:

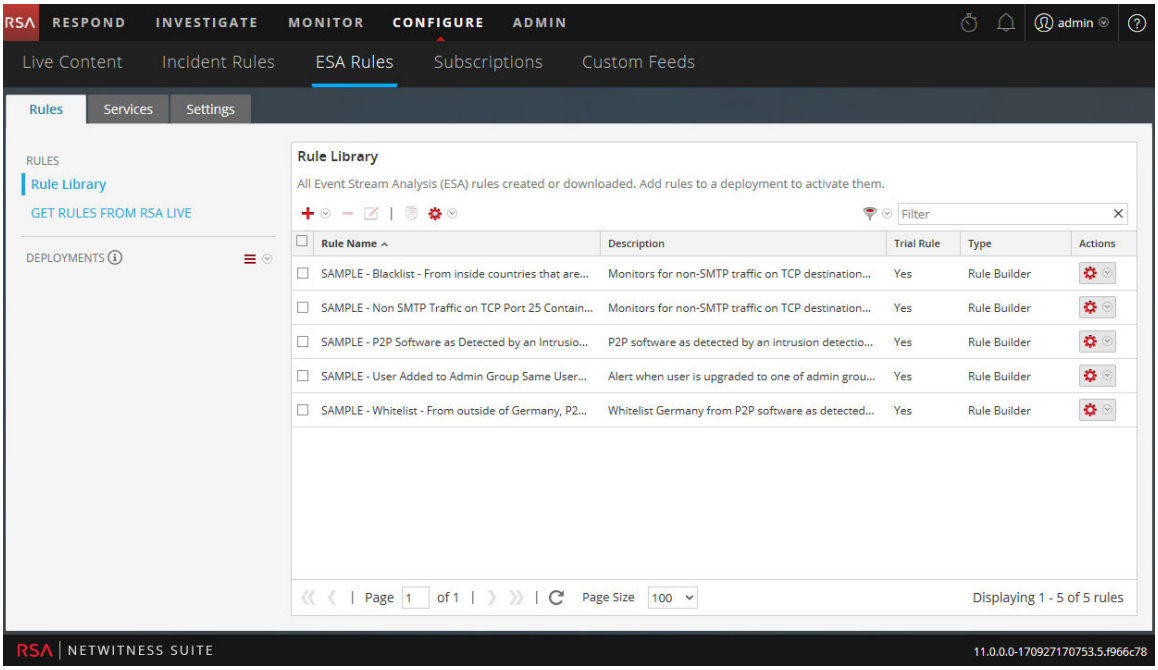
- SAMPLE: P2P Software as Detected by an Intrusion Detection Device
- SAMPLE: Non SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: Whitelist - From outside of Germany, P2P Software as Detected by an Intrusion Detection Device.
- SAMPLE: Blacklist - From inside countries that are not the US, Non-SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: User Added to Admin Group Same User su Sudo

Each name begins with SAMPLE to distinguish the rules that are installed with NetWitness Suite from the rules you download and create.

Rule Library

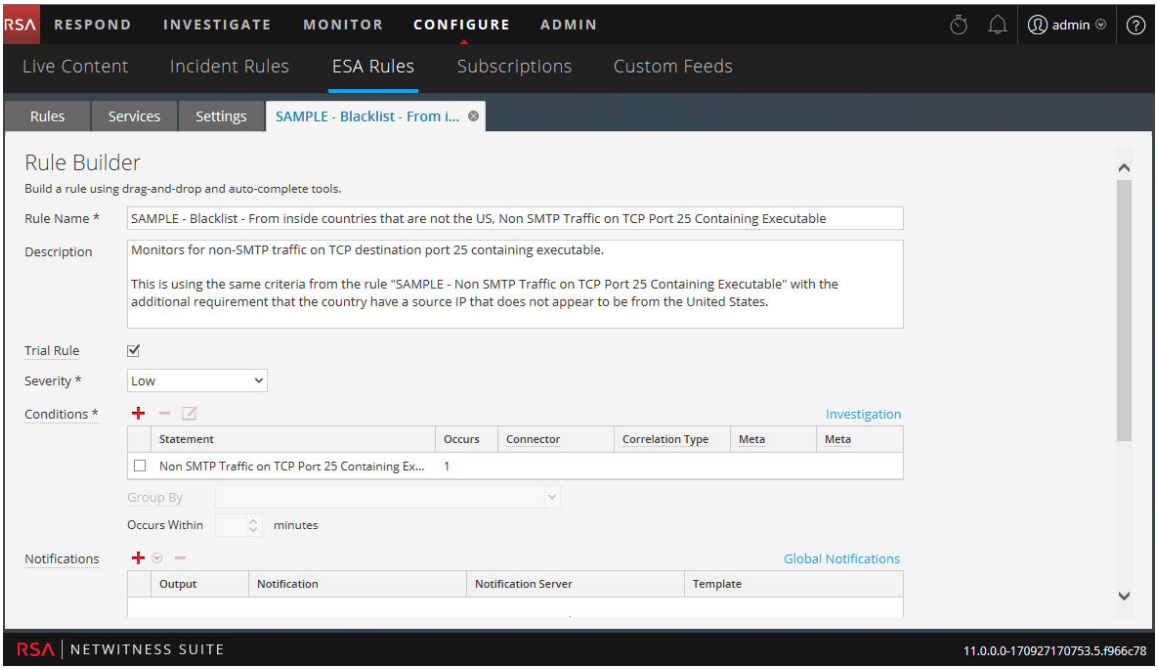
The Rule Library shows the following information for a rule:

- **Name** summarizes the data or events the rule collects.
- **Description** explains the rule in more detail, although only the beginning shows in the Rule Library.
- **Trial Rule** indicates if trial mode is enabled or disabled for the rule.
- **Type** shows the origin of the rule, built in Rule Builder or Advanced EPL, or downloaded from RSA Live.



Procedure

1. Go to **CONFIGURE > ESA Rules**.
   The ESA Rules view is displayed with the Rules tab open.
2. In the **Rule Library**, select a sample rule and click , or double-click a rule.
   The rule is opened in Rule Builder.



3. To practice with a starter pack rule, refer to the following topics for detailed descriptions and procedures:
   - To familiarize yourself with the Rule Builder user interface, see Rule Builder Tab for a description of each field.
   - To learn how to edit a rule, see Add a Rule Builder Rule for a step-by-step procedure.
   - To deploy a starter pack rule, see Deploy Rules to Run on ESA to learn how to associate the rule with an ESA service.

After you practice with starter pack rules, you will be able to download, create, and deploy your own rules.

Work with Trial Rules

When rules use too much memory, your ESA service can become slow or unresponsive. To ensure rules do not use excessive memory, you can enable trial rules for any type of rule. By default, new rules you create and RSA Live rules you import are configured to be trial rules. RSA recommends you disable the trial rule setting only after testing the new rule in your environment during normal and peak network traffic. When you create a trial rule, you set a global threshold of the percentage of memory that rules may use. If that configured memory threshold is exceeded, all trial rules are disabled.

The NetWitness Suite Event Stream Analysis (ESA) service is capable of processing large volumes of disparate event data from Concentrators. However, when working with Event Stream Analysis, it is possible to create rules that use excessive memory. This can slow your ESA service or even cause it to shut down unexpectedly. To ensure that this doesn't happen, you can configure your rule as a trial rule. When you configure a trial rule, you also set global threshold of the percentage of memory that rules may use. If that configured memory threshold is exceeded, all trial rules are disabled automatically.

For suggestions on creating more efficient rules, see "Best Practices for Writing Rules" in Best Practices

By default, new rules and RSA Live rules are configured as trial rules. As a best practice, when you edit an existing rule, select the Trial Rule option, which allows you to:

- Deploy the rule with an added safeguard.
- Optionally, view a snapshot of memory utilization to understand if the rule creates memory issues.
- Know if you must modify the rule criteria to improve performance.

Note: Run a rule as a trial rule long enough to assess the performance during normal and peak network traffic.

Deploy Rules as Trial Rules

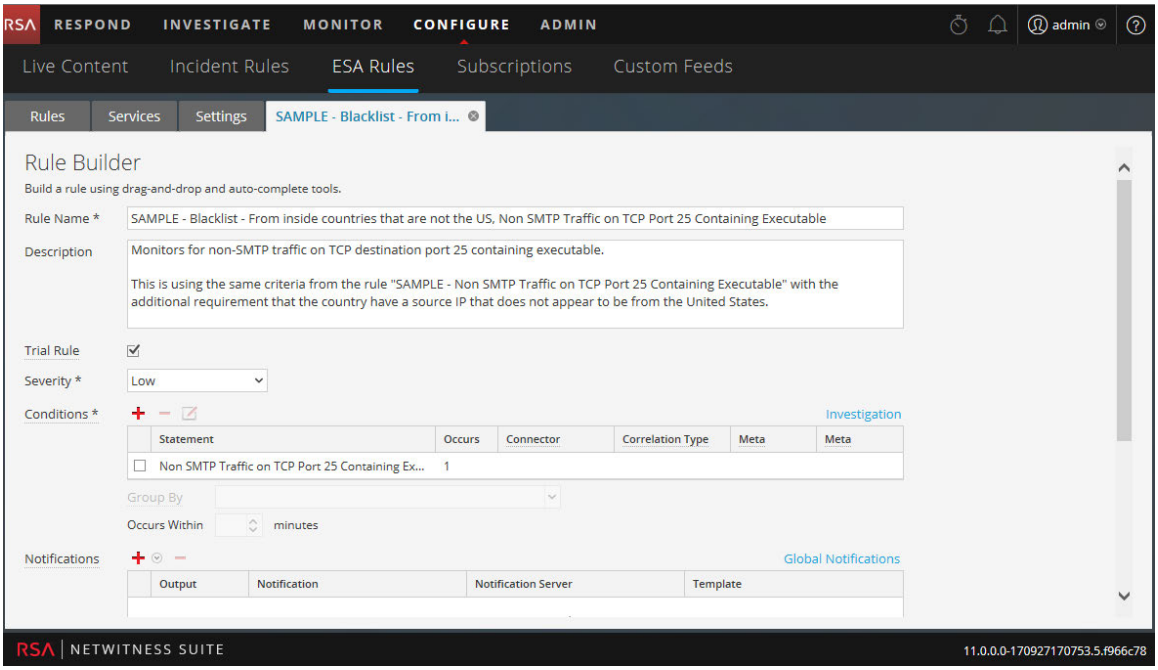
This topic explains to administrators how to enable trial rules when creating new rules or editing rules. Trial rules are automatically disabled if a specified total JVM memory utilization threshold is exceeded.

Procedure

To deploy rules as trial rules:

1. Go to **CONFIGURE** > **ESA Rules**.
   The Configure ESA Rules view is displayed with the Rules tab open.

2. From the Rule Library, choose to add or edit a rule. The rule builder is displayed in a new tab.



3. To make a new or existing rule a trial rule, select the **Trial Rule** checkbox.
4. Add the rule conditions or modify the rule as needed. For instructions on editing rules, see Add Rules to the Rule Library.
5. Click **Save**.
6. Ensure that trial rules are enabled for your ESA and that you are satisfied with the thresholds configured for trial rules.
   The memory threshold is set in the configuration file. To configure it, see "Change Memory Threshold for Trial Rules" in the *ESA Configuration Guide*.
   The threshold is configured per ESA and is a percentage of Java Virtual Memory.
   The configuration parameter, MemoryThresholdforTrialRules default is 85.
7. Optionally, you can set up the policies in Health and Wellness to send you an email notification if the total JVM memory utilization threshold is exceeded.

The next time you deploy the rule, it runs in trial rule mode.

Note: If a trial rule is disabled, you will need to go to the **CONFIGURE** > **ESA Rules** > **Services** tab to re-enable the trial rules. For more instructions on re-enabling trial rules on a service, see View ESA Stats and Alerts.

View Memory Metrics for Rules Using Trial Mode

This topic tells ESA rule writers how to view memory metrics when the memory threshold configured for trial rules is exceeded. If the memory threshold is exceeded, you can configure a snapshot to be taken of the memory usage for ESA rules at the time that trial rules are disabled, allowing you to investigate memory usage and edit the rules to be more efficient.

When you configure trial rules and enable the Memory Snapshot feature, if the memory threshold is exceeded, all trial rules are disabled and a snapshot of the memory usage for all ESA rules is taken at the time of disablement. This allows you to see how much memory was used so that you can modify your ESA rules to be more efficient. The memory snapshot can be viewed in the Health & Wellness System Stats browser, so you will need permissions to access this module. Once you view the details in the System Stats browser, you can modify the trial rule syntax and re-enable the trial rules.

At a high level, you will need to complete the following steps to use the Memory Snapshot to troubleshoot memory usage for rules:

1. Enable trial rules for any new rules you deploy. See Deploy Rules as Trial Rules.
2. Ensure that you have configured Health & Wellness ESA policies to send an email if memory thresholds are exceeded.
3. Ensure you have the correct permissions to view the Health & Wellness module. For information on roles and permissions, see Role Permissions.
4. Ensure that the Memory Snapshot feature is enabled (via the EnabledCaptureSnapshot parameter via NetWitness Suite Explorer). The Memory Snapshot feature is disabled by default. See "Enabling and Disabling the Memory Snapshot Feature" below. RSA recommends you disable the feature once you have completed testing new rules.
5. View the memory threshold statistics in Health & Wellness if the memory threshold is triggered for trial rules.
6. Modify the rule or rules that triggered the alarm. For best practices for rule writing, see Best Practices.
7. Re-enable the trial rules that were disabled when the memory threshold was triggered. For instructions on re-enabling trial rules on a service, see View ESA Stats and Alerts.
8. Continue to test the trial rules.

Note: Like any Debug tool, there can be exceptional overhead associated with using the Memory Snapshot feature. When actively taking a snapshot, the Memory Snapshot feature can add delays to your ESA services. The ESA service stops generating alerts while taking a snapshot. RSA recommends you disable the feature once you have completed testing new rules. If you disable the Memory Snapshot feature, trial rules will still be disabled when memory usage exceeds configured thresholds, but the memory snapshot will not be taken, and the statistics will not appear in the Health & Wellness System Stats browser.

Prerequisites

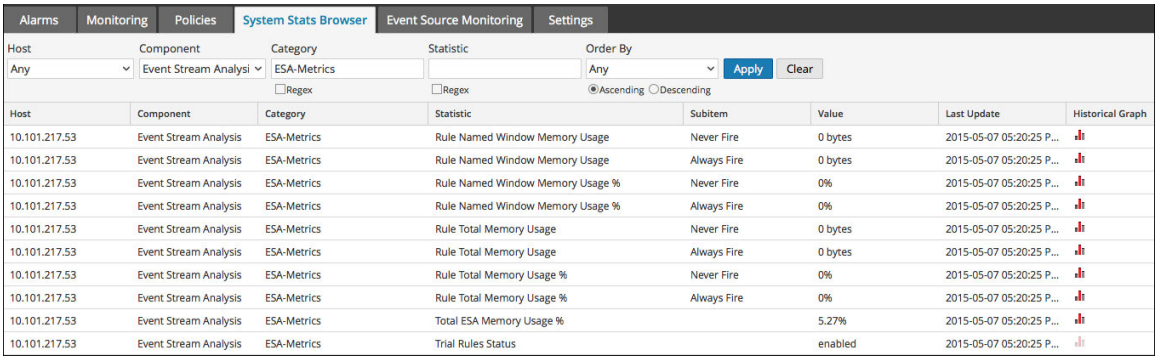
These are the requirements for viewing memory metrics:

- One or more ESA rules must be configured as a trial rule.
- Memory Snapshot must be enabled (via the EnabledCaptureSnapshot parameter via NetWitness Suite Explorer).
- The user must have the appropriate permissions to view Health & Wellness statistics.
- The user must have configured the ESA Health & Wellness policy to send an email when memory thresholds are exceeded.

Procedures

View Memory Metrics

1. Go to **ADMIN** > **Health & Wellness** > **System Stats Browser**.
2. For component, select **Event Stream Analysis**. For category, enter **ESA-Metrics**.



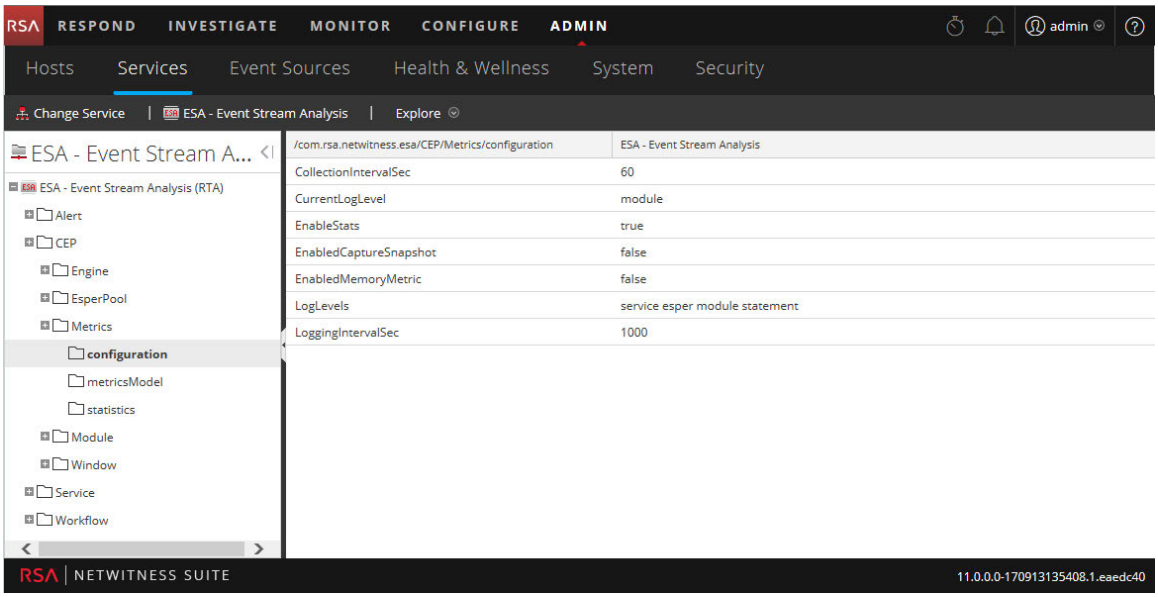
Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

The name of the rule is displayed in the **Subitem** field, and the memory usage is displayed in the **Value** column.

Note: The **Last Update** field reflects when Health & Wellness polls ESA. However, the Memory Snapshot only occurs when memory thresholds are exceeded, so this field does not reflect when the snapshot was taken or updated. The snapshot remains static until the memory threshold is exceeded again. For example, if the memory threshold is exceeded on 10/10/15 at 12 p.m., but Health & Wellness polls at 10/10/15 at 3 p.m., the **Last Update** field will display a date of 10/10/15 3 p.m.

Enable or Disable the Memory Snapshot Feature

1. Go to **ADMIN** > **Services**and select your ESA.
2. Select > **View** > **Explore**, and navigate to CEP > Metrics > Configuration as shown below.



3. Change the field EnabledCaptureSnapshot to **true** or **false** depending on whether you want to enable or disable the Memory Snapshot feature.

Add Rules to the Rule Library

This topic explains how to add each type of rule to the rule library. You must add a rule to the Rule Library before you can deploy it. Permission to manage rules is required for all tasks in this section. To add rules, you can download them from ESA Live, create a rule via the Rule Builder, or write advanced EPL rules.

For more details on each of these procedures, see:

- Download Configurable RSA Live ESA Rules
- Add a Rule Builder Rule
- Add an Advanced EPL Rule

In addition to deploying a rule, you can edit, duplicate, import, export, and remove a rule in the Rule Library. For details on these procedures, see Working with RulesWorking with Rules

Download Configurable RSA Live ESA Rules

This topic explains how to download configurable rules from the NetWitness Suite Live Content Management System so you can customize them to meet your needs.

RSA Live contains a catalog of rules. Each rule has configurable parameters so you can customize the rule for your environment. If RSA Live has a rule to detect events that you want to detect in your network, download the rule to save time. You can edit the configurable parameters and save the rule in your Rule Library.

This is a sample of how each RSA Live ESA rule is described on RSA Live:

Rule Name	Description
Logins across Multiple Servers	Detects logins from the same user across 3 or more separate servers within 5 minutes. The time window and number of unique destinations are configurable.

As the name shows, the rule looks for logins across multiple servers. The description explains the rule criteria in more detail and specifies which parameters you modify.

Note: When a rule description includes a configurable parameter, the default setting for the parameter is used. In the sample rule, the description states 5 minutes. However, the time window is configurable so 5 is the default number of minutes.

Prerequisites

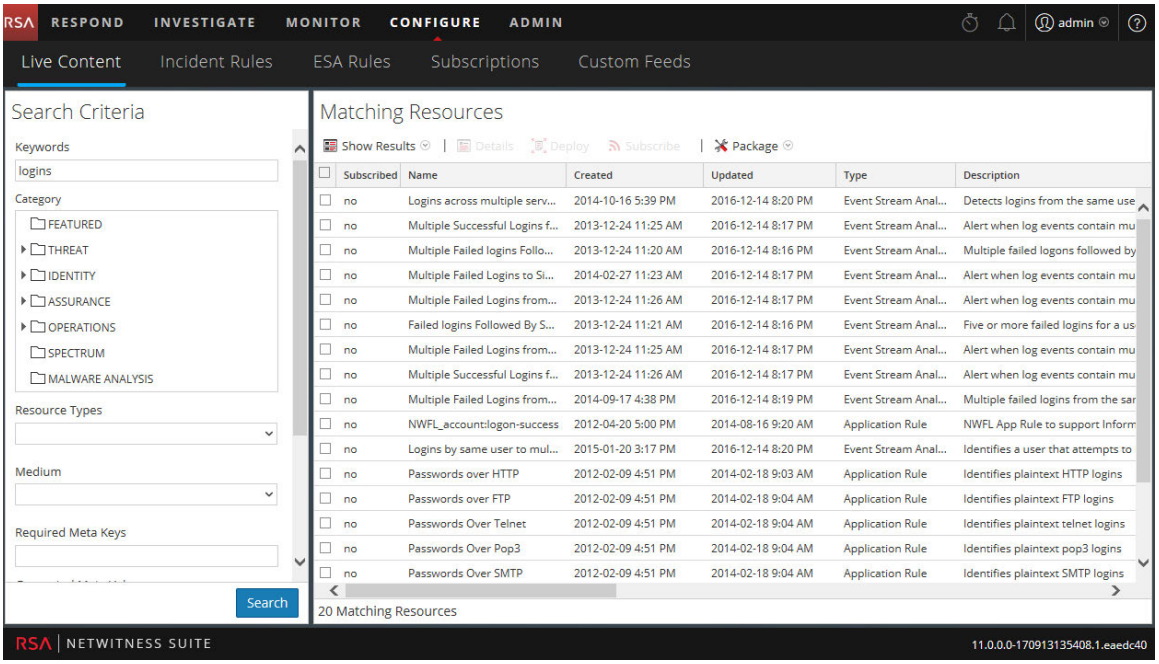
These are the prerequisites for downloading configurable RSA Live ESA rules;

- Have permission to manage rules
- Create a Live Account. See the *Live Services Management Guide* for details.
- Set up Live on NetWitness Suite. See the *Live Services Management Guide*for details.

Procedure

To download configurable RSA Live ESA rules:

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab is displayed.
2. In the options panel, click **Get Rules from RSA Live**.
   The Live Content Search view is displayed.



3. In **Search Criteria**, for **Resource Type** select **RSA Event Stream Analysis Rule**.
4. Specify any of the following criteria to find a rule to configure for your environment.
   For a detailed description of the search criteria, see "The Live Search View" in the *Live Services Management Guide*.
   a. Keywords
   b. Tags

c. Required Meta Keys

d. Generated Meta Values

e. Resource Created Date

f. Resource Modified Date

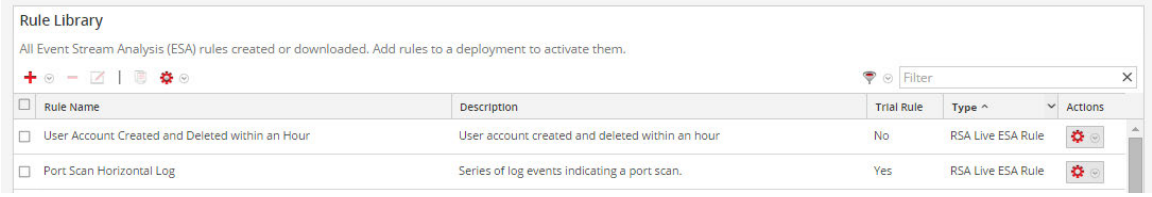
5. Click **Search**. Rules that match the search criteria are displayed in Matching Resources.
6. Select each rule to download and click **Deploy**.
   The Deployment Wizard is displayed
7. Follow the steps in the wizard. If you need more information, see "Deploy Resources in Live" in the *Live Services Management Guide*.

When you finish the steps in the wizard, the selected rules are displayed in the Rule Library.

Customize an RSA Live ESA Rule

This topic explains how to configure parameters in an RSA Live ESA rule. When you download an RSA Live ESA rule, the rule appears in the Rule Library which includes the following columns:

- Name
- Description
- Trial Rule
- Type



The type is RSA Live ESA Rule.

Prerequisites

- Administrator, Operator, SOC Manager, or DPO role permissions are required.
- Rules must be downloaded to the Rule Library.

Procedure

To customize an RSA Live ESA rule:

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
2. In the **Rule Library**, select an RSA Live ESA Rule and click .
   The RSA Live ESA Rule tab is displayed.
3. (Optional) Change the following fields:
   - Rule Name
   - Description
   - Trial Rule (Enabled by default. RSA recommends you run a rule as a trial rule long enough to assess the performance during normal and peak network traffic.)
   - Severity
4. To configure the rule for your environment, in the **Parameters** section replace the default in the **Value** Column.

5. Click **Save**

Add a Rule Builder Rule

This topic introduces a set of end-to-end procedures for adding a Rule Builder type rule.

Each ESA rule is designed to detect something in your network and to generate an alert for it:

- User activity that is not allowed, such as attempting to download software that is not sanctioned
- Suspicious behavior, such as mass audit clearing
- Known malicious threats, such as worm propagation or a password-cracking tool

There are two methods to design a rule in ESA:

- Rule Builder is an easy-to-use interface. You provide a meta key and value, then select choices from lists to complete the criteria.
- Advanced EPL allows you to write queries in the Event Processing Language. You must know EPL syntax.

If you know EPL, you can use either method. If you do not know EPL, you must use Rule Builder. These topics explain the Rule Builder.

Step 1. Name and Describe the Rule

This topic provides instructions to identify a rule, indicate if it is a trial rule and assign a severity level. When you add a new rule, the first information to provide is a unique name and description of what the rule detects. After you save the rule, this information is displayed in the Rule Library.

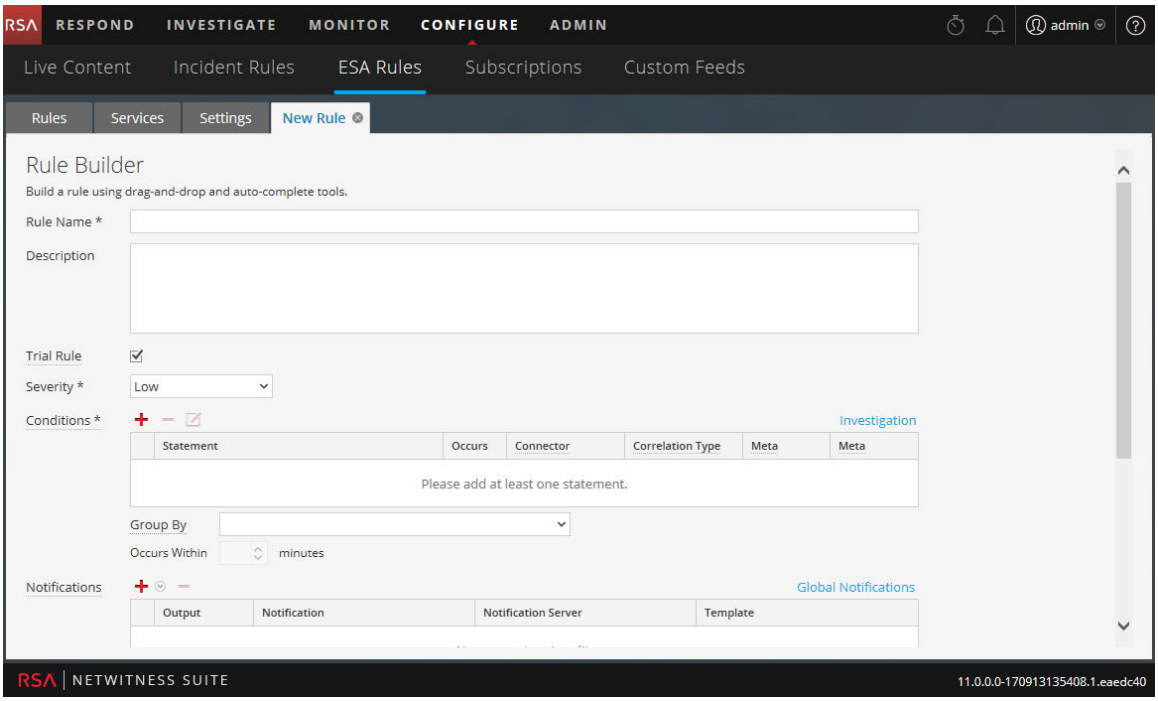
Prerequisites

You must have permission to manage rules. See Role Permissions.

Procedure

To name and describe a rule:

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
2. In the **Rule Library**, select + > **Rule Builder**.
   The New Rule tab is displayed.



3. Type a unique, descriptive name in the **Rule Name** field.
   This name will appear in the Rule Library so be specific enough to distinguish the rule from others.
4. In the **Description** field, explain which events the rule detects.
   The beginning of this description will appear in the Rule Library

5. By default, new rules are configured as a Trial Rule. A trial rule automatically disables the rule if all trial rules collectively exceed the memory threshold. If you are editing an existing rule, you can select **Trial Rule** to safely test the rule edits.
   Use trial rule mode as a safeguard to see if a rule runs efficiently and to prevent downtime caused by running out of memory. For more information, see Work with Trial Rules.
6. For **Severity**, classify the rule as Low, Medium, High or Critical.

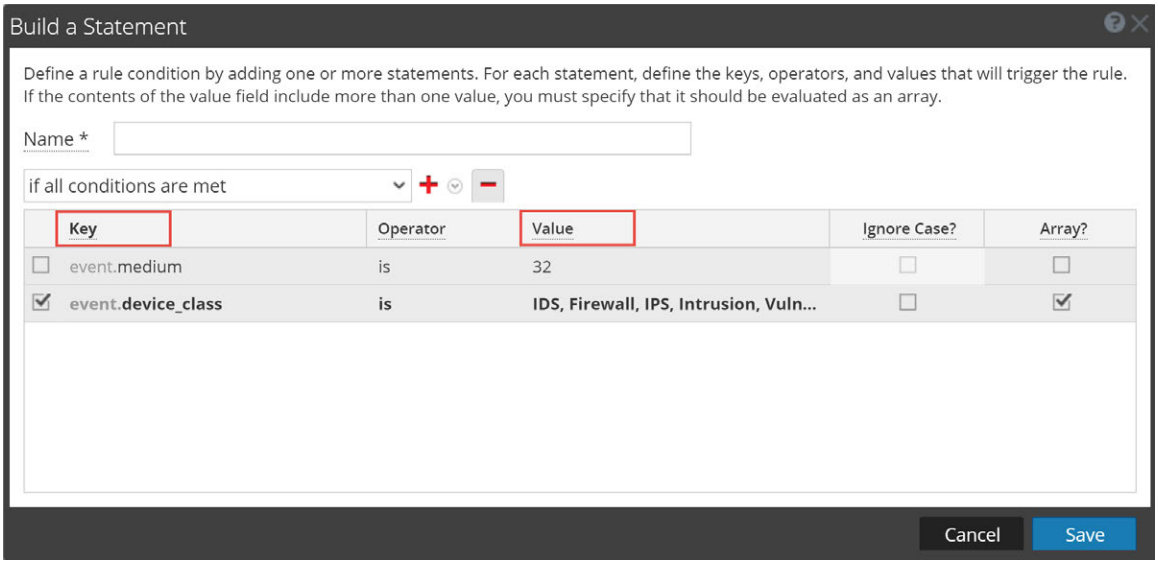
Step 2. Build a Rule Statement

This topic provides instructions to define rule criteria in Rule Builder by adding statements. A statement is a logical grouping of rule criteria in the Rule Builder. You add statements to define what a rule detects.

Example

The following graphic shows an example of a Rule Builder statement.

Every statement contains a key and value. Then, you build logic around the pair by selecting an option in each other field.



Prerequisites

To build a rule statement, you must know the meta key and the meta value.
For a complete list of meta keys, go to **CONFIGURE > ESA Rules > Settings > Meta Key References**.

Procedure

To build a rule statement:

1. Go to **CONFIGURE > ESA Rules**.

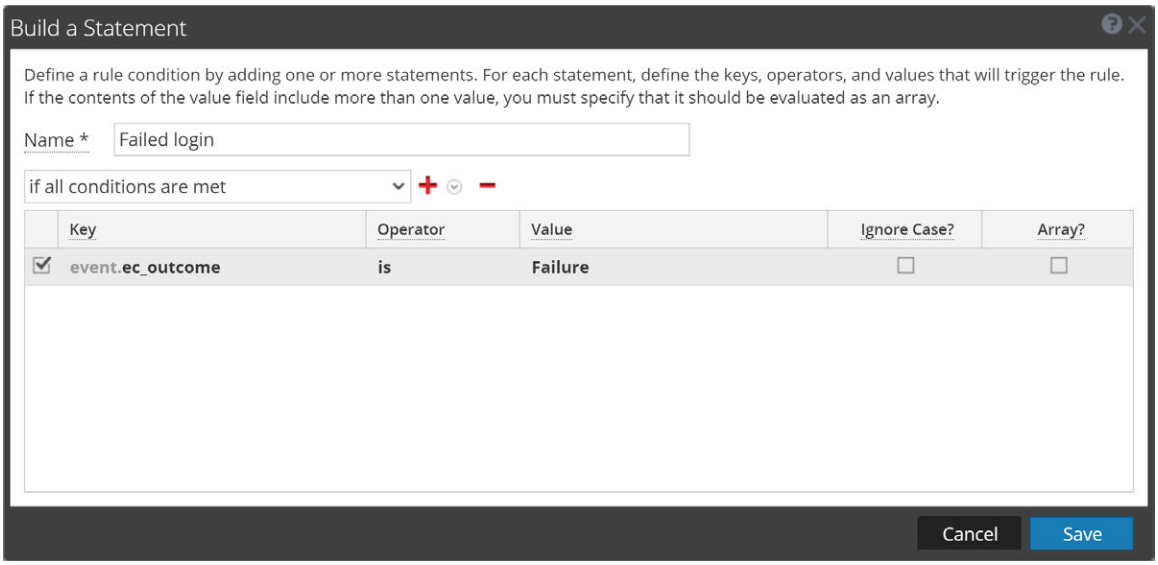
   The Rules tab is displayed by default.

2. In the **Rule Library**, click + > **Rule Builder** or edit an existing Rule Builder rule.

   The Rule Builder view is displayed.

3. In the **Conditions** section, click + .

   The Build Statement dialog is displayed.



4. **Name** the statement. Be clear and specific. The statement name will appear in the Rule Builder.
5. From the drop-down list, select which circumstances the rule requires:
   - if **all conditions** are met
   - if **one of these conditions** are met
6. Specify the criteria for the statement:
   a. For **Key,** type the name of the **Meta Key**.
   b. For **Operator** specify the relationship between the meta key and the value you will provide for it.
      The choices are: is, is not, is not null, is greater than (>), is greater than or equal to (>=), is less than (<), is less than or equal to (<=), contains, not contains, begins with, ends with
   c. Type the **Value** for the meta key.
      Do not add quotes around a value. Separate multiple values with a comma.

d. The **Ignore Case?** field is designed for use with string and string array values. By choosing the **Ignore Case** field, the query will treat all string text as a lowercase value. This ensures that a rule that searches for the user named Johnson would trigger if the event contains "johnson," "JOHNSON," or "JoHnSoN."

e. The **Array?** field indicates if the contents of the Value field represent one or more than one value.

   Select the Array checkbox if you entered multiple, comma-separated values in the **Value** field. For example, "ec_activity is Logon, Logoff" requires you to select the Array checkbox.

7. To use another meta key in the statement, click +, select **Add Meta Condition** and repeat step 6.
8. To add a whitelist, click + and select **Add Whitelist Condition**.
9. To add a blacklist, click + and select **Add a Blacklist Condition**.
10. To save the statement, click **Save**.

To Add a Whitelist

You use a whitelist to ensure that specified events are excluded from triggering the rule. Whitelists can be based on geographic location, or customer-defined enrichment CSV or Context Hub list sources. For example, if you want to create a rule that only triggers for IP addresses outside of the US, you can create a whitelist of US IP addresses.

1. After you add a meta condition, click + and select **Add Whitelist Condition**.
2. In the **EnterWhitelist Name** field, select an enrichment source. Any enrichment source loaded from a CSV or Context Hub list, or a named window in Esper, can be used as the source for a whitelist.
3. For the subcondition:

   a. If you used a GeoIP source for the whitelist, ipv4 is automatically entered for the subcondition. Enter the meta value for the corresponding value field. For example, enter *ipv4 is ip_src* to ensure the GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database. In addition, if you used a GeoIP source for the whitelist, you might want to add a subcondition to specify the geographic region to exclude from the rule results. For example, to specify that the country code must be USA, enter "*CountryCode is US*".

b. If you used a Context Hub list for the whitelist, select a column name from the list, then select an operator and enter the meta value for the corresponding value field.

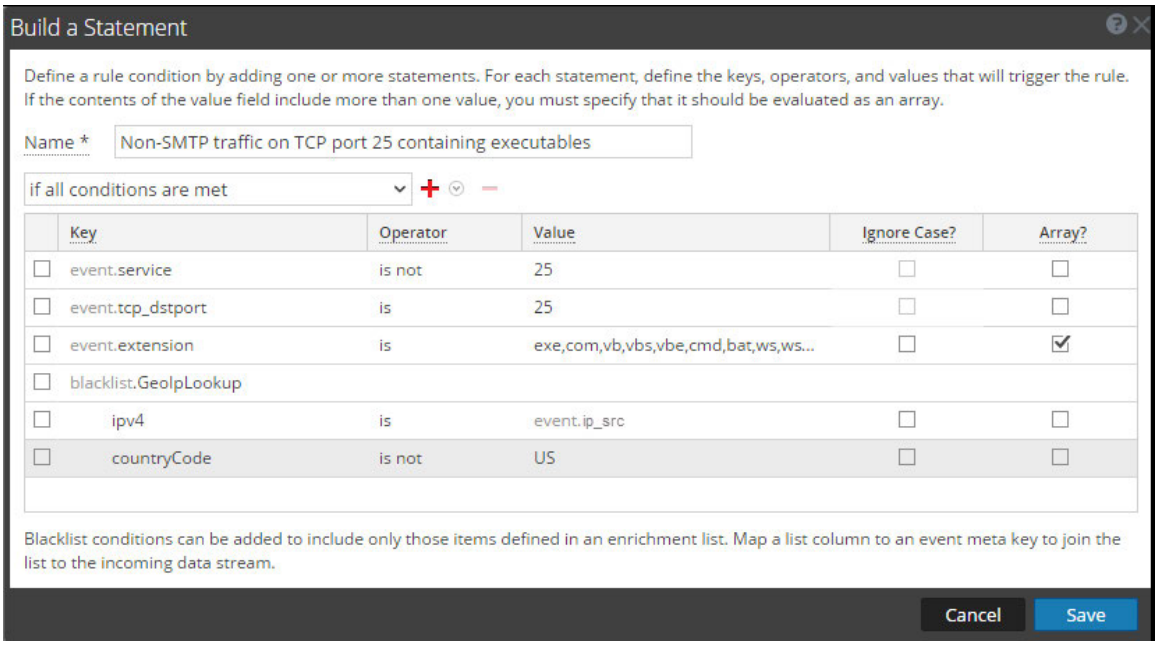
To Add a Blacklist

You use a blacklist to ensure that specified events trigger the rule. Blacklists can be based on geographic location, or customer-defined enrichment CSV or Context Hub list sources. For example, you can specify that the rule only includes results from Germany.

1. After you add a meta condition, click + and select **Add Blacklist Condition**.
2. In the **Enter Blacklist Name** field, select an enrichment source. Any enrichment source loaded from a CSV or a Context Hub list, or a named window in Esper, can be used as a source for a blacklist.
3. For the subcondition:
   a. If you used a GeoIP source for the blacklist, ipv4 is automatically entered for the subcondition. Enter the meta value for the corresponding value field. For example, enter ipv4 is ip_src to ensure the GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database. In addition, if you used a GeoIP source for the blacklist, you might want to add a subcondition to specify the geographic region to include in the rule results. For example, to specify that the rule only includes results for Germany, enter "*CountryCode is DE*".
   b. If you used a Context Hub list for the blacklist, select a column name from the list, then select an operator and enter the meta value for the corresponding value field.

Example: Blacklist

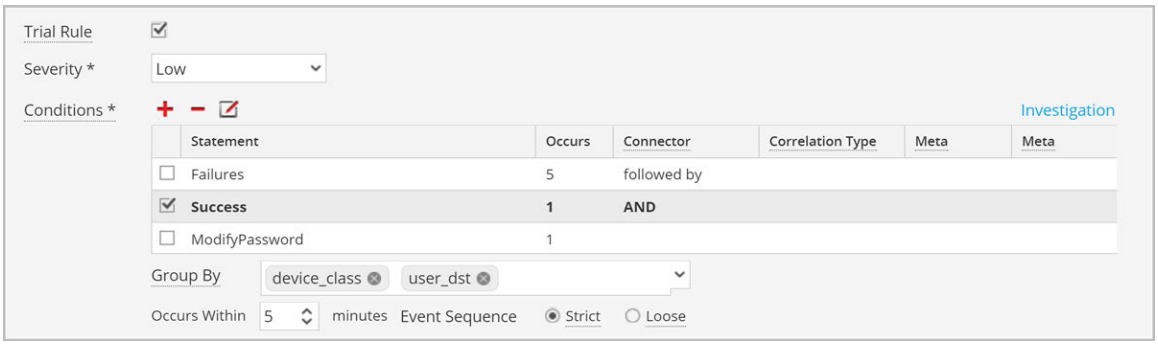
The following statement shows a blacklist statement for a rule that monitors for non-SMTP traffic on TCP destination port 25 containing an executable from countries that are outside of the United States.



Statement	Description
service is not 25	The traffic is not SMTP traffic.
tcp_dstport is 25	The traffic is running on TCP port 25.
extension is exe, com,vb,vbs,vbe,cmd,bat,ws,wsf,src,sh	The file extension is an executable.
GeoIpLookup	The blacklist is based on a GeoIPLookup source.
ipv4 is ip_src	The GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database.
countryCode is not US	When looking up the IP address Event.ip_src in the GeoIP database, the record it returns does not contain "US" in the countryCode field.

Example: Ignoring Case, Strict Pattern Matching, and Using The *Is Not Null* Operator

The following example uses the ability to ignore case, exclude null values, and create a strict pattern match to ensure that it returns the expected rule results. The following conditions make up the rule:

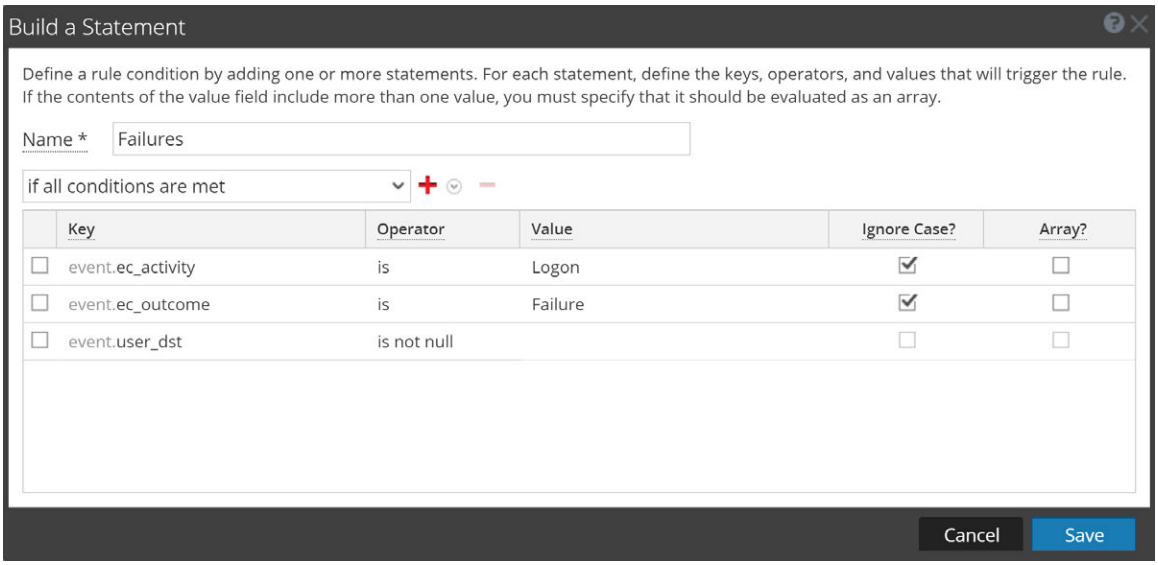


Rule Condition	Description
Failures	This condition searches for five failed logins with a "followed by" connector, meaning that the condition (Failures) must be followed by the next condition (Success).
Success	This condition searches for one successful login.
ModifyPassword	This condition searches for an instance where the password is modified.
GroupBy: user_dst, device class	The GroupBy field ensures that all the previous conditions are grouped by the user_dst meta (the user destination account) and device class. This is important to the construction of the rule because the rule attempts to find a case where a user has attempted to log into the same destination account multiple times, finally logged in successfully, and then changed the password. Grouping by device class ensures that the user logged in from the same machine attempted to log into an account multiple times. The rule may give unexpected results if you do not group the results.
Occurs within 5 minutes	The time window for the events to occur is five minutes. If the events occur outside of this time window, the rule does not trigger.

Rule Condition	Description
Event Sequence: Strict	The event sequence is configured for a strict pattern match. This means that the pattern must match exactly as it is specifiedwith no intervening events. Strict pattern matching allows you to ensure that the Esper engine only generates alerts for rules that exactly match the pattern you want to find. For example, a common rule might be to search for five failed logins followed by a successful login. If you select a loose pattern match, this rule will trigger if there are any number of successful logins between the failed logins. Since the point of the rule is to find frequent *and* sequential login attempts, a strict match is required to ensure that you get the results you expect.

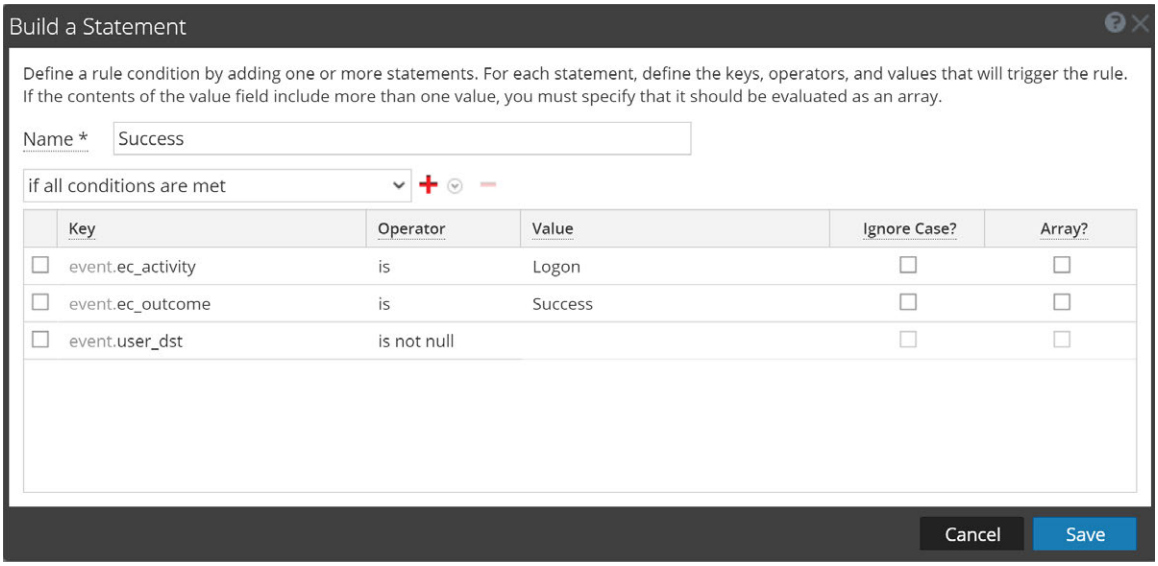
Note: Each of these conditions is explained in further detail in the sections below.

For each condition, a statement is built in the Rule Builder. The following statement makes up the Failures condition:



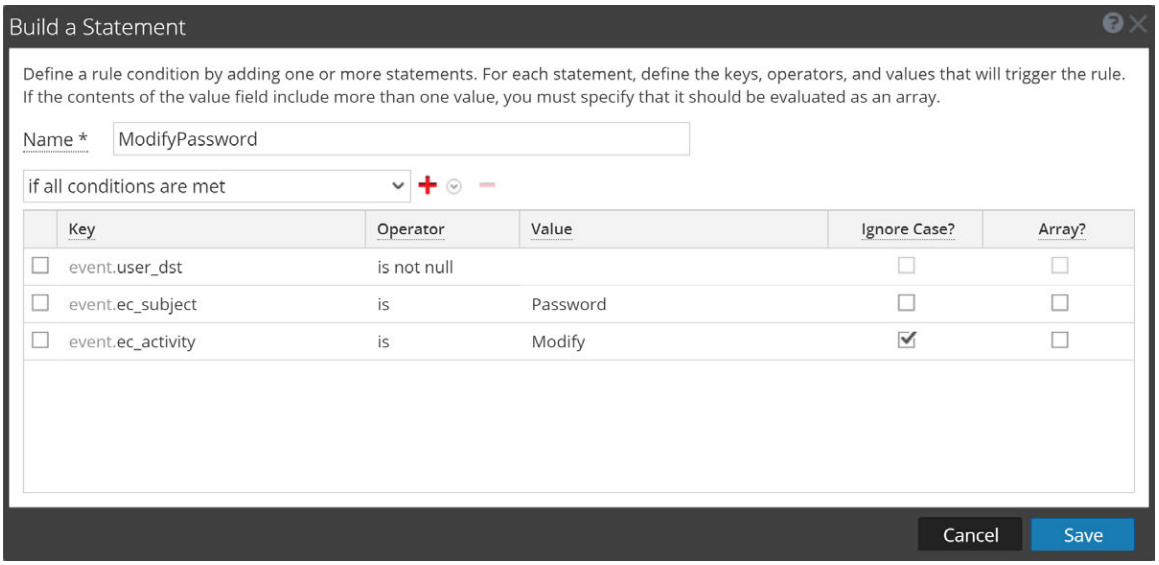
Rule Statement	Description
ec-activity is Logon (ignore case)	Identifies activity that attempts to log on to a system. The **Ignore Case** field is designed for use with string and string array values. By choosing the **Ignore Case** field, the query will treat all string text as a lowercase value. You may want to use this field if you are unsure what case may be used when logging a particular event. Because the case is ignored, the rule can trigger if the activity is logged as Logon, logon, or LoGoN.
ec_outcome is Failure (ignore case)	Identifies activity outcome logged as "failure." Because the case is ignored, the rule can trigger if the activity is logged as "failure", "Failure," or "FaiLuRe."
user_dst is not null	Ensures that the condition is only true if user_dst is populated. The **is not null** operator allows you to ensure that a field returns a value. You may want to use this field when a rule depends on a particular field returning a value. For example, you want to create a rule that identifies the same user attempting to log into the same destination account multiple times (potentially a password-guessing attack). If the field that represents the user destination account is empty, you don't want the rule to trigger. To ensure the field contains a value, you use the **is not null** operator.

The following statement makes up the Success condition:



Rule Statement	Description
ec_activity is Logon	Identifies logon activity.
ec_outcome is Success	Identifies a logon that is successful.
user_dst is not null	Ensures that user destination account field must be populated for the condition to be true.

The following statement makes up the ModifyPassword condition:



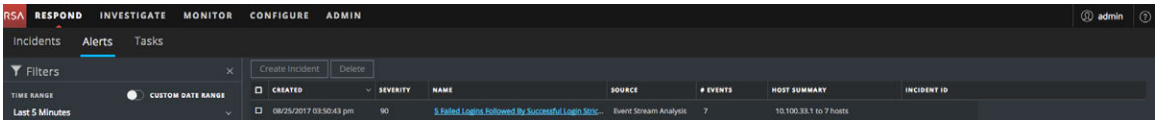
Rule Statement	Description
user_dst is not null	Ensures the user destination account field must be populated for the condition to be true.
ec_subject is Password	Identifies a subject of Password.

Rule Statement	Description
ec_activity is Modify	Identifies activity where the password was modified.

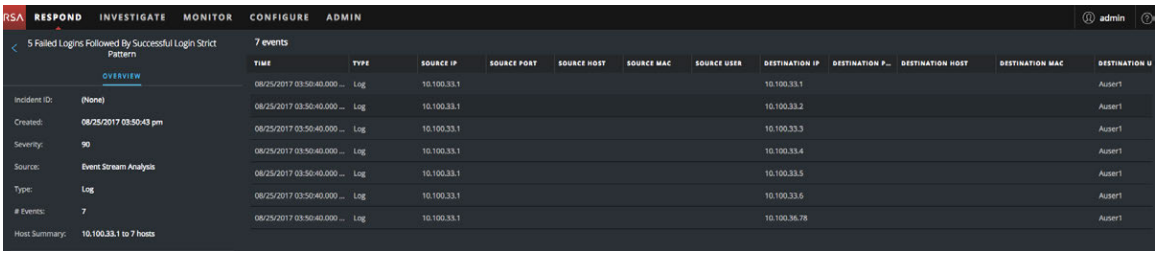
Example Results

When the alert fires for the example rule, you can see that the rule triggered for seven events, and that each event contains a user. You can also see that the events follow a strict pattern: five failed login events, followed by a successful login event, followed by a modification to the account.

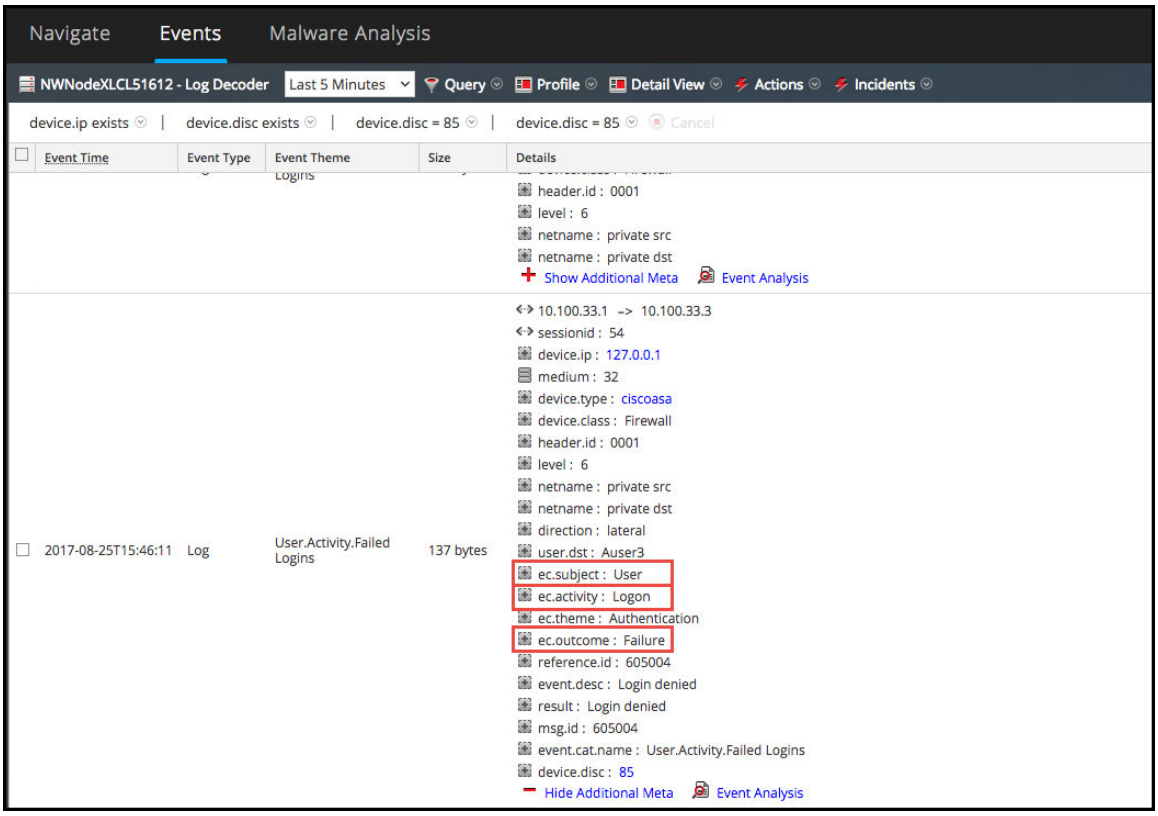
The following figure shows the alert in the Respond Alerts List view.



The next figure shows the events in the alert in the Respond Alert Details view.



Drilling down into the Investigation module by clicking on the source for one of the events, you can see the case for each of the string values. Because you used **Ignore Case**, the rule would trigger if the string values were upper or lower case.

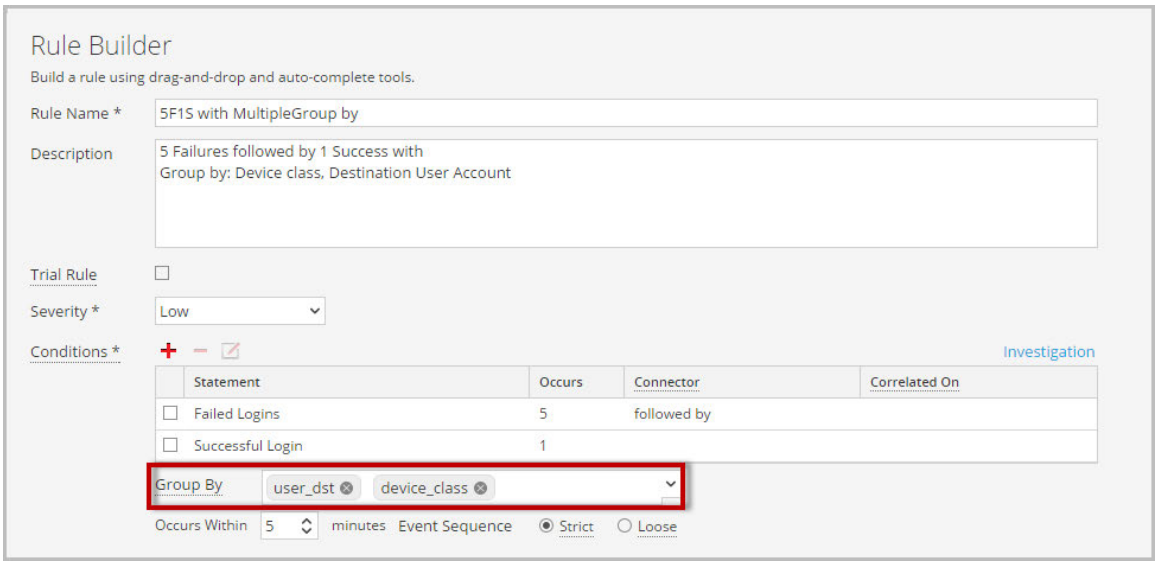


Example: Grouping the Rule Results

The **Group By** field allows you to group and filter rule results. For example, suppose that there are three user accounts; Joe, Jane, and John and you use the **Group By** meta, user_dst. The result will show events grouped under the accounts for Joe, Jane, and John.

You can also group by multiple keys, which can further filter rule results. For example, you might want to group by user destination account and machine to see if a user logged into the same destination account from the same machine attempts to log into an account multiple times. To do this, you might group by device_class and user_dst.

The following example shows a rule grouped by device_class and user_dst.

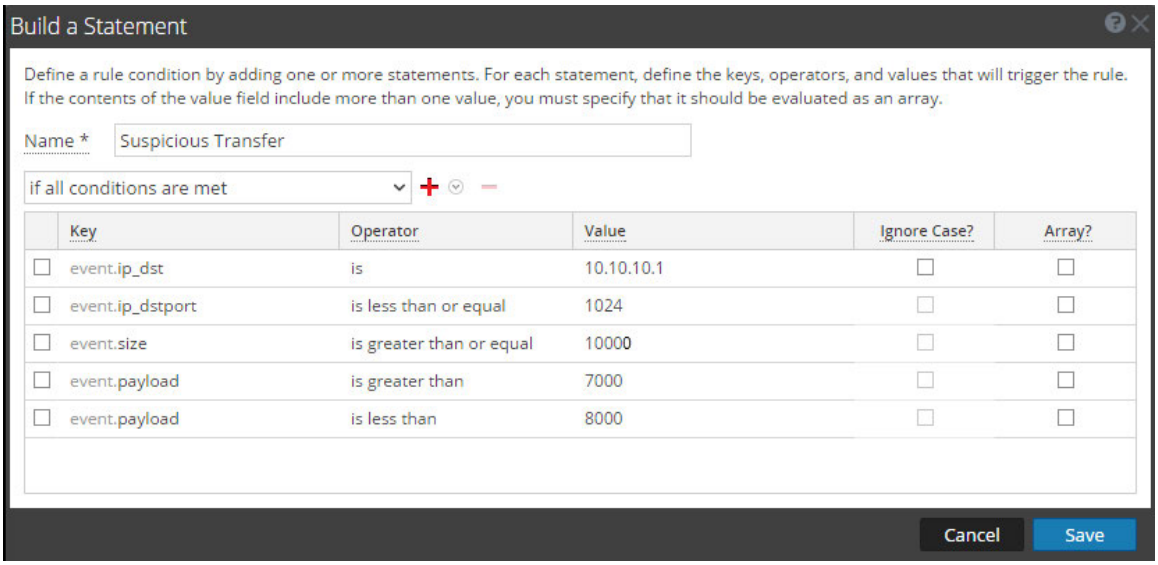


Rule Condition	Description
Failed Logins	Identifies five failed login attempts (must be followed by the next condition; i.e., the five failed logins must be followed by a successful login).
Successful Login	Identifies one successful login.
Group By: user_dst and device_class	Groups the rule results by user_dst (user destination account) and device_class (type of machine the user is logging in from). This allows the rule to look for a user logged in from the same machine to the same destination account, resulting in a much more targeted rule result.
Occurs within 5 minutes with a strict pattern match	The events must occur within five minutes, and the pattern matching is strict, meaning it must follow the pattern exactly for the rule to trigger.

Example: Working with Numeric Operators

Numeric operators allow you to write rules against numeric values, such as specifying that a value is greater than, less than, or equal to a specific value. This is useful particularly for cases where you might want to specify a numeric threshold, i.e., *payload is greater than 7000*.

The following example attempts to identify a data transfer to a particular destination through the common ports where the transfer size is high and the payload is in a suspicious range.



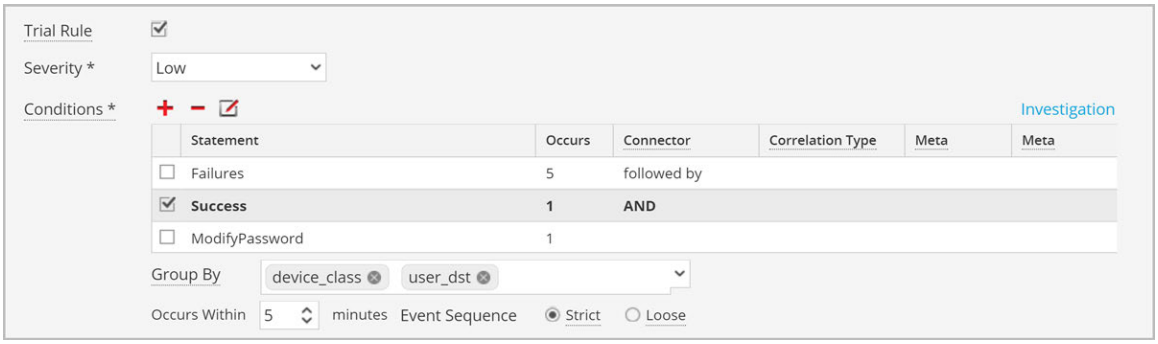
Rule Statement	Description
ip_dst is 10.10.10.1	The destination port is 10.10.10.1.
ip_dstport is greater than or equal to 1024	The destination port is in a commonly used port range, 1024 or greater.
size is greater than or equal to 10000	The size of the transfer is 10000 or greater, which is a suspiciously large transfer.
payload is greater than 7000	The payload is between 7000 and 8000, which is a suspiciously large payload.
payload is less than 8000	The payload is between 7000 and 8000, which is a suspiciously large payload.

Step 3. Add Conditions to a Rule Statement

This topic provides instructions to add conditions, such as specifying a certain time frame, to a rule statement. When you build a statement, you specify what a rule detects. You add conditions to make further stipulations, such as how many times or when the criteria must occur.

Example

The following graphic shows an example of the conditions for Rule Builder statements. Combined, the statements and conditions comprise the rule criteria.



This rule detects 5 failed logon attempts followed by one successful logon, which could be the sign that someone has hacked into user account. This is the criteria for the rule:

A. 5 failed logons are required.

B. 1 successful logon must follow the failures

C. A password was changed.

D. All events must occur within 5 minutes.

E. Group alerts by user (user_dst), because steps A and B must be performed on the same user destination account. Also, group by machine (device_class) to ensure that the user logged in from the same machine attempts to log into an account multiple times.

F. The match is a strict pattern, meaning that the pattern must match exactly with no intervening events.

Procedure

To add conditions to a rule statement:

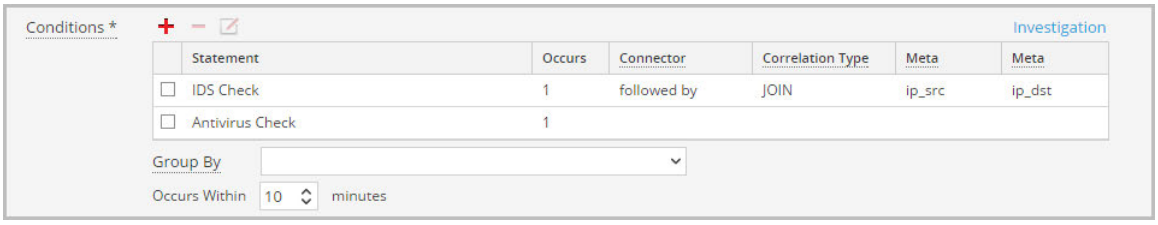
1. In the **Conditions** section, select a statement and click .
2. For **Occurs**, enter a value to specify how many occurrences are required to meet the rule criteria.

3. If you have multiple statements, in the **Connector** field select a logical operator to join one statement to another:
   - followed by
   - not followed by
   - AND
   - OR
4. **Correlation Type** applies only to **followed by** and **not followed by**. If you choose a correlation type of SAME, select one meta to correlate on, and if you choose a correlation type of JOIN, select two meta to correlate on. You may want to use JOIN if you are trying to correlate on meta from two different data sources. For example, say you want to correlate an AV alert with an IDS alert. See the examples below for a use case where two meta from different sources are joined.
5. If events must happen within a specific timeframe, enter a number of minutes in the **Occurs Within** field.
6. Choose whether the pattern must follow a **Strict** match or a **Loose** match. If you specify a strict match, this means that the pattern must occur in the exact sequence you specified with no additional events occurring in between. For example, if the sequence specifies five failed logins (F) followed by a successful login (S), this pattern will only match if the user executes the following sequence: F,F,F,F,F,S. If you specify a loose match, this means that other events may occur within the sequence, but the rule will still trigger if all of the specified events also occur. For example, five failed login attempts (F), followed by any number of intervening successful login attempts (S), followed by a successful login attempt might create the following pattern: F,S,F,S,F,S,F,S,F,S which would trigger the rule despite the intervening successful logins.
7. Choose the fields to group by from the dropdown list. The **Group by** field allows you to group and evaluate the incoming events. For example, in the rule that detects 5 failed logon attempts followed by 1 successful attempt, the user must be the same, so user_dst is the **Group By** meta key. You can also group by multiple keys. Using the previous example, you might want to group by user and machine to ensure that the same user logged in from the same machine attempts to log into an account multiple times. To do this, you might group by device_class and user_dst.

Example

The following graphic shows an example of the conditions for a rule that allow you to evaluate the same entities across multiple devices so you can accomplish complex use cases. For example, you can create a rule that triggers if an IDS (Intrusion Detection System) alert is followed by an AV(Anti-virus) alert for the same workstation. The work station key is not the same between the two (IDS & AV) sources, so you can perform a JOIN in order to evaluate the different entities.

In the IDS alert, the workstation is identified by the source IP address from the IDS alert, and would be compared to the destination IP address from the AV alert.



This is the criteria for the rule:

A. An IDS alert occurs.

B. The destination IP address from the AV alert and source IP address for the workstation from the IDS alert are joined to allow you to view the same entities across different sources.

C. An Antivirus alert follows the IDS alert.

Add an Advanced EPL Rule

This topic provides instructions to define rule criteria by writing an EPL query. EPL is a declarative language for handling high-frequency time-based event data. It is used to express filtering, aggregation, and joins over possibly sliding windows of multiple event streams. EPL also includes pattern semantics to express complex temporal causality among events.

Write an advanced EPL rule when rule criteria is more complex than what you can specify in Rule Builder.

It is outside the scope of this guide to explain EPL syntax.

- For EPL Documentation, see http://www.espertech.com/esper/documentation.php.
- For the EPL Online Tool, see http://esper-epl-tryout.appspot.com/epltryout/mainform.htm

Prerequisites

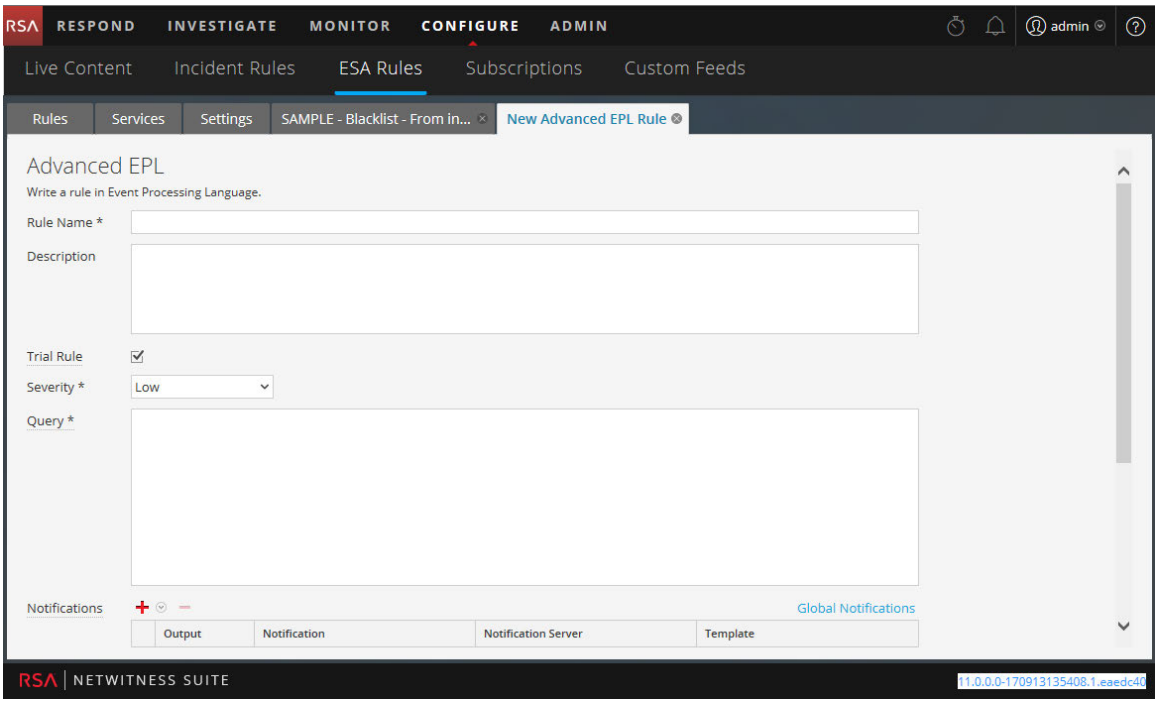
The following are prerequisites for adding an advanced rule:

- You must know Event Processing Language (EPL).
- You must understand ESA Annotations to mark which EPL statements are linked to generating alerts.

Procedure

To add an Advanced EPL rule:

1. Go to **CONFIGURE > ESA Rules**.
2. In the **Rule Library**, select + > **Advanced EPL**.



3. Type a unique, descriptive name in the **Rule Name** field.

   This name will appear in the Rule Library so be specific enough to distinguish the rule from others.

4. In the **Description** field, explain which events the rule detects.

   The beginning of this description will appear in the Rule Library

5. Select **Trial Rule** to automatically disable the rule if all trial rules collectively exceed the memory threshold.

   Use trial rule mode as a safeguard to see if a rule runs efficiently and to prevent downtime caused by running out of memory. For more information, see Work with Trial Rules.

6. For **Severity**, classify the rule as Low, Medium, High or Critical.

7. To define rule criteria, write a **Query** in EPL.

   Note: For all meta key names, use an underscore not a period. For example, `ec_outcome` is correct but `ec.outcome` is not.

8. For dynamic statement name generation in ESA, you must enclose the meta keys in curly brackets and include this annotation in the syntax:

   ```
   @Name("RIG {ip_src} {alias_host} {ec_activity}")
   ```

   where,

   - RIG is the static part of the statement name
   - {ip_src}, {alias_host}, {ec_activity} is the dynamic part of the statement name

   Note: If any of the metas in the dynamic part of the statement name has a null value, it is displayed as a static text.

   If a rule should generate an alert, include this ESA annotation in the syntax:

   ```
   @RSAAlert
   ```

   For more information on ESA Annotations, see ESA Annotations.

Event Processing Language (EPL)

This topic describes Event Processing Language (EPL), a declarative language for dealing with high frequency time-based event data. ESA uses Event Processing Language (EPL), a declarative language for dealing with high frequency time-based event data. It is used for express filtering, aggregation, and joins over possibly sliding windows of multiple event streams. EPL also includes pattern semantics to express complex temporal causality among events. It can perform, but is not limited to, the following functions:

- Filter Event
- Alert Suppression
- Compute percentages or rations
- Average, count, min and max for a given time window
- Correlate events arriving in multiple stream
- Correlate events that arrive out of order
- On-Off Windows
- Followed-by and Not Followed-by support
- Regex filter support

Databases require explicit querying to return meaningful data and are not suited to push data as it changes. The developer must implement the temporal and aggregation logic himself. By contrast, the EPL engine provides a higher abstraction and intelligence and can be thought of as a database turned upside-down. Instead of storing the data and running queries against stored data, EPL allows applications to store queries and continuously run the data through. Response from the EPL engine is real-time when conditions occur that match user defined queries.

Advanced ESA rules require correct character case, but in the Investigation view all characters are converted to lowercase. However, the meta may not be lowercase despite appearances in the Investigation view. To ensure you are using the correct case, RSA recommends you use the *toLowerCase()* function. For example,

```
@RSAAlert(oneInSeconds=0)
SELECT * FROM Event(
/* Statement: Download PDF File */
(filetype.toLowerCase() IN ( 'pdf' ) AND medium IN ( 1 ))
OR
/* Statement: Download EXE File */
(filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' , 'windows executable' ) AND medium IN ( 1 ))
).win:time(5 Minutes)
MATCH_RECOGNIZE (
PARTITION BY ip_src
MEASURES E1 as e1_data , E2 as e2_data
PATTERN (E1+ E2)
DEFINE
E1 as (E1.filetype.toLowerCase() IN ( 'pdf' ) AND E1.medium IN ( 1 )),
E2 as (E2.filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' , 'windows executable' ) AND E2.medium IN ( 1 ))
```

For the purposes of online help, basic statements are used to illustrate how to set up ESA; however, for more information about writing EPL statements, the http://www.espertech.com site provides tutorials and examples.

Note: ESA supports Esper version 5.3.0.

ESA Annotations

This topic describes annotations that NetWitness Suite provides to use in advanced EPL rules.

@RSAAlert Annotation

The @RSAAlert annotation is used to mark which EPL statements are linked to generating alert notifications. It is designed to work with the alert notification suppression feature in the Rule Builder user interface.

The @RSAAlert annotation can be useful when working with alert notifications, especially if you want to filter notifications, such as sending one notification for each user that triggers an alert.

For example, suppose you want to generate alert notifications for login failures. You could add the following statement:

*@RSAAlert select * from event(msg_id="login_fail")*

Event number	Message ID	username	src_IP	Time
1	login_fail	alice	1.2.3.4	10:00
2	login_fail	alice	1.2.3.4	10:01
3	login_fail	alice	6.7.8.9	10:01
4	login_fail	bob	1.2.3.4	10:01
5	login_fail	alice	1.2.3.4	10:03

For the above statement, five alert notifications are generated.

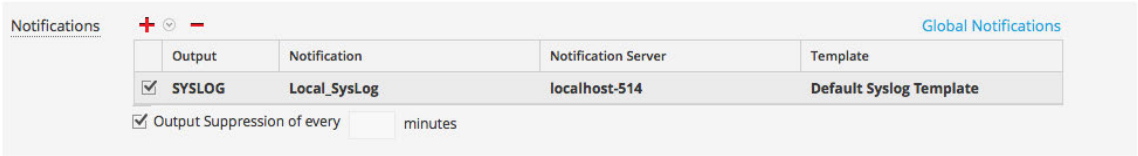
However, suppose you wanted to modify the statement to generate one alert for each separate username. You can use the *identifier* attribute. For example, the statement *@RSAAlert (identifier={"username"}) SELECT* FROM Event(msg_id="login_fail")* generates one notification for the first alert for "bob" and one for the first alert for "alice." Subsequent alerts for "bob" and "alice" are ignored.

You can further distinguish the users by adding details via the identifier variable. For example, you can distinguish by user and IP address using the following statement: *@RSAAlert(identifier={"username", "src_ip"}) SELECT* FROM Event(msg_id="login_fail")*. Then, you would see notifications generated by user name and IP address (one alert for "alice" at 1.2.3.4, another alert for "alice" at 6.7.8.9, and an alert for "bob" at 1.2.3.4).

To Use Identifiers with Alert Notification Suppression:

The @RSAAlert annotation is designed to work with the alert notification suppression feature in the Rule Builder user interface. To do this:

1. Create a rule in the Rule Builder user interface, and select the alert suppression feature when configuring notifications.



2. Copy the code from the Rule Builder rule into a new advanced rule.
3. Configure the advanced rule to include identifiers (as described above) and save the advanced rule.
4. Delete the original rule builder rule.

@RSAPersist Annotation

The @RSAPersist annotation is used to mark a named window as an ESA managed window for persistence. By marking the named window as an ESA managed window, ESA periodically writes the contents of the window to disk and restores them back if the window is un-deployed and re-deployed. The systems take a snapshot just before the module is un-deployed and the window is removed. Conversely, it restores the window contents from the snapshot just after the module is re-deployed. This ensures that the contents of the window are not lost if the module state is altered or if the ESA service goes down.

For example, consider a named window, `DHCPTracker` that holds a mapping from IP addresses to each assigned hostname.You can annotate the statement with the @RSAPersist annotation as:

```
@RSAPersist
 create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
 insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

Note: All windows definitions are not suitable for persistence. `@RSAPersist` annotation must be used with care. If the window has timed-records or if it depends on time based constraints it is very likely that the reverted snapshots will not restore it to the correct state. Also, any changes to the window definition will invalidate the snapshots and reset the window to a blank state. The system does not do any semantic analysis to determine if the changes to the window definition are conflicting or not. Note that other parts of a module (i.e. other than the particular CREATE WINDOW call that defines the window) may change, without invalidating the snapshots.

@UsesEnrichment (10.6.1.1 and later)

The @UsesEnrichment can be used in advanced EPL rules to reference enrichments. In order to synchronize enrichments with ESA, all enrichment dependencies in EPL rules must be referenced with the @UsesEnrichment annotation.

The @UsesEnrichment annotation uses the following format:

```
@UsesEnrichment(name= '<enrichment_name>')
```

For example, the following EPL references a whitelist enrichment:

```
@UsesEnrichment(name = 'Whitelist')
@RSAAlert
SELECT * FROM Event(ip_src NOT IN (SELECT ip_address FROM Whitelist))
```

@Name

The @Name is the statement name defined in ESA advanced rules. It is used to dynamically generate statement names in ESA alerts. The statement name of only an alert triggering statement is displayed. This annotation has meta keys enclosed in curly brackets.

The @Name annotation uses the following format:

```
@Name("<static_part_of_statement_name> {meta_key1} {meta_
key2}…")
```

For example, the following EPL references meta keys *ip_src* and *user_name* whose values will be dynamically generated.

@Name(“Login Event to {ip_src} by {user_name}”)

Note: You can specify any number of meta keys in the statement for dynamic statement name generation.
The length of individual meta key is limited to 64, after which the value is truncated and appended with “…”.
The length of the dynamic generation of statement name is limited to 128, after which the value is truncated to 128 and appended with “…”. All the remaining values post truncation will be treated as static values.

Sample Advanced EPL Rules

Following are the examples of Advanced ESA rules. Each example has multiple ways of implementing the same use-case.

Example #1:

Create an user account and delete the same user account in 300s. User information is stored in user_src meta.

EPL #1:

Rule Name	CreateuseraccountFollowedbyDeletionof Useraccount1
Rule	Create a user account followed by an action to delete the same user account in

Description	300 seconds.

Rule Code	`SELECT * FROM Event(ec_subject='User'`
	`  AND ec_outcome='Success'`
	`  AND user_src is NOT NULL`
	`  AND ec_activity IN ('Create', 'Delete')`
	`  ).win:time(300 seconds)`
	`match_recognize (partition by user_src`
	`   measures C as c, D as d`
	`   pattern (C D)`
	`  define`
	`   C as C.ec_activity='Create' ,`
	`   D as D.ec_activity='Delete');`

Note	• Filter events needed for pattern in given time frame. Filter conditions should be such that only required events are passed to match recognize function. In this case, they are create and delete user account Events. i.e. Event(ec_subject='User' AND ec_outcome='Success' AND user_src is NOT NULL AND ec_activity IN ('Create', 'Delete') • Partition by creates buckets. In this case, esper creates buckets per value of user_src. And hence value of user_src is common between both events. • Define pattern you want. Right now it is set to Create Followed by Delete. You can do multiple creates followed by delete (C+ D). Pattern is very similar to regular expression. • Most efficient use case.

EPL #2:

Rule Name	CreateuseraccountFollowedbyDeletionof Useraccount2
Rule Description	Create a user account followed by an action to delete the same user account in 300 seconds.

Rule Code	`SELECT * from pattern[every (a= Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create'))`
	`  ->`
	`( Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create') AND`

	user_src = a.user_src)))where timer:within(300 Sec)];
Note	• Lets say same user is created twice and deleted once in that order. Then the above pattern will fire 2 alerts. • A thread is created for every User creation. • There is no way to control threads. It is important to have time bonds and preferably small intervals.

Example #2:

Detect pattern where user created followed by login by same user and user is deleted in end. In case of windows logs user info is stored in either user_dst or user_src depending on event.

user_src(create) = user_dst(Login) = user_src(Delete)

EPL #3:

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.
Rule Code	SELECT * FROM Event(ec_subject='User' and ec_activity in ('Create','Logon','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success').win:time(300 seconds) match_recognize (measures C as c, L as l, D as d pattern (C L D) define C as C.ec_activity = 'Create', L as L.ec_activity = 'Logon' AND L.user_dst = C.user_src, D as D.ec_activity = 'Delete' AND D.user_src = C.user_src);
Note	• Since user_src/user_dst is not common across all events we can't use partition. It will be 1 single bucket running 1 pattern at a time. For example, for user 1 and 2 if the stream of events are C1C2L1D1, C1L1C2D1, there will be no alert because C1 thread got reset by C2. Alert will be fired only if C1L1D1 are in order and no other event either from same user or other user

	falls in between. • Another solution would be to use Named Window and merge user_dst and user_src into single column and then run match recognize. (EPL #3). • Pattern can also be used. You might get more alerts than expected. (EPL #4).

EPL #4: Using NamedWindows and match recognize

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.

Rule Code	`@Name('NormalizedWindow')create window FilteredEvents.win:time(300 sec) (user String, ecactivity string, sessionid Long);`
	`@Name('UsersrcEvents') Insert into FilteredEvents select user_src as user, ec_activity as ecactivity, sessionid from Event(ec_subject='User' and ec_activity in ('Create','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_src is not null );`
	`@Name('UsrdstEvents') Insert into FilteredEvents select user_dst as user, ec_activity`
	`as ecactivity, sessionid from Event(ec_subject='User' and ec_activity in (Logon') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_dst is not null );`
	`@Name('Pattern')`
	`@RSAAlert(oneInSeconds=0, identifiers={"user"})`
	`select * from FilteredEvents`
	`match_recognize (`
	`partition by user`
	`measures C as c, L as l, D as d`
	`pattern (C L+D)`
	`define C as C.ecactivity= 'Create',`
	`L as L.ecactivity= 'Logon',`
	`D as D.ecactivity='Delete'`
	`);`

EPL #5: Using Every @RSAAlert(oneInSeconds=0, identifiers={"user_src"})

SELECT a.time as time,a.ip_src as ip_src,a.user_dst as user_dst,a.ip_dst as ip_dst,a.alias_host as alias_host from pattern[every (a=Event (`ec_subject`='User' and `ec_activity`='Create' and `ec_theme`='UserGroup' and `ec_outcome`='Success') -> (Event(`ec_subject`='User' and `ec_activity`='Logon' and `ec_theme`='Authentication' and `user_src`=a.user_dst) -> b=Event (`ec_subject`='User' and `ec_activity`='Delete' and `ec_theme`='UserGroup' and `user_dst`=a.user_dst))) where timer:within(300 sec)];

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.

Example #3:

Excessive login failures from same sourceIP

EPL #6: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Rule Name	ExcessLoginFailure
Rule Description	The same user tried logging in from the same Source IP and faced login failures
Rule Code	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time_length_batch(300 sec, 10) GROUP BY ip_src HAVING COUNT(*) = 10;`
Note	• Creates window per ip_src • Uses time_length_batch: Looks at events in batches(tumbling window). Every event will be part of only 1 window. Window releases events either when time elapses or count is reached. • One of issues with tumbling windows that events occurring towards end of batch might not lead to an alert. In below sequence of events at t=301 even though 10 login failures occurred for same login in last 300 secs there will be no alert because batch of events was dropped at t=300

Time t	Login Failures for Specific Users	Alert	Time Batch
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3
850	3	0	3
900	1	1	3 ends and 4 begins

- Above problem can be resolved using win:time windows (EPL#7)instead of win:time_length_batch windows.
- Outer group by is to control events when time elapses. Say you have 9 events at end of 60 secs, esper engine will push those 9 events to listener. Group by and count will restrict it since count is not equal to 10.
- Time and count can be modified as needed.

EPL #7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Rule Name	ExcessLoginFailure
Rule Description	The same user tried logging in from the same Source IP and faced login failures
Rule Code	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_src HAVING COUNT(*) = 10`
Note	• This is sliding window and hence once alert is fired for a set of events they can be used for another alert as well till time has passed. • If 10 events were involved in causing alert only last event will appear

	• If < or > are used then you might see more than 1 alert. You should use alert suppression accordingly.

Example #4:

Multiple failed logins from multiple different users from same source to same destination, a single user from multiple different sources to same destination.

EPL #8: using groupwin , time_length_batch and unique

Rule Name	MultiplefailedLogins
Rule Description	There are multiple failed logins for the following cases: - From multiple users from same source to same destination. - Single user from multiple sources to the same destination.
Rule Code	`SELECT * FROM Event( ec_activity='Logon' AND ec_outcome='Failure' AND ip_src IS NOT NULL AND ip_dst IS NOT NULL AND user_dst IS NOT NULL ).std:groupwin(ip_src,ip_dst).win:time_length_batch(300 seconds, 5}).std:unique(user_dst) group by ip_src,ip_dst having count(*) = 5;`
Note	• ip.dst and ip.src are common across all events. • user_dst is unique for all events. • Alert is fired when there are atleast 5 different users try to login from same ip.src and ip.dst combination.

Example #5:

No Log traffic from a device in a given timeframe.

EPL #9: using groupwin , time_length_batch and unique

Rule Name	NoLogTraffic
Rule Description	There is no log traffic observed from a device in a given time frame.
Rule Code	`SELECT * FROM pattern [every a = Event(device_ip IN ('10.0.0.0','10.0.0.1') AND medium = 32) -> (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND`

Note	`device_type = a.device_type AND medium = 32))];` • Rule only detects sudden loss of traffic. It won't alert if there is no traffic to begin with. You need at least 1 event for rule to alert. • List of device ip address or device hostnames as input. Only these systems will be tracked. • Time input is required. Alert is fired when time interval between events exceeds input time.

Example #6:

Multiple Failed Logins NOT followed by a Lockout event by the same user.

EPL #10: using groupwin , time_length_batch and unique

Rule Name	FailedloginswoLockout
Rule Description	There are multiple failed logins that are not followed by Lockout event by the same user.

Rule Code	`SELECT * FROM pattern [every-distinct(a.user_dst, a.device_ip, 1 msec) (a= Event(ec_activity='Logon' and ec_outcome='Failure' and user_dst IS NOT NULL)-> [2]( Event( device_ip =a.device_ip and ec_activity='Logon' and ec_outcome='Failure' and user_dst=a.user_dst)`
	`AND NOT Event( ( ec_activity='Logon' and ec_outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst))))`
	`where timer:within(60 seconds) -> (timer:interval(30 seconds) and not Event(device_ip=a.device_ip and user_dst=a.user_dst and ec_activity='Lockout'))];`

Note	• Above query detects the absence of a Lockout Event after the occurrence of 2 failed logins from same user. • The occurrence of the multiple failed logins are timed and are assumed to occur within a certain period of time. Also, in-practice the Lockout event is assumed to occur within a short time after the occurrence of the last failed login event because the threshold value of Failed logins per user is set in a

	given domain. • In current query, every distinct will suppress new thread for combination of user and device for 1 millisec. • Time allowed for 3 failed logins is 60 secs since 1st failed attempt. Wait period for lockout event to occur is 30 secs

Example #7:

Custom functions to perform LIKE and REGEX operations for ARRAY elements.

EPL #11: @RSAAlert(oneInSeconds=0)

Rule Name	MatchLikeRegex
Rule Description	There are custom functions to perform LIKE and REGEX comparisons of array meta keys.

Rule Code	`SELECT * FROM pattern[`
	`e1=Event(matchLike(alias_host, "10.0.0.%")) AND`
	`e2=Event(matchRegex(alias_host, "10\.0\.0\.1[0-9][0-9]"))`
	`where timer:within(5 Minutes)];`

Note:
1. "." in meta keys should be replaced with ("_").
2. All patterns should be time bound.
3. Use of appropriate tags in front of statements
 a) @RSAPersist:
 b) @RSAAlert:

For additional details you can refer to:

- EPL Documentation: http://www.espertech.com/esper/documentation.php
- EPL Online Tool: http://esper-epl-tryout.appspot.com/epltryout/mainform.html

Working with Rules

This topic discusses additional procedures you can perform on rules. You may want to perform any of the following procedures:

- Edit, Duplicate or Delete a Rule
- Filter or Search for Rules
- Import or Export Rules

Edit, Duplicate or Delete a Rule

This topic provides instructions to edit, duplicate, or delete an Event Stream Analysis (ESA) rule. When you edit a rule, ESA applies the updated criteria going forward. No changes are made to previously generated alerts.

Procedures

Edit a Rule

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
   The Rules tab is displayed.
2. In the **Rule Library**, select the rule you want to edit and click .
   Depending on the rule type, the respective rule tab is displayed.
3. Modify the required parameters.
4. Click **Save**.

Duplicate a Rule

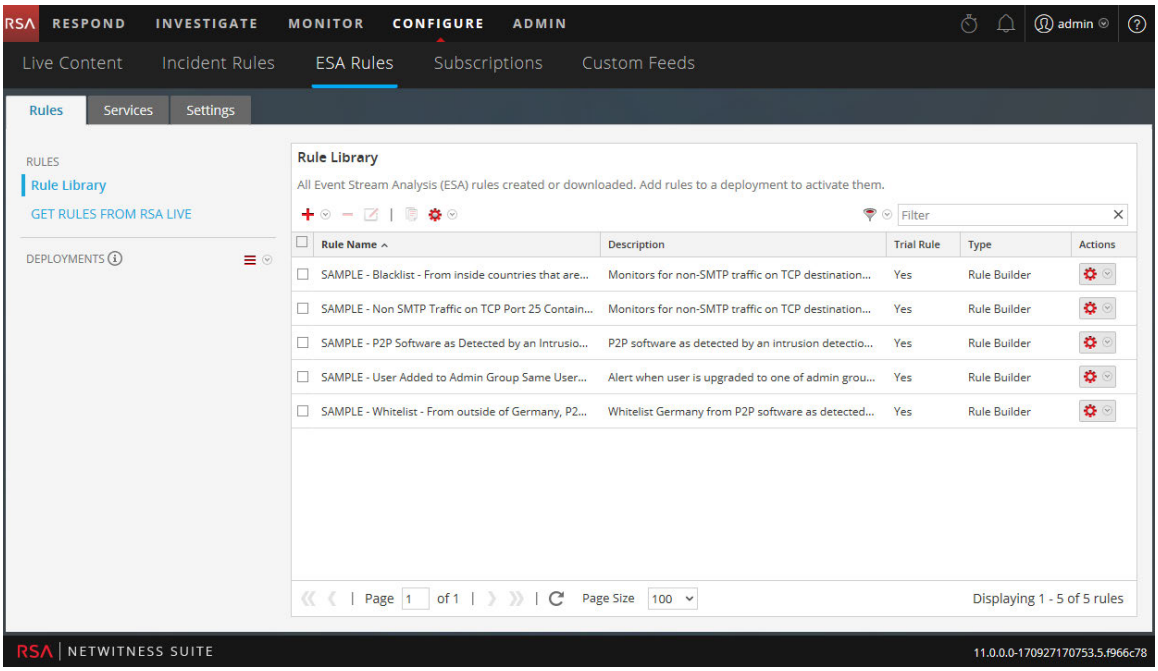
1. In the **Rule Library**, select the rule you want to duplicate and click .
2. The Duplicate a Rule dialog is displayed. The system adds **Copy of** in front of the rule name.

3. In the **Name** field, type a unique name for the duplicate rule and click **OK**.

A duplicate rule with the new name is added to the Rule Library.

Delete a Rule

1. Go to **CONFIGURE > ESA Rules > Rules**.
   The Rules tab is displayed.



2. In the Rule Library, select one or more rules and click −.

   A warning dialog is displayed.

3. Click **Yes**.
   A confirmation message that the rule is deleted successfully is displayed and the selected rule is deleted from the Rule Library.

Filter or Search for Rules

This topic shows analysts how to specify the type of rules that display in the Rule Library.

Prerequisites

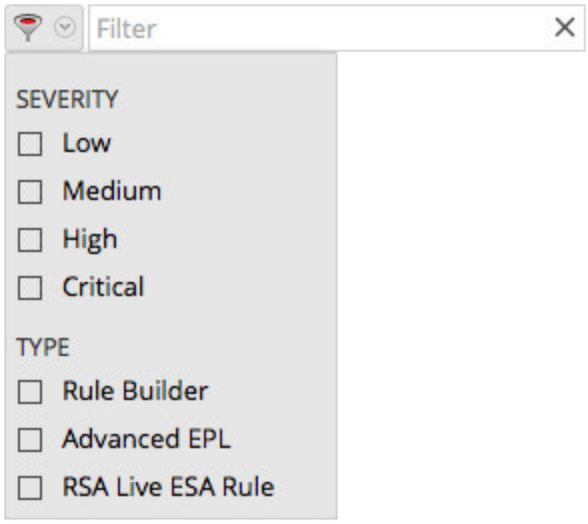
Make sure that you understand the Rule Library view components. For more information, see Rule Library Panel.

Procedures

Filter

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab is displayed by default.

2. In the **Rule Library** panel toolbar, click and select the severity and type of rules that you would like to appear in the Rule Library list. The following figure shows the Filter drop-down list.



The selected rule types appear in the list.

Search

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab is displayed by default.
2. In the **Rule Library** panel toolbar, type a rule name in the Filter field.
   The Rule Library panel lists the rules that match the names entered in the Filter field.

Import or Export Rules

The topic provides instructions to import ESA rules from a NetWitness Suite instance and to export ESA rules to your hard drive so you can keep a local copy.

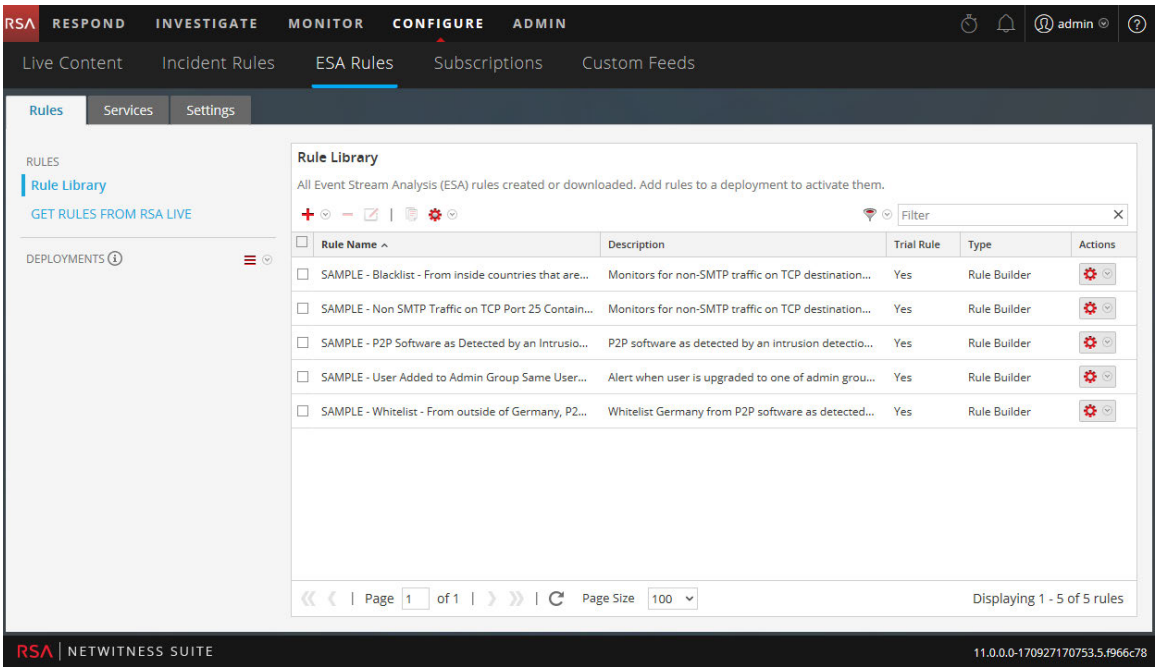
If you exported a rule in an earlier version of NetWitness Suite, the following conditions apply when you import the rule in version 10.5 or later:

- Exported in version 10.3 – You cannot import rules to version 10.5 or later.
- Exported in version 10.4 – You can import rules to version 10.5 or later.

Procedures

Import ESA Rules

1. Go to **CONFIGURE >ESA Rules > Rules** tab.
   The Rules tab is displayed.



2. In the **Rules Library** toolbar, select > **Import**.
   The Import ESA Rules dialog is displayed.

3. Click **Browse** to browse and select the file containing the ESA rules.
4. Click **Import**.

Export

1. Select an ESA rule or multiple rules and select > **Export** in the Rule Library toolbar.
   A warning dialog is displayed.
2. Click **Yes**.
   The Export Rules dialog is displayed.
3. In the **Enter File Name** field, type a filename for the file with the ESA rules and click **Export**.
   The file is exported as a binary file to your machine.

Note: The binary file cannot be edited.

Choose How to be Notified of Alerts

This topic explains the different notification methods and how to add a notification method to a rule. Administrator, SOC Manager or DPO role permissions are required for all tasks in this section.

When a rule triggers an alert, ESA can send a notification in the following ways:

- Email
- SNMP
- Syslog
- Script

To configure a notification, you configure these components:

- Notification server – After you configure a notification server, you can add it to a rule. When the rule triggers an alert, the rule will use that server to send alert notifications.
- Notifications – These are the outputs, which can be email, script, SNMP, and Syslog. When you design a rule, you can specify the notification for an alert.
- Templates – The format of an alert notification is defined in a template.

Alert suppression and alert rate regulation are two features that Event Stream Analysis provides. Alert suppression ensures that multiple emails are not sent out for the same alert. For example, consider a rule to detect failed user logins. If you set the alert suppression to three minutes, you will see only the alerts generated in that time frame. This is fewer than the number of alerts you would see without alert suppression. Some alerts can be duplicates. With alert suppression, emails are not sent for duplicate alerts. This ensures the inbox is not flooded with redundant alert notifications.

Alert rate regulation is a preventive measure to ensure that alerts from misconstrued rules do not flood the system. This ensures that ESA does not send more than the configured limit of emails within one minute.

Notification servers, notifications, and templates are configured in the Administration System view. For more information, see "Configure Notification Servers", "Configure Notification Outputs", and "Configure Templates for Notifications" in the *System Configuration Guide*.

Notification Methods

When a rule triggers an alert, ESA can send a notification in the following ways:

- Email
- SNMP
- Syslog
- Script

Email Notifications

Event Stream Analysis can send notifications to users through email about various system events.

To configure these email notifications, you need to:

- Configure the SMTP email server as an output provider. For instructions, see "Configure the Email Settings as Notification Server" in the *System Configuration Guide*.
- Set up an email account to receive notifications. For instructions, see "Configure Email as a Notification" in the *System Configuration Guide*.
- Configure a template for email notification. For instructions, see "Configure a Template" in the *System Configuration Guide*.

SNMP

Event Stream Analysis can send events as an SNMP trap to a configured SNMP trap host.

Note:
The MIB file **NETWITNESS-MIB.txt** is located on the ESA RPM at the following location */usr/share/snmp/mibs*. With the MIB file, you will be able to identify the SNMP alerts trigerred from ESA. And, the Trap OID value for ESA is 20.

To configure these SNMP notifications, you need to:

- Configure SNMP trap host settings as an output provider. For instructions, see "Configure the SNMP Settings as Notification Server" in the *System Configuration Guide*.
- Configure SNMP trap settings as an output action. For instructions, see "Configure SNMP as a Notification" in the *System Configuration Guide*.
- Configure a template for SNMP. For instructions, see "Configure a Template" in the *System Configuration Guide*.

Syslog

Event Stream Analysis can send events and consolidate logs in Syslog format to a Syslog server.

To configure these Syslog notifications, you need to:

- Configure Syslog server settings as an output provider. For instructions, see "Configure the Syslog Settings as Notification Server" in the *System Configuration Guide*.
- Configure Syslog message format as an output action. For instructions, see "Configure Syslog as a Notification" in the *System Configuration Guide*.
- Configure a template for Syslog. For instructions, see "Configure a Template" in the *System Configuration Guide*.

Script Alerter

Apart from the alert notifications ESA allows users to run scripts in response to ESA alerts.

Scripts enable you to do custom integration with applications that exist in your environment. For example, if you want to open an incident ticket from an application when a specific alert is triggered, Script Alerter lets you write a script that calls the application API and has ESA invoke it when the specific ESA rule is triggered. You can configure a FreeMarker template to define what details you want to extract from the output of the ESA rule and pass it as command line arguments to the script.

To use the Script Alert, you need to:

- Configure the user identity and other details that are required to execute the script. For instructions, see "Configure Script as a Notification Server" in the *System Configuration Guide*.
- Define the Script. For instructions, see "Configure Script as a Notification" in the *System Configuration Guide*.
- Configure a template for the script. For instructions, see "Configure a Template" in the *System Configuration Guide*.

Add Notification Method to a Rule

This topic tells administrators how to add a notification, such as email, to a rule. ESA uses the notification method when it generates an alert for an event that meets rule criteria.

You add a notification to a rule so ESA can let you know when a rule triggers an alert. Although the notification fields are not required, it is a best practice to add a notification to a rule.

When you add a notification method to a rule, you select the following information:

- Output
- Notification
- Notification Server
- Template

Prerequisites

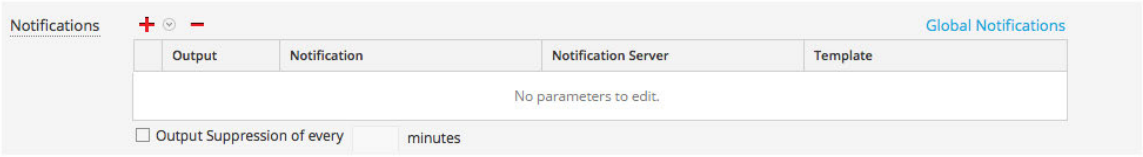
- Your role must have permission to manage rules.
- The rule must exist.
- The notification method must be configured with a supported server and template:
  Go to **ADMIN** > **System > Global Notifications**.

  For detailed procedures, see the *System Configuration Guide*.

Procedure

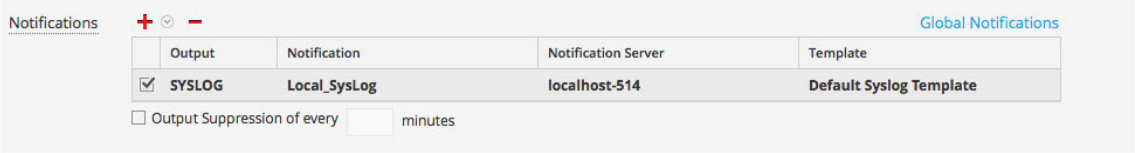
To add a notification method to a rule:

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
2. In the **Rule Library**, click to add a new rule or select an existing rule and click .
   Depending on the rule type, the Rule Builder or Advanced EPL tab is displayed.
   The Notifications section is the same for both tabs.



3. Click and select the **Output** for the alert:
   - Email
   - SNMP
   - Syslog
   - Script
4. Double-click the **Notification** field and select the name of a previously configured output.
   For example, Level 1 Analyst could be the name of an email notification that goes to the L1-Analysts email distribution group.
5. Double-click the **Notification Server** field and select the server that sends the notification.

6. Double-click the **Template** field and select a format for the alert.
   The following figure shows the settings for a Syslog notification.

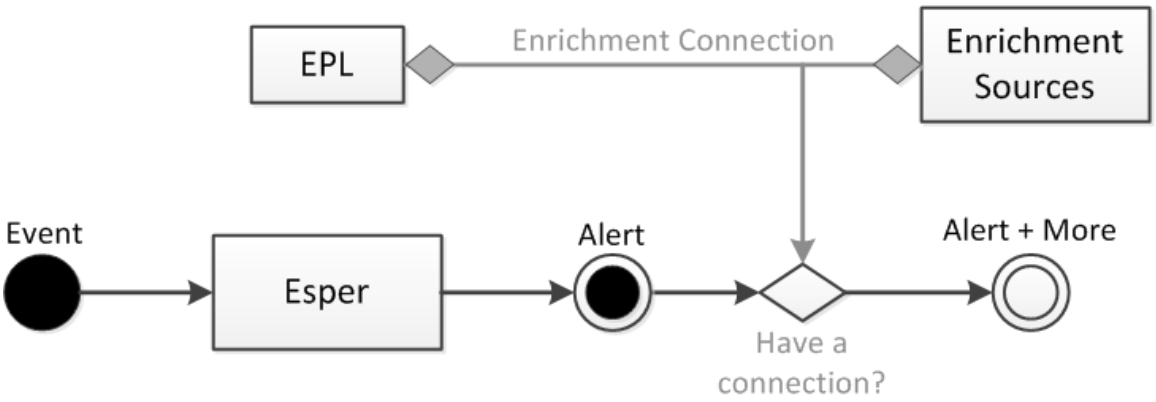


7. If you want to specify frequency, select **Output Suppression**, then enter the number of **minutes**.
8. If you want to add another notification, repeat steps 3-7.
9. Click **Save**.
   When ESA generates an alert for an event that matches the rule criteria, you will be notified of the alert via each notification method added to the rule.

Add a Data Enrichment Source

This topic tells how to add a previously configured enrichment source to a rule. When ESA creates an alert, information from the source gets included in it.

Enrichments provide the ability to include contextual information into correlation logic and alert output. Without enrichments, all information included in an ESA alert is from a Core service. With enrichments, you can request for look ups into a variety of sources and include the results into the outgoing alerts. The following figure illustrates the enrichment feature.



Enrichment configuration is made up of two logical units:

- Enrichment Sources – These are data stores of contextual information.
- Enrichment Connections – These act as connectors between alert meta and source columns.

ESA allows you to make connections between Event Processing Language (EPL) statements and enrichment sources. Once the connections are established, the system joins the selected fields from the alert output with the information in the sources and uses the matching data to enrich the alert that is sent out. ESA can connect with the following sources:

- Esper Named Windows
- Relational Database tables
- MaxMindGeoIP Database
- RSA Warehouse Analytics Watchlists

Note: The geoIP enrichment source can neither be created nor deleted. It is provided out of the box to the user.

Sample Rule with Enrichment

The following sample rule illustrates the enrichment feature provided by ESA:

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login
Failure')
```

The rule generates an alert for every logon failure and thus if the following (simplified) event stream is received at ESA:

sessionid	ec_ theme	username	ip_src	ip_dst	host_dst
1	Login Success	dshrute	23.xx.23x.16		
2	Login Failure	jhalpert	23.xx.23x.16	31.1x.x9.1x8	www.facebook.com

An alert with the following constituent `events` might be generated in response to the second session:

```
{
     "events": [
         {
             "username": "jhalpert",
             "host_dst": "www.facebook.com",
             "ip_dst": "31.1x.x9.1x8",
             "sessionid": 2,
             "ec_theme": "Login Failure",
             "esa_time": 1406148964130,
             "ip_src": "23.xx.23x.16"
         }
     ]
 }
```

The JSON output shows all the information available for inclusion into an ESA notification using an appropriate FreeMarker
template. For instance, the template expression `${events[0].username}` would evalute to `jhalpert`.

With enrichments, the same module, with the same event stream, can generate the alert shown below. The system
can make multiple enrichment connections and pull contextual data to make the alert more meaningful.

For example:
`${events[0]["RSADataScienceLookup"][0].score}` gives the **"risk"** score of the destination domain computed by the RSA Warehouse Analytics module while `${events[0]["orgchart"][0].supervisor}` gives the name of the supervisor of the employee that the alert pertains to (pulled from an HR database) and `${events[0]["LoginRegister"][0].username}` gives the name of the user with the last successful logon from the same `ip_src` (using a stream based Named Window).


```
{"events": [
     {
         "username": "jhalpert",
         "host_dst": "www.facebook.com",
         "GeoIpLookup": [
         {
             "city": "Cambridge",
             "longitude": -71,
             "countryCode": "US",
             "areaCode": 617,
             "metroCode": 506,
             "region": "MA",
             "dmaCode": 506,
             "ipv4Obj": "/23.62.236.16",
             "countryName": "United States",
             "postalCode": "02142",
             "ipv4": "23.62.236.16",
             "latitude": 42,
             "organization": "Verizon Business"
         }
     ],
     "RSADataScienceLookup": [
         {
             "model_id": "suspiciousDomains_1",
             "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
             "score": 10,
             "key": "www.facebook.com"
         }
     ],
     "orgchart": [
         {
             "supervisor": "mscott",
             "name": "James Halpert",
             "extension": 3692,
             "location": "Scranton",
             "department": "Sales",
```

```
            "id": "jhalpert"
        }
    ],
    "ip_dst": "31.13.69.128",
    "sessionid": 2,
    "LoginRegister": [
        {
            "username": "dshrute",
            "ip_src": "23.62.236.16"
        }
    ],
    "ec_theme": "Login Failure",
    "esa_time": 1406155218912,
    "ip_src": "23.62.236.16"
    }
]}
```


Configure a Database Connection

This topic provides information to configure a connection to an external database that can provide additional information in alerts. You configure a database connection so you can then configure the database as an enrichment source, to add further details to alerts. There are three steps in the process:

1. Configure a connection to a database.
2. Configure the external database as an enrichment source.
3. Add the enrichment source to a rule

This topic explains Step 1.

Example

This example illustrates how adding a database as an enrichment source adds value to alerts.

A rule detects users that attempt to sign up for a stealth email service. Twenty-five users match the rule criteria. Without the enrichment, the alert contains 25 User IDs. With the enrichment, the alert also includes the following information for each User ID:

- Name
- Title
- Department
- Office Location

Dependencies

When you configure a database, the following conditions apply:

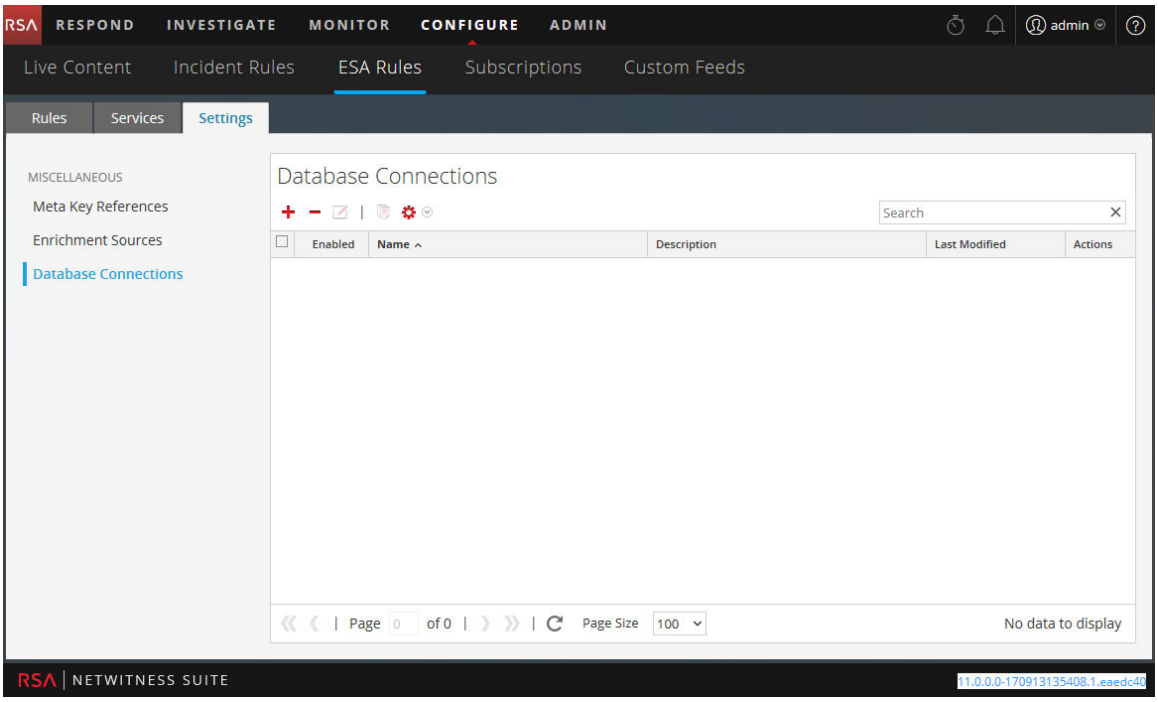
- A reference to the database is deployed on every ESA, even if the ESA does not deploy rules that use the database as an enrichment source.
- If the server that hosts the database goes down, it impacts a deployment.
  - An active deployment will continue to gather data and run rules but enrichments will not appear in alerts.
  - A new deployment will fail until you restart the host.

Procedure

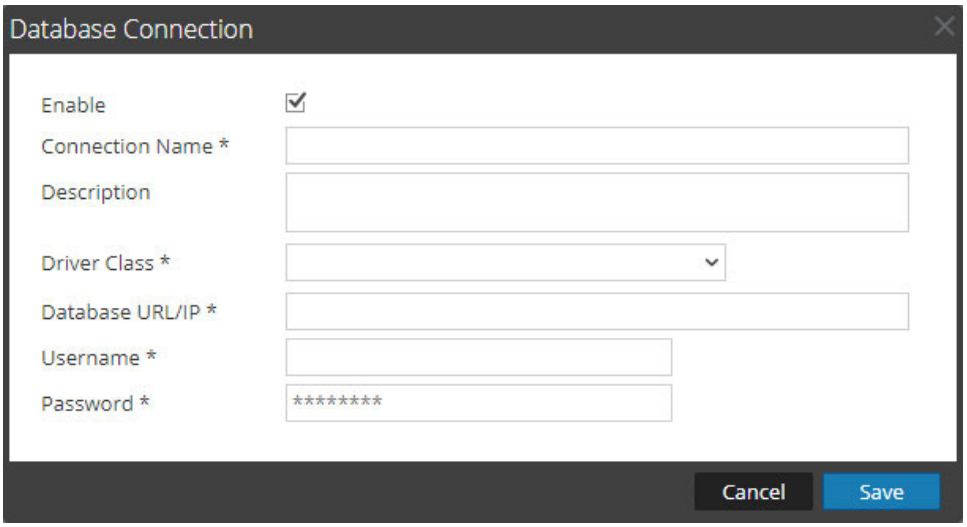
To configure a database connection:

1. Go to **CONFIGURE > ESA Rules**.
2. Click the **Settings** tab.
3. In the options panel, select **Database Connections**.

   The Database Connections panel is displayed.



4. Click + to add a database connection.



5. In the **Database Connection** dialog, provide the following information.

Field	Description
Enable	Select Enable to enrich the alert with additional data. By default, Enable is selected. Deselect Enable to exclude additional data from the alert.
Connection Name	Type a name to identify the connection. When you add a database as an enrichment source, this name appears in the list of Database Connections.
Description	(Optional) Type a brief description about the database connection.
Driver Class	Select an appropriate driver class for the database. Two drivers come with NetWitness Suite, MongoDB and Postgres.
Database URL or IP address	Type the URL or the IP address of the database to configure.
Username	Type the username to access the Database.
Password	Type the password to access the Database.

6. Click **Save**.

For related information, see Settings Tab.

Enrichment Sources

This topic explains options for adding an external data source to provide additional information in alerts. Enrichment sources provide additional information in alerts. For example, a database can provide a name, department, and office location if a user matches rule criteria. There are four types of enrichment sources:

- External DB Reference
- In-Memory Table
- Warehouse Analytics
- Context Hub List

Configure a Database as Enrichment Source

You can configure a database as an enrichment source so you can add it to a rule. Then the Esper engine that analyzes events can access the information in the database to provide additional information in the alert.

For example, a rule detects users that attempt to sign up for a stealth email service. Twenty-five users match the rule criteria. The alert contains 25 User IDs. An external database would enhance the alert by providing the following additional information for each User ID:

- Name
- Title
- Department
- Office Location
- Reports To

You can edit, duplicate, import or export a database connection.

Prerequisites

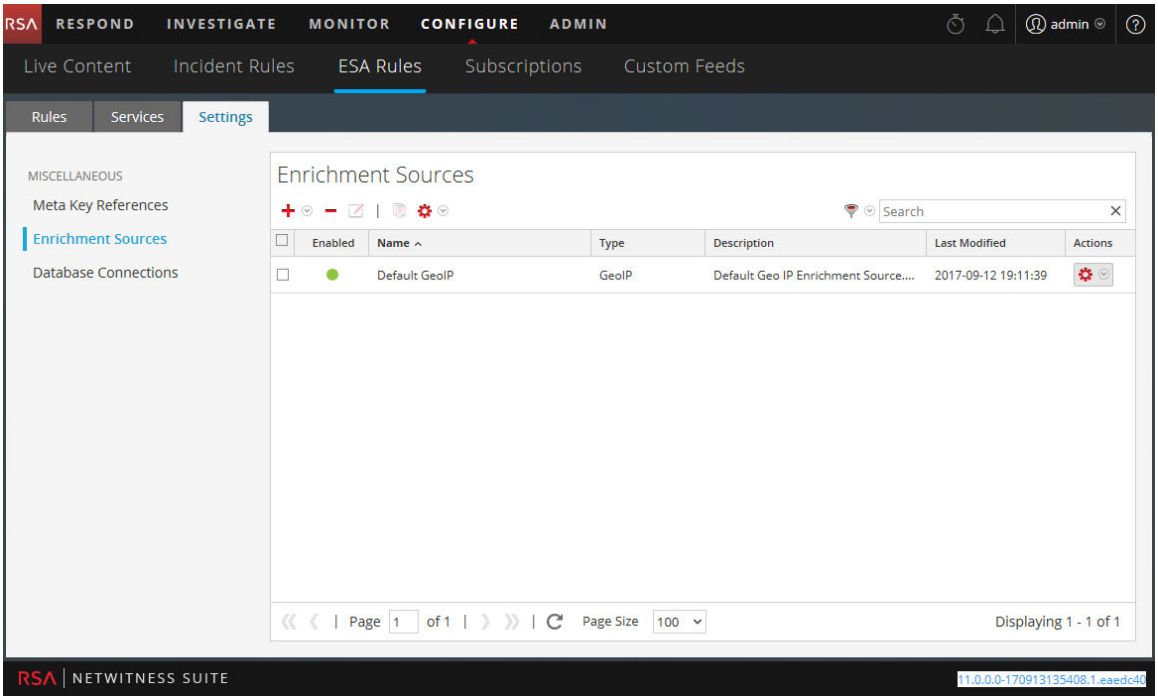
You must configure a database connection. For more information, see Configure a Database Connection.

Procedure

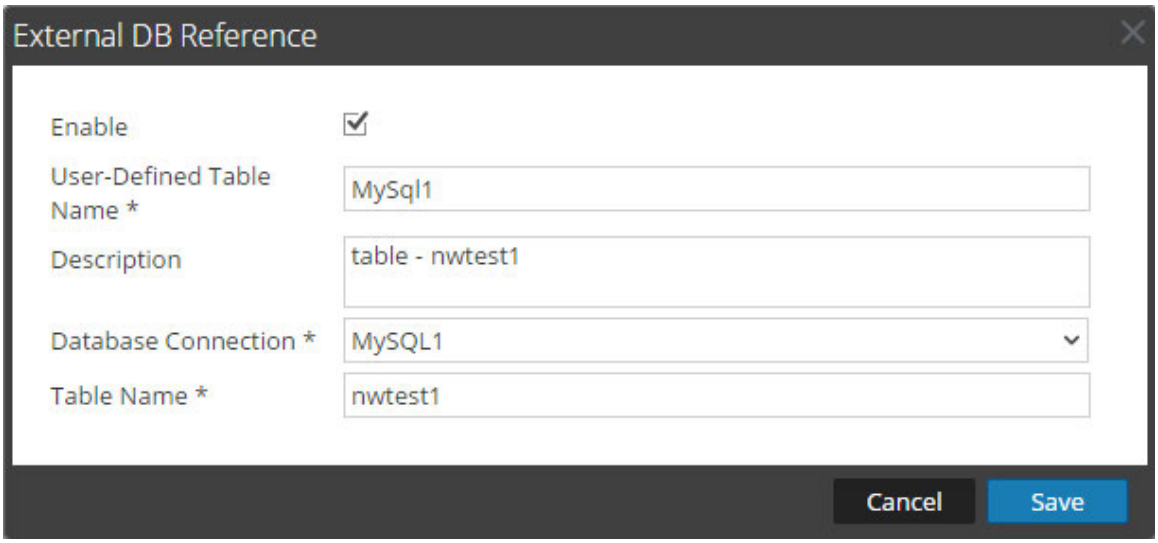
To configure database as an enrichment source:

1. Go to **CONFIGURE > ESA Rules**.
2. Click the **Settings** tab.
   The Settings tab is displayed.

3. In the options panel, select **Enrichment Sources**.
   The Enrichment Sources panel is displayed.



4. From the drop-down menu, select **External DB Reference**. You have to add a DB reference in order for the DB to be listed.
   The External DB Reference dialog is displayed.



5. Select **Enable** to enrich alert with additional data. This is selected by default. If disabled, the alert will not be enriched with additional data.

6. In the **User-Defined Table Name** field, type a name to identify or label the database configuration.
7. In the **Description** field, type a brief description about the database configuration.
8. In the **Database Connection** drop-down menu, select the database connections defined.
9. In the **Table Name** field, enter database table name.
10. Click **Save**.

For details on parameters and their descriptions, see Settings Tab.

Configure In-Memory Table as an Enrichment Source

This topic provides instructions on how to configure an in-memory table. When you configure an in-memory table, you upload a .CSV file as an input to the table. You can associate this table with a rule as an enrichment source. When the associated rule generates an alert, ESA will enrich the alert with relevant information from the in-memory table.

For example, a rule could be configured to detect when a user tries to download freeware and to identify the person by user ID in the alert. The alert could be enriched with additional information from an in-memory table that contains details such as full name, title, office location and employee number.

An in-memory table is ideal for handling lightweight data. It is easy to set up and requires less maintenance than a database. For example, the AllTech Company is a small organization so the system administrator can maintain employee information in a .CSV file. If AllTech grows into a very large company, the administrator would have to configure an external database reference as an enrichment and associate the database with a rule.

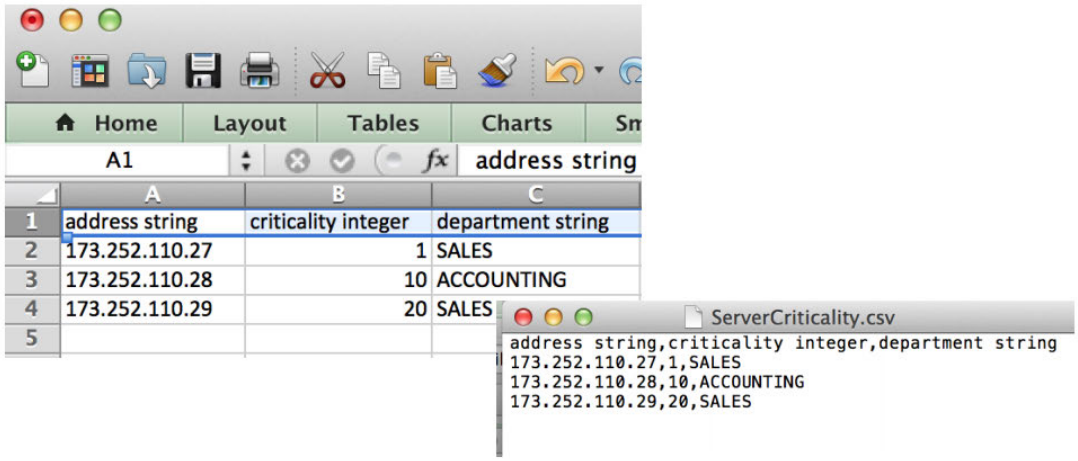
Prerequisites

The column name in the .CSV file cannot have whitespace characters.

For example *Last_Name* is correct, and *Last Name* is incorrect.

The .CSV file must begin with a header line that defines fields and types.
For example, *address string* would define the header field as *address*, and the type as *string*.

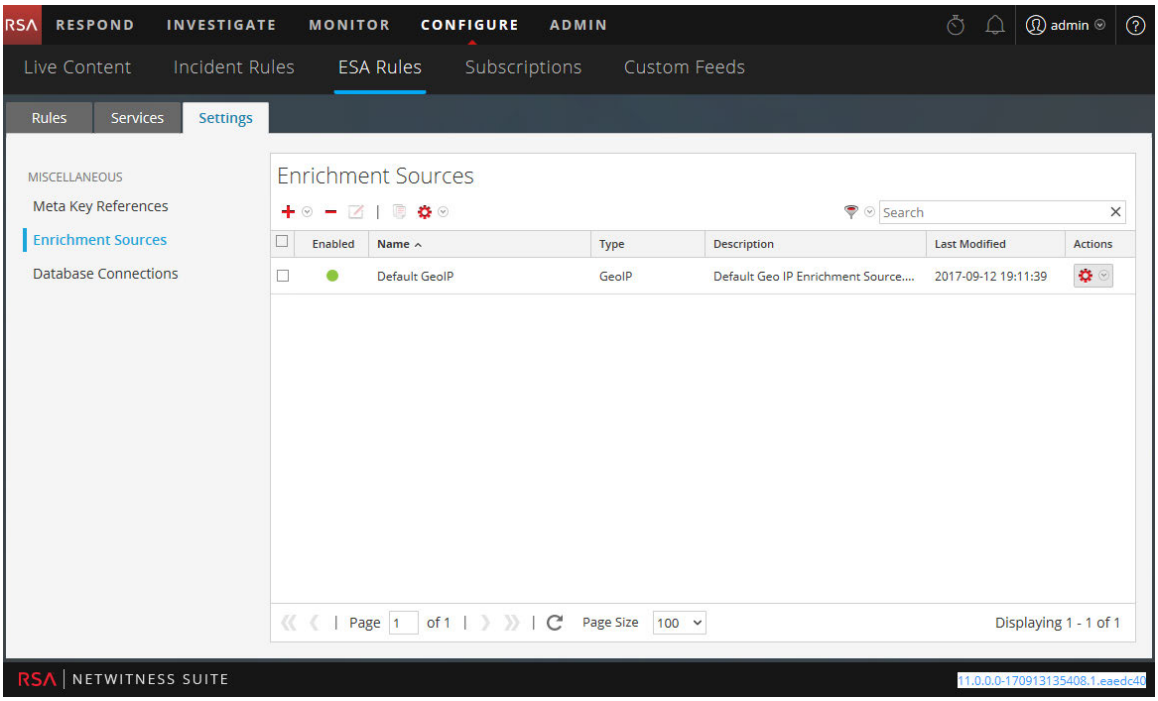
The following shows a valid .CSV file represented as a .CSV and as a table.



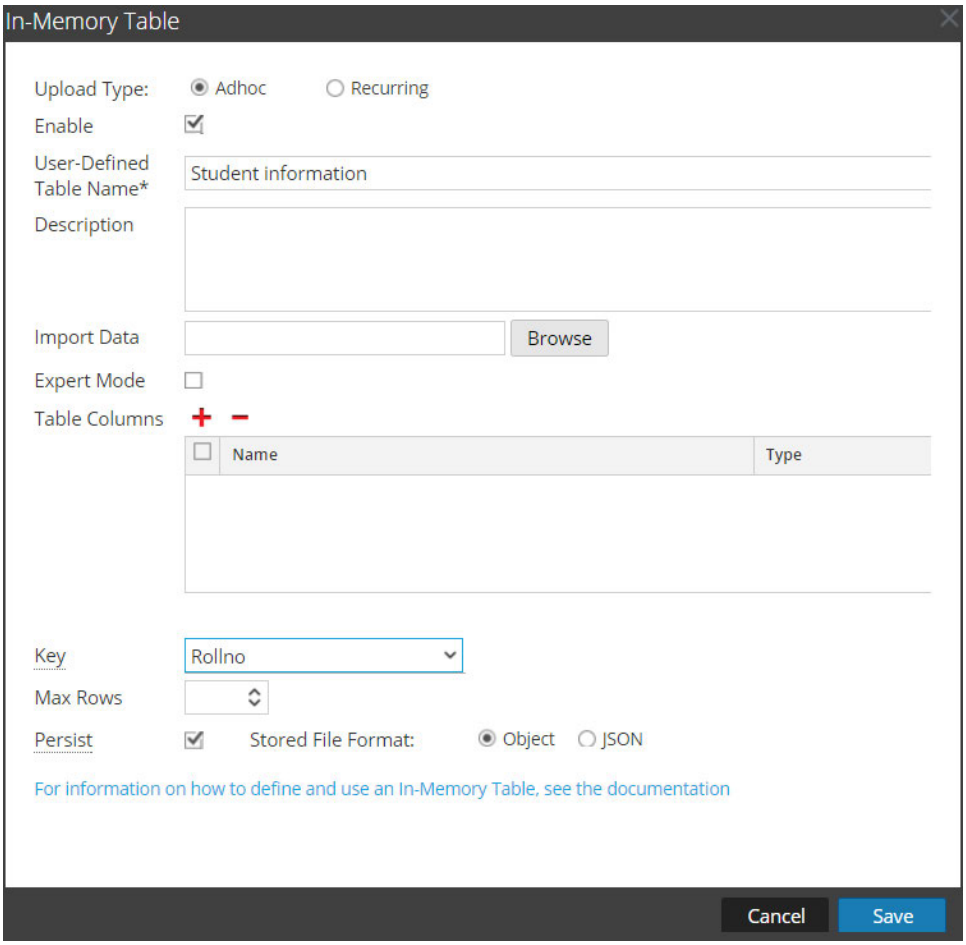
Procedures

Configure an Ad hoc In-Memory Table

1. Go to **CONFIGURE > ESA Rules**.
   The Configure view is displayed with the ESA Rules tab open.
2. Click the **Settings** tab.
3. In the options panel, select **Enrichment Sources**.



4. In the **Enrichment Sources** section, click + > **In-Memory Table**.



5. Describe the in-memory table:

   a. Select **Ad hoc**.

   b. By default, **Enable** is selected. When you add the in-memory table to a rule, alerts will be enriched with data from it.
   If you add an in-memory table to a rule but do not want alerts to be enriched, deselect the checkbox.

   c. In the **User-Defined Table Name** field, type a name, such as Student Information, for the in-memory table configuration.

   d. If you want to explain what the enrichment adds to an alert, type a **Description** such as:
   When an alert is grouped by Rollno, this enrichment adds student information, such as name and marks.

6. In the **Import Data** field, select the .CSV file that will feed data to the in-memory table.

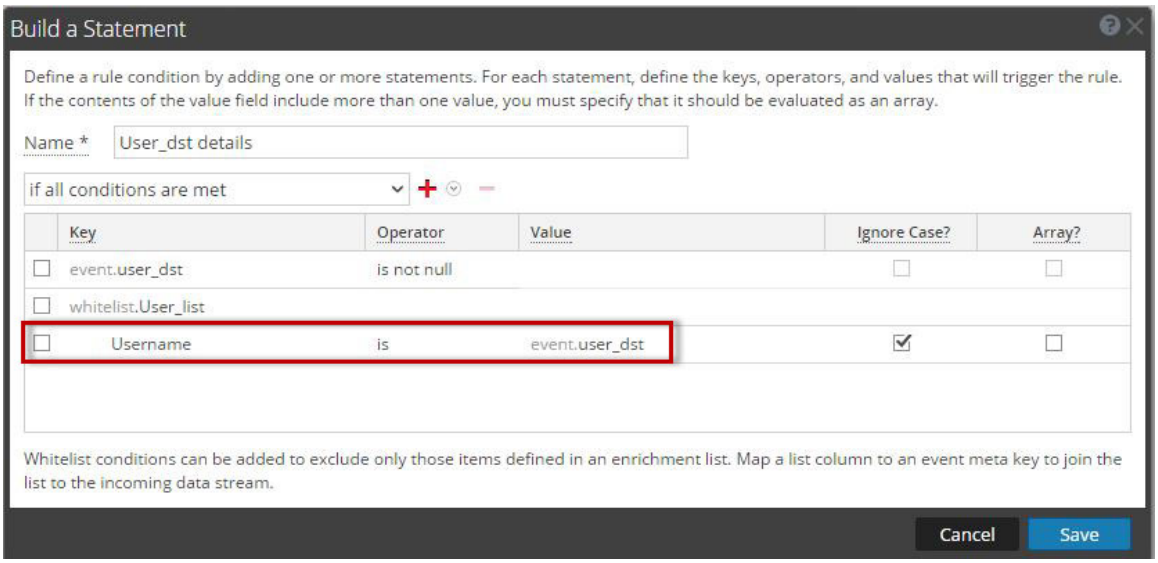
7. If you want to write an EPL query to define an advanced in-memory table configuration, select **Expert Mode**.
   The Table Columns are replaced by a **Query** field.
8. In the **Table Columns** section, click + to add columns to the in-memory table.
9. If a valid file is selected in the Import Data field, the columns populate automatically.

Note: If you selected Expert mode, a Query field is displayed instead of Table Columns.

10. In the **Key** drop-down menu, select the field to use as the default key to join incoming events with the in-memory table when using a CSV-based in-memory table as an enrichment. By default, the first column is selected. You can also later modify the key when you open the in-memory table in enrichment sources.
11. In **Max Rows** drop-down menu, select the number of maximum number of rows that can reside in the in-memory table at a particular instance.
12. Select **Persist** to preserve the in-memory table on disk when the ESA service stops and to re-populate the table when the service restarts.
13. In **Stored File Format** field, do one of the following:
    - Select **Object**, if you want to store the file in a binary format.
    - Select **JSON**, if you want to store the file in a text format.
      By default, **Object** is selected.
14. Click **Save**.
    The adhoc in-memory table is configured. You can add it to rule as an enrichment or part of the rule condition. See Add an Enrichment to a Rule.

When you add an in-memory table, you can add it to a rule as an enrichment or as a part of the rule condition. For example, the following rule uses an in-memory table as a part of the rule condition to create a whitelist, and it also uses an in-memory table of details in the user_dst file to enrich the alert that is displayed.

The rule shows the in-memory table as a whitelist rule condition:



Next, the alert is enriched with the User_list in-memory table:

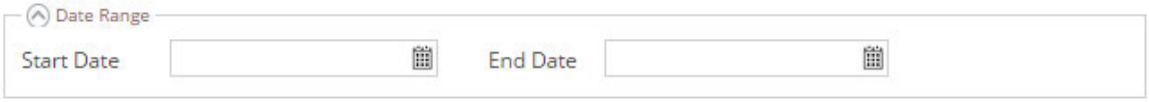
Therefore, the user_dst in-memory table is used to create a whitelist, and it is also used to enrich the data in the alert if the alert is triggered.

Add a Recurring in-Memory Table

1. Go to **CONFIGURE > ESA Rules**.
   The Configure view is displayed with the ESA Rules tab open.
2. Click the **Settings** tab.
3. In the options panel, select **Enrichment Sources**.
4. Click > **In-Memory Table**.
5. Describe the in-memory table:
   a. Click **Recurring**.
   b. By default, **Enable** is selected. When you add the in-memory table to a rule, alerts will be enriched with data from it.
   If you add an in-memory table to a rule but do not want alerts to be enriched, deselect the checkbox.
   c. In the **User-Defined Table Name** field, type a name, such as Student Information, for the in-memory table configuration.

d. If you want to explain what the enrichment adds to an alert, type a **Description** such as: When an alert is grouped by Rollno, this enrichment adds student information, such as name and marks.

6. Type the URL of the .CSV file that will feed data to the in-memory table. Click Verify to validate the link and populate the columns in the .CSV file. You can add or remove columns using the plus or minus button.
7. If the server is configured behind another server, select **Use Proxy**.
8. If the server requires logon credentials, select **Authenticated**
9. For **Recur Every**, indicate how frequently ESA must check for the most recent .CSV:
   a. Select Minute(s), Hour(s), Day(s), or Week.
   b. If you select Week, select a day of the week.
   c. Click **Date Range** to select a **Start Date** and **End Date** for the recurring schedule.



10. In the **Key** drop-down menu, select the field to use as the default key to join incoming events with the in-memory table when using a CSV-based in-memory table as an enrichment. By default, the first column is selected. You can also later modify the key when you open the in-memory table in enrichment sources.
11. In **Max Rows** drop-down menu, select the number of rows that can reside in the in-memory table at a particular instance.
12. Select **Persist** to preserve the in-memory table on disk when the ESA service stops and to re-populate the table when the service restarts.
13. In **Stored File Format** field, do one of the following:
    - Select **Object**, if you want to store the file in a binary format.
    - Select **JSON**, if you want to store the file in a text format.
      By default, **Object** is selected.
14. Click **Save**.
    The recurring in-memory table is configured. You can add it to rule as an enrichment or part of the rule condition. See Add an Enrichment to a Rule.

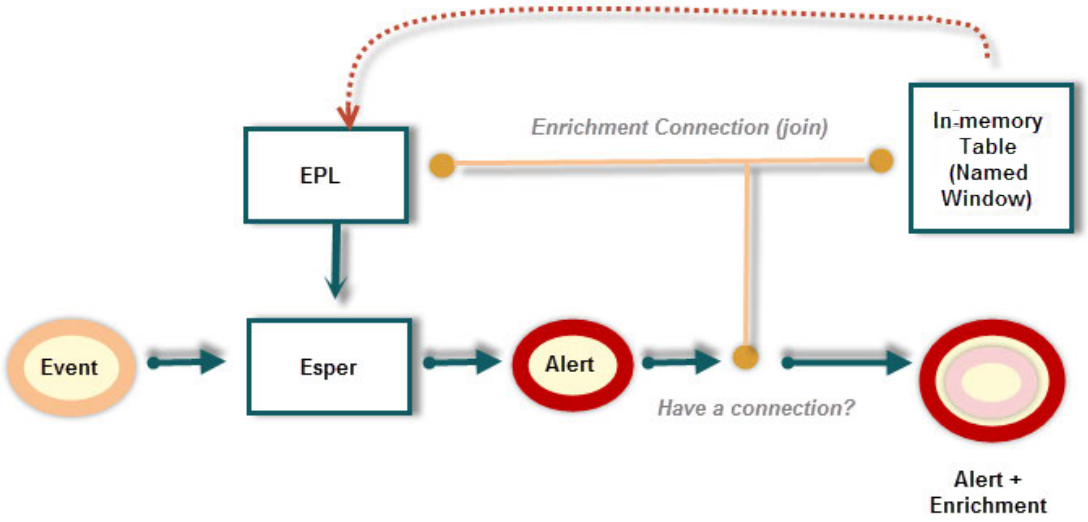
Configuring an Esper Query as an Enrichment Source

When you use "expert mode," you can create an enrichment source or named window based on an Esper query. This allows you to have more control over the content and create more dynamic content. When you do this, an EPL query constructs the named window to capture interesting state from event stream.

Workflow

The following shows the workflow for creating a query using a named window:

1. The event is sent to the Esper Engine.
2. An EPL query is generated.
3. An alert is triggered.
4. The query checks to see if there is a connection between the event and the Named Window.
5. If there is a connection, the query that populates the Named Window is run and populated.
6. The content from the Named Window is added to the alert content and sent or displayed (depending on your settings).



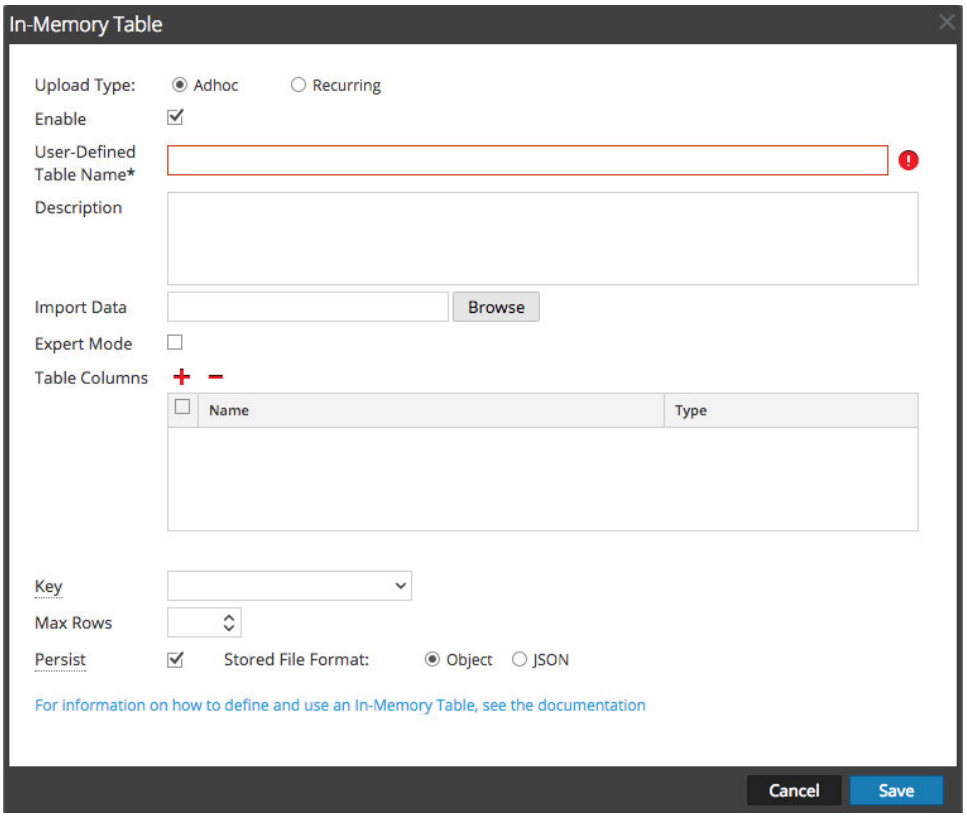
Prerequisites

- The meta used in the EPL statement must exist in the data.
- You must create well-formed EPL statements.

Procedure

Configure an In-Memory Table Using an EPL Query

1. Go to **CONFIGURE > ESA Rules**.
   The Configure view is displayed with the Rules tab open.
2. Click the **Settings** tab.
3. In the options panel, select **Enrichment Sources**.
4. In the **Enrichment Sources** section, click > **In-Memory Table**.



5. Select **Adhoc**.
   By default, Enable is selected. When you add the in-memory table to a rule, alerts will be enriched with data from it.
6. In the **User-Defined Table Name** field, type a descriptive name to describe the in-memory table.
7. If you want to explain what the enrichment adds to an alert, enter information in the **Description** field.
   This description displays when you view the list of enrichments from the Enrichment Sources

view, so it's a good idea to enter a thorough description as a best practice. Doing this allows other users to understand the content of the enrichment without opening it to examine its contents.

8. Select **Expert Mode** to define an advanced in-memory table configuration by writing an EPL query.
   The Table Columns are replaced by a **Query** field.
9. Select **Persist** to preserve the in-memory table on disk when the ESA service stops and to re-populate the table when the service restarts.
10. Enter the EPL query in the **Query** field. The query should be well-formed, and it's a good idea to test it before entering it in the field.
11. Click **Save**.

Example

For example, you created a rule that searches for five failed attempted logins followed by a successful login. When that rule is triggered, you may want the notification to contain information about the last user logged into the system when this successful login occurred. To add this enrichment to the notification, you might choose to create a stream-based in-memory lookup table that is populated from incoming events to maintain a mapping of IP addresses to the last user logged in from that address. To do this, you create an enrichment using a query as your source.

Step 1: Create Your Rule

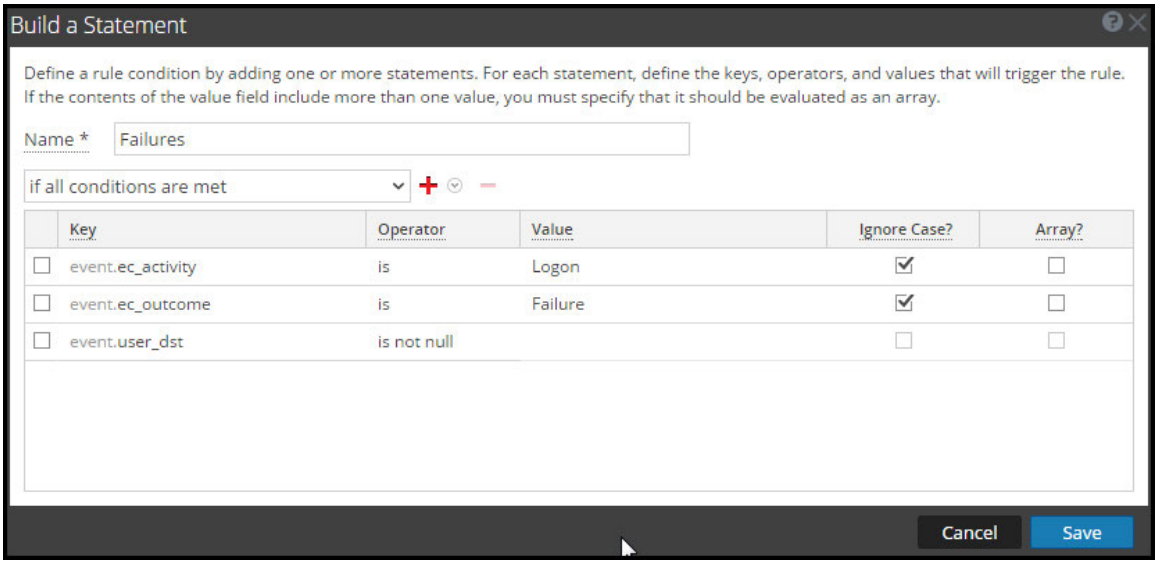
First, you need to create your correlation rule. In this case, you create failure and success rule conditions, and group by the ip_src.

Rule Condition	Description
Failures	This condition searches for five failed logins with a "followed by" connector, meaning that the condition (Failures) must be followed by the next condition (Success).
Success	This condition searches for one successful login.

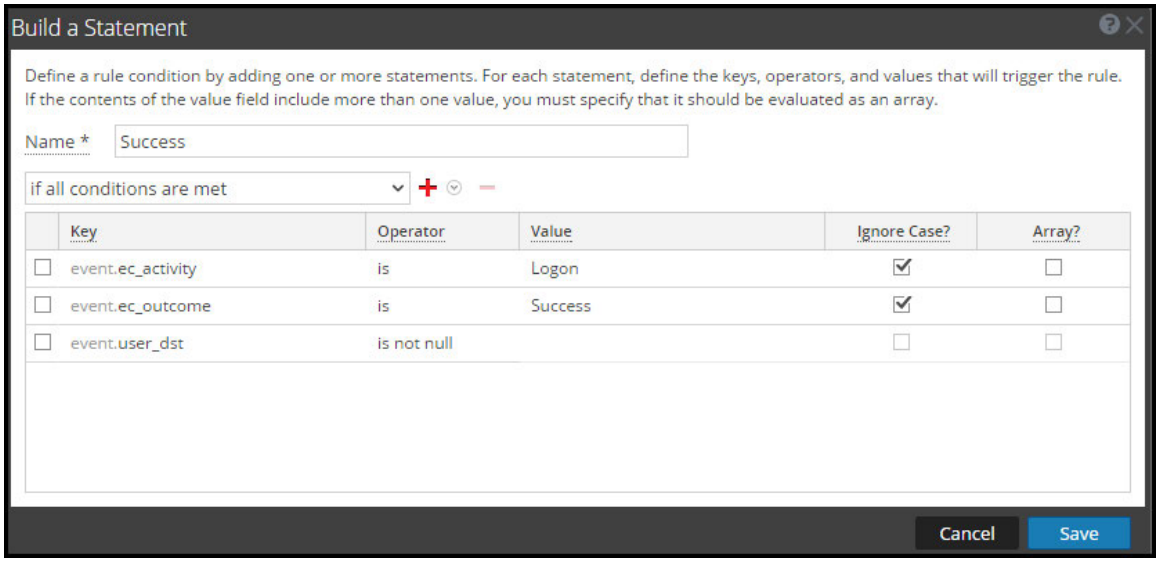
Rule Condition	Description
GroupBy: ip_src, device class	The GroupBy field ensures that all the previous conditions are grouped by the ip_srcand device class. This is important to the construction of the rule because the rule attempts to find a case where a user has attempted to log into the same destination account multiple times, and finally logged in successfully. Grouping by device class ensures that the user logged in from the same machine attempted to log into an account multiple times. The rule may give unexpected results if you do not group the results.
Occurs within 5 minutes	The time window for the events to occur is five minutes. If the events occur outside of this time window, the rule does not trigger.
Event Sequence: Strict	The event sequence is configured for a strict pattern match. This means that the pattern must match exactly as it is specifiedwith no intervening events.

For the rule conditions, you create the following statements:

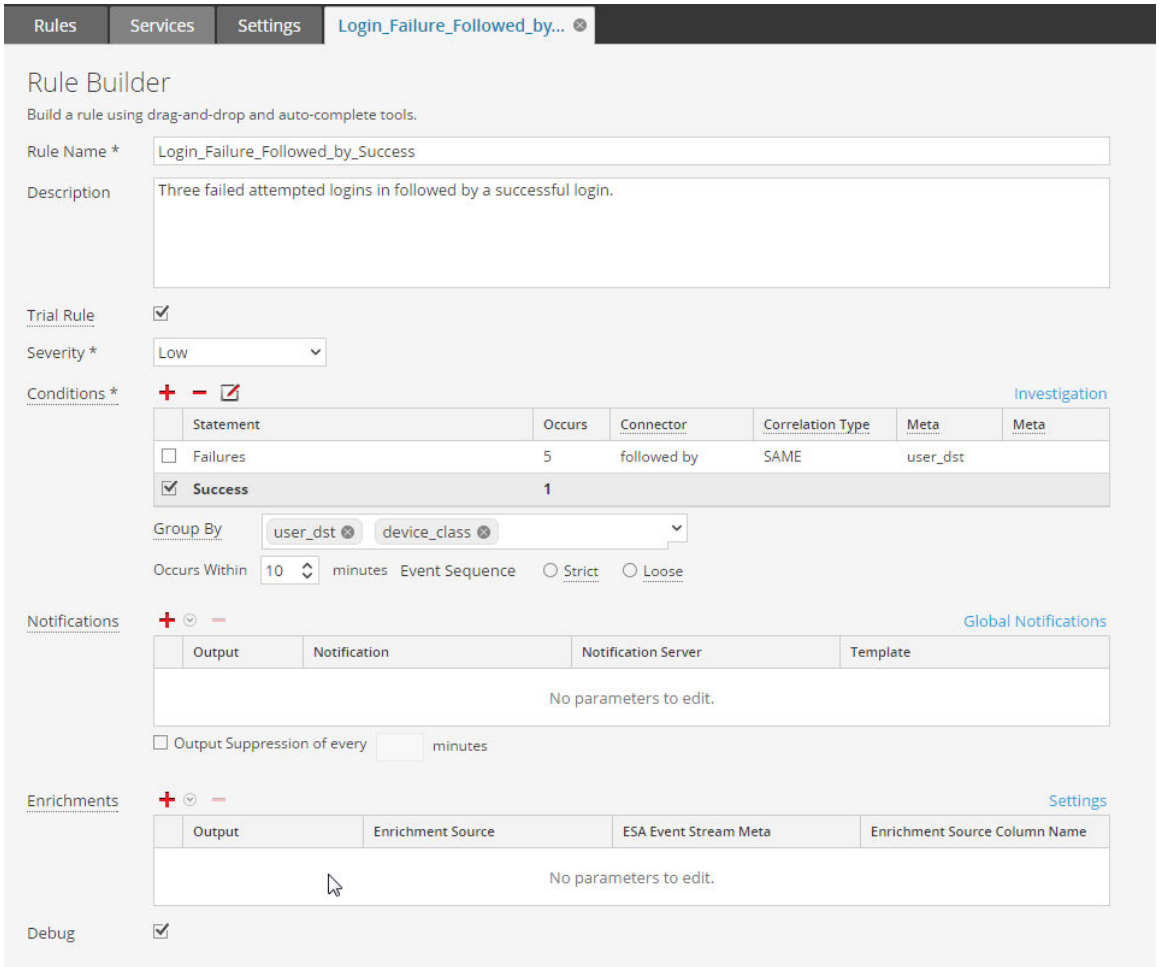
- The "Failures" statement searches for failed login attempts:



- The "Success" statement searches for one successful login:



- Combined, you have the following correlation rule:

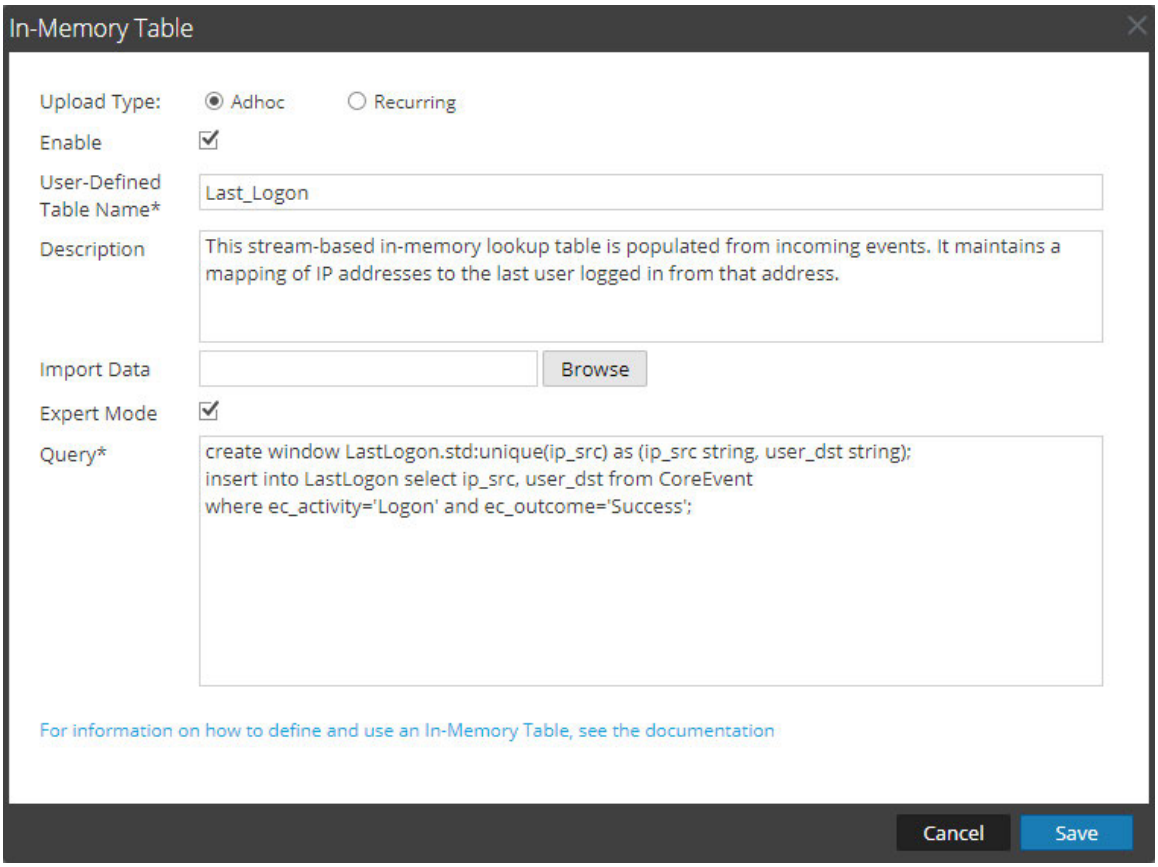


Step 2: Create the Enrichment

Now that you have created your rule, you need to create the enrichment to add to the notification output. Follow the steps above to create the enrichment, name it *Last_Logon*, and add the following query:

```
create window LastLogon.std:unique(ip_src) as (ip_src string, user_dst string);

insert into LastLogon select ip_src, user_dst from CoreEvent

where ec_activity='Logon' and ec_outcome='Success';
```

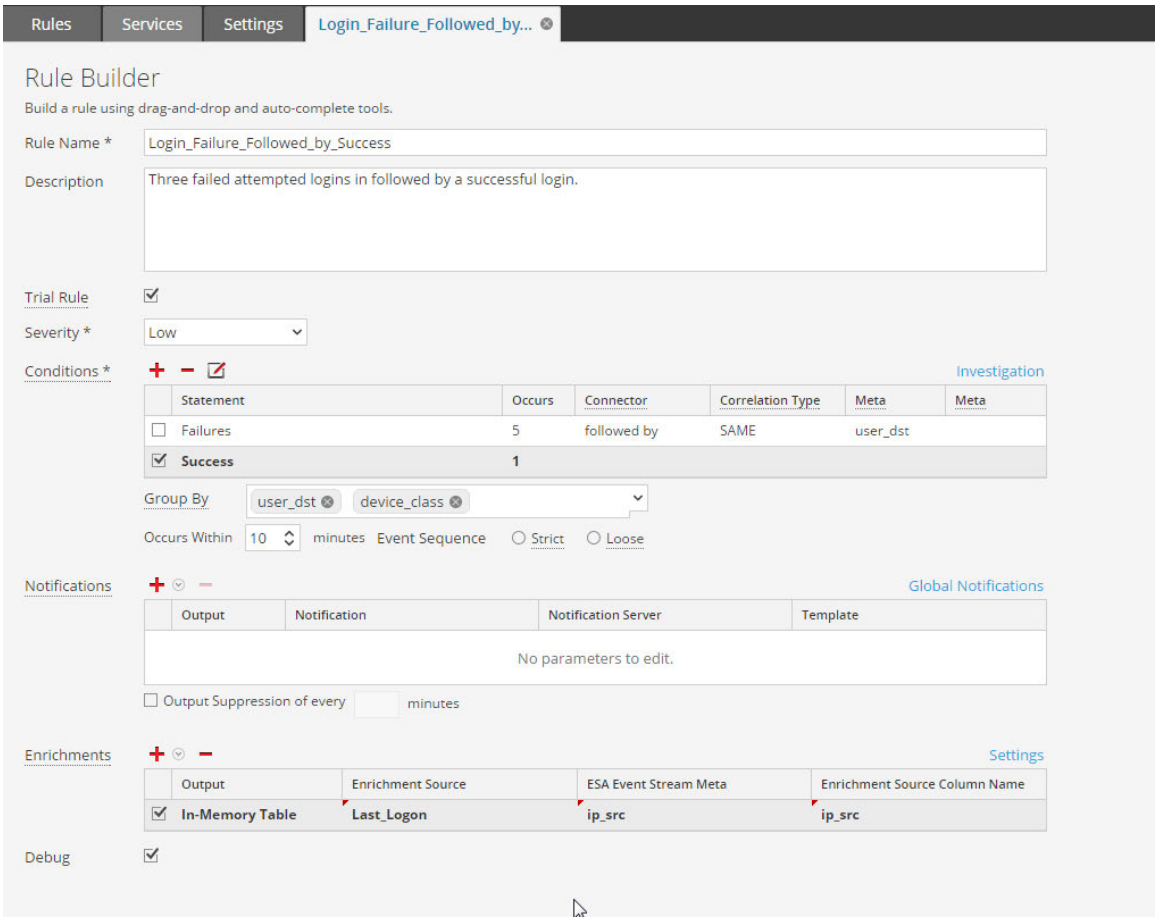
The enrichment should look like the following:



Step 3: Add the Enrichment to the Rule

Now that you have created your basic rule and your enrichment, you'll need to add the enrichment to the rule and join (or connect) the enrichment to the meta in the rule.

Open the Login_Failure_Followed_by_Success rule for editing.



Field	Enter	Description
Output	In-Memory Table	The In Memory Table option creates a Named Window, which can be populated with the EPL query data.
Enrichment Source	Last_Logon (the enrichment you created above).	This is the stream-based in-memory lookup table that is populated from incoming events to maintain a mapping of IP addresses to the last user logged in from that address.
ESA Event Stream Meta	ip_src	This is an event stream meta that you can join to the enrichment data you are populating. Essentially, ip_src is the join condition .
Enrichment Source Column Name	ip_src	This is the meta from the enrichment that you can join to the event stream data. It must be the same as join condition from the Event Stream Meta field.

Once you have added the enrichment, you can save the rule.

When the rule is triggered, the ESA runs the query in the enrichment and populates the Named Window with the data. If the data in the Named Window matches the join condition, the data is added to the output you can view in Email, SNMP, Syslog or Script, depending on how you configured notifications.

Configure Warehouse Analytics as an Enrichment Source

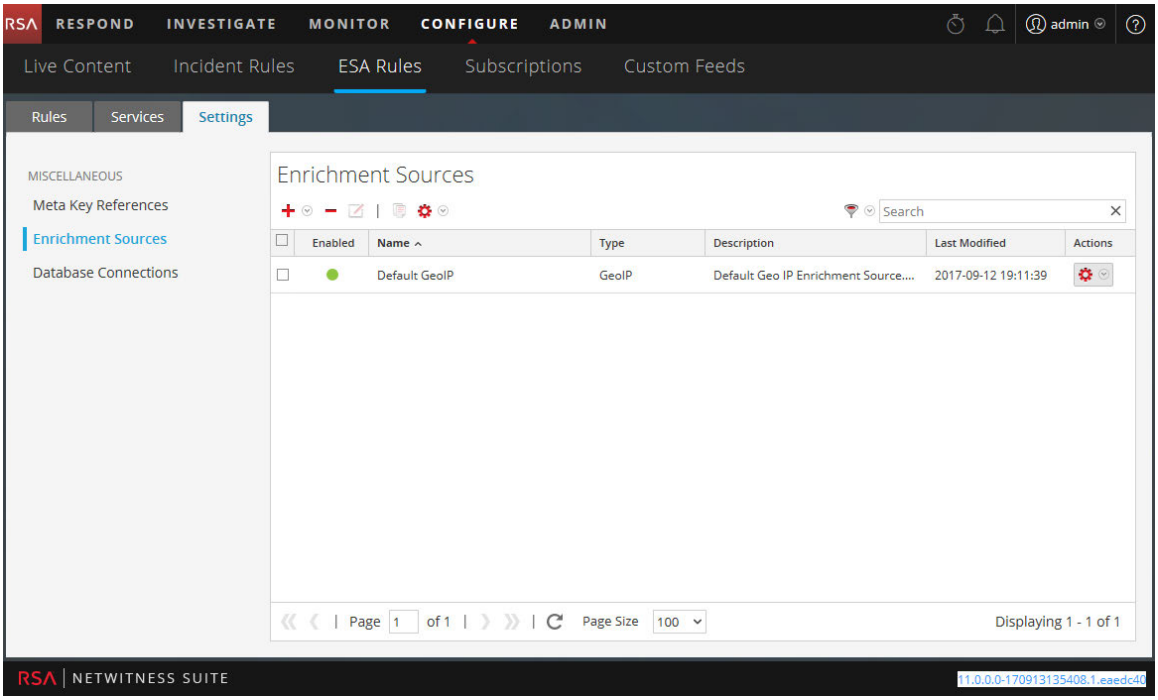
This topic provides instructions on how to configure RSA Warehouse Analytics as an enrichment source for ESA. Data analysts can leverage Warehouse Analytics data to analyze session and log data.

Procedure

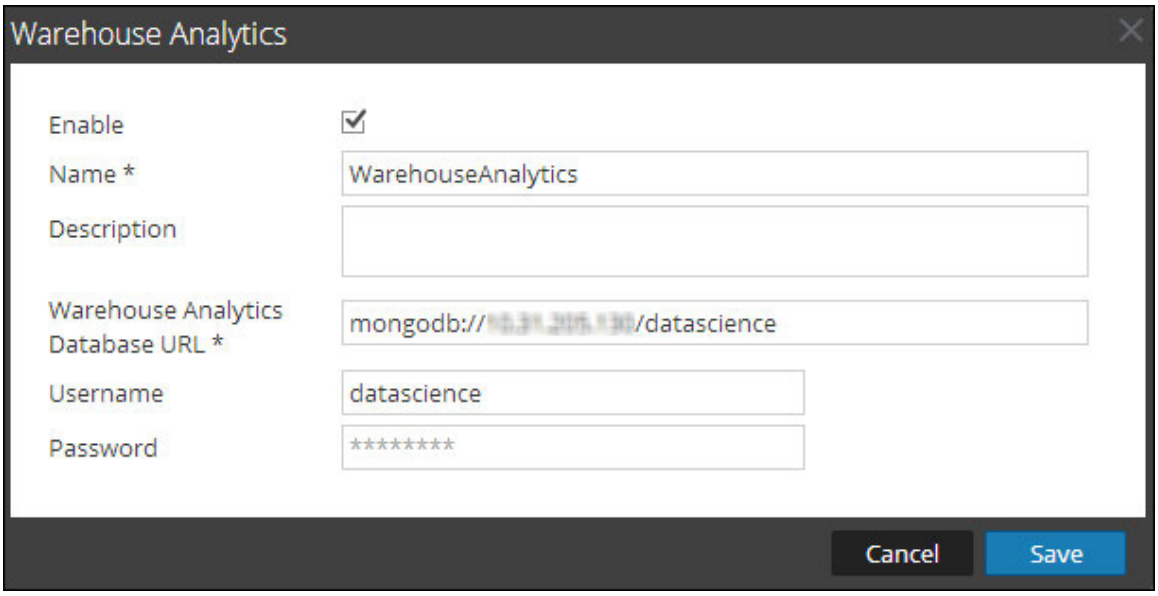
To configure Warehouse Analytics as an enrichment source:

1. Go to **CONFIGURE > ESA Rules > Settings** tab.
2. In the options panel, select **Enrichment Sources**.

   The Enrichment Sources panel is displayed.



3. From the + drop-down menu, select **Warehouse Analytics**.



4. Select **Enable** to enrich alerts with additional data. This is selected by default. If disabled, the alerts will not be enriched with additional data.
5. In the **Name** field, type a name to identify or label the Warehouse Analytics configuration.
6. In the **Description** field, type a brief description about the Warehouse Analytics configuration.
7. In the **Warehouse Analytics Database URL** field, type theMongoDb URL to the Warehouse Analytics database.
8. In the **Username** field, type the username to access the MongoDB.
9. In the **Password** field, type the password to access the MongoDB.
10. Click **Save**.

For more information, see Settings Tab.

Configure Context Hub List as an Enrichment Source

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

This topic provides instructions on how to configure a Context Hub list as an enrichment source for ESA. Once a Context Hub list is added as an enrichment source, analysts can use the configured list as a statement condition when creating an ESA rule. Any changes made to the list from within Context Hub are automatically reflected in the enrichment source in real-time. For example, you could create a list of IP addresses in Context Hub and then use that list as either a blacklist or whitelist as part of a correlation rule condition. Any subsequent changes made to the IP list in Context Hub will be reflected in the enrichment source in real-time, to ensure the correlation rule operates with a constantly updating set of information.

Prerequisites

Before configuring a Context Hub list as an enrichment source, the list must first be created as a data source in Context Hub. Any list created in Context Hub is supported and the lists may contain string or numeric values, including IP addresses. For information on creating a list as a data source in Context Hub, see the *RSA NetWitness Context Hub Configuration Guide*.

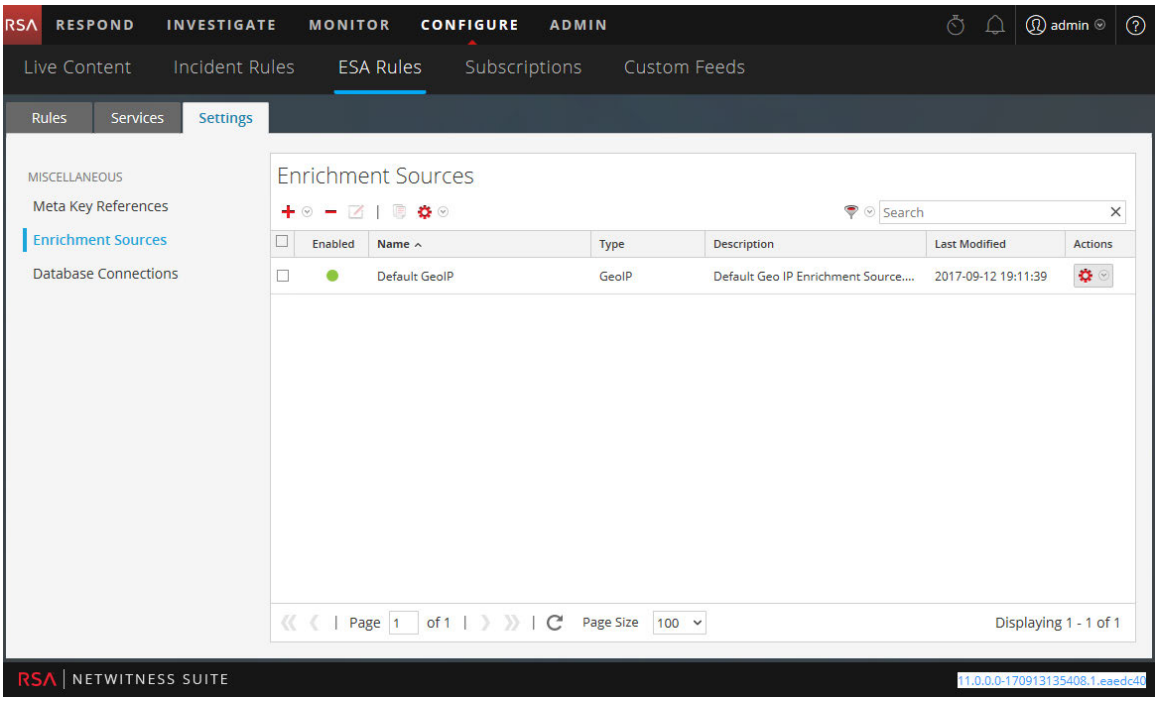
Caution: When creating a Context Hub list for use as an enrichment source, the list name and its field names cannot include any spaces or special characters, or start with a number. If you do not follow this naming convention, when you attempt to add the list as an enrichment source in ESA, an error message will be displayed and you will not be allowed to add the list.

Procedure

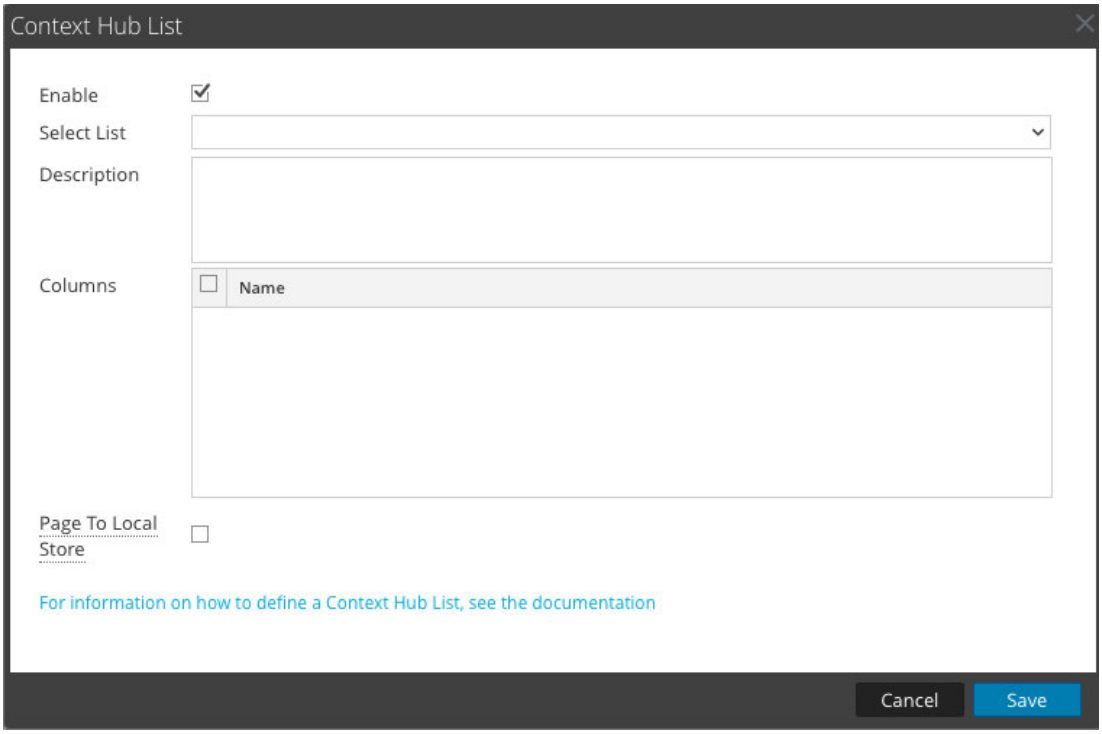
To configure a Context Hub list as an enrichment source:

1. Go to **CONFIGURE > ESA Rules> Settings** tab.
2. In the options panel, select **Enrichment Sources**.

   The Enrichment Sources panel is displayed.



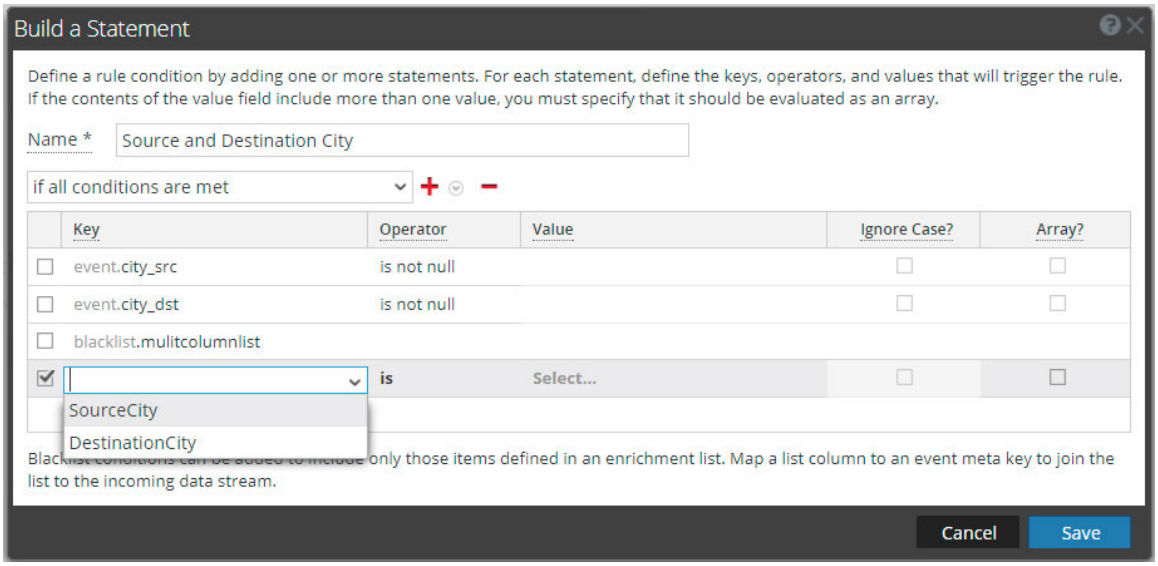
3. From the drop-down menu, select **Context Hub**.



4. Select **Enable** to enrich alerts with a Context Hub list. This is selected by default. If disabled, the alerts will not be enriched with the configured Context Hub list.

5. Select the desired Context Hub list from the **Select List** drop-down menu of pre-configured lists.
6. (Optional) In the **Description** field, type a brief description about the selected Context Hub list. The text entered here is displayed on the Enrichment Sources panel.
7. In the **Columns** field, all columns included in the selected Context Hub list are listed. Click to enable or disable the columns in the list that you wish to include when using this list as an enrichment source in an alert.
8. (Optional) Click to enable the **Page To Local Store** option. This option is useful if you have a very large list and performance is affected. If this is the case, enabling this option will write a copy of the Context Hub list to the local disk to improve performance.
9. Click **Save**.
   The Context Hub list is configured. You can now add it to an ESA rule as part of a condition statement as either a blacklist or a whitelist condition.

The following figure illustrates adding a Context Hub list as part of a condition statement. In this example, a context Hub list named "multicolumnlist" was added as a blacklist condition. The list contains two columns, SourceCity and DestinationCity. The next step would be to select one of the column names as the subcondition and then specify the operator and enter the meta value for the corresponding value field.



For complete details for adding a whitelist or blacklist to a condition statement, see Step 2. Build a Rule Statement.

To add a Context Hub list as a condition to an existing rule, select to edit the desired rule in the Rule Library, then add a condition in the Conditions section and select to add a whitelist or blacklist condition to the new condition statement.

Add an Enrichment to a Rule

This topic tells how to add a previously configured enrichment source to a rule. When ESA creates an alert, information from the source gets included in it.

Adding an enrichment to a rule allows you to request for look ups into a variety of sources and include the results in the outgoing alerts, giving you a more detailed alert. This procedure requires role permissions for Administrator, DPO, and SOC Manager.

Note: This procedure does not apply to adding a Context Hub list as an enrichment to a condition statement in an existing rule. For information see Configure Context Hub List as an Enrichment Source.

Procedure

To add an enrichment to a rule:

1. Go to **CONFIGURE > ESA Rules**.
2. In the **Rule Library** view, do one of the following:
   - Double-click a rule.
   - Select a rule and click in the **Rule Library** toolbar.

   The Rule Builder panel is displayed in a new NetWitness Suite tab.
3. In the **Enrichments** section, click and select any of the following enrichment types:
   - In-Memory Table
   - External DB Reference
   - Warehouse Analytics
   - GeoIP

   Note: If you use a GeoIP source, ipv4 is automatically populated, and is not editable.

   The enrichment types that you have selected are displayed in the table.
4. For the added enrichment type, perform the following:
   - In the **Output** column, select the type that you have configured.
   - In the **Enrichment Source** drop-down list, select the enrichment source defined.

- In the **ESA Event Stream Meta** field, type the event stream meta key whose value will be used as one operand of join condition.

- In the **Enrichment Source Column Name** field, type the enrichment source column name whose value will be used as another operand of the join condition.

5. Select **Debug**. This will add a @Audit('stream') annotation to the rule. This is useful when debugging the esper rules.
6. Click **Show Syntax** to test if the defined ESA rule is valid.
7. Click **Save**.

For details on parameters and their descriptions, see Rule Builder Tab.

Deploy Rules to Run on ESA

This topic explains how to select an ESA and the rules to run on it. Administrator, SOC Manager or DPO role permissions are required for all tasks in this section.

To create a deployment, you need to perform the steps described in Deployment Steps

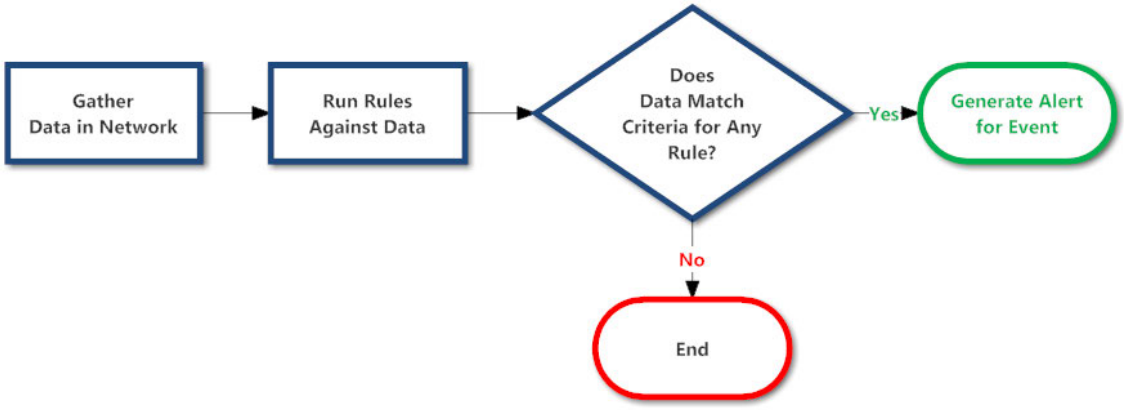
How Deployment Works

A deployment consists of an ESA service and a set of ESA rules. When you deploy rules, the ESA service runs them to detect suspicious or undesirable activity in your network. Each ESA rule detects a different event, such as when a user account is created and deleted within one hour.

The ESA service performs the following functions:

1. Gathers **data** in your network
2. Runs ESA **rules** against the data
3. Applies rule **criteria** to data
4. Generates an **alert** for the captured event

The following graphic shows this workflow:



In addition, you may want to perform other steps on your deployment, such as deleting an ESA service in your deployment, editing or deleting a rule from your deployment, editing or deleting a deployment, or showing updates to a deployment. For descriptions of these procedures, see Additional Deployment Procedures

Deployment Steps

This topic explains how to add a deployment, which includes an ESA service and a set of ESA rules. You can add a deployment to organize and manage ESA services and rules. Think of the deployment as a container for both components:

1. An ESA service
2. A set of ESA rules

For example, if you add a Spam Activity deployment it could include ESA London and a set of ESA rules to detect suspicious email activity.

To add a deployment, you need to complete the following procedures:

- Step 1. Add a Deployment
- Step 2. Add an ESA Service
- Step 3. Add and Deploy Rules

Step 1. Add a Deployment

Prerequisites

The following are required to add a deployment:

- The ESA service must be configured on the host. See "Configure ESA" in the *Event Stream Analysis (ESA) Configuration Guide*.
- Rules must be in the Rule Library. See Add Rules to the Rule Library.

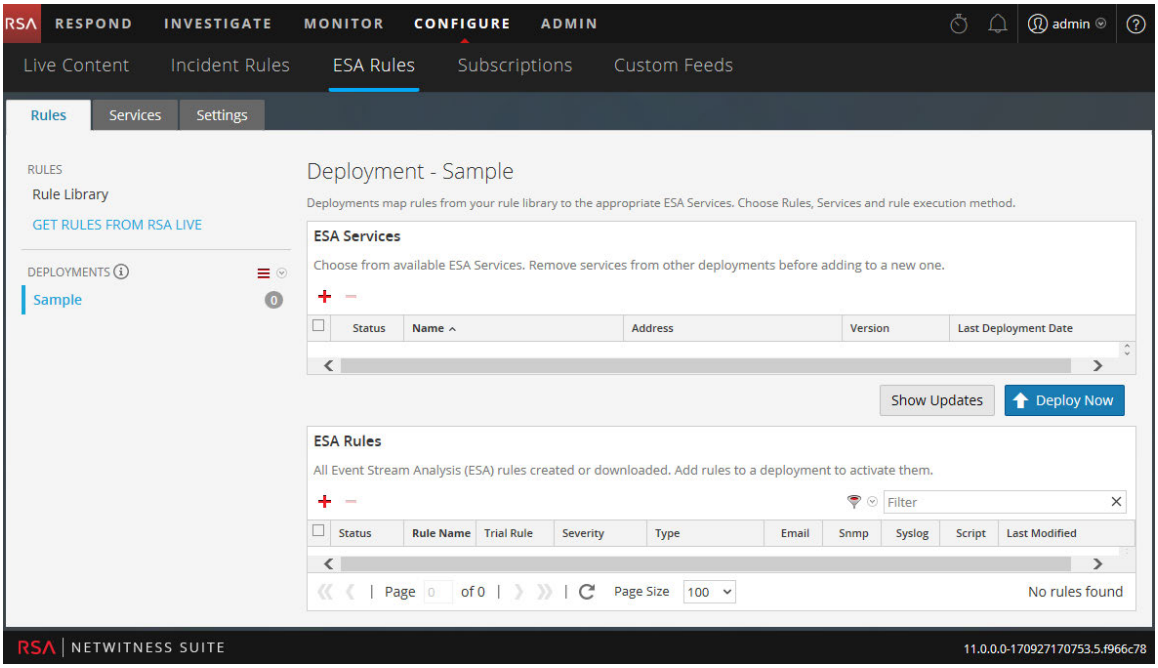
Procedure

To add a deployment:

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab is displayed.

2. In the options panel, next to Deployments, select > **Add**.

   The Deployment view is displayed on the right.

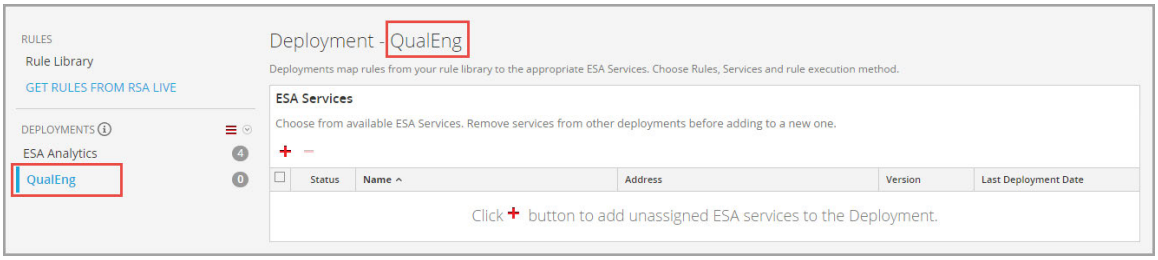


3. In the options panel, type a **name** for the deployment. The naming convention is up to you.

   For example, it could indicate the purpose or identify an owner.

4. Press **Enter**.

   The deployment is added.



Step 2. Add an ESA Service

The ESA service in a deployment gathers data in your network and runs ESA rules against the data. The goal is to capture events that match rule criteria, then generate an alert for the captured event.

You can add the same ESA to multiple deployments. For example, ESA London could be in the these deployments simultaneously:

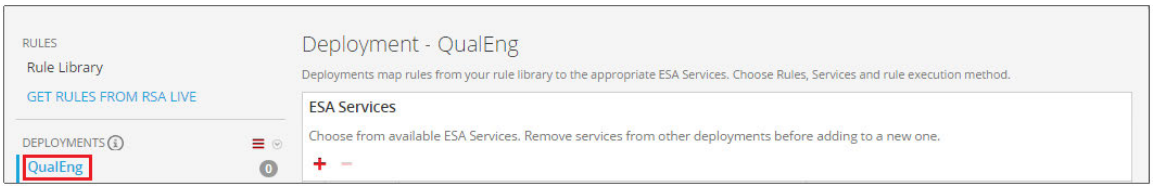
- Deployment EUR, which includes one set of ESA rules
- Deployment CORP, which includes another set of ESA rules

When you remove an ESA from a deployment, the rules are also removed from the ESA. For example, Deployment EUR could include ESA London and a set of 25 rules. If you remove ESA London from Deployment EUR, the 25 rules are also removed from ESA London. Consequently, if an ESA is not part of any deployment the ESA does not have any rules.

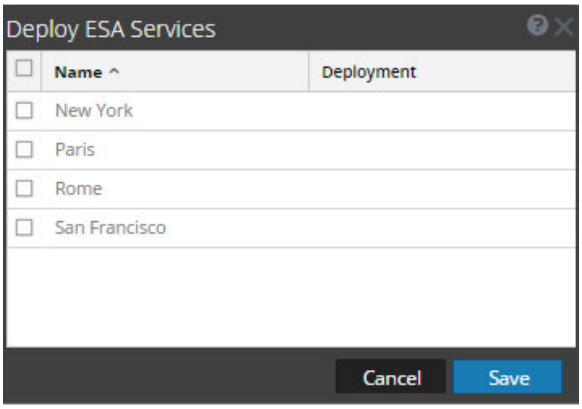
Procedure

To add an ESA service:

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab is displayed.
2. In the options panel, select a **deployment**:



3. In the **Deployment** view, click + in **ESA Services**.
   The Deploy ESA Services dialog lists each configured ESA.



4. Select an ESA and click **Save**.
   The Deployment view is displayed. The ESA is listed in the **ESA Services** section, with the status Added.

Step 3. Add and Deploy Rules

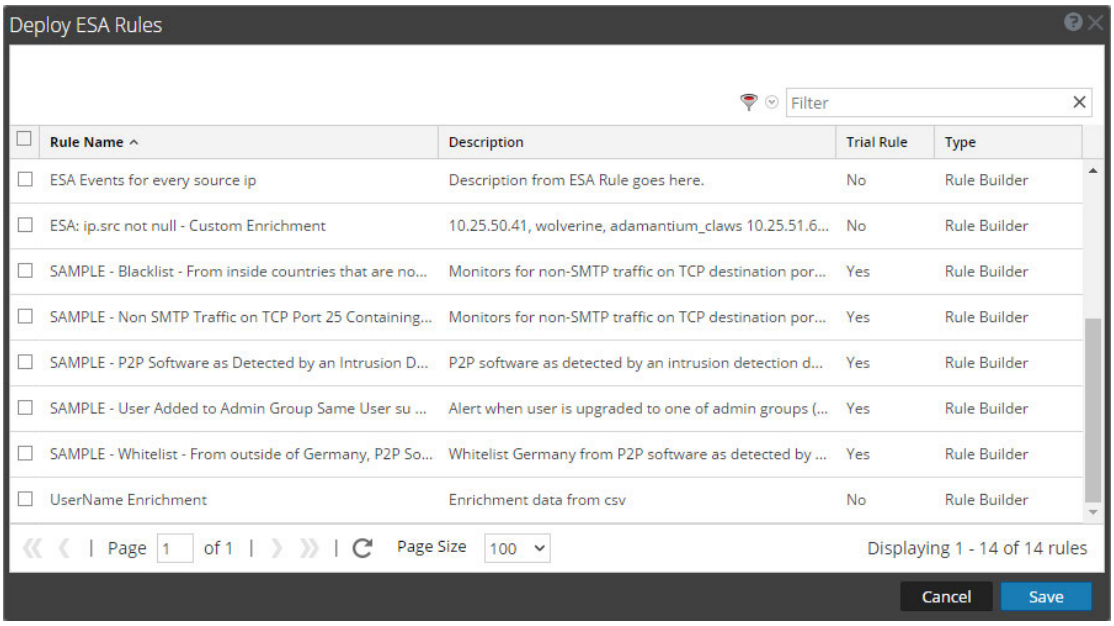
This topic explains how to add ESA rules to a deployment and then deploy the rules on ESA. Each ESA rule has unique criteria. The ESA rules in a deployment determine which events ESA captures, which in turn determine the alerts you receive.

For example, Deployment A includes ESA Paris and, among others, a rule to detect file transfer using a non-standard port. When ESA Paris detects a file transfer that matches the rule criteria, it captures the event and generates an alert for it. If you remove this rule from Deployment A, ESA will no longer generate an alert for such an occurrence.

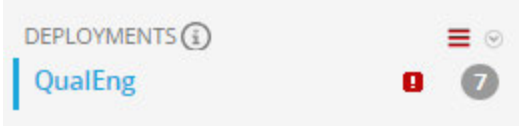
Procedure

To add and deploy rules:

1. Go to **Configure > ESA Rules**.
   The Rules tab is displayed.
2. In the options panel, select a deployment.
3. In the **Deployment** view, click + in **ESA Rules**.
   The Deploy ESA Rules dialog is displayed and shows each rule in your Rule Library:



4. Select rules and click **Save**.
   The Deployment view is displayed.
5. The rules are listed in the ESA Rules section.
   - In the Status column, **Added** is next to each new rule.
   - In the Deployments section, ! indicates there are updates to the deployment.
   - The total number of rules in the deployment is on the right.



6. Click **Deploy Now**.
   The ESA service runs the rule set.

Additional Deployment Procedures

In addition to deploying an ESA service and rules, you may want to perform other steps on your deployment, such as deleting an ESA service in your deployment, editing or deleting a rule from your deployment, editing or deleting a deployment, or showing updates to a deployment.

To perform these procedures, go to:

- Delete ESA Service in a Deployment
- Edit or Delete Rule in a Deployment
- Edit or Delete a Deployment
- Show Updates to a Deployment

Delete ESA Service in a Deployment

This topic provides instructions to delete an ESA service in a deployment. On a deployment with a service, you can edit the rules which are applied to the service and delete the service from the deployment.

Each of the following procedures starts in the Rules tab.

Procedure

To delete an ESA service:

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
   The Rules tab is displayed.
2. In the options panel, under **Deployments**, select a deployment.
3. In the **ESA Services** panel, select a service and click − in the toolbar.
   A confirmation dialog is displayed.
4. Click **Yes**.
   The service is deleted.

Edit or Delete Rule in a Deployment

On a deployment with rules, you can edit and delete rules to customize the deployment. Each of the following procedures starts in the Rules tab.

Procedures

Edit a Rule

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
   The Rules tab is displayed.
2. In the options panel, under Deployments, select a deployment.
3. In the **ESA Rules** panel, double-click a rule to open it in a new tab.
4. Modify the rule, then click **Apply**.
   The rule is saved.

Delete a Rule

1. Go to **CONFIGURE > ESA Rules > Rules** tab.
   The Rules tab is displayed.
2. In the options panel, under **Deployments**, select a deployment.
3. In the **ESA Rules** panel, select a rule and click in the toolbar.
   A confirmation dialog is displayed.
4. Click **Yes**.
   The rule is deleted.

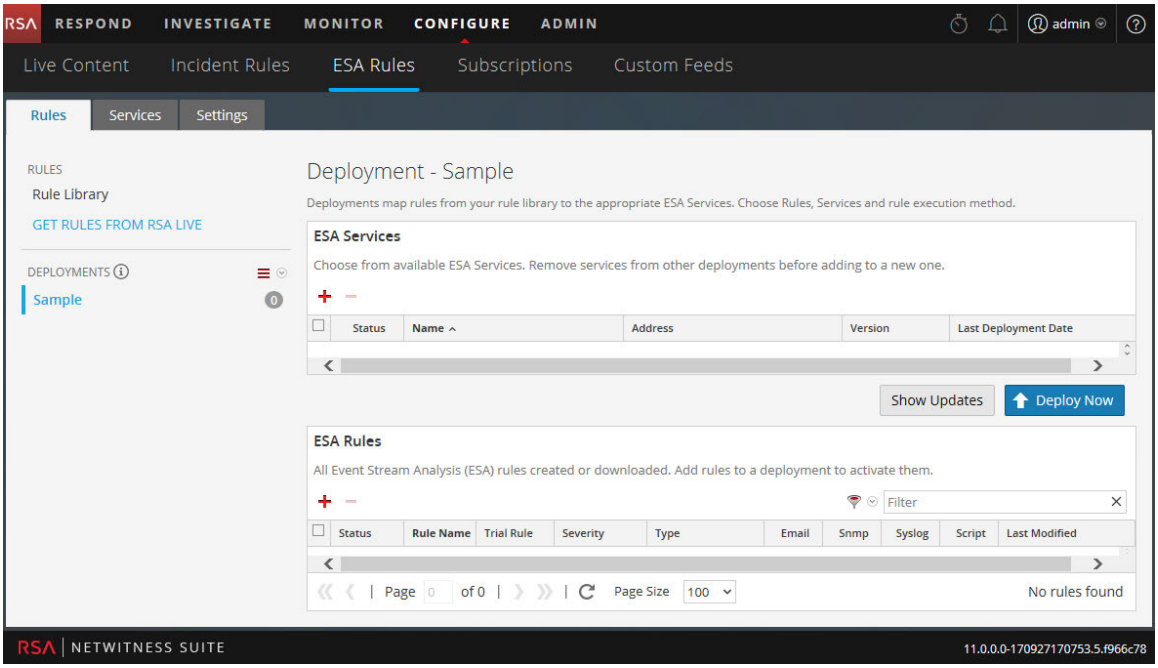
Edit or Delete a Deployment

This topic explains how NetWitness Suite forwards a correlation rule to each ESA service in a correlation group. In a correlation group, each ESA service must run the same set of rules. When you add a rule to a correlation group, NetWitness Suite forwards the rule to each ESA in the group.

To access the deployments:

1. Go to **CONFIGURE > ESA Rules**.
   The Configure view is displayed with the Rules tab open.
2. In the options panel, under **Deployments**, select a deployment.

The Deployment view is displayed.



Edit a Deployment

1. In the options panel, under **Deployments**, select a deployment.

   The Deployment view is displayed.

2. Select > **Edit**.

   The deployment name is made available for editing.

Delete a Deployment

1. In the options panel, under **Deployments**, select a deployment.

   The Deployment view is displayed.

2. Select > **Delete**.

   A confirmation dialog is displayed.

3. Click **Yes**.

   The deployment is deleted.

Show Updates to a Deployment

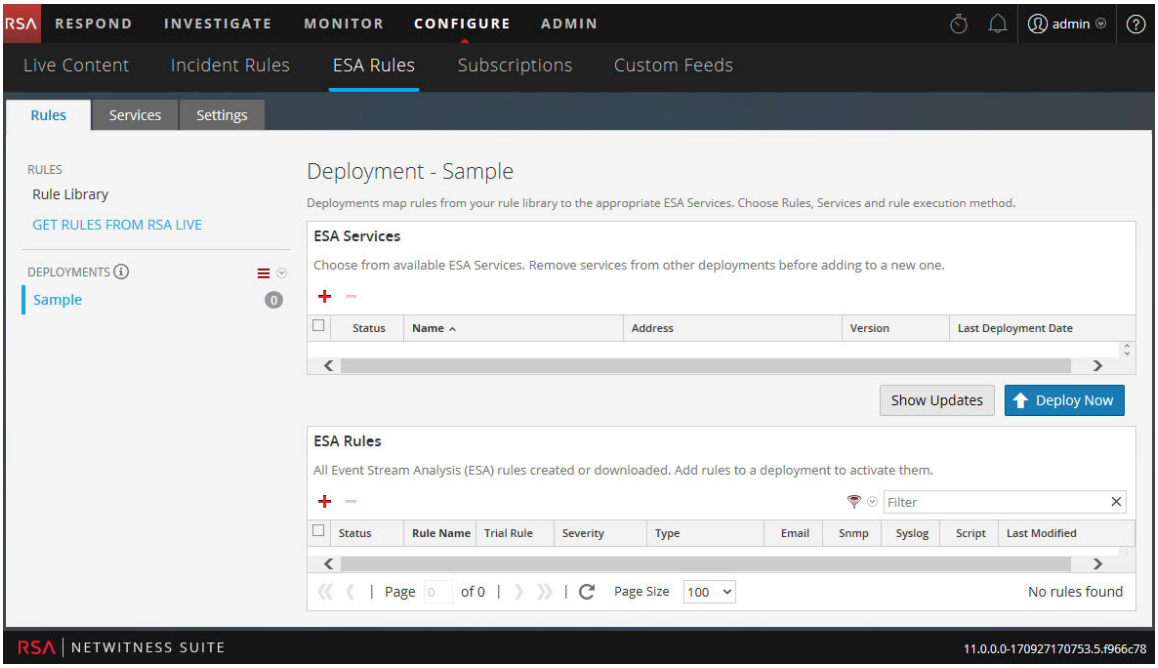
This topic explains how to show updates, such as adding or deleting rules, to a deployment.

When you make a change to a deployment, the update icon ( ) appears next to the name of the deployment.

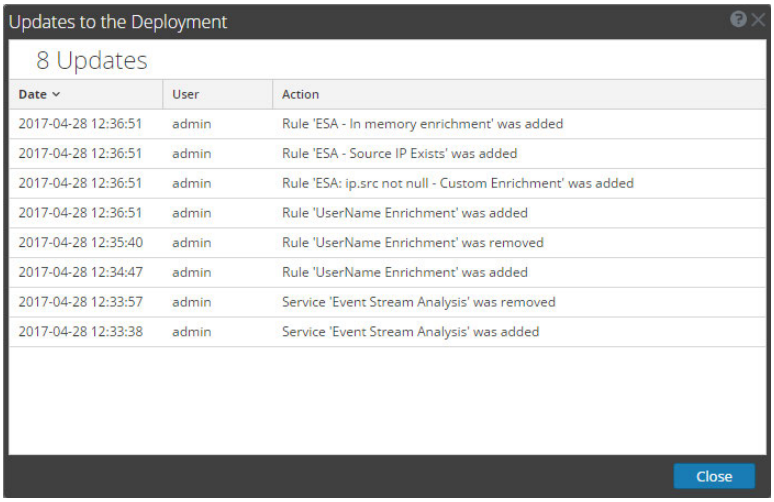
Procedure

To show the updates to a deployment:

1. Go to **CONFIGURE > ESA Rules.**
   The Rules tab is displayed.
2. In the options panel, under **Deployments** click **Show Updates** on the far right.



   The Updates to the Deployments dialog opens and shows the changes to the deployment.



3. Click **Close**.

View ESA Stats and Alerts

When the ESA generates alerts, you can view details about how the rules performed, such as statistics on the engine, rule, and alert, and you can also view information on which rules are enabled or disabled. For instructions on viewing ESA stats, see View Stats for ESA Service

When your ESA generates alerts, you can view the results in the Alerts Summary page. This enables you to see trends and understand both the volume and frequency of alerts. For instructions on viewing alerts, see View a Summary of Alerts

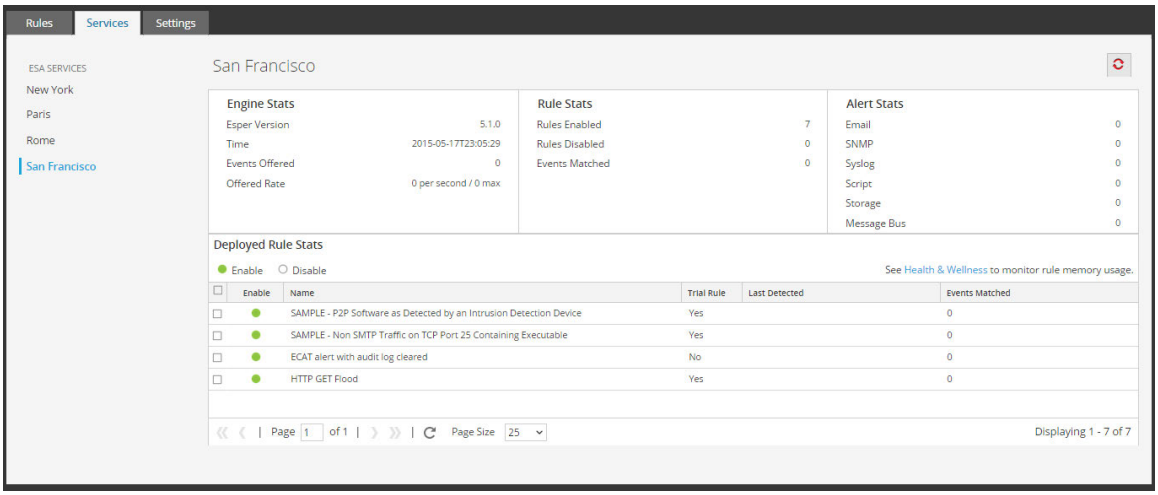
View Stats for ESA Service

This topic describes how to view the deployment stats for an ESA service. This procedure is useful when you are attempting to determine the effectiveness of a rule or troubleshoot a deployment.

Procedures

View ESA Stats

1. Go to **CONFIGURE > ESA Rules > Services** tab.
2. From the **ESA Services** list on the left, select a service.
   The deployment stats for the selected service are displayed.



3. Review the following sections of ESA stats.
   For a complete description of each statistic in each section, see Services Tab.

- **Engine Stats**
- **Rule Stats**
- **Alert Stats**

4. In the Deployed Rule Stats, review details about the rules deployed on the ESA.
   For a complete description of each column in each section, see Services Tab.
   - If the rule is enabled or disabled
   - What the rule name is
   - If the rule is running in Trial Rule mode
   - Last detected
   - Events matched
5. To get a snapshot of the rule memory, click **Health & Wellness**.

Enable or Disable Rules

1. In the **Deployed Rule Stats** panel, select a rule from the grid.
2. Click Enable to enable the rule, or click Disable to disable the rule.
   The Services tab is refreshed to show the changes, which take effect immediately.

Refresh the Statistics

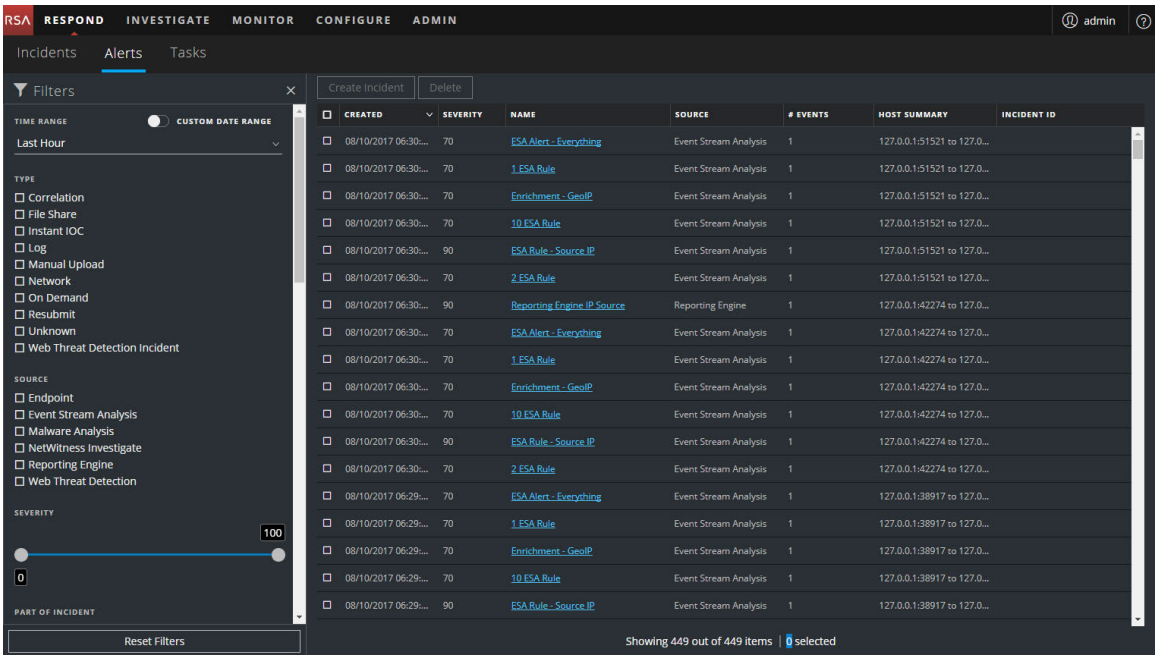
The Services tab does not update statistics automatically unless you enable or disable a rule. To ensure you view current statistics:

1. Click in the upper right corner to refresh the information.
2. View the updated information.

View a Summary of Alerts

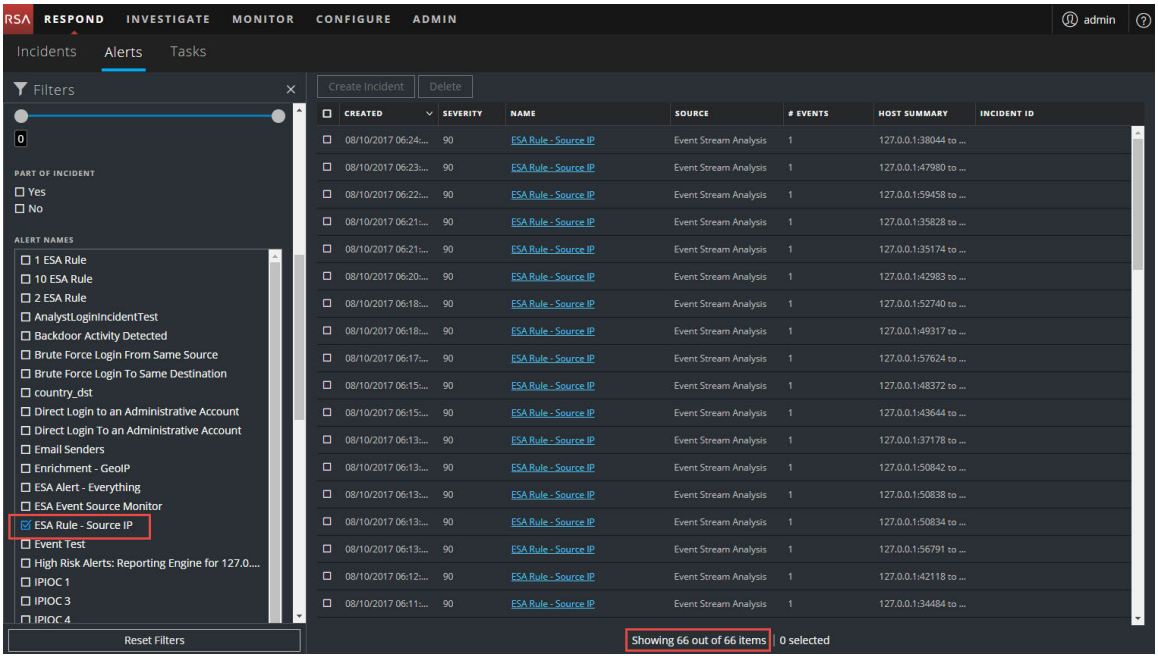
In the RESPOND view, you can browse through various alerts from multiple sources. You can filter the alerts list to show only alerts of interest, such as by Alert Name, alert source, and a specific time range.

1. Go to **RESPOND > Alerts**.
   The Respond Alerts List view displays a list of all NetWitness Suite alerts.



2. In the **Filters** panel on the left, you can filter the alerts list to view specific alerts for a specific time frame. For example, in the ALERT NAMES section, you can select an alert for an ESA rule, such as ESA Rule - Source IP, and leave the TIME FRAME set to Last Hour.

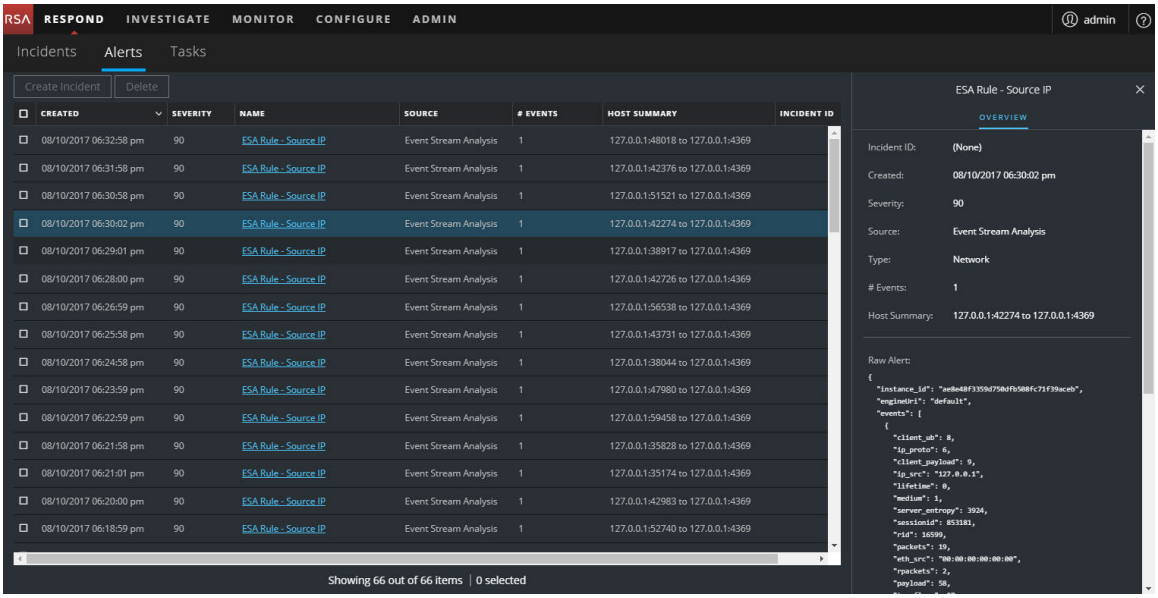
   The alerts list to the right shows a list of alerts that match your filter selection along with a count of the alerts at the bottom of the alerts list.



   The alerts list shows information about each of the alerts.

- **Created**: Displays the date and time when the alert was created in the source system.
- **Severity**: Displays the level of severity of the alert. The values are from 1 to 100.
- **Name**: Displays a basic description of the alert.
- **Source**: Displays the original source of the alert.
- **# of Events**: Indicates the number of events contained within an alert.
- **Host Summary**: Displays details of the host, like the host name from where the alert was triggered.
- **Incident ID**: Shows the incident ID of the alert. If there is no incident ID, the alert does not belong to an incident.

3. You can click on an alert in the list to open an **Overview** panel on the right where you can view raw alert metadata.



For more information about filtering alerts and viewing alert details, see the *NetWitness Respond User Guide*.

ESA Alert References

In the Alerts module, you configure and deploy ESA rules to get alerted about potential network threats.

These topics explain the user interface in the Alerts module.

- New Advanced EPL Rule Tab
- Build a Statement Dialog
- Deploy ESA Rules Dialog
- Deploy ESA Services Dialog
- Rule Builder Tab
- Rules Tab
- Rule Syntax Dialog
- Services Tab
- Settings Tab
- Updates to the Deployment Dialog

New Advanced EPL Rule Tab

The Advanced EPL Rule tab enables you to define rule criteria with an Event Processing Language (EPL) query.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Define an Advanced EPL rule.	Add an Advanced EPL Rule
Content Expert	See examples of an Advanced EPL Rule.	Sample Advanced EPL Rules

Related Topics

- Add a Rule Builder Rule
- Enrichment Sources

Advanced EPL Rule

To access the Advanced EPL Rule tab:

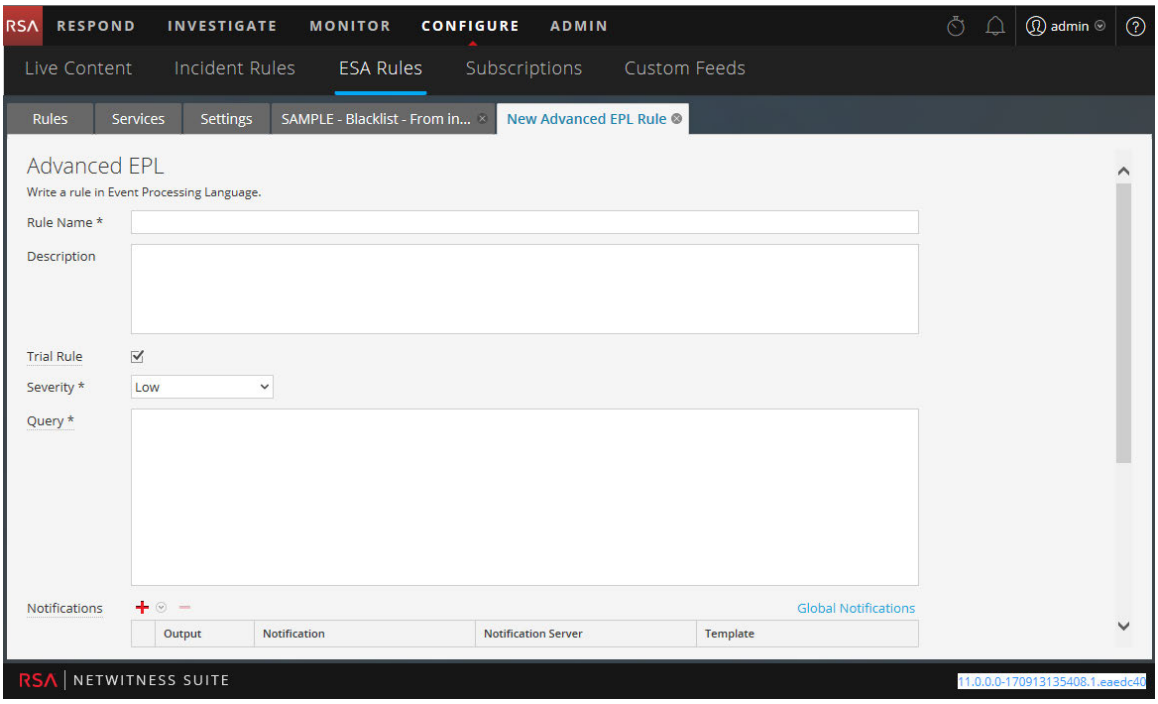
1. Go to **CONFIGURE > ESA Rules**.

   The Configure view is displayed with the Rules tab open by default.

2. In the **Rule Library** toolbar, select **> Advanced EPL**.

   The Advanced EPL Rule tab is displayed.

Below is a screen shot of the Advanced EPL Rule tab.



The following table lists the parameters in the Advanced EPL Rule tab.

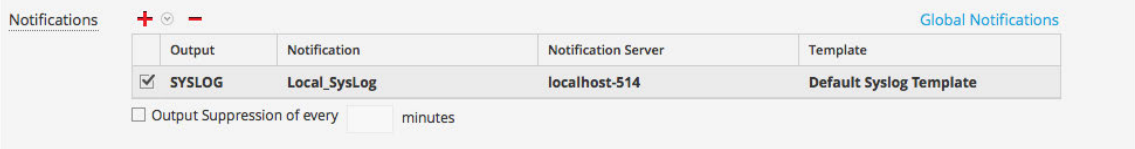
Parameters	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.
Query	EPL query that defines rule criteria.

Notifications

In the Notifications section, you can choose how to be notified when ESA generates an alert for the rule.

For more information on the alert notifications, see Add Notification Method to a Rule.

The following figure shows the Notifications section.



Parameter	Description
+	To add an alert notification type.
−	To delete the selected alert notification type.
Output	Alert notification type. Options are: • Email • SNMP • Syslog • Script
Notification	Name of previously configured output, such as an email distribution list.
Notification Server	Name of server that sends the output.
Template	Name of template for the alert notification.
Output Suppression of every	Option to specify alert frequency.
Minutes	Alert frequency in minutes.

Enrichments

In the Enrichments section, you can add a data enrichment source to a rule.

For more information on the enrichments, see Add an Enrichment to a Rule.
The following figure shows the Enrichments section.

Parameter	Description
+	To add an enrichment.

Parameter	Description
−	To delete the selected enrichment.
Output	Enrichment source type. Options are: • In-Memory Table • External DB Reference • Warehouse Analytics • GeoIP
Enrichment Source	Name of previously configured enrichment source, such as a .CSV filename for an In-Memory Table.
ESA Event Stream Meta	ESA meta key whose value will be used as one operand of join condition.
Enrichment Source Column Name	Enrichment source column name whose value will be used as the other operand of the join condition.

Build a Statement Dialog

The Build a Statement dialog allows you to construct a condition statement when creating a new Rule Builder rule.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Configure a rule statement.	Add an Advanced EPL Rule
Content Expert	Add conditions to the rule.	Step 3. Add Conditions to a Rule Statement

Related Topics

- Add a Rule Builder Rule

Build a Statement Dialog

To access the Build a Statement dialog:

1. Go to **CONFIGURE > ESA Rules**.

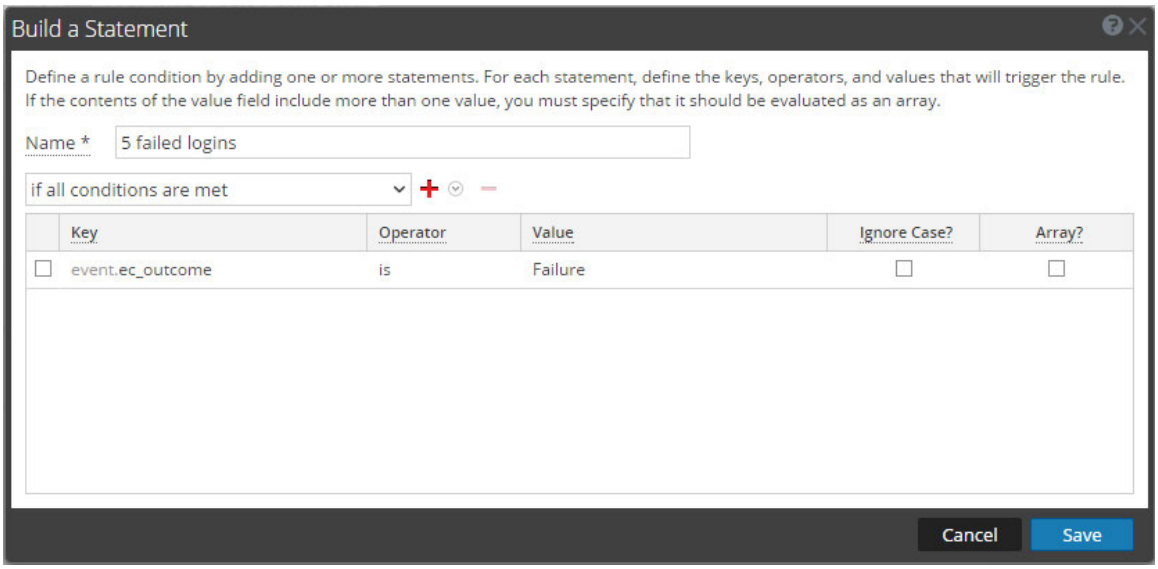
   The Configure ESA Rules view is displayed with the Rules tab open.

2. In the **Rule Library** toolbar, select **> Rule Builder**.

   A New Rule tab is displayed..

3. In the **Conditions** section, click .

   The Build a Statement dialog is displayed.



The following table describes the parameters in the Build a Statement dialog.

Parameter	Description
Name	Purpose of the statement.
Select	Conditions the rule requires. There are two options: • If all conditions are met • If any of these conditions are met
Key	Key for ESA to check in the rule statement.

Parameter	Description
Evaluation Type	Relationship between the meta key and value for the key: • is • is not • is not null • is greater than (>) • is greater than or equal to (>=) • is less than (<) • is less than or equal to (<=) • contains • not contains • begins with • ends with
Value	Value for ESA to look for in the key.
Ignore Case?	This field is designed for use with string and array of string values. By choosing the **Ignore Case** field, the query will treat all string text as a lowercase value. This ensures that a rule that searches for the user named Johnson would trigger if the event contains "johnson," "JOHNSON," or "JoHnSoN."
Array?	Choice to indicate if contents of Value field represent one value or multiple values: • Select the box to indicate multiple values. • Clear the box to indicate one value.
+	Add a statement. You can add a meta condition, whitelist condition, or blacklist condition.
−	Delete selected statement.
Save	Add statement to the Conditions section of the Rule Builder tab.

The following table shows the operators you can use in the Rule Builder:

Operator	Required Value	Usage	Example	Meaning
is	Singular string value	The meta key is equal to the *value* field.	***user_dst*** is John Doe.	***user_dst*** is equal to the string *"John Doe"*.
is	Array string value	The meta key is equal to one of the elements of the *value* field.	*user_dst* is John, Doe, Smith.	*user_dst* is equal either to the string *"John"* or to the string *"Doe"* or to the string *"Smith"* (Note, the spaces are stripped.).
is not	Singular string value	The meta key is not equal to the *value* field.	***size*** is not 200.	***size*** is not equal to the number 200 (size is a numeric value).
is not	Array string value	The meta key is not equal to any of the elements of the *value* field.	***size*** is not 200, 300, 400.	***size*** is equal neither to *200* nor to *300* nor to *400*.
is not null	N/A (looks for any value)	The meta key value is not null.	***user_dst*** is not null.	***user_dst*** is a meta that contains a value.
is greater than (>)	Number	The numeric value of the meta key is greater than the number in the *value* field.	***payload*** is greater than 7000.	***payload*** is a numeric value that is greater than 7000.
is greater than or equal to (>=)	Number	The numeric value of the meta key is greater than or equal to the number in the *value* field.	***payload*** is greater than or equal to 7000.	***payload*** is a numeric value that is greater than or equal to 7000.
is less than (<)	Number	The numeric value of the meta key is less than the number in the *value* field.	***ip_dstport*** is less than 1024.	***ip_dstport*** is a numeric value that is less than the numeric value 1024.
is less than or equal to (<=)	Number	The numeric value of the meta key is less than or equal to the number in the *value* field.	***ip_dstport*** is less than or equal to 1024.	***ip_dstport*** is a numeric value that is less than or equal to numeric value 1024.
contains	String	The *value* field is a substring of the meta key (This operator is only available for a string-valued meta key).	***ec_outcome*** contains failure.	***ec_outcome*** is a string that contains the substring *"failure"*.
not contains	String	The *value* field is not a substring of the meta key (This operator is only available for a string-valued meta key).	***ec_outcome*** not contains failure.	***ec_outcome*** is a string that does not contain the substring*"failure"*.

Operator	Required Value	Usage	Example	Meaning
begins with	String	The *value* field is the beginning of the meta key (This operator is only available for a string-valued meta key).	***ip_dst*** begins with 127.0.	***ip_dst*** is a string that starts with *"127.0"*.
ends with	String	The *value* field is the end of the meta key (This operator is only available for a string-valued meta key).	***user_dst*** ends with son.	***user_dst*** is a string that ends in*"son"*.

Note: Terms in ***bold italic*** are Meta that may not exist in all customer enviroments.

Deploy ESA Rules Dialog

The Deploy ESA Rules dialog enables you to filter and select rules to deploy to an ESA service.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Configure a deployment.	Step 1. Add a Deployment
Content Expert	Deploy a rule	Step 3. Add and Deploy Rules

Related Topics

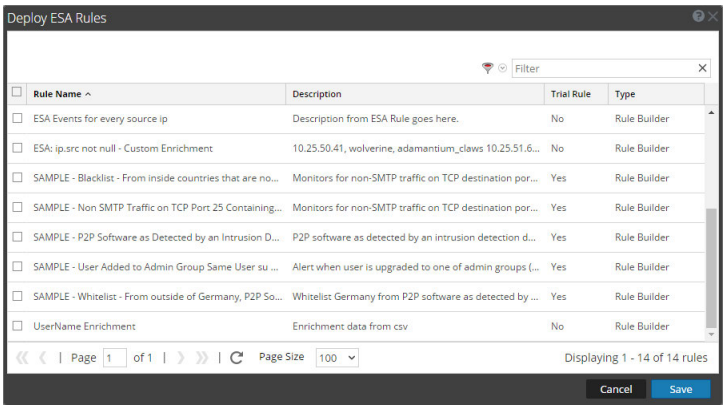
- Additional Deployment Procedures

Deploy ESA Rules Dialog

To access this dialog:

1. Go to **CONFIGURE** > **ESA Rules**.
   The Rules tab opens by default.
2. In the options panel, under the **Deployment** section, select or add a new deployment by clicking > **Add**.
3. If you add a new deployment, type the name of the deployment in the box in the options panel.
4. In the **ESA Rules** panel, click .
   The Deploy ESA Rules dialog is displayed.

The following figure shows an example of this dialog.



The following table describes the parameters of the Deploy ESA Rules dialog.

Parameters	Description
	Filters the list of rules based on severity and type. The text box beside this icon filters based on rule name.
Rule Name	Displays the name of the rule.
Description	Describes the rule.
Trial Rule	Indicates whether or not the rule is a trial rule.
Type	Indicates the type of rule: RSA Live ESA, Advanced EPL, or Rule Builder.

Deploy ESA Services Dialog

The Deploy ESA Services dialog displays all ESA services available to be added to a deployment.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Configure a deployment.	Step 1. Add a Deployment
Content Expert	Deploy a service	Step 2. Add an ESA Service

Related Topics

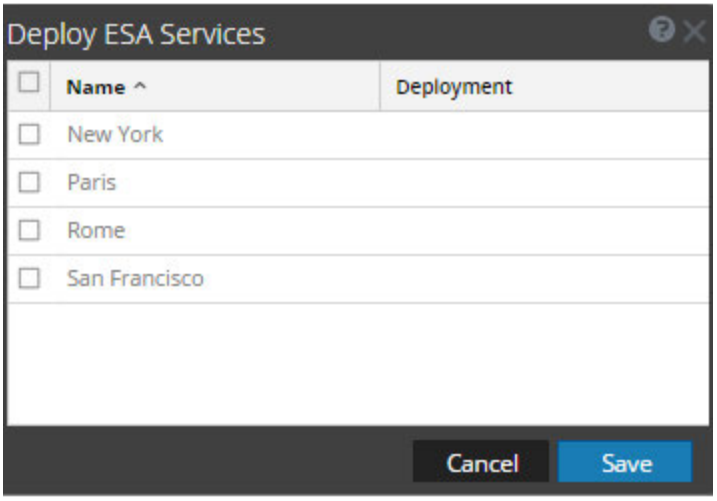
- Additional Deployment Procedures
- View Stats for ESA Service

Deploy ESA Services Dialog

To access this dialog:

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab opens by default.
2. In the options panel, under the **Deployment** section, select or add a deployment.
3. In the **ESA Services** panel, click .
   The Deploy ESA Services dialog is displayed.

The following figure is an example of this dialog.



The following table describes the parameters of the Deploy ESA Services dialog.

Parameters	Description
Name	Displays the name of configured ESA services.
Deployment	Displays the deployments to which the service has already been added.

Rule Builder Tab

The Rule Builder tab enables you to define a Rule Builder rule.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Define a Rule Builder rule.	Add a Rule Builder Rule
Content Expert	Define rule criteria.	Step 2. Build a Rule Statement
Content Expert	Add conditions to the rule.	Step 3. Add Conditions to a Rule Statement

Related Topics

- Add an Advanced EPL Rule

Rule Builder

To access the Rule Builder tab:

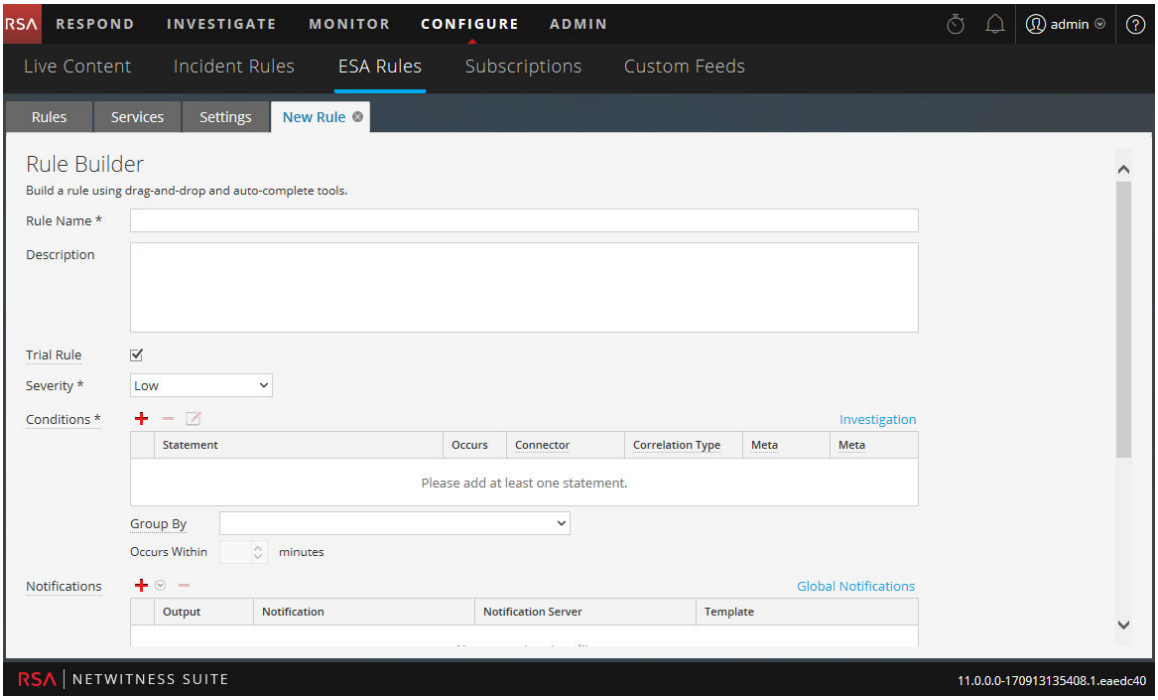
1. Go to **CONFIGURE** > **ESA Rules**.

   The Rules tab opens by default.

2. In the **Rule Library** toolbar, select > **Rule Builder**.

   The Rule Builder tab is displayed.

The following figure shows the Rule Builder tab.



The following table lists the parameters in the Rule Builder tab.

Parameters	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.

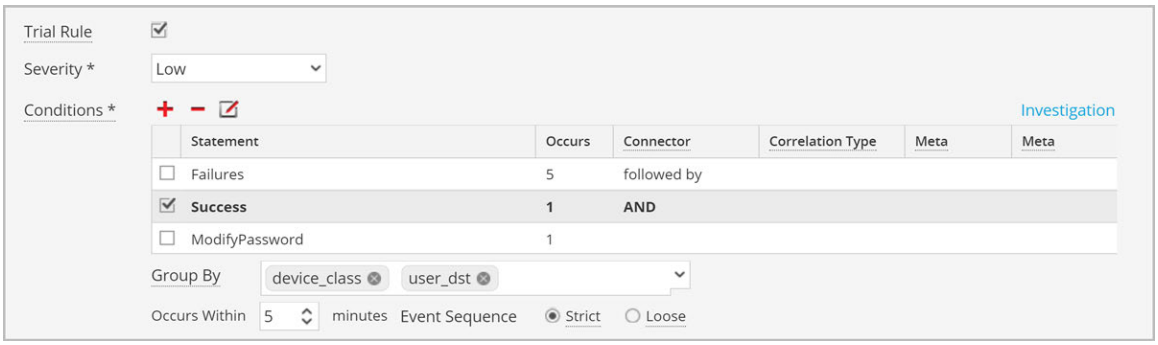
The Rule Builder includes the following components:

- Conditions section
- Notifications section
- Enrichments section

Conditions Section

In the Conditions section of the Rule Builder tab, you define what the rule detects.

The following figure shows the Conditions section.



The following table lists the parameters of the Conditions section.

Parameter	Description
+	Add a statement.
−	Remove selected statement.
✎	Edit selected statement.
Statement	Logical group of conditions for one operation.
Occurs	Alert frequency if the condition is met. This specifies that there must be at least that many events that satisfy the criteria in order to trigger an alert. The time window in minutes binds the Occurs count.

Parameter	Description
Connector	Options to specify relationship among the statements: • followed by • not followed by • AND • OR The Connector joins two statements with AND, OR, followed by, or not followed by. When followed by is used, it specifies that there is a sequencing of those events. AND and OR build one large criteria. The followed by creates distinct criteria that occurs in sequence.
Correlation Type	**Correlation Type** applies only to **followed by** and **not followed by**. If you choose a correlation type of SAME, select one meta to correlate on, and if you choose a correlation type of JOIN, select two meta to correlate on. You may want to use JOIN if you are trying to correlate on meta from two different data sources. For example, say you want to correlate an AV alert with an IDS alert.
Meta	Enter the meta condition if choosing a correlation type of SAME or JOIN (as described above).
Meta	Enter the second meta condition if choosing a correlation type of JOIN (as described above). For example, The destination IP address from the AV alert and source IP address for the workstation from the IDS alert are joined to allow you to view the same entities across different sources.
occurs within minutes	Time window within which the conditions must occur.

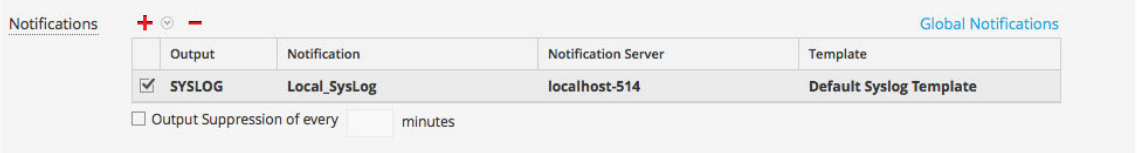
Parameter	Description
Event Sequence	Choose whether the pattern must follow a *strict* match or a *loose* match. If you specify a strict match, this means that the pattern must occur in the *exact* sequence you specified with no additional events occurring in between. For example, if the sequence specifies five failed logins (F) followed by a successful login (S), this pattern will only match if the user executes the following sequence: F,F,F,F,F,S. If you specify a loose match, this means that other events may occur within the sequence, but the rule will still trigger if all of the specified events also occur. For example, five failed login attempts (F), followed by any number of intervening successful login attempts (S), followed by a successful login attempt might create the following pattern: F,S,F,S,F,S,F,S,F,S which would trigger the rule despite the intervening successful logins.
Group By	Select the meta key by which to group results from the dropdown list. For example, suppose that there are three users; Joe, Jane, and John and you use the Group By meta, **user_dst** (user_dst is the meta field for the user destination account). The result will show events grouped under the user destination accounts, Joe, Jane, and John. You can also group by multiple keys. For example, you might want to group by user and machine to see if a user logged in from the same machine attempts to log into an account multiple times. To do this, you might group by device_class and user_dst.

Notifications

In the Notifications section, you can choose how to be notified when ESA generates an alert for the rule.

For more information on the alert notifications, see Add Notification Method to a Rule.

The following figure shows the Notifications section.



Parameter	Description
+	To add an alert notification type.
−	To delete the selected alert notification.

Parameter	Description
Output	Alert notification type. Options are: • Email • SNMP • Syslog • Script
Notification	Name of previously configured output, such as an email distribution list.
Notification Server	Name of server that sends the output.
Template	Name of template for the alert notification.
Output Suppression of every	Option to specify alert frequency.
Minutes	Alert frequency in minutes.

Enrichments

In the Enrichments section, you can add a data enrichment source to a rule.

For more information on the enrichments, see Add an Enrichment to a Rule.

The following figure shows the Enrichments section.

Parameter	Description
+	To add an enrichment.
−	To delete the selected enrichment.

Parameter	Description
Output	Enrichment source type. Options are: • In-Memory Table • External DB Reference • Warehouse Analytics • GeoIP
Enrichment Source	Name of previously configured enrichment source, such as a .CSV filename for an In-Memory Table.
ESA Event Stream Meta	ESA meta key whose value will be used as one operand of join condition.
Enrichment Source Column Name	Enrichment source column name whose value will be used as the other operand of the join condition. For an in-memory table, If you configured a key when creating a .CSV-based enrichment, this column automatically populates with the selected key. However, you can change it if you like. For a GeoIP enrichment source, ipv4 is automatically selected.

Rules Tab

The Rules tab enables you use to manage ESA rules and deployments.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	View types of rules.	ESA Rule Types
Content Expert	Deploy Trial Rules.	Work with Trial Rules
Content Expert	Create a rule.	Add Rules to the Rule Library
Content Expert	Deploy a rule.	Deploy Rules to Run on ESA

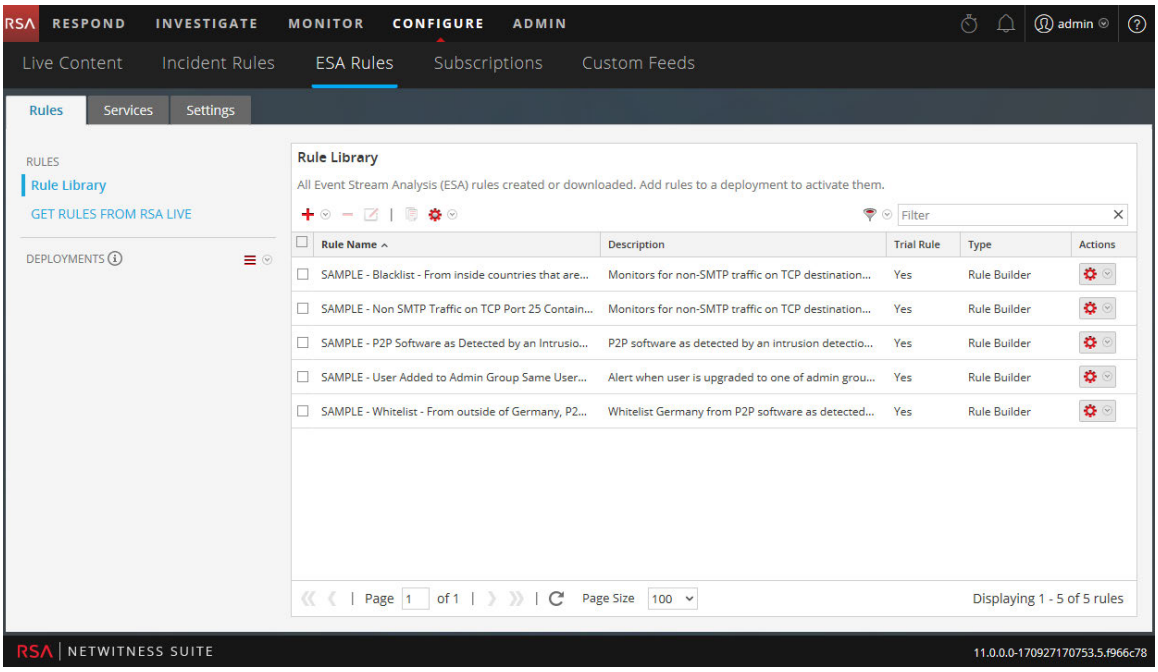
Related Topics

- Getting Started with ESA

Rule Builder

The Rules tab is displayed when you go to **CONFIGURE > ESA Rules**.

The following figure shows the Rules tab.



The Rules tab is divided into three sections:

- Rules Tab Options Panel
- Rule Library Panel
- Deployment Panel

Rules Tab Options Panel

In the **Rules** tab options panel to the left, you can view ESA rules in the Rule Library and create deployments.

What do you want to do?

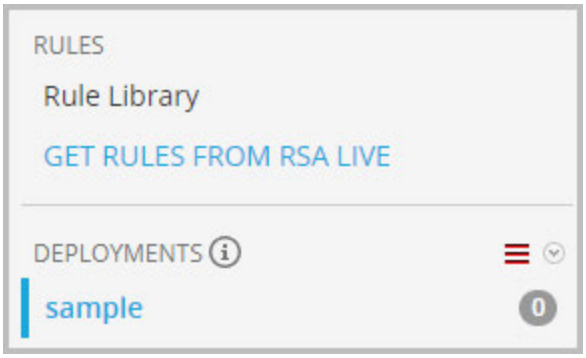
Role	I want to ...	Show me how
Content Expert	View an ESA rule.	Add Rules to the Rule Library
Content Expert	Create a deployment.	Deployment Steps

Related Topics

- Working with Rules

Options Panel

The following figure shows the options panel in the **Rules** tab.



There are two sections in the options panel: Rules and Deployments.

Rules Section

The Rules section contains two options. **Rule Library** is selected by default, and when it's selected, the Rule Library view is displayed within the tab. **Get Rules From RSA Live** navigates to the Live Search view, where you can search for rules.

Deployments Section

The Deployments section lists deployments and indicates whether there are updates to the deployments. From this section, deployments can be added, deleted, edited, and refreshed. Selecting a deployment from the list displays the Deployment panel within the tab. The following table describes the features of this section.

Feature	Description
	Displays a drop-down menu from which you can choose to add, edit, or delete a deployment. You can also refresh the list of deployments to see if there are any new updates to the list.
	Indicates whether there are any updates to the deployment.
	Indicates the number of rules in the deployment.

Rule Library Panel

The Rule Library panel allows you to manage rules.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Add an ESA rule.	Add a Rule Builder Rule
Content Expert	Edit, duplicate, or delete an ESA rule.	Edit, Duplicate or Delete a Rule
Content Expert	Import or export ESA rules.	Import or Export Rules
Content Expert	Filter the ESA rules list.	Filter or Search for Rules

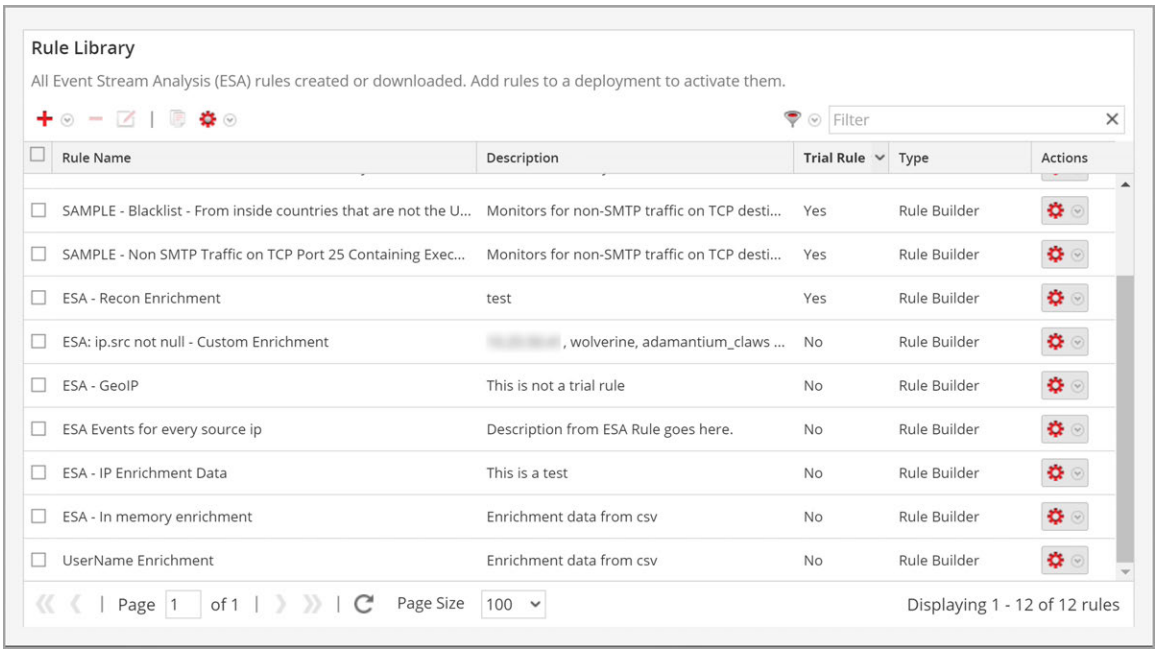
Related Topics

- Add an Advanced EPL Rule

Rule Library Panel

To access this view, go to **CONFIGURE > ESA Rules**. The Rules tab is displayed and the Rule Library panel is on the right.

The following figure shows the Rule Library panel.



The Rule Library panel includes the following components:

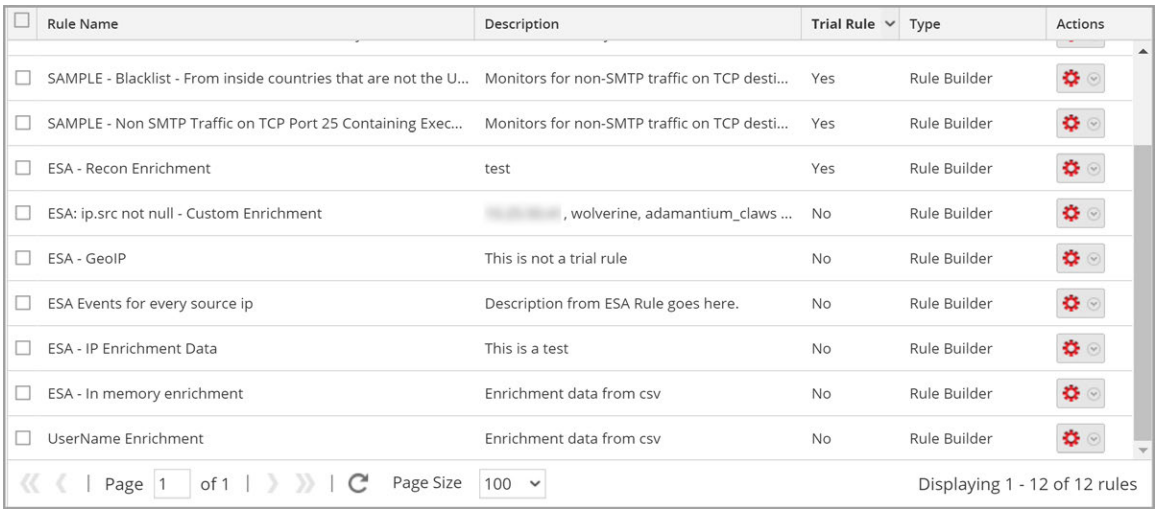
- Rule Library toolbar
- Rule Library list

Rule Library Toolbar

The Rule Library toolbar allows you to add, delete, edit, duplicate, filter, export, and import ESA rules. The following figure shows the icons for these actions.

Rule Library List

The following figure shows the Rule Library list.

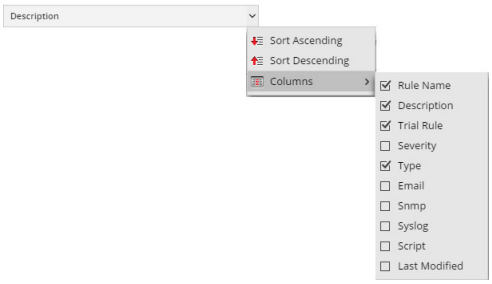


The Rule Library list shows all the ESA rules that have been downloaded from RSA Live or created in the Advanced EPL and Rule Builder tabs. The following table lists the columns in the Rule Library list and their description.

Column	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Type	The type of rule.

Column	Description
Actions (⚙)	Menu to delete, edit, duplicate, or export the selected rule.
Severity	Threat level of alert triggered by the rule.
Email	Indicates whether an alert notification for the rule is sent by email. This column is not visible by default.
Snmp	Indicates whether an alert notification for the rule is sent using SNMP. This column is not visible by default.
Syslog	Indicates whether an alert notification for the rule is sent using Syslog. This column is not visible by default.
Script	Indicates whether an alert notification for the rule executes a script. This column is not visible by default.
Last Modified	The date and time when the ESA rule was last modified. This column is not visible by default.

To display columns which aren't visible by default, hover over the title of a column and click the **v** on the right. This opens a drop-down menu in which you can sort the contents of the column or choose which columns you want to see in the Rule Library list.



Deployment Panel

This topic provides an overview of the Deployment panel. The Deployment panel enables you to create and configure the deployments. The Deployment panel includes the following sections:

- ESA Services
- ESA Rules

What do you want to do?

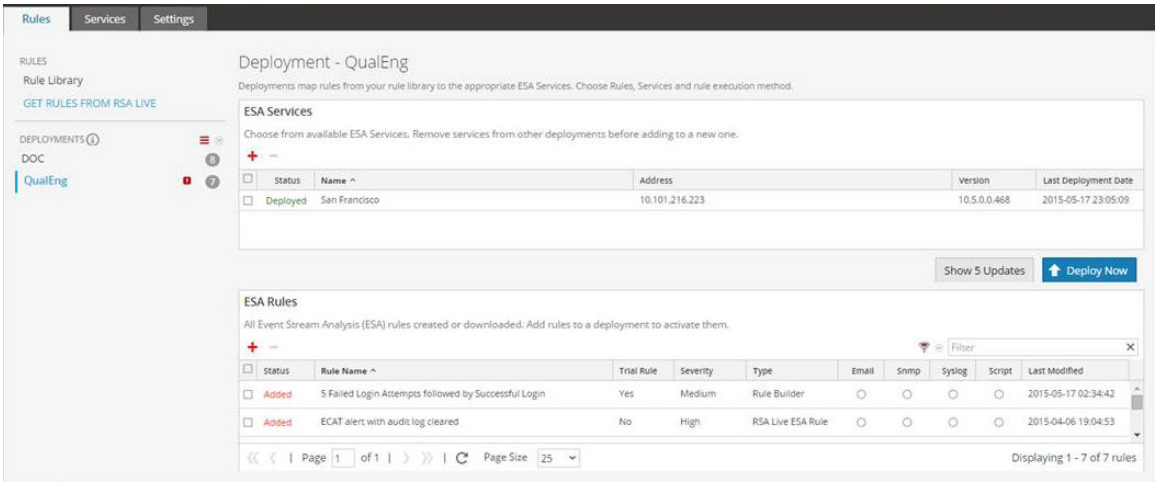
Role	I want to ...	Show me how
Content Expert	Add a deployment.	Deployment Steps
Content Expert	Manage deployments.	Additional Deployment Procedures

Related Topics

- View Stats for ESA Service

Deployment Panel

The following figure shows the Deployment panel.



ESA Services

Using the ESA Services section, you can manage each ESA service in the deployment.

In the ESA Services section, you can perform the following.

Task	Description

Task	Description
	Add an ESA service to the deployment.
	Remove the selected ESA service from the deployment.
Show Updates	Open the Updates to the Deployment dialog.
Deploy Now	Deploy current set of rules.

The following table lists the parameters of the ESA Services section.

Parameter	Description
Status	Indicates if the deployment status is **Added**, **Deployed**, **Updated**, or **Failed**.
Name	Name of the ESA service.
Address	IP address of the host where the ESA service is installed.
Version	Version of the ESA service.
Last Deployment Date	The date and time when the ESA service was last deployed.

ESA Rules

In the ESA Rules section, you manage rules in the deployment. This section lists all rules that are currently in the deployment.

In the **ESA Rules** section, you can perform the following.

Task	Description
	Open the Deploy ESA Rules dialog, where you can select a rule.
	Remove the selected ESA rules from the deployment.
	Filter the list of rules.

Task	Description
Filter	Search for a rule.

The following table lists the parameters of the ESA Rules section.

Parameter	Description
Status	Indicates the rule status: • Deployed - the rule is deployed. • Updated - the rule has been updated since the last deployment. • Added - the rule has been added since the last deployment. • Failed - the deployment failed.
Rule Name	Purpose of the ESA rule.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.
Output	The type of the ESA rule.
Email, SNMP, Syslog, Script	Indicates which notification types are used for alerts generated by the rules.
Last Modified	The date and time when the ESA rule was last modified.

Rule Syntax Dialog

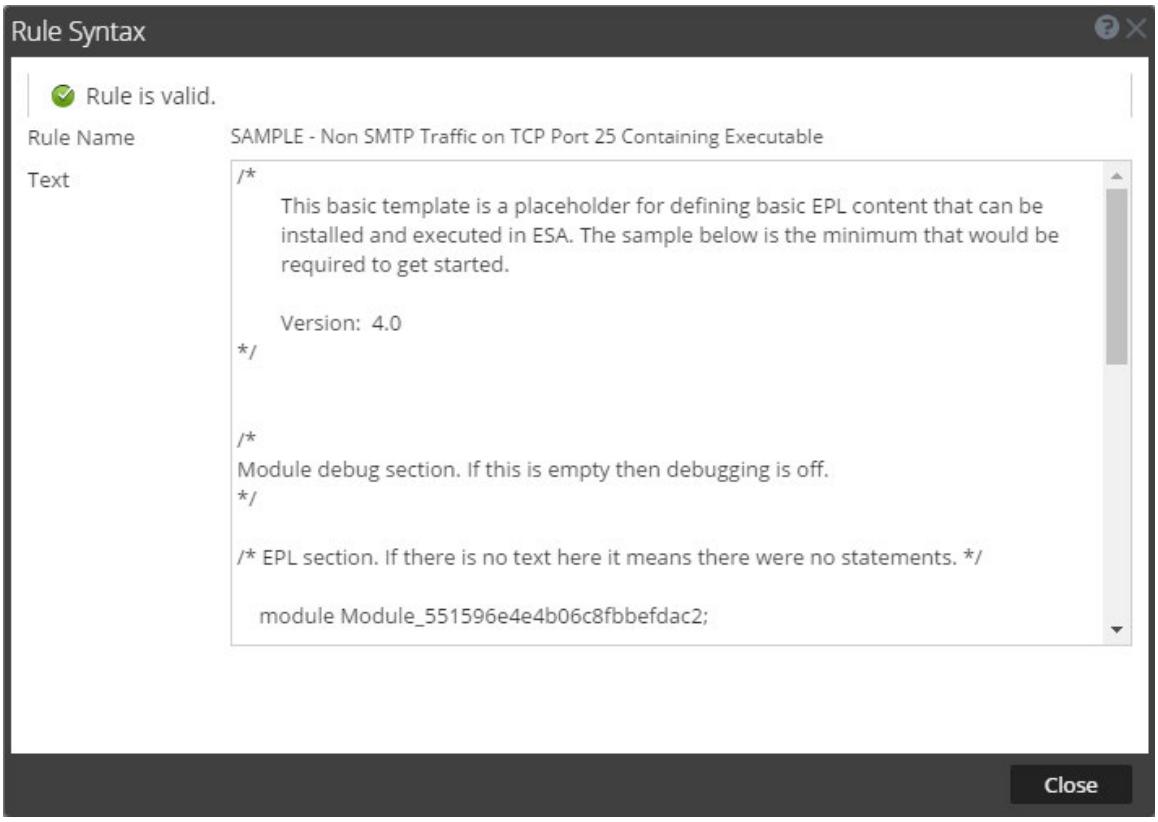
This topic describes the features of the Rule Syntax dialog. The Rule Syntax dialog displays the EPL syntax of conditions, statements, and debugging parameters, and provides a warning when the syntax is invalid.

Rule Syntax Dialog

To access this dialog:

1. Go to **CONFIGURE > ESA Rules**.
2. In the **Rule Library** view, do one of the following:
   a. Click + and select **Advanced EPL** or **Rule Builder**.
   b. Double-click an existing rule.
   c. Select an existing rule and click in the **Rule Library** toolbar.
   d. In the row of an existing rule, select > **Edit**.
   The new or existing rule is displayed in a new tab, available to edit.
3. Click **Show Syntax** at the bottom of the tab.

The following figure shows an example of the Rule Syntax dialog.



The following table describes the Rule Syntax dialog parameters.

Parameters	Description
Rule is valid or **Validation error in rule**	Indicates whether the rule syntax is valid or needs to be changed.
Rule Name	Displays the name of the rule.
Text	Displays the EPL syntax of conditions, statements, and debugging parameters if the rule is valid.

Services Tab

This topic provides an overview of the **CONFIGURE > ESA Rules > Services** tab. The Services tab provides details of the ESA services added to NetWitness Suite.

What do you want to do?

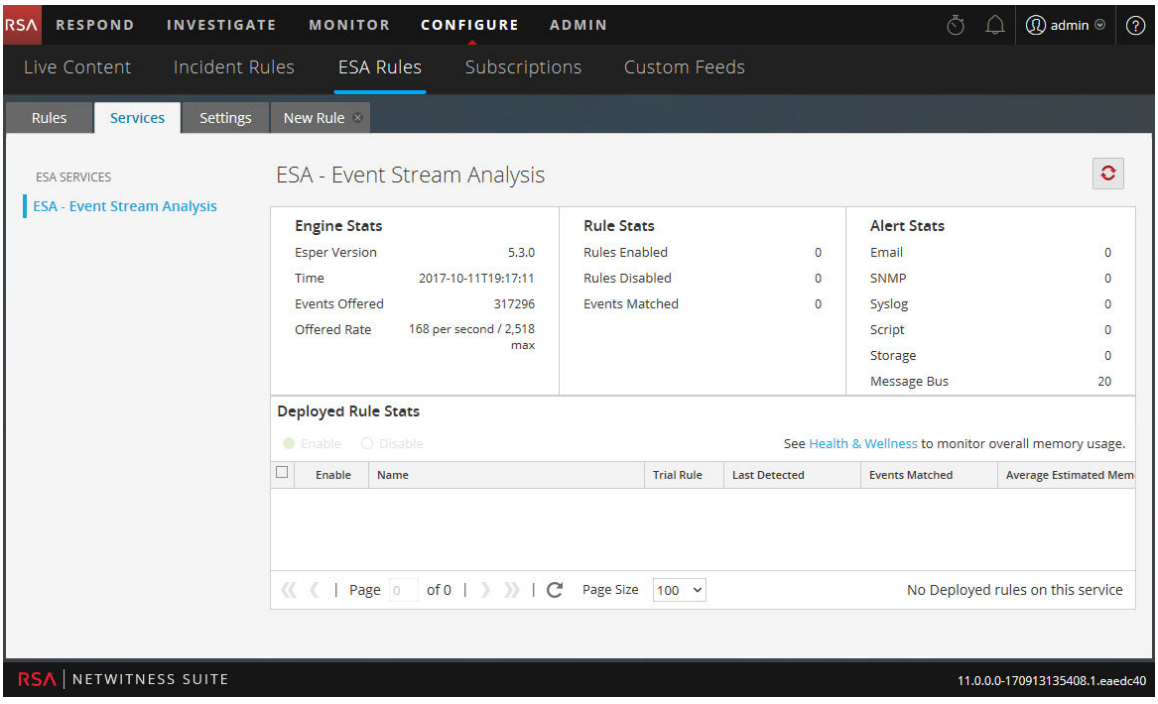
Role	I want to ...	Show me how
Content Expert	Troubleshoot Services Tab.	Troubleshoot ESA
Content Expert	View deployment Stats for an ESA Service.	View Stats for ESA Service

Related Topics

- View a Summary of Alerts

Services

The following figure shows the Services tab:



The Services tab has the following sections:

- ESA Services panel
- General Stats panel
- Deployed Rule Stats panel

ESA Services Panel

The ESA Services panel lists the name of each ESA service added to NetWitness Suite.

General Stats Panel

The General Stats panel provides information on the Esper engine, rules and alerts.

The General Stats panel contains the following sections:

- Engine Stats
- Rule Stats
- Alert Stats

The following figure shows the General Stats panel.

The table lists and describes the parameters in each section.

Sections	Parameter	Description
Engine Stats	Esper Version	Esper version running on the ESA service
	Time	Time when the last event was sent to Esper Engine
	Events Offered	Number of events analyzed by the ESA service since the last service start
	Offered Rate	Current events offered rate on the ESA service

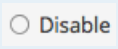
Sections	Parameter	Description
Rule Stats	Rules Enabled	Number of rules enabled.
	Rules Disabled	Number of the rules disabled
	Events Matched	Total number of events matched to all rules on the ESA service
Alert Stats	Email	Number of email notifications sent by the ESA service
	SNMP	Number of SNMP notifications sent by the ESA service
	Syslog	Number of Syslog notifications sent by the ESA service
	Script	Number of Script notifications sent by the ESA service
	Storage	Total number of alerts stored in database
	Message Bus	Total number of alerts sent to the message bus

Deployed Rule Stats Panel

The Deployed Rule Stats panel provides details on the rules that are deployed on the ESA service.

The following figure shows the Deployed Rule Stats panel.

The table lists the various parameters in the view and their description.

Parameters	Description
	Indicates the rule is enabled. Enables a rule that was disabled.
	Indicates the rule is disabled. Disables a rule that was enabled.
Health & Wellness	Displays a snapshot of memory usage when trial rules get disabled
Enable	Indicates whether the rule is enabled or disabled. Green icon indicates rule is enabled. White icon indicates rule is disabled.
Name	Name of the ESA rule.
Trial Rule	Indicates if the rule is running in trial rule mode.
Last Detected	The last time alert was triggered for the rule.
Events Matched	The total number of events that matched the rule.

Settings Tab

This topic describes the components of the **CONFIGURE > ESA Rules > Settings** tab. In the Settings tab, you can perform the following tasks:

- View a list of meta keys
- Configure a data enrichment source
- Add a connection to an external database

What do you want to do?

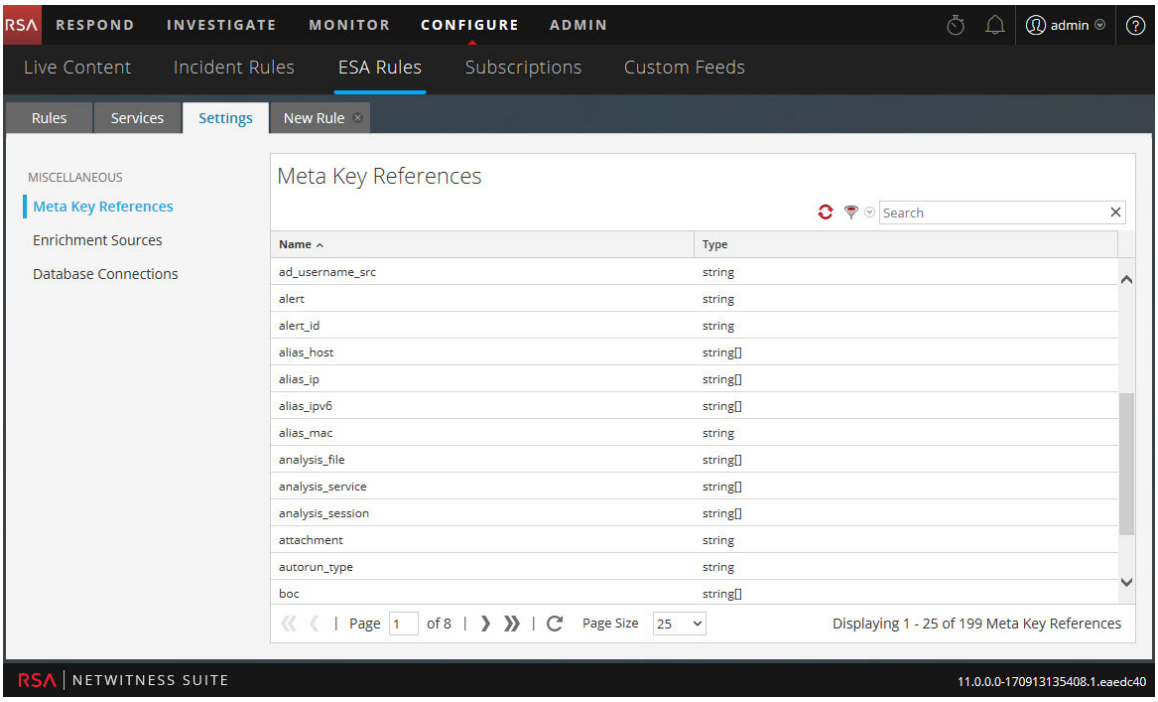
Role	I want to ...	Show me how
Content Expert	Configure a connection to an external database.	Configure a Database Connection
Content Expert	Configure a database as an enrichment source.	Enrichment Sources

Related Topics

- Add a Data Enrichment Source

Settings

The following figure shows the Meta Key References section in the Settings tab.



Meta Key References

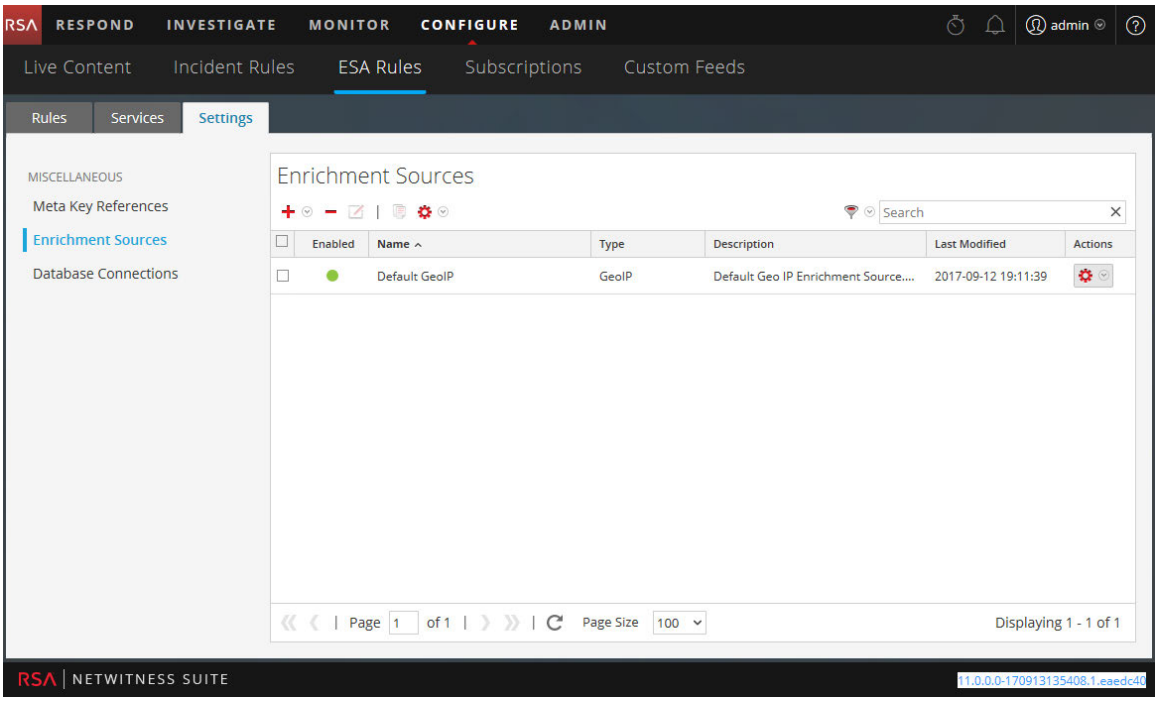
The Meta Key References section lists each meta key and the type of value the key requires.

Enrichment Sources

In the Enrichment Sources section, you can configure the following external data sources:

- GeoIP
- External Database Reference
- In-Memory Table
- Warehouse Analytics
- Context Hub List

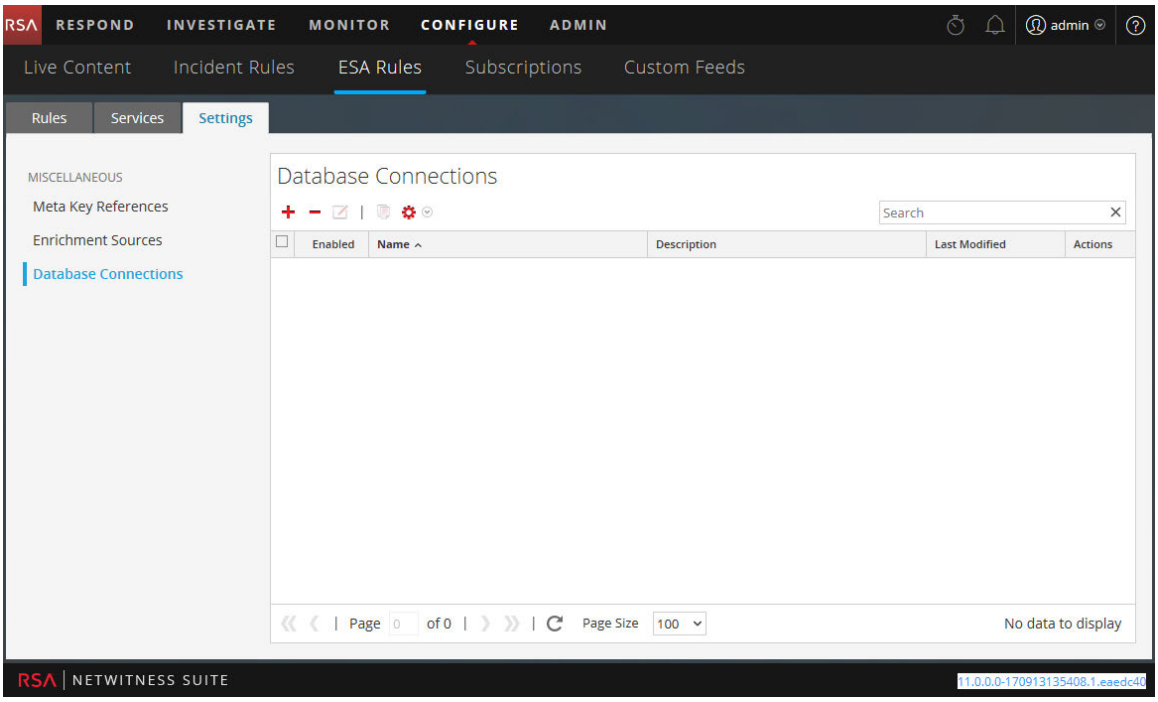
The following figure shows the Enrichment Sources section in the Settings tab.



Database Connections

In the Database Connections section, you can configure a connection to an external database so ESA can access that data.

The following figure shows the Database Connections section in the Settings tab.



In the Database Connections section you can perform the following:

- Add a Database Connection
- Delete a Database Connection
- Edit a Database Connection
- Duplicate a Database Connection
- Import a Database Connection
- Export a Database Connection

Updates to the Deployment Dialog

The Updates to the Deployment dialog displays changes to the deployment, such as adding a rule or service. Deployment updates are indicated by the update icon ( ) next to the name of the deployment in the Rules tab options panel.

What do you want to do?

Role	I want to ...	Show me how
Content Expert	Deploy rules to run on ESA.	Deployment Steps
Content Expert	Edit or delete a deployment.	Edit or Delete a Deployment
Content Expert	View deployment updates.	Show Updates to a Deployment

Related Topics

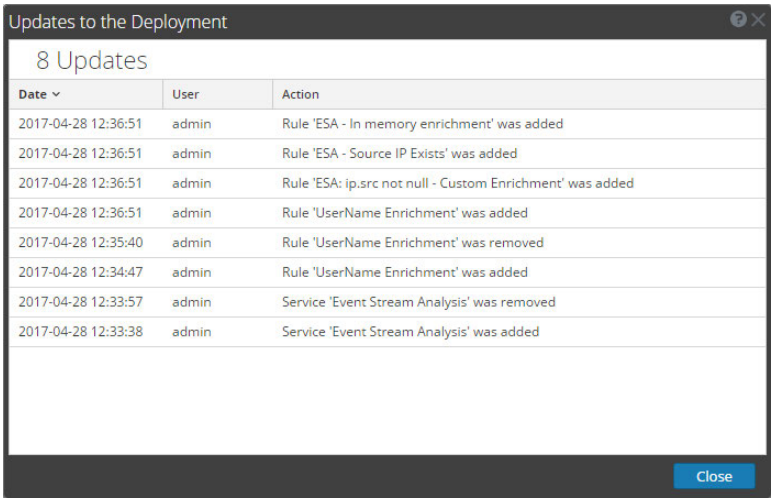
- Delete ESA Service in a Deployment
- Edit or Delete Rule in a Deployment

Deployment Dialog

To access this dialog:

1. Go to **CONFIGURE > ESA Rules**.
   The Rules tab opens by default.
2. In the options panel, under the **Deployments** section, select or add a deployment.
3. In the **Deployment** panel, click **Show Updates**.
   The Updates to the Deployment dialog is displayed.

The following figure is an example of this dialog.



The Updates to the Deployment dialog displays the number of updates at the top of the dialog. The following table describes the parameters of this dialog.

Parameters	Description
Date	Displays the day and time of the update.
User	Displays the user who made the update.
Action	Describes the update.

RSA NETWITNESS® SUITE

Event Source Management User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

About Event Source Management 7

Workflow 7
Automatic Mapping 8
Navigate to Event Source Management 8
How Alarms and Notifications Work 10
Large Email Notifications 11
High and Low Thresholds Both Triggered 11
Automatic Alerting 12
Common Scenarios for Monitoring Policies 13
Ordering the Groups 13
Managing Event Source Groups 15
Definitions 15
Manage Tab Details 15
Default Groups 15
Creating Event Source Groups 16
Procedure 16
Examples 17
Creating Event Source Group Form 19
Parameters 19
Rule Criteria 20
Acknowledging and Mapping Event Sources 22
Acknowledge Event Source Types 23
Manually Map Event Source Types 23
Viewing Logs from Pre-11.0 Log Decoder 24
Editing or Deleting Event Source Groups 24
Edit an Event Source Group 24
Delete an Event Source Group 24
Creating an Event Source and Editing Attributes 25
Mandatory Attributes 26
Create an Event Source 26
Update Attributes for an Event Source 27
Bulk Editing Event Source Attributes 27

Bulk Edit Attributes 27
Importing Event Sources 29
Import Event Source Attributes 29
Troubleshooting the Import File 31
Exporting Event Sources 31
Export Event Sources 32
Sorting Event Sources 33
Monitoring Policies 34
Configuring Event Source Group Alerts 34
Procedures 34
Setting Up Notifications 36
Prerequisites 36
Add Notifications for an event source group 37
Disabling Notifications 38
Prerequisites 39
Disable Notifications 39

Viewing Event Source Alarms 40

Sort the Alarms Information 40
Filter Alarms by Type 41

Configuring Automatic Alerting 42

Prerequisites 42

Event Source Management References 44

Discovery Tab 45
Toolbar and Features 48
Manage Tab 50
Groups Panel 51
Event Sources Panel 52
Sorting 54
Manage Event Source Tab 55
Workflow 55
What do you want to do? 56
Related Topics 56
Quick Look 57
Features 60
Event Sources View 62

Workflow 62
What do you want to do? 62
Related Topics 62
Quick Look 63
Create/Edit Group Form 65
Details View 67
Manage Parser Mappings 70
Advanced Configuration 72
Alarms Tab 73
Monitoring Policies Tab 76
Event Groups Panel 78
Thresholds Panel 78
Notifications Panel 79
Settings Tab 83
About Automatic Alerting 84
Features 86
Log Parser Rules Tab 88
Log Parsers List Panel 90
Details Panel 90
Rules Panel 93
Default Log Parser and Log Parser Rules 94
Default Log Parser 94
Highlight Matching Patterns 95

ESM Troubleshooting & Appendix 97

Alarms and Notifications Issues 97
Alarms 97
Notifications 97
Duplicate Log Messages 98
Details 98
Clean Up Duplicate Messages 99
Troubleshooting Feeds 99
Details 99
How it Works 99
Feed File 100
Troubleshooting Feeds 100
Import File Issues 106

Negative Policy Numbering 106
Details 106
Clean Up Duplicate Messages 107
Viewing Logs from Pre-11.0 Log Decoder 108

About Event Source Management

The Event Source module in NetWitness Suite provides an easy way to manage event sources and configure alerting policies for your event sources.

Workflow

This workflow shows the overall process for managing event sources, and configure monitoring for them. It also shows where configuring alarms and alerts settings are located in the process.

Prerequisites

There are two permissions that affect Event Source Management:

- **View Event Sources** is needed for users to view event sources, their attributes, and their thresholds and policies.
- **Modify Event Sources** allows users to add, edit, and otherwise update event sources.

For details, see the following topics:

- The *Roles Tab* topic available in the **System Security and User Management** guide > **References** > **Administration Security View** > **Roles Tab**.
- The *Role Permissions* topic describes the built-in NetWitness Suite system roles, which control access to the user interface. Available in the **System Security and User Management** guide > **How Role-Based Access Control Works**.
- The *Manage Users with Roles and Permissions* topic describes how to manage users in NetWitness Suite, using roles and permissions. Available in the **System Security and User Management** guide > **Manage Users with Roles and Permissions**.

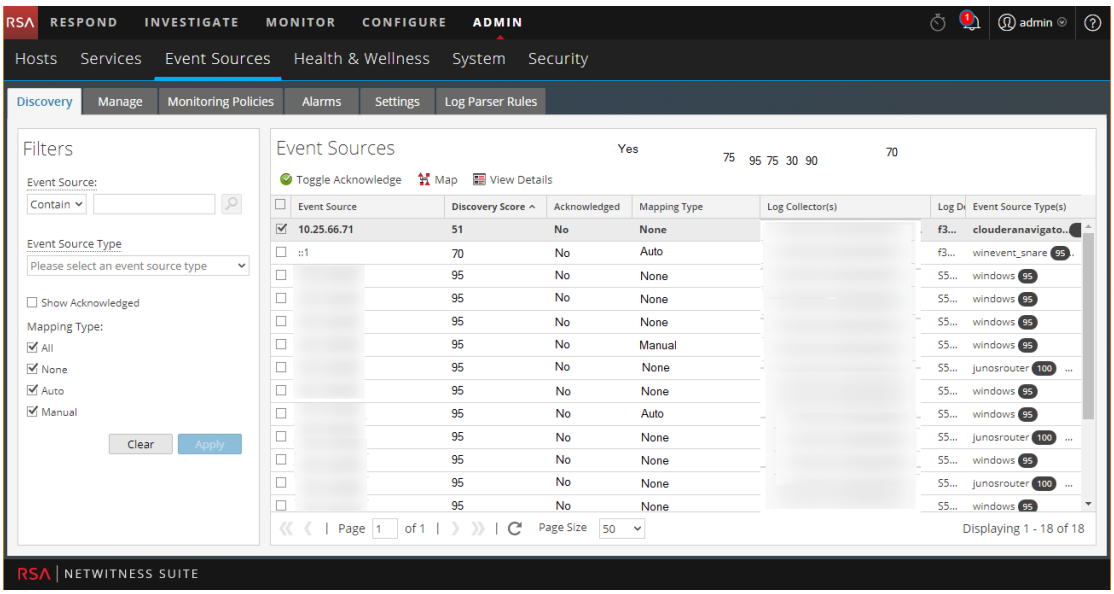
Automatic Mapping

Introduced in RSA NetWitness® Suite version 11.1, the system automatically maps incoming events to a type based on previous logs received from that address, reducing the mis-parsing of messages and reducing the number of items that need attention in the Discovery workflow. The UI indicates that an address has been auto-mapped in the Discovery workflow.

Navigate to Event Source Management

You can view the details about your existing event source groups by doing the following:

1. Go to **ADMIN> Event Sources**.



2. Click any of the following:

   - The **Discovery** tab. Use this tab to review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified completely accurately.
   - The **Manage** tab. This tab allows you to add, edit, and delete event source groups as well as viewing details for your existing event source groups.
   - The **Monitoring Policies** tab. Use this tab to view or edit your event source alerting configuration.
   - The **Alarms** tab. Use this tab to see the details of the alarms that have been generated. Alarms are generated when event sources exceed or fall below their set thresholds.
   - The **Settings** tab. Use this tab to view or change the behavior for automatic alerts.
   - The **Log Parser Rules** tab. Use this tab to view log parser rules as well as viewing how those rules will parse specified logs.

Note: When the system receives logs from an event source that does not currently exist in the Event Source List, NetWitness Suite automatically adds the event source to the list. Additionally, if it matches the criteria for any existing group, it becomes part of that group.

How Alarms and Notifications Work

The Event Source module in NetWitness Suite displays alarms and sends notifications based on alarms that are triggered.

For alarms, consider the following:

Alarms are of two types: **automatic** (triggered when baselines are exceeded or not met) and **manual** (configured using thresholds).

- **Automatic**: If you turn on automatic alerts, the system reports alarms for **all** event sources that go above or below their normal baselines by the required amount. You can specify the over / under percentage on the Settings Tab.
- **Manual**: The system alerts whenever an event source exceeds the thresholds in the policy for the associated groups.
- Alarms appear on the UI, in the Alarms Tab.

For notifications, consider the following:

- To receive manual notifications (via email, SNMP or Syslog):
  - Specify a policy for an event source group.
  - Set a high or low (or both) threshold.
  - Enable the policy.
- To receive automatic (baseline) notifications:
  - Baseline alerting must be on. This is turned on by default.
  - You must enable notifications from automatic monitoring. See Configuring Automatic Alerting for details.
  - The event source that triggers the alarm must be in a group that has a policy enabled.
- If you have automatic alerting turned on, and you have configured a policy and threshold for a group:
  - If the event source goes outside its baseline, you see an automatic alert and receive a notification.
  - If the event source goes outside its thresholds, you see a manual alert and receive a notification.
  - If both occur (threshold and baseline exceeded or not met), you receive two alarms (visible on the Alarms tab) and a notification that indicates both alarms. That notification will list

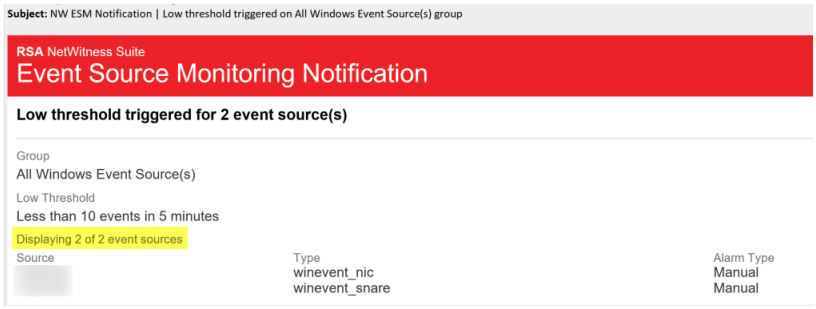
the event source that double alarmed twice; one listing indicating it was an automatic alarm.

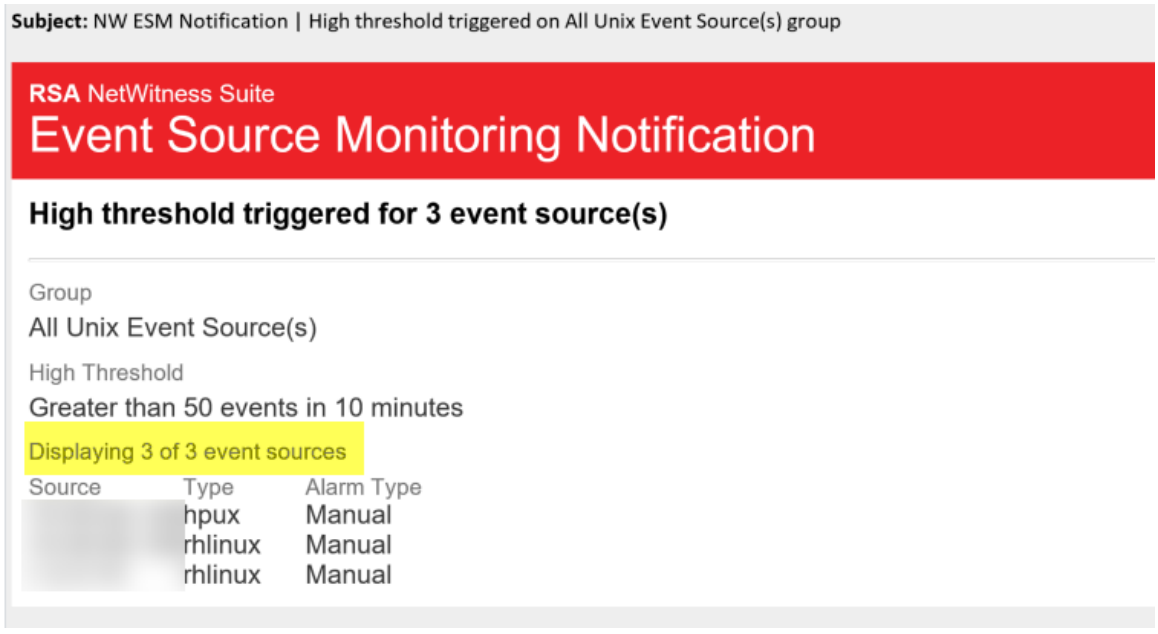
Large Email Notifications

If you have set up email notifications, keep in mind that the email can grow very large, depending on the number of event sources in the notification.

If the number of event sources in the alarmed state exceeds 10,000, then the email notification contains the details for only the first 10,000 and a total count. This is to ensure that the email is successfully delivered.

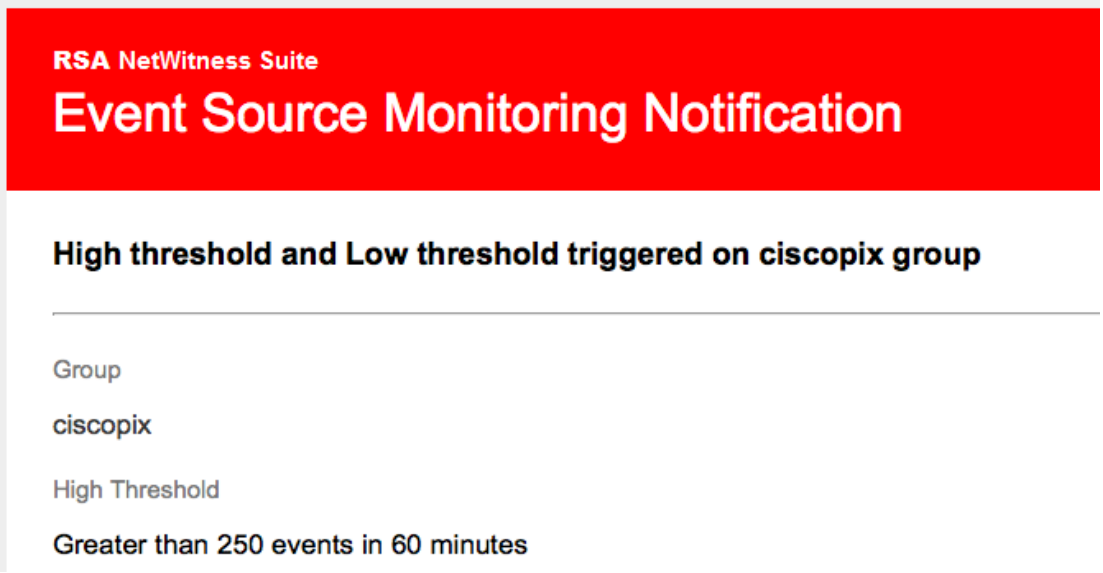
The following examples show a low threshold triggered for two event source groups and a high threshold triggered for three event source groups.





High and Low Thresholds Both Triggered

There may be occasions when both the high and low alarms are both triggered for a particular event source group. The easiest way to see when this happens is to read the email header, which clearly states when both thresholds are triggered, as shown in this image:



In this example, the header states, "High threshold and Low threshold triggered on ciscopix group." To see the details for the low threshold event sources, you may need to scroll down past hundreds, or even thousands, of the high threshold event sources.

Automatic Alerting

This topic describes automatic alerts, which are based on baseline settings.

Note: Automatic alerting, and all of the parameters that determine its behavior, are currently in Beta testing.

You can set up policies and thresholds for your event source groups. You do this so that you receive notifications when the thresholds are not met. NetWitness Suite also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

To trigger automatic alerts, you can use baseline values. This way, you do not need to set up numerous group thresholds and policies in order to receive alerts. Any anomalous amount of messages trigger alerts, without needing to do any configuration (except for turning on automatic alerting).

Note the following:

- Once you begin collecting messages from an event source, it takes the system approximately a week to store a baseline value for that event source. After this initial period, the system alerts you when the number of messages for a period are above or below the baseline by a set amount. By default, this amount is 2 standard deviations above or below the baseline.
- Base your high and low deviation settings on how "regular" your event sources behave. That is, if you expect little or no variance in the number of messages that arrive for a given time

(for example, 8 to 9 am on a weekday), then you can set a low value for the Deviation. Conversely, if you often see peaks and valleys, set the Deviation value higher.

- If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic alerting.

Common Scenarios for Monitoring Policies

Typically, organizations monitor their event sources in "buckets" based on how critical the event sources are. One typical example is as follows:

- There is a group of PCI devices, and it is critical to know if any of these devices stop sending messages (or send too few messages) within a half hour.
- There is a group of Windows devices, and it is useful to know if any of these devices stop sending messages after four hours.
- There is a group of quiet devices that do not typically send a lot of messages, but you would like to know if they do not send anything for 24 hours.

Many organizations may have a network that resembles this example. You may have more or different categories, but this example is used to discuss this feature.

You may have dozens or even hundreds of event source groups, and still only have a few groups for which you need to set thresholds and alerts.

Note: If an Event Source is a member of multiple groups that have alerting configured, it will only alert on the first matching group in the ordered list. (The Monitor Policies tab presents an ordered list of your groups.)

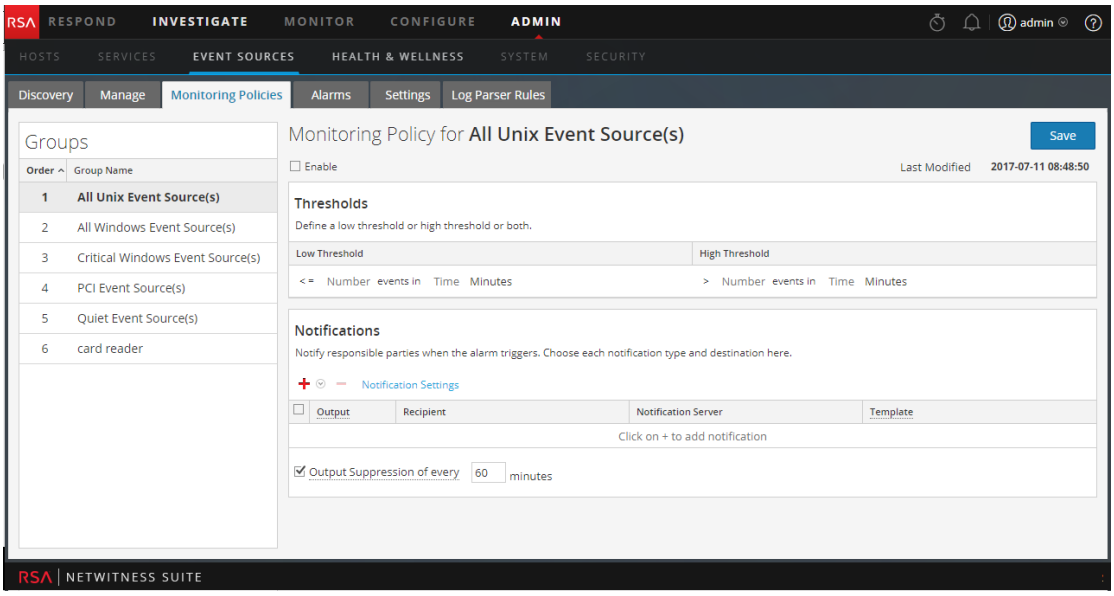
Ordering the Groups

Note: To change the order of the groups, drag and drop a group to its new location. The higher a group is listed, the higher the precedence for that group's thresholds: RSA NetWitness Suite checks the thresholds in the order provided in this panel. Thus, your highest priority groups should be at the top of this list.

The first thing to keep in mind is how to order your groups on the Monitoring Policies page. Assuming that you have the three groups mentioned above, you should order them as follows:

1. Quiet event sources. Having this group first ensures that you will not get numerous false alerts.
2. High priority PCI event sources. The highest priority devices should be after the quiet devices

3. Windows event sources. The time range is longer (four hours versus a half hour) for these devices than for the PCI devices. Therefore, they should come after the PCI devices.
4. All event sources. Optionally, you could set thresholds for all devices as a catch-all. This ensures that your entire network is operating as expected. For the catch-all group, you do not need to specify any thresholds—you can use automatic alerting to generate alarms for the event sources in this group.



In the figure above, note the following:

- The groups are ordered as discussed in the previous section.
- The threshold for PCI devices is to alert if the number of messages coming in to NetWitness Suite is fewer than 10 messages in 30 minutes.
- A low threshold is defined, but not a high threshold. This is typical for many use cases.

After you have set up and ordered your groups and begun to receive alerts, you may need to adjust the order. Use these guidelines to help you adjust the ordering:

- If you receive more notifications than you need, you can move the group down in the order. Similarly, if you are getting too few notifications, move the group up towards the top.
- If you notice that one event source is creating more alerts than it should, you can move it to another group, or create a new group for that event source.

Managing Event Source Groups

Definitions

When dealing with event source groups in NetWitness Suite, note the following:

- An **event source** is essentially the combination of values for all of its attributes.
- An **event source group** is the set of event sources that match a set of criteria that are defined for that group.

For example, you might have the following groups:

- A group named **Windows Devices**, consisting of all the event source types associated with Microsoft Windows event sources (`winevent_nic`, `winevent_er`, and `winevent_snare`).
- A group named **Low Priority Services**, consisting of all services where the Priority attribute has been set lower than 5.
- A group named **U.S. Sales Servers**, where you gather event sources located in the U.S.A. and having an Organization attribute of Sales, Finance, or Marketing.

Manage Tab Details

The Manage tab in the Event Source module provides an easy way to manage event sources. In this tab, you can:

- Set up event source groups in a consistent way.
- Work with event source attributes in a consistent, straightforward manner.
- Easily search through your entire set of event sources.
- Bulk edit and update your event sources and event source groups.

You can view the details about your event source groups by doing the following:

1. Go to **ADMIN** > **Event Sources**.
2. Select the **Manage** panel to see the details for your existing event source groups.

Note: When the system receives logs from an event source that does not currently exist in the Event Source List, NetWitness Suite automatically adds the event source to the list. Additionally, if it matches the criteria for any existing groups, it becomes part of that group.

Default Groups

RSA NetWitness Suite has several default groups. You can customize these as required and use them as templates for creating new groups.

The default groups are as follows:

- All Event Sources
- All Unix Event Sources
- All Windows Event Sources
- Critical Windows Event Sources
- PCI Event Sources
- Quiet Event Sources

You can edit any of these groups to investigate the rules that define the groups.

Note: You cannot edit or delete the **All** event source group.

Creating Event Source Groups

Administrators must receive notifications when event sources are no longer being collected by NetWitness Suite. They need to be able to configure how long the event sources can be quiet (that is, not collect any log messages) before sending a notification based on different factors.

RSA NetWitness Suite provides event source groups so that you can group similarly important devices together. You can create groups based on attributes that you imported from your CMDB (configuration management database), or by manually choosing event sources to add to the group.

For example, these are some of the types of event source groups that you can create:

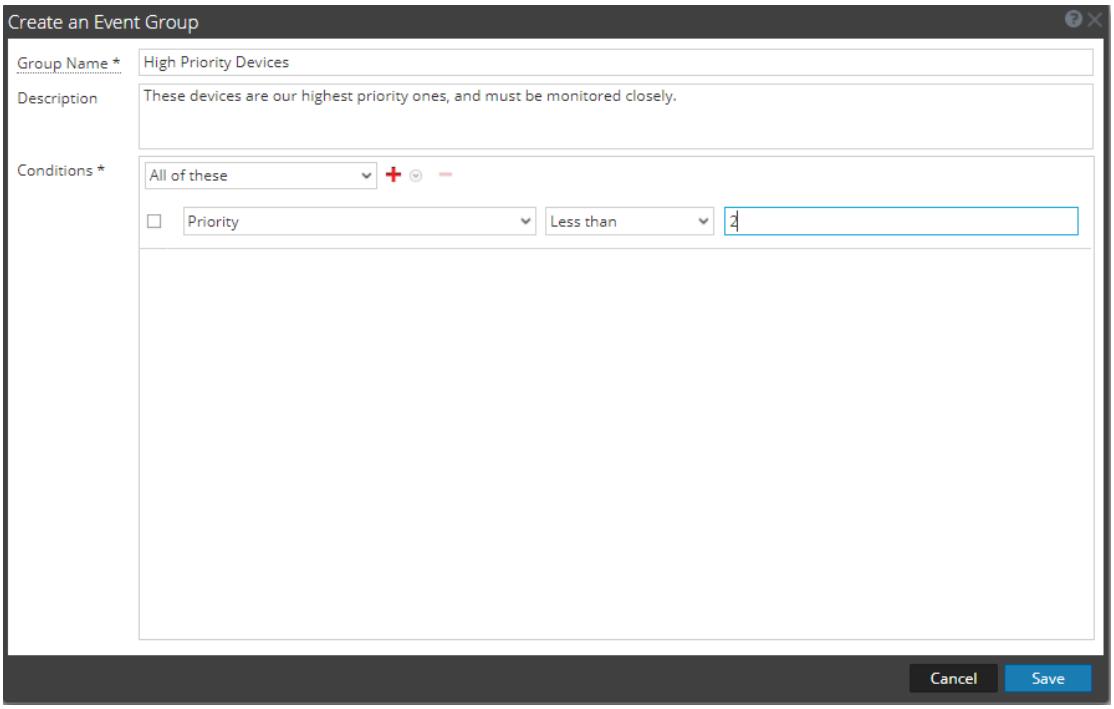
- PCI sources
- Windows Domain Controllers
- Quiet sources
- Finance Servers
- High Priority devices
- All Windows sources

Procedure

To create an Event Source group:

1. Go to **ADMIN** > **Event Sources**.
2. In the **Manage** panel, click .

   The Create an Event Group dialog is displayed.



3. Enter a Group Name.
4. Enter a Description.
5. Click + to add a condition. Continue adding conditions as necessary. For details on constructing conditions, see Create/Edit Group Form.
6. Click **Save**.

   The new group is listed in the **Manage** panel.

Examples

This section describes a simple example, and then discusses how to set up a more complex set of rules.

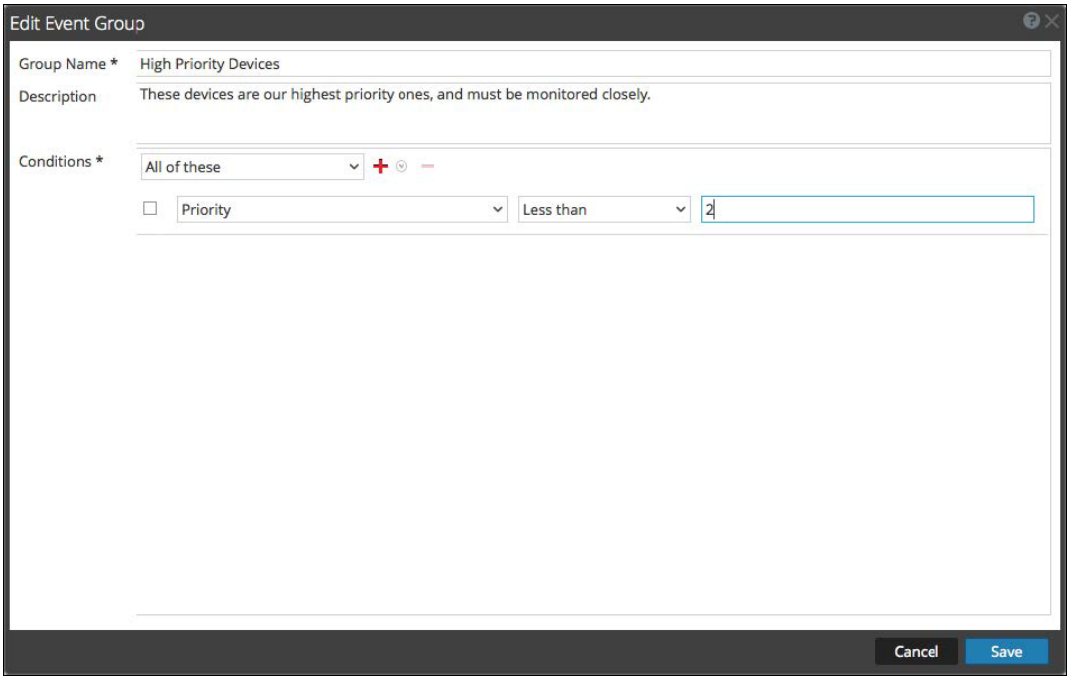
Simple Example

If you want to create an event source group that contains all of your high priority event sources, this example describes the necessary steps.

1. Go to **ADMIN > Event Sources**.
2. In the **Manage > Groups** panel, click + .
3. Enter **High Priority Devices** for the Group Name.
4. Enter a description, such as, "These devices are our highest priority ones, and must be monitored closely."

5. Leave **All of these** selected and click + to add a condition.
6. Select **Add condition** from the drop-down menu.
   a. Select an Attribute: **Priority**.
   b. Select an Operator: **Less than**.
   c. Enter a value: **2**.

   The following figure displays the updated Edit Event Group dialog.



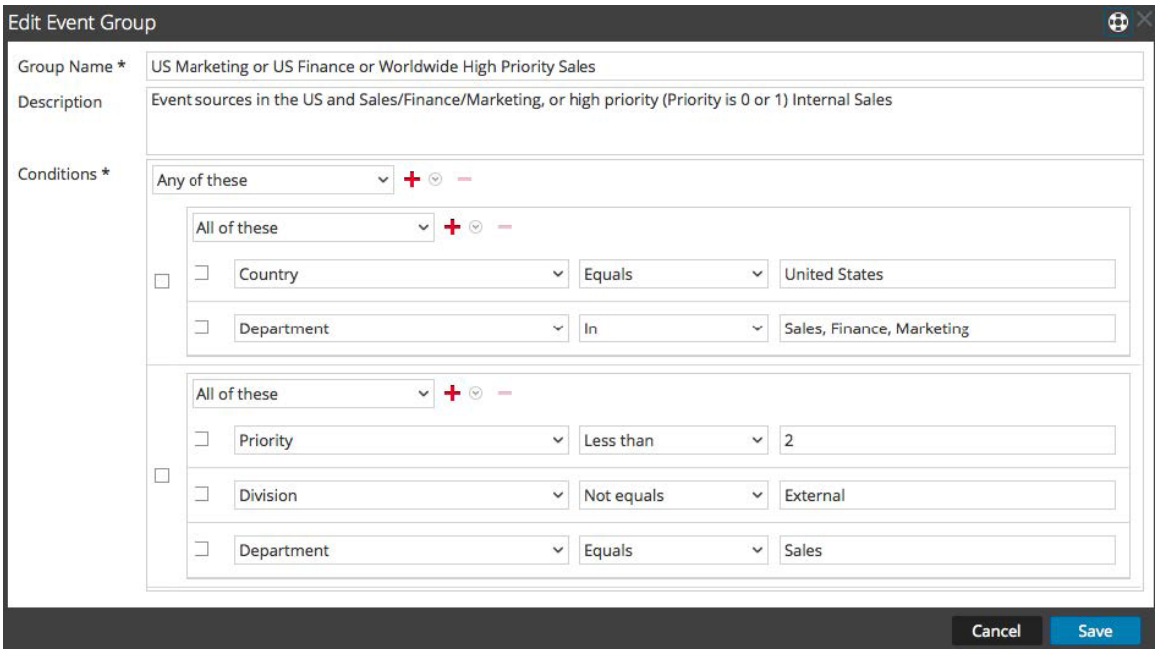
7. Click **Save**.

Complex Example

In this example, you want to create a fairly complex rule: match event sources that are in the United States, and in either the Sales, Finance, or Marketing departments. Also, match worldwide internal, high priority Sales event sources. High Priority is assumed to be where the priority is 1 or 0. Logically, the definition is as follows:

```
(Country=United States AND (Dept.=Sales OR Dept.=Finance OR
Dept.=Marketing))
 OR
 (Priority < 2 AND Division != External AND Dept.=Sales)
```

The following figure is an example of the criteria for creating such an Event Source Group.



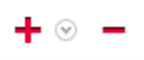
Creating Event Source Group Form

The Create Event Source Group form is displayed when you are creating or editing an Event Source Group.

Parameters

The following table describes the fields on the Create/Edit an Event Group form.

Field	Description
Group Name	This field is required, and appears throughout the NetWitness Suite UI as the identifier for the group.
Description	An optional description to help describe the purpose or details for the group.

Field	Description
Tools 	The following items are available on the toolbar: • **Add (+)**: clicking the **Add** displays a menu where you can choose to add a condition or a group. • **Remove (−)**: removes the selected rule or group of rules from the list. When you add a new group, that has the effect of creating nested levels of conditions.
Conditions	Described below, in the **Rule Criteria** table.
Cancel / Save	**Cancel** and **Save** options are available in the form.

Rule Criteria

The rules that you specify determine the event sources that will become part of this event source group. A rule consists of the following:

- Grouping: how the rule interacts with other rules
- Attribute: which attribute the rule is matching against
- Operator: how the rule matches the attribute
- Value: the attribute value used for the rule

The following table provides details on these rule constructors.

Rule Constructor	Details
Grouping	You can group conditions, in order to create complex rules for an event source group. The following choices are available when grouping your rules: • **All of these**: logically equivalent to AND • **Any of these**: logically equivalent to OR • **None of these**: logically equivalent to NOT If you are creating a simple group, and specifying a single condition, you can leave the default value (**All of these**) selected.
Attribute	This contains a drop-down list, consisting of all event source attributes. The attributes are displayed by the section to which they belong. For example, all of the **Identification** attributes are displayed first, followed by the **Properties**, **Importance**, and so on.

Rule Constructor	Details

Operator	Choose from the following options:
	• **Equals**: matches the provided value
	• **Not equals**: returns event sources whose specified attribute not equal to the provided value
	• **In**: provide a list of values in comma separated format, and event sources that match any of the provided values are included. For example:
	`Where IP in 10.25.50.146, 10.25.50.248`
	This condition returns event sources that have either `10.25.50.146 or 10.25.50.248` as their IP attribute.
	• **Not in**: similar to **In**, except that it matches items whose attribute is not equal to any of the listed values.
	• **Like**: matches items that begin with the provided string. For example:
	`Where Event Source Type Like Apache`
	This condition returns event sources whose Event Source Type begins with `Apache`.
	• **Not like**: similar to **Like**, except that it matches items whose attribute does not begin with the provided string.
	• **Greater than**: matches items whose attribute is greater than the provided value. For example, if you specify Priority Greater than 5, the condition would match any item with a priority of 6 or higher.
	• **Less than**: similar to **Greater than**. Matches items whose attribute is less than the provided value.

Value	Enter a value or group of values. The value type depends on the attribute for the condition. For example, for IPv6, you need to specify a value in IPv6 format.

Acknowledging and Mapping Event Sources

In RSA NetWitness® Suite version 11.1, RSA introduced Automatic Mapping. The system automatically maps incoming events to a type based on previous logs received from that address, reducing the number of items that need attention in the Discovery workflow. The UI indicates that an address has been auto-mapped in the Discovery workflow.

Acknowledge Event Source Types

The Discovery tab lets you review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified accurately. If the discovered event source types are correct, you can acknowledge to filter out that event source from the view by default. If incorrect, you can set the allowed event source types for a particular address so that future logs will parse against the correct parsers.

To acknowledge event sources:

1. Go to **ADMIN > Event Sources**.

   The Discovery tab is displayed.

2. Select one or more event sources.
3. Click **Toggle Acknowledge**.

Note the following:

- Once Event Sources are Acknowledged, they are no longer displayed in the Event Source Type(s) column.
- The **Toggle Acknowledge** button behaves as follows:
  - If the Acknowledged state for all of the selected event sources is the same, all values are toggled. That is, if you select only event sources with **Yes** in Acknowledged column, the value changes to **No** for all of them. Similarly if they all have **No** in the Acknowledged column, the value changes to **Yes** for all selected event sources.
  - If you select a multiple event sources, and the value for some is **Yes** and for other it is **No**, when you click **Toggle Acknowledge**, all of the values are set to **Yes** for the selected event sources.

Note: Acknowledged Event Sources are not displayed by default.

Manually Map Event Source Types

When discovered event source types are not completely accurate, you can manually map the parsers to obtain additional information.

To map one or more event sources:

1. Go to **ADMIN > Event Sources**.

   The Discovery tab is displayed.

2. Select one or more event sources.

3. Click Map .

   The Manage Parser Mappings dialog box is displayed.

4. Add or remove parser mappings, and change the priority order, based on the needs of your organization. For more details, see Manage Parser Mappings .

Note: Discovery scores for the mapped Event Sources are listed in the Event Source Type(s) column from the lowest to highest discovery scores. Discovery scores range from 0 (least confident) to 100 (most confident).

Viewing Logs from Pre-11.0 Log Decoder

RSA NetWitness® Suite 11.0 added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available. For more details, see Viewing Logs from Pre-11.0 Log Decoder.

Editing or Deleting Event Source Groups

You may occasionally need to remove an event source group. For example, if you close an office, and you had a group consisting of all the event sources in that office, you can remove the group, since none of those event sources will send information to NetWitness Suite.

Similarly, you may need to change some of the conditions that are used to populate the group.

Note: You cannot edit the event source group name. Once you create a group, that name exists as long as the group itself exists.

Edit an Event Source Group

1. Go to **ADMIN > Event Sources**.
2. In the **Manage** panel, select an existing Event Source Group.
3. Click .

   The Edit Event Group dialog is displayed.

4. Modify any of the details, or add, edit or remove conditions as necessary.
5. Click **Save**.

Delete an Event Source Group

Note the following:

- You can delete any group except for the **All** group, which lists all configured event sources in the system.
- If you delete a group, the associated policy for that group also gets deleted automatically.
- If there are any event sources that belong **only** to the deleted group, they would no longer have a policy alarm associated with them. Remember that event sources can belong to multiple groups.
- Deleting a group has no effect on baseline alarms.

To delete an event source group:

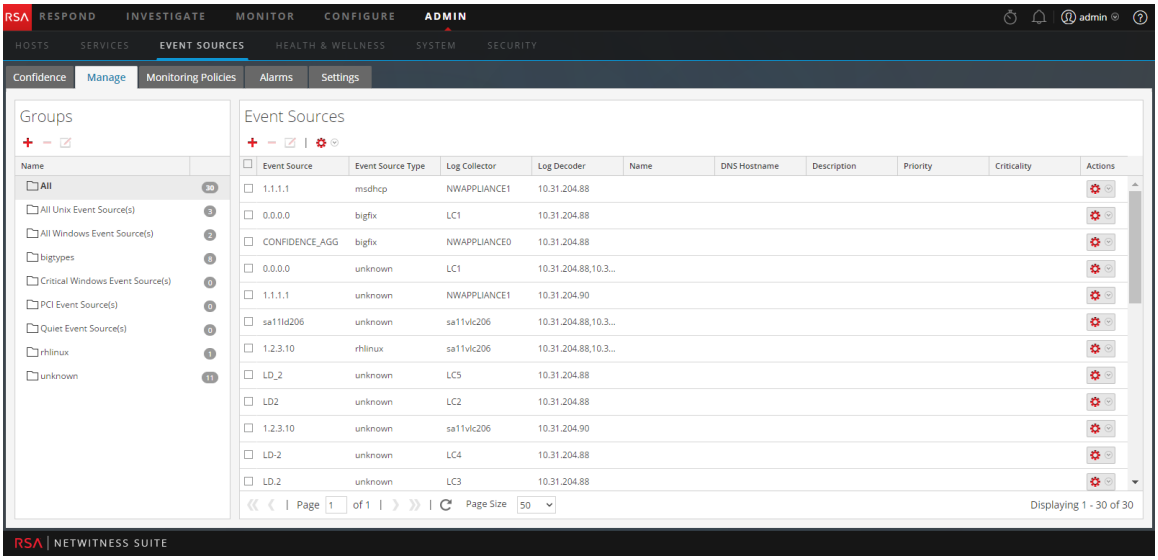
1. Go to **ADMIN > Event Sources**.
2. In the **Manage** panel, select an existing Event Source Group.
3. Click − .

   A confirmation dialog is displayed.
4. Click **Yes** to delete the group.

Creating an Event Source and Editing Attributes

You can organize your event sources into groups. You do this by entering values for various attributes for each event source. For example, for all of your high priority event sources, you could set the **Priority** to 1. You can see details about the available attributes on the Manage Event Source Tab.

The following figure shows an example of the Event Sources panel:



Event source attributes are a combination of auto-populated and user-entered information. When an event source sends log information to NetWitness Suite, it is added to the list of event sources, and some basic information is auto-populated. At any time after that, users can add or edit details for other event source attributes.

Mandatory Attributes

The following identification attributes are handled specially: **IP**, **IPv6**, **Hostname**, **Event Source Type**, **Log Collector**, and **Log Decoder**. If you create an event source manually, you can enter these values. Once you save the event source, these values can no longer be changed.

Event sources can also be auto-discovered; any event source that sends messages to the Log Decoder will be added to the list of event sources. If you edit the attributes for an auto-discovered event source, you cannot edit any of these fields.

Note that not all of these fields are mandatory. To uniquely identify an event source, the following information is required:

- IP or IPv6 or Hostname, and
- Event Source Type

Additionally, RSA NetWitness Suite uses a hierarchy for IP, IPv6, and Hostname. The order is as follows:

1. IP
2. IPv6
3. Hostname

If you enter event sources manually, then you need to keep this order in mind, otherwise, you may end up with duplicates when messages are received from the event sources that you manually added.

All other attributes (such as Priority, Country, Company, Vendor, and so on) are optional.

Create an Event Source

1. Go to **ADMIN > Event Sources**.
2. Select the **Manage** tab.
3. In the **Event Sources** panel, click to open the details screen, which contains all of the event source attributes.

   The Manage Event Source Tab is displayed.
4. Enter or change the values for any attributes.
5. Click **Save**.

Update Attributes for an Event Source

1. Go to **ADMIN> Event Sources**.
2. Select the **Manage** tab.
3. In the **Event Sources** panel, select an event source from the list.
4. In the **Event Sources** panel, click to open the details screen, which contains all of the event source attributes.

   The Manage Event Source Tab is displayed.
5. Enter or change the values for any attributes, except for certain attributes that cannot be altered once entered.
6. Click **Save**

Bulk Editing Event Source Attributes

You can select multiple event sources, or an entire group, or even all event sources for bulk editing. For example, you might want to change the Priority or the Manager for a large number of your event sources.

Note: You cannot select individual event sources across displayed pages. For example, if you have a group with 225 event sources, and your Page Size is 50, you can only select event sources from the currently displayed 50 items.

If you want to edit items that span multiple pages, you can do the following:

- In the browser, increase the page size (the maximum is 500 entries on a single page). If your page size is small, you might be able to get all of your items on a single page.
- Create a new event source group that contains only the items that you want to bulk edit. Then, you can select all items for that group, rather than selecting individual items.
- Bulk edit incrementally. On the first page, select the items that you want to edit. Make your edits, then go to the next page and repeat the process, until you have made all of your changes.

Bulk Edit Attributes

Note: Mandatory fields cannot be edited; IP, IPv6, Hostname, Event Source Type, Log Collector, and Log Decoder.

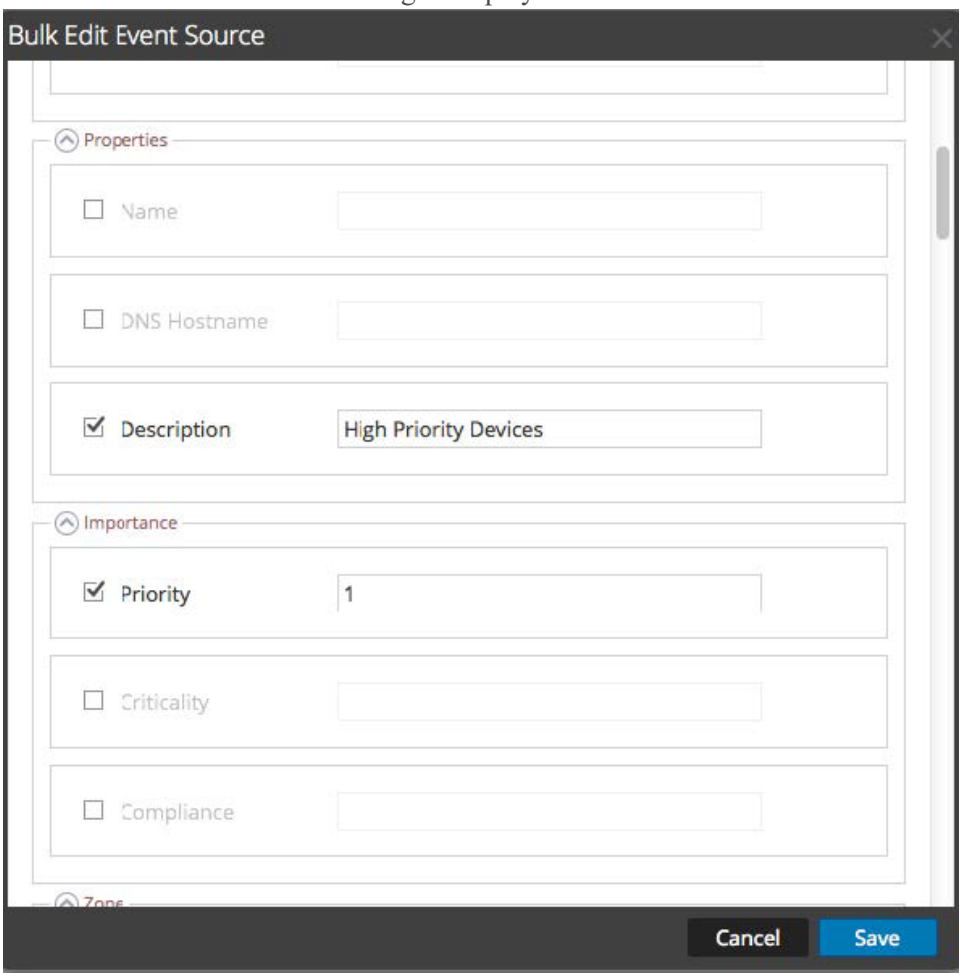
To bulk edit attributes for Event Sources:

1. Go to **ADMIN > Event Sources**.
2. Select the **Manage** tab.
3. Optionally, select an event source group.
4. In the **Event Sources** panel, select one or more event sources to edit.

   Note: To select all event sources, select the box next to the **Actions** column in the last (far-right) column of the list table.

5. Select the **Edit** icon from the menu bar.

   The Bulk Edit Event Source dialog is displayed.



6. Enter values for any of the available attributes. In the screen shot above, the Name and Priority attributes have been updated.
7. When you have updated as many attributes as required, click **Save**.

Importing Event Sources

You can import event source attributes from a CSV-formatted file. To import information from a configuration management database (CMDB), a spreadsheet, or other type of file, first convert or save the information to a CSV file.

Note: The following identification attributes are handled specially: **IP**, **IPv6**, **Hostname**, **Event Source Type**, **Log Collector**, and **Log Decoder**. If you import an event source that includes a different value for any of these fields (when compared with the value in NetWitness Suite), the original value in NetWitness Suite will **not** be overwritten.

The imported attributes are associated with the matched Event Source and are available for use in rules to create Event Source Groups.

RSA NetWitness Suite treats the import file as the correct, complete record. This assumption leads to the following behaviors related to importing event source attributes:

- By default, when you import attributes, the system updates attributes for existing event sources only.
- If the event source exists in the import file, but not in NetWitness Suite, the attributes for that event source are ignored. That is, NetWitness Suite does **not** create a new event source for these attributes.
- If the event source exists in both the import file and NetWitness Suite, values for that event source are overwritten.
- If an attribute is blank in the import file, it clears the corresponding attribute in NetWitness Suite.
- If an attribute is not specified in the import file, then the corresponding attribute is ignored in NetWitness Suite (that is, it is **not** cleared).

Note: There is a difference between a blank attribute vs. one that is not specified at all. If an attribute is specified but blank, the assumption is that it is meant to be blank, and NetWitness Suite clears that attribute for the corresponding event source. However, if an attribute is not specified at all, it is assumed that no change is expected.

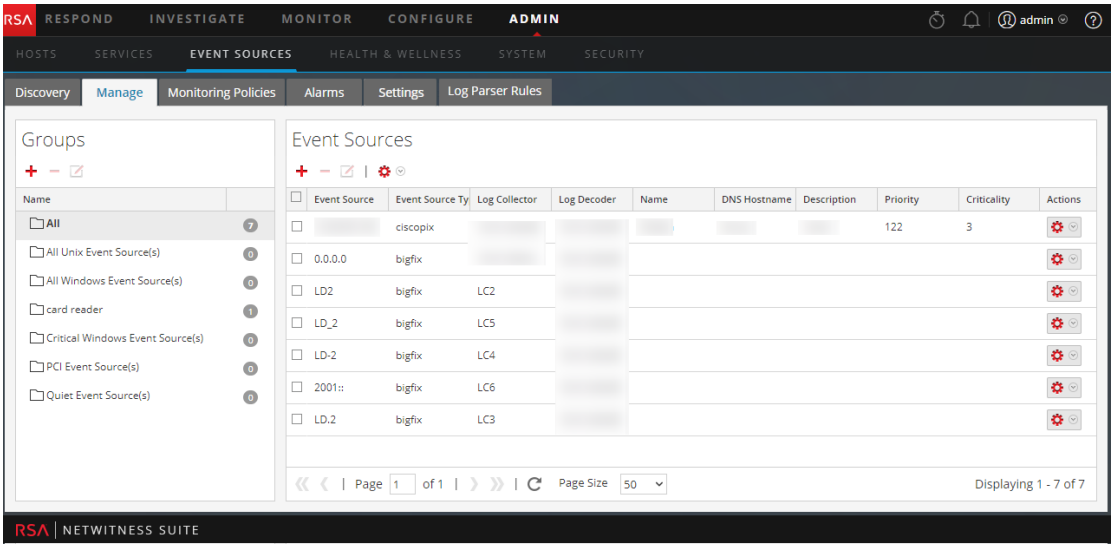
The above behaviors are the defaults—you can change the behavior as specified in the following procedure.

Import Event Source Attributes

To import Event Source attributes from a file:

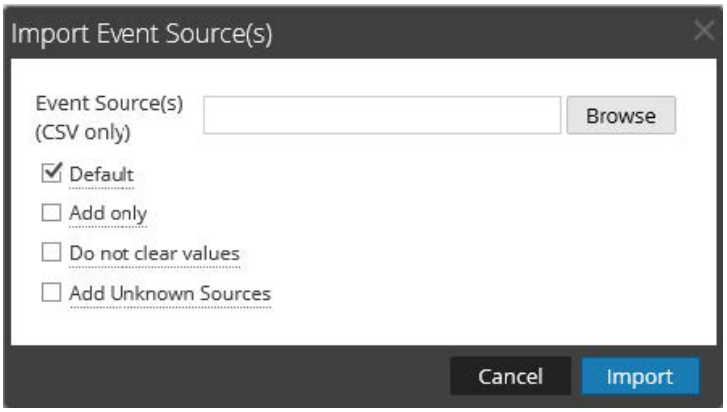
1. Go to **ADMIN > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.



3. From the Import/Export menu in the toolbar ( ), select **Import** (Import).

   The Import Event Sources dialog is displayed.



4. Navigate to the import file, and select the appropriate boxes:
   - **Default**: The default behavior is described above.
   - **Add only**: Imports an attribute only if the corresponding field in NetWitness Suite is blank. Thus, no existing values will be overwritten.
   - **Do not clear values**: Does not clear attribute values in NetWitness Suite for items in the

import file that are blank.

- **Add Unknown Sources**: Adds new event sources based on items in the import file.

  Note: You can select multiple options.

5. Click **Import**.
6. Click **Yes** in the confirmation dialog to perform the import.

Troubleshooting the Import File

If your import file is not formatted correctly, or is missing required information, an error is displayed, and the file is not imported.

Check the following:

- If you are adding unknown sources, each line in the file must contain a combination of the required attributes:
  - IP or IPv6 or Hostname, and
  - Event Source Type
- The first line of the file must contain header names, and the names must match the names in NetWitness Suite. To get a list of correct column names, you can export a single event source. Examine the exported CSV file: the first row of the file contains the correct set of attribute/column names.

If your import file is not formatted correctly, or is missing required information, an error is displayed, and the file is not imported.

Exporting Event Sources

You can export all or some of your event sources, along with their corresponding attributes, to a CSV file.

Note the following:

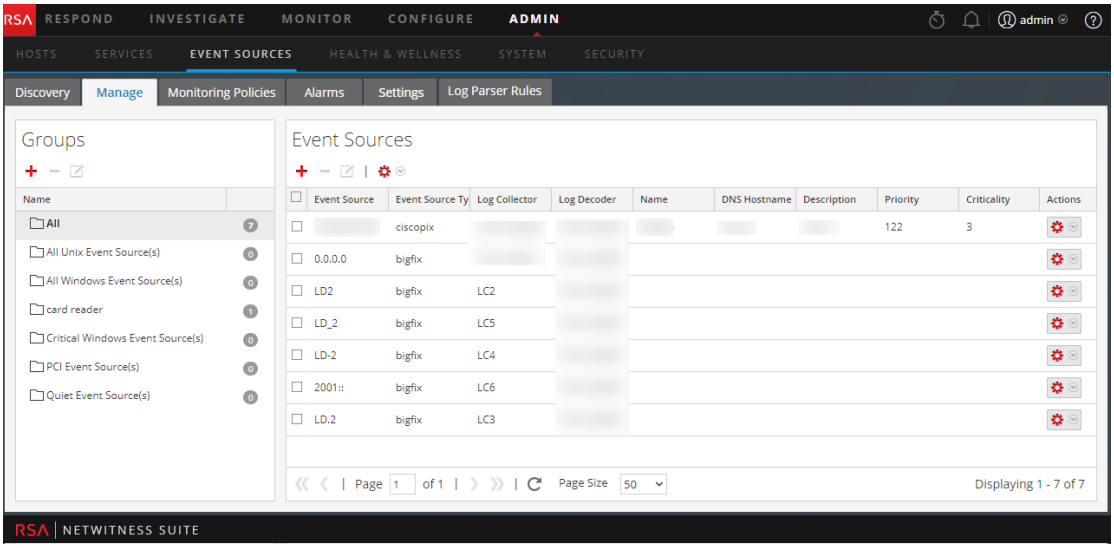
- The exported CSV includes all attribute columns.
- The exported CSV includes a header line at the top, listing each column name.
- You can export all entries in a group.
- You can export all entries (select the **All** group).
- You can select entries and export only those entries.

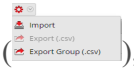
Export Event Sources

To export your Event Sources:

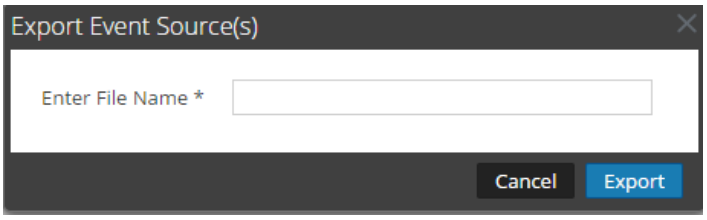
1. Go to **ADMIN > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.



3. Select the group that contains the event sources to export.
4. Select as many event sources as you need. Alternatively, you can export the entire group: to export the entire group, you do not need to select any individual event sources.
5. From the Import/Export menu in the toolbar (), select **Export (.csv)** or **Export Group (.csv)**.

   The Export Event Sources dialog is displayed.



6. Enter a file name and click export.ddd

The event source attributes are saved to the file name you specified, in a CSV format.

Sorting Event Sources

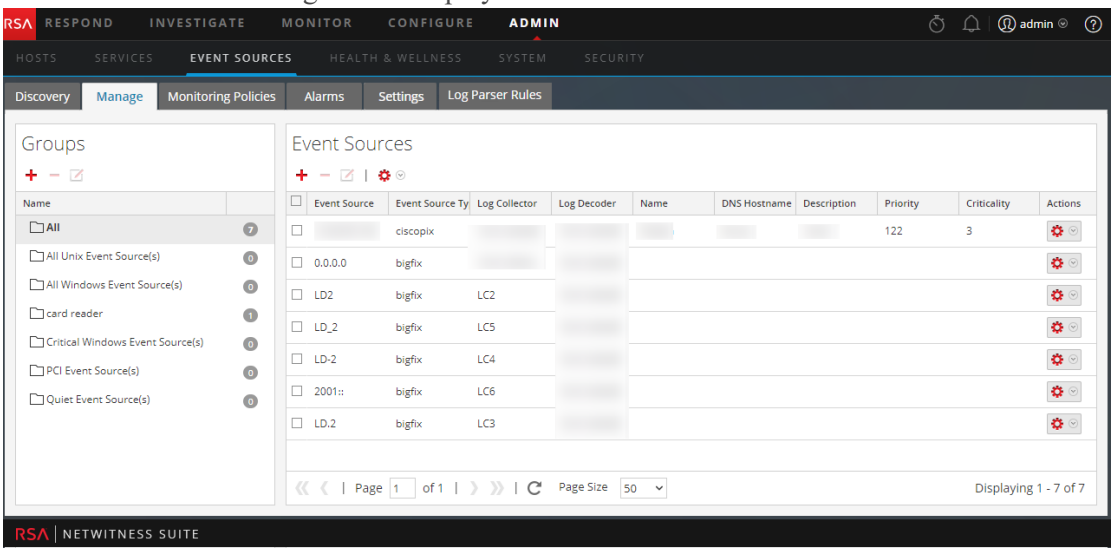
The event sources panel displays attributes for the currently selected event source group. You can configure the list of attributes that are displayed, as well as sort the list on any of the displayed attributes.

Note: The entire list is sorted, not just the items displayed on the current page. (The navigation bar at the bottom of the page shows how many pages exist for this list of event sources.)

To sort your event sources:

1. Go to **ADMIN > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.



3. To sort a column, click + in the column header.

   The Sort Options drop-down menu is displayed.

4. Select the sort order that you want.

Monitoring Policies

Use the Monitoring Policies view to manage alert configuration for your event source groups.

You can create policies that alert on event source groups, by setting thresholds and notifications:

- Thresholds set ranges for frequency of log messages. You can specify a low threshold, a high threshold, or both.
- Notifications describe how and where to send alerts when thresholds are not met.
- You combine thresholds and notifications to create alerts based on the frequency you specify.
- If automatic alerting is enabled (it is by default), you can create and enable a policy ***without*** setting any thresholds. If you then turn on automatic notifications, notifications will be sent whenever an event source in the group is above or below its baseline by the specified amount.

For example, let's say that you have created an event source group that consists of all your Windows event sources based in the United Kingdom. You could specify a policy that alerts you whenever fewer than 1000 events per 30 minutes arrive.

Note: In addition to, or instead of setting up monitoring policies for your event source groups, you can Configuring Automatic Alerting to view alarms when the number of messages for an event source are outside of the normal bounds.

Configuring Event Source Group Alerts

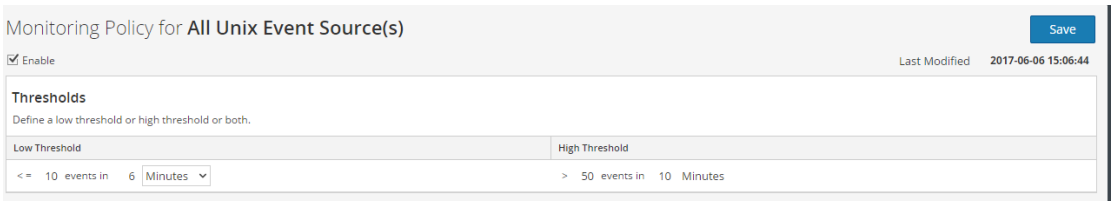
Each event source group can have its own alerting policy. This includes setting the thresholds for when to alert, and setting the notification type when an alert is triggered. This topic describes the steps involved in creating an alert policy for an event source group.

Procedures

Create an Alert Policy for an Event Source Group

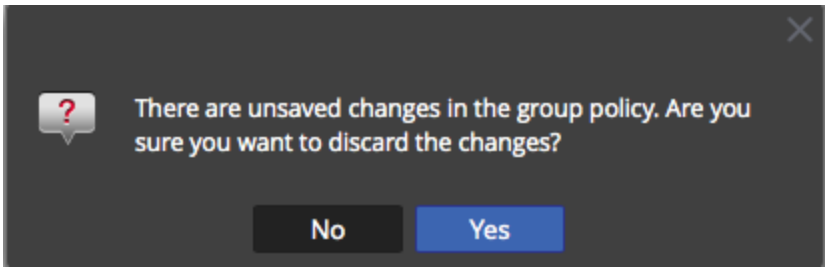
1. Go to **ADMIN > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
4. Enter values for the Low Threshold and High Threshold fields.

   This is an example of alert thresholds.



5. Select **Enable** and click **Save** to enable the alert policy that you have configured.

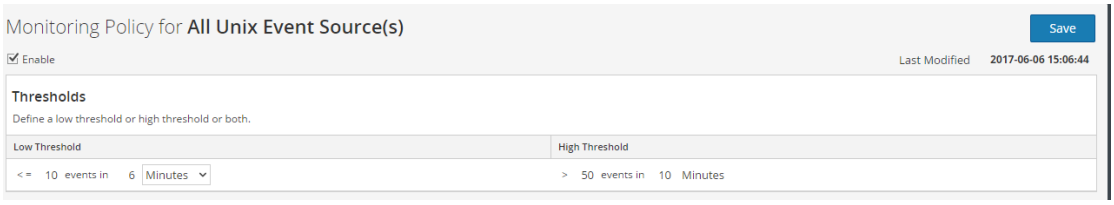
Note: If you make changes to a policy, and attempt to exit the page before you save your changes, an Unsaved Changes warning message is displayed:



Set and View the Thresholds for an Alert Policy

Every event source group is also an alert policy. Thresholds are part of an alert policy. You can set thresholds for each alert policy. For each policy, you can set a low threshold, a high threshold, or both. Additionally, you can enable a policy without setting any thresholds; this allows you to receive notifications based on automatic alerts. Automatic alerts are generated when the baseline for an event source is out of normal bounds.

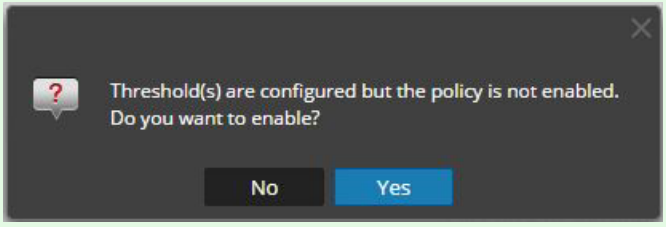
1. Go to **ADMIN > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
   Any thresholds set for the selected group are displayed in the **Thresholds** panel.



4. Edit the values in either the Low or High Threshold as follows:
   a. Enter the number of events for the threshold.
   b. Enter the number of minutes or hours for the threshold. The minimum value is 5 minutes.

   Note: For each threshold, you can set either the low values, the high values, or both.
5. Select **Enable** to enable alarms when thresholds are not met.

Note: If you configure a threshold and attempt to save the page without enabling it, you receive a confirmation message, asking you whether or not to enable the policy: ddd



For example, suppose you enter 10 and 30 for the values for the low threshold: `10 events in 30 minutes`, and 20 and 30 for the values for the high threshold: `20 events in 30 minutes`. This means that you expect between 10 to 20 events are logged in 30 minutes (for the selected event source group). That is, anything between the low and high threshold is considered normal, and does not trigger an alarm.

Note: Once you add a threshold for a policy, you cannot delete it. You can disable the policy, or set the low or high threshold to 0 events in 5 minutes. Five minutes is the minimum duration for a threshold.

Setting Up Notifications

This topic describes how to configure notifications for event source groups. Notifications are sent when thresholds are not met.

Notifications go hand-in-hand with Thresholds. Before you configure notifications, you should set up Thresholds for an event source group.

Note: After configuring the thresholds for an event source group, if you do not set any notifications, then even if an alarm is triggered, users are not notified. However, all alarms are visible on the Alarms Tab.

Prerequisites

Before you set up notifications for an event source group, you should review the available notification items:

- **Notification Servers:** These are the servers that you want to receive notifications from the system. For more details, see the **Notification Servers Overview** topic in the *System Configuration Guide*.
- **Notification Templates:** These are the available templates for each type of notification. For Event Source Management, default templates are supplied for Email (SMTP), SNMP,

and Syslog. You can use these templates as supplied, or customize them if necessary. For more details, see the **Templates Overview** topic in the *Systems Configuration* Guide.

- **Notification Output:** The outputs contain the parameters for the notification type. For example, an email notification type contains the email addresses and subject for the notification. For more details, see the **Notification Outputs Overview** topic in the *Systems Configuration* Guide.

Add Notifications for an event source group

To add notifications for an event source group:

1. Go to **ADMIN > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.

   Note: You should have already set a threshold for the group. If not, see Set and View the Thresholds for an Alert Policy to set a threshold, and then return to this procedure. Alternatively, if you have automatic alerting turned on, then you do not need to set thresholds for a policy. Automatic alarms generate notifications without the need to set thresholds.

4. In the Notifications panel, click +, and from the drop-down menu, select the type of notification you want to add:
   - Email
   - SNMP
   - Syslog

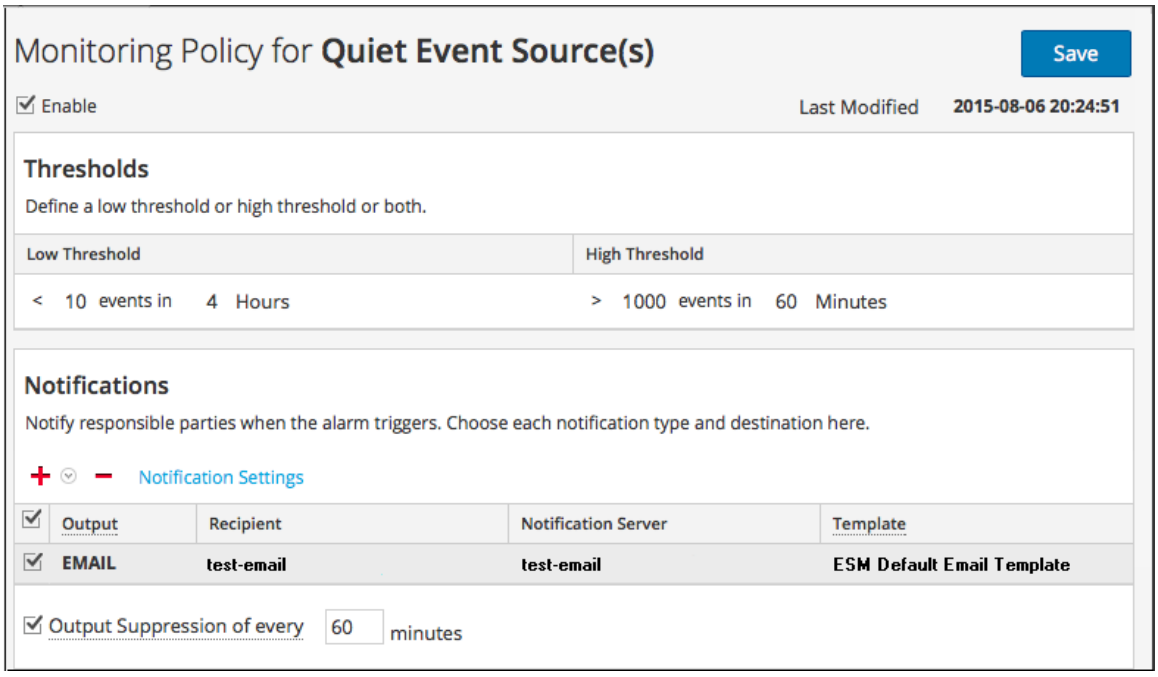
   Note: Default ESM (Event Source Monitoring) templates are provided for each type of notification.

5. Enter values for the Notification, Notification Server, and Template fields.
   a. For Notification, select from the list, or add a suitable notification type in **Notifications**, and then select it here.
   b. For the Server, select one from the list, or add a suitable server in **Notifications**, and then select it here.
   c. For Template, select an available template, or create a suitable template in **Notifications**, and then select it here.

> **Note:** If you need to add or edit one of these items, click **Notification Settings**. A new browser window opens on the **Administration > System > Global Notifications** page. Use this page to view or update the available Notification items.

6. Optionally, you can limit the rate of notifications for a policy.
   a. Select **Output Suppression** to enable setting a limit.
   b. Enter a value, in minutes, for the suppression rate. For example, if you enter **30**, notifications for this policy are limited to one notification every 30 minutes.
   c. Click **Save**.

Here is an example of a monitoring policy that contains a threshold and notification for an event source group.



Disabling Notifications

Notifications are sent when thresholds are not met. Additionally, automatic notifications are sent when baselines are not met. However, you may determine that you no longer require notifications for the event sources in a particular group. In this case, you can disable notifications for the event source group.

> **Note:** Even if you disable all notifications, the details for alarms are still visible on the Alarms Tab.

Prerequisites

You must have configured thresholds and notifications for an event source group, and enabled them. For automatic notifications, you must have selected **Enable Notifications From Automatic Monitoring** on the Alarms Tab

Disable Notifications

To disable notifications (both manual and automatic) for an event source group:

1. Go to **ADMIN> Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
4. Click **Enable** to remove the check mark. Clearing this option means that notifications are not sent for this event source group, even if thresholds are not met or exceeded.
5. Additionally, you can remove all notifications. However, this is not required to stop the notifications.

Viewing Event Source Alarms

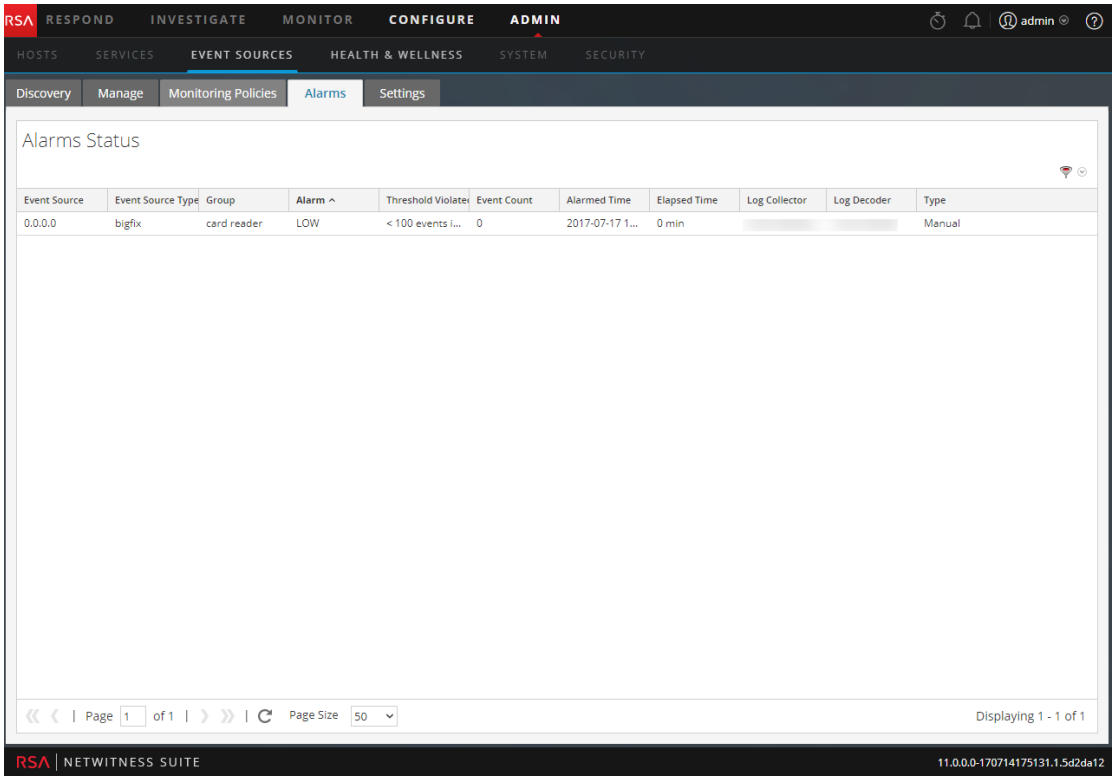
This topic describes how to view alarms for your event source groups. Once you have configured and set alerts, you can view all of the generated alarms in the **Alarms** tab of the **Event Sources** view.

Sort the Alarms Information

When you first access this view, the data is sorted by most recent alarm (the Alarmed time column). You can sort by any column.

1. Go to **ADMIN> Event Sources**.
2. Mouse over a column that you want to sort.
3. Click the Select the **Alarms** tab.
4. Mouse over the column that you want sorted, and click the icon.

   This is an example when you mouse over the Alarm column.



5. Select either **Sort Ascending** or **Sort Descending** to sort the column in the way you wish.

   The data is sorted across all pages.

Note: You can also sort by two columns. To do this, first sort by the secondary column, then sort by the primary column. For example, if you want to see all the HIGH alarms by their group order, first sort on **Group**, then sort on **Alarm**.

Filter Alarms by Type

You can also filter the alarms by their type: you can display only the Manual or Automatic (baseline) alarms. To filter by alarm type, select the filter icon on the right side of screen, in the heading area:

Select either Automatic or Manual:

- If you select Automatic, only the alerts based on baselines are displayed.
- If you select Manual, only the alarms for which you have set thresholds are displayed.

Configuring Automatic Alerting

Note: Automatic alerting, and it settings, are currently in Beta testing.

Prerequisites

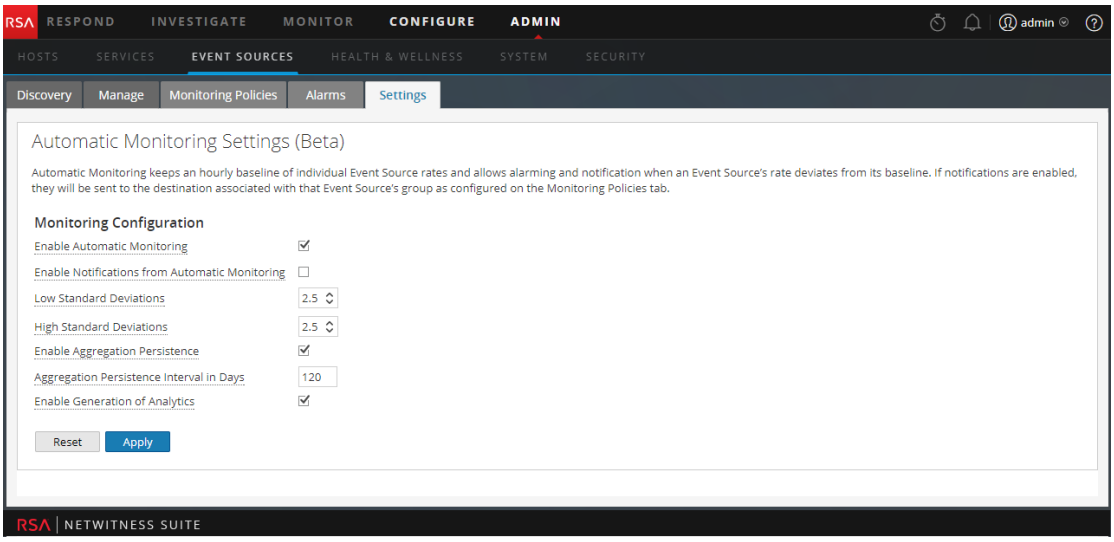
Before you set up notifications for an event source group, you should review the available notification items:

- **Notification Servers:** These are the servers that you want to receive notifications from the system. For more details, see the **Notification Servers Overview** topic in the *System Configuration Guide*.
- **Notification Templates:** These are the available templates for each type of notification. For Event Source Management, default templates are supplied for Email (SMTP), SNMP, and Syslog. You can use these templates as supplied, or customize them if necessary. For more details, see the **Templates Overview** topic in the *Systems Configuration* Guide.
- **Notification Output:** The outputs contain the parameters for the notification type. For example, an email notification type contains the email addresses and subject for the notification. For more details, see the **Notification Outputs Overview** topic in the *Systems Configuration* Guide.

To configure automatic alerting:

1. Go to **ADMIN > Event Sources**.
2. Select the **Settings** tab.

   The Settings tab is displayed.



3. By default, automatic monitoring is turned on. To turn off automatic alerting, clear the **Enable Automatic Monitoring** option.
4. By default, notifications for automatic alerts is turned off. To turn on automatic notifications, select the **Enable Notifications From Automatic Monitoring** option.
5. Configure the parameters, based on your usage patterns:
   - **Low Standard Deviations**: standard deviations below which to receive alerts. Default is **2.5** (95% confidence).
   - **High Standard Deviations**: standard deviations above which to receive alerts. Default is **2.5** (95% confidence).

   Note: You can adjust the standard deviation settings in increments of 0.1 (one tenth) of a standard deviation.
6. Click **Save** to close the dialog and save your settings.

Event Source Management References

The following topics contain reference information for Event Source Management:

- Discovery Tab
- Manage Tab
- Manage Event Source Tab
- Event Sources View
- Create/Edit Group Form
- Details View
- Manage Parser Mappings
- Alarms Tab
- Monitoring Policies Tab
- Settings Tab
- Log Parser Rules Tab
- Default Log Parser and Log Parser Rules

Discovery Tab

To access the Discovery tab, go to NetWitness ADMIN> Event Sources. The Discovery tab is displayed.

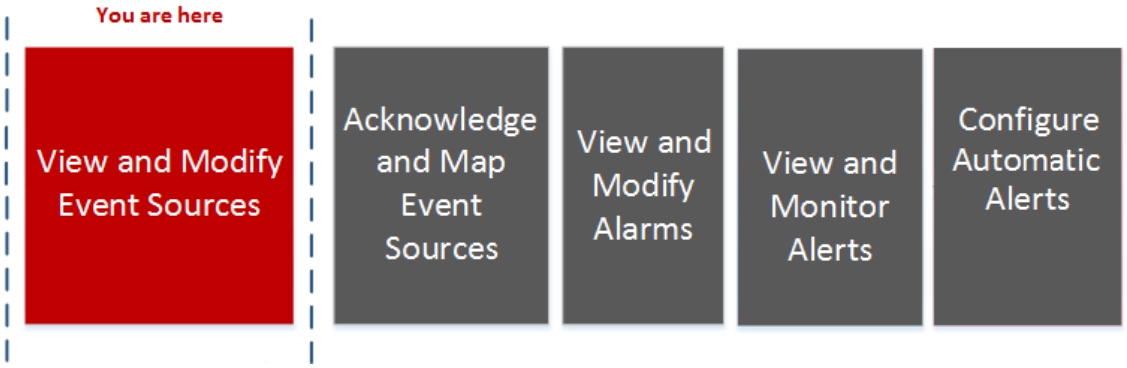
The Discovery tab lets you review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified completely accurately. If the discovered event source types are correct, you can acknowledge to filter out that event source. If incorrect, you can set the allowed event source types for a particular address so that future logs will parse against the correct parsers.

Note: The following features apply to RSA NetWitness® Suite version 11.1 and later:
- Acknowledging multiple event sources
- Filtering by event source type
- Mapping filter options include None, Auto, and Manual.
- Mapping multiple event sources
- Searching for event sources on the Event Source Discovery page

Introduced in RSA NetWitness Suite version 11.1, the system automatically maps incoming events to a type based on previous logs received from that address, reducing the mis-parsing of messages and reducing the number of items that need attention in the Discovery workflow. A value of **Auto** in the **Mapping Type** column indicates that an address has been auto-mapped.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	Acknowledge and map event sources.*	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder.*	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

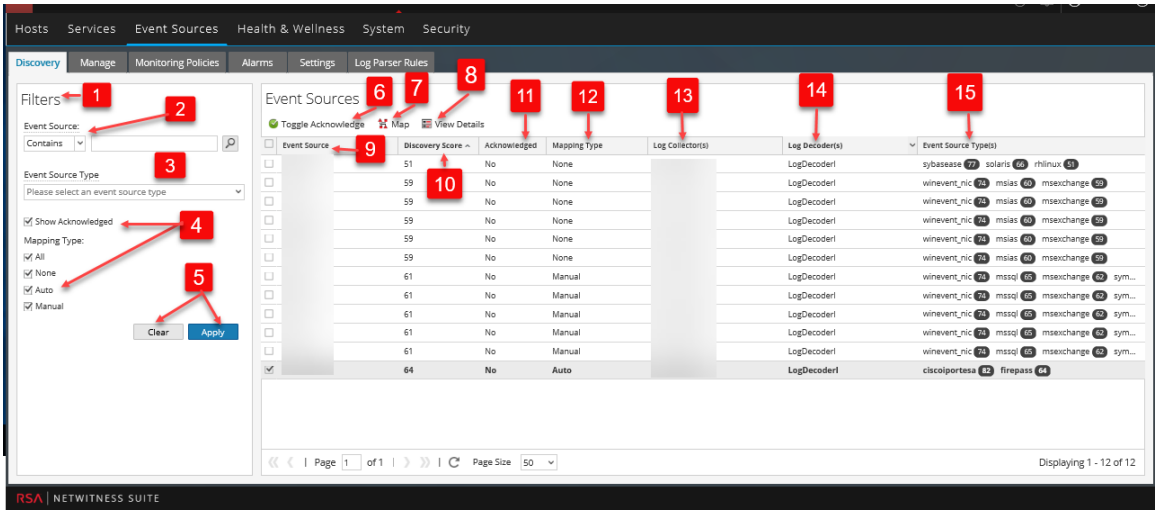
Manage Parser Mappings

Details View

Quick Look

The following example displays a list of addresses and their discovered Event Source types. The Event Source types display the Event Sources that have been discovered.

This is an example of the tab.

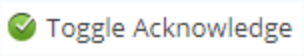
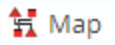


1	Displays the Filters and Event Sources panels with the Discovery tab open.
2	Displays the Event Source Filter field with a drop-down menu that offers the following options: • Enter the full or partial address (IP, IPv6 or Hostname) of the source(s) you want to review. You can also enter multiple entries that are separated by commas. For example, **10.10.10.10,10.10.10.11,host1.company.com** • **Exact:** Returns sources that completely match the search term. For example, **10.10.10.10** only returns **10.10.10.10**, not **10.10.10.101**. • **Starts With:** Returns sources that start with the search term. For example,**10.10.10.** returns the whole **10.10.10.x subnet**. • **Contains:** Returns sources that start with the search term. For example, **exch** returns all terms such as **us-exch-1.company.com**, or **lab21** returns all **hostx.lab21.company.com** terms. • **Ends With:** Returns sources that end with the search term. For example, **lab21.company.com** returns all hosts. **Note:** When specifying the search string, you can use **. - :** (period, dash, colon).
3	The Event Source Type drop-down menu filters for addresses containing all of the selected event source types.
4	• Select the **Show Acknowledged** checkbox to display acknowledged Event Sources. • Mapping filter options can include just one of the mapping types listed in the Filter Panel, or multiple Mapping Types can be selected. **Note:** If no mapping filter options are selected, the default is to display **All**, **None**, **Manual**, and **Auto** mapping types.
5	• The **Apply** button uses all criteria that is set in all filters. • The **Clear** button clears all filters from the panel.
6	Toggles the event sources between acknowledged and not acknowledged states.
7	Maps the selected event sources.
8	View Details button to view details of the selected Event Source.
9	Displays the addresses of the selected Event Sources.
10	Displays the discovery scores of the selected Event Sources.
11	Displays whether or not the selected Event Sources have been acknowledged.

12	Displays the selected Event Source Mapping type as Auto, Manual, or None. Any changes to the mapping are only displayed here.
13	Displays the host names of the Log Collectors where the Event Sources are located.
14	Displays the host names of the Log Decoders where the Event sources are located.
15	Displays the discovered Event Source Types and their associated discovery scores.

Toolbar and Features

The Discovery tab contains the following features:

Field	Description
Tools   	The following items are available on the toolbar: • **Toggle Acknowledge**: Toggles the acknowledged state for the selected Event Source between **Yes** and **No**. • **Map**: Opens the Manage Parser Mappings dialog box, where you can map an event source to the correct log parser. • **View Details**: Provides details on the selected Event Source.
Event Source	The IP, IPv6, or Hostname of the Event Source.
Discovery Score	Displays the overall discovery score associated with that particular address. Higher scores indicate better confidence. Discovery scores range from 0 (least confident) to 100 (most confident).
Acknowledged	Selections are either **Yes** (you have acknowledged the Event Source) or **No** (you have not acknowledged the Event Source).

Field	Description
Mapping Type	Selections are **Manual** (you mapped the Event Source), **Auto** (the system automatically mapped the Event Source), or **None** (you have not mapped the Event Source). **Note:** This features applies to RSA NetWitness version 11.1 and later.
Log Collector(s)	Log Collectors that have received logs from this Event Source address.
Log Decoder(s)	Log Decoders that have received logs from this Event Source address.
Event Source Type(s)	The parsed type(s) of the Event Source address and the corresponding Discovery Score for each type.

Note: Discovery Scores are only available for 11.0 and above Log Decoders. Discovery Scores for pre-11.0 Log Decoders display as Unavailable.

The following table describes the sorting order for discovery scores. To access the Sorting Order drop-down menu, click on the down arrow in the Event Sources column.

Field	Description
Sort Ascending	Sort the column by discovery score in ascending order.
Sort Descending	Sort the column by discovery score in descending order.
Columns	Used to hide or show one or more columns.

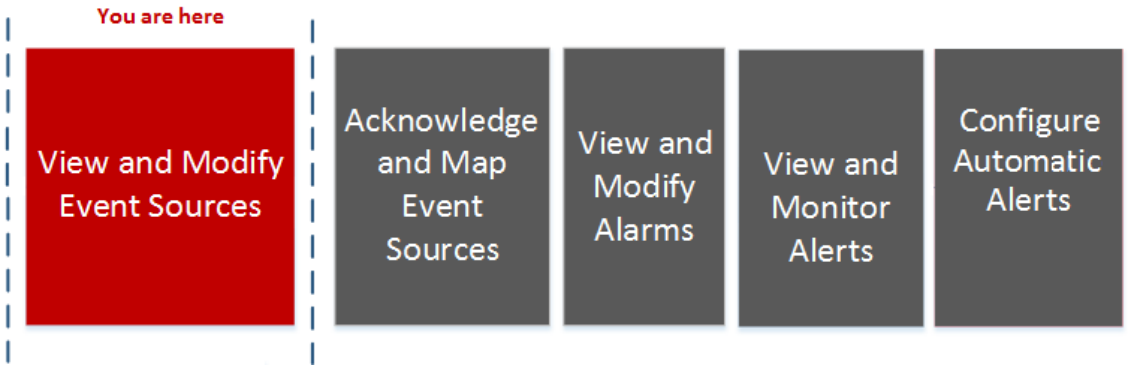
Manage Tab

The Manage tab organizes event sources into groups, and displays attributes for each event source.

To access this tab, go to **ADMIN > Event Sources > Manage**.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	*View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map event sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

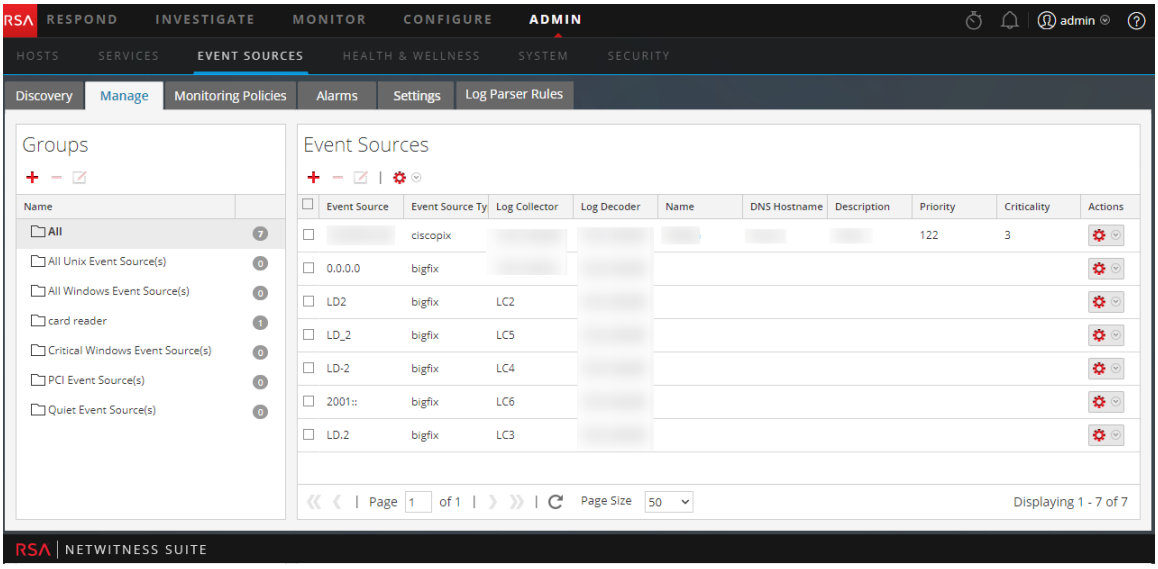
Related Topics

Creating Event Source Groups

Creating an Event Source and Editing Attributes

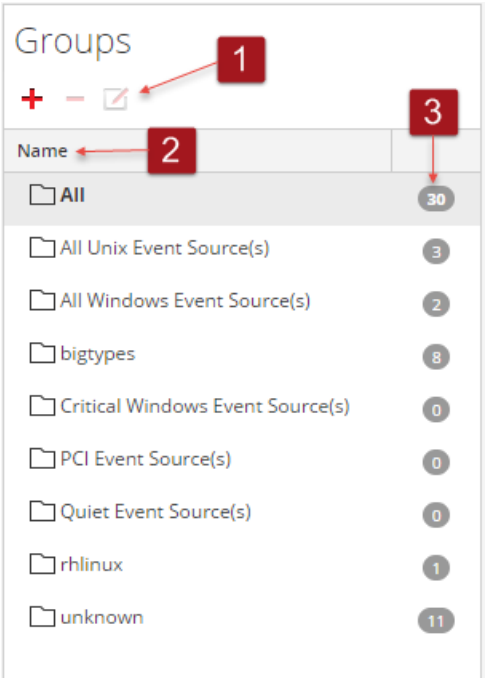
Quick Look

The Manage tab organizes event sources into groups, and displays attributes for each event source. The Manage tab consists of two panels, Groups and Event Sources.



Groups Panel

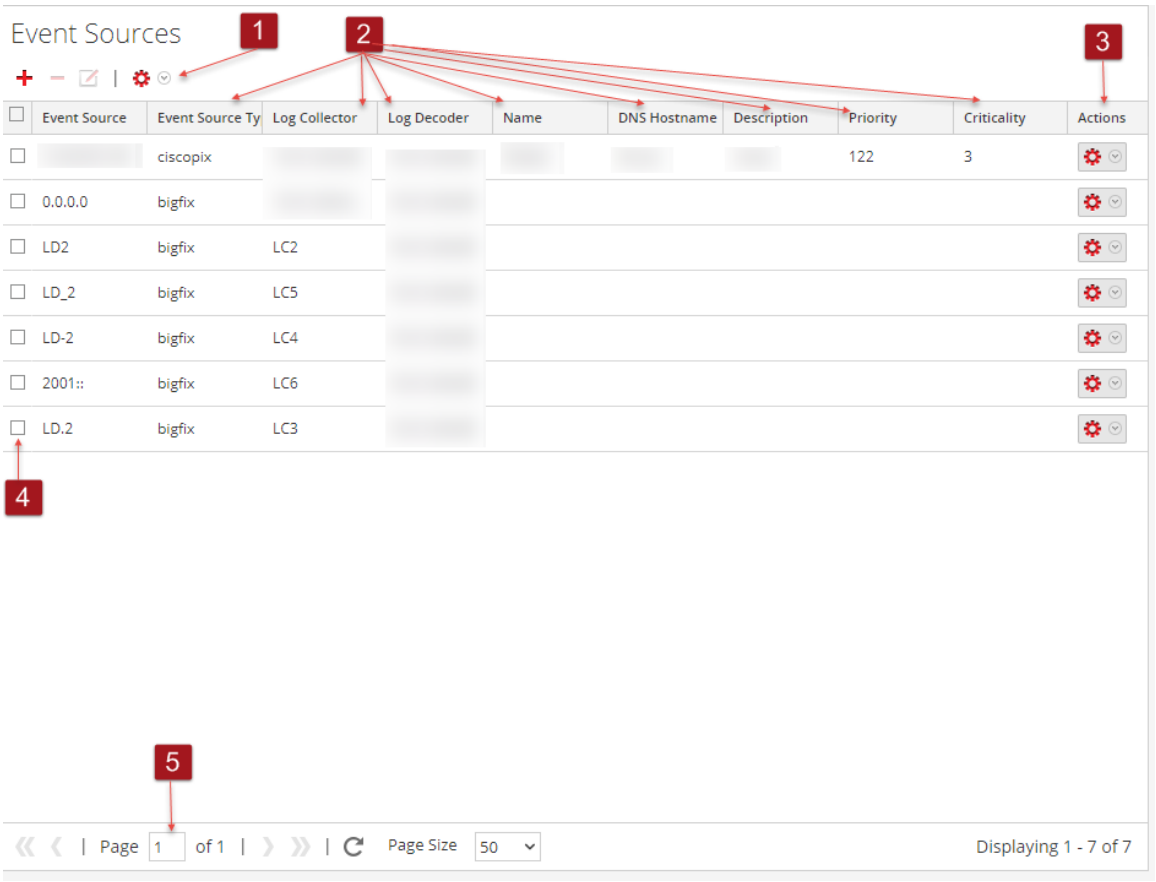
The Groups Panel lists the event source groups, as well as a count of the members for each group. To see all event sources, select **All** from the groups list. This is an example of the Groups panel.



1	Displays the standard NetWitness Suite icons for adding, removing, or editing groups.
2	Lists the identifier for each group in the Name column. You can use the group names to quickly identify some of the criteria used to form the group. For example, if you create a group that consists of Windows event sources for the Sales organization, you could name the group **Windows Sales Sources**. **Note:** The event source group name is not editable. Once you create a group, that name exists as long as the group itself.
3	The count for an event source group indicates the number of event sources in that group. That is, the number of event sources that match the criteria used to define the group. **Note:** The count is not dynamically updated when new event sources are added. Thus, you may need to refresh to see an updated group count.

Event Sources Panel

The Event Sources panel displays the attributes for the event sources in the selected group. Or, if All is selected in the Groups panel, the Event Sources panel lists all event sources.



1 The toolbar contains the following tools:

- **Add**: manually add an event source
- **Remove**: remove an event source
- **Edit**: Update attributes for an existing event source
- **Import / Export** menu: Displays a menu with the following options:
  - **Import**: Import event sources from a Content Management Database (CMDB), spreadsheet, or other tool.
  - **Export**: Export selected event sources and their attributes in CSV format.
  - **Export Group**: Export the entire group that is currently selected.

2 Columnar display of attributes. You can choose which attributes to display.

3 Actions: Shortcut menu for often-used commands: Edit, Delete, and Export.

4	Checkboxes: Select rows to use when performing tasks on multiple event sources, such as bulk editing.
5	Navigation Tools: At the bottom of the screen, there are items that help in navigating your group: • **Page *x* of *y***: indicates which page you are currently displaying, and how many total pages exist for this group. • **<<**, **<**, **>** and **>>**: click these icons to move between pages either one at a time (< and >) or to the first (<<) or last (>>) page. • **Page Size**: use this selector to choose your page size. • **Displaying *x* - *y* of *z***: quick check of which event sources are currently displayed out of the total number for the group.

Sorting

In the Event Sources panel, the list of items is presented in a sorted order. You can choose which column on which to sort. Note, however, that the sort order depends on capitalization.

For any string column, if the values contains a mix of lower case and upper case, the upper case appear in the list before the lower case values.

For example, assume the Event Source Type column contains the following entries: Netflow, APACHE, netwitnessspectrum, ciscoasa. The sort order would be as follows:

- APACHE
- Netflow
- ciscoasa
- netwitnessspectrum

Manage Event Source Tab

The Manage Event Source screen has several integrated components that present different perspectives of an event source.

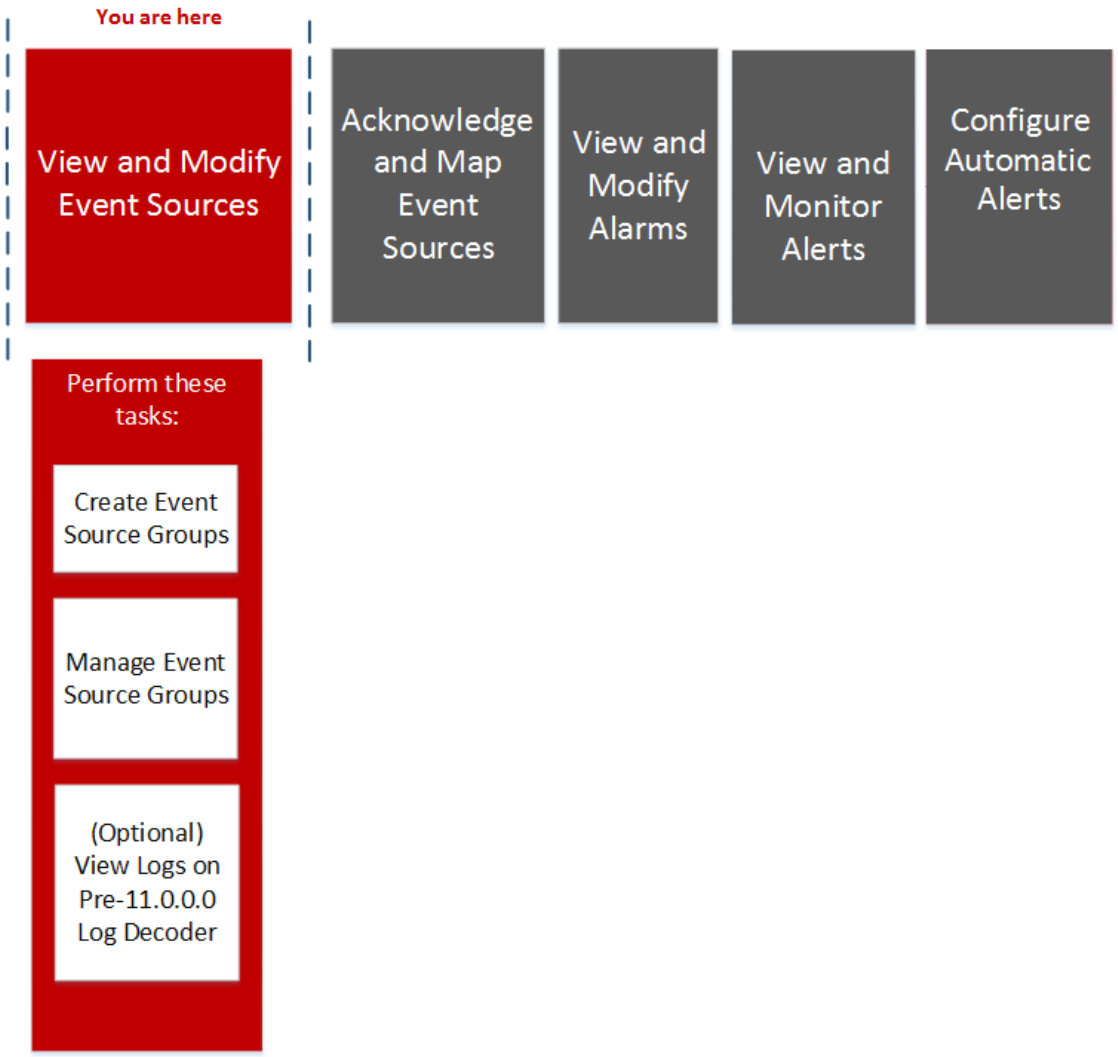
- Show Event Source Details
- Add attribute values to an event source
- Remove attribute values for an event source

To view the Manage Event Source screen for an event source:

1. Go to **ADMIN> Event Sources**.
2. Select the **Manage** tab.
3. From the Event Sources pane, select an event source from the list and click + .

Workflow

This workflow shows the end-to-process for modifying, acknowledging, mapping, and configuring event sources, along with viewing and configuring event source alarms and alerts.



What do you want to do?

Role	I want to...	Documentation
Administrator	Create an event source group that contains all the high priority event sources.	Creating Event Source Groups
Administrator	Edit event source attributes.	Creating an Event Source and Editing Attributes

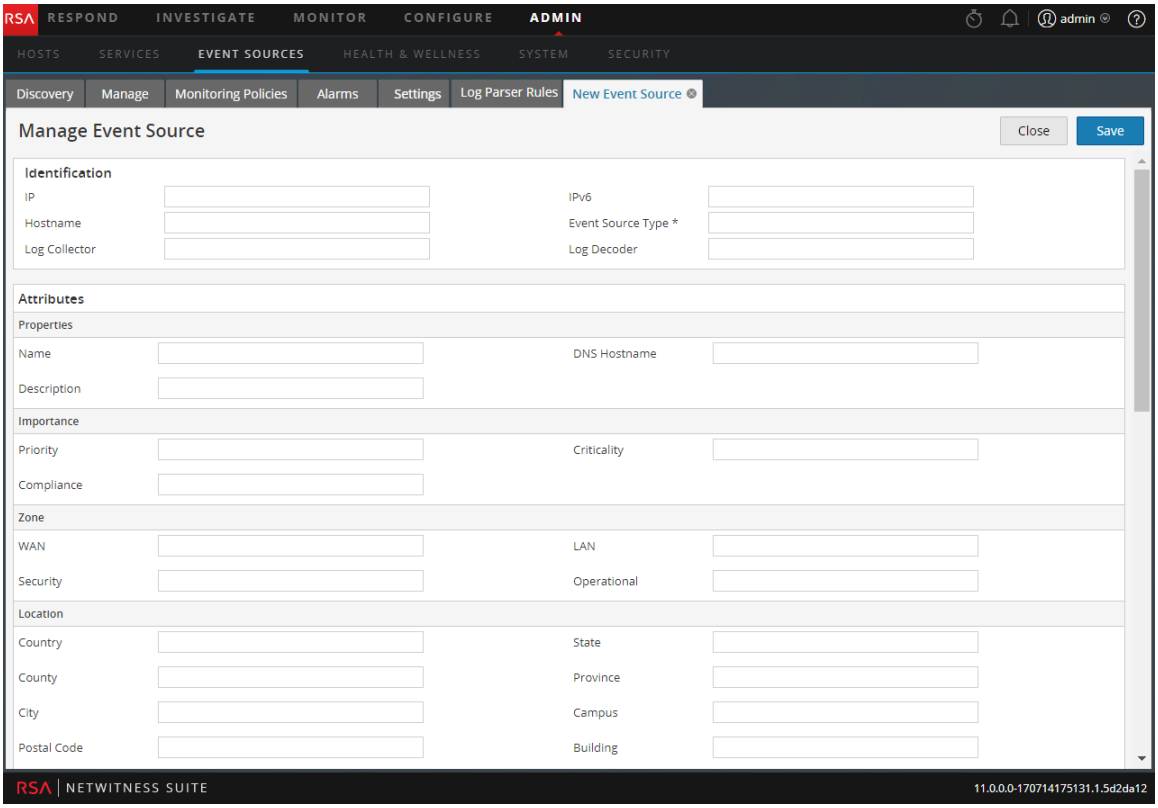
Related Topics

Creating an Event Source and Editing Attributes

Creating Event Source Groups

Quick Look

This is an example of the New Event Source tab:



This table describes event source attribute categories.

Attribute Section	Description
Identification	These attributes are the main attributes that collectively identify an event source. The following attributes are auto-populated, and cannot be changed while on this screen: • IP address • IPv6 value • Hostname • Event Source Type These attributes can be modified: • Log Collector • Log Decoder
Properties	These attributes provide the name and description. • Name • DNS Hostname • Description
Importance	These attributes can be used for grouping by priority. • Priority • Criticality • Compliance
Zone	These attributes can be used for grouping by zone. • WAN (Wide Area Network) • LAN (Local Area Network) • Security • Operational

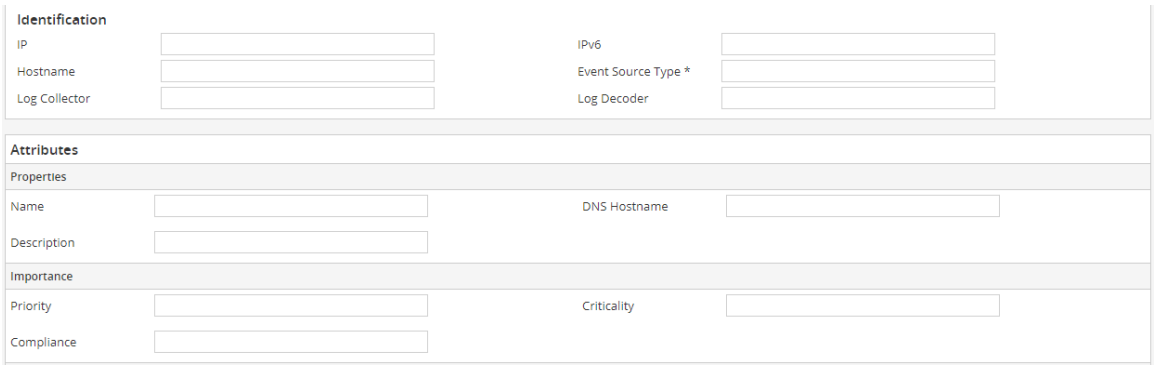
Attribute Section	Description
Location	These attributes can be used to group by the physical or geographical location. • Country • State • County • Province • City • Campus • Postal Code • Building • Floor • Room
Organization	These attributes can be used to group by organization, and also to provide contact information. • Company • Division • Business Unit • Department • Group • Contact • Contact Phone • Contact Ema
Owner	These attributes specify those responsible for the event source. • Manager • Primary Administrator • Backup Administrator

Attribute Section	Description
Physical	These attributes specify the physical properties for the event source. • Vendor • Serial Number • Asset Tag • Voltage • UPS Protected • Rack Height • Depth • BTU Output • Color
Function	These attributes can be used to group by function. • Primary Role • Sub Role 1 • Sub Role 2
System Information	These attributes specify system information. • Domain Name • System Name • Identifier • System Description
Custom	This section provides eight custom attributes, for any other attributes that your organization might need.

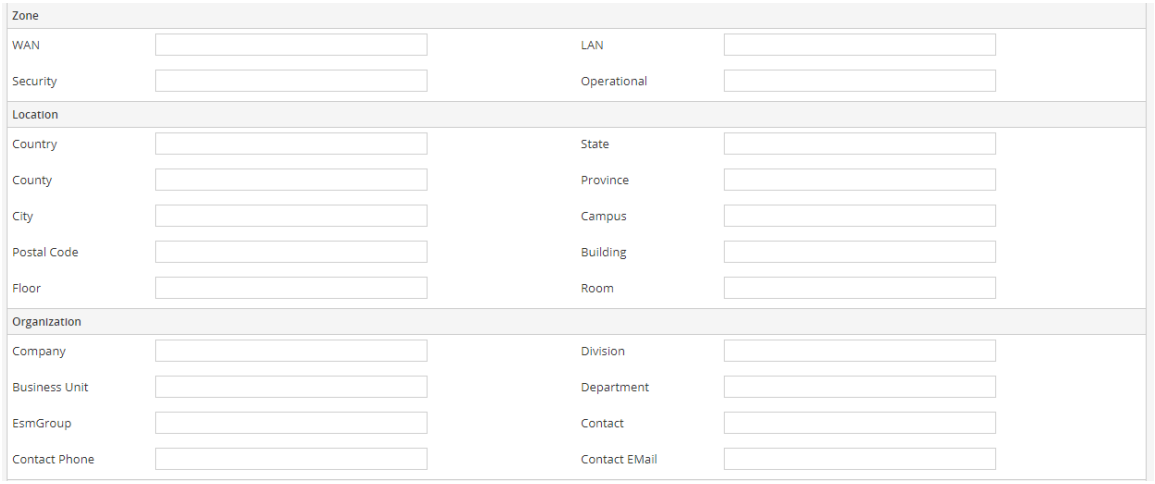
Features

The settings in the Manage Event Source tab are a combination of auto-populated and user-entered information. When an event source sends log information to NetWitness Suite, it is added to the list of event sources, and some basic information is auto-populated. At any time after that, users can add or edit details for other event source attributes.

This figure shows an example of the **Identification**, **Properties**, and **Importance** sections.



This figure shows an example of the **Zone**, **Location**, and **Organization** sections.



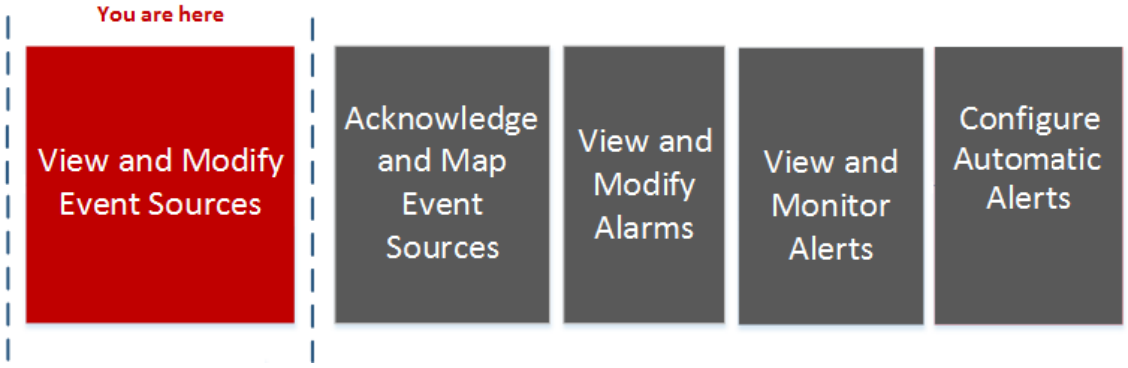
Event Sources View

The Event Source Attributes panel has the following tabs.

To access this panel, go to **ADMIN > Event Sources**.

Workflow

This workflow shows the end-to-process for modifying, acknowledging, mapping, and configuring event sources, along with viewing and configuring event source alarms and alerts.



What do you want to do?

Role	I want to...	Documentation
Administrator	Create an event source group.	Creating Event Source Groups
Administrator	Edit or delete an event source group.	Editing or Deleting Event Source Groups
Administrator	Edit event source attributes.	Creating an Event Source and Editing Attributes

Related Topics

Managing Event Source Groups

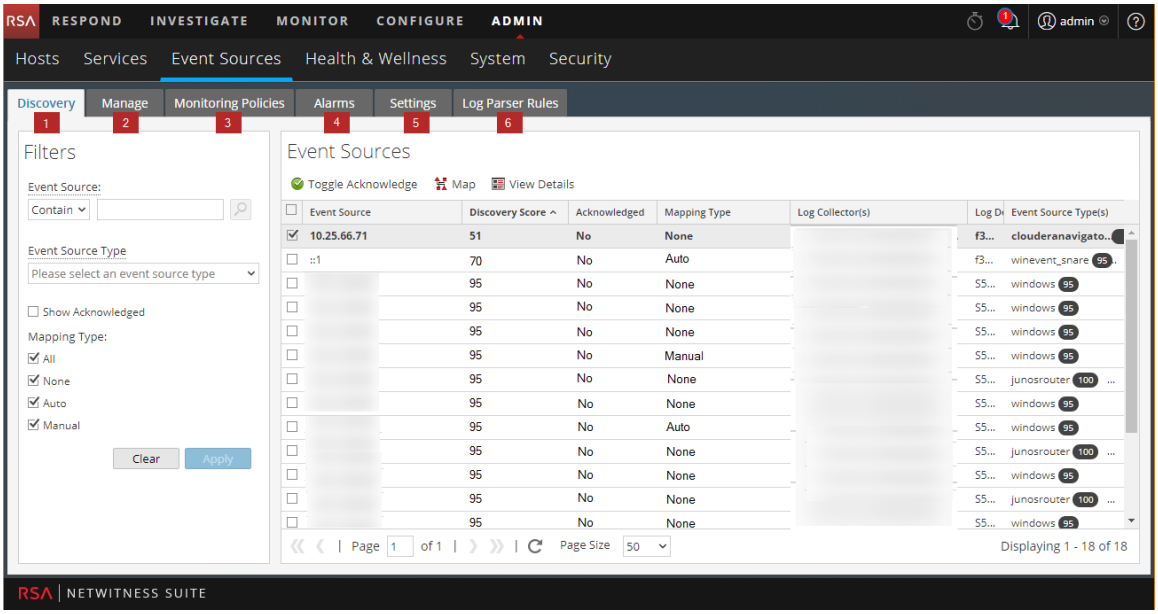
Creating Event Source Groups

Editing or Deleting Event Source Groups

Creating an Event Source and Editing Attributes

Quick Look

The Event Sources view presents the details for Event Sources that are discovered, acknowledged, or mapped by RSA NetWitness Suite.



1. [Discovery Tab]

   Use this tab to review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified accurately.

2. [Manage Tab]

   Use this tab to create, edit, and delete Event Source Groups. It presents a customizable, searchable view of all of your event sources and groups.

3. [Monitoring Policies Tab]

   Use this tab to manage alert configuration for event sources.

4. [Alarms Tab]

   Use this tab to see the details of the alarms that have been generated.

5. [Settings Tab]

   Use this tab to view or change the behavior for automatic (baseline) alerts.

6. [Log Parser Rules Tab]

   Use this tab to display information about individual log parsers, as well as the default, "parse all" parser.

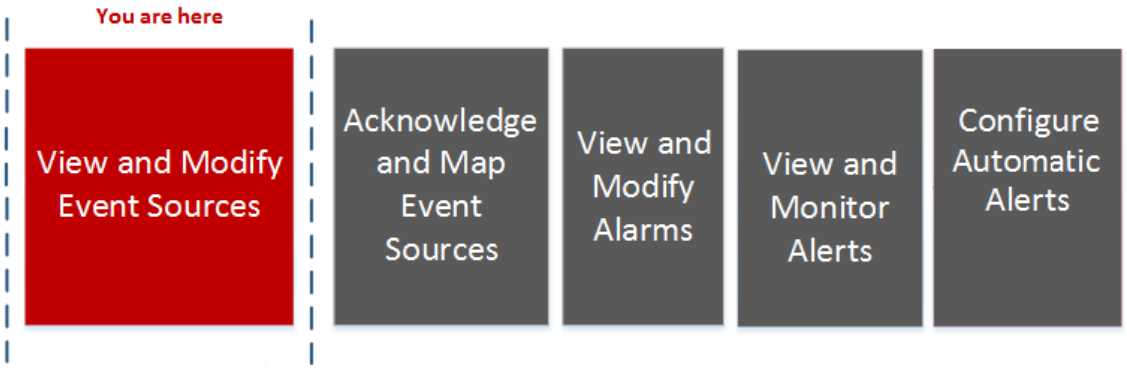
   Note: The Log Parser Rules tab is only available in RSA NetWitness® Suite versions 11.1 and later.

Create/Edit Group Form

This Create Event Source Group form is displayed when you are creating or editing an Event Source Group.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	*View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Creating Event Source Group Form

Managing Event Source Groups

Details View

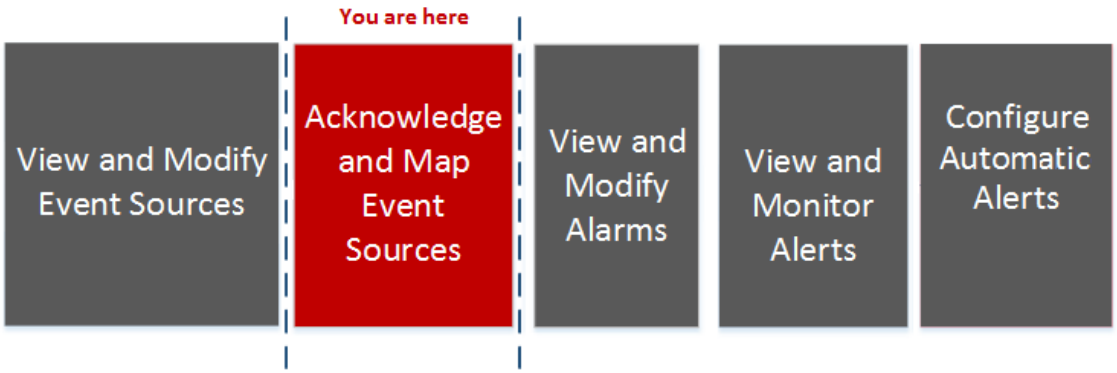
The **Details** view allows you to see details about the Event Source, as well as viewing a sample of the logs identified for each type in order to verify their accuracy.

You can access the **Details** view in a couple of ways.

- From the Toolbar, click the **View Details** button. Or, you can
- Double-click on the Event Source you selected.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	*Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View log parser details	Manage Parser Mappings

Role	I want to...	Documentation
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

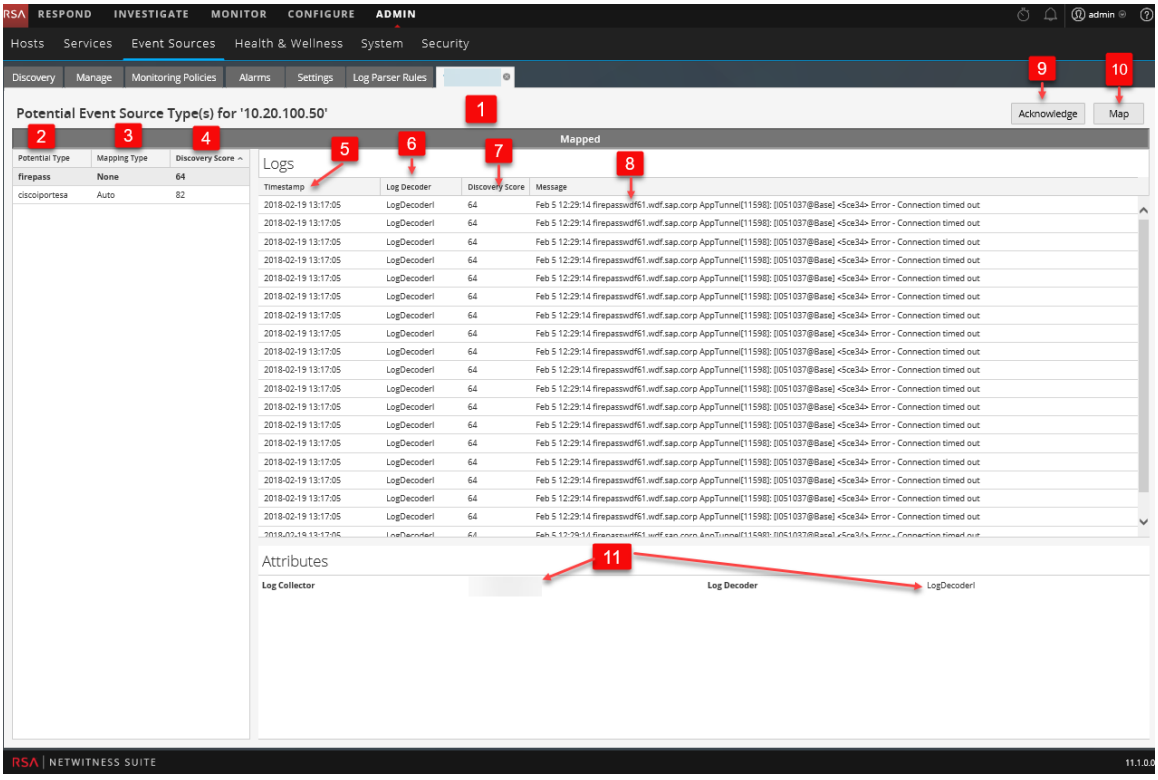
Related Topics

Viewing Logs from Pre-11.0 Log Decoder

Quick Look

The following example shows the discovery scores, event source types, logs, and attributes that correspond with the Event Source you selected in the Event Sources panel for a single Log Decoder.

Note: Device logs are only available for 11.0.0.0 and above Log Decoders.



1 Displays the address of the selected Event Source.

2 Displays the potential type of the selected Event Source.

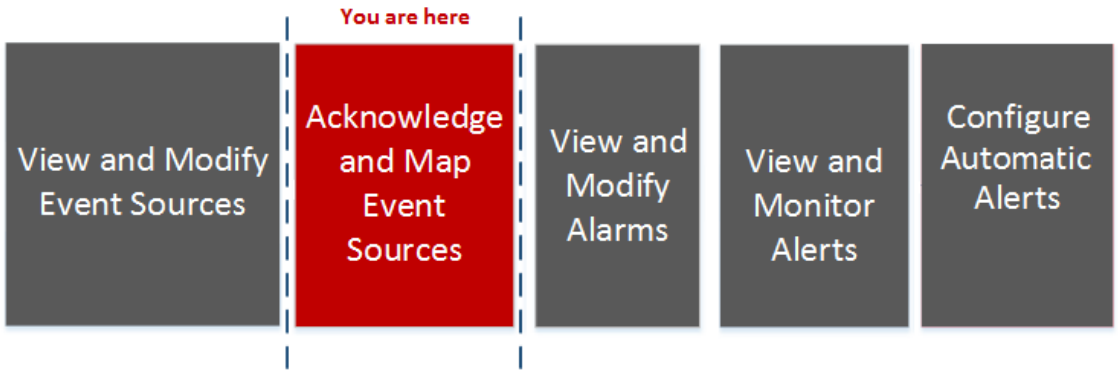
3	Displays the selected Event Source Mapping Type as Auto-Mapped, Manually Mapped, or None. Any changes to the Event Source Mapping are only displayed here.
4	Displays the discovery score for the selected Event Source type from least confident (0) to most confident (100).
5	Displays timestamps for the last few logs that have been parsed to the selected Event Source Type.
6	Displays the address of the Log Decoder that is parsing event sources.
7	Displays the discovery score of the corresponding log.
8	Displays logs for the selected Event Source type.
9	Allows you to acknowledge that all the discovered Event Source types are correct.
10	Allows you to set the appropriate parsers for selected Event Source addresses.
11	Displays the Event Source Management attributes for the selected Event Source Type.

Manage Parser Mappings

The **Manage Parser Mappings** dialog allows you to map the appropriate parsers for selected Event Source addresses. From the **Details** view, select the **Map** button.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

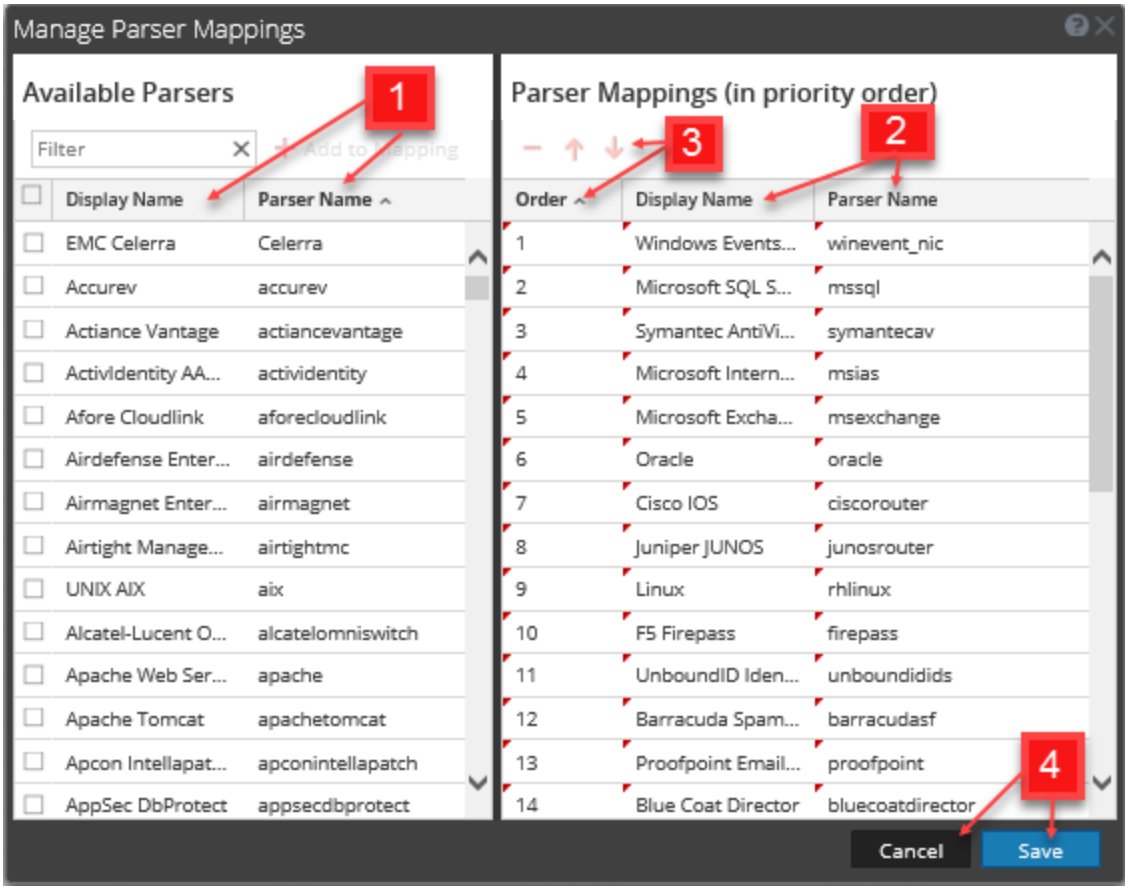
Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	*Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Viewing Logs from Pre-11.0 Log Decoder

Quick Look



1 Displays all the available parsers that you can map based on the event sources that you selected from the **Discovery** view. Also displays the mappings that are already present in the Log Decoders for the selected event source or the parsers that have been discovered.

To filter your available parsers, type the first few letters of the parser name that you want to map.
Click the **Add to Mapping** button to add the parser to the parser mappings listed in the right panel.

You need to select parsers before the **Add toMapping** button is enabled.

Add the selected parser by clicking the **Add to Mapping** button in the right panel.

You can rearrange the order of the parser mappings using the up and down arrow keys and you can also drag and drop selected parser mappings. You can select multiple

mappings by pressing the **Ctrl** key.

2 Displays the names of the selected parsers that you want to map.

3 Displays the order of the selected parser mappings.

You can delete parser mappings by selecting the minus sign ( ).
Press the **Ctrl** key to select multiple mappings to perform group operations on them.

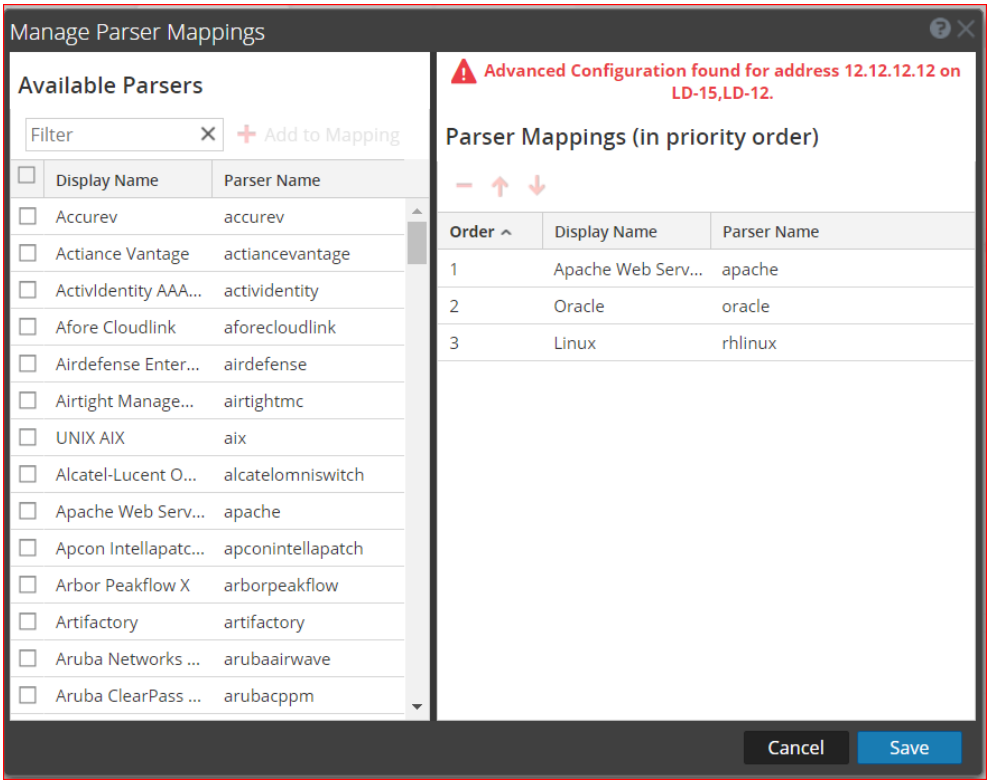
4 Click **Save** to save your mappings to all the Log Decoders. A pop-up message informs you that your mappings are successfully saved. When the window is closed, the banner on the **Details** tab is updated to reflect the status. If mapped, the text displayed is **Mapped**.
Click **Cancel** to return to the **Details** tab.

Advanced Configuration

Mapping configurations with the Log Collector are not displayed in the Parser Mappings window. If the mapping is saved, it is saved for the corresponding IP address, not for the corresponding Log Collector entry. If no mappings are found for the corresponding IP address, the discovered event source types are displayed in the Parser Mappings window.

If advanced Log Decoder configurations are discovered, a message similar to the one below displays in the Manage Parser Mappings dialog.

Note: If you want to edit the advanced configuration, you need to navigate to the Log Decoder service's parser mappings configuration.



Alarms Tab

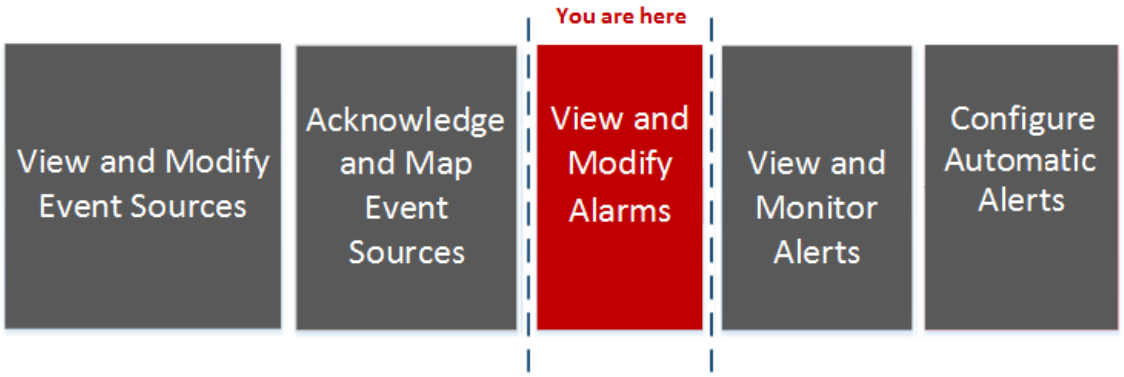
From the Alarms tab you can view details of the alarms that have been generated.

The Alarms tab has one panel that displays Alarm status.

To access this tab, go to ADMIN > Event Sources > Alarms.

Workflow

This workflow shows the overall process for configuring event sources. It also shows where configuring alarms and alerts settings are located in the process.



What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	*View event source alarms.	Viewing Event Source Alarms

Role	I want to...	Documentation
Administrator	View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

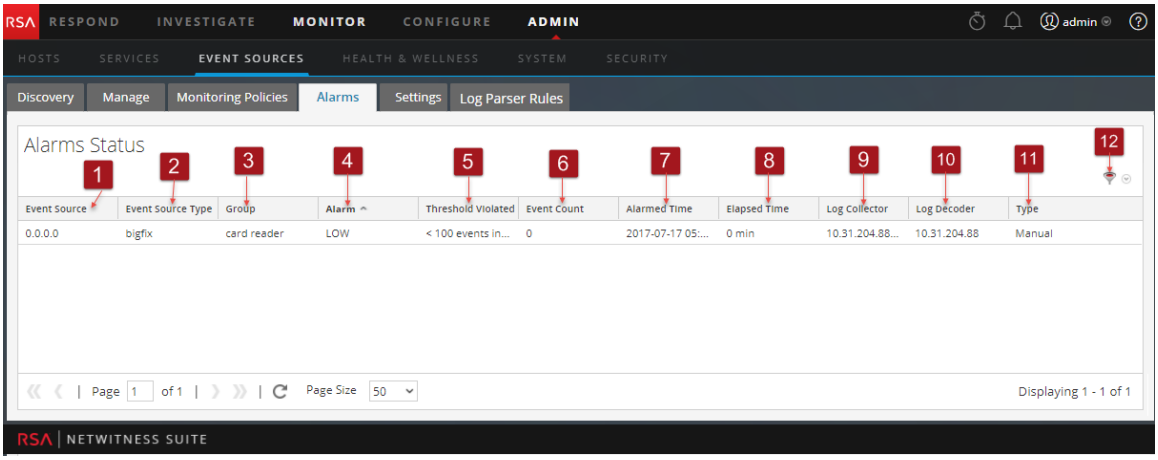
*You can perform this task here.

Related Topics

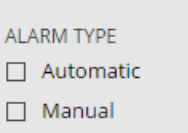
Configuring Automatic Alerting

Quick Look

The Alarms tab presents the details for Event Sources that are currently in violation of a policy and threshold. Only Event Sources in violation of a policy appear in the list. Once the event source returns to a normal state, the corresponding alarm disappears from the list.



1	Displays the IP, IPv6, or Hostname of the event source that is alarmed.
2	Displays the type of the alarmed event source. For example, **winevent_nic** (for Microsoft Windows) or **rhlinux** (for Linux).
3	Displays the event source group that contains the event source for which the alarm has been triggered.
4	Displays the type of threshold that was triggered: **High** or **Low**
5	Displays the conditions of the threshold that was triggered. For example: `5,000,000 events in 5 minutes`
6	Displays the number of events in the threshold time period causing the alarm.

7	Displays the initial time the event source went into an alarmed state. **Note:** When you first access this view, the data is sorted by this column (most recent alarm first).
8	Displays the elapsed time since the event source entered an alarmed state.
9	Displays the Log Collector last collecting from this event source.
10	Displays the Log Decoder last receiving from this event source.
11	Displays the alarm type. Alarm type is either **Manual** or **Automatic**: • **Manual**: these are alarms that violate the configured threshold policy. • **Automatic**: these are alarms that deviate from the baseline for the alarmed event source.
12	Select the **Filter** icon to display the **Filter** menu:  Select either **Automatic** or **Manual**: • If you select **Automatic**, only the alerts that are based on baselines are displayed. • If you select **Manual**, only the alarms for which you have set thresholds are displayed. **Note:** You can hide or show columns by right-clicking in the table header and choosing **Columns** from the drop-down menu. Select a column to display it, or clear the column to hide it.

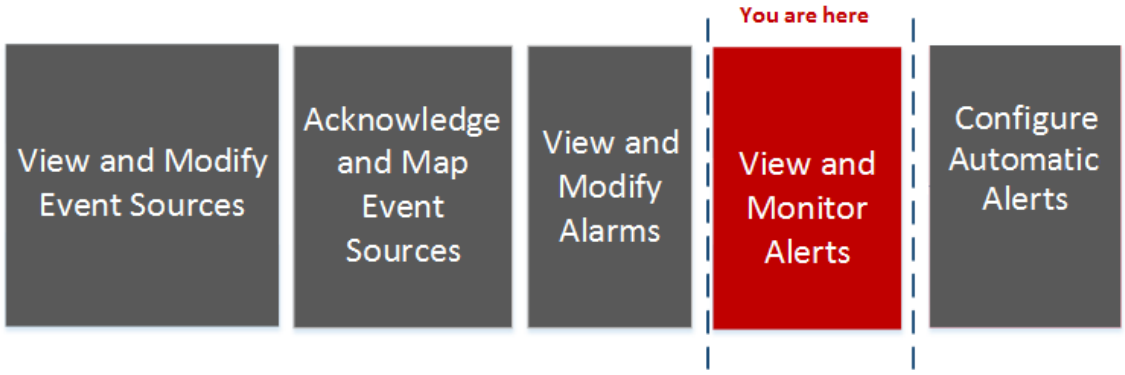
Monitoring Policies Tab

The Monitoring Policies tab organizes thresholds by event source group.

To access this tab, go to **ADMIN > Event Sources**. The **Manage** tab is displayed. Select the **Monitoring Policies** tab.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	*View Monitoring Policies.	Monitoring Policies
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Setting Up Notifications

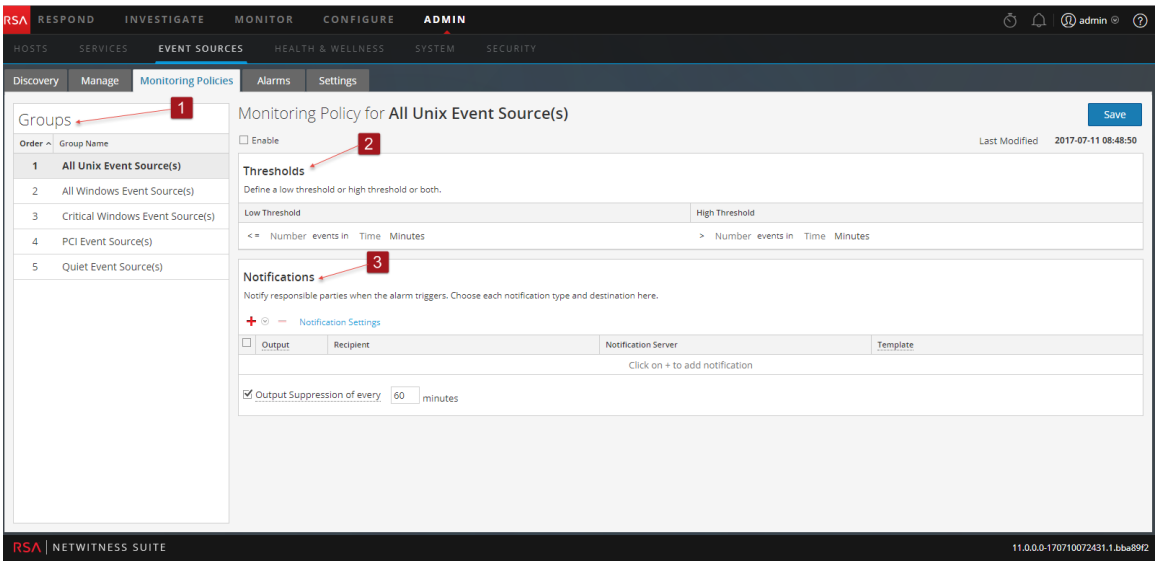
Disabling Notifications

Quick Look

The **Monitoring Policies** tab consists of three panels:

- Event Groups Panel
- Thresholds Panel
- Notifications Panel

This is an example of the **Monitoring Policies** tab.



1	Displays the Groups panel.
2	Displays the Thresholds panel.
3	Displays the Notifications panel.

Event Groups Panel

The group selected in this panel determines which thresholds appear in the Thresholds panel. You can define a set of thresholds for each event source group. Notice that the groups are listed in a specific order:

- Drag and drop groups to change the specified order.
- The higher a group is listed, the higher the precedence for that group's thresholds: RSA NetWitness Suite checks the thresholds in the order provided in this panel. Thus, your highest priority groups should be at the top of this list

Thresholds Panel

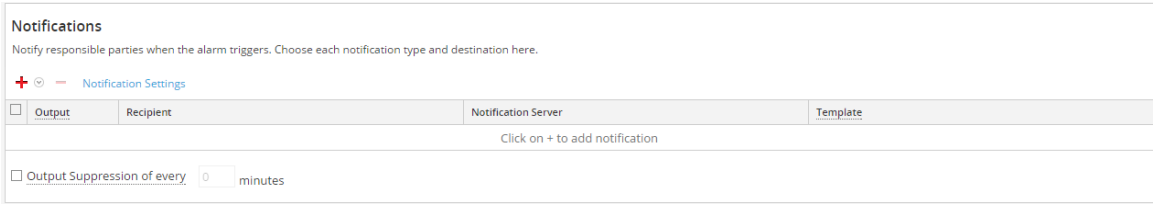
This is an example of the Thresholds panel for an event source group.

The Thresholds Panel contains the following features.

Feature	Description
Enable	The Enable checkbox designates whether or not the thresholds that you define for a group are enabled. If so, notifications are sent whenever the thresholds for that group are outside of the defined range. If not, then no monitoring of that event source group is occurring. **Note:** If you configure a threshold and attempt to save the page without enabling it, you receive a confirmation message, asking you whether or not to enable the policy. If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic notifications. See below for more details on the look of notifications.
Low number of events Low number of minutes or hours	This is the low end of the threshold. Enter the fewest number of events and the time range. If the event source group receives fewer messages than specified here, the threshold is not met, and notifications are sent.
High number of events High number of minutes or hours	Works similarly as for the low values: If more messages than specified here are received, the threshold is not met, and notifications are sent.
Last Modified date and time	This field indicates the last time and date that the thresholds were changed.
Save	Saves the changes you have made to the thresholds.

Notifications Panel

This is an example of the Notifications panel for an event source group.

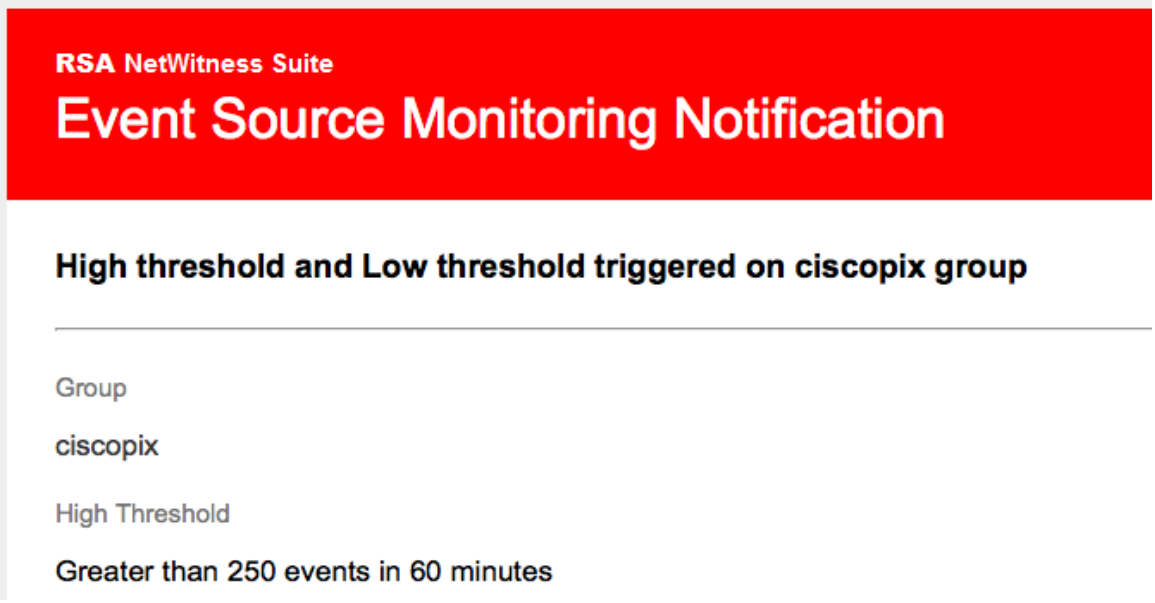


The following table describes the fields on the Notifications panel

Field	Description
Tools + -	The following items are available on the toolbar: • **Add (+)**: clicking the **Add** presents a menu where you can choose the type of the notification • **Remove (-)**: removes the selected row from the list.
Notification Settings	Clicking this link opens a new browser tab, and takes you to the **Admin** > **System** > **Notifications** page in NetWitness Suite.
Type	Displays the type of the notification that you have chosen. The available options are as follows: • Email • SNMP • Syslog
Notification	See the **Configure Notification Outputs** topic in the *System Configuration Guide* for more details.
Notification Server	See the **Configure Notification Servers** topic in the *System Configuration Guide* for more details
Template	For Event Source Management, RSA provides three out-of-the-box templates for notifications. You can use the following templates as delivered, or customize them based on the needs of your organization: • **Email template**: sends notifications to the specified email addresses. • **SNMP template**: sends notifications to the specified SNMP server • **Syslog** template: sends notifications to the specified Syslog server. See the **Configure /Templates for Notifications** topic in the *System Configuration Guide* for more details.

Field	Description
Output Suppression	Use this item to limit how often notifications are received for this policy, in case a lot of alerts are triggered in a short period of time.

The following are sample notifications, based on the supplied Templates.



- Email:

  For email notifications, the third column, **Alarm Type**, specifies whether the triggered alarm was based on a user threshold, or the baseline data being out of normal bounds. If you have automatic monitoring or notifications turned off, you will not receive any **Automatic** notifications. The same is true for Syslog and SNMP, except those notifications are formatted differently.

- SNMP trap:

```
11-11-2015 11:57:33 Local7.Debug 127.0.0.1 community=public,
enterprise=1.3.6.1.4.1.36807.1.20.1, uptime=104313, agent_
ip=10.251.37.92, version=Ver2,
1.3.6.1.4.1.36807.1.20.1="NetWitness Suite Event Source
Monitoring Notification:
Group: PCI Event Source(s)
High Threshold:
Greater than 500 events in 5 minutes
10.17.0.10,ciscopix,Manual
10.17.0.13,ciscopix,Manual
```

```
10.17.0.8,ciscopix,Manual
10.17.0.8,ciscopix,Automatic
10.17.0.12,ciscopix,Manual
10.17.0.5,ciscopix,Manual
10.17.0.6,ciscopix,Manual
10.17.0.4,ciscopix,Manual
10.17.0.4,ciscopix,Automatic
10.17.0.3,ciscopix,Manual"
```

- Syslog sample:

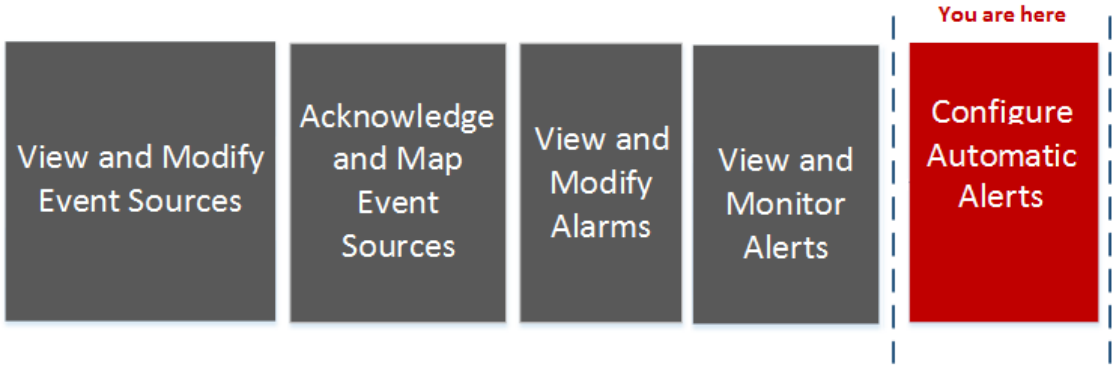
```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33
localhost CEF:0|RSA|NetWitness Suite Event Source
Monitoring|10.6.0.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source
(s)|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|sr
c=10.17.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src
=10.17.0.12,ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10
.17.0.6,ciscopix,Manual|src=10.17.0.4,ciscopix,Manual|src=10.17.
0.4,ciscopix,Automatic|src=10.17.0.3,ciscopix,Manual|
```

Settings Tab

The Settings tab presents options for automatic monitoring (baseline alerting). To access this tab, go to ADMIN> Event Sources > Settings.

Workflow

This workflow shows the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	*Configure Automatic Alerts.	Automatic Alerting
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Automatic Alerting

Disabling Notifications

Quick Look

You can set up policies and thresholds for your event source groups. You do this so that you can receive notifications when the thresholds are not met. NetWitness Suite also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

About Automatic Alerting

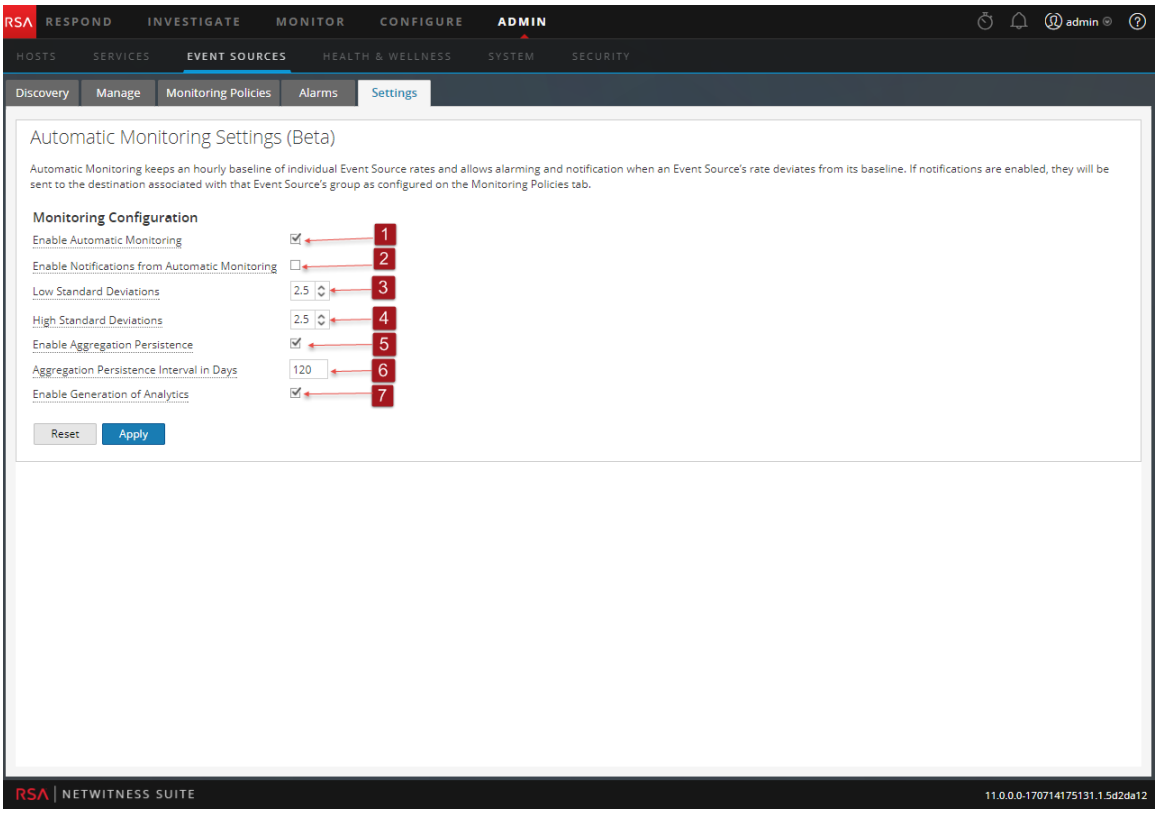
You can set up policies and thresholds for your event source groups. You do this so that you receive notifications when the thresholds are not met. NetWitness Suite also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

To trigger automatic alerts, you can use baseline values. This way, you do not need to set up numerous group thresholds and policies in order to receive alerts. Any anomalous amount of messages trigger alerts, without needing to do any configuration (except for turning on automatic alerting).

Note the following:

- Once you begin collecting messages from an event source, it takes the system approximately a week to store a baseline value for that event source. After this initial period, the system alerts you when the number of messages for a period are above or below the baseline by a set amount. By default, this amount is 2 standard deviations above or below the baseline.
- Base your high and low deviation settings on how "regular" your event sources behave. That is, if you expect little or no variance in the number of messages that arrive for a given time (for example, 8 to 9 am on a weekday), then you can set a low value for the Deviation. Conversely, if you often see peaks and valleys, set the Deviation value higher.
- If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic alerting.

Note: Automatic alerting, and it settings, are currently in Beta testing.



1	Determines whether automatic alerting is on or off. By default, this option is selected (automatic alerting turned on)
2	Determines whether notifications for automatic alerts are on or off. By default, this option is cleared (automatic notifications are not sent when automatic alerts are triggered)
3	The standard deviations below which to receive alerts. Default is **2.0** (95% confidence)
4	The standard deviations above which to receive alerts. Default is **2.0** (95% confidence)
5	When selected, this option stores event source counts per one-hour interval. The data that is collected is used to form the baseline values for each event source. • **Enabled (default)**: one count per hour per event source is stored in the underlying database. These one-hour counts (or aggregations) form the historical basis for computing the normal range for each event source. • **Disabled**: when the SMS Server is restarted, Event Source Monitoring will have no historical data with which to compute the normal range and the user will have to wait until enough data (about a week's worth) is collected to form a new basis for each event source
6	Controls how much historical data (see **Enable Aggregation Persistence**) to maintain for each event source. The default value of 120 days means roughly 4 months of history is

kept and used when reconstructing the basis for each event source

7 When enabled, data about the behavior of the automatic alerting is stored to disk. The default value is **Enabled**.

The data retained includes baseline value over time and the alerting history for each event source. Note, however, the event source address and type is anonymized, so only your event rate information is revealed.

Since automatic alerting is a beta feature, this data is important to measure the efficacy of the feature. This can be disabled without affecting the automatic alerting functionality

8 The **Reset** option discards any unsaved changes for all settings on the page.

9 Click **Apply** to save any changes you made to the values on the page.

Features

The Settings tab contains the following features.

Feature	Description
Enable Automatic Monitoring	Determines whether automatic alerting is on or off. By default, this option is selected (automatic alerting turned on)
Enable Notifications From Automatic Monitoring	Determines whether notifications for automatic alerts are on or off. By default, this option is cleared (automatic notifications are not sent when automatic alerts are triggered)
Low Standard Deviations	The standard deviations below which to receive alerts. Default is **2.0** (95% confidence)
High Standard Deviations	The standard deviations above which to receive alerts. Default is **2.0** (95% confidence)

Feature	Description
Enable Aggregation Persistence	When selected, this option stores event source counts per one-hour interval. The data that is collected is used to form the baseline values for each event source. • Enabled (default): one count per hour per event source is stored in the underlying database. These one-hour counts (or aggregations) form the historical basis for computing the normal range for each event source. • Disabled: when the SMS Server is restarted, Event Source Monitoring will have no historical data with which to compute the normal range and the user will have to wait until enough data (about a week's worth) is collected to form a new basis for each event source
Aggregation Persistence Interval in Days	Controls how much historical data (see **Enable Aggregation Persistence**) to maintain for each event source. The default value of 120 days means roughly 4 months of history is kept and used when reconstructing the basis for each event source
Enable Generation of Analytics	When enabled, data about the behavior of the automatic alerting is stored to disk. The default value is **Enabled**. The data retained includes baseline value over time and the alerting history for each event source. Note, however, the event source address and type is anonymized, so only your event rate information is revealed. Since automatic alerting is a beta feature, this data is important to measure the efficacy of the feature. This can be disabled without affecting the automatic alerting functionality
Reset	This option discards any unsaved changes for all settings on the page.
Apply	Click **Apply** to save any changes you made to the values on the page.

Log Parser Rules Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

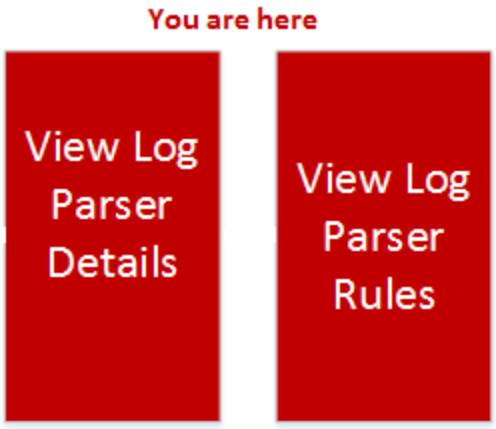
The Log Parser Rules tab displays information about individual log parsers, as well as the default, "parse all" parser that can parse logs that are not associated with a particular log parser. To access this tab, go to **ADMIN > Event Sources > Log Parser Rules**.

This tab contains the following information:

- You can view the rules for a particular event source type, including the default parser.
- You can view the Names, Literals, patterns, and meta for each configured log parser.

Workflow

This workflow is separate from the overall process for configuring event sources.



What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder.	Manage Parser Mappings

Role	I want to...	Documentation
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	*View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Default Log Parser and Log Parser Rules

Creating Event Source Groups

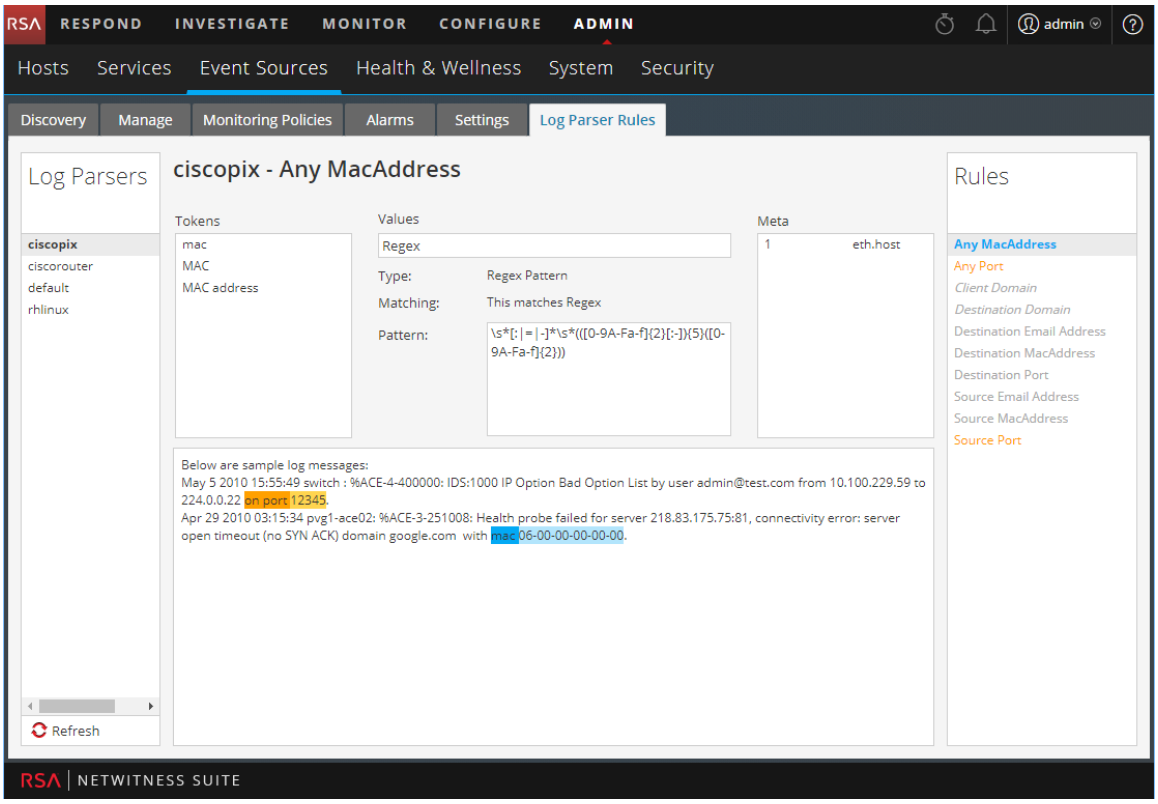
Creating an Event Source and Editing Attributes

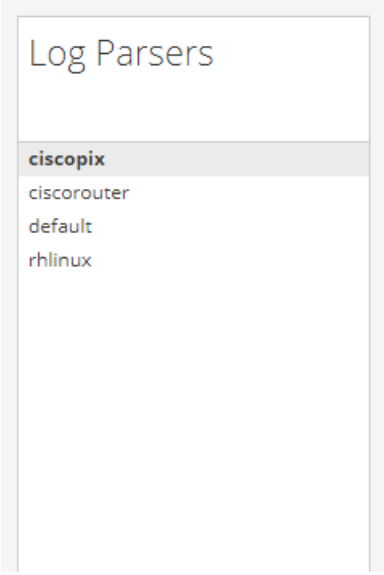
Viewing Logs from Pre-11.0 Log Decoder

Quick Look

Note: The list of log parsers is based on the first Log Decoder that is installed or registered by the Orchestration Server. If you have more than one Log Decoder, this tab only lists log parsers that configured on the first one.

The Log Parser Rules tab organizes displays information about the configured log parsers in your system. This tab consists of three panels: Log Parsers list, Details for the selected log parser, and Rules for the selected log parser.



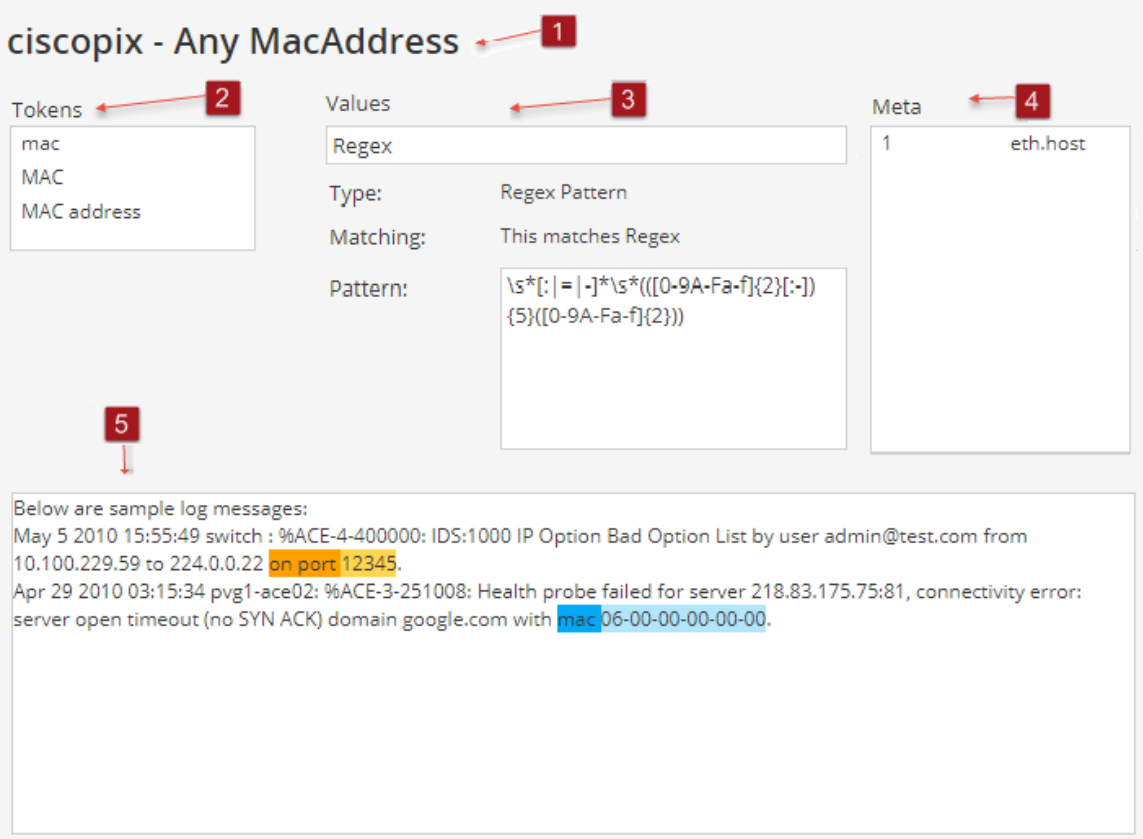


Log Parsers List Panel

The Log Parsers Panel lists the configured log parsers. Select a specific log parser to view its details in the Details and Rules panels.

Details Panel

The details panel shows the token matching, value matching, and mapping information for the selected log parser. Additionally, it shows how a sample log message is parsed.



1	Displays the name of the selected log parser, and the currently selected rule. This value changes when you select a different rule for this parser.
2	Displays the token matching for the selected log parser. The values here are determined by the selected Rule.
3	Displays the type and pattern of the value matching for the selected parser. The values here are determined by the selected Rule.
4	Displays the NetWitness meta to which the selected rule maps any matched tokens. The values here are determined by the selected Rule.
5	Displays a sample log message, and highlights strings that match tokens in the selected log parser. You can edit this field, and add in your own logs to preview how the selected parser will parse your logs.

For example, consider the following scenario:

- The **default** parser is selected.
- The **Any Domain** rule is selected.
- The Tokens matching list displays all of the tokens that are matched when found in a log message: **Domain**, **Domain Name**, **domain**, **ADMIN_DOMAIN**, and so on.

- The Meta list displays the NetWitness meta to which the value for the token is mapped: **domain**.

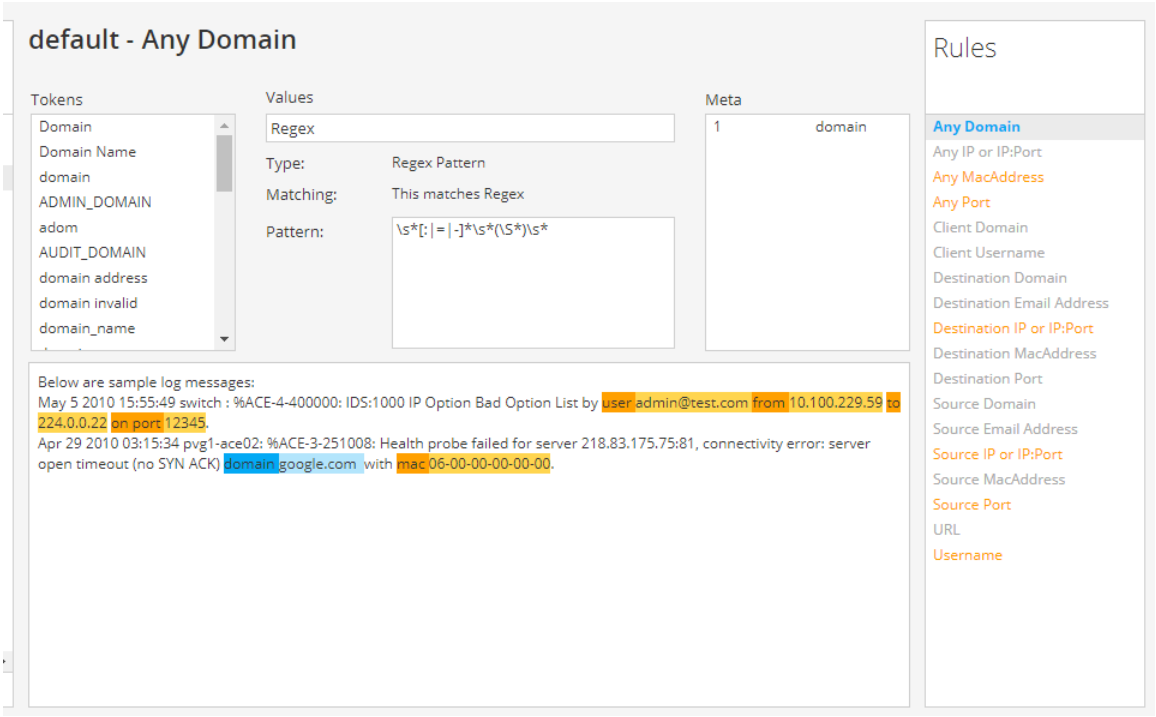
So, let's say the sample log message area has the following text:

Below are sample log messages:

May 5 2010 15:55:49 switch : %ACE-4-400000: IDS:1000 IP Option Bad Option List by user admin@test.com from 10.100.229.59 to 224.0.0.22 on port 12345.

Apr 29 2010 03:15:34 pvg1-ace02: %ACE-3-251008: Health probe failed for server 218.83.175.75:81, connectivity error: server open timeout (no SYN ACK) domain google.com with mac 06-00-00-00-00-00.

In this case, the Sample Log Message area looks like this:



Note that some strings are highlighted, and that there are two "pairs" of highlight colors:

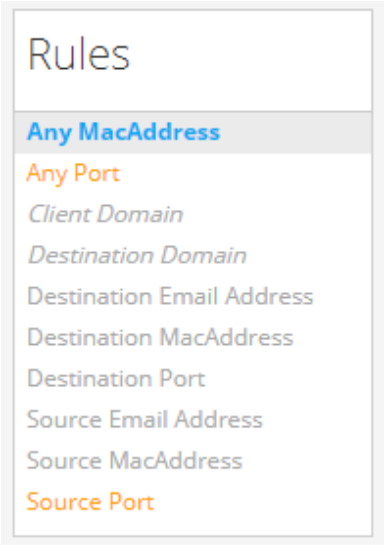
- Dark blue and light blue highlighting is applied to the strings that match the currently selected rule.
  - Dark Blue highlighted strings match a token in the selected rule. In this case, **domain** is the token that is matched for the **Any Domain** rule.
  - Light Blue highlighted strings are the values that correspond to the tokens in dark blue. For example, **google.com** is highlighted in light blue, because it corresponds to the **domain** token.

- Orange and yellow highlighting is applied to the strings that match rules for the current parser that are *not* currently selected.
  - Orange highlighted strings match a token in a rule that is not currently selected.
  - Yellow highlighted strings are the values that correspond to the tokens in orange. For example, the **user** token matches the **Username** rule (which is not currently selected).

In this example, the **domain** meta would be assigned a value of **google.com** for this log message, if it was parsed using the default log parser.

Rules Panel

The Rules panel displays the list of rules used by the selected log parser. When you select a rule, you change the values that are displayed in both the **Tokens** and **Values** areas of the panel.



Note the highlighted rules:

- The currently selected rule is highlighted in blue.
- Other rules that match tokens in the sample log message area are highlighted in orange.

Default Log Parser and Log Parser Rules

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

This tab displays information about pattern matching and rules for the parsers in your system. The features on this tab apply to all log parsers, , including the Default Log Parser

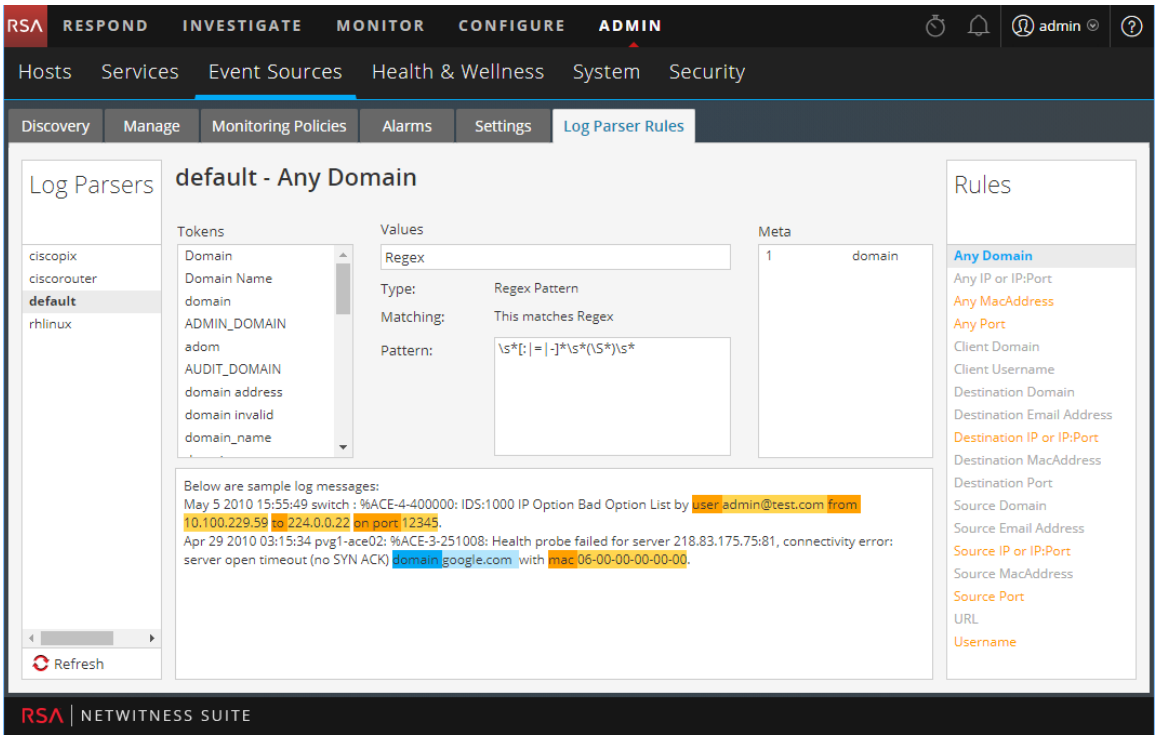
Default Log Parser

The NetWitness Suite default log parser is used to parse logs coming from the Log Decoder that do not match any of the configured log parsers. This default parser parses these logs by using a default set of rules and tokens.

You can view the default log parser and its details by going to **ADMIN > Event Sources > Log Parser Rules** and selecting **default** from the Log Parsers panel.

Note: The list of log parsers is based on the first Log Decoder that is installed or registered by the Orchestration Server. If you have more than one Log Decoder, this tab only lists log parsers that configured on the first one.

This is a view of the Log Parser Rules tab, showing the **Default Log Parser** and **Any Domain** rule selected:



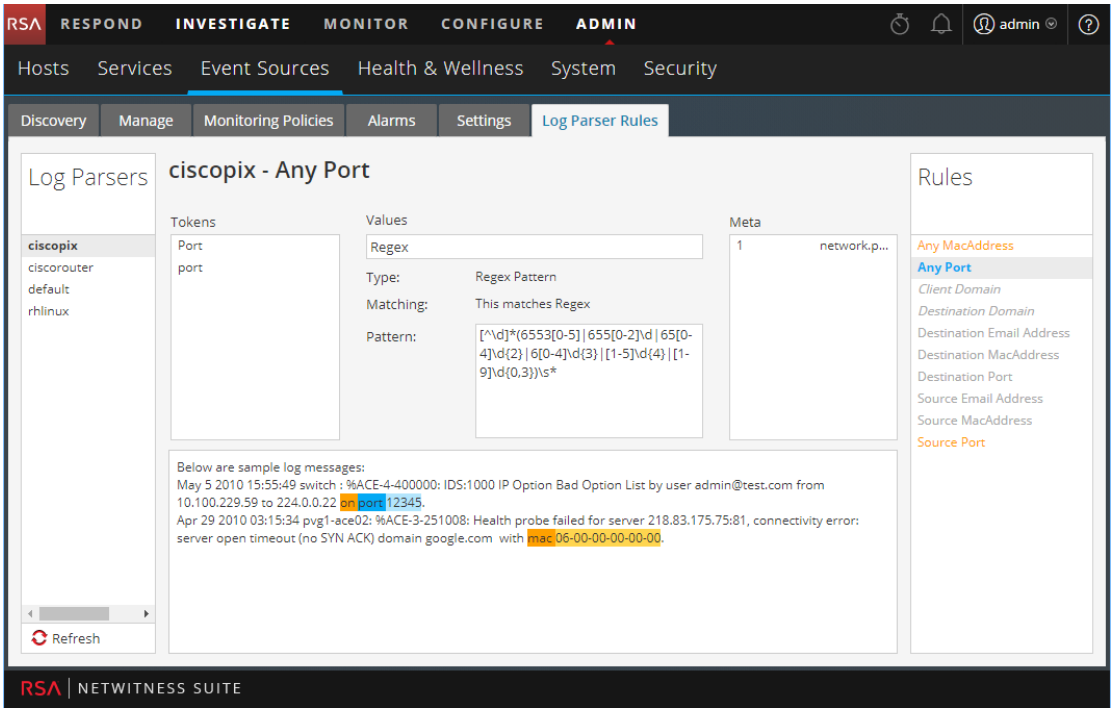
The Log Parser Rules Tab topic describes the items available for the Log Parsers tab.

Highlight Matching Patterns

You can paste logs into the Log Messages text box, and the system highlights the matching literals and patterns for the rules for the selected event source type. Use this feature to confirm that the parser is behaving as expected.

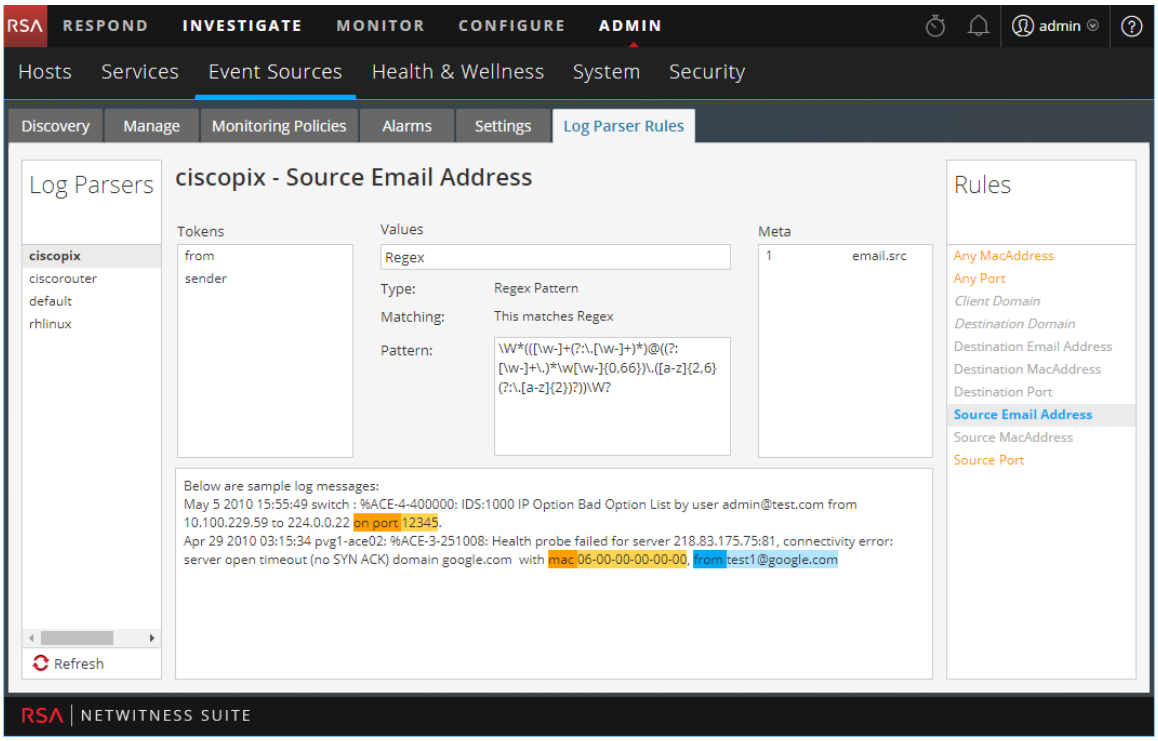
1. In the NetWitness Suite UI, navigate to **ADMIN > Event Sources > Log Parser Rules**.
2. From the **Log Parsers** pane, select a log parser.
3. From the **Rules** pane, select a rule.

   For example, this screen shows the **Any Port** rule for the **cisopix** log parser:



4. Add text or paste in a sample log message.

Strings that match tokens for the selected rule are highlighted in blue. Strings that match other rules for the parser (and the rules themselves) are highlighted in orange.



For example, in the previous screen, note:

- The source email address, matching the **from** token, is highlighted in blue. The token is in dark blue, and the matching string is highlighted in light blue. This is because the **Source Email Address** is the currently selected Rule.
- The strings highlighted in orange match tokens for rules for **Any MacAddress**, **Any Port** and **Source Port**. This is because they are in rules for the **ciscopix** parser that are not currently selected.

ESM Troubleshooting & Appendix

Troubleshooting Topics:

- Alarms and Notifications Issues
- Duplicate Log Messages
- Troubleshooting Feeds
- Import File Issues
- Negative Policy Numbering

Appendix: Viewing Logs from Pre-11.0 Log Decoder

Alarms and Notifications Issues

This topic describes how to address problems you may encounter with alarms or notifications.

Alarms

If you are not seeing alarms that you expect to see, make sure that you have configured all the necessary items, as discussed below.

Automatic Alarms

To see automatic alarms appear on the Alarms screen, the **Enable Automatic Monitoring** option must be selected.

This option is on the **Setting** tab (**ADMIN** > **Event Sources** > **Settings**), and is selected by default. However, at some point someone may have cleared this option.

Manual Alarms

To see manual alarms appear on the Alarms screen, all of the following conditions must be met:

- The event source must be part of a Group.
- The Group must have a policy with either a low or high (or both) threshold defined.
- The Group Policy must be enabled.

Notifications

If you are seeing alarms, but are not receiving the expected notifications, make sure that you have configured all the necessary items, as discussed below.

Also, make sure that you have correctly configured the Notification Servers and Notification Outputs. Much of the preliminary configuration for Notifications is done from **ADMIN > System > Global Notifications**. For details, see the **Global Notifications Panel** topic in the *System Configuration Guide*.

Automatic Notifications

To have the system send automatic notifications, all of the following conditions must be met:

- The **Enable Automatic Monitoring** option must be selected (this option is selected by default).
- The **Enable Notifications From Automatic Monitoring** option must be selected. This option is cleared by default, so you or someone in your organization must select it. Navigate to **ADMIN** > **Event Sources** > **Settings** to see this option.
- The event source that triggered the alarm must be in a group that has a policy enabled: note that no thresholds need to be set for automatic notifications.
- The policy must at least one notification configured (either email, SNMP or Syslog).

Manual Notifications

To have the system send manual notifications (that is, a notification which says that a manual alarm was triggered):

- The event source that triggered the alarm must be in a group that has a group policy enabled.
- There must be a threshold set for the policy.
- At least one notification has been configured for the policy.

Duplicate Log Messages

It is possible that you are collecting messages from the same event source on two or more Log Collectors. This topic describes the problem and ways to troubleshoot the issue.

Details

If the ESM aggregator detects the same events for the same event source on multiple Log Collectors, you receive a warning similar to the following:

```
2015-03-17 15:25:29,221 [pool-1-thread-6] WARN
com.rsa.smc.esm.groups.events.listeners.EsmStatEventListener -
 192.0.2.21-apache had a previous event only 0 seconds ago; likely
because it exists on multiple log collectors
```

This warning message means the `192.0.2.22-apache` event source is being collected by multiple hosts. You can see the list of hosts in the Log Collector column in the **Manage** tab in the Administration > Event Sources view.

Clean Up Duplicate Messages

1. Stop collectd on NetWitness Suite and Log Decoders:

   ```
   Service collectd stop
   ```

2. Remove the ESM Aggregator persisted file on NetWitness Suite:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Reset the Log Decoder.

   a. Navigate to the Log Decoder REST, at `http://<LD_IP_Address>:50102`.

   b. Click **decoder(*)** to view the properties for the decoder.

   c. In the Properties drop-down menu, select **reset**, then click **Send**.

4. In the Event Sources panel from the Event Sources Manage tab, select all event sources and then click − to remove them.

Troubleshooting Feeds

The purpose of the feed generator is to generate a mapping of an event source to the list of groups to which it belongs.

If you have an event source from which you are collecting messages, and yet it is not displayed in the correct event source groups, then this topic provides background and information to help you track down the problem.

Details

The ESM Feed maps multiple keys to single value. It maps the DeviceAddress, Forwarder, and DeviceType attributes to groupName.

The purpose of the ESM feed is to enrich event source Meta with the groupName collected on the Log Decoder.

How it Works

The feed generator is scheduled to update every minute. However, it is triggered only if there are any changes (create, update, or delete) in event sources or groups.

It generates a single feed file with event source to group mapping, and pushes the same feed to all of the Log Decoders that are connected to NetWitness Suite.

Once the feed file is uploaded on the Log Decoders, for any new events, it enriches events Meta data with groupName, and appends this groupName to logstats.

Once the groupName is in logstats, the ESM Aggregator groups information and sends it to ESM. At this point, you should see the **Group Name** column under the **Event Source Monitoring** tab.

The entire process can take some time. Therefore, you may need to wait for several seconds after you add a new group or event source, before the Group name is displayed.

Note: If the event source type attribute changes when the feed is updated, NetWitness Suite adds a new logstats entry, rather than updating the existing one. Thus, there will be two different logstats entries in logdecoder. Previously existing messages would have been listed under the previous type, and all new messages are logged for the new event source type.

Feed File

The format of the feed file is as follows:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

The `DeviceAddress` is either `ipv4, ipv6`, or `hostname`, depending on which of these have been defined for the event source.

The following is a sample of the feed file:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apac
hegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","
Apachegrp"
```

Troubleshooting Feeds

You can check the following items to narrow down where the problem is occurring.

10.5 Log Decoders

Are your NetWitness Suite Log Decoders at version 10.5 or later? If not, you need to upgrade them. For NetWitness Suite version 10.6, feeds are sent only to version 10.5 and later Log Decoders.

Feed File Existence

Verify that the feeds ZIP archive exists in the following location:

`/opt/rsa/sms/esmfeed.zip`

Do not modify this file.

Group Meta Populated on LD

Verify that the group meta is populated on the Log Decoder. Navigate to the Log Decoder REST and check logstats:

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

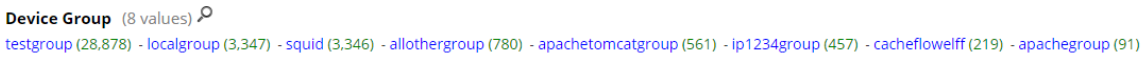
This is a sample logstats file with group information:

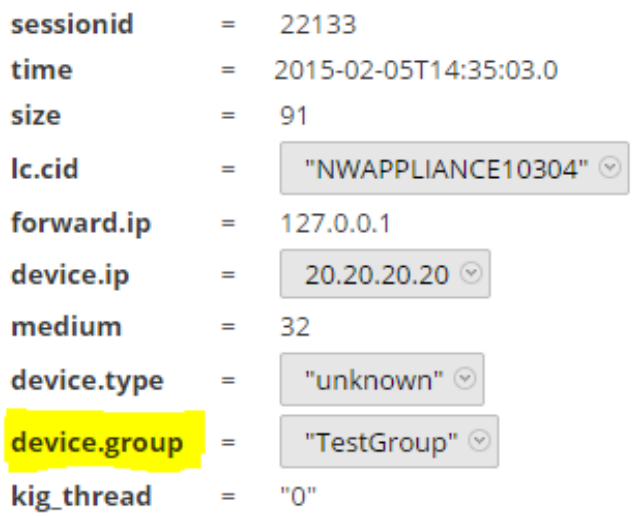
```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4
count=338 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304
source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04
22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19
groups=AllOtherGroup,ApacheTomcatGroup
```

In the above text, the group information is bolded.

Device Group Meta on Concentrator

Verify that the **Device Group** meta exists on the Concentrator, and that events have values for the `device.group` field.





SMS Log File

Check the SMS log file in the following location to view informational and error messages: `/opt/rsa/sms/logs/sms.log`

The following are example *informational* messages:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

The following are example *error* messages:

```
 Error creating CSV File : <reason>Unable to push the
ESM Feed: Unable to create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> :
Error: <error>
Unable to push the ESM Feed: CSV file is empty, make
sure you have al-least on group with al-least one
eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file
on LogDecoder-<logdecoderIP>Unable to push the ESM
Feed: admin@<logdecoderIP>:50002/decoder/parsers
received error: The zip archive
"/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could
not be opened
Unable to push the ESM Feed: <reason>
```

Verify Logstats data is getting Read & Published by ESMReader & ESMAggregator

These are the steps to verify that logstats are collected by **collectd** and published to Event Source Management.

ESMReader

1. On Log Decoders add **debug "true"** flag in **/etc/collectd.d/NwLogDecoder_ESM.conf**:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>
        </stats>
    </Module>
    <Module "NgEsmReader" "update">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>
        </stats>
    </Module>
</Plugin>
```

2. Run the command:

```
collectd service restart
```

3. Run the following command:

   ```
   tail –f /var/log/messages | grep collectd
   ```

   Verify that ESMReader is reading logstats and there are no errors. If there are any read issues, you will see errors similar to the following:

   ```
   Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
   all: error getting ESM data for field "groups" from logstat
   device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
   <reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
   NgEsmReader_update: error getting ESM data for field "forwarder" from
   logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
   ```

ESMAggregator

1. On NetWitness Suite, uncomment the verbose flag in **/etc/collectd.d/ESMAggregator.conf**:

   ```
   # ESMAggregator module collectd.conf configuration file
   #
   # Copyright (c) 2014 RSA The Security Divsion of EMC
   #
   <Plugin generic_cpp>
   PluginModulePath "/usr/lib64/collectd"
   <Module "ESMAggregator">
           verbose 1
           interval "60"
           cache_save_interval "600"
           persistence_dir "/var/lib/netwitness/collectd"
   </Module>
   </Plugin>
   ```

2. Run the following:

   ```
   collectd service restart.
   ```

3. Run the following command:

   ```
   run “tail –f /var/log/messages | grep ESMA
   ```

   Look for ESMAggregator data and make sure your logstat entry is available in logs.

Sample output:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
```

```
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Configure JMX Feed Generator Job Interval

Although the feed generation job is scheduled to execute every minute by default, you can change this by using **jconsole**, if necessary.

To change the feed generator job interval:

1. Open **jconsole** for the SMS service.
2. On the MBeans tab, navigate to **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributes**.
3. Modify the value for the property **FeedGeneratorJobIntervalInMinutes**.

4. Go to **Operations** under the same navigation tree, an click **commit()**. This persists the new value in the corresponding json file under **/opt/rsa/sms/conf**, and uses the value if SMS is restarted.

Setting a new value reschedules the feed generator job for the new interval.

Import File Issues

If your import file is not formatted correctly, or is missing required information, an error is displayed, and the file is not imported.

Check the following:

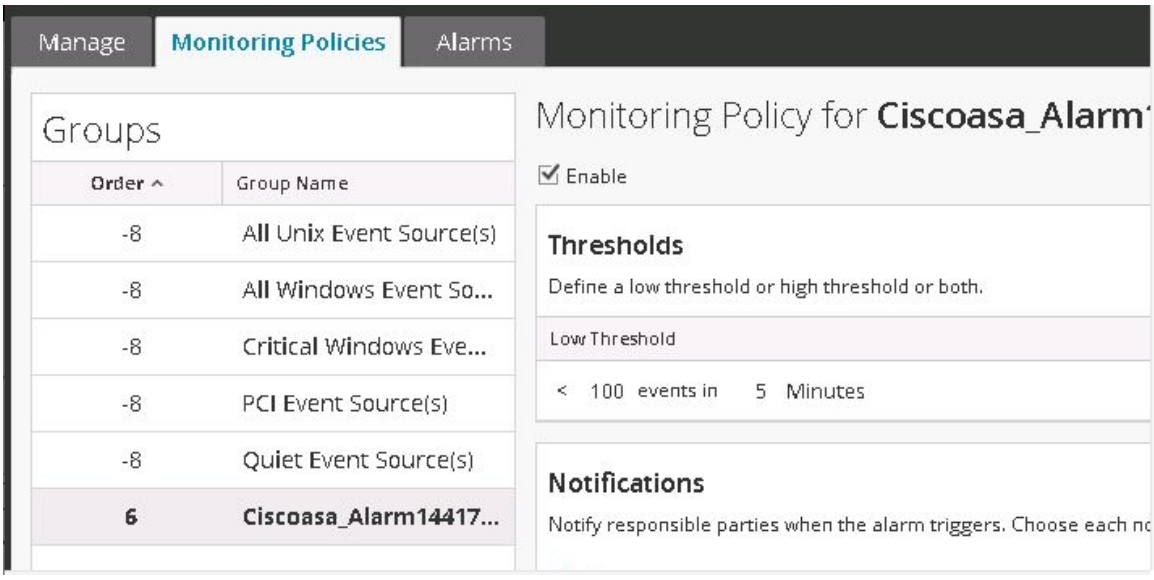
- If you are adding unknown sources, each line in the file must contain a combination of the required attributes:
  - IP or IPv6 or Hostname, and
  - Event Source Type
- The first line of the file must contain header names, and the names must match the names in NetWitness Suite. To get a list of correct column names, you can export a single event source. Examine the exported CSV file: the first row of the file contains the correct set of attribute/column names.

Negative Policy Numbering

You may see negative numbers in the Order field in the Groups section of the Monitoring Polices tab. This topic describes a workaround to restore the correct numbering scheme for your policies.

Details

The following screen shows an example of the situation where the numbers of group policies become negative.



If you encounter this situation, drag and drop the top group (**All Unix Event Source(s)** in the above image) to after the last group (**Ciscoasa_Alarm14417**). This restores normal, ordinal numbering. You can then continue to drag and drop groups until you have them in their proper order for your organization.

Clean Up Duplicate Messages

1. Stop collectd on NetWitness Suite and Log Decoders:

   ```
   Service collectd stop
   ```

2. Remove the ESM Aggregator persisted file on NetWitness Suite:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Reset the Log Decoder.

   a. Navigate to the Log Decoder REST, at `http://<LD_IP_Address>:50102`

   b. Click **decoder(*)** to view the properties for the decoder.

   c. In the Properties drop-down menu, select **reset**, then click **Send**.

4. In the Event Sources panel from the Event Sources Manage tab, select all event sources and then click − to remove them.

Viewing Logs from Pre-11.0 Log Decoder

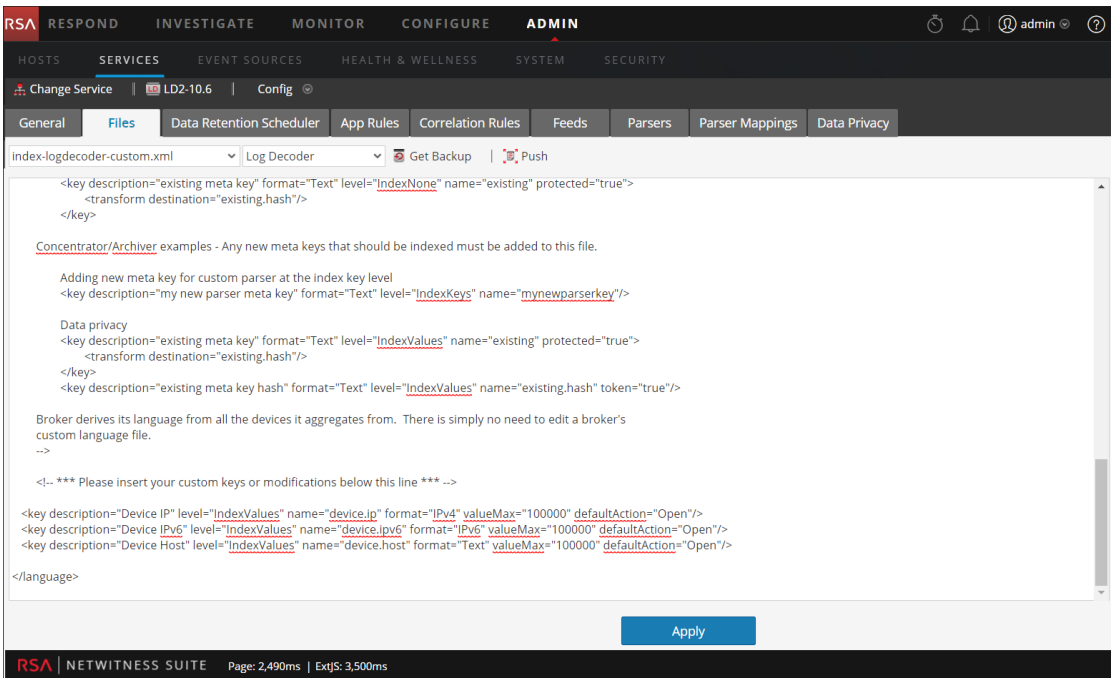
RSA NetWitness® Suite 11.0 added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available.

To enable logs preview for a pre-11.0.0.0 Log Decoder, follow these steps on the Log Decoder:

1. Go to **ADMIN > Services >** select a Log Decoder, then select **> View > Config**.
2. Click **Files** tab, then select **index-logdecoder-custom.xml** from the drop-down menu.
3. Add the following three lines at the end of the file (before the closing language tag):

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
valueMax="100000" defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

4. Click **Apply**.



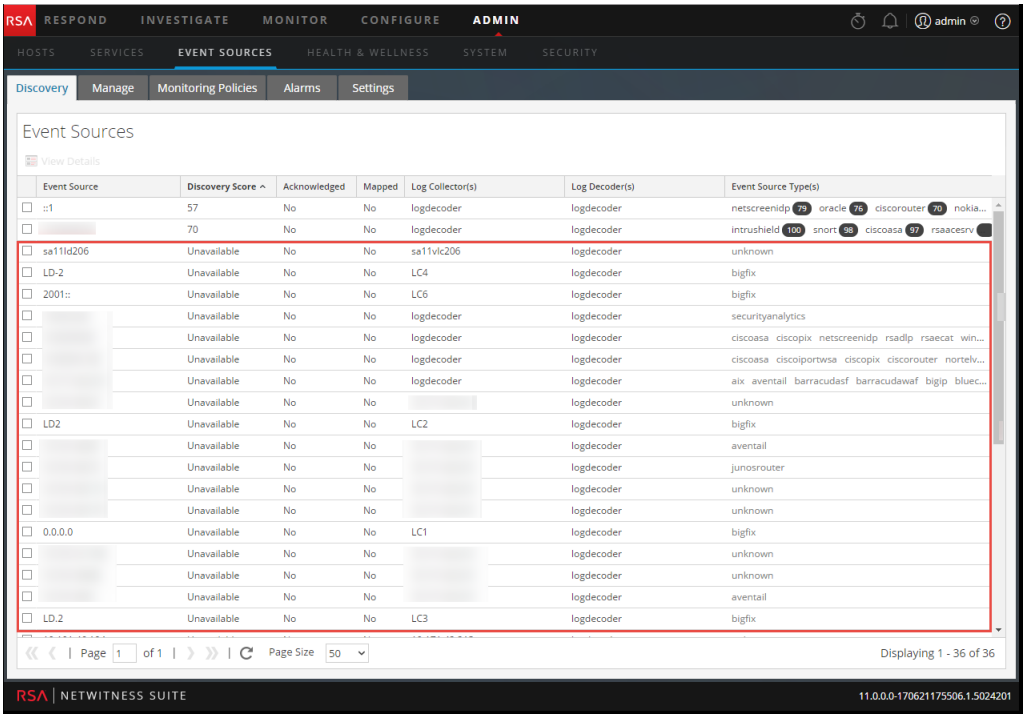
5. Restart the Log Decoder as follows.

   Select **Log Decoder > Explore > sys > Properties > shutdown**

This is an example of the **index-logdecoder-custom.xml** file.

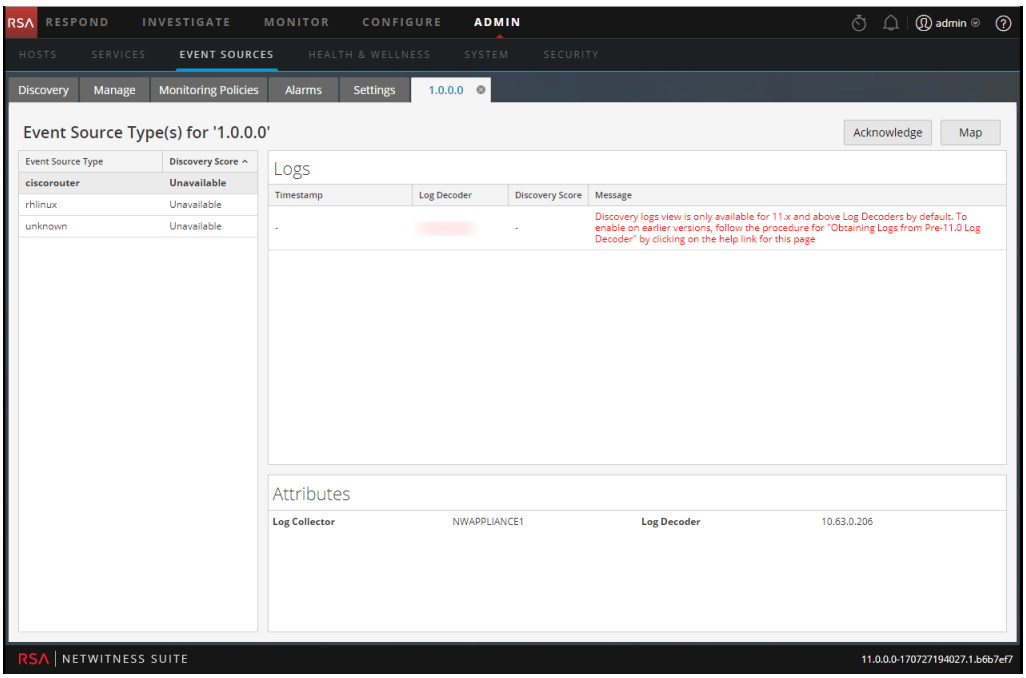
Note: Discovery Scores are only available for 11.0 and above Log Decoders. Discovery Scores for pre-11.0 Log Decoders display as Unavailable.

The following example displays the Discovery Score as **Unavailable** in the **Details** view for a pre-11.0 Log Decoder.



Note: Device logs are only available for 11.0 and above Log Decoders.

The following example shows the message that displays in the displays in the Logs panel for a pre-11.0 Log Decoder.



RSA NETWITNESS® SUITE

RSA NetWitness

Log Parser Tool User Guide

for Version 1.0

RSA

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

NetWitness Log Parser Tool Overview 5

About NetWitness Log Parser Tool 5
Parser Structure 5
Obtaining a Log File 6
Understanding Events 7
How Logs are Parsed in NetWitness 9

Getting Started with NetWitness Log Parser Tool 11

Getting a Log File from NetWitness 12
Creating a Log Parser File 13
Selecting an Event from the Log File 13
Defining a Header 13
Header Order 13
Defining a Message 14
Message Order 15
Editing a Log Parser File 16
Validating the Precedence of Pattern Definitions 16
Viewing Parsed Events and Associated Definitions 16
Custom Table Map Files 17
GitHub Community Link 17

NetWitness Log Parser Tool Workflow 19

Installing the NetWitness Log Parser Tool 19
Setting Preferences 19
Creating a Log Parser 21
Editing an Existing Parser 24
Parser Version 25
Deploying Parsers on a Log Decoder 26
Opening a Log File 27
Auto Splitting Log Files 27
Generating Parsing Summary Report 28
Status Bar 30

Understanding the Log Data Section Workflow 30
Determining the Parser Definition Method 30
Example: Extract Generic Information 30
Defining the Header Pattern 31
Defining the Message Pattern 34
Defining a Throw-away Variable 35
Adding a Constant Function 35
Adding an Event Time Function 36
Event Time Function Formatting Characters 36
Adding a Custom Table Map 37
Deleting a Message 38
Using Undo and Redo 38

Log Filter Functionality 39

Parser Header and Message Search Functionality 41

Header Search Functionality 41
Message Search Functionality 42

Advanced Search Options 44

Advanced Log Filter Options 44
Advanced Header Search 45
Advanced Message Search 46

TAGVALMAP Feature 47

Using the TAGVALMAP Feature 47
Setting Up a Header and Creating a Message 48

NetWitness Log Parser Tool Overview

About NetWitness Log Parser Tool

NetWitness Log Parser Tool (NwLPT) is a graphical tool that enables you to create and edit log parsers that run on the NetWitness Log Decoder. Using the NetWitness Log Parser Tool, you can define how a NetWitness Log Decoder identifies, parses, and extracts information from the events of a specific event source. These parser definitions are stored as an XML file, called a log parser XML file, which is deployed on the NetWitness platform.

You can create a new log parser for an event source that is not currently supported by NetWitness. You can also edit an existing log parser to add or edit definitions for events, or to correct errors. You may need to edit an log parser in one of the following situations:

- You upgrade to a new version of an event source that contains new, updated, or deprecated log messages.
- You want to include additional definitions in existing events.
- You want to update the definition for an existing event in a log parser.

Parser Structure

The NetWitness Log Parser Tool uses the device type of the log parser to create the structure for the parser. The NetWitness Log Parser Tool also appends the device type to the directory that you specify for your parser.

When you create an log parser, you select a device type for it. The device type must start with a letter. The RSA naming convention is to make the device type all lowercase and remove the spaces. For example, Cisco ASA would have the device type **ciscoasa** and Actiance Vantage would be **actiancevantage**. It is not necessary to follow the RSA naming convention to use this tool.

In your log parser directory, the NetWitness Log Parser Tool creates two files with the correct name for NetWitness:

- **INI file.** This is the parser configuration file. (Example: ciscoasa.ini)
- **XML file.** This is the log parser XML file that contains the parser definitions. (Example: ciscoasamsg.xml). The device type is appended with **msg**.

Both of these files are required to deploy your parser in NetWitness.
When you finish creating or updating your parser, you have the option of retrieving the completed parser in four formats:

- **Individual Files: Parser (.XML) and Configuration (.INI)** (In the main menu, select **File > Save** or **Save As**) This option creates a device type folder containing an XML file and a configuration INI file. These individual files are good to view the raw Parser and Configuration files, but they cannot be imported directly into a NetWitness Log Decoder.
- **Parser Package: .envision** (In the main menu, select **Actions > Export Parser**) This option creates an event source package that consists of the log parser XML and configuration INI file. This format is used to import the event source to a Log Decoder directly.
- **Live Resource: .zip** (In the main menu, select **Actions > Export Resource**) This option creates an event source package in a .zip format that consists of all the log parser XMLs and configuration INI files. The .zip format can be used to deploy parsers through RSA Live. It enables deployment of parsers to multiple Log Decoders simultaneously.
- **To deploy a parser on a Log Decoder** (In the main menu, select **Actions > Deploy Parser**) This option enables you to deploy the parser directly to the Log Decoder. It also supports deployment of parsers to multiple Log Decoders simultaneously. For more information, see Deploying Parsers on a Log Decoder.

See the "Download Log Parsers from Live and Deploy from Local Network" topic in the *RSA Content and Resources* documentation for information on how to upload the event source log parsers from your local network to the NetWitness Log Decoder.

See the "Deploy Resources from a Resource Package" topic in the *Live Services Management Guide* for Version 11.0 for information on how to upload the event source log parsers from your local network to the NetWitness Log Decoder at the following location: https://community.rsa.com/docs/DOC-74332.

See the "Enable and Disable Parsers and Log Parsers" topic in the 11.0 *Decoder and Log Decoder Configuration Guide* for Version 11.0 at the following location: https://community.rsa.com/docs/DOC-74332.

Obtaining a Log File

To create a log parser that a NetWitness Log Decoder can use to identify, parse, and extract information from a specific event source, you must obtain a log file from the event source that you want to integrate with NetWitness. After you obtain the log file, you can use NetWitness Log Parser Tool to create a log parser.

Before getting started with NetWitness Log Parser Tool, you must know the log collection protocol that was configured when the event source was deployed with NetWitness.

If the log collection protocol that you configured when you set up the event source in NetWitness is Syslog, you can use a log file generated by the event source to create or edit a log parser.

If you configured any other log collection protocol, you must export a log file from NetWitness in text format.

RSA recommends that you compile a log file that contains all the unique events generated by the event source that you want to integrate with NetWitness. While compiling the log file, ensure that:

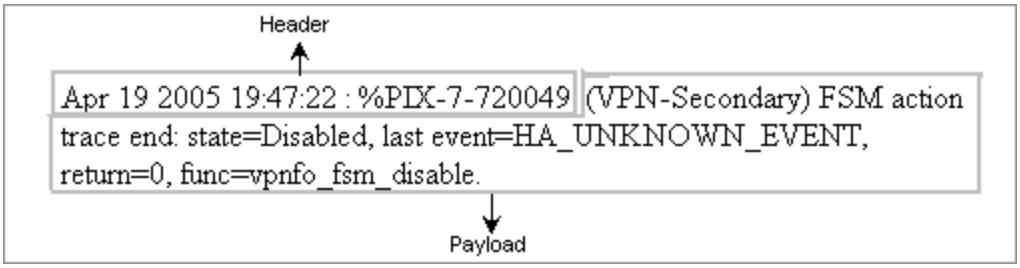
- All the events are from a single event source.
- Each event is listed in a single line, without any line breaks.
- The maximum size of any event is 64 KB.
- The log file contains one or two instances of each unique event.

Note: The recommended maximum size of the log file is 25 MB. A larger file can be used, but it will take more time to load and parse.

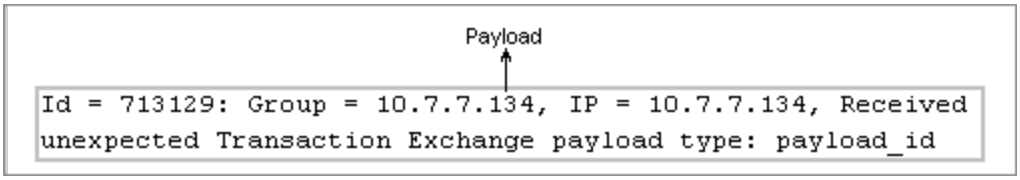
For events transmitted by Syslog, you can put the raw logs directly in the NetWitness Log Parser Tool. For all other event formats, you need to get the log data from NetWitness.
To get log data from NetWitness, see Understanding Events.

Understanding Events

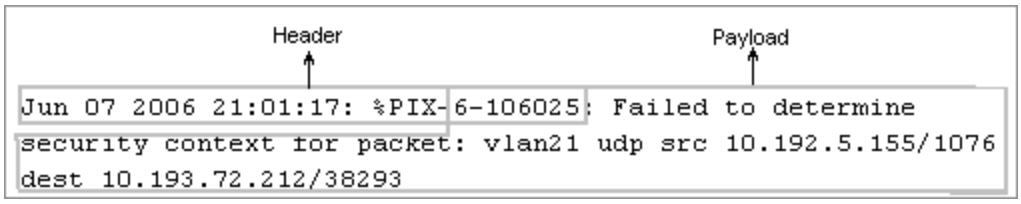
Typically an event consists of two main elements, a header and a payload. The following figure shows an example of an event with a header and a payload.



In some events, you may define the entire event as payload as shown in the following figure.



In some events, you may define the payload to begin from the header, and the header and payload may overlap.

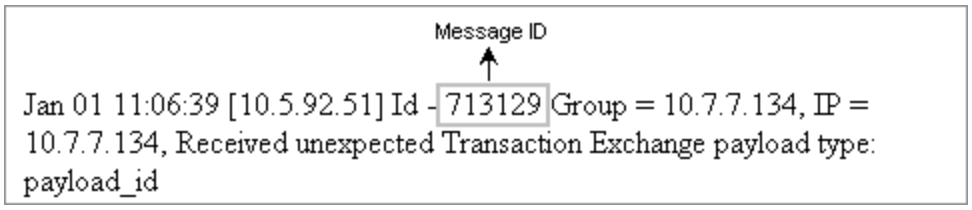


Header

The header consists of the following elements, which are common across multiple events:

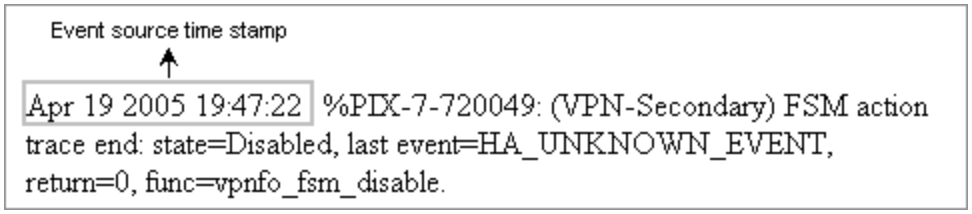
MessageID . Indicates a unique identifier for the message in the event. In the examples in the following figures, the MessageID is unique to the event.

Note: Make sure to define a single MessageID for each header.

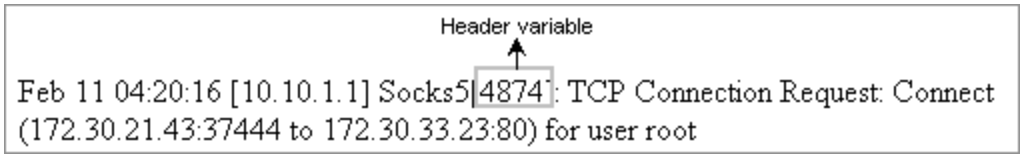


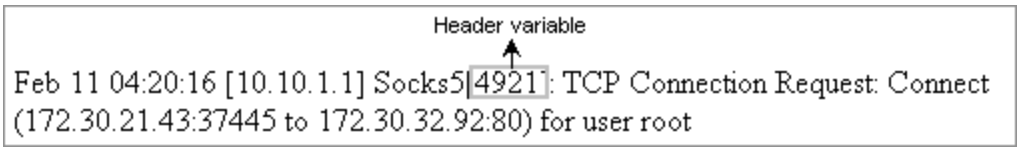
Caution: If you create a header that is too generic and can be used to identify a wide variety of logs, it could match logs that are currently parsed through other parsers.

. (Optional) Consists of the date and time when the event was generated by the event source. Some events may not contain an event source time stamp.



Header Variable. (Optional) Contains a value in the event header that varies across similar types of events. In the examples in the following figures, 4874 and 4921 are header variables that indicate the session ID in the events.

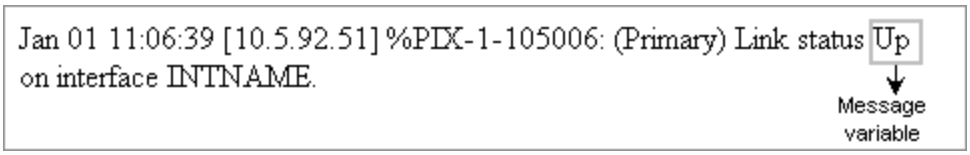


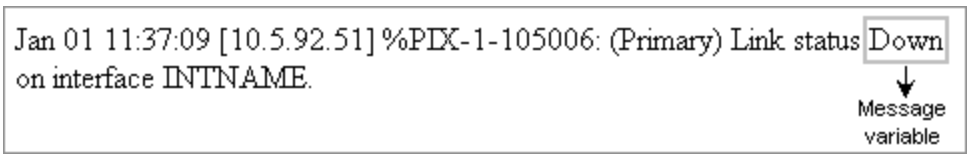


Payload

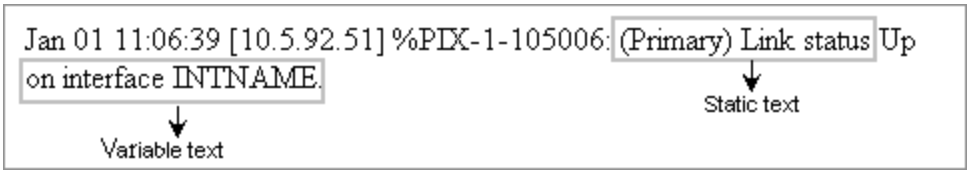
The payload is everything in the event that is not the header. It contains detailed information about the event. The payload is the message in the event. NetWitness uses this information for analysis and reporting. The payload consists of message variables and static text.

A message variable is a value in the payload that varies across similar types of events. In the examples in the following figures, Up and Down are message variables that indicate the link status of the INTNAME interface.



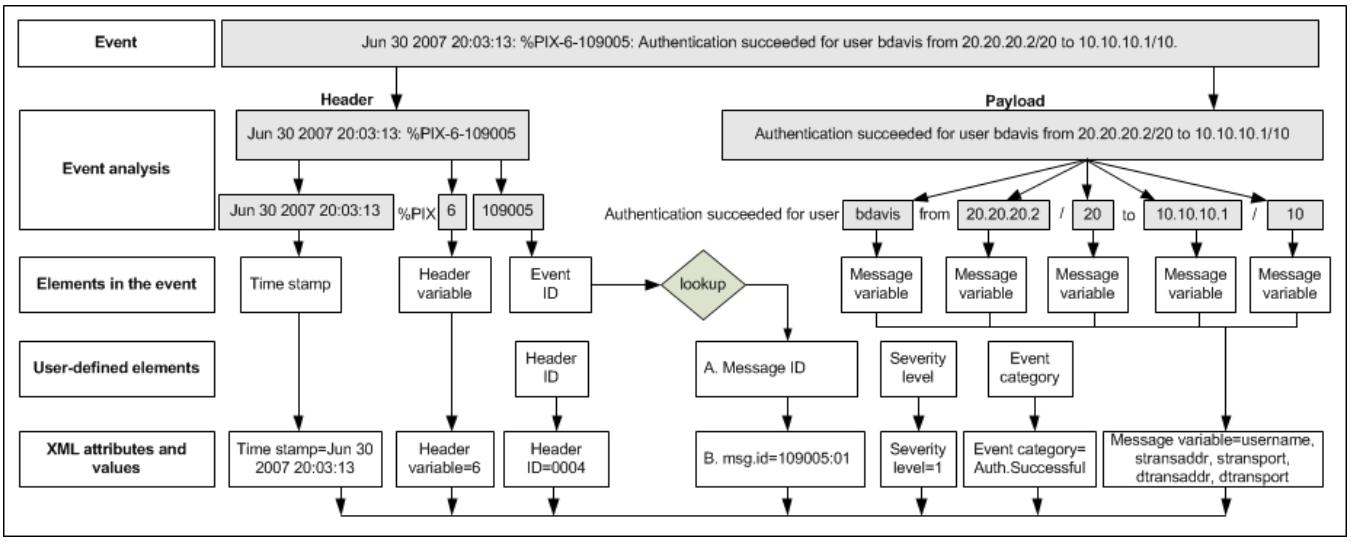


NetWitness Log Parser Tool classifies all the values in the payload that are not message variables as static text. The following figure shows an example of values that NetWitness Log Parser Tool classifies as static text.



How Logs are Parsed in NetWitness

The following figure shows an example of how you can create an XML definition that makes the event data available for analysis and reporting in NetWitness. It also shows the various elements in an XML definition.


Event
Jun 30 2007 20:03:13: %PIX-6-109005: Authentication succeeded for user bdavis from 20.20.20.2/20 to 10.10.10.1/10.
Header
Payload
Event analysis
Jun 30 2007 20:03:13: %PIX-6-109005
Authentication succeeded for user bdavis from 20.20.20.2/20 to 10.10.10.1/10
Jun 30 2007 20:03:13
%PIX
6
109005
Authentication succeeded for user
bdavis
from
20.20.20.2
/
20
to
10.10.10.1
/
10
Elements in the event
Time stamp
Header variable
Event ID
lookup
Message variable
Message variable
Message variable
Message variable
Message variable
User-defined elements
Header ID
A. Message ID
Severity level
Event category
XML attributes and values
Time stamp=Jun 30 2007 20:03:13
Header variable=6
Header ID=0004
B. msg.id=109005:01
Severity level=1
Event category= Auth.Successful
Message variable=username, stransaddr, stransport, dtransaddr, dtransport

Getting Started with NetWitness Log Parser Tool

The following table provides a high-level overview of the tasks that you can perform using NetWitness Log Parser Tool.

Goal	Task	Reference
Integrate an event source that is not supported by NetWitness.	1. Create a parser file that contains definitions for the events generated by the event source.	Creating a Log Parser File
	2. (Optional) View events that are parsed by a header or message definition.	Viewing Parsed Events and Associated Definitions
	3. (Optional) View the header and message definition that parse a selected event.	Viewing Parsed Events and Associated Definitions
	4. Create an event source package for deployment to a NetWitness Log Decoder.	Parser Structure
	5. In NetWitness, deploy the event source package.	Deploying Parsers on a Log Decoder See the "Add or Update Supported Event Source Log Parsers" topic in the *RSA Content and Resources* documentation. The "Download Log Parsers from Live and Deploy from Local Network" section provides information on how to upload the event source log parsers from your local network to the NetWitness Log Decoder.

Goal	Task	Reference
Upgrade an event source that is already supported by NetWitness.	1. Edit the existing log parser file.	Editing a Log Parser File
	2. (Optional) View events that are parsed by a header or message definition.	Viewing Parsed Events and Associated Definitions
	3. (Optional) View the header and message definition that parse a selected event.	Viewing Parsed Events and Associated Definitions
	4. In NetWitness, deploy the event source package.	Deploying Parsers on a Log Decoder See the "Add or Update Supported Event Source Log Parsers" topic in the *RSA Content and Resources* documentation. The "Download Log Parsers from Live and Deploy from Local Network" section provides information on how to upload the event source log parsers from your local network to the NetWitness Log Decoder.

Getting a Log File from NetWitness

1. In the **NetWitness** menu, go to **Investigate > Events**.
2. In the **Investigate** dialog, select a Log Decoder, Archiver, Concentrator, or Broker service and click **Events**In the **Events** view, select the events and in the Actions menu, select **Export > Export All Logs**.
3. In the **Enter file name for extraction** dialog, enter a name for your log file and click **OK**.
4. In the **Export Log Format** dialog, select **Text** and click **Export**.
   You will receive a Scheduled Job notice.
5. Check the Job Notifications tray to view the status of the log file. Click the **View** link to go the Jobs panel in the Profile view to download the log file.

Creating a Log Parser File

Creating a log parser file involves creating a definition for each type of event in the log file generated by an event source. Creating an event definition involves the following tasks:

- Selecting an Event from the Log File
- Defining a Header
- Defining a Message

Selecting an Event from the Log File

Select an event from the log file to define the various elements of the header and message in the event.

Defining a Header

Define the header by assigning the values in the event to header elements. The purpose of defining a header is to identify the event source from which the event is generated. When you define a header with all its elements, the definition can parse similar types of events in the log file.

RSA recommends that you define a generic header definition that will parse multiple events that follow similar formats. The NetWitness Log Parser Tool generates a unique identifier, the HeaderID, for each header definition to identify the header definitions available in the log parser XML file. However, you can change the generated identifier to provide a unique HeaderID of your choice.

You can include the following elements when defining how to locate the MessageID in the header:

- MessageID, used in the Event ID lookup, which enables you to specify one of the following options:
  - MessageID variable
  - Variable suffix
  - Concatenation

Header Order

Header order determines the precedence of the headers. In general, headers should be ordered from specific to generic (see Validating the Precedence of Pattern Definitions).

A header's position can be changed by selecting the header and using **Move Up/Down** menu items on the **Edit** menu (or using the keyboard shortcuts for the up and down arrow keys (**Ctrl+Up** and **Ctrl+Down**). You can also right click on a header or message to bring up a popup Context menu that has options to move up and down.

For more information on these elements, see Understanding Events.

Defining a Message

Define the message by assigning the values in the payload to message variables and defining message elements. A single message definition may parse one or more similar events in your log file.

The following table lists the message elements that you must define.

Message Element	Description
MessageID	Indicates the identifier by which NetWitness identifies the event uniquely. The MessageID can be defined in one of the following ways: • Same as the event ID. • A combination of the event ID defined in the header definition and a unique variant. For example, if the event ID is 109801, the MessageID can be defined as 109801:02. • A brief description that identifies the event. For example, in the following event, the event ID is 187698, and the MessageID can be defined as CableFailover. `Jan 01 11:06:39 [10.5.92.51] %PIX-1-101001: (PRIORITY) Error reading failover cable status.` **Note:** Make sure to define a single MessageID for each header..
Event category	Indicates the category to which the event belongs, based on the NetWitness taxonomy.

Message Element	Description
Functions	(Optional) Define actions to be performed on variables in an event to generate user-defined values. The NetWitness Log Parser Tool supports the following functions: • **Assign Constant** assigns user-defined values to variables. • **Assign Message Variable** assigns the value of a message variable to another variable. • **Calculation** performs a calculation on values and variables in the event. • **Convert Domain** converts domain names to IP addresses. • **Event Time** assigns the date and time information in the event to a message variable. • **Remove Quotes** removes quotes from a variable. • **URL Part** extracts parts of a URL string.

Message Order

All messages are displayed in order by message group. Messages with differing message group values cannot be re-ordered. However, messages with the same group can be re-ordered, as order determines the precedence within the group. In general, messages within a group should be ordered from specific to generic (see Validating the Precedence of Pattern Definitions

When applicable, a message's position within its message group can be changed by selecting the message and using the **Move Up/Move Down** menu items on the **Edit** menu (or using the keyboard shortcuts for the up and down arrow keys (**Ctrl+Up** and **Ctrl+Down**). You can also right-click to open a context menu with the **Move Up/Move Down** options.

When creating a new message or editing the group of an existing message, the message is (re)positioned based on the new message group value. If there are existing messages with that group value, the message is positioned at the end of the message group.

Editing a Log Parser File

Before you edit a log parser file, identify and analyze the events in the corresponding log file. You can edit a log parser file that was created by the NetWitness Log Parser Tool or any other source.

Editing a log parser file involves the same header and message definition tasks as creating a log parser file. However, you may not need to define the header pattern if the headers are all defined. For example, you may want to edit a parser to add new messages to Windows or other platforms. You may also want to adjust an existing parsed message. For example, you may need to change IP source to IP destination in a particular event.

Validating the Precedence of Pattern Definitions

It is important to consider the precedence of pattern definitions when defining headers and messages with the same event ID.

You must arrange the definitions in the log parser file in order from specific to generic so that events are parsed against the specific header or message definition.

For example, suppose that a log parser file contains the following message definitions:

- Message 10123 < A B C >, where A, B, and C are elements in the message
- Message 10124 < A B C D >, where A, B, C, and D are elements in the message

If the order of the message definitions is as shown, NetWitness parses an A B C event from the event source using the Message 10123 definition. NetWitness also parses an A B C D event from the event source using the Message 10123 definition. The A B C D event must be parsed against the Message 10124 definition, which is specific. Therefore, you must ensure that the specific definition, Message 10124, appears before the generic definition, Message 10123, in the log parser file, as follows:

- Message 10124 <A B C D>
- Message 10123 < A B C >

After validating the log parser for data pattern warnings, you must validate the precedence of the header and message definitions in the log parser file.

The NetWitness Log Parser Tool displays the errors that occur in the header and message definition order. For better analysis and reporting, you must resolve all the precedence errors.

Viewing Parsed Events and Associated Definitions

After defining the log parser , you can view the highlighted header and message definitions in the parsed logs within the NetWitness Log Parser Tool. You can also view the header and message definition for a selected event in the log file.

While defining the log parser, you can view parsed events and the associated header and message definitions. For example, if you have defined two header definitions and one message definition in the log parser file, you can view parsed events for these definitions, and then continue to define more header and message definitions depending on the parsed events already viewed.

Custom Table Map Files

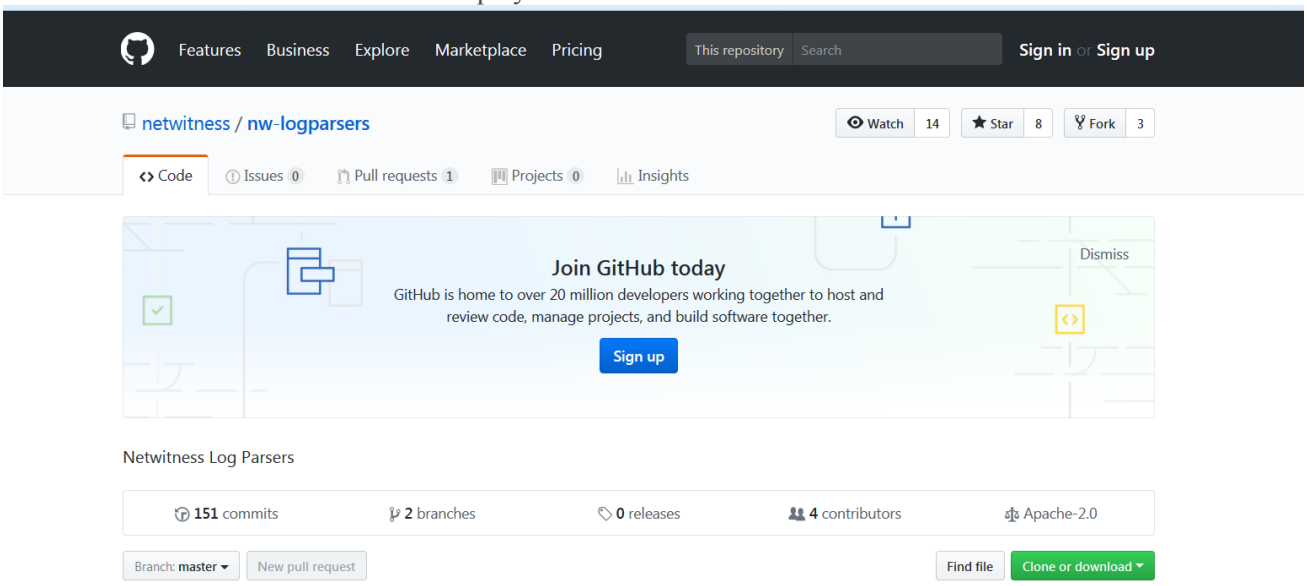
If you changed the table map file (**table-map.xml**) or created a custom table map file (**table-map-custom.xml**), get the changed table mapping files from NetWitness. You can add these custom table map files to the NetWitness Log Parser Tool.

GitHub Community Link

The GitHub Community link provides access to a repository where you can share and contribute event source log parsers for the NetWitness Log Decoder.

To access the GitHub Community Link:

1. From the GitHub Welcome screen, go to **Help > Parser Community**. You can also use the keyboard shortcut **F3** to access the GitHub Community Link.
   The GitHub Welcome screen is displayed.



GitHub members can contribute to the repository by adding or editing a log parser by raising a Pull Request that is reviewed by NetWitness Engineers. As a member of the GitHub community, you can create a new log parser for an event source that is not currently supported by NetWitness and share it with the NetWitness community. You can also edit an existing log parser to add or edit definitions for events, or to correct errors.

You may need to edit an log parser in one of the following situations:

- You upgrade to a new version of an event source that contains new, updated, or deprecated event messages.
- You want to include additional definitions for existing events.
- You want to update the definition for an existing event in a log parser.

NetWitness Log Parser Tool Workflow

The following figure shows the workflow of the NetWitness Log Parser Tool user interface.

Installing the NetWitness Log Parser Tool

You can download the Windows and MacOS versions of the NetWitness Log Parser Tool from the following location:

https://community.rsa.com/docs/DOC-85016

If you are using a Beta version of the Event Source Integrator Tool, you need to un-install Event Source Integrator and download the new NetWitness Log Parser Tool installer from the following location:

https://community.rsa.com/docs/DOC-85016

Note: The Recent Parsers and Open Recent sections are empty, since this is a new installer.

Setting Preferences

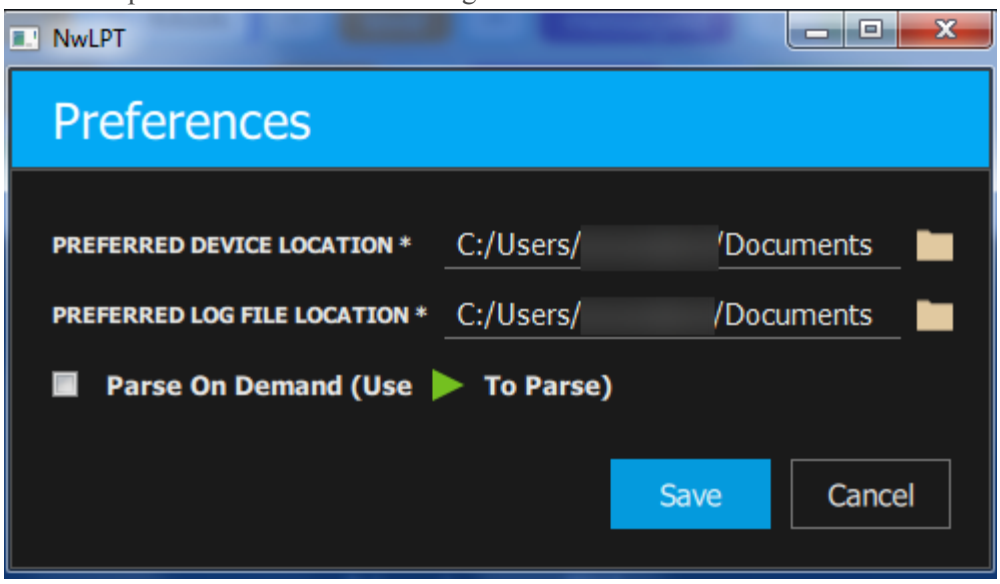
The Preferences dialog allows you to provide paths for logs and parsers, and to select a parsing mode for the application.

Note: The default path is your Documents folder and the default parsing mode is Auto.

To access the Preferences settings:

- For Windows systems: From the main menu, go to **File > Preferences**.
- For MacOS systems: From the NetWitness Log Parser Tool menu, select **Preferences**.

An example of the Preferences settings is shown below.



The default paths and modes are explained in the following table.

Field	Description
Preferred Device Location	• Default directory that is opened when you open an existing parser. • The default directory is the location where a new parser is created. • Imported parsers are saved in this directory by default.
Preferred Log File Location	Directory that the NetWitness Log Parser Tool opens when you want to load a log file.

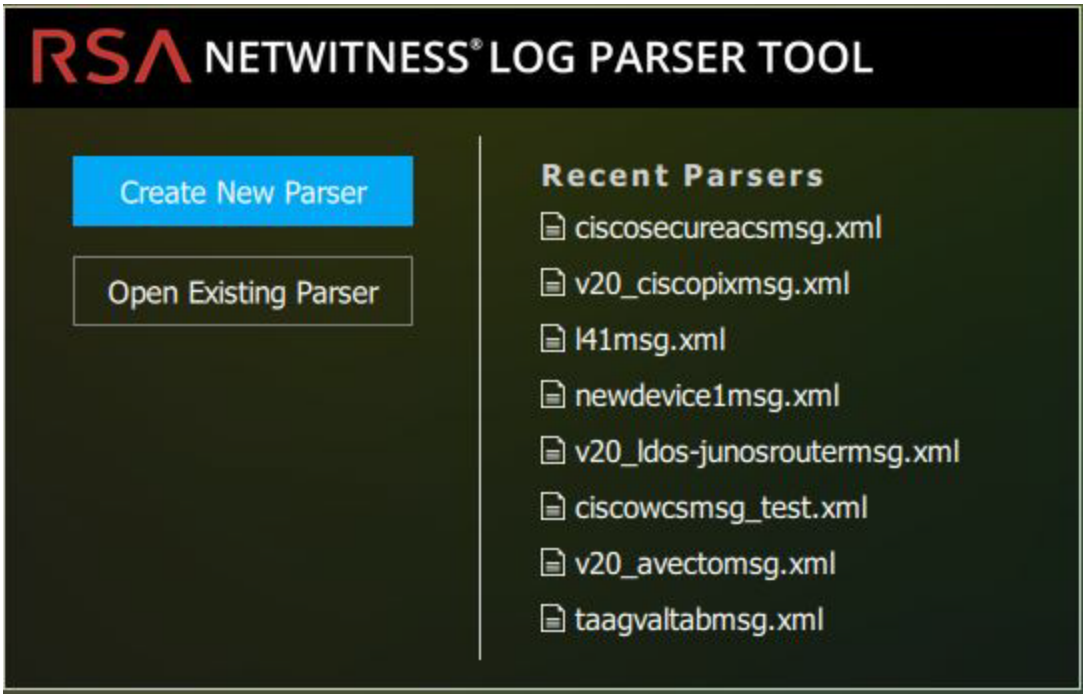
Parsing Mode	By default, the NetWitness Log Parser Tool uses **Continuous Parse** mode, which means the log file is reparsed whenever there is a change to the parser. **Note:** You can change the mode to **Parse On Demand** if you notice that it is taking a while to parse the log file. A Play icon ( ) is displayed in the middle divider that can be used to parse the log when a sufficient number of changes is complete. You can also use the **F5** keyboard short-cut to facilitate log file parsing.

Creating a Log Parser

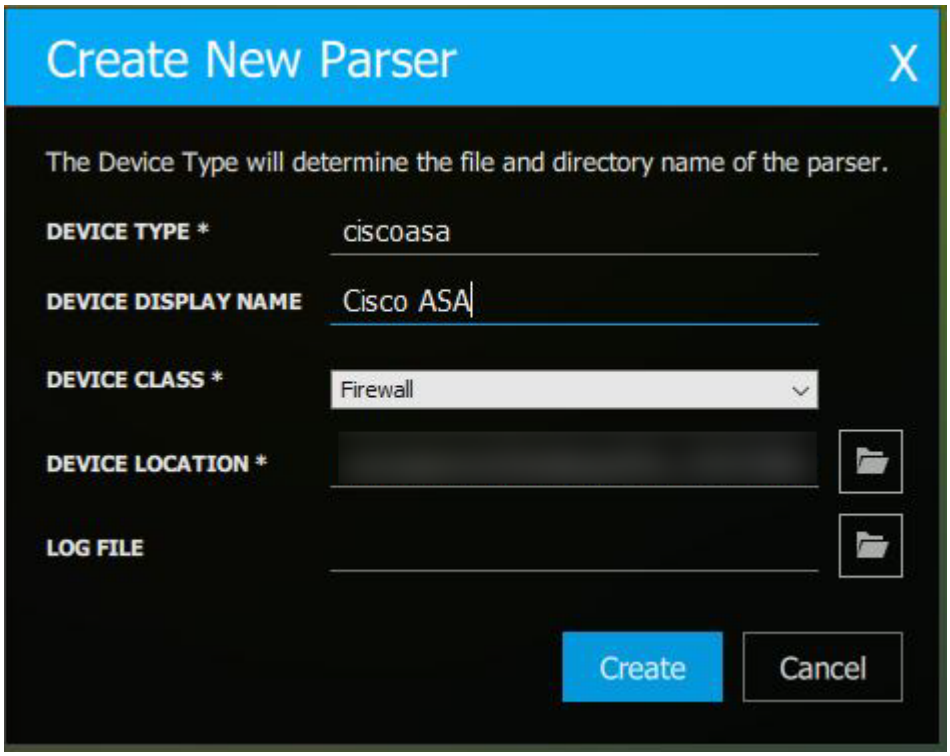
Note: All parsers opened in the tool are auto-saved as backups at an interval of 30 seconds. The last saved time is displayed in the Status Bar of the tool. If you experience unexpected system or performance issues while creating parsers, the auto-saved content acts as a backup of your work.

To create a new parser, follow these steps.

1. Select **Create New Parser**.



The **Create New Parser dialog** is displayed.



2. In the **Create New Parser** dialog:
   a. Enter the **Device Type**. The **Device Type** must start with a letter. The RSA naming

convention is to make the device type all lowercase and remove the spaces. For example, Cisco ASA would have the device type **ciscoasa** and Actiance Advantage would be **actianceadvantage**. It is not necessary to follow the RSA naming convention to use this tool. The device type provides additional information about the event.

Note: Special characters are not allowed for the Device Type.

b. Enter the **Device Display Name**. For example, Cisco ASA.
c. Select a **Device Class** from the drop-down menu. For example, Firewall.
d. In the **Device Location** field, specify the directory where you want to create the parser. In the directory that you specify, the NetWitness Log Parser Tool creates two files with the correct name for NetWitness:

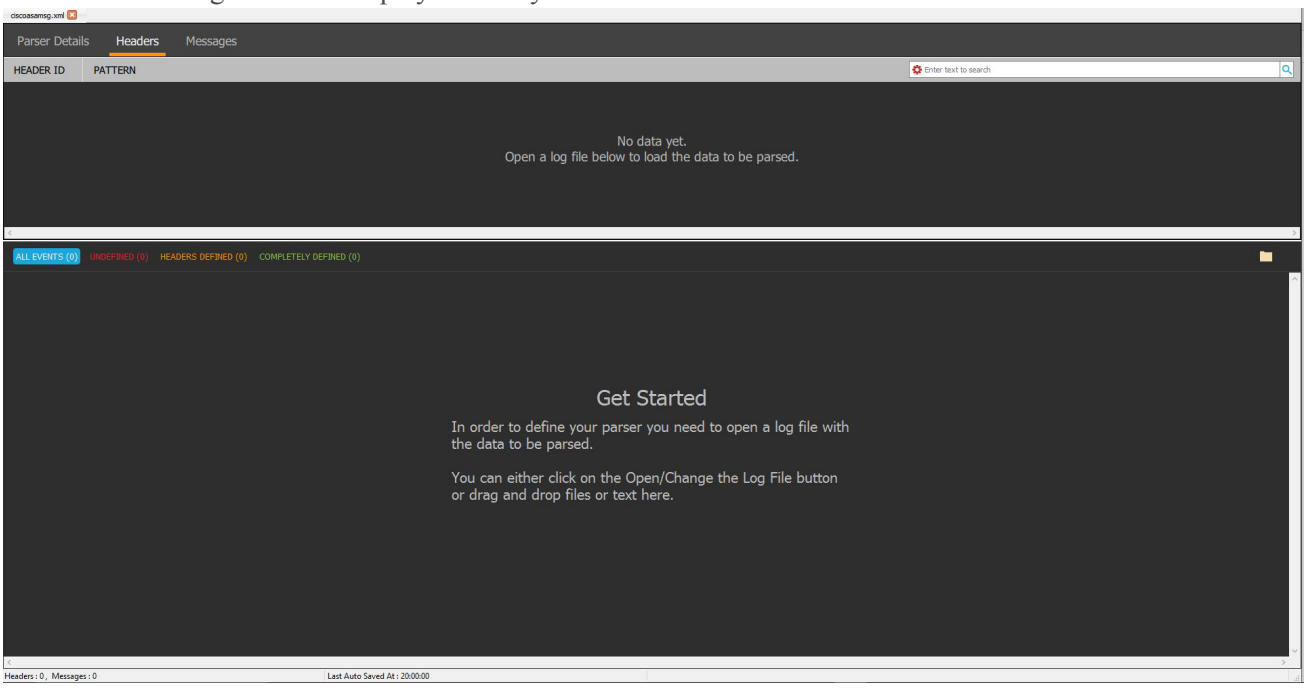
INI file (Example: ciscoasa.ini)

XML file (Example: ciscoasamsg.xml) The device type is appended with **msg**.

Note: The parser path that is set in the **Preference** page is auto-populated here.

e. In the **Log File** field, select a log file. This field is optional and can be selected at a later time.

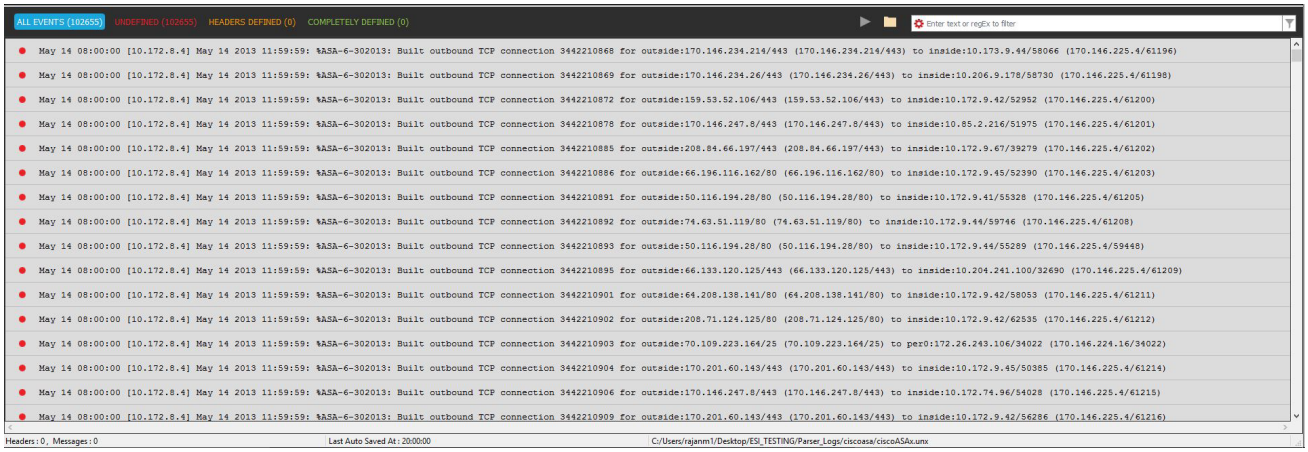
3. Click **Create** to create a new parser, or click **Cancel** to return to the **Welcome** page.
   The following screen is displayed after you select **Create New Parser**.



4. Click the **Open/Change Log File** icon ( ). Browse to find the log file that you want to open and click **Open**.

For more information, see Opening a Log File

All the events in the selected log file are displayed, as shown in the following example.

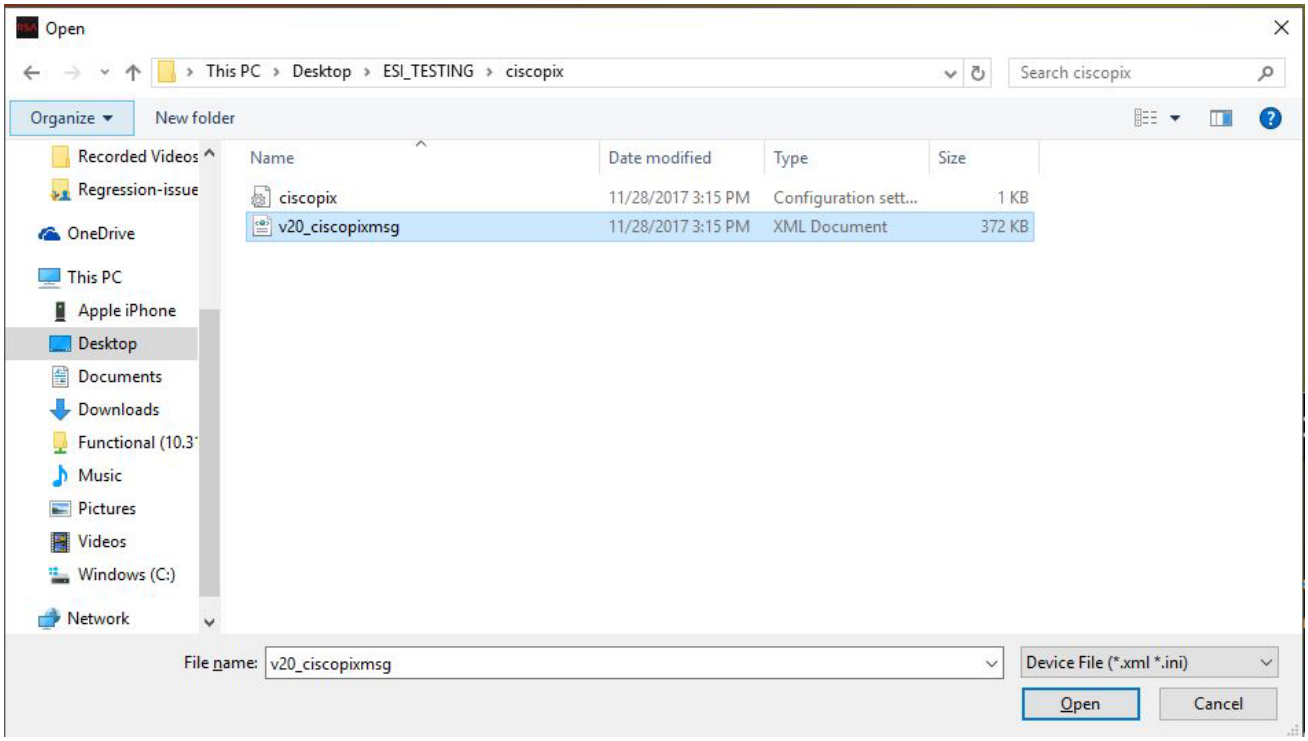


Editing an Existing Parser

To continue defining a parser, follow these steps.

Note: If you opened your parser previously in the NetWitness Log Parser Tool, you can open the parser from the **Recent Parsers** section of the Welcome screen. Note that the most recent parsers are displayed (with a maximum of eight parsers).

1. In the Welcome screen, select **Open Existing Parser** and click **Open**.
   The directory which is set as the default device location under **Preferences** is opened when **Open Existing Parser** is selected.
   The directory for NetWitness Log Parser Tool parsers is displayed, as shown in the following example.



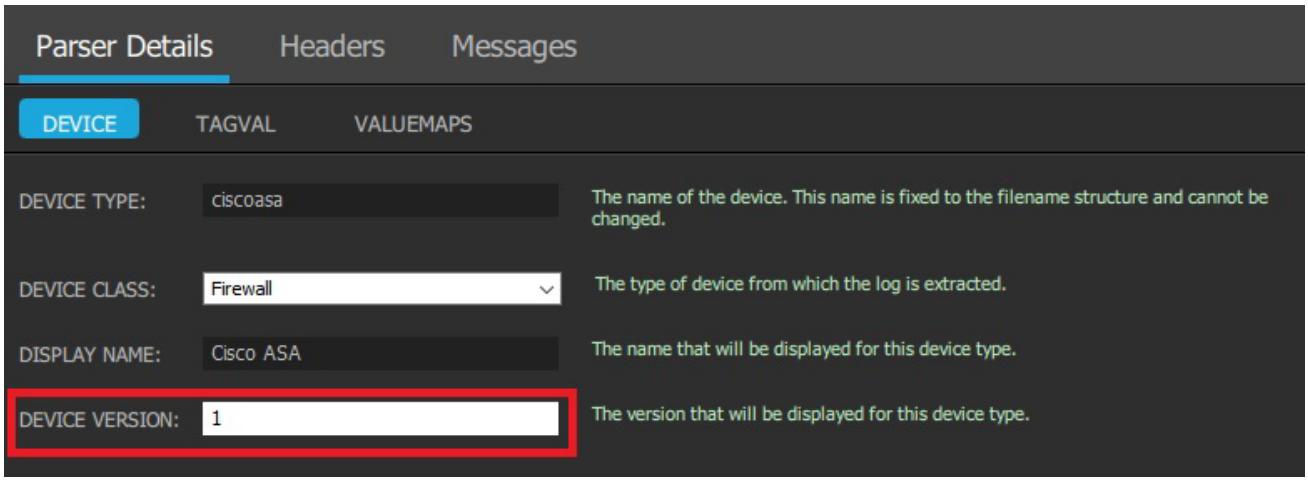
2. Type or select the name of the parser that you want to edit and click **Open**. For example, ciscoasamsg.xml.

Note: Parsers are auto saved every 30 seconds in a temporary location. This acts as a back up in case the NetWitness Log Parser Tool performance slows down significantly while you are using it.

Note: Opening and editing multiple parsers may result in slow performance.

Parser Version

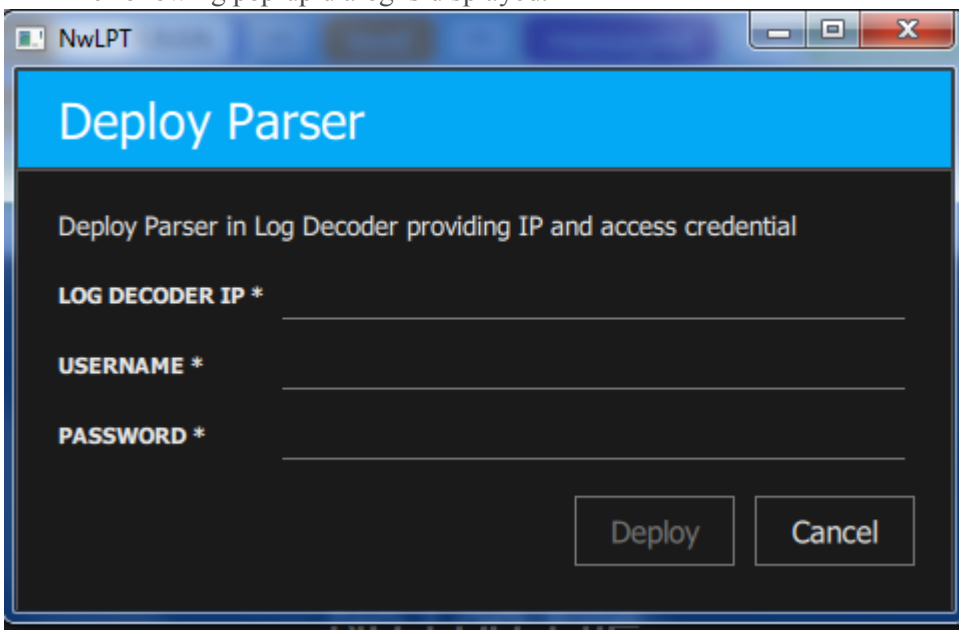
In the Parser Details section there is a Parser Version field. If there is a specific version associated with the parser, that version is displayed in the Parser Version field. You can also manually change the Parser Version in the Parser Version field.



Deploying Parsers on a Log Decoder

Using the NetWitness Log Parser Tool, you can deploy parsers on a Log Decoder by following these steps:

1. Open the parser that you want to deploy on the Log Decoder.
2. Go to **Actions > Deploy Parser**.
   The following pop-up dialog is displayed.



3. Enter the IP address of the Log Decoder where you want to add the parser, along with the credentials of the Log Decoder.

4. Click **Deploy** to add the parser to the Log Decoder, or click **Cancel** to return to the previous screen. After you click **Deploy**, the parser is added to the Log Decoder. And subsequently, all log parsers are reloaded.

Note: These entries are not retained, all the fields must be re-entered every time this dialog is opened.

Opening a Log File

Note: The first time you open the log file for a parser, the location that is set in **Preferences** is the default location.

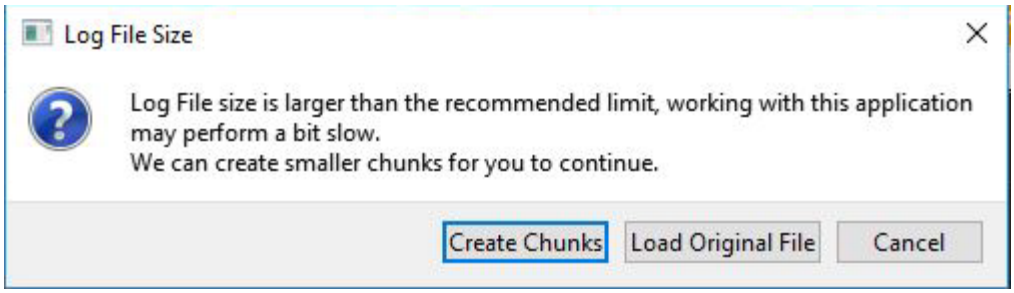
In the **Log Data** section, do one of the following to add a log file for parsing:

- Click **Open/Change Log File** icon.
- Drag and drop the log file.
- Drag and drop the text of a plain log.

Note: When a log file is open, you can change to a different log file using the **Open/Change Log File** icon.

Auto Splitting Log Files

When you upload a log file, the following dialog is displayed if your log file exceeds 25 MB.



The Log File Auto Splitting option allows you to split the size of a log file that exceeds 25 MB.

- If you select **Create Chunks**, the log file is split into smaller sized files without affecting the original log file.
- If you select **Load Original File**, the log file may load slowly, because it exceeds the recommended maximum size of 25 MB.
- If you select **Cancel**, you can select a different log file to load.

Note: If a file larger than 25 MB is used, it is recommended that you use On-Demand Parsing so that the parser does not attempt to parse a large log file after every change.

Generating Parsing Summary Report

You can generate a report on the parsing details of the parser and log file that you loaded. This report provides detailed information about the parsed messages and headers, as well as information about unused headers and messages and top 10 meta values. The report opens automatically in your default browser and is saved your Documents folder on your computer.

Note: Each time you generate a Parsing Summary Report, the existing report is overwritten. If you want to retain the existing report, it is recommended that you re-name the generated report.

To generate a report, follow these steps:

1. Open the parser associated with the report that you want to generate.
2. Open the log file that is associated with your selected parser. Note that if your log file is extremely large, a dialog is displayed that asks if you want the log file broken into smaller chunks.
3. Go to **Actions > Generate Parsing Summary**.

An example of the Generate Parsing Summary Report is shown below.

NwLPT Parsing Summary Report

Device Parser : *C:/*
Device Log File : *C:/*

Overall Parsing Summary

This section gives the summary of the overall parsing for the selected log file against the device parser

Total Log(s)	Parsed Log(s)	UnParsed Log(s)	Only Header Parsed Log(s)
20	20	0	0

Header Parsing Summary

This section gives the summary for the Header(s) in the device parser. Primarily it summarizes the Top 10 used HeaderId(s) and the list of HeaderId (s) that were unsed for this selected log file

Header Utilization** = **18.18%

#	HeaderId	Matching Log Count	Matching Log Percentage
1	0001	19	95.00
2	0004	1	5.00

Unused HeaderId(s)
0002, 0003, 0005, 0006, 0007, 0008, 0009, 0010, 0033

Message Parsing Summary

This section gives the summary for the Message(s) in the device parser. Primarily it summarizes the Top 10 used MessageId(s) and the list of MessageId(s) that were unsed for this selected log file

Message Utilization** = **1.73%

#	MessageId	Matching Log Count	Matching Log Percentage
1	104002:01	2	10.00
2	101001	1	5.00
3	101002	1	5.00
4	101003	1	5.00
5	101004	1	5.00
6	101005	1	5.00
7	102001	1	5.00
8	103001	1	5.00
9	103002	1	5.00
10	103003	1	5.00

Unused MessageId(s)
105001, 105002, 105003, 105004, 105005, 105006, 105007, 105008, 105009, 105010, 105011, 105020, 105021, 105031, 105032, 105034,

Metas Parsing Summary

This section gives the summary for the metas in the device parser. Primarily it summarizes the Top 10 used metas

#	Meta Name	Meta Count
1	context	20
2	event_description	20
3	level	20
4	messageid	20
5	result	5
6	day	1
7	month	1
8	resultcode	1
9	time	1
10	year	1

Status Bar

Within the NetWitness Log Parser Tool user interface, there is a status bar located at the bottom of the page that displays the following information:

- Header and Message count
- Latest auto-save time
- Progress Bar that displays to show the progress of a log file being loaded or parsed
- Log file path is displayed that is replaced with the rows that match your query during a search

The following example Status Bar shows the most recent time that a log file was auto-saved.

Understanding the Log Data Section Workflow

The following figure shows the workflow of the Log Data section.

After you have defined a new parser or opened a parser to edit, work from the Log Data section to define the headers and messages. Events move from **Undefined** (Header and Message not defined) to **Header Defined** (Message not defined) and then to **Completely Defined** (Header and Message defined).

Note: All defined Headers and Messages can be duplicated. This allows a simplified parser development where a similar pattern is needed for a Message or Header.

Determining the Parser Definition Method

There are two main methods to specify a parser definition depending upon the type of information that you need to collect in the logs:

- Identify events with a specific type and extract generic information.
- Extract as much detailed information as possible from an event.

Example: Extract Generic Information

The following example shows how to create a parser that extracts generic information from a Cisco ASA log. It uses the following event from the Cisco ASA log:

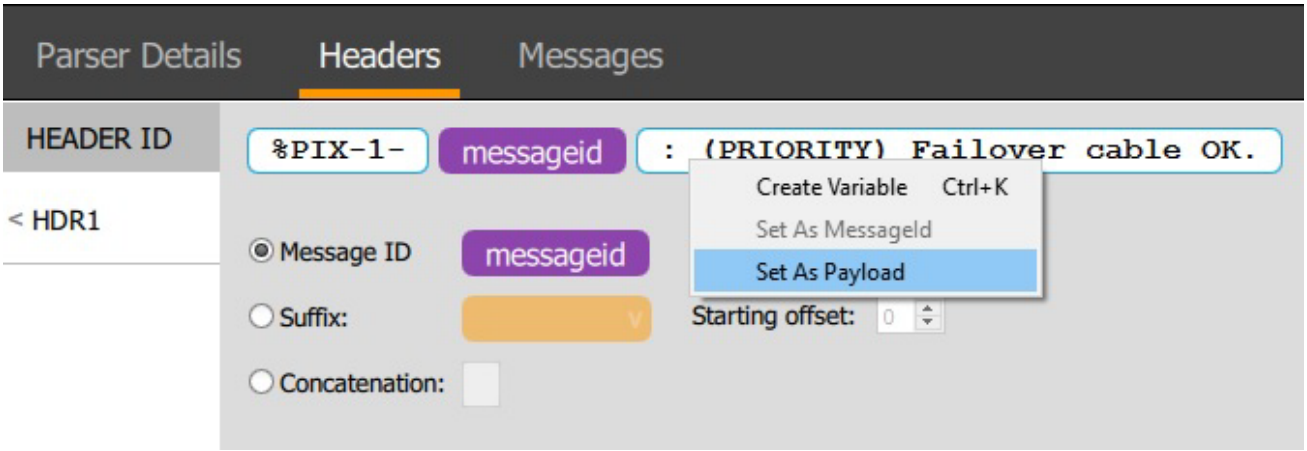
```
%ASA-1-101001: (PRIORITY) Failover cable OK.
```

Defining the Header Pattern

To define the header pattern, follow these steps:

1. Select an undefined event.
2. Identify the text as the MessageID and highlight it.
3. Click **Create Header** to create the header.
4. If you want to change the log file, then click the **Open/Change Log File** icon.

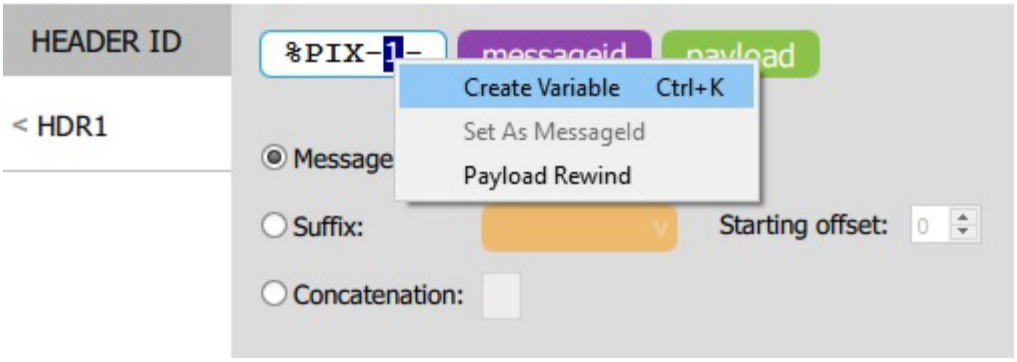
5. To start the payload, select the text to be marked as payload, right-click, then click **Set as Payload**. Alternatively, place your cursor at the start of the payload, right-click, and select **Set as Payload**.



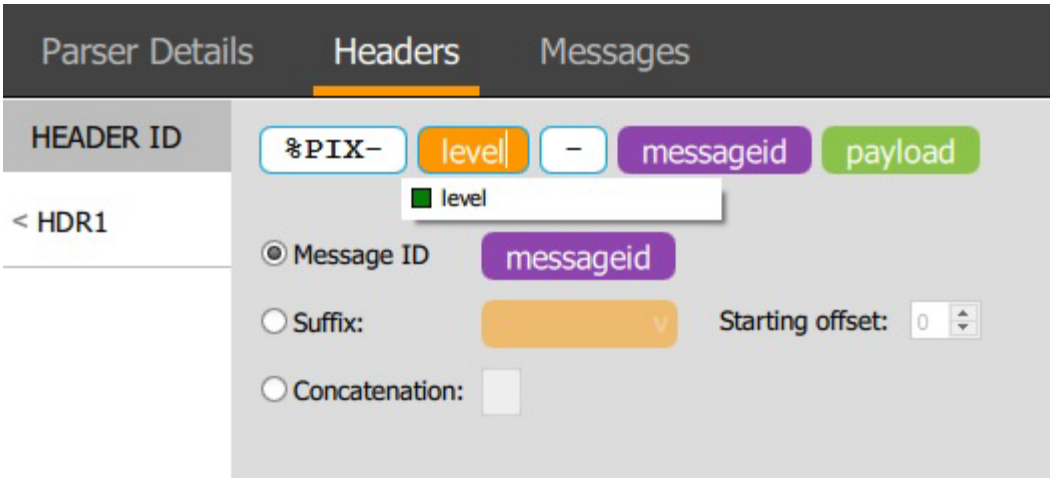
6. Define a variable for anything that can change. To define a variable:

   a. Highlight the text that you want to change to a variable.

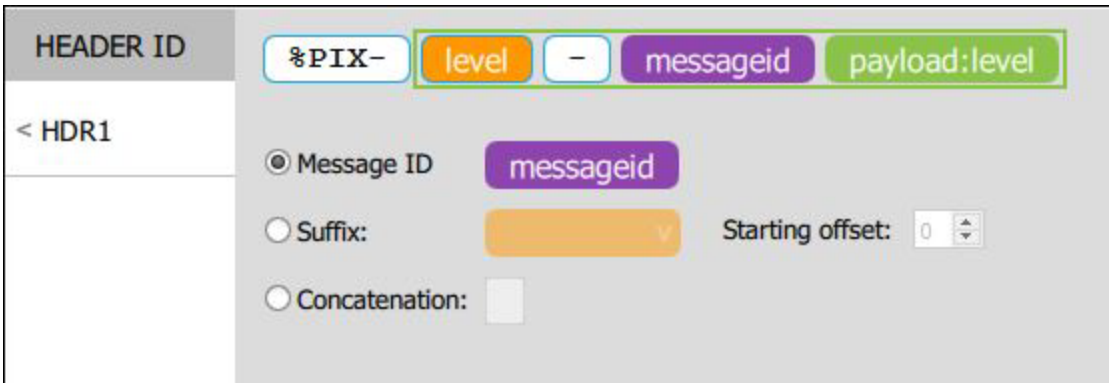
   b. Press **CTRL+K** (**COMMAND+K** for MacOS). You can also right-click to get a context menu that provides an option to create a variable. The background changes to orange, which indicates a variable.
   This example shows changing 1 to a variable.



   c. Start typing the name of the variable in the variable field, use the down and up arrow keys to select the variable, and press **ENTER** or you can also double-click the variable to select it.

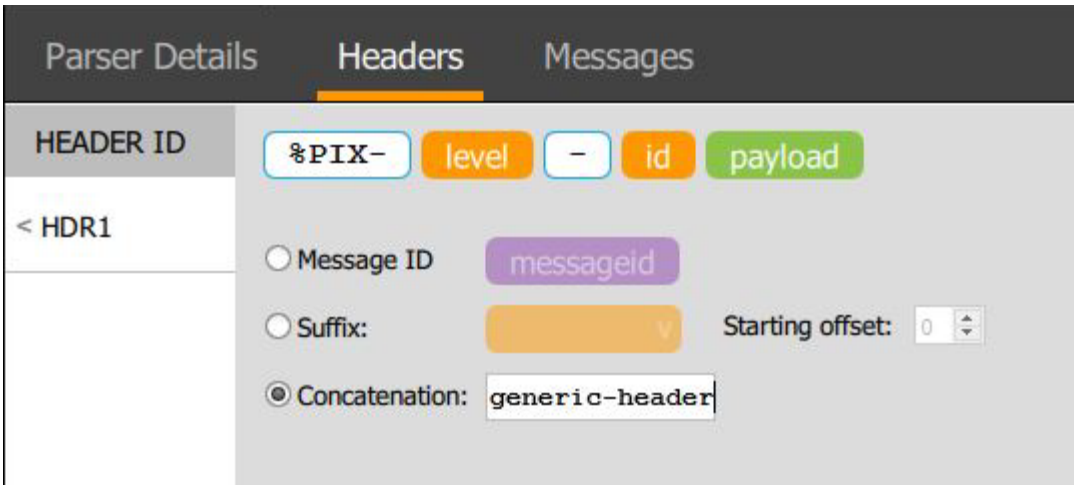


7. To change where the payload starts, or to start at the header, right-click a variable and select **Payload Rewind**. For example, right-click the **Level** variable and select **Payload Rewind**. The green box indicates a complete payload with a Message Header.



8. To change the MessageID to a generic value:

   a. Select **Concatenation**, type a generic text string in the text field, and press **ENTER**.



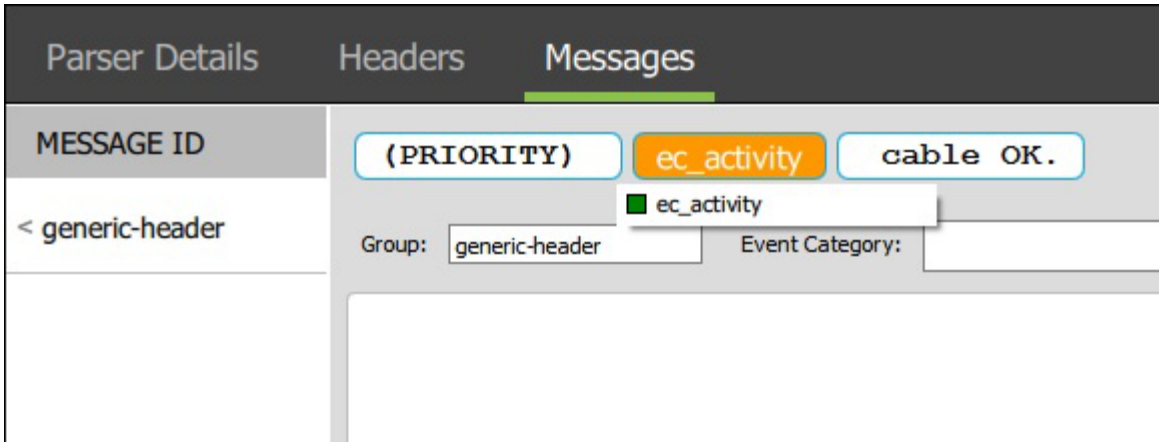
Note: Each Header needs a MessageID and a payload. Make sure to define a single MessageID for each header.

Note: The **Create Message** button in the log section is only enabled when the MessageID and Payload are defined.

Note: If you want to change your MessageID, you may need to delete the header and recreate it.

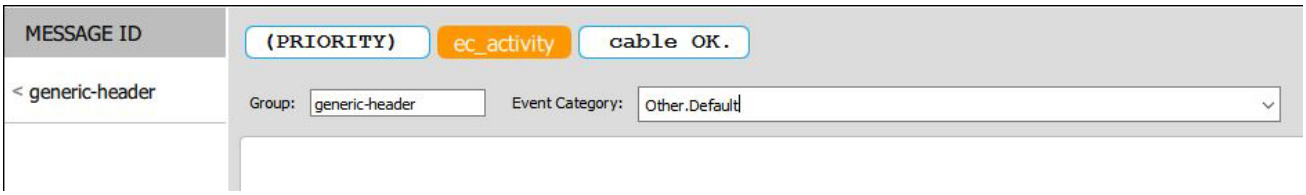
Defining the Message Pattern

1. After the MessageID and payload are defined in the event, the **Create Message** button is enabled.
   Click on the **Create Message** button. This takes you to the **Messages** tab with the payload populated as the message.
2. In the message pattern, define variables for the values that you want to extract as meta. To define a variable:
   a. Highlight the text that you want to change to a variable and press **CTRL+K** (**COMMAND+K** for MacOS). Or you can select the **Create Variable** option from the context menu. The background changes to orange, which indicates a variable.
   b. Start typing the name of variable in the variable field, use the down and up arrow keys to select the variable, and press **ENTER**.



Note: The variables that you define create meta in the Log Decoder.

3. In the **Event Category** field, select a generic category for the message. For example, Other.Default.



   The **Group** field populates from the header. The event shows as completely defined in the **Select an Event** section.
4. To save your changes, select **File > Save** or **File > Save As**, or press **Ctrl+S** (**COMMAND+S** for MacOS).

5. After you complete and save your changes, retrieve the completed parser.
   You have a choice of three formats:
   - **.envision** (In the menu, select **Actions > Export Parser**) This option creates an event source package that consists of the event source XML and configuration (INI) file.
   - **.zip** (In the menu, select **Actions > Export Resource**) This option creates an event source package in a .zip format that consists all the event source XMLs and configuration INI files.
   - Deploy the parser directly deployed from the Log Parser Tool to the Log Decoder. From the main menu, select **Actions > Deploy Parser**.
6. Deploy the event source package in the NetWitness platform to integrate the event source. RSA recommends that you first deploy the parser to a test system to verify that it parses log traffic correctly.

Defining a Throw-away Variable

To add a throw-away field variable for information that you do not care about, create a variable and give it a name that is not defined in the variable list, such as **fld1**, **fld2**, or **fld3**.

1. Highlight the text that you want to change to a variable and press **CTRL+K** (**COMMAND+K** for Mac). You can also right-click to get a context menu that provides an option to create a variable. The background changes to orange, which indicates a variable.
2. Type the name of the throw-away field. For example, **fld1**
   Since throw-away fields are not in the mapping, the information contained will be removed when parsing.

Adding a Constant Function

1. Right-click the box below the **Group** field and select **Add Function > Assign Constant**.
2. In the **value** field, type the value that you want to assign to the variable.
3. In the **Set Variable** field, type the name of a variable that was not previously selected.

Adding an Event Time Function

Use the Event Time function to change the format of an event source timestamp.

1. Right-click the box below the **Group** field and select **Add Function > Event Time**.
2. In the **Set Value** field, type the format that you want to assign to the time variable. For example, **%B %F %W %N:%U:%O**, which appears in the format **Jan 27 2015 23:55:29**.
3. In the **from** field, select whether to parse event time in this format from the message (MSG) or from the header (HDR).
4. Right-click the **Select Variable** fields and select a variable from the list. To add additional variables as required, right-click a variable and select **Add**.

Event time example:

Event Time Function Formatting Characters

The following table shows the format characters that Log Decoder supports for the Event time function.

Format Character	Description
%C	Dates of this format: 04/20/05 14:01:57
%R	Full Month Name, fixed width field: January, February, March, April, May, June, July, August, September, October, November, December
%B	Abbreviated Month Name, fixed width field: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
%M	Numeric Month, fixed width field: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
%G	Numeric Month Variable width field: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
%D	Numeric Month Day, fixed width field: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, ... , 23, 24, 25, 26, 27, 28, 29, 31
%F	Numeric Month Day Variable width field: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, ... , 23, 24, 25, 26, 27, 28, 29, 31
%H	Hour, fixed width field: 00-23

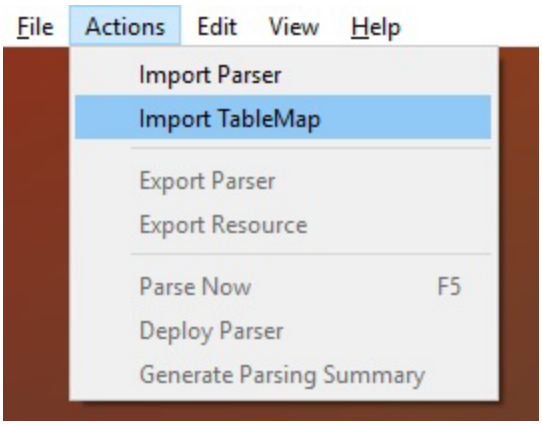
%I	Hour, fixed width field: 00-12
%N	Hour: Variable width field: 00-12 , 00-24
%T	Minute, fixed width field: 00-59
%U	Minute: Variable width field: 00-59
%J	Julian day, fixed width field: 001-365
%P	Alpha, fixed width field: AM or PM
%Q	A.M./P.M.
%S	Seconds, fixed width field: 00-59
%O	Variable width field: Seconds: 00-59
%Y	Year: 00-99
%W	Year, fixed width field: 0000-9999
%Z	Hours:Min:Sec
%A	Days
%X	Unix Time-Stamp (for example: 1424849941)

Adding a Custom Table Map

Note: If you changed the table mapping file (**table-map.xml**), or created a custom table mapping file (**table-map-custom.xml**), you can upload this updated file to the NetWitness Log Parser Tool.

To create a custom table map:

From the Welcome screen, select **Actions > Import TableMap** and choose the **table-map** that you want to upload.



Note: Before your file is overwritten, a confirmation message is displayed in the dialog box if you have already created a custom table map with the same name. This message does not display if you are a uploading a **table-map-custom.xml** file for the first time.

Deleting a Message

Shortcuts for deleting a message have been added for Windows and MacOS . In Windows operating systems, the shortcut **Ctrl+Del** will delete a message. In MacOS, the shortcut **Fn+Ctrl+Del** will delete a message.

You can also delete a message using the **Context** menu or the **Edit Menu** option.

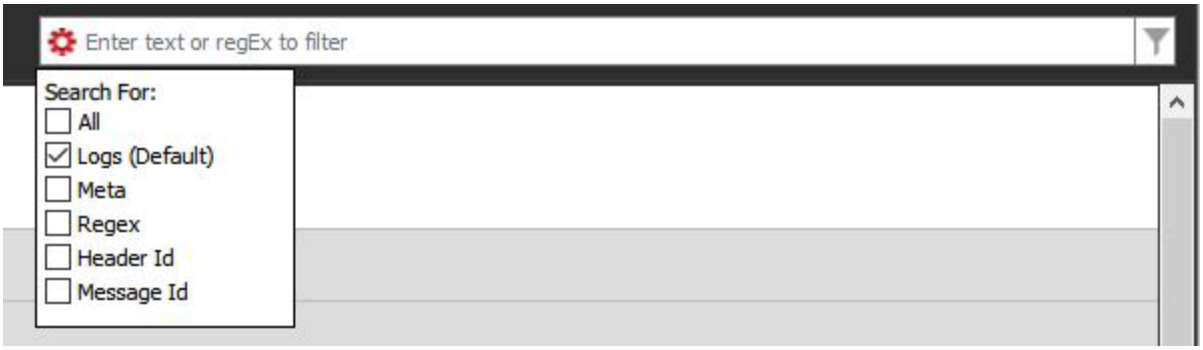
Using Undo and Redo

The Undo and Redo options allow you to undo and redo any number of commands while the parser is being built or updated. Using the Undo option reverts to the last change that you made to a single message or header. Using the Redo option allows you to make changes to a single message or header.

- To Undo your changes, press **CTRL + Z**, or from the main menu, select **Edit > Undo**.
- To Redo your changes, press **CTRL + Y**, or from the main menu, select **Edit > Redo**.

Log Filter Functionality

The following example shows the filter options that are available from the Log Filter drop-down menu.



Log filter options are described in the following table.

Log Filter Option	Description
Logs	Searches for the selected value for log search. Searches for any log that contains the selected search text. For example, you can search for **Bangalore**. Search results include any logs that contain **Bangalore** as part of a log.
Meta	Searches for any meta in the logs section. For example, you can search for the term **username**. Search results include logs that contain **username** as part of a log.
Regex	Searches for the selected regex pattern in the logs section. For example, you can search for **\d+\.\d+.*** and the search results include logs that contain IP addresses as part of the logs.
Header ID	Searches for the selected HeaderID. For example, you can search for a HeaderID that is listed as **0008**. The search results include the number of headers that contain **008*** defined as part of the header.

Message ID	Searches for the selected MessageID. For example, you can search for a MessageID such as **04_TACACSAcc**. The search results include the number of messages that contain **04_TACACSAcc*** defined as part of the message.
All	Searches for any logs, HeaderIDs, MessageIDs, variables, meta, or regex that matches the selected search text. For example, you can search for the text **syslog**, and the search results include any logs, HeaderIDs, MessageIDs, variables, meta, or regex that matches **syslog**.

The following example shows the search results for logs. The Search field and the Status Bar Message Count fields are highlighted.

Parser Header and Message Search Functionality

Within the Parser section, you can search on a HeaderID or Message Group by entering the value in the search field.

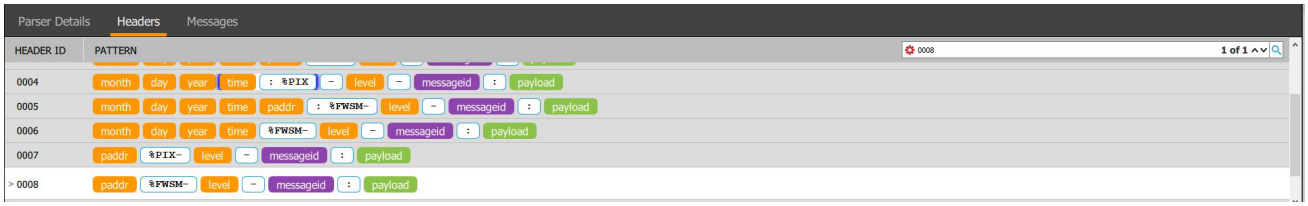
Header Search Functionality

The following example shows the search options that are available from the Header Search drop-down menu.

Header Search options are described in the following table.

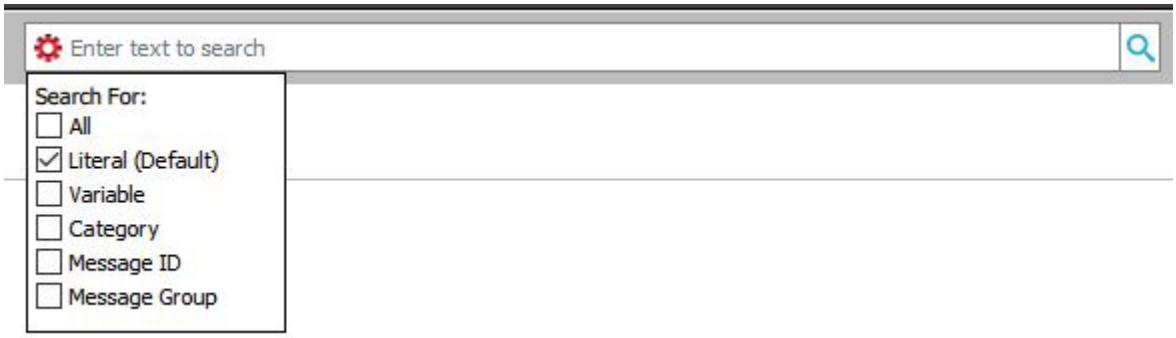
Header Search Option	Description
Literal	Default search option that matches literals. This option searches for any literal within the Header section. For example, you can search for **Bangalore** with this option selected. The search results include the number of headers that contain **Bangalore** as part of a literal.
Variable	Searches for any variable or meta defined in the Header section. For example, you can search for **saddr** with this option selected. The search results include the number of headers that contain **saddr** defined as part of the header.
HeaderID	Searches for the selected HeaderID. For example, you can search for a HeaderID that is listed as **0008**. The search results include the number of headers that contain **008*** defined as part of the header.
All	Searches for any selected text. For example, you can search for the text **syslog**, and a search is performed on any literal, HeaderID, or variable that matches the selected search text.

The following example shows the header search results.



Message Search Functionality

The following example shows the message search drop-down menu with the Literal option selected.

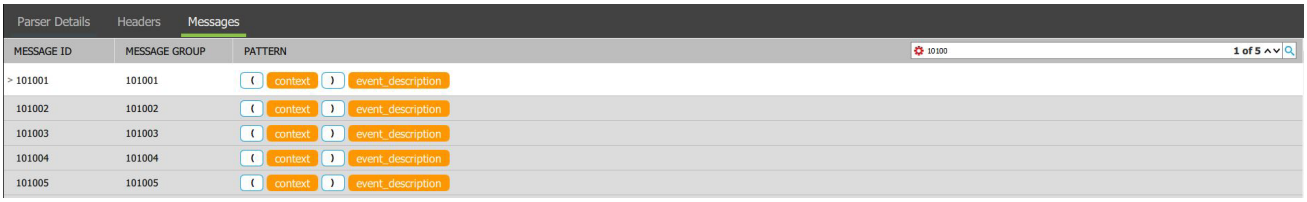


Message Search options are described in the following table.

Message Search Option	Description
Literal	Default search option that matches literals. Default selected value for Message searches. This option searches for any literal within the Message section. For example, you can search for **Bangalore** with this option selected. The search results include the number of messages that contain **Bangalore** as part of a literal.
Variable	Searches for any variable or meta defined in the Message section. For example, you can search for **saddr** with this option selected. The search results include the number of messages that contain **saddr** defined as part of the message.

Category	Searches for a particular event category that is part of the selected message. the search results include the number of messages that contain **Auth.Successful.*** defined as part of the selected message.
MessageID	Searches for the selected MessageID. For example, you can search for a MessageID such as **04_TACACSAcc**. The search results include the number of messages that contain **04_TACACSAcc*** defined as part of the message.
Message Group	Searches for the selected Message Group. For example, you can search for the text **syslog**. The search results include any literal, MessageID, variable, category, or Message Group that contain **syslog**.
All	Searches for any selected text. For example, you can search for the text **syslog**, and a search is performed on any literal, MessageID, variable, category, or Message Group that matches the selected search text.

The following example shows message search results.



Advanced Search Options

Note: To perform an advanced search, use **&&**, which is an **AND** condition that helps drill down to your exact search pattern. This applies to all three advanced header and message search options.

Note: When you are performing a combination search, it is an **OR** condition for the search. The search begins after you press **ENTER**.

Note: The context menu for Headers and Messages has a new option called **Parsed Logs** that displays all the logs parsing from the selected Header or Message.

Note: All search options listed below can be used individually, as well as with other search options. The advanced search options can be used also be used in the logs section.

Advanced Log Filter Options

Note: When using the Advanced Search, you must select **All** from the Log Filter drop-down menu.

The following table shows the advanced log filter options.

Message Search Option	Description
Header Search	If you need to filter logs that parse with a specific header, use the **@hid** option, followed by the HeaderID (for example, **@hid:0001**).
Message Search	If you need to filter logs that parse with a specific header, use the **@hid** option, followed by the HeaderID (for example, **@hid:0001**).
Variable Name Search	If you want to filter logs that contain a specific variable or meta item, use the **@<Variable-name> @saddr** option. This option lists all logs that contain **saddr** meta keys.
Variable Value Search	If you want to filter logs that have a specific variable value, use the **@<variable-name>:<variable-value>** option (for example, **@dport:10**). This option lists all logs with a value of meta key **dport** as **10**.

Regex Search	If you want to search the logs using a regex, use the **@regex** option (for example, **@regex:\d+\.\d+.*** This option displays all logs that contain an IP address.
Free Text Search	If you use this option, any text provided will be searched in the logs. If two words are provided, both of them are searched separately (similar to the way that Google performs text searches). As an example, if you enter the words **rsa bangalore**, **rsa** and **bangalore** are searched separately and all logs containing either word are displayed.

Note: If you want to search on terms as though they are in a sentence, you need to enclose your search query in quotation marks (for example, **"rsa bangalore"**).
If the search query is not properly enclosed within quotation marks, the error is not automatically corrected, and no error message is displayed.

Note that when you search on a header, message, variable name or variable value, by default all searches only perform a contains match. For example, if you enter the search text **@hid:0001**, all headers containing **id 0001, 0001:01, 0001:02**, and so on will be displayed. If you want an exact match, the query should be entered as **@hid:"0001"** so that only logs that match **header-id 0001** are displayed.

Advanced Header Search

The following table shows the advanced header search options.

Advanced Header Search Option	Description
@id:	Searches for the selected HeaderID. Syntax: **@id:<header>id>**, where **header_id** is the HeaderID that you are searching for. For example, **@id:0008** displays the number of headers that contain **0008*** defined as headers that you can search.
@var:	Searches for any variable or meta defined in the header section. Syntax: **@var:<variable>**, where variable is the variable or meta to search. For example: **@var:saddr** displays the number of headers that contain **saddr** defined as a part of the header that you can search.

@literal:	Searches for any literal content in the header section. Syntax: **@literal:<text>**, where text is the literal to search. For example, **Bangalore** displays the number of headers that contain **Bangalore** as part of the literal that you can search.

Advanced Message Search

Advanced message search options are explained in the following table.

Advanced Message Search Option	**Description**
@id:	Searches for the selected MessageID. Syntax: **@id:<message_id>**, where **message_id** is the MessageID that you are searching for. For example, **@id:04_TACACSAcc** displays the number of messages that contain **04_TACACSAcc*** defined as messages that you can search.
@var:	Searches for any variable or meta defined in the header section. Syntax: **@var:<variable>**, where variable is the variable or meta to search. For example: **@var:saddr** displays the number of headers that contain **saddr** defined as a part of the header that you can search.
@literal:	Searches for any literal content in the message section. Syntax: **@literal:<text>**, where text is the literal to search. For example, **Bangalore** displays the number of messages that contain **Bangalore** as part of the literal that you can search.

TAGVALMAP Feature

The **<TAGVALMAP>** feature is an advanced feature that enables easy parsing of event logs using the **<TAGVAL>** format. The parsing of **<TAGVAL>** logs is different from other logs, as the Log Decoder allows listing all **Tag=value** in a single MessageID where the tags can display in any order in the log.

Using the TAGVALMAP Feature

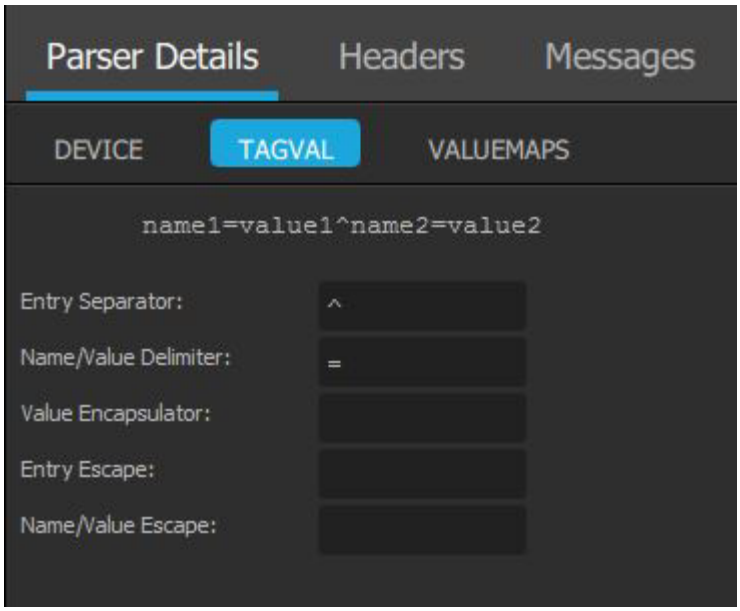
Using the **<TAGVALMAP>** feature saves you from writing different messages for the same MessageID if your log messages only differ in the order of variables within the payload, or if some parameters do not show up in the payload.

When you define your delimiters, the parser does not work the same way by matching the payload character by character, but the payload string is split around the delimiters into ><*key-value* pairs. For every <*key-value*> pair, the static text is matched against the appropriate key and the value goes to the corresponding parameter in the table.

There are types of event logs where the part logs have a pattern of <*tag-value*> (<*name-value*), which means the the tag parts remain the same, but the value is changed.

The Entry Separator has a maximum limit of three characters, while Entry Escape and Name Value Escape allow only one character.

The following example shows a **TAGVAL** parameter in the Parser Details section.



After you save the data, the corresponding XML file content looks similar to the following example:

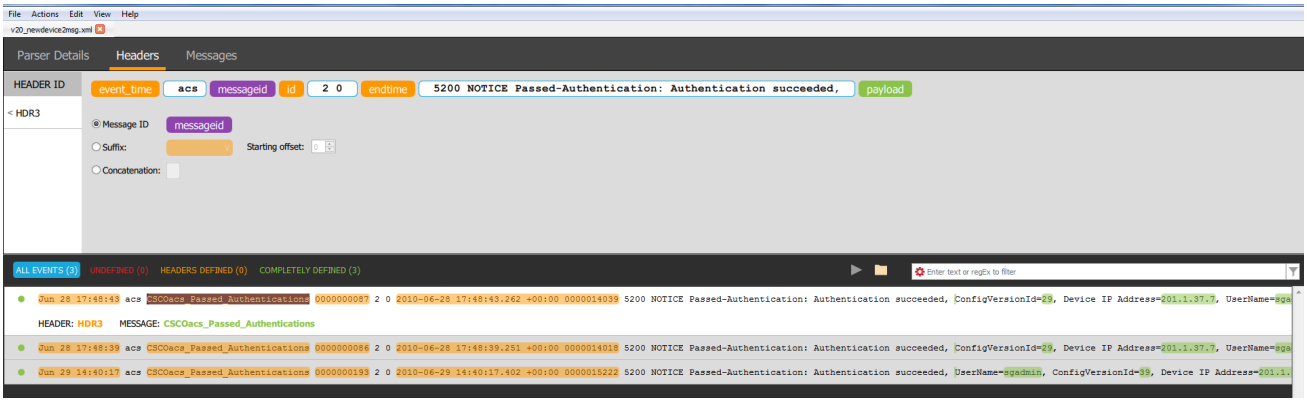
```
<TAGVALMAP
```

```
pairdelimiter=","
encapsulator="'"
valuedelimiter="="
escapeValueDelim=" "
escapePairDelim=" "/>
```

Note: Press **ENTER** after you change each delimiter.

Setting Up a Header and Creating a Message

The following example shows a header and message that is created.



The corresponding Header XML definition is shown below:

```
<HEADER
id1="HDR3"
id2="HDR3"
content="&lt;event_time&gt; acs&lt;messageid&gt;&lt;id&gt; 2 0
&lt;endtime&gt; 5200 NOTICE Passed-Authentication: Authentication
succeeded, &lt;!payload&gt;"/>
```

Create Message

When you create a message, the **Name Value Pair** check box should be checked in order for the messages to be parsed. Note that if you do not select the **Name Value Pair** check box, the parser does not parse **<TAGVAL>** messages with a different order. The **Name Value Pair** is disabled by default and it is enabled for user input only if the message definitions satisfy the **<TAGVAL>** format, as shown in the following examples.

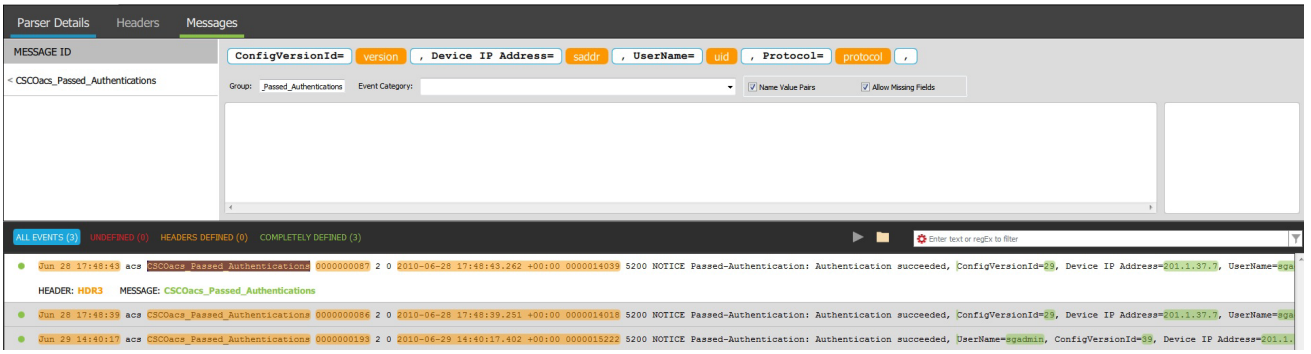
The **TAGVAL** format is either:

```
<literal><valuedelimiter><variable><pairdelimiter>….<literal><valuedeli
miter><variable> format
```

Or

```
<literal><valuedelimiter><variable><pairdelimiter>….<literal><valuedeli
miter><variable><pairdelimiter> format
```

The **Allow Missing Fields** option is used to parse event logs that missed some **<TAGVALUE>** pairs defined in the message definition. This means not all **<TAGVALUE>** pairs defined in the message definition need to be parsed.



The corresponding Message XML definition is shown below:

```
<MESSAGE

id1="CSCOacs_Passed_Authentications"

id2="CSCOacs_Passed_Authentications"

tagval="true"

missField="true"

content="ConfigVersionId=&lt;version&gt;, Device IP
Address=&lt;saddr&gt;, UserName=&lt;uid&gt;,
Protocol=&lt;protocol&gt;,"/>
```

Listed below are sample payload parts of event logs that are parsed:

```
ConfigVersionId=29, Device IP Address=201.1.37.7, UserName=sgadmin,
Protocol=Radius,

ConfigVersionId=29, Device IP Address=201.1.37.7, UserName=sgadmin,

Authentication succeeded, UserName=sgadmin, ConfigVersionId=39, Device
IP Address=201.1.37.7, Protocol=Radius
```

RSA NETWITNESS® SUITE

NetWitness Investigate User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

How NetWitness Investigate Works 15

Metadata, Meta Keys, Meta Values, and Meta Entities 15

Triggers for an Investigation 16

Workflow of an Investigation 16

Focus on Metadata, Query, and Time 19

Focus on Endpoint Analysis 20

Focus on NetWitness Respond Incidents and Alerts 21

NetWitness Investigate Views 21

Navigate View 21

Events View 22

Event Analysis View 23

Hosts View 24

Files View 25

Malware Analysis View 26

Contextual Information for an Event 27

Event Reconstruction 28

Configuring NetWitness Investigate Views and Preferences 31

Configure the Navigate View and Events View 32

Access the Navigate View and Events View Settings 32

Calibrate Navigate View Value Loading Parameters 33

Configure Navigate View and Events View Parameters 34

Configure the Default Log Export Format 35

Configure the Default Meta Export Format 36

Calibrate Events View Retrieval and Default Reconstruction 36

Enable or Disable Cascading Style Sheet Rendering in Web Content Reconstructions 37

Configure Search Options 37

Configure the Event Analysis View 38

Set the Default Investigate View 39

Configure the Event Analysis View 39

Configure the Malware Analysis Summary of Events View 42

Add a Dashlet 42

Modify or Delete a Dashlet Using Toolbar Options 43
Apply Threshold Filter to Multiple Dashlets 43
Set Title and Category Options for a Dashlet 44
Order Dashlets 45
Restore Default Dashlets 46

Beginning an Investigation 47

Focus on Metadata, Raw Events, and Event Analysis 47
Focus on Hosts and Files 47
Focus on Scanning Files for Malware 47
Begin an Investigation in the Navigate or Events View 49
Begin an Investigation (No Default Service) 50
Set or Clear the Default Service 51
Begin an Investigation (Default Service Specified) 52
Change the Service or Collection to Investigate 53
Investigate Workbench Restoration Collections 56
Begin an Investigation in the Event Analysis View 57
Access the Event Analysis View (Version 11.1 and Later) 57
Access the Event Analysis View (Version 11.0) 61

Investigating Metadata in the Navigate View 62

Filter Results in the Navigate View 63
Set the Time Range 63
Set the Quantification Method and Sort Sequence of Meta Key Results 65
Manage and Apply Default Meta Keys in an Investigation 67
Drill into Data in the Navigate View Time Chart 69
Drill into Data in the Values Panel 70
Manage Meta Groups 79
Out-of-the-Box Meta Groups 79
Create a Meta Group and Add Meta Keys 80
Duplicate and Edit an Out of the Box Meta Group 83
Edit a Meta Group 83
Delete a Meta Group 84
Export a Meta Group 85
Import a Meta Group 85
Visualize Metadata as Parallel Coordinates 87
Best Practices for Effective Parallel Coordinates Charts 87

RSA Meta Groups for Parallel Coordinates Use Cases 88
View a Parallel Coordinates Visualization 88
Select Meta Keys for a Parallel Coordinates Visualization 91
Optimize a Parallel Coordinates Visualization 95
Sample Use Case 96
Sample Visualization of a Large Data Set 97
Open an Event in the Events List 98
Export or Print a Drill Point 100
Launch an External Lookup of a Meta Key 102
Launch an ECAT IOC Lookup 103
Lauch Other External Lookups 105
Launch a Malware Analysis Scan from the Navigate View 106
Visualize the Current Drill Point in Informer 108

Examining Raw Events in the Events View 110

Filter and Search Results in the Events View 111
Filter Events Displayed in the Events View 111
Search for Events in the Events View 113
Manage Column Groups in the Events View 115
Create Custom Column Group 115
Select a Column Group 118
Export Events in the Events View 120
Add Events to an Incident for Response 121
Combine Events from Split Sessions 123
Contextual Fragment Parsing 123
Session Fragments Highlighting 124
Find and Combine Fragments 125

Querying and Acting on Data in the Navigate and Events Views 128

Create a Custom Query 129
Create a Query Using the Basic Method 129
Create a Query Using the Advanced Method 130
Apply a Recent Query 132
Manage Context Hub Lists and List Values in Investigate 133
Add Meta Values to an Existing List 134
Remove a Meta Value from a Context Hub List 135
Create a New List 135

View Additional Context for a Data Point 136
Use Profiles to Encapsulate Custom Views 138
Navigate to the Manage Profiles Dialog 138
Create and Edit Profiles 139
Change Active Profile 139
Import Profiles 140
Download Profiles 140
Search for Text Patterns 141
Keyword Text Search 141
Search Examples 144
View and Modify Queries Using URL Integration 146
Service Id Known 146
Host and Port Known 147
Examples 147
Additional Notes 148
Reconstruct an Event 149
Reconstruct an Event from the Navigate View 150
Reconstruct an Event 151
View Side by Side or Top to Bottom 152
Select Event Information to View 152
Select Event Reconstruction Type 153
Open or Download an Email Attachment 153
Export an Event as a PCAP File 153
Extract Files from a Reconstructed Event 154

Analyzing Raw Events and Metadata in the Event Analysis View 155

Recontruction Types in the Event Analysis View 156
The Text Analysis Panel 157
The Packet Analysis Panel 160
The File Analysis Panel 162
Analytical Tools for Each Type of Event Analysis 163
Filter Results in the Event Analysis View 166
How the Breadcrumb Works 166
Keyboard Actions to Use in the Breadcrumb 167
Add a Filter to the Breadcrumb 168
Edit a Filter in the Breadcrumb 170
Query Using Selected Filters in the Breadcrumb 170

Delete a Filter in the Breadcrumb 171
Examine Events in the Event Analysis View 172
Select the Event Analysis Type 172
Open, Close, and Adjust the Size of the Panels in the Event Analysis View 172
Select a Column Group and Columns in Event Analysis 174
Adjust the Display of Requests and Responses 176
View Event Metadata for an Event 177
Show or Hide the Event Header 179
Page Through Events in the Packet Analysis Panel 179
Expand Truncated Text Entries in the Text Analysis Panel 180
Perform URL and Base64 Encoding and Decoding in the Text Analysis Panel 181
View Decompressed Text in an HTTP Network Session in the Text Analysis Panel 184
Use the Payload Only Option in the Packet Analysis Panel of a Network Session 186
View Highlighted Bytes in the Packet Analysis Panel 187
Highlight Common File Types in the Packet Analysis Panel 188
Download Data in the Event Analysis View 190
Download a Log in the Text Analysis Panel 190
Download Network Event Data in the Text Analysis Panel or the Packet Analysis Panel 192
Download Files from a Network Event in the File Analysis Panel 193
Act on Data in the Event Analysis View 195
Open an Endpoint Event in the NetWitness Endpoint Thick Client 195
Perform Lookups of Meta Values in Event Analysis 197

Investigating Hosts and Files 199

Investigate Hosts 200
Filter Hosts 200
Scan Hosts 201
Pivot to the Navigate and Event Analysis Views 203
Investigate Host Details 204
Delete a Host 207
Set Hosts Preference 208
Export Host Attributes 209
Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts 209
Investigate Files 210
Filter Files 210
Pivot to Navigate and Event Analysis Views 211

Set Files Preference 212
Export Global Files 212

Conducting Malware Analysis 214

Malware Analysis Functions 215
Functional Description 215
Analysis Method 217
Scoring Method 218
Deployment 218
Malware Scoring Modules 219
Network 219
Static Analysis 220
Community 220
Sandbox 220
Begin a Malware Analysis Investigation 221
Launch a Malware Investigation from a Malware Analysis Dashlet 222
Begin a Malware Analysis Investigation (No Default Service) 223
Set or Clear the Default Service 224
Upload and Scan Files 225
Begin an Investigation (Default Service Specified) 225
Apply Time Parameters Filter for Results 226
Apply a Threshold Filter to Continuous Mode Results 226
Delete or Resubmit an On-Demand Scan with New Bypass Settings 227
View the Files List 228
View the Events List 229
Implement Custom YARA Content 231
Prerequisites 231
YARA Version and Resources 231
Meta Keys in YARA Rules 231
YARA Content 232
Add Custom YARA Rules 234
Examine Scan Files and Events in List Form 235
Sort the Files List or Events List 236
Filter the List by Filename or MD5 File Hash 236
Delete Events from the Scan 237
Return to the Summary of Events 238
Open the Detailed Analysis for an Event 238

Filter Dashlet Data in the Summary of Events View 239
Configure the Score Wheel Dashlet 239
Configure the Meta Treemap Dashlet 241
Configure the Meta Breakdowns Dashlet 241
Configure the Events Timeline Dashlet 242
Configure the Top Listing of Highly Suspicious Malware Dashlet 243
Configure the Malware with High Confidence IOCs and High Scores Dashlet 244
Configure the Top Listing of Possible Zero Day Malware Dashlet 244
Upload Files for Malware Analysis Scanning 245
Upload Files Manually 245
Upload Files from a Watched Folder 247
View Detailed Malware Analysis of an Event 250
View Malware Analysis Details for an Event 250
Pivot Network Analysis Results 251
Use File Actions in the Static Analysis Results 251
View Community Analysis Results Details 252
View Sandbox Analysis Results in the ThreatGrid User Interface 253

Troubleshooting NetWitness Investigate 255

Event Analysis Issues 255
Hosts View Issues 258
Files View Issues 259

Investigate Reference Materials 261

Add Events to an Incident Dialog 263
Workflow 263
What do you want to do? 263
Quick Look 265
Add/Remove from List Dialog 267
Workflow 267
What do you want to do? 267
Related Topics 268
Quick Look 269
Context Lookup Panel 271
Workflow 271
What do you want to do? 271
Related Topics 272

Quick Look 273
Lookup Results 274
Create an Incident Dialog 277
Workflow 277
What do you want to do? 277
Event Analysis View 281
Workflow 281
What do you want to do? 282
Related Topics 283
Quick Look 283
Event Analysis View - File Analysis Panel 288
Workflow 288
What do you want to do? 288
Related Topics 290
Quick Look 290
Event Analysis View - Packet Analysis Panel 292
Workflow 292
What do you want to do? 292
Related Topics 294
Quick Look 294
Event Analysis View - Text Analysis Panel 297
Workflow 297
What do you want to do? 297
Related Topics 299
Quick Look 299
Event Reconstruction View 301
Workflow 302
What do you want to do? 302
Related Topics 303
Quick Look 303
Events View 306
Workflow 306
What do you want to do? 307
Related Topics 308
Detailed Description 311
Files View 314

Workflow 314
What do you want to do? 314
Related Topics 315
Quick Look 315
Investigate Dialog 317
Workflow 317
What do you want to do? 317
Related Topics 318
Quick Look 319
Investigation Tab - User Preferences Panel 321
What do you want to do? 321
Related Topics 321
Quick Look 321
Investigate View 326
What do you want to do? 327
Hosts View 329
Workflow 329
What do you want to do? 330
Related Topics 330
Quick Look 331
Hosts View - Autoruns Tab 333
Workflow 333
What do you want to do? 333
Related Topics 334
Quick Look 334
Hosts View - Drivers Tab 337
Workflow 337
What do you want to do? 337
Related Topics 338
Quick Look 338
Hosts View - Files Tab 340
Workflow 340
What do you want to do? 340
Related Topics 341
Quick Look 341
Hosts View - Libraries Tab 344

Workflow 344
What do you want to do? 344
Related Topics 345
Quick Look 345
Hosts View - Overview Tab 348
Workflow 348
What do you want to do? 348
Related Topics 349
Quick Look 349
Hosts View - Process Tab 352
Workflow 352
What do you want to do? 352
Related Topics 353
Quick Look 353
Hosts View - System Information Tab 356
Workflow 356
What do you want to do? 356
Related Topics 357
Quick Look 357
Malware Analysis View 359
Workflow 359
What do you want to do? 360
Related Topics 361
Quick Look 361
Malware Analysis Events List and Files List 367
Workflow 367
What do you want to do? 368
Related Topics 369
Quick Look 369
Manage Column Groups Dialog 374
Workflow 375
What do you want to do? 375
Related Topics 376
Quick Look 377
Manage Default Meta Keys Dialog 380
Workflow 380

What do you want to do? 380
Manage Meta Groups Dialog 384
Workflow 384
What do you want to do? 385
Manage Profiles Dialog 389
What do you want to do? 389
Related Topics 390
Quick Look 390
Navigate View 393
Workflow 393
What do you want to do? 394
Related Topics 395
Quick Look 396
Toolbar 396
Pause/Reload Button and Breadcrumb 401
(Optional) Debug Information 402
Time Banner 402
Visualizations 403
Values Panel 406
Query Dialog 413
Scan For Malware Dialog 418
Select a Malware Analysis Service Dialog 421
Settings Dialogs for Investigate Views 425
Event Analysis View Preferences Panel 431

How NetWitness Investigate Works

NetWitness Investigate provides the data analysis capabilities in RSA NetWitness® Suite, so that analysts can analyze packet, log, and endpoint data and identify possible internal or external threats to security and the IP infrastructure.

Note: In Version 11.1, the Hosts and Files views are part of the NetWitness Suite for analysts to investigate endpoint data.

Metadata, Meta Keys, Meta Values, and Meta Entities

RSA NetWitness Suite audits and monitors all traffic on a network. One type of service, a Decoder, ingests, parses, and stores the packets, logs, and endpoint data traversing the network.

The configured parsers and feeds on the Decoder create *metadata* that analysts can use to investigate the ingested logs and packets. Another type of service, called a Concentrator, indexes and stores the metadata.

The metadata is in the form of a *meta key* and *meta values* for the key. For example, `ip.src` is a meta key, and an IP address that is the source of the traffic is tagged as `ip.src`. When you view data in Investigate, you see the meta key `ip.src` and all of the IP addreses (values) that are tagged with that key. Some meta keys are built-in and others may be custom keys defined by the administrator.

Meta entities are available in Version 11.1 and later. A *meta entity* is an alias that groups together the results from other meta keys. Meta entities organize similar meta keys into a single, easier to use, meta type. Some meta entities are already included by default, and the administrator can create custom meta entities. In Investigate, analysts can use a meta entity in a query, a meta group, a column group, and a profile. Parallel coordinates visualizations do not support meta entities. Administrators can use meta entities to define a query prefix to apply to a user role and a user. The *Decoder Configuration Guide* provides additional information about creating meta entities and how they can be used in rules.

For example, the default Core database language includes distinct meta keys for IP source and IP destination. One of the built-in meta entities named `ip.all` represents the combined set of all IP sources and destinations.

Analysts usually query the Concentrator to discover threats. The Concentrator handles queries, only going to the Decoder when a full reconstruction of sessions or raw logs is required. ESA, Malware Analysis, and Reporting Engine also query the Concentrator, where they can quickly get all the pertinent metadata associated with an event and generate information on the event without having to go to each Decoder. In some special cases, analysts may query a Decoder.

Note: While a hybrid appliance can perform the Concentrator function, a separate Concentrator appliance is required for any large environment that needs greater bandwidth or events per second (EPS). The Concentrator appliance has storage layout that uses solid state drives for the index, which increases read performance.

Triggers for an Investigation

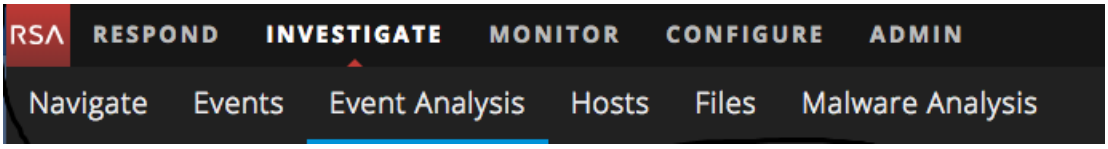
These are a few examples of triggers for an investigation:

- You receive intelligence from a third party about a new active directory hack. Starting in the Events view, you use that intelligence to run a search across all of your raw Active Directory log data for the last 24 hours.
- You are asked by the SOC manager to find any Pokemon Go malware due to its current popularity. Starting in the Navigate view, you craft a query to look for an HTTP session using a specific user agent related to the malware he found on a security blog.
- An incident responder escalates a ticket that shows some odd indicators related to a host. Starting in the Hosts view, you examine that host to find specific details.
- You are looking for the next zero day attack and start pivoting through network metadata in the Navigate view to find any abnormal automated sessions leaving the enterprise.
- You are asked by your SOC manager to find any information related to user `jarvis`, an employee who was just let go. Starting in the Hosts view, you query against the past week for that username.

Workflow of an Investigation

Analysts can investigate data captured by NetWitness Suite, and deep dive from information on a NetWitness Suite dashboard, a NetWitness Respond incident or alert, a report created by the NetWitness Suite Reporting Engine, or a third-party application. During the course of an investigation, analysts can move seamlessly between the views in Investigation: the Navigate view, the Events view, the Event Analysis view, the Hosts view (Version 11.1 and later), the Files view (Version 11.1 and later), and the Malware Analysis view.

This figure illustrates the NetWitness Investigate submenus.



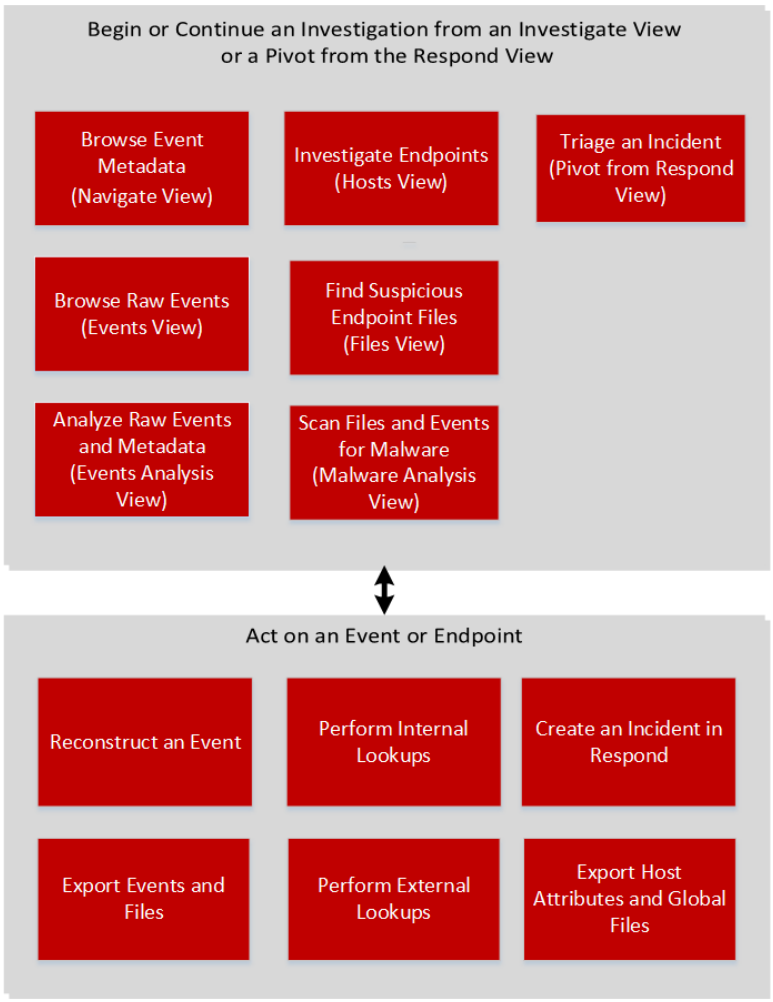
Note: Specific user roles and permissions are required for a user to conduct investigations and malware analysis in NetWitness Suite. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

You can access each view from the Investigate submenu and from other Investigate views. You can also go directly into an Investigate view from NetWitness Respond, and go directly from NetWitness Investigate to NetWitness Respond and standalone NetWitness Endpoint. Your use case determines the starting point for your investigation. This table provides general guidance on the starting view for different use cases.

Go to...	Focus
Navigate view	All meta keys and meta values for logs, endpoints, and packets, grouped by meta key. You can pivot through the data to refine results, then go to the Events view or Event Analysis view, or look up in Malware Analysis or Live. This is the default NetWitness Investigate view. (See Investigating Metadata in the Navigate View.)
Events view	Events are listed in order by time. You can view the raw event and related metadata, view a reconstruction, and download events and files. You can go to the Event Analysis view. (See Examining Raw Events in the Events View)
Event Analysis view	Events are listed in the order by time. You can view all meta keys and meta values for logs, endpoints, and packets. You can view the raw event and related meta data, view a reconstruction that offers helpful cues to identify points of interest in a reconstruction. You can go to the Hosts view, pivot to standalone Endpoint, look up in Live, and do external lookups. External lookups allow you to search the internet for meta values that you interacted with, determine passive DNS information related to an IP address, ascertain if a URL is blacklisted, and other third-party context integrations. (See Examining Raw Events and Meta Data in the Event Analysis View.)

Go to...	Focus
(Version 11.1 and later) Hosts view	Hosts on which the NetWitness Endpoint Insights Agents are running are listed. For every host, you can view processes, drivers, DLLs, files (executables), services, and autoruns that are running, and information related to logged-in users. From the Hosts view, you can go to the Navigate and Event Analysis views. (See Investigate Hosts)
(Version 11.1 and later) Files view	Unique files such as PE, Macho, and ELF in your deployment are listed. For each file, you can view details such as, file size, entropy, format, company name, signature, and checksum. From the **Files** view, you can go to the Navigate and Event Analysis views. (See Investigate Files)
Malware Analysis view	If you are running a Malware Analysis appliance, you can automatically or manually scan files and see the results of four types of analysis: network, static, community, and sandbox. If a file is malware, you can go to the Hosts view to see which hosts downloaded the file. (See Conducting Malware Analysis

Every situation is unique in terms of the types of information the analyst is attempting to find. Many investigations start in one view, and end in a different view as the analyst learns something and then needs to follow that result to a different line of questioning. This figure shows the high-level workflow of an investigation.



Focus on Metadata, Query, and Time

Analysts use NetWitness Investigate to hunt for events that drive the incident response workflow and to do strategic analysis after another tool has generated an event. Beginning in the Navigate view, Events view, or Event Analysis view:

- You start by executing a query on a service for a specific time range, then filter using metadata to a subset of events, reconstruct or analyze an event, and repeat the process to reconstruct or analyze another event.
- When you encounter an event that bears a closer look, you view the context around the event, and decide whether to create an incident or add the event to an incident. If you decide not to

add the event to an incident, you run another query to gain further insight, which starts again at the beginning of the workflow.

- If you notice suspicious activity or files on a specific host in the network, you can gather additional information about the host and files found on the host in the Hosts and Files view, or in a stand-alone NetWitness Endpoint server.
- If you find a file or event that potentially contains malware, you can do a Malware Analysis scan of the file or you can open Malware Analysis and start a scan of the service on which the event was seen.

For example, if there is a concern regarding suspicious traffic with foreign countries, the Destination Country meta key reveals all destinations and the frequency of the contact. Drilling into those values yields the specifics of the traffic, such as the IP address of the originator and the recipient. Checking other metadata can expose the nature of attachments exchanged between the two IP addresses.

Focus on Endpoint Analysis

Analysts use the Hosts and Files view to investigate or perform analysis on the hosts or files using various attributes, such as IP address, host name, Mac address, and so on.

- During an incident triage in the Respond view, review the key information (such as, hostname, filename), and view the context highlights.
- Pivot to Investigate to open the Navigate view. Select the Endpoint Analysis meta group and review the metadata created.
- View the metadata in the Event Analysis view to analyze the events. Select the host lookup using the Event Meta panel.
- In the Hosts view, click on the hostname to view the summary of the endpoint data, snapshots, security configurations, and so on.
- Perform an on-demand scan to get the most recent information (if required).
- Search on all snapshots for a specific filename, path, or hash to narrow the search.
- Review the processes, autoruns, files, libraries, drivers, and system information to investigate further.
- In the Files view, filter the files using a few indicators (such as, file name, file size, entropy, format, company name, signature, checksum) and pivot to the Navigate view to see if it exists on other hosts in the network.

Focus on NetWitness Respond Incidents and Alerts

An analyst who is working on an incident or an alert in NetWitness Respond can open it in NetWitness Investigate (Navigate view) to do a deeper analysis of the event or alert.

- The workflow to respond to an incident typically begins in the Respond view, where the analyst who is investigating an incident needs to gather intelligence about the incident in NetWitness Investigate. After you launch an investigation from NetWitness Respond, defined meta keys are queried and the contents of captured packets, logs, and endpoint events is displayed in the Navigate view.
- If you find events that are relevant to the incident, you can add the events to the incident in Respond. You can also create a new incident in Respond based on one or more events found in Investigate.

NetWitness Investigate Views

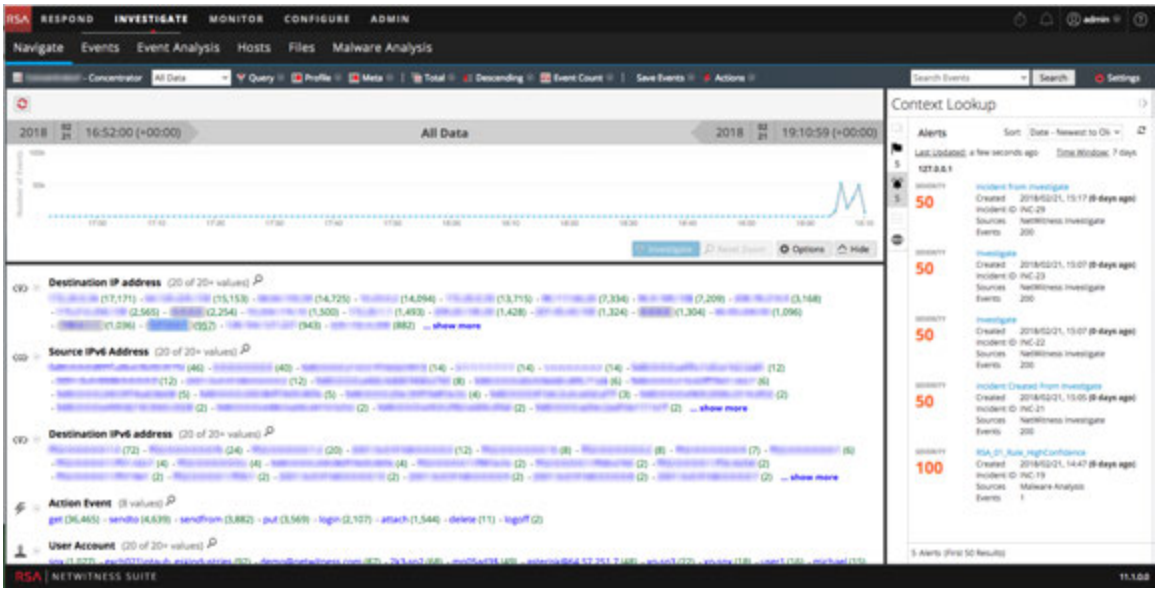
This section provides a brief description and example of each main view (Navigate, Events, Event Analysis, Hosts, Files, and Malware Analysis) and introduces views that provide two deep-dive capabilities: additional context for data found and event reconstruction.

Navigate View

The Navigate view provides the capability to drill into and query contents of captured packets, logs, and endpoint events on a Broker, Concentrator, or Decoder (though investigating a Decoder is not typical).

- When you select a service, the defined meta keys for that service are queried, and values are returned along with the number of events. Clicking on a value at any given level, reveals the results in detail.
- For certain configured meta keys, such as IP address, or hostname, you can search for additional context information around a value using the Context hub. The additional context may include incidents, alerts, and other sources where the value was mentioned.
- The Navigate View also provides a sequential visualization of the data in a timeline. Here you can zoom in on a selected time period.

This figure illustrates the Navigate view.

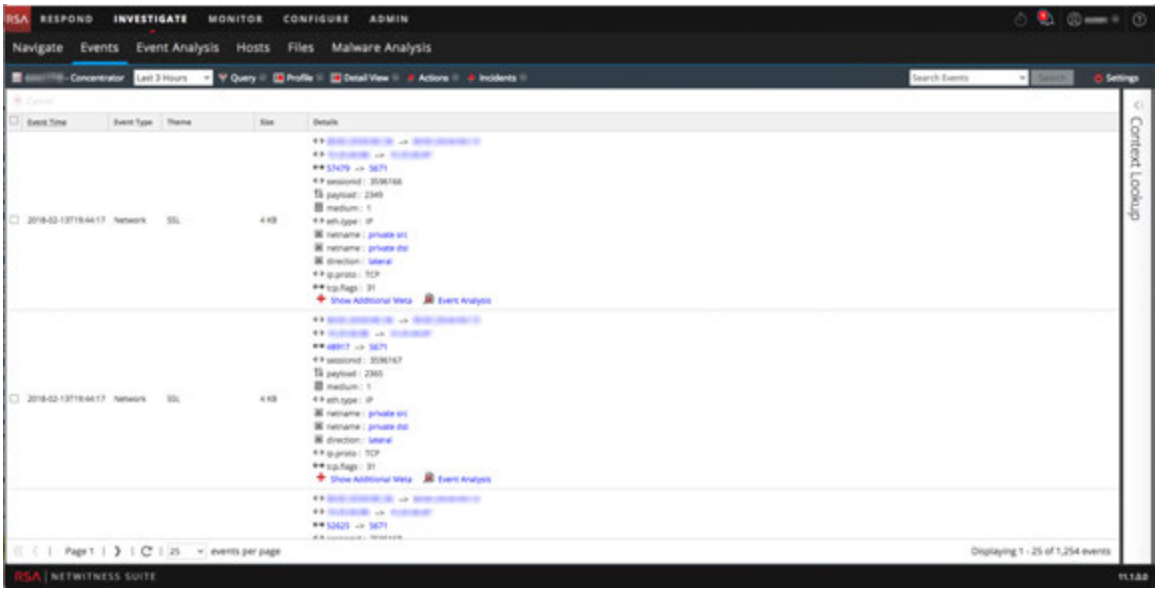


Events View

The Events view provides a view of packet, log, and endpoint events in list form so that you can view events sequentially and reconstruct events safely.

- You can open the Events view for a meta value that you see in the Navigate view.
- For analysts without sufficient privilege to navigate a service, the Events view is a standalone investigation view in which analysts can access a list of network, log, and endpoint events from a NetWitness Suite Core service without having to drill down through metadata first.
- The Events view presents event information in three standard forms, a simple grid listing of events, a detailed listing of events, and a log view.
- You can export events and associated files, and create an incident from an event.

This figure illustrates the Events view.

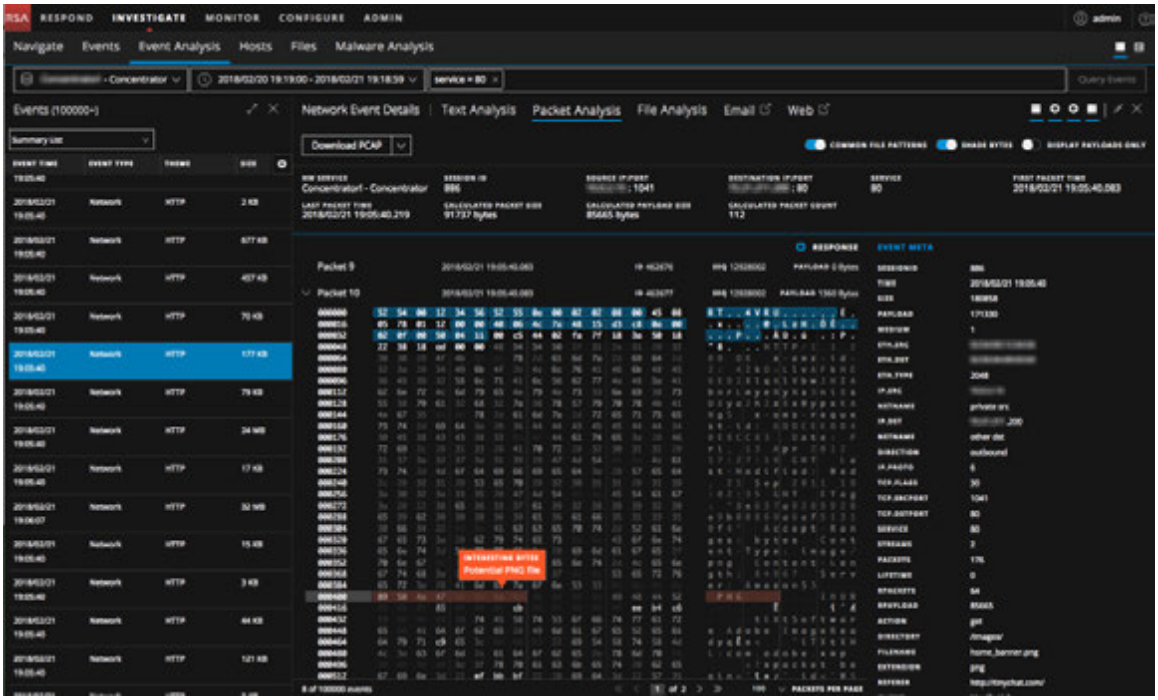


Event Analysis View

The Event Analysis view is an interactive tool to help analysts see the packets, text, or files in an event with visual cues for certain types of information. Depending on the type of reconstruction, for example, packets, text, or files, different information is relevant.

- When viewing files, you can export files in a zip archive to your local file system.
- You can download logs from the Text view, and export packets from the Packet view.

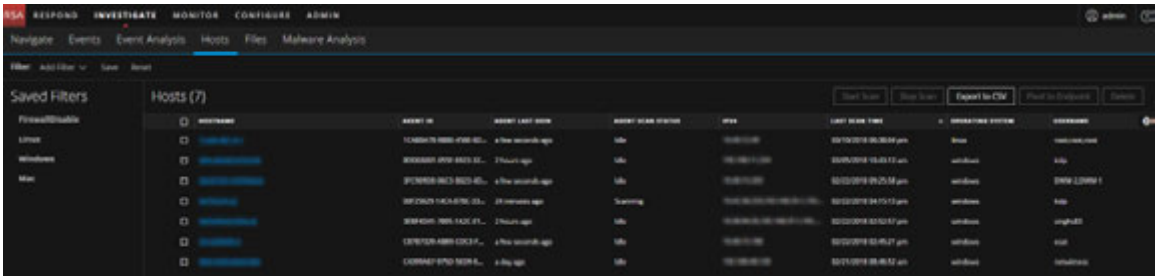
This figure is an example of the Event Analysis view.



Hosts View

The Investigate > Hosts view lists all hosts with an agent. By default, the hosts are listed based on the last scan time, with the most recently scanned hosts at the top of the list. It provides the capability to drill into the details of the host for investigation.

This figure is an example of the Hosts view.



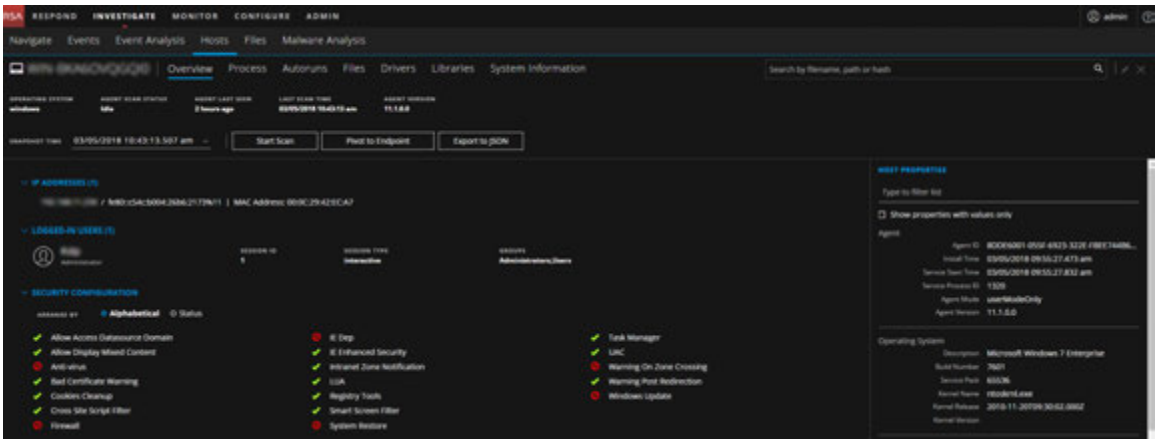
In this view, you can:

- Filter and sort hosts to narrow down on the host investigation
- Export the host attributes to a CSV file
- Start or stop a scan for the selected hosts
- Drill-down for host details

- Pivot to the Navigate or Event Analysis view to investigate on the host
- Delete hosts

Note: If you have NetWitness Endpoint 4.4.0.2 or later in your deployment, the hosts on which the 4.4.0.2 agent is installed are listed, and can be identified using the agent version. For more information on how you can investigate these hosts, see Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts.

To view details of a host, click on the hostname. The following screen is displayed:



You can:

- Search on all snapshots (file name, file path, and file SHA-256 checksum are the supported search fields).
- View multiple snapshots. By default, the data for the latest snapshot is displayed.
- View additional host information in the following tabs: Overview, Processes, Autoruns, Files, Driver, Libraries, and System Information.
- Export all categories of endpoint data for the selected host for a specific snapshot in the JSON format.

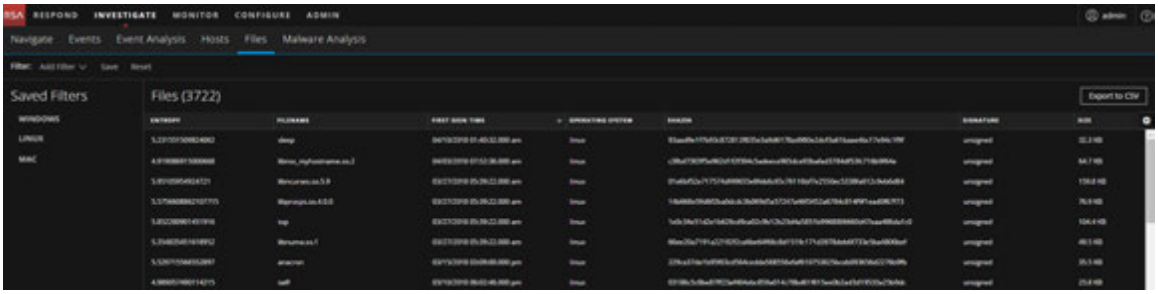
Files View

The Files view provides a list of unique files found in your deployment and their associated properties. By default, the files are listed based on the first seen time. The following file types, loaded in the memory, are collected during the scan.

- Portable Executable (PE) (Windows) - These are exe, dll, and sys files. You can view the following properties for each file - checksum, compile details, different sections present in the file, imported libraries, and certificate details (signer, thumbprint, company name).

- Macho (Mac) - These are app bundles, dylibs, and kernel extensions. You can view the following properties for each file - checksum, different sections present in the file, imported libraries, and certificate details (signer, thumbprint, company name).
- Executable and Linkable Format (ELF) (Linux) - Each file contains information about checksum, different sections present in the file, and imported libraries. You can view the following properties for each file - checksum, different sections present in the file, and imported libraries.

This figure is an example of the Files view.



In the Files view, you can:

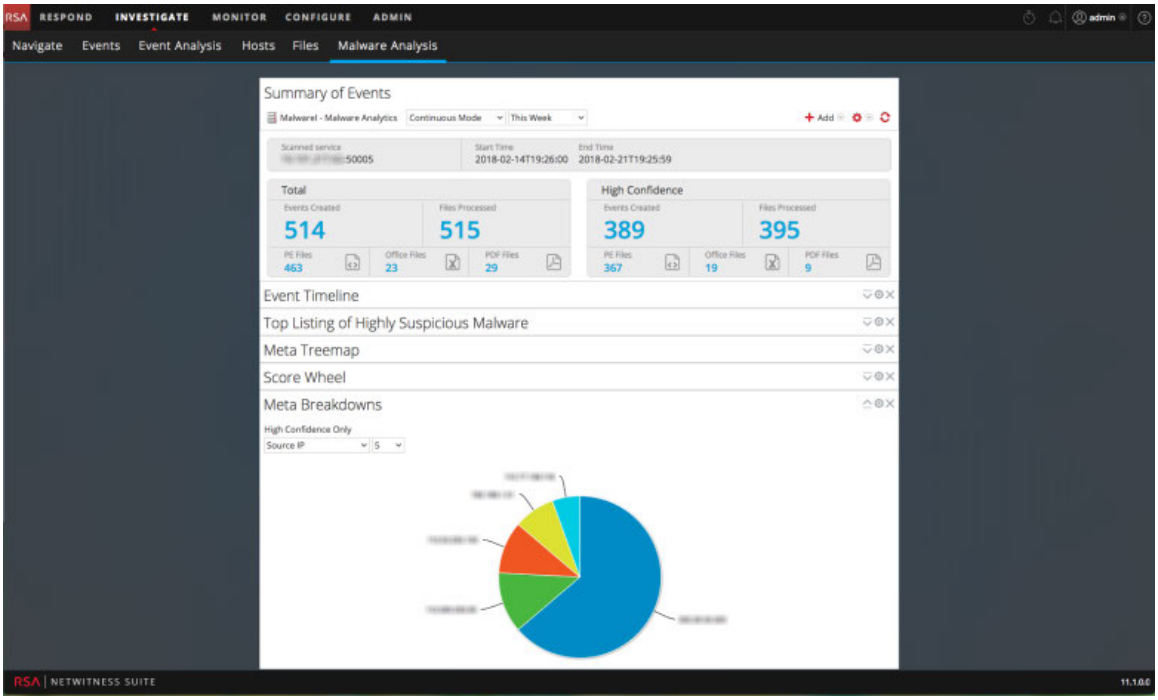
- Filter and sort files to narrow down on the investigation
- Pivot to the Navigate or Event Analysis view to investigate on the file
- Export the files to a CSV file

Malware Analysis View

The Malware Analysis view provides a means to analyze certain types of file objects (for example, Windows portable executable (PE), PDF, and MS Office) to assess the likelihood that a file is malicious.

- You can open the Malware Analysis view directly or you can use a context menu action to Scan for Malware from a meta value in a current drill point from the Navigate view.
- The malware analyst can leverage the multilevel scoring modules to prioritize the massive number of files captured in order to focus analysis efforts on the files that are most likely to be malicious.

This figure illustrates the Malware Analysis view.

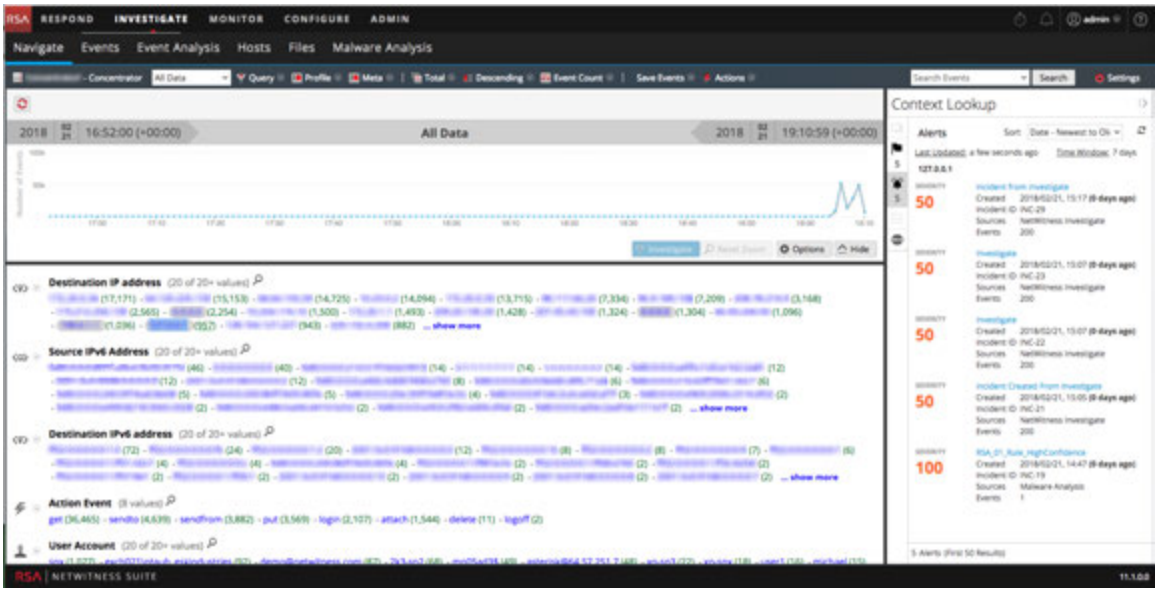


Contextual Information for an Event

In the Navigate view and the Events view, the Context Lookup panel shows details about elements associated with an event (IP Address, User, Host, Domain, MAC Address, Filename, File hash) in the Context Hub.

- You can interact with the elements of an event to get further insight including related incidents, alerts, custom lists, Archer assets, active directory details, and NetWitness Endpoint IIOCs.
- You can click on a data point to return to the Navigate view.

The following figure shows the Context Lookup panel in the Navigate view.



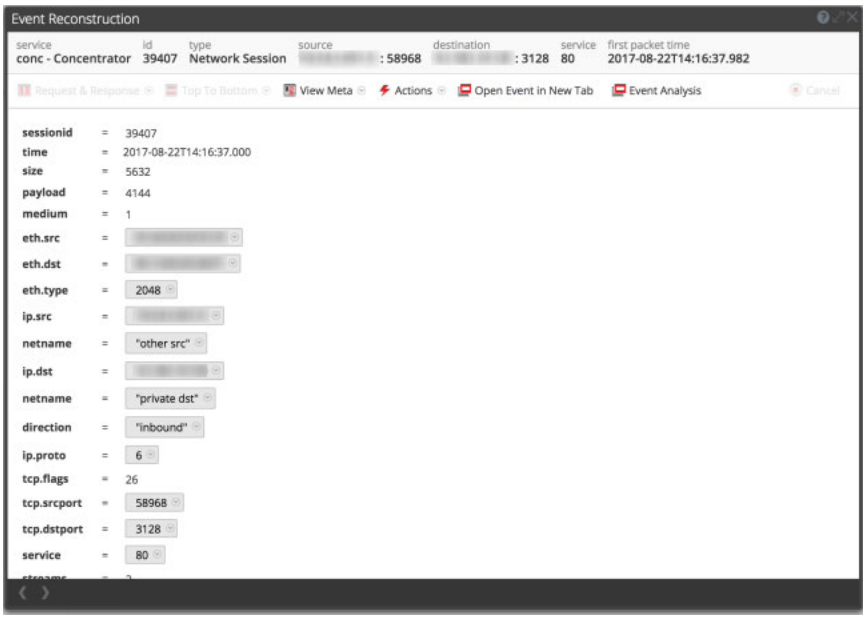
Note: For the NetWitness Endpoint, the context lookup is only available for the NetWitness Endpoint 4.4.0.2 or later hosts but not for the NetWitness Endpoint 11.1 hosts.

Event Reconstruction

Three NetWitness Investigate views offer the ability to reconstruct an event: Navigate view, Events view, and Event Analysis view. When you discover an event that merits additional investigation, you can reconstruct an event safely in a form similar to its native form. The rendering of events restricts the use of dynamic or active code that might be contained in the event to limit any adverse outcome to your system or browser. Cache is used to improve performance when viewing previously viewed events. Each analyst has a separate cache of reconstruction data, and you can only access reconstructed events in your own cache.

The Event Reconstruction in the Events view or the Navigate view presents the raw data and the meta keys and meta values for an event in a list form .

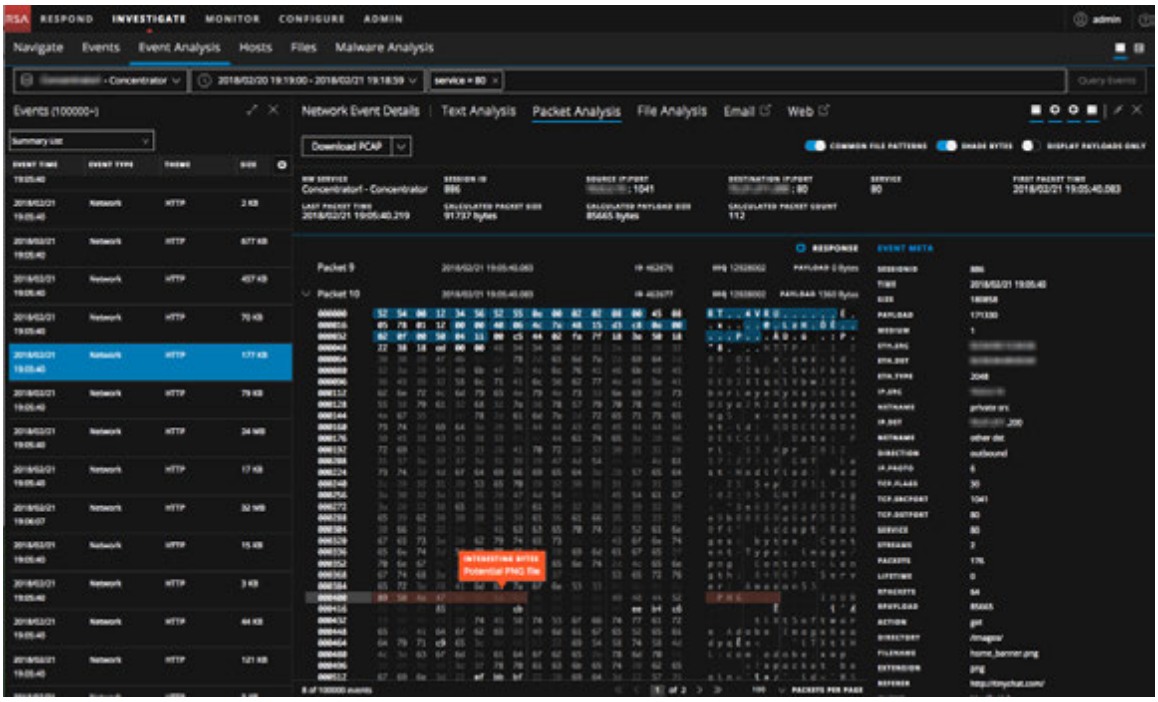
- You can page through the reconstruction to view the next event in this form.
- Events can be reconstructed using different methods to suit the type of data: meta data, text, hexadecimal, packets, web, mail, files, or the best reconstruction selected automatically.
- You can export packet capture files, extract files, and export the meta values for the event. This figure is an example of the Event Reconstruction.



The Event Analysis view present a interactive event reconstruction, which includes raw data, meta keys and values. Interactive options:

- Highlight and decode information in headers and payloads.
- Identify common file signatures.
- Allow you to search for locations of certain meta keys or values in the reconstruction.
- You can export events and files.

This figure is an example of a reconstruction in the Event Analysis view.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
Navigate
Events
Event Analysis
Hosts
Files
Malware Analysis
Network Event Details
Text Analysis
Packet Analysis
File Analysis
Email
Web
Download PCAP

Configuring NetWitness Investigate Views and Preferences

Analysts can configure some aspects of NetWitness Investigate views and behavior. You can customize the way that Investigate views appear, the types of information displayed, and factors that affect performance in returning results and reconstructing events. All configurable settings have default values that are effective in most deployments; however, analysts have the option to adjust these if necessary.

Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles and permissions as described in the *System Security and User Management Guide*. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

These topics provide details:

- Configure the Navigate View and Events View
- Configure the Event Analysis View
- Configure the Malware Analysis Summary of Events View

Configure the Navigate View and Events View

Analysts can set preferences that affect performance and behavior of NetWitness Suite when analyzing data using the Navigate view and Events view. Some of the same settings are available in two places in NetWitness Suite, and changes made in either location are applied in the other view:

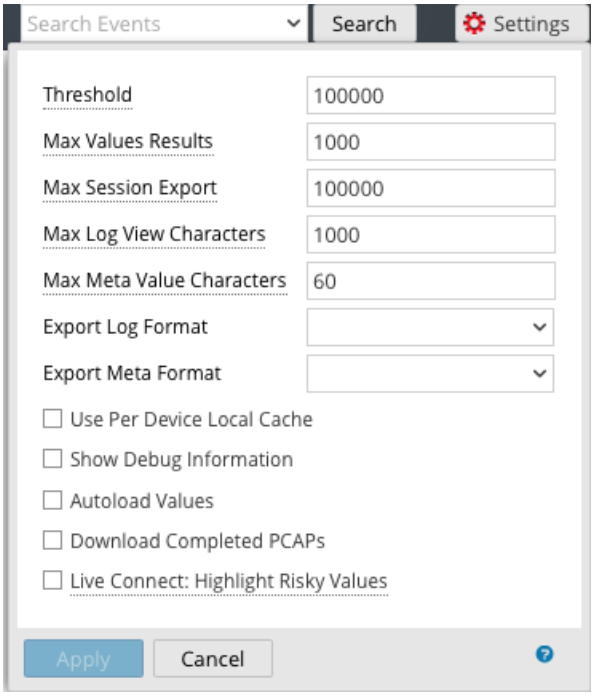
- Investigate view > Settings dialog for the Navigate view and the Events view.
- Profiles > Preferences panel > Investigation tab.

There are also configurable settings in the Search Options drop-down from the Search field in the Navigate view and the Events view.

Access the Navigate View and Events View Settings

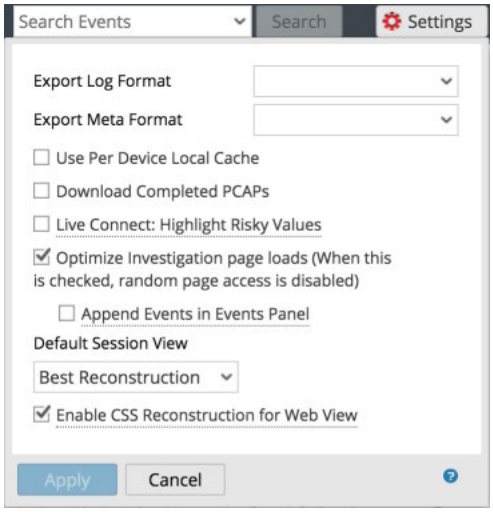
To access the settings, do one of the following:

- In the **Navigate** view toolbar, select the **Settings** option.
  The Settings dialog for the Navigate view is displayed. Version 11.0 included a setting to Append Events in Events Panel, and this has been moved to the Events view settings panel.



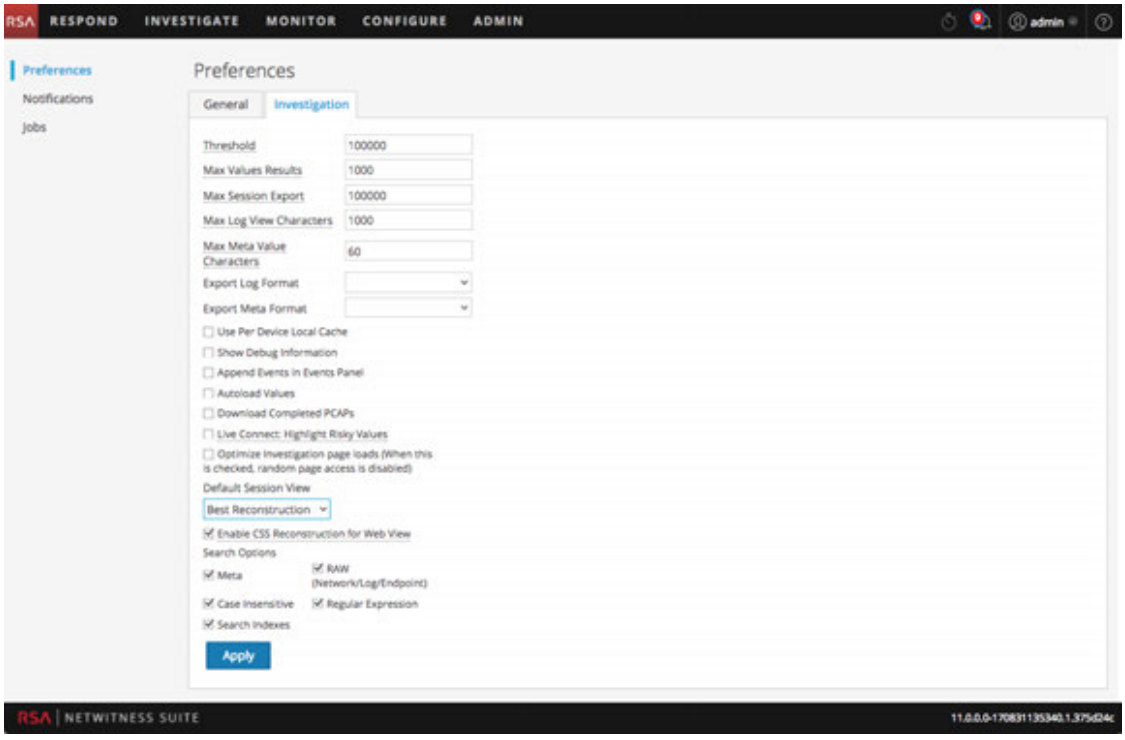
- In the **Events** view toolbar, select the **Settings** option.
  The Settings dialog for the Events view is displayed. Version 11.1 and later includes the

Append Events in Events Panel setting.



- In the top right corner of NetWitness Suite, go to > , Profile, and in the**Preferences** panel click the **Investigation** tab.

  The Investigation panel is displayed.



Calibrate Navigate View Value Loading Parameters

Several settings influence the performance of NetWitness Suite when loading values in the Values panel. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations.

To adjust these settings:

1. Go to the **Investigation** tab or to the **Settings** dialog for the Navigate view.
2. Adjust the following parameters:

- **Threshold:** Set the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.
- **Max Values Results:** Set the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
- **Max Session Export:** Specify the number of events that can be exported in a single PCAP or Log file.
- **Max Log View Characters:** Set the maximum number of characters to be displayed on **Investigate > Events > Log Text**. The default value is **1000**.
- **Max Meta Value characters:** Set the maximum number of characters in a meta value name displayed in the Navigate view Values panel. The default value is **60**.
- **Show Debug Information:** If you want NetWitness Suite to display the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker, check this option. The default value is **Off.**
- **Append Events in Events Panel:** This option affects paging in the Events panel and is described below under "Calibrate Events View Retrieval and Default Reconstruction."
- **Autoload Values:** If you want NetWitness Suite to automatically load values for the selected service in the Navigate view, check this option. When not selected, NetWitness Suite displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.

3. Click **Apply**.

The settings become effective immediately and are visible the next time you load values.

Configure Navigate View and Events View Parameters

Several settings influence the performance of NetWitness Suite when loading values in the Navigate view and the Events view. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations. You can set these parameters separately in the Navigate view and the Events view. When configured in one view, the setting does not automatically apply to the other view.

To adjust these settings:

1. Go to the **Investigation** tab or to the **Settings** dialog for the Navigate view or the Events view.
2. Adjust the following parameters:
   -Live Connect: Highlight Risky Values: If you want NetWitness Suite to highlight and display only IP addresses that are considered as risky by RSA community, check this option. When not selected, NetWitness Suite displays all IP addresses. By default, this option is not selected (**Off**).
   -Use Per Device Local Cache: You can specify the use of locally cached data from the selected service. By default, this option is not selected **(Off)**. When unchecked, Investigate sends a fresh query to the database rather than displaying cached data in the Investigate views after the initial load. If checked, Investigate uses the data from local cache.
   -Download Completed PCAPs: You can automate the downloading of extracted PCAPs in the Navigate view and Events view so that the browser downloads the extracted PCAP and opens it in the default application for opening PCAP files, such as Wireshark. By default, this option is not selected (**Off**). If you are going to enable this option, ensure that an application that can open PCAPs is installed on your local file system and that the application is set as the default application to handle PCAP file formats.
   Live Connect: Highlight Risky Values: If this option is unchecked, all the meta values that have context available in Live Connect are highlighted in the Navigate view Values panel. If the option is checked, among the values that have context in Live Connect, only those values deemed Risky/Suspicious/Unsafe by the community are highlighted. By default this option is unchecked (**Off**).
3. Click **Apply**.
   The settings become effective immediately.

Configure the Default Log Export Format

You can export logs from the Navigate view and Events view in different formats. Available options are Text, XML, comma-separated values (CSV), JSON. There is no built-in default value for the log export format. If you do not select a format here, NetWitness Suite displays a selection dialog when you invoke export of logs.

To select the format for exported logs:

1. Go to the **Investigation** tab or to the **Settings** dialog for the Navigate view, Events view, or Event Analysis view.
2. Select one of the options from the **Export Log Format** drop-down menu.
3. Click **Apply**.
   The setting goes into effect immediately.

Configure the Default Meta Export Format

You can export meta values from the Navigate view and Events view in different formats. Available options are Text, CSV, tab-separated values (TSV), and JSON. There is no built-in default value for the meta export format. If you do not select a format here, NetWitness Suite displays a selection dialog when you invoke export of meta values.

To select the format for exported meta values:

1. Go to the **Investigation** tab or to the **Settings** dialog for the Navigate view or Events view.
2. Select one of the options from the **Export Meta Format** drop-down menu.
3. Click **Apply.**
   The setting goes into effect immedia tely.

Calibrate Events View Retrieval and Default Reconstruction

You can configure several parameters that control the how NetWitness Suite retrieves events and reconstructs events in the Events view. To do so:

1. Go to the **Investigation** tab or to the **Settings** dialog for the Events view.
2. Configure the following parameters.
   -Optimize Investigation page loads: Set a paging option. When optimized, results are returned as quickly as possible, sacrificing the original ability to go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is **enabled**.
   -Default Session View: Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.
3. Navigate to the **Investigation** tab or to the **Settings** dialog for the Navigate view and set the **Append Events in Events Panel** option. When this option is selected, the events displayed in the **Events Panel** are added incrementally. For example, each time you click the next page icon, the next increment of events is added, at first you see 1 to 25, then 1 to 50, then 1 to 75 and so on. This option is available only if the **Optimize Investigation Page Loads** option is enabled.
4. To activate the changes immediately, click **Apply**.

Enable or Disable Cascading Style Sheet Rendering in Web Content Reconstructions

Analysts can enable the use of cascading style sheets (CSS) when reconstructing web content. If enabled, the web reconstruction includes CSS styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Disable this option if there are problems viewing specific websites.

Note: The appearance of the reconstructed content may not match the original web page perfectly if related images and style sheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically through the client side javascript will not render in the reconstruction because all client side javascript is removed for security purposes.

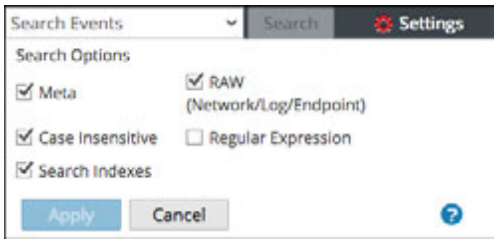
To enable or disable this option:

1. Go to the **Investigation** tab .
2. Click the **Enable CSS Reconstruction for Web View** checkbox.
3. Click **Apply**.
   The setting becomes effective immediately and is visible in the next web content reconstruction.

Configure Search Options

You can configure search options to apply when you type a search string in the Search field.

1. Click in the **Search** field of the Events view or the Navigate view to display the Search Events drop-down menu.



2. Select one or more search options to apply to the search. Search for Text Patterns provides detailed information about each option.
3. To save the search settings, click **Apply**.
   The preferences are saved and effective immediately.

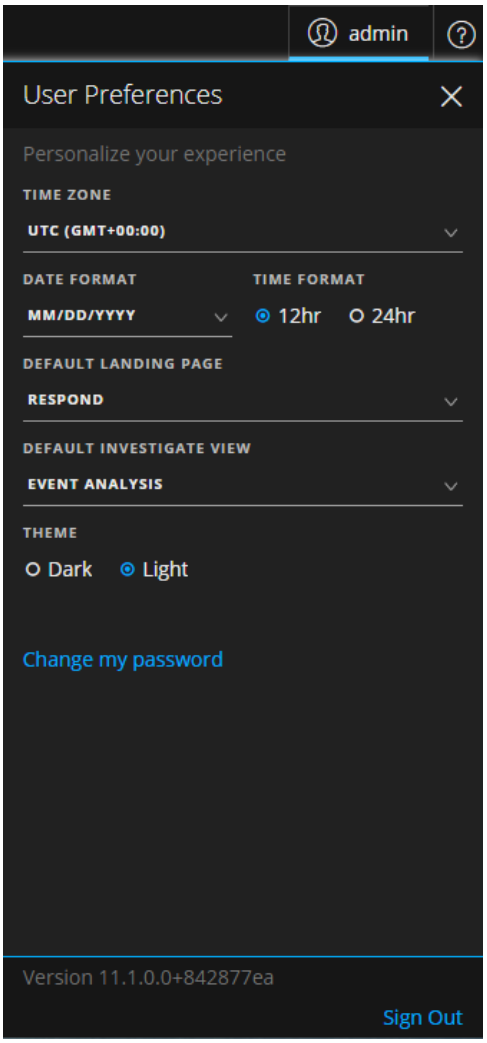
Configure the Event Analysis View

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

Beginning with Version 11.1, analysts can set preferences that affect the behavior of NetWitness Suite when analyzing data using the Investigate > Event Analysis view. The main toolbar in Investigate has a different appearance when the Event Analysis view is open; these two buttons give access to preferences dialogs: and . The User menu ( ) is focused on global user preferences such as time zone, while the Event Analysis preferences menu () is focused on user preferences for behavior in the Event Analysis view. The rest of this section describes both sets of preferences.

Set the Default Investigate View

The default Investigate view is set in the global User Preferences dialog (in the upper right corner of the NetWitness Suite browser window, select).
The User Preferences dialog shows your current preferences for the Investigate view. You can select the default view when you open Investigate here: Navigate view, Events view, Event Analysis view, Hosts view, Files view, or Malware Analysis view.



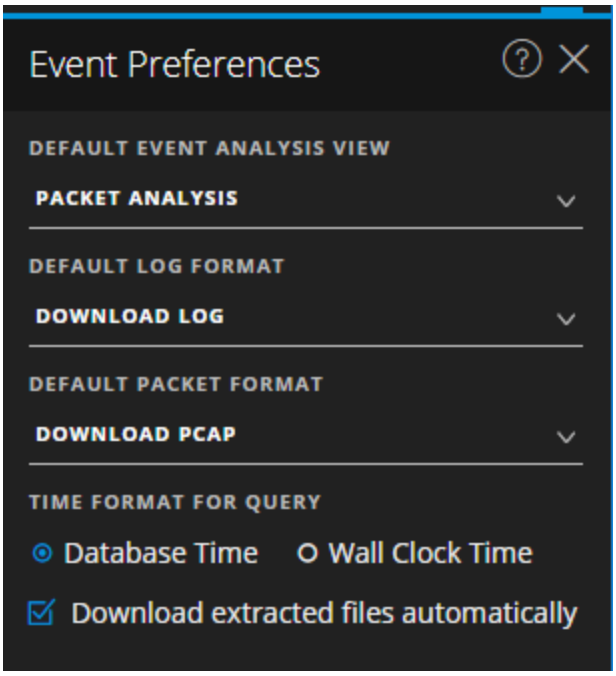
The global user preferences are described in detail in the *NetWitness Suite Getting Started Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Configure the Event Analysis View

In Version 11.1, you can set preferences relevant to the Event Analysis view. The preferences selected here persist per user and are available whenever the specific user logs in to the application.

To set default values for working in the Event Analysis view:

1. With the Event Analysis view open, click .



2. In the **Default Event Analysis View** drop-down menu, select the default reconstruction type when you open an event in the Event Analysis panel: **Text Analysis**, **Packet Analysis**, **File Analysis**.
   If you have not selected a default analysis type, when you open an event, the default reconstruction type is the Packet Analysis, except for log and endpoint events, which open to the Text Analysis. If you select a default reconstruction type, the reconstruction type is the default reconstruction that you specified. In both cases, the default is the starting point, and if you change the type while you are working, the type you choose is used for the next reconstruction.
3. In the **Default Log Format** drop-down, select the download format for exporting logs: **Download Log**, **Download XML**, **Download CSV**, or **Download JSON**. If you do not select a format here, the default download format is **Download Log**. These options are also available at the time of download in a drop-down menu.
4. In the **Download PCAP** drop-down menu, select the default format for downloading packets. These options are also available at the time of download in a drop-down menu:
   Download PCAP to download the entire event as a packet capture (*.pcap) file
   Download All Payloads to download the payload as a *.payload file
   Download Request Payload to download the request payload as a *.payload1 file
   Download Response Payload to download the response payload as a *.payload2 file

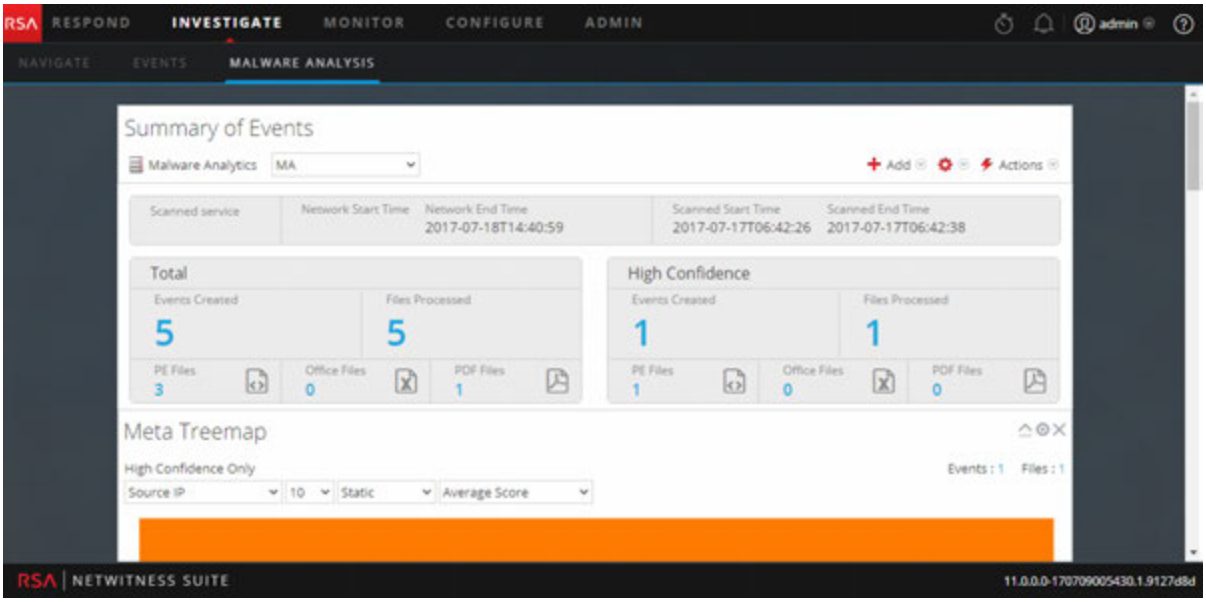
5. Under **Configure the Time Format for queries**, choose either **Database Time** or **Wall Clock Time**. The Event Analysis view can display results based on the database time or the current clock time. When you set the time format here, your individual user preference is saved until changed again. The default setting for this preference is **Database Time**, which is the same time format used to display query results in the Navigate view and Events view.
   When **Database Time** is selected, the start and end time for a query is based on the time that the event was stored.
   When **Wall Clock Time** is selected, the query is executed with current time in accordance with the timezone set in user preferences.

Configure the Malware Analysis Summary of Events View

The Summary of Events provides a summary of the scan being investigated, and below the summary are configurable dashlets such as visualization charts and listings. By default, the Summary of Events for a scan opens with the default dashlets displayed. You can customize the view by adding, modifying, and deleting default dashlets. The configured customization of dashlets persists through different scan investigations, and you can restore default dashlets at any time. The default dashlets are:

- Summary of Events (Fixed)
- Event Timeline
- Top Listing of Highly Suspicious Malware
- Meta Treemap
- Score Wheel
- Meta Breakdowns

The following figure is an example of the default Summary of Events.



The rest of this topic provides instructions for managing and configuring dashlets.

Add a Dashlet

You can add multiple copies of dashlets in the Malware Analysis Summary of Events. To add a dashlet:

1. In the toolbar, select **Add**.
   The drop-down list of dashlets is displayed. There are four visualization options: Score Wheel, Meta Treemap, Meta Breakdowns, and Event Timeline. The other three dashlets are the same dashlets available in the NetWitness Suite dashboard: Malware with high Confidence IOCs and High Scores, Top Listing of Highly Suspicious Malware, Top Listing of Possible Zero Day Malware. Details for these common dashlets are provided in "Dashlets" in the RSA Content for RSA NetWitness Suite.
2. Select a dashlet.
   The new dashlet is added as the last dashlet below the existing dashlets.
3. If the dashlet is a duplicate of an existing dashlet, change the name of the new dashlet so that it is unique.

Modify or Delete a Dashlet Using Toolbar Options

Each dashlet has a toolbar that offers options for modifying the dashlet. The visualization charts have the same configuration settings, while some of the other dashlets have different additional settings.

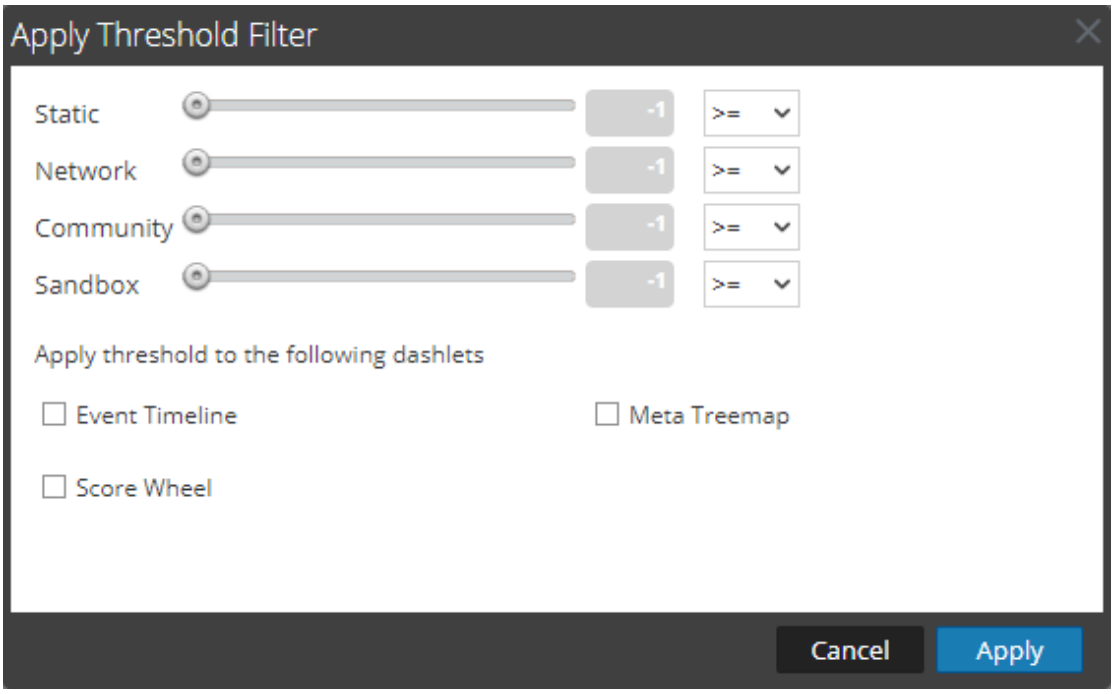
To use the toolbar options:

- To close a dashlet so that only the title bar is displayed, click .
- To open a dashlet that is closed, click .
- To display the configurable settings for a dashlet, click .
  The settings dialog for the dashlet is displayed.
- To delete a dashlet, click .

Apply Threshold Filter to Multiple Dashlets

Within dashlets, you can set a threshold to show only events equal to, above, or below a certain score in the four categories (Static, Network, Community, and Sandbox). This procedure sets the thresholds by dashlet type for these dashlets: Event Timeline, Score Wheel, and Meta Treemap. You can also set the threshold for individual dashlets.

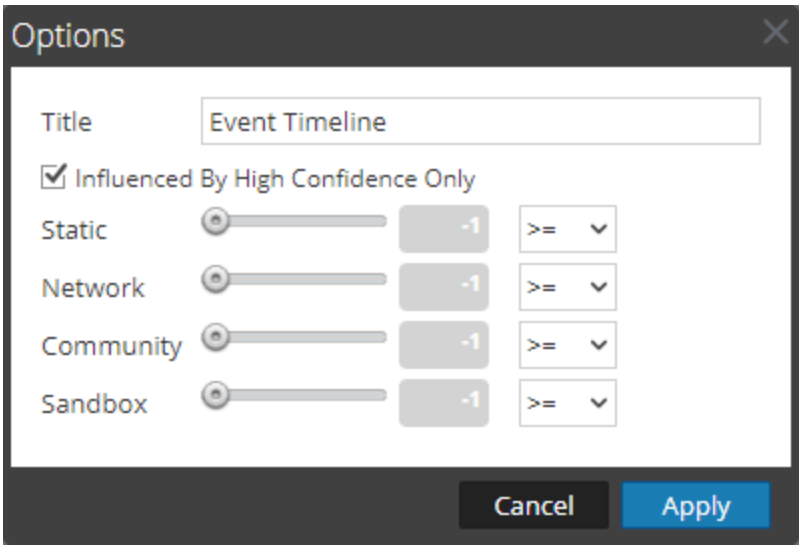
1. In the toolbar, select > **Apply Threshold Filter**.
   The Apply Threshold Filter dialog is displayed.



2. Select one or more dashlet types: Event Timeline, Score Wheel, and Meta Treemap.
3. Drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.
4. Click **Apply**.
   The threshold filters are applied to the selected dashlet types in the Summary of Events.

Set Title and Category Options for a Dashlet

1. To display the configurable settings for a dashlet, click ⚙.
   The Options dialog for the dashlet is displayed.

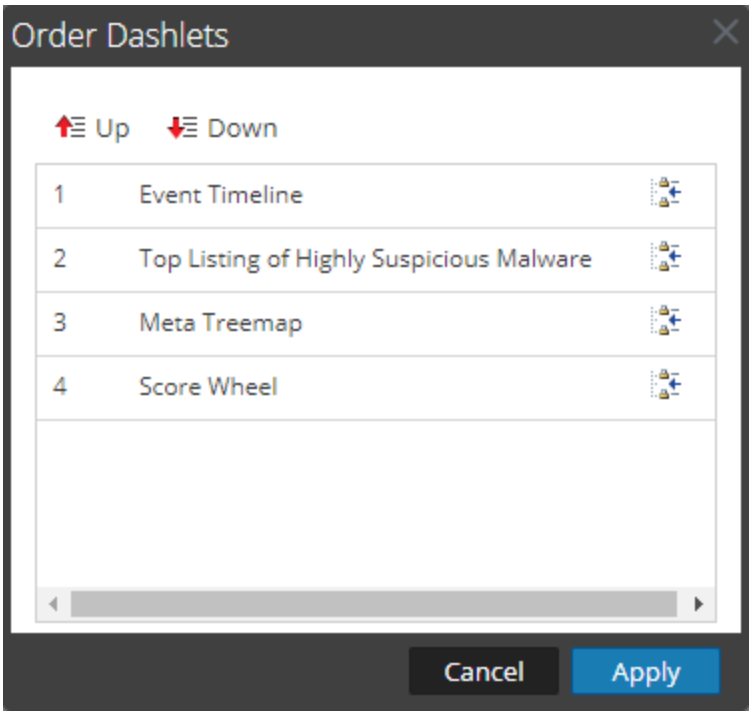


2. Type a new title for the dashlet in the **Title** field.
3. If you want to see only events that are influenced by a High Confidence tag, which means there is high confidence that the event contains harmful code, check the **Influenced By High Confidence Only** option.
4. If you want to see only events that were given a score above a certain score in the four categories (Static, Network, Community, and Sandbox), drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.
5. Click **Apply**.
   The title and filters are applied to the dashlet.

Order Dashlets

To change the order of dashlets as they appear beneath the Summary of Events:

1. In the toolbar, select > **Order Dashlets**.
   The Order Dashlets dialog is displayed.



2. Select a dashlet that you want to move up or down, and click Up or Down.
3. When you are satisfied with the order, click **Apply**.
   The dialog closes and the order of dashlets below the Summary of Events is changed to match your choices.

Restore Default Dashlets

After you have added, modified, and arranged dashlets, you can revert to the default settings for dashlet display. To restore the default dashlets:

1. In the toolbar, select > **Restore Default Configuration**.
   A dialog requests confirmation that you want to restore the configuration.
2. Do one of the following:
   a. If you decide to keep the dashlet arrangement you have configured, click **No**.
   b. If you are sure that you want to restore the defaults, click **Yes**,
      The dashlet display reverts to the default display.

Beginning an Investigation

NetWitness Suite offers differen starting points based on the question you are attempting to answer: Navigate view, Events view, Event Analysis view (Version 11.1), Hosts view (Version 11.1), Files view (Version 11.1), and Malware Analysis view.

Note: Specific user roles and permissions are required for a user to conduct investigations in NetWitness Suite. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you. The Hosts view and Files view are available in Version 11.1 and above. The Event Analysis view is available in Version 11.0, but the method of accessing it is through the Events view.

Focus on Metadata, Raw Events, and Event Analysis

To hunt for events that drive the incident response workflow and to do strategic analysis after another tool has generated an event, you should begin in the Navigate view, Events view, or Events Analysis view. You investigate the metadata for a single Broker or Concentrator. In each of these views, you start the investigation by opening the view, where you can execute a query and filter the results by narrowing the time range and querying metadata. These topics provide details about beginning an investigation in each view:

- Begin an Investigation in the Navigate or Events View
- Begin an Investigation in the Event Analysis View

Focus on Hosts and Files

To hunt for information on hosts that have the agent running, begin the investigation in the Hosts view (**Investigate > Hosts**). For every host, you can see processes, drivers, DLLs, files (executables), services, and autoruns that are running, and information related to logged-in users. (See Investigate Hosts)

You can begin the investigation on files in your deployment in the Files view (**Investigate > Files**). (See Investigate Files.)

Focus on Scanning Files for Malware

To scan files for potential malware, or set up a continuous scan of a service, you begin in the Malware Analysis view. Results are expressed as four types of analysis: network, static, community, and sandbox with an indicator of compromise (IOC) rating. There are several ways to begin working in Malware Analysis:

- You can begin Malware Analysis from the Malware Analysis dashlets in the Monitor view to quickly see the riskiest potential threats.
- You can go to **Investigate > Malware Analysis** to opne the Malware Analysis Summary of Events.
- You can right-click ameta key in the Navigate view, and select **Scan for Malware**.

See Conducting Malware Analysis for details on working in the Malware Analysis view.

Begin an Investigation in the Navigate or Events View

The Navigate view is the default view for Investigate unless you have selected a different view as your opening view. This user preference is set on the application level as described in Configuring NetWitness Investigate Views and Preferences. In these views, you are hunting for events of interest based on a query. In the Navigate view you can also refine results by clicking on meta keys and meta values. When you find interesting events, you can take a closer look at the event in the other Investigate views.

To begin an investigation in the Navigate view or Events view, a service must be specified.

- NetWitness Suite opens the Navigate view or the Events view with the user-specified default service selected.
- If no default service is currently specified and the service id is not in the URL, NetWitness Suite presents a dialog for selecting the service or collection to investigate.
- When a service has been selected manually or by default in the Navigate view or Events view, you can change the service or collection to investigate by selecting the service name in the toolbar. NetWitness Suite presents the dialog for selecting the service to investigate.

Note: The Archiver service does not appear in the Navigate view to minimize user experience of slow performance when performing investigations. The Archiver is available in the Events view for log exports and enhanced search capabilities.

With a service or collection selected, NetWitness Suite is ready to load data for the service or collection. It is recommended that you also select a time range so that results load faster. Several settings in the Navigate View and Events View Settings dialog or the Profiles > Preferences panel > Investigations tab affect the loading process: Threshold, Max Values Results, Show Debug Information, Autoload Values, and Optimize Investigation page loads (see Configure Investigation Views and Preferences).

Note: In the Events view data loads automatically. If you specified Autoload Values in the Navigate view preferences, NetWitness Suite populates the data automatically. Otherwise, you must select the Load Values button. NetWitness Suite populates the meta data in the Navigate view Values panel and results become visible almost immediately.

The rest of this topic provides instructions for beginning the investigation of data on a service.

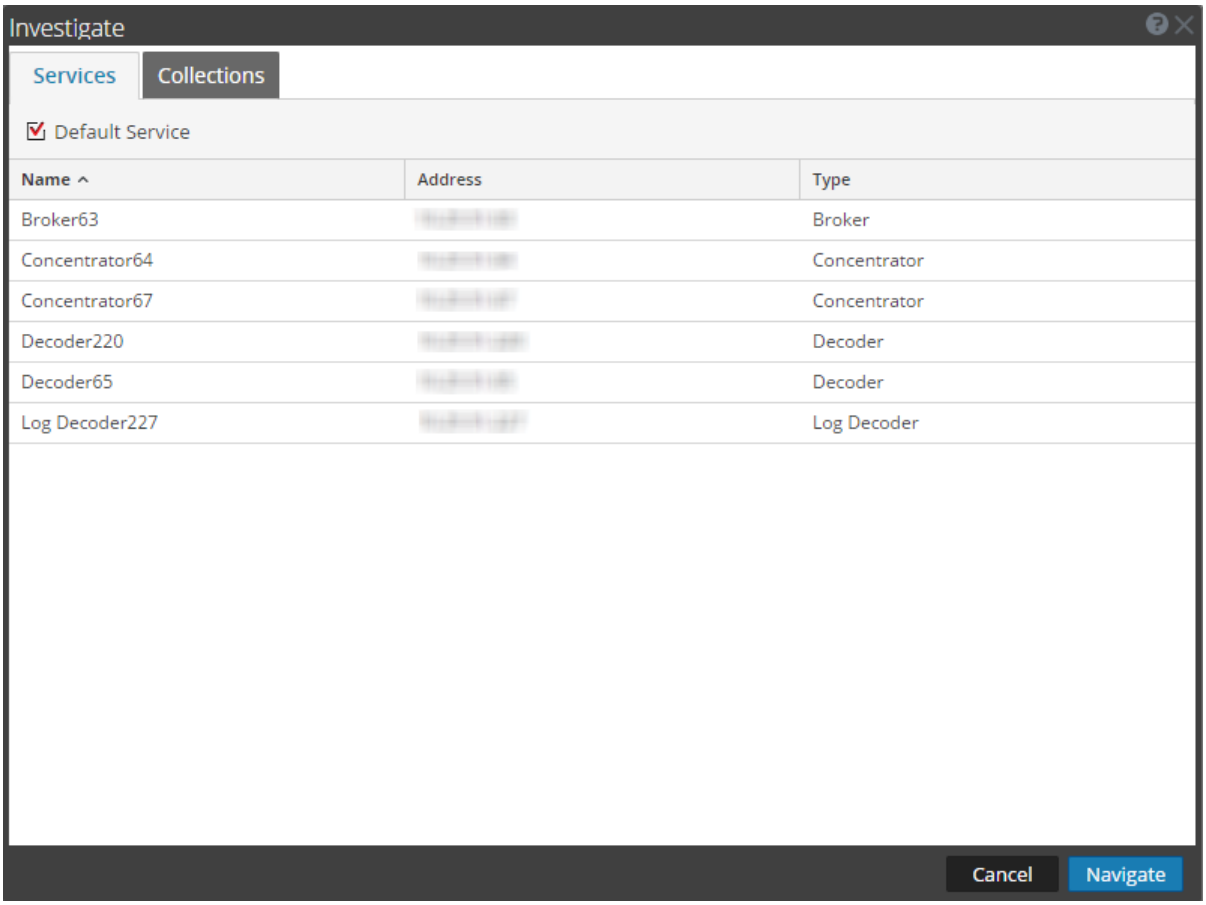
Note: Only users with the administrator role can create a collection, and only the creator of the collection is able to investigate a collection.

After loading data in the Navigate or the Events view:

1. View query results in the Navigate view (see Investigating Metadata in the Navigate View) and Events view (see Examining Raw Events in the Events View).
2. Reconstruct an Event (see Reconstruct an Event) or view the interactive Event Analysis of an event (see Analyze Events in the Event Analysis View).
3. Act on a drill point or an event (see Acting on a Drill Point in the Navigate View and Examining Events. For example, you can View Additional Context for a Data Point, Launch a Malware Analysis Scan from the Navigate View, or Add Events to an Incident for Response.

Begin an Investigation (No Default Service)

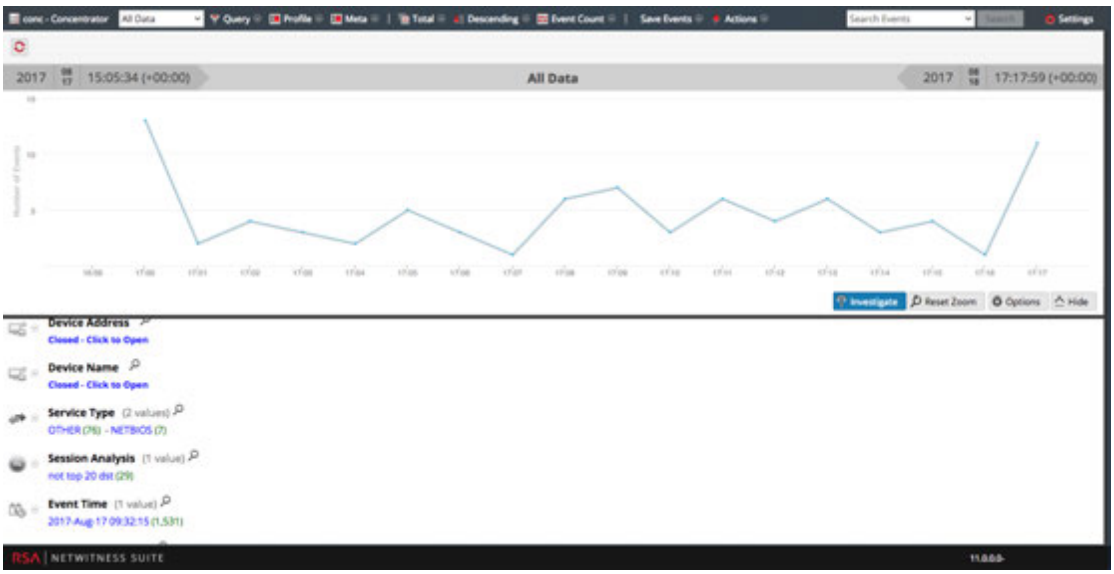
1. Go to **INVESTIGATE > Navigate** or **Events**.
   The Investigate dialog is displayed.



2. Double-click a service or select a service, usually a Concentrator, and click **Navigate**.
   The data loads automatically in the Events view. If you are working in the Navigate view,

the resulting panel displays the activity for the selected service, but the data is not loaded automatically.

3. (Recommended) Select a specific time range so that results load faster.
4. If you want to modify investigation options before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query as described in Filter Information in Navigate View You can also modify options at any time during the investigation. Filter and Search Results in the Events View provides information about refining results in the Events view.
5. To load data in the Navigate view, click Load Values.
   The data for the selected service begins loading.

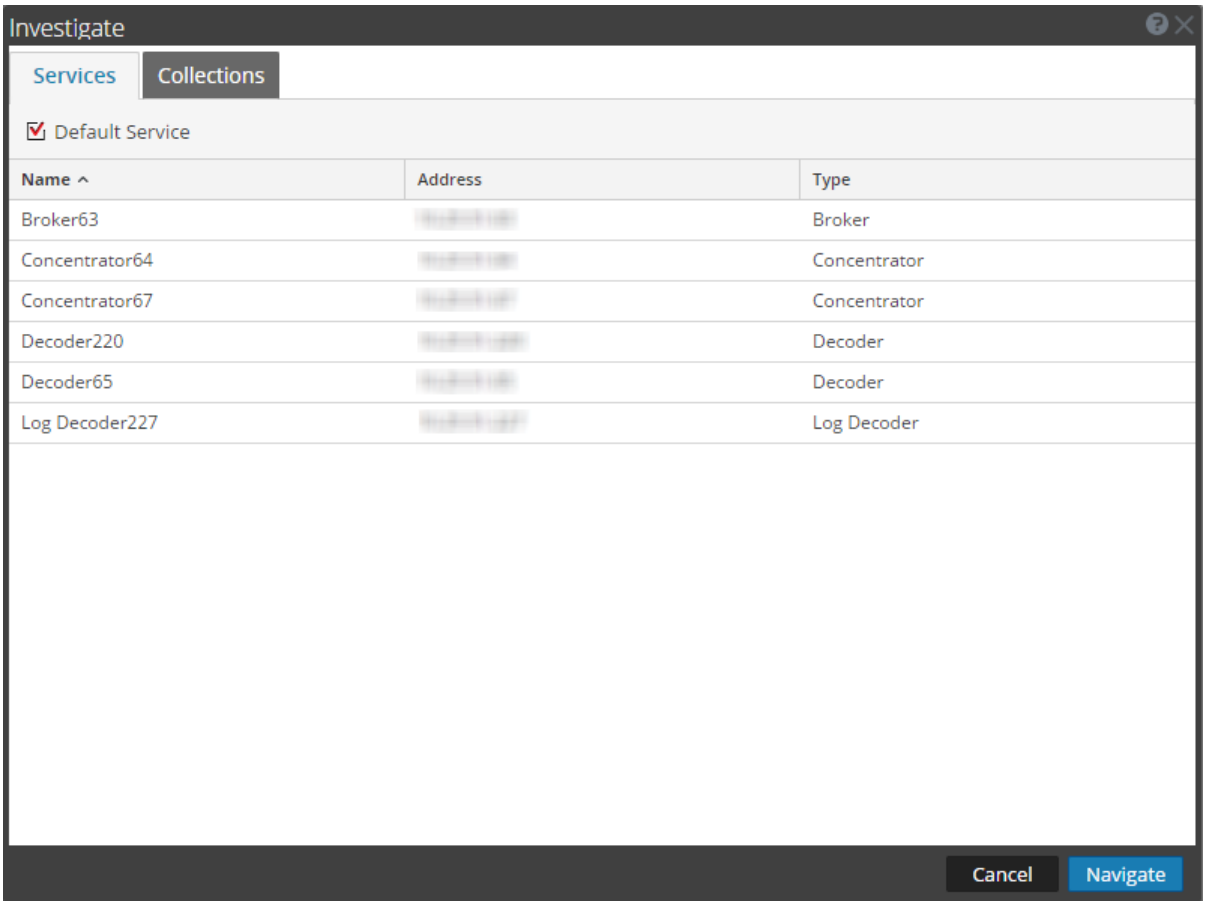


With the service selected and data loaded, you are ready to begin analyzing the data.

Set or Clear the Default Service

You can set the default service and clear the default service in the Investigate a Service dialog.

1. Click the service name in the toolbar.
   The Investigate dialog is displayed.



2. Select a service on the **Services** grid, and click Default Service.
   The service becomes the default, (indicated by **Default** in parentheses after the service name).

3. To clear the default service, select the default service in the grid, click Default Service, and click **Cancel** to close the dialog.
   No default service is set.

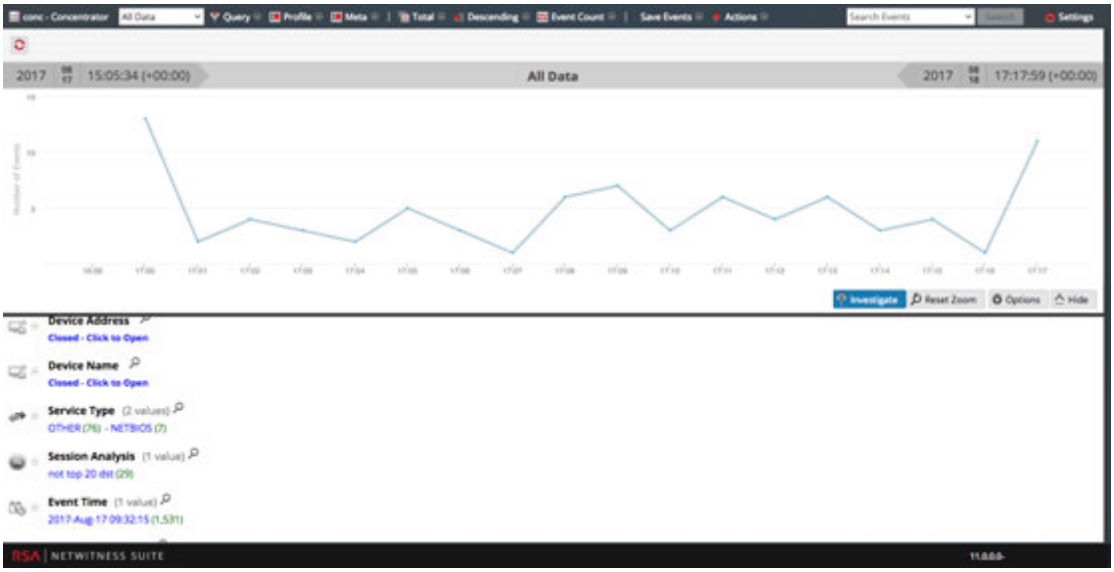
> **Note:** The Cancel button does not cancel your selection of the default service. It simply closes the dialog without navigating to the currently selected service in the grid. Setting a default service that is different from the service currently being investigated, does not refresh the Navigate view. You must explicitly select and Navigate to a different service.

Begin an Investigation (Default Service Specified)

1. Go to **INVESTIGATE > Navigate** or **Events**.
   If the Autoload Values setting is set to off, the Navigate view is displayed with the default

service selected, and ready to load data. If the Autoload Values setting is on, the values are loaded as shown in Step 3. In the Events view, the data is loaded automatically.

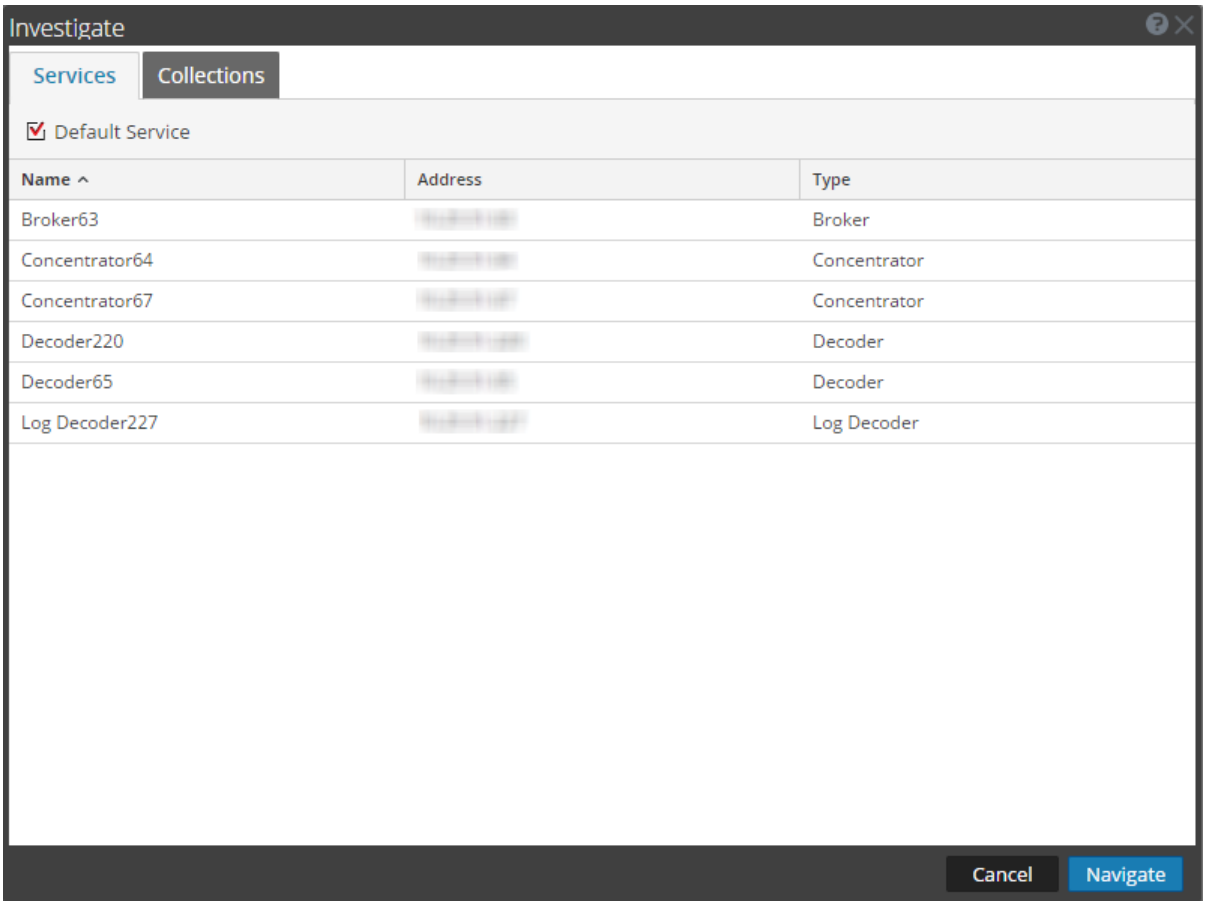
2. If you want to modify investigation options in the Navigate view before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query.
3. When ready, click Load Values.
   The values for the service are loaded in accordance with the selected options.



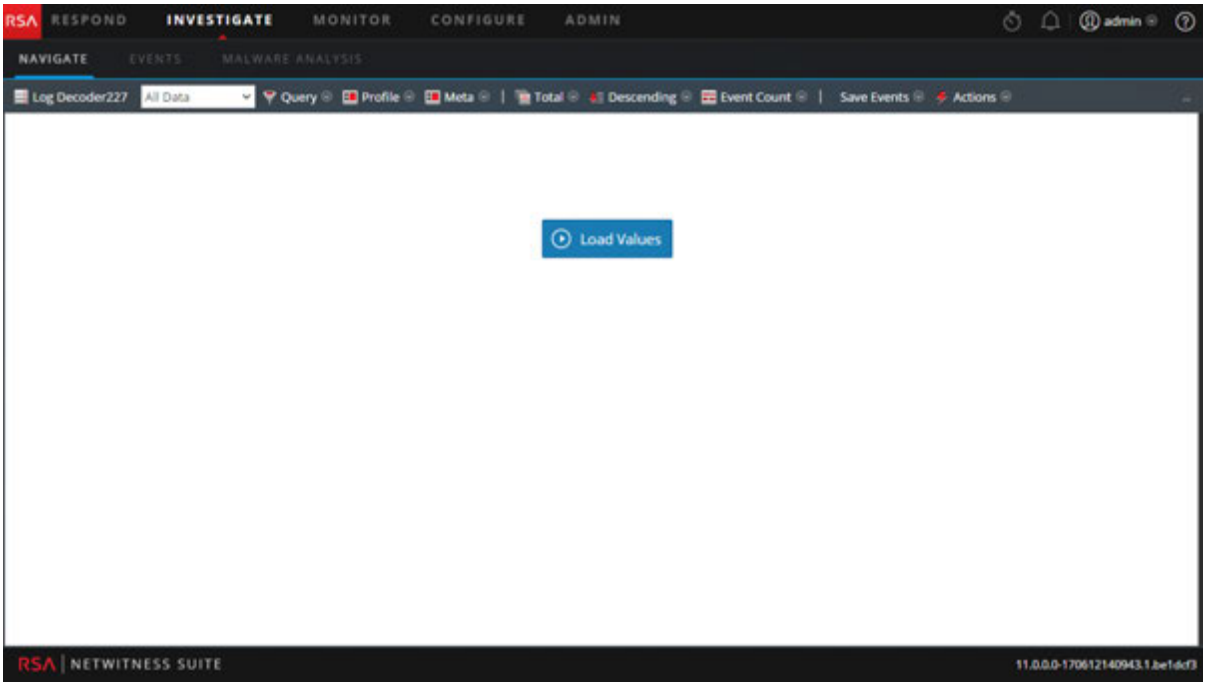
With the service selected and data loaded you are ready to begin analyzing the data.

Change the Service or Collection to Investigate

1. In the Navigate view or the Events view, click the service name at the top of the options panel.
   The Investigate dialog is displayed.

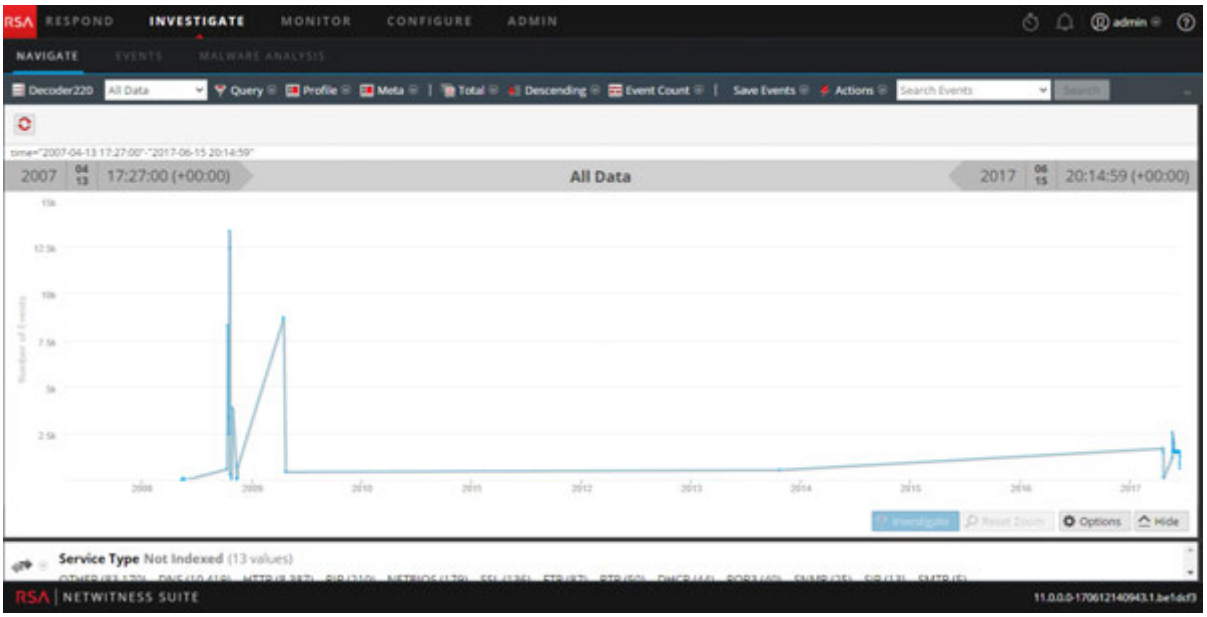


2. Double-click a service or select a service and click **Navigate**. The resulting panel displays the activity for the selected service.
   If the Autoload Values setting is on, the values are loaded as shown in Step 3.
   Otherwise, the Navigate view is displayed with the default service selected, and data ready to load. In the Events view the data is loaded automatically.



3. When ready, click .

   The values for the service begin loading in accordance with the selected options.



With the service selected and data loaded you are ready to begin analyzing the data.

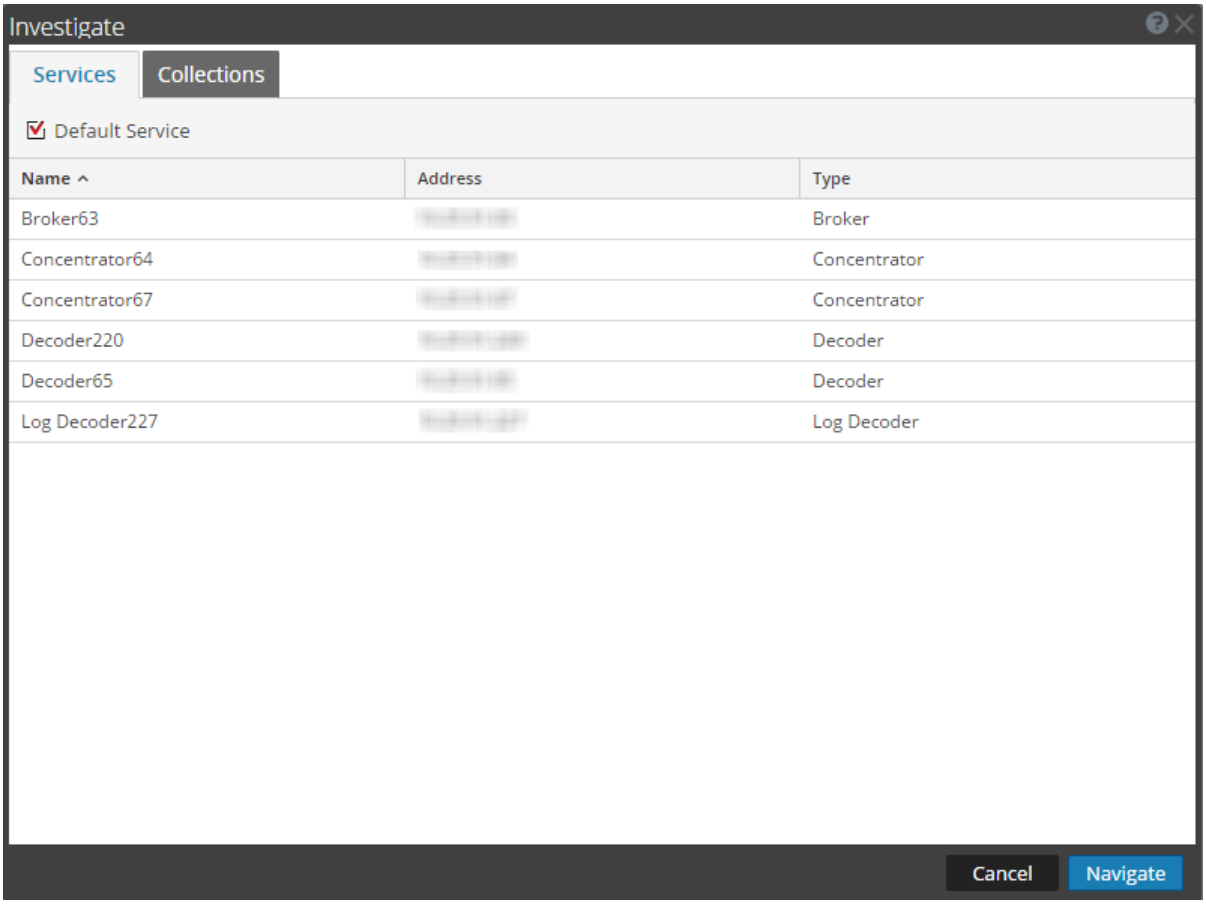
Investigate Workbench Restoration Collections

This procedure enables Administrators to select content from an existing collection to reprocess for further investigation. This applies to Decoders that use Workbench services.

Note: Only a user with administrative privileges can create a collection, and you can view only those collections that you created.

To reprocess data for further investigation:

1. Go to **INVESTIGATE > Navigate** or **Events**.
   The Investigate dialog is displayed.



2. Select a workbench service and workbench name that you want to investigate.
3. Click **Navigate** to perform an investigation on your selected workbench service.
   Click **Cancel** to select a different workbench service to investigate.
   The Investigation view is displayed.
   With the collection selected and data loaded you are ready to begin analyzing the data.

Begin an Investigation in the Event Analysis View

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Event Analysis view offers most of the features that are available in both the Navigate view and the Events view. Similar to the Navigate view, there is a view into meta keys and meta values for logs, endpoints, and packets. Like the Events view, an events list shows events listed in the order by time, and you can view the raw event, related meta data, and a reconstruction of an event. The Event Analysis reconstruction has some helpful cues to identify points of interest in a reconstruction. See Examining Raw Events and Meta Data in the Event Analysis View.

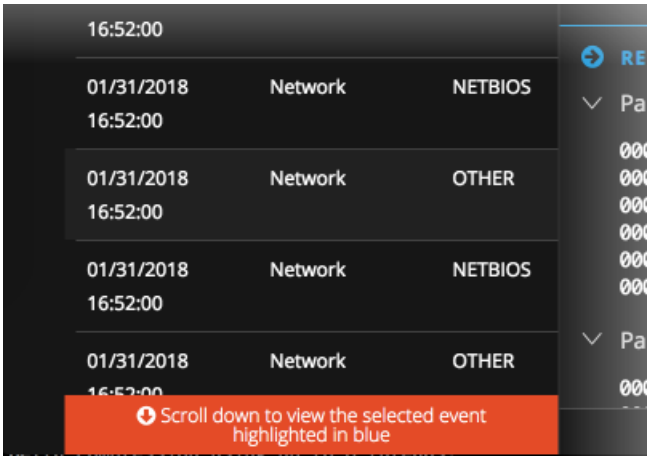
Note: In Version 11.0 you cannot begin an investigation in the Event Analysis view. Instead, you begin the investigation in the Navigate or Events view, and open an event in the Event Analysis view. In Version 11.1, an INVESTIGATE submenu gives you direct access to the Event Analysis view along with the ability to select a different service, time range, and create a query.

Access the Event Analysis View (Version 11.1 and Later)

Several ways to access the Event Analysis view are available in Version 11.1.

- When you use the **Actions > Go to event in Event Analysis** option in the Navigate view, and enter an event ID, the Event Analysis view opens the single event as a reconstruction. To simplify the view, the toolbar does not include the unnecessary options to expand, contract, and close windows. You can begin working as described in Examining Raw Events and Meta Data in the Event Analysis View.

- When you hover over a count (the green number after a meta value) in the Navigate view and click **Open Event Analysis in new tab**, the Event Analysis view opens with the list of events for the selected drill point, and you can begin working as described in Examining Raw Events and Meta Data in the Event Analysis View. The list of events can be very large, and there is a chance that the event you selected is not visible in the current page of events. In this case, a message advises you to scroll down to view the event.



- You can also access the Event Analysis view directly by going to **INVESTIGATE > Event Analysis** or going to **INVESTIGATE** if you have made the Event Analysis view your opening Investigate view. When you land on the Event Analysis view for the first time, you need to select a service to begin analysis. If this is not the first time you opened Event Analysis, the last used service is remembered until the localStorage is cleared.
  When you open the Event Analysis view from one of the other Investigate views, the service and query from that view are in effect. You can change the service, select a time range, and enter a query if you want to refine the results before opening the Event Analysis view as described in Filter Results in the Event Analysis View.

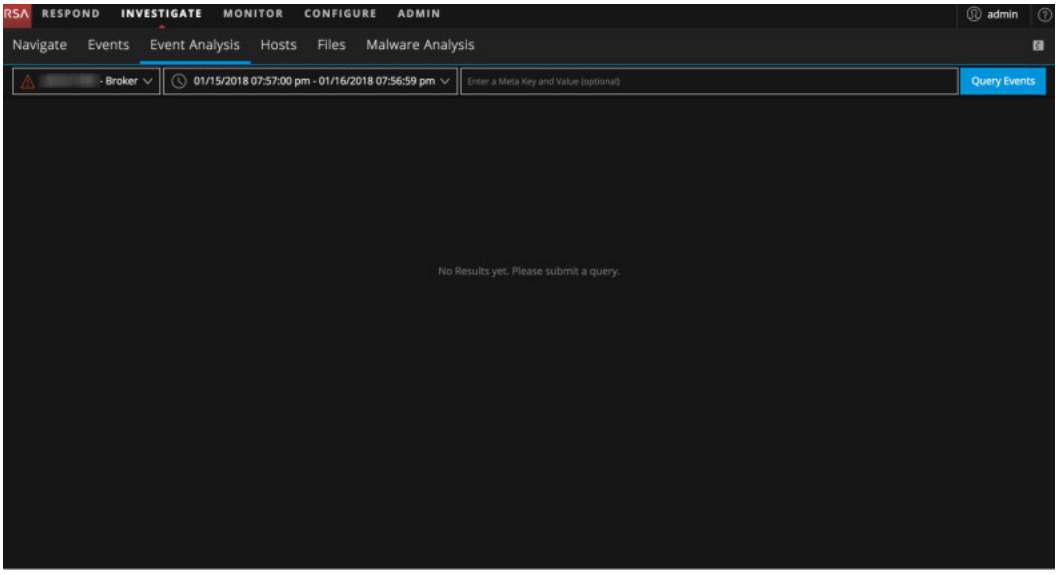
To access the Event Analysis view directly,

1. Go to **INVESTIGATE > Event Analysis**.
   The Event Analysis view opens with the first service in the service list selected and no data displayed. The **Select a service** field is populated initially with the first service in the list or the last selected service. A drop-down menu offers a list of available services in alphabetical order. By default the list of available services is retrieved every twelve hours and cached on the NetWitness server. If a service is added or removed from the NetWitness server, the cache is updated with the latest list of services. At the beginning of the field an icon provides the status of the query.
   and no service name = no service is selected.

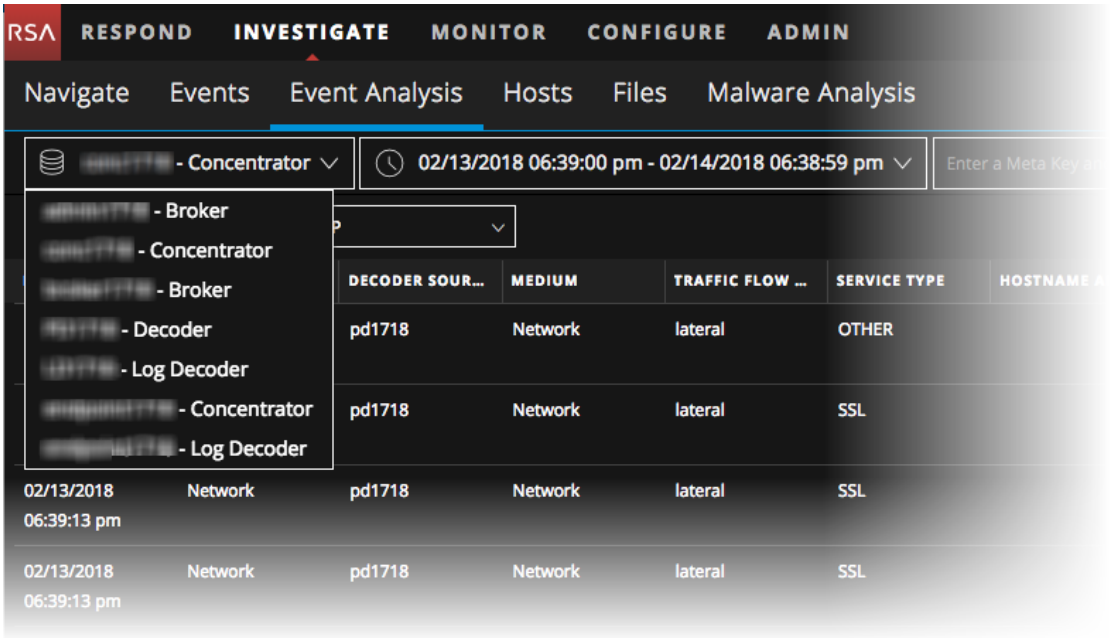
and selected service name= the service is selected.

= Investigate is attempting to connect to the selected service.

=Investigate cannot connect to the selected service or there is no data. In this state, the service selector control also turns red, and a tooltip explains why the connection attempt failed and advises you to choose another service.

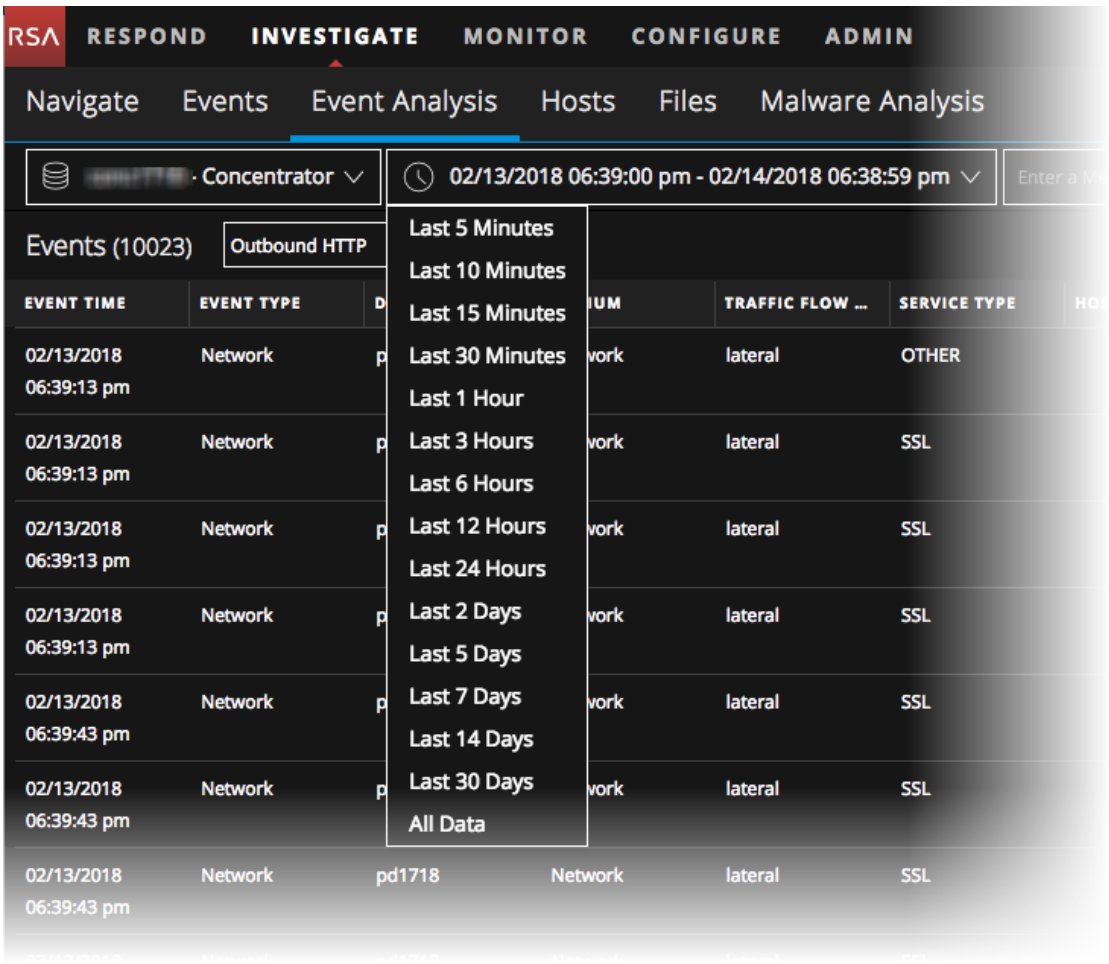


2. (Optional) Select a service, usually a Concentrator, from the drop-down list.



The time range selector shows either the default time range of 24 hours, or the time range that you last selected for this service. The Query Events button becomes active and you can enter filters. If you launch a query now, the selected time is used.

3. (Optional) To select a time range from the Time Range selector, click in the **Time Range** selector and select a time range from the drop-down list. Options are Last 5, 10, 15 or 30 Minutes; the Last 1, 3, 6, 12, or 24 hours; the Last 2, 5, 7, 14 or 30 days; or all Data. (The time range is based on preferences set for the Event Analysis view. The default basis for time range is database time; you can change it to wall clock.)
   The selected time range is stored in your browser for this service; you can set different time ranges for different services.



4. Type a query by creating one or more filters that contain at a minimum a meta key or meta entity, operator, and optional value. See Filter Results in the Event Analysis View for details on entering queries.

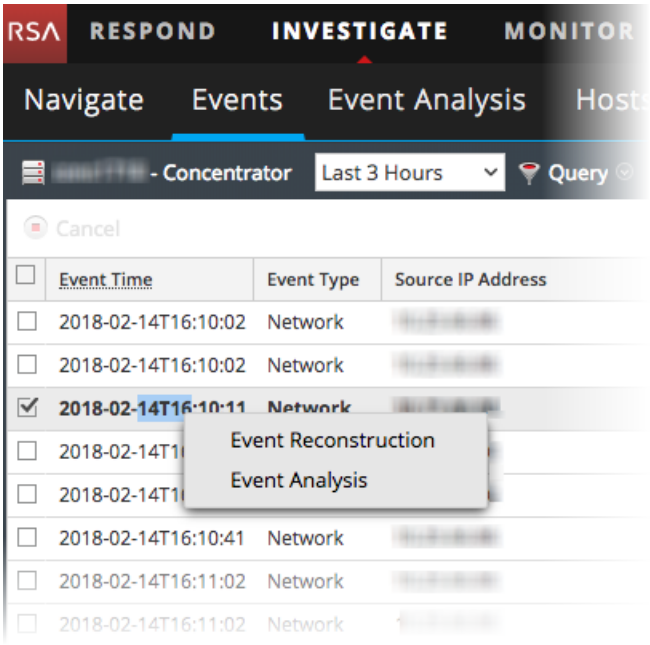
5. Click **Query Events**.
   The Event Analysis view displays the activity for the selected service and time range, in accordance with permissions assigned to your role by the administrator. With the service selected and data loaded, you are ready to begin analyzing the data. Refer to Examining Raw

Events and Meta Data in the Event Analysis View to learn how to work in the Event Analysis view.

Access the Event Analysis View (Version 11.0)

To open and event in the Event Analysis view:

1. Go to **Navigate > Events**.
2. Right-click an event in the listed events, and select **Event Analysis** in the menu.



Refer to Examining Raw Events and Meta Data in the Event Analysis View to learn how to work in the Event Analysis view.

Investigating Metadata in the Navigate View

When conducting an investigation in the Navigate view, analysts have multiple methods, specific to the Navigate view, to refine the results, visualize data, and act on data.

- Filter Results in the Navigate View
- Manage Meta Groups
- Visualize Metadata as Parallel Coordinates
- Open an Event in the Events List
- Export or Print a Drill Point
- Launch an External Lookup of a Meta Key
- Launch a Malware Analysis Scan from the Navigate View
- Visualize the Current Drill Point in Informer

In addition, you can use these methods of querying data and acting on results that are common to the Navigate view and the Events view.

- Search for Text Patterns
- Create a Custom Query
- View and Modify Queries Using URL Integration
- Use Profiles to Encapsulate Custom Views
- Manage Context Hub Lists and List Values in Investigate
- View Additional Context for a Data Point
- Reconstruct an Event

Filter Results in the Navigate View

When conducting an investigation in the Navigate view, there are several methods available to refine the results displayed when meta key values are loaded in the Navigate view. Basic filtering methods available to analysts are:

- Set the Time Range
- Set the Quantification Method and Sort Sequence of Meta Key Results
- Manage and Apply Default Meta Keys in an Investigation
- Drill into Data in the Navigate View Time Chart
- Drill into Data in the Values Panel

The rest of this topic is focused on the basic methods of filtering data. In addition, more advanced methods allow configuration of meta groups, profiles, and parellel coordinates visualizations.

- Visualize Metadata as Parallel Coordinates
- Manage Meta Groups
- Use Profiles to Encapsulate Custom Views

A separate topic is provided for each of the more advanced methods.

Set the Time Range

When conducting an investigation in the Navigate view, the time range options limit the results returned. You can select:

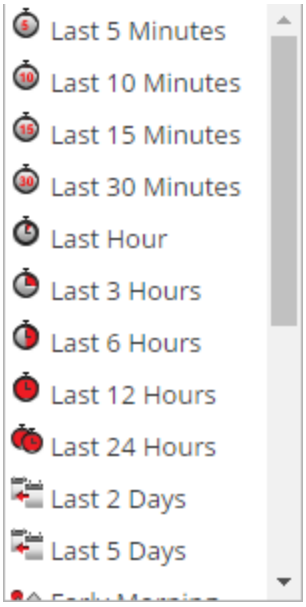
- A time range relative to the collection. Ranges relative to the collection are based on the last collection time for data.
- A time range relative to the calendar.
- A custom date range.
- All data.

The selected Date Range (type) is shown in the Navigate view tool bar as the Time Range label; by default the label is **Last 3 Hours**. The Time Range display shows the first and last timestamp for the date range being used for the metadata.

Note: Time range is based on the Time Zone configured in the Profile Preferences panel as described in "Setting User Preferences" in the *RSA NetWitness Suite Getting Started Guide*.

To select a built-In time range:

1. Click the **Time Range** option in the Navigate view toolbar. The default time range is for the **Last 3 Hours**, but a different value from the selection list, for example, **All Data** or **Last Hour,** may already be selected and used as the label in the options panel.
   The Time Range selection list is displayed.



2. Do one of the following:
   - If you want to see all data, select **All Data**.
   - If you want to set a time range in minutes, hours, or days that is relative to the collection, select a value such as **Last 10 minutes**, **Last 3 Hours**, or **Last 5 days**.
   - If you want to set a time range relative to today, select **Yesterday**,**This Week**(Version 11.1), **Last Week** (Version 11.1), **All Day**, or a part of the day such as **Early Morning**, **Morning**, **Afternoon**, or **Evening**.
   - If you want to set a time range relat
   - If you want to set a unique date range, select **Custom** in the **Time Range** menu and follow the procedure below.
     The selected time range is applied to the current results in the Values panel.

To specify a custom time range:

1. Select **Custom** in the **Time Range** menu.
   Date selection options are displayed in the toolbar.

2. Within the time **Start Date** and **End Date** fields, do the following to specify the date and time:
   a. Click a date from the calendar.
   b. (Optional) Select the time from the Hour, Minute, Second fields or click **Now**. The time selection defaults to the current time of day.

Note: If you specify custom start or end times in seconds, the value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time is interpreted as "HH:MM:00 - HH:MM:59." Seconds display in this format in **Investigation > Navigate** functions.

3. To apply the range, click **Go**.
   The selected time range is applied to the current results in the Values panel.

Set the Quantification Method and Sort Sequence of Meta Key Results

You can select the way results for each meta key are quantified and sequenced in the Navigate view.

Note: If meta entities (Version 11.1 and later) are used in meta groups, the results will show the top 20 values that matched any of the meta keys contained in the meta entity.

Each meta key section in the Navigate view contains an ordered list of values showing each meta key value (Value) and its count (Total). You can specify whether:

- The results in each meta key section are sorted based on Value or Total.
- The results are sorted in ascending or descending order.
- The values shown for each meta key are quantified by number of packets (Packet Count), number of sessions or logs (Quantify by Event Count) or by the size of events (Quantify by Event Size).

Note: If you have both a log decoder and a packet decoder for which you are viewing the metadata, the calculation of what is actually being counted is dependent on the type of key. If you select to Quantify by Packet Count and are looking at logs, the Navigate view output is the same output as if you had selected Quantify by Event Count (see Navigate View for details).

This image shows the `Event Type` meta key presented in order by **Total** in **Descending** order. The value with the greatest count of matches is presented first. The value `failure audit` has 71 matches and is listed first. The value `logon` has only one match and is presented last. The quantification method is **Event Count**.

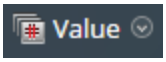
This image shows the `Event Type` meta keys presented in order by **Value** in **Descending** order. The value names are presented in alphabetical order starting at the end of the alphabet. The value `success audit` is listed first. The value `connect` is presented last. The quantification method is **Event Count**.

To select the quantification method of meta key count and ordering of meta key results displayed in the Navigate view:

1. In the toolbar, select **Event Count**, **Event Size**, or **Packet Count** and choose one of the quantification options in the drop-down menu. The label for the menu displays the selected option.

   The current view is reloaded according to your selection.

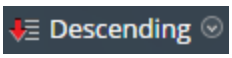
2. In the toolbar, select **Total** or **Value** and choose one of the ordering methods in the drop-down menu. The label for the menu displays the selected option.

   The current view is reloaded according to your selection.

3. In the toolbar, select **Ascending** or **Descending** and choose one of the sort order options in the drop-down menu. The label for the menu displays the selected option.

   The current view is reloaded according to your selection.

Manage and Apply Default Meta Keys in an Investigation

When analysts are conducting an investigation of captured data in Investigation, a default set of meta keys is loaded and displayed in a default sequence in the Navigate view > Values panel. The default content and sequence is based on the meta keys for the service being investigated. Analysts can specify the meta keys to display during navigation by selecting the default meta keys or by selecting a user-defined group of meta keys, which provides great flexibility to define meta keys. This can help to drill down more directly to the desired data and to reduce the load time by preventing the loading of meta that is not of interest in the current investigation.

Note: In Version 11.1 and later, wherever meta keys are used, you can also use configured meta entities.

If no custom meta groups are in effect, the Navigate view is displayed with the meta key visibility specified in the Default Meta Keys dialog. To optimize loading of meta keys in the Navigate view > Values panel, NetWitness Suite does not open non-indexed meta keys by default. When you open a non-indexed meta key in the Values view, NetWitness Suite begins loading values for that meta key. If the load time is excessive, the load of the meta key times out with a message. Title, values, and counts for non-indexed meta keys are not drillable in the Values panel. Additional labeling in Investigation identifies the non-indexed meta keys.

To select the meta keys to apply to your investigation, you can.

- Select the default meta keys.
- Select a user-defined set of meta keys, called a meta group.

Note: Once created, user-defined meta groups can be edited, deleted, exported for use on other services, and imported to the service you are investigation. All of these procedures are provided in a separate topic: Manage Meta Groups.

The Default Meta Keys dialog allows you to specify the default view and display sequence for meta keys during navigation in the Investigate > Navigate view for a specific service. For each key or for all keys, you can set the default view to:

- Hidden: Results for default meta key are hidden and are not available to load.
- Open: Results for default meta key are open with all values and counts displayed.
- Close: Results for default meta key are closed with only the meta name visible.
- Auto: The loading of default meta keys is controlled by the index level, which must be Indexed By Value.

When using the default meta keys, be aware that these can be modified for different services, and you may not be seeing the same set of default meta keys when navigating to a drill point on different services. If you do not see the expected data, you may need to change the initial view of the default meta keys.

When you change the initial state of default meta keys from within the Navigate view, the change persists for that service. When new keys are added to the custom index file for a Core service (for example, `concentrator-custom-index.xml` or `decoder-custom-index.xml`), the new keys are added to the default meta keys list. The changes made in the Navigate view apply only to the current service.

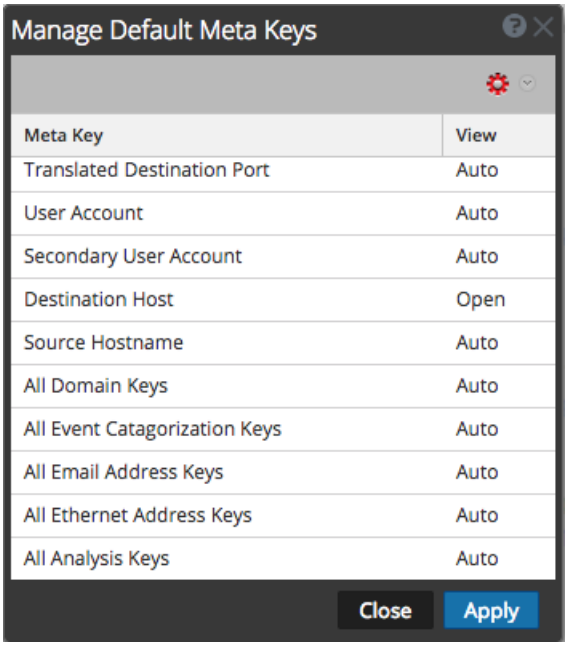
To specify that the initial Navigate view opens using default meta keys:

1. Go to **INVESTIGATE > Navigate**.
2. Select a service and select **Navigate**.
3. In the **Meta** menu, select **Use Default Meta Keys**.
   If an investigation is already in progress, the data is reloaded in the current view and an icon highlights the selected option. If no data is loaded yet, the default meta keys are used for the next load.

Configure Default Meta Keys

To configure the default view of default meta keys in the Navigate view:

1. In the **Navigate** view toolbar, select **Meta > Manage Default Meta Keys**.
   The Manage Default Meta Keys dialog is displayed with the list of available meta keys for the service.



2. (Optional) To change the order of the keys, select one or more keys, and drag the values up or down through the list of keys.

3. Do one of the following:
   - (Optional) To change the default view for all meta keys, make sure that no keys are selected and in the toolbar, select .
   - (Optional) To change the default view for one or more keys, select the keys and in the toolbar, select .

     A drop-down of possible initial views for all default meta keys is displayed.
   - (Optional) To revert to the default view for meta keys as specified in the service index file, make sure that no keys are selected and in the toolbar, select > **Auto**.

     When you modify the default meta keys for a non-indexed meta key, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.
4. Select one of the views.
5. To save the changes, click **Apply**.

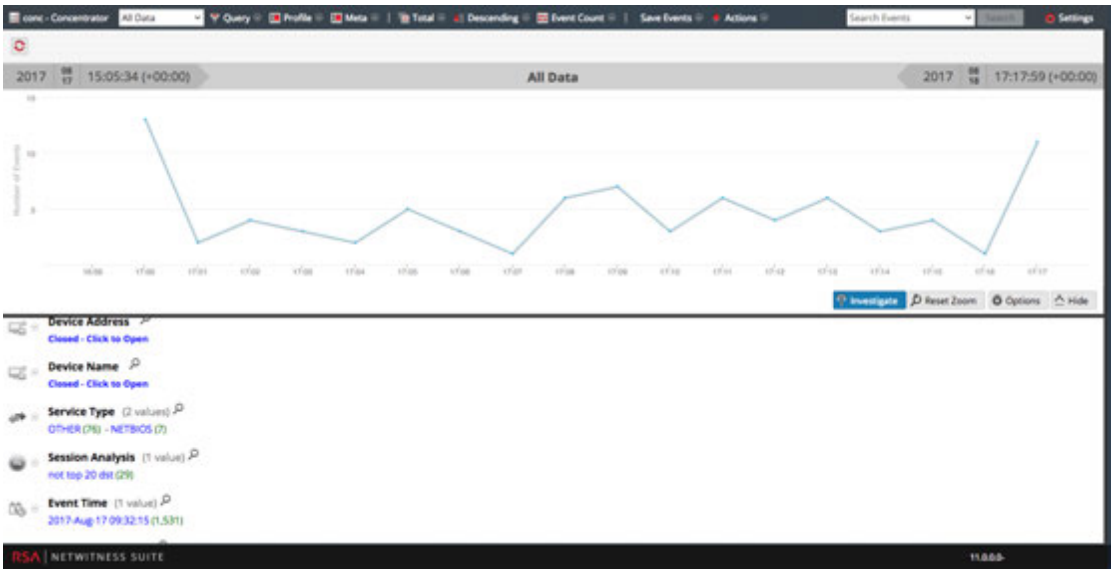
   The meta keys displayed in the Navigate view are set to your specifications. If the default meta keys are hidden, values for the meta keys are not shown in the investigation at all. If the default meta keys are closed, the values for the meta keys are not loaded by default, but you can load individual meta keys manually in the Navigate view.

Drill into Data in the Navigate View Time Chart

The Time Chart visualization allows analysts to visualize activity over time. You can zoom into the data by selecting a time window then selecting the Investigate option. You can then reset the navigation to the time range that was in effect before zooming.

1. Go to **INVESTIGATE > Navigate**.

   The Time Chart for the current drill point and selected time range is displayed.



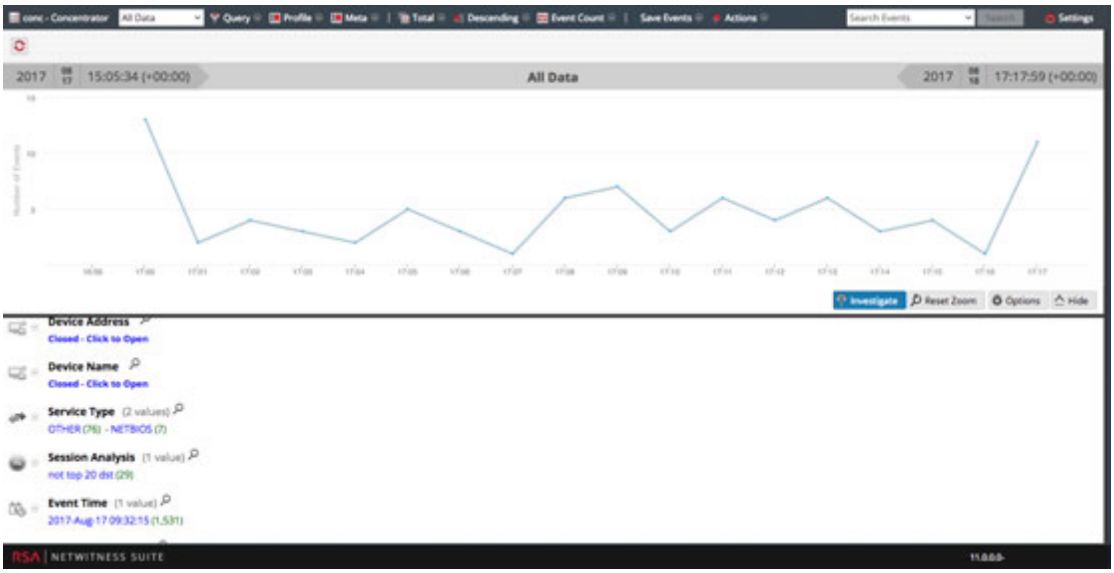
2. To highlight a period of time on the Time Chart, click over the desired time period and drag the mouse.
   The Time Chart is redrawn for the selected time range, however the meta values are unchanged.
3. To drill into the data for the selected time range, click **Investigate**.
   The URL is updated to reflect the time range override. and the Investigation options panel is updated to reflect the custom time range. The Time Chart is redrawn and the meta values are loaded for the selected time range.
4. To reset the Time Chart to original time range, click **Reset Zoom**.
   The URL is updated to reflect the original URL prior to zooming into the data, and the Investigation options panel is updated to reflect the time range selected before zoom. The Time Chart is redrawn for the selected time range and the meta values are loaded for that time range.

Drill into Data in the Values Panel

NetWitness Suite displays the activity and values for the selected service in the Investigation > Navigate view. To investigate data, analysts drill into data by clicking on a meta key or a meta value, which is treaty as a query. In the Values panel, each query is added to the breadcrumb data in the Values panel. This results in a breadcrumb at the top with a crumb for each query. You can edit the breadcrumb to insert or remove a query.

To drill into a subset of the metadata:

1. Begin an investigation so that metadata is displayed in the Navigate view.

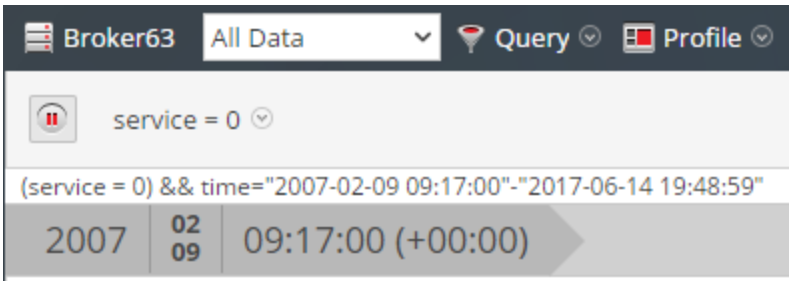


2. To drill down into the metadata, do any combination of the following:

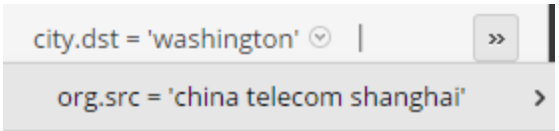
   a. Click a **meta key**, for example, **Service Type**.

   b. Click a **meta value**, the blue text in the results. For example, **OTHER**.

   Each time you click a meta key or meta value, the investigation query pivots to a narrowed focal point, or drill point, in the data. At each drill point, the Values panel is updated and the new drill point is displayed in the breadcrumb. Below is an example of the first breadcrumb.



   This is an example of a long breadcrumb that does not fit in the toolbar. The last query that fits is followed by a drop-down menu that lists additional queries. To select a drill point within the overflow, click the overflow icon and a query in the drop-down list.



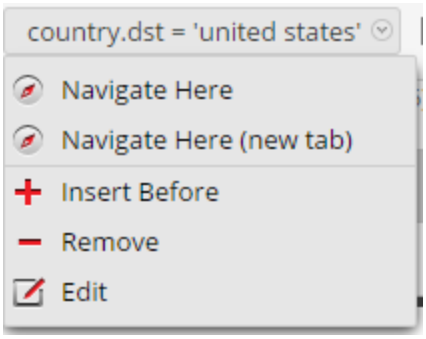
To add a query in the breadcrumb:

In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, NetWitness Suite refreshes the results.

To add a query in the breadcrumb:

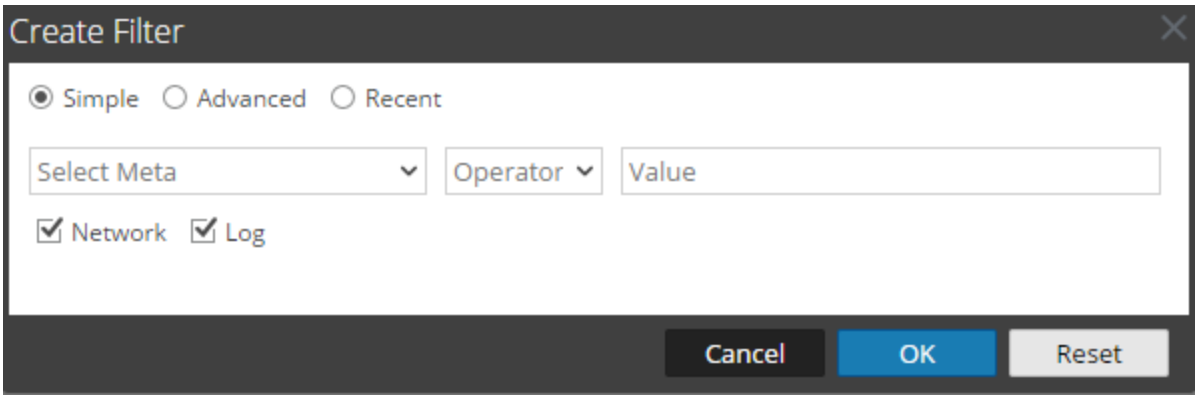
1. Click a crumb.

   The Breadcrumb menu is displayed.



2. To add a query in the breadcrumb, select **Append** or **Insert Before**.

   The Create Filter dialog is displayed.



3. Create the Query as described in Create a Custom Query.

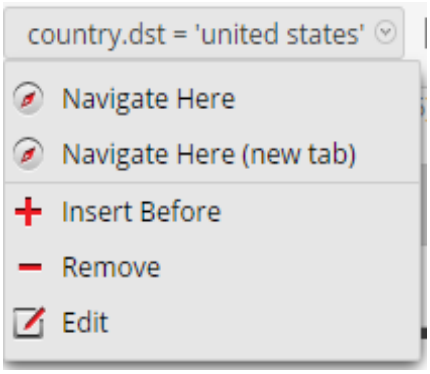
To edit a query in the breadcrumb:

In the breadcrumb, you can click any of the crumbs to display the Query menu. You can delete a crumb and edit a query in a crumb. After each edit in the breadcrumb, NetWitness Suite refreshes the results.

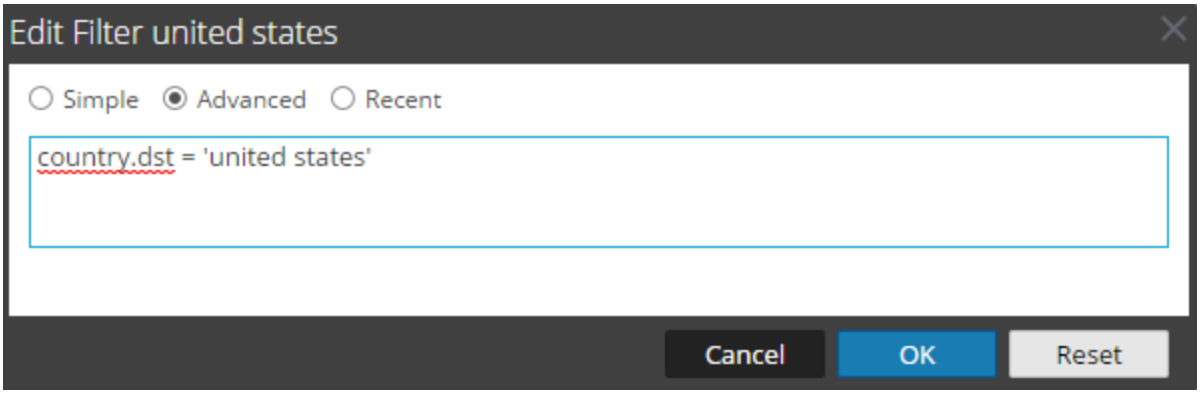
To work with queries in the breadcrumb:

1. Click a crumb.

   The Breadcrumb menu is displayed.



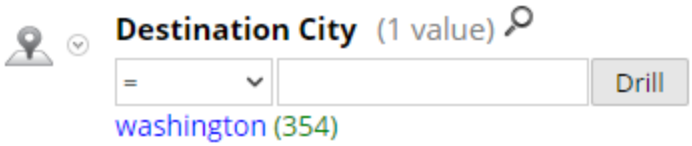
2. To edit a query in the breadcrumb, select **Edit**.
   The Create dialog is displayed with the selected query open for editing.



3. Edit the fields as described in Create a Custom Query.

To quick search within a meta key:

1. Move the mouse over a meta key section and click the magnifying glass.
   The Quick Search form, which contains a comparator and an optional operand for the search, is displayed.

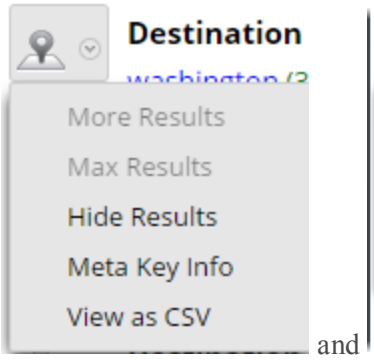


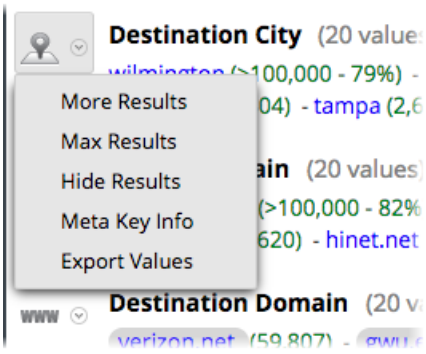
2. (Optional) If you want to close the search form, click the magnifying glass again.
3. Select the operation from the drop-down list on the left and type the text value to search for. Then click **Drill** to perform the execution.
   The metadata for that meta key is used to drill down in the current metadata.

To view meta key Information:

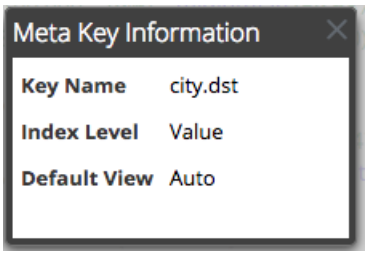
To view details about a meta key, specifically the key name, index level set for displaying the meta key, and the default view set for the meta key:

1. Click the drop-down menu next to the meta key. These two figures show the drop-down menu for Version 11.0.0.x and 11.1 and later.



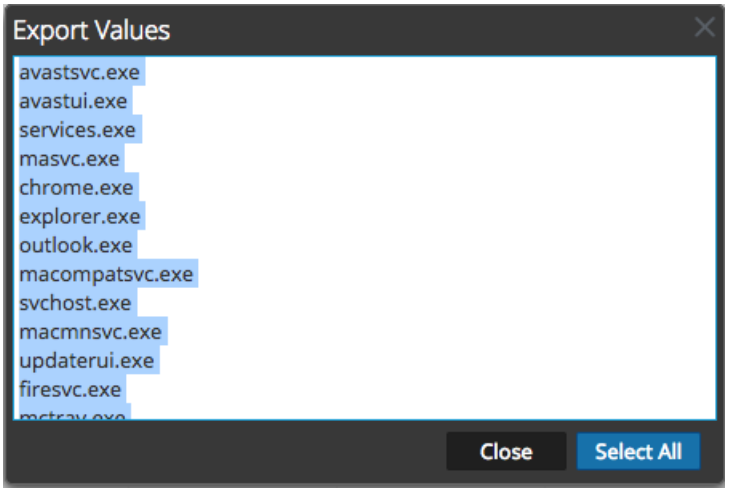
and


2. Select **Meta Key Info**.
   The Meta Key Info dialog is displayed.



3. When finished viewing, click ■.
4. (Optional for Version 11.0) To view meta names found for the meta key as a comma-separated value list, click the drop-down menu next to the meta key and select **View as CSV**.
   The Showing Values in CSV Format dialog is displayed. When finished viewing, click **Close**.
5. (Optional for Version 11.1) To view meta names found for the meta key in a list, click the drop-down menu next to the meta key and select **Export Values**.

The Export Values dialog is displayed.



6. (Optional) If you want to hide the results for the meta key in the current drill point, click the drop-down menu next to the meta key and click **Hide Results**.

To display events associated with a meta value:

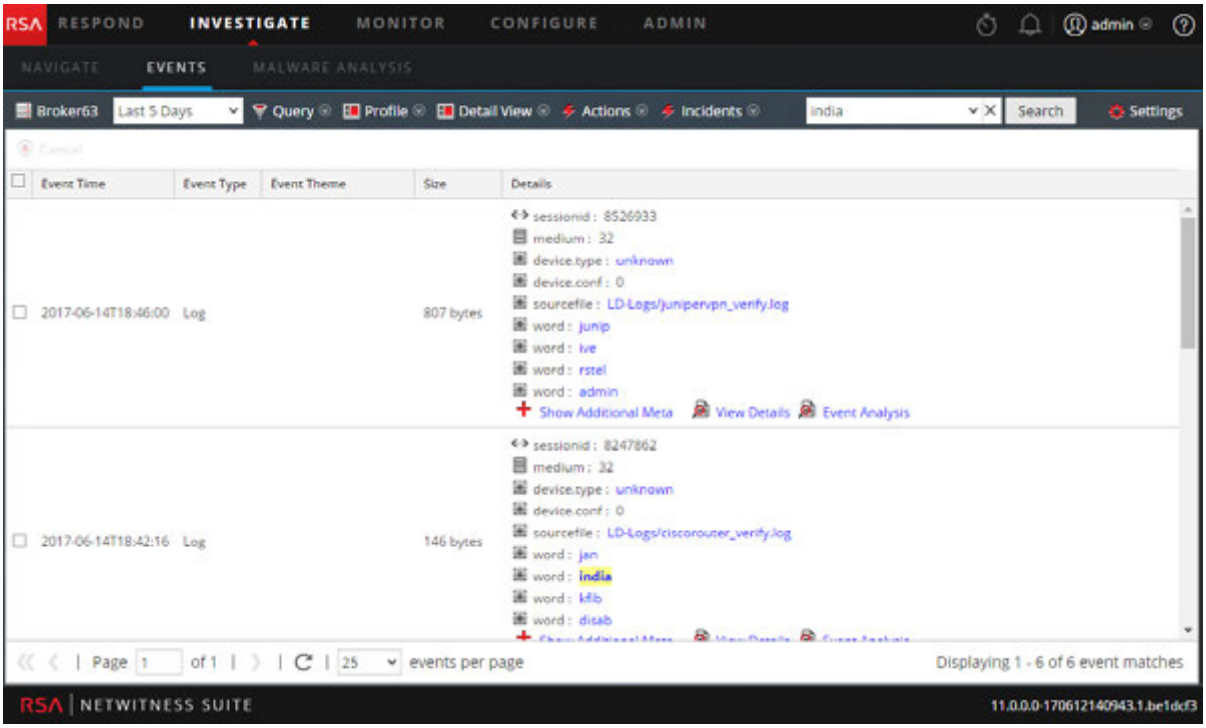
The Events view provides additional details for an event in two different views: Events List and Detail View.

1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Click the count (the number in green) next to a blue meta value.
   The Events view corresponding to the current drill point is displayed.
   The operations that you can perform in the events view are described in Examining Raw Events in the Events View.

To search for specific events associated with a meta value:

1. In the Navigate view, drill into metadata that is the focus of your investigation (click a meta value or add a query).
2. Type a search string in the Search box and press **Enter** or click **Search**.
   You can also select and set search mode preferences. See Search for Text Patterns for detailed search information.
   The Events view opens in a new tab and shows the search results. If you do not see the search term highlighted, click **Show Additional Meta**. Your time range selection and drills

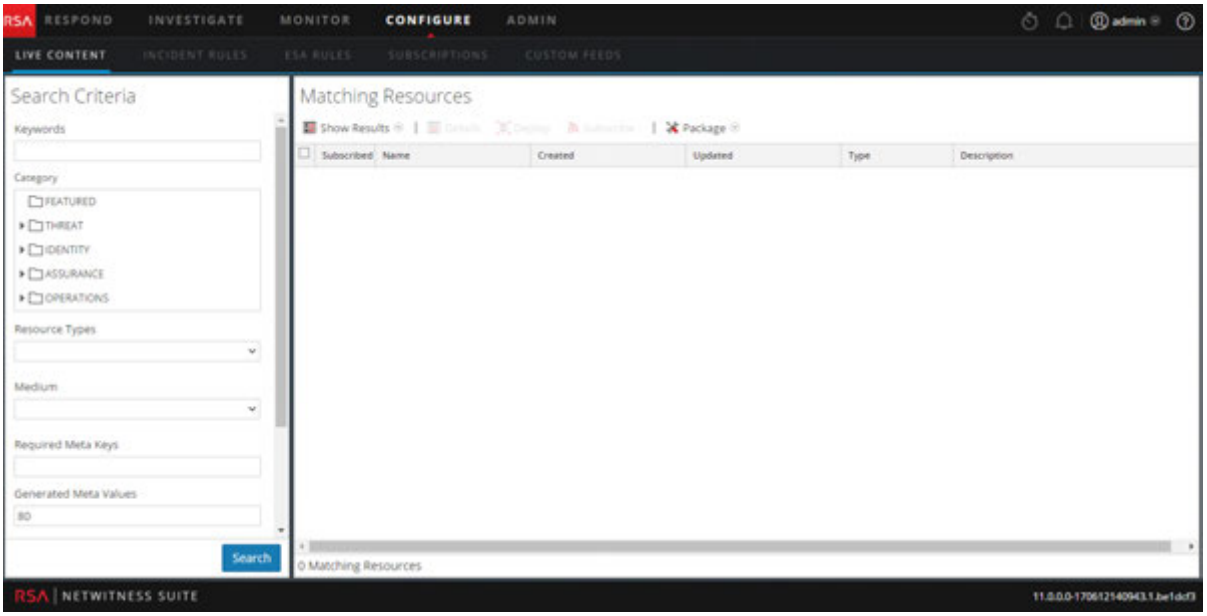
(queries) carry forward to the Events view.



To view a selected meta value in RSA Live:

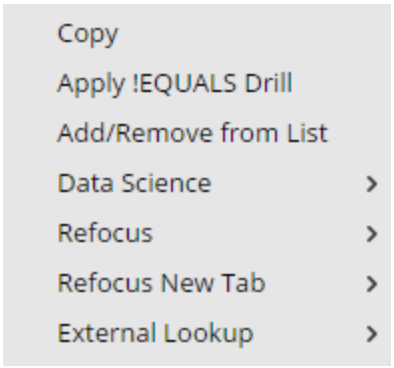
1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.
3. To look up the meta value in RSA Live, select **Live Lookup**.
   The Live Search view is displayed with the meta value entered in the Generated Meta

Value(s) field, and ready for a search.



To refocus the investigation in a drill point:

1. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.



2. Choose one of the refocus options.
   The drill is refocused according to your choice.

To look at a specific count in a new tab:

To view a count for a meta value in a new tab or view a Geomap of the locations for the selected meta value:

1. Right-click a count for a meta value (the green number following the blue meta value).
   The context menu is displayed.

2. (Optional) To open a separate investigation for the specific meta value, select **Open in New Tab**.
3. (Optional) to open a geomap showing the locations where the selected meta value originated, select **Geo-Map Locations in New Tab**.

Manage Meta Groups

A meta group combines selected meta keys into a group to show only data in which the meta keys and meta entities were found.

Note: In Version 11.1 and later, you can also use configured meta entities in meta groups.

In the Investigate > Navigate view, you can use meta groups to filter data displayed in an investigation. A fresh installation of NetWitness Suite includes out-of-the-box (OOTB) meta groups to help you find interesting data sets in Investigate. The OOTB meta groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. You can create your own groups and you can duplicate and edit an OOTB group to create a custom group.

With a meta group in effect during an investigation, the information in the Values panel shows only the meta keys in the selected group. When you open a Parallel Coordinates visualization, the meta keys and meta entities in a group appear as axes from left to right. It may be useful to create two versions of each custom meta group; one for analysis of meta values and one for creating a parallel coordinates chart focusing on a smaller subset of the same use case.

Custom meta groups are visible to all users of a service and may be exported for import to any service, limited by the available meta keys for that service.

Note: When an administrator adds custom meta groups manually by editing the custom index file for a service, the new groups become available to Investigation after the service is restarted.

This section describes how to add, edit, import, export, and delete custom meta groups to be used during navigation on a specific service.

Out-of-the-Box Meta Groups

The OOTB meta groups a built-in to RSA NetWitness Suite. The default meta groups are useful to focus an investigation on common use cases and to support threat detection using the RSA Hunting Pack.

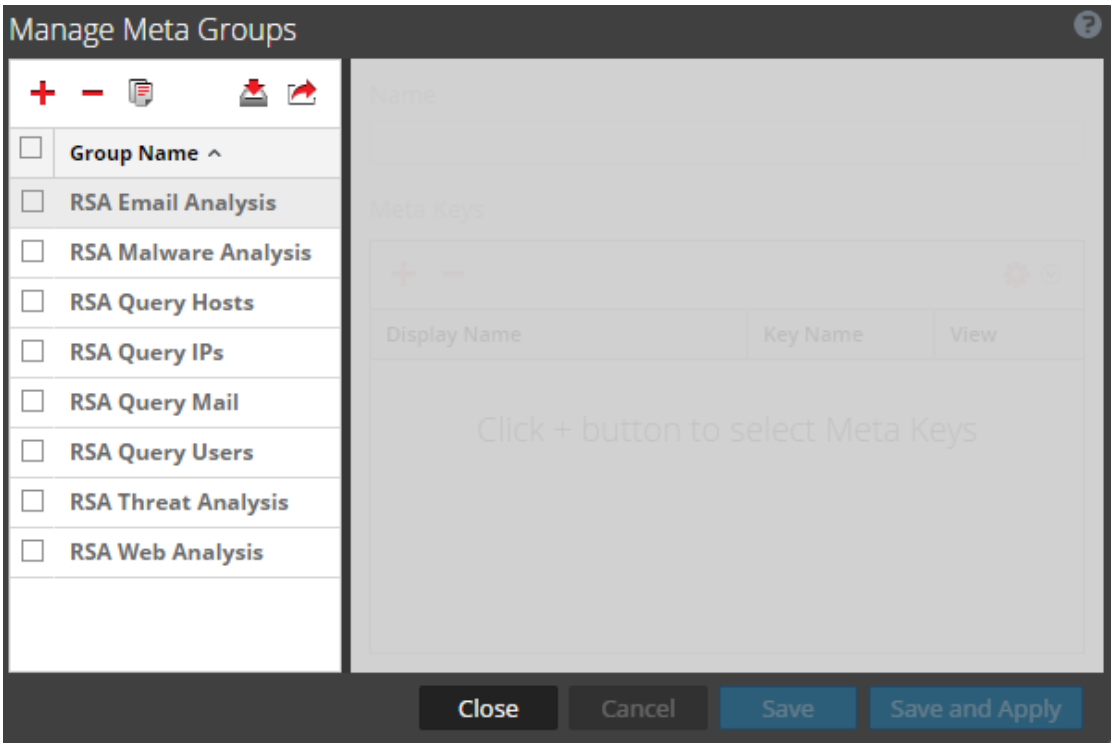
These are the OOTB meta groups:

- RSA Email Analysis includes meta keys that outline email interactions.
- RSA Endpoint Analysis contains meta keys that provide insight on processes, files, users, and connections from NetWitness Endpoint (NWE) hosts.
- RSA Malware Analysis includes meta keys that mark indicators of compromise in files contained in events.
- RSA Outbound HTTP includes meta keys that provide insight into outbound web traffic.

- RSA Outbound SSL/TLS includes meta keys that focus on encrypted web traffic.
- RSA Query Hosts includes a meta keys that encompass all the meta keys to find hosts.
- RSA Query IPs includes meta keys that encompass all the meta keys to find IP addresses.
- RSA Query Mail includes meta keys that encompass all the meta keys to find email.
- RSA Query Users includes meta keys that encompass all the meta keys to find users.
- RSA Threat Analysis includes meta keys that mark potential threats in the data set.
- RSA Web Analysis includes meta keys that mark anomalies in web traffic.

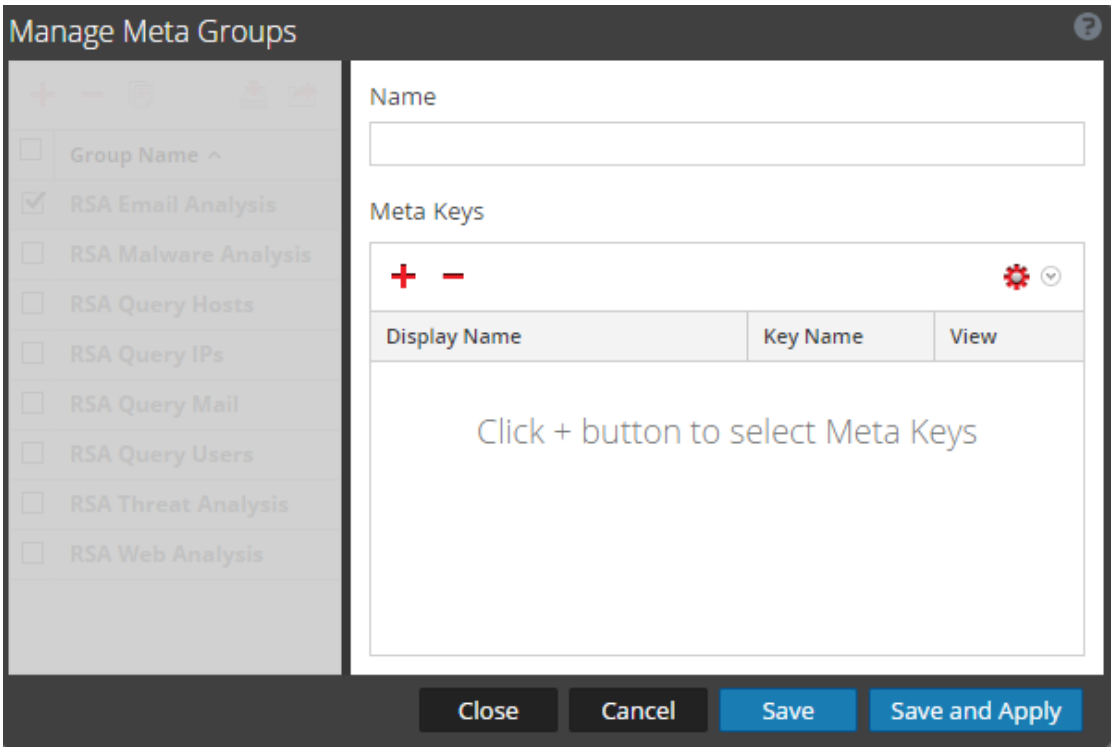
Create a Meta Group and Add Meta Keys

1. While investigating a service in the **Investigate > Navigate** view, select **Meta > Manage Meta Groups** in the toolbar.
   The Manage Meta Groups dialog is displayed. Initially only OOTB groups are configured for a service and listed under Group Name. If other custom groups have been configured, they are also listed under Group Name.

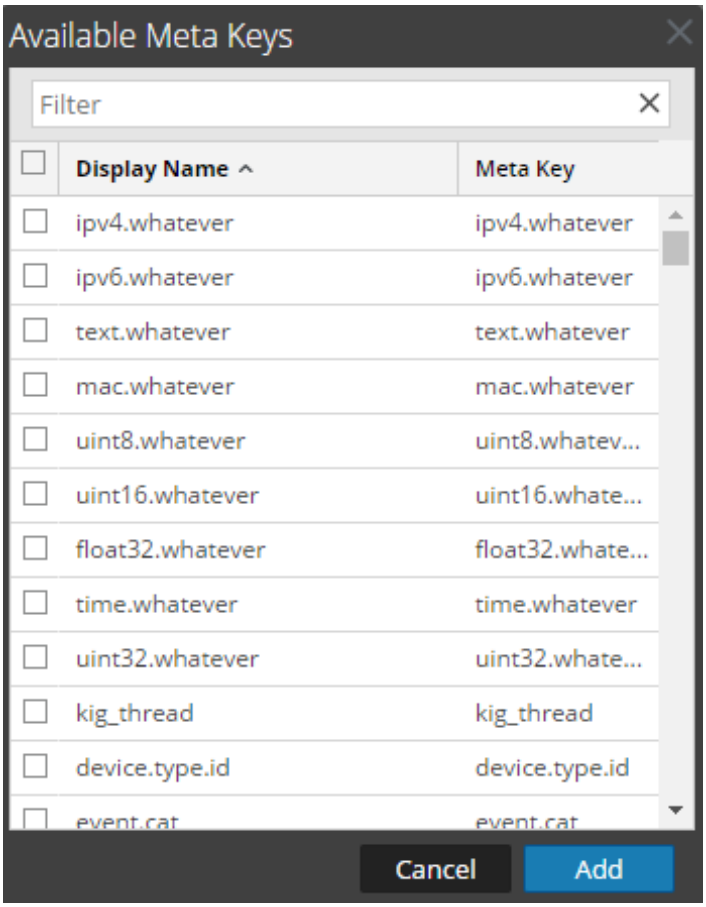


2. In the grid toolbar, click +.
   A new row is inserted at the top of the Meta Groups grid.

3. Type a name for the new meta group, and press **Enter**.
   The form to the right opens for editing.



4. (Optional) If you want to change the name of meta group, type a new value in the **Name** field.
5. In the **Meta Keys** toolbar, click **+**.
   The Available Meta Keys dialog is displayed, with keys in alphabetical order.

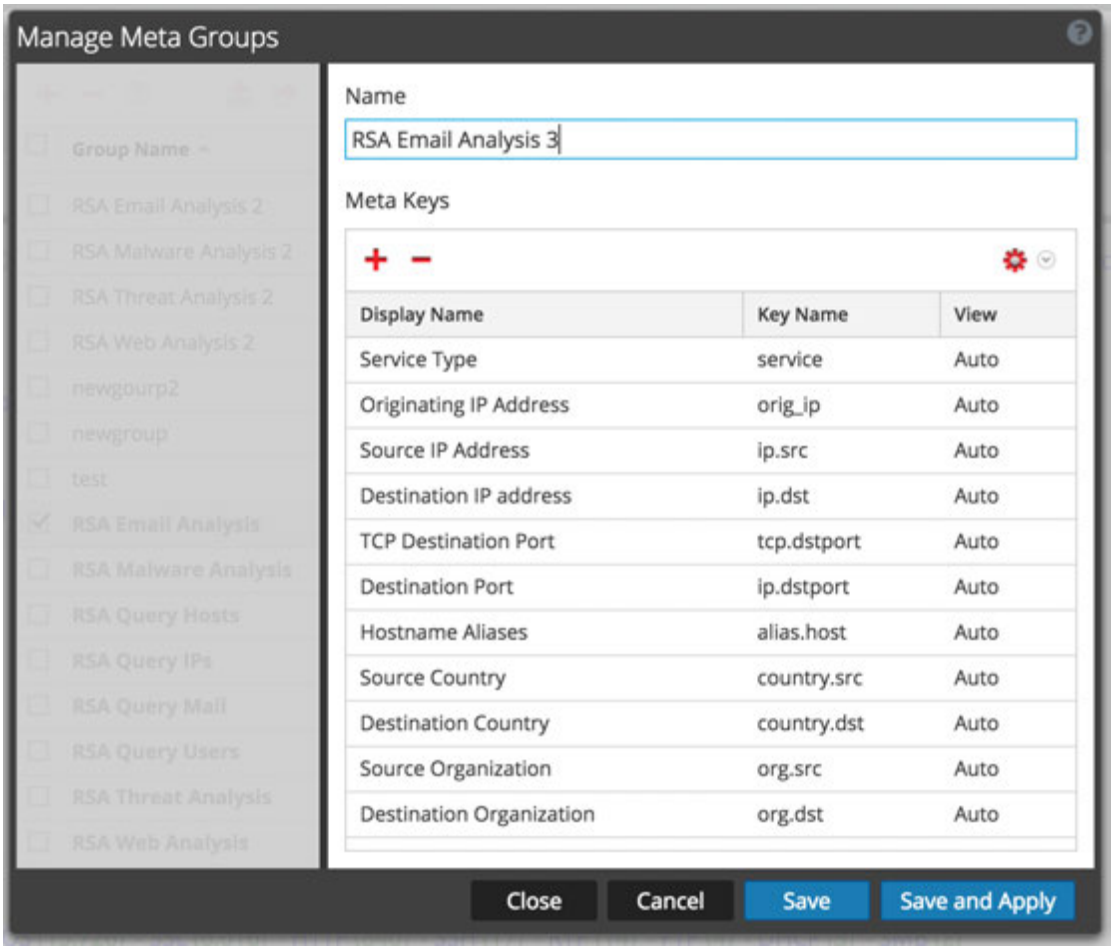


6. To filter the list of meta keys, type a word or phrase in the **Filter** field and select **Enter**.
   The list displays matching meta keys based on a case-insensitive search. Delete the filter text and press **Enter** to remove the filter.
7. To select meta keys to include in the meta group, click the checkboxes. To select all meta keys, click the checkbox in the title bar and click **Add**.
   The selected meta keys are added to the meta keys list.
8. (Optional) If you want to change the order in which the meta keys load and are listed in an investigation, click and drag one or more meta keys to a new position.
9. To finish creating the meta group do one of the following:
   a. To save the meta group, click **Save**.
      The group is created and available for use.
   b. To save and apply the meta group to the current Investigation view, click **Save and Apply**.
      The group is created and applied immediately to the current Investigation view.
10. Click **Close**.

Duplicate and Edit an Out of the Box Meta Group

If you want to customize an OOTB meta group, you need to duplicate the group and then edit the duplicate.

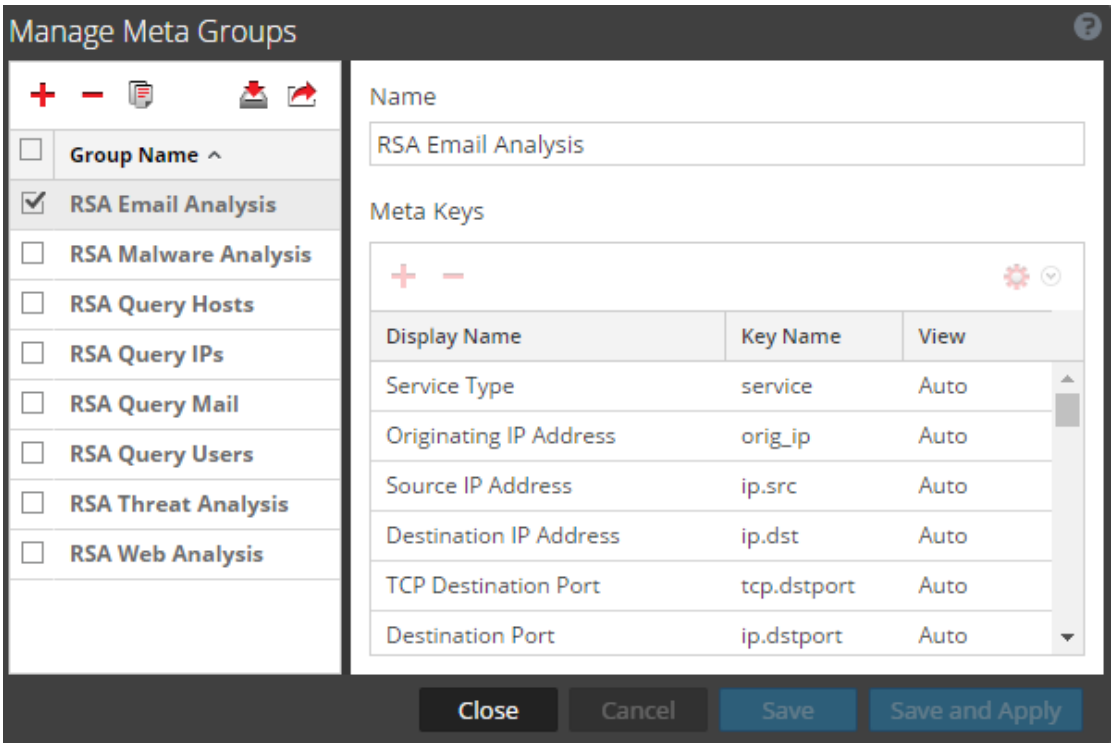
1. Select an OOTB meta group from the Manage Meta Groups grid and click .
   The form to the right opens for editing with all of the meta keys as they are in the OOTB group.



2. Enter a name for the new group and continue editing as described in "Edit a Meta Group" below.

Edit a Meta Group

1. Select a group from the **Meta Groups** grid.
   The form to the right opens for editing.



2. (Optional) Edit the Name of the group.
3. (Optional) Add new meta keys, as described above in Create a Meta Group and Add Meta Keys.
4. (Optional) To set the order for the keys, drag and drop one or more keys.
5. (Optional) To change the initial view of a meta key, click and choose one of the possible views.
   When you modify the meta group, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.
   The value for the initial view is displayed in the View column.
6. To save, the changes, click **Save**.
7. To apply the changes to the current Navigation view, click **Save and Apply**.

Delete a Meta Group

1. In the **Meta Groups** grid, select the group to be removed.
2. Click .
   A confirmation dialog provides an opportunity to cancel or complete the request.

3. Click **OK**.
   The meta group is deleted. When you close the window, if the deleted group was the currently applied meta group, it is removed and the default meta keys are used to build the view.

Export a Meta Group

User-defined meta groups are created on individual services. To make meta groups available to another service, you must export them to your local file system. To export one or more meta groups:

1. In the **Meta Groups** grid, select one or more groups to be exported.
2. Click .
   The selected groups are downloaded to your local file system as a **MetaGroups.jsn file**. Every download of meta groups has the same name with a numeral appended to avoid overwriting previous downloads.

Import a Meta Group

To make user-defined meta groups from another service available to the currently investigated service, you must import the `MetaGroups.jsn` file from the local file system. When you import meta groups, an error message is displayed if any of the groups are already present. To import a group that is a duplicate, you must first delete the existing group. If you want to delete a meta group, it cannot be in use by a profile.

To import meta groups:

1. In the **Meta Groups** grid, select a file to import and click .
   The selection dialog is displayed.

2. Click **Browse** and navigate to the directory on your local file system where the downloaded `MetaGroups.jsn` files are stored. Select a file and click **Open**.
   The filename is displayed in the Upload File field.
3. Click **Upload**.
   The upload process begins, and a message indicates that the upload was successful. The

meta groups are added to Meta Group grid. If the file is a duplicate of an existing meta group, a dialog tells you that the meta group already exists.

Visualize Metadata as Parallel Coordinates

Analysts can use the parallel coordinates visualization in the Navigate view to focus the investigation on combinations of meta keys and values that may indicate events are abnormal and worth investigation.

Note: In Version 11.1 and later, wherever meta keys are used, you can also use configured meta entities.

The parallel coordinates chart is a way of visualizing the current drill point in Investigation to examine more than two meta keys simultaneously. Visualizing multiple meta keys simultaneously can help in identifying security issues associated with multivariate patterns and comparisons, such as when individual meta keys and values may not be of concern, but combining them together may bring an abnormal pattern or relationship to light. Meta groups (see Manage Meta Groups) can be used effectively to define a collection of meta keys that you want to visualize as parallel coordinates.

Best Practices for Effective Parallel Coordinates Charts

To create effective parallel coordinates charts, follow these recommendations:

- Start from a drill point in the Navigate view rather than attempting to visualize all data.
- Limit the time range if necessary.
- Choose the smallest useful set of meta keys to display as axes.
- Specify the sequence of axes to highlight anomalies between the meta values as you follow a line across the chart.
- When you can identify a useful set of meta keys and sequence, create a custom meta group to use for future investigations. For example, you can create a custom meta group for Windows executable file types.
- Use the RSA out-of-the-box (OOTB) meta groups that are included in a new installation.
- Re-use and share custom meta groups by importing and exporting groups as .jsn files.
- It may be useful to create two versions of each custom meta group. One for analysis of meta values and one for creating a parallel coordinates chart focusing on a smaller subset of the same use case.

Note: When you import meta groups, an error message is displayed if any of the groups are already present. To import a group that is a duplicate, you must first delete the existing group. If you want to delete a meta group, it cannot be in use by a profile.

To help build better parallel coordinates charts, several optimizations are included in NetWitness Suite.

- Analysts can specify that only sessions in which all meta keys exist are rendered in the chart.
- The administrator can increase the number of meta values rendered in the Parallel Coordinates Settings in the Administration System view.

RSA Meta Groups for Parallel Coordinates Use Cases

A set of predefined meta groups is included with NetWitness Suite. If you want to get the latest version, you can import the meta groups file, `MetaGroups_ootb_w_query.jsn`, in the Manage Meta Groups dialog. Some of the targeted activities that lend themselves well to Parallel Coordinates visualizations are:

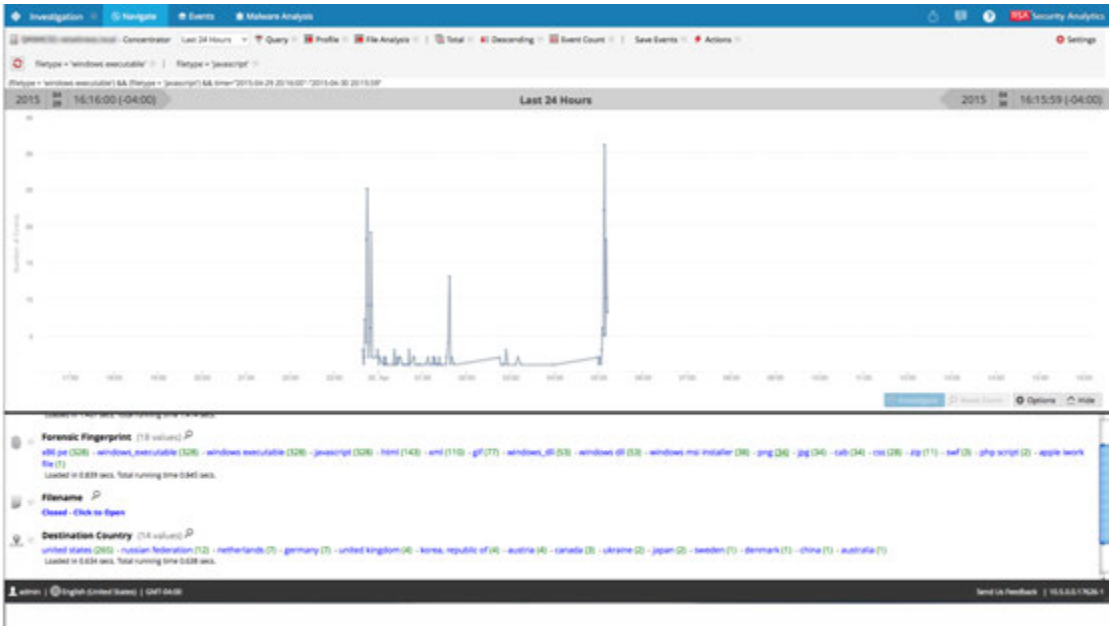
- Botnet Beaconing
- Covert Channels
- Email
- Encrypted Sessions
- Endpoint Analysis
- File Analysis
- Malware Analysis
- Outbound HTTP
- Outbound SSL/TLS
- SQL Injection Attacks
- Threat Analysis
- Web Analysis

View a Parallel Coordinates Visualization

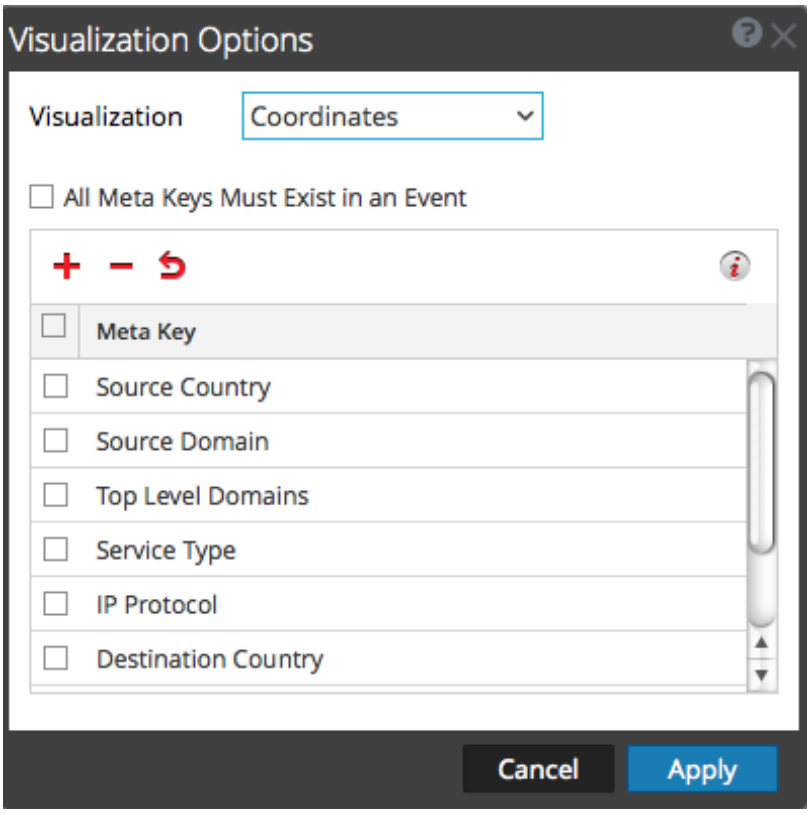
From an investigation in the Investigate > Navigate view:

1. If the Visualization panel above the Values panel is closed, select **Visualization**.
2. In the toolbar, select Meta > **Use Meta Group > File (Malware) Analysis**.
3. In the **Values** panel, in the **Forensic Fingerprint** meta key, click `windows_executable` and then `x86 pe`, so that the breadcrumb reads `filetype = 'windows_executable' | filetype = 'x86 pe'`.

4. A default visualization for the current drill point is displayed as a timeline.



5. In the **Visualization** panel, select **Options**.
   The Visualization Options dialog is displayed.
6. In the **Visualization** drop-down list, select **Coordinates** and click **Apply**.

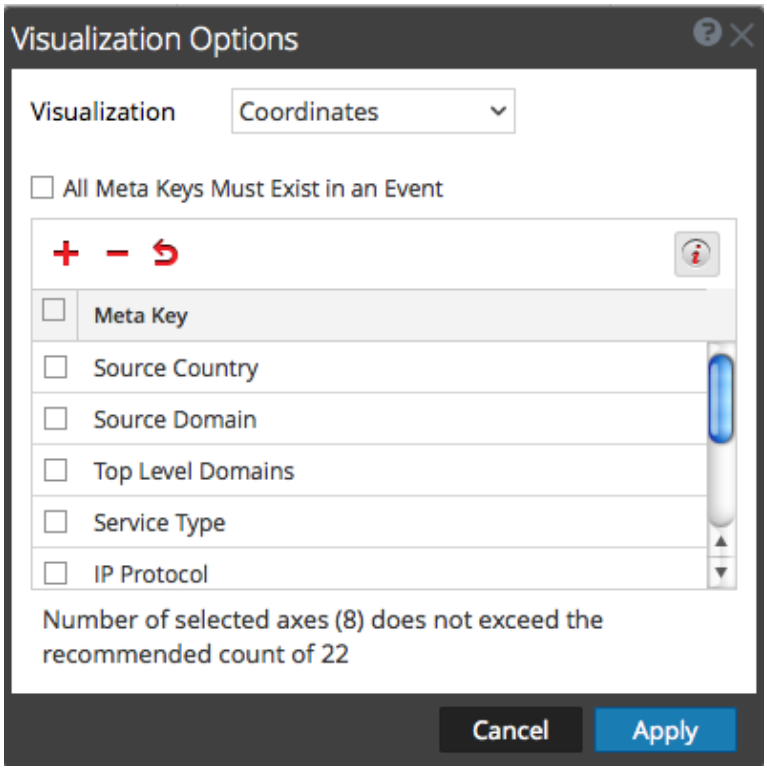


The visualization is loaded. In this example, 249 events are found and 199 unique paths are visualized.

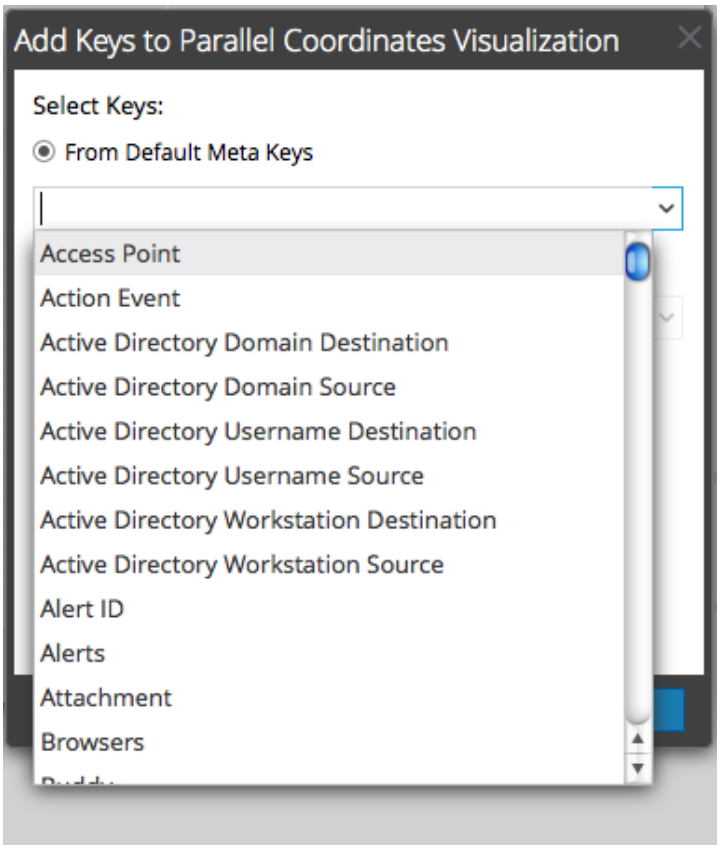
Select Meta Keys for a Parallel Coordinates Visualization

With a Parallel Coordinates visualization open, do the following:

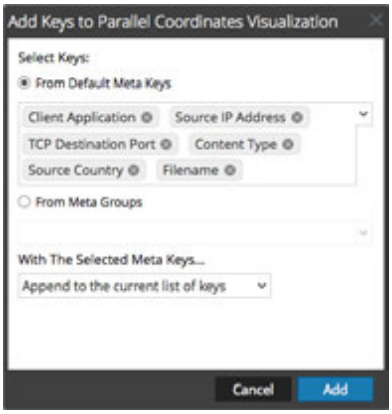
1. In the Visualization panel, select **Options**.
   The Visualization Options dialog is displayed. In the toolbar, click to display the recommended number of axes for a readable visualization. When a recommended count of keys is displayed, the count changes based on the browser size. If you make the browser window larger, the recommended count is increased.



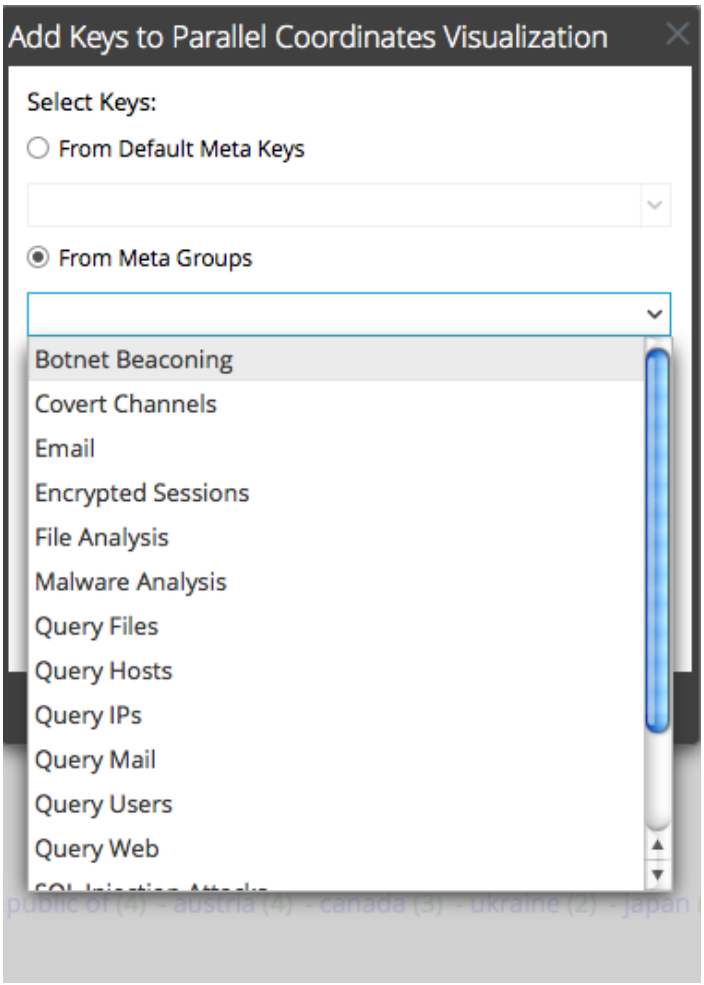
2. If you want to change the sequence of the meta keys, drag meta keys up or down to the desired sequence.
3. If you want to delete any meta keys, click in the selection box, and click .
   The meta keys are removed, but the change has not been applied.
4. If you want to revert to the previous state, click .
   Any meta keys you have deleted are restored and any changes that you made are removed.
5. If you want to select individual meta keys, click , select **From Default keys**, and in the drop-down list, select the meta keys.



The selected keys are listed.

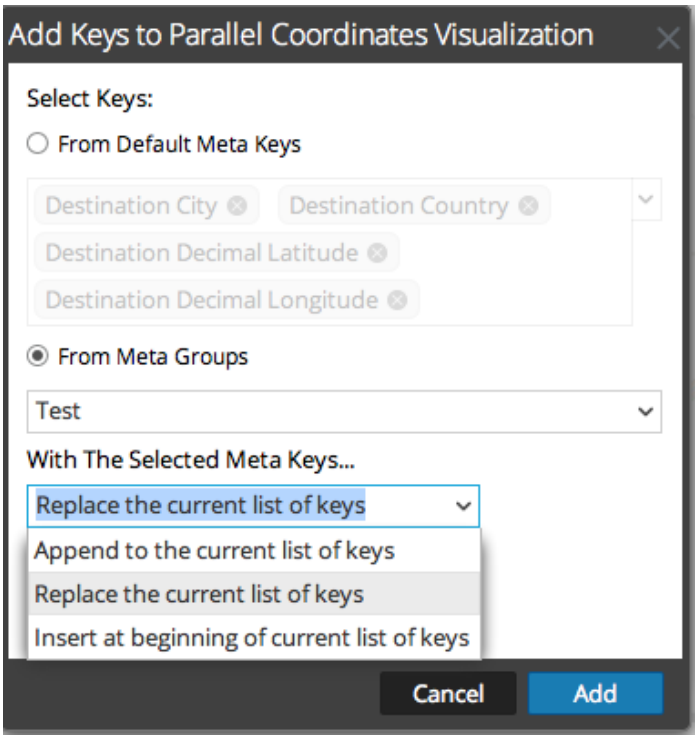


6. If you want to add all the keys in a meta group, you cannot add individual meta keys. Select **From Meta Groups**, and select a group from the drop-down list.



The selected meta groups are listed in the field.

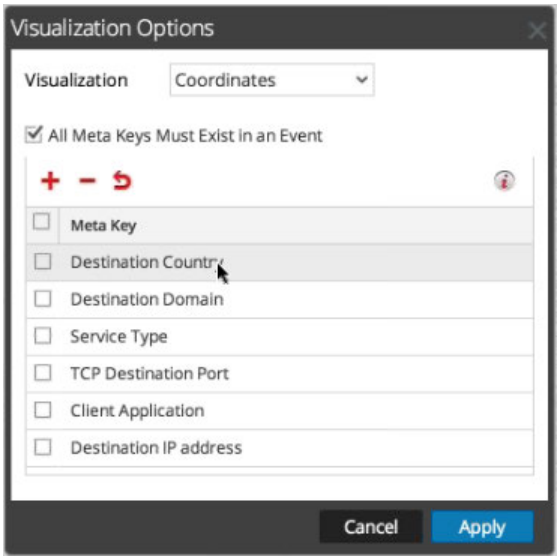
7. Select the method of adding the keys or groups: **Replace the current list of keys**, **Append to the current list of keys** (at the end), or **Insert at the beginning of current list of keys.**



8. To complete the procedure, click **Add**.
   The Visualization Options dialog is displayed with the meta keys or groups you selected.
9. To display the new visualization chart, click **Apply**.

Optimize a Parallel Coordinates Visualization

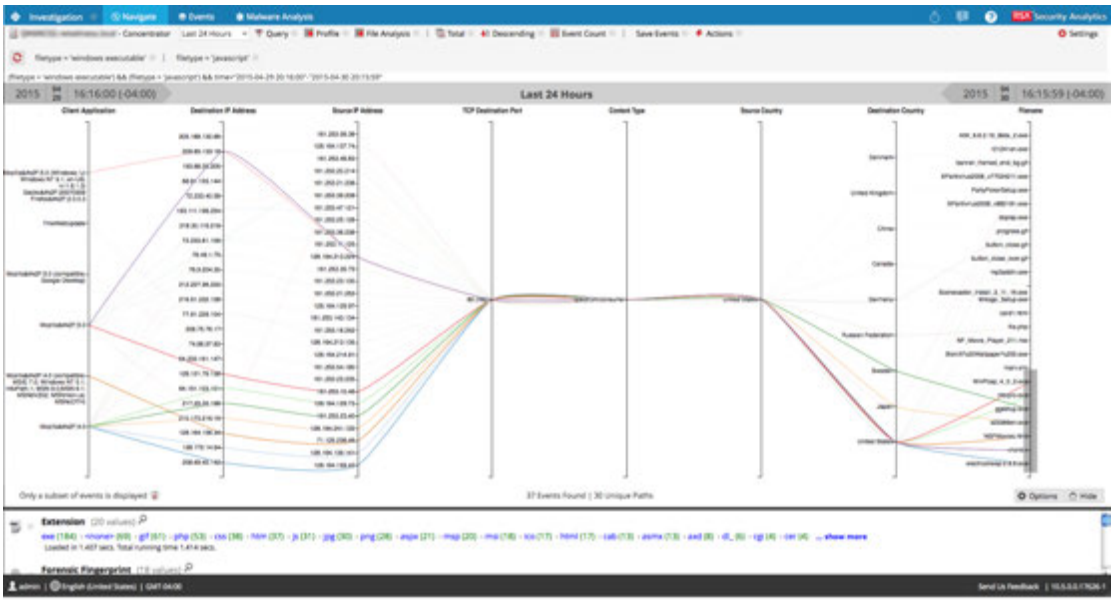
1. To optimize the visualization by removing events in which not all meta keys exist, select **Options.**



2. In the Visualization Options dialog, select **All Meta Keys Must Exist in an Event**. Click **Apply**.
   The resulting graph is more readable and useful and has fewer unique paths.

3. If you want to highlight a small set of points to see the path of the line from right to left, click on an axis. The cursor changes to cross hairs, which you can drag to select one or more

values. When you let go of the mouse, the lines are highlighted. In the example below, the SSL service type is highlighted by a gray box.



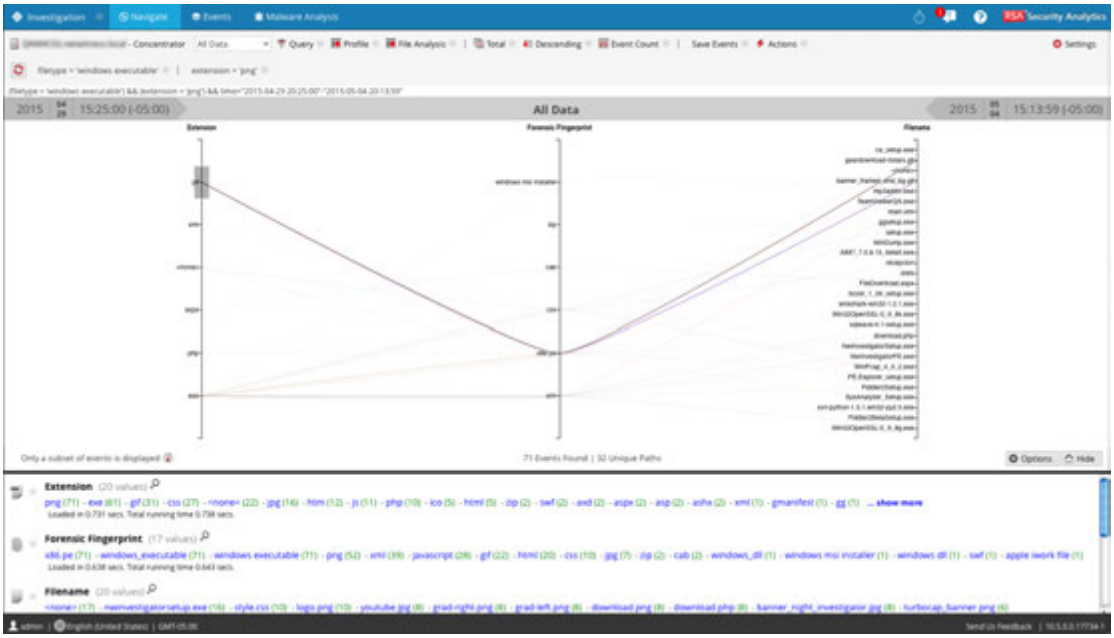
4. If you want to enlarge the visualization, drag the bottom edge of the panel down and drag the right edge of the browser window wider.

Sample Use Case

Below is an example of a parallel coordinates visualization of meta keys representing file metadata in a session. There are three meta keys or axes from left to right: Extensions, Forensic Fingerprint, and Filename with values listed along each axis. Values on the Extension axis show the file extension, and values on the Forensic fingerprint axis are windows executables. Normally the file type matches the expected forensics fingerprint; however, it is abnormal for a `gif` file type to be combined with the Windows executable fingerprint. The `gif` file type is selected to highlight the correlations of that file type, `x86pe` , and two filenames in the third axis so that an analyst can quickly identify the files that merit investigation.

To reach this view:

1. Order by Value and Sort in Ascending order.
2. Apply two filters (file type = 'windows executable' and extension = 'gif') in the Navigate view to limit the amount of data.
3. Configure a parallel coordinates chart by choosing three axes: `file extension`, `forensic fingerprint`, and `filename`.



Sample Visualization of a Large Data Set

This example of a parallel coordinates visualization applied to a larger set of data illustrates several messages that help analysts to understand what has been charted.

- To create a chart, NetWitness Suite begins scanning meta values and returning results. A typical time range could have up to 10,000,000 meta values. When the number of meta values returned reaches the Meta Values Result Limit, the chart is rendered even if NetWitness Suite has not scanned a number of meta values equal to the Meta Values Scan Limit.
- There is a fixed limit on the amount of data that can be rendered as a parallel coordinates chart. In NetWitness Suite 10.4 and prior, the limit is based on the number of axes times data values: 1000 x the number of axes to protect performance, but in NetWitness Suite 10.5 and above the administrator configures parallel coordinates limits as part of the Investigation settings In the Administration System view.

With a larger set of data, the parallel coordinates chart takes longer to process than the smaller set of data and meta keys. To preserve performance, NetWitness Suite renders the meta values from the Values panel below until the limits set by the Administrator are reached. An informational message tells you: **Only a subset of events is displayed.**

Of all the data visualized for 249 events, there were only 199 unique parallel coordinates paths. Some events are included though they do not include some of the meta keys; these are labeled **DNE** because the meta does not exist in the event.

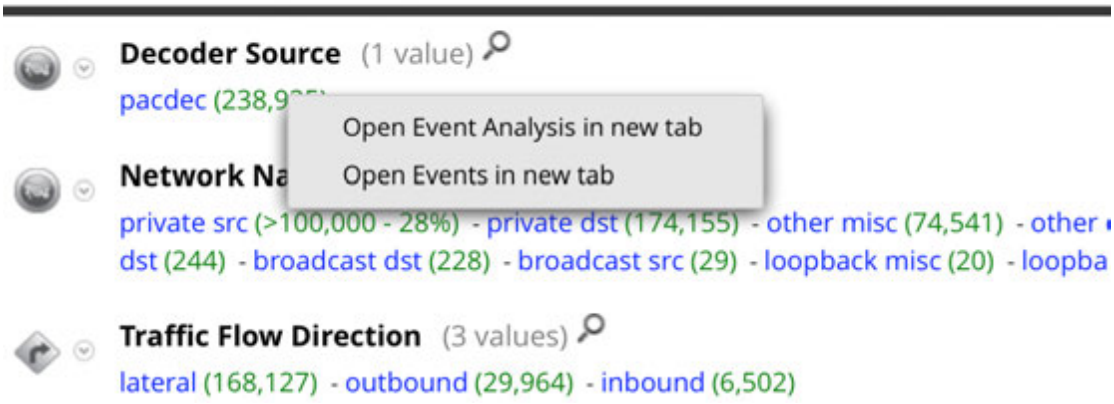
Open an Event in the Events List

Analysts can view a list of events associated with a session in the Investigate > Events view or in the Event Analysis view.

To display events in the Events view do one of the following:

1. To use the default query for the default service, go to **INVESTIGATE** > **Events**. NetWitness Suite runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
2. To view events for a specific meta value, go to **INVESTIGATE > Navigate** and when events are loaded in the Values panel, click a meta count (the meta count is in green text). You can also right-click the meta count for a meta value . When the context menu is displayed, click **Open Events in new tab**. (The Open Event Analysis in new tab option is

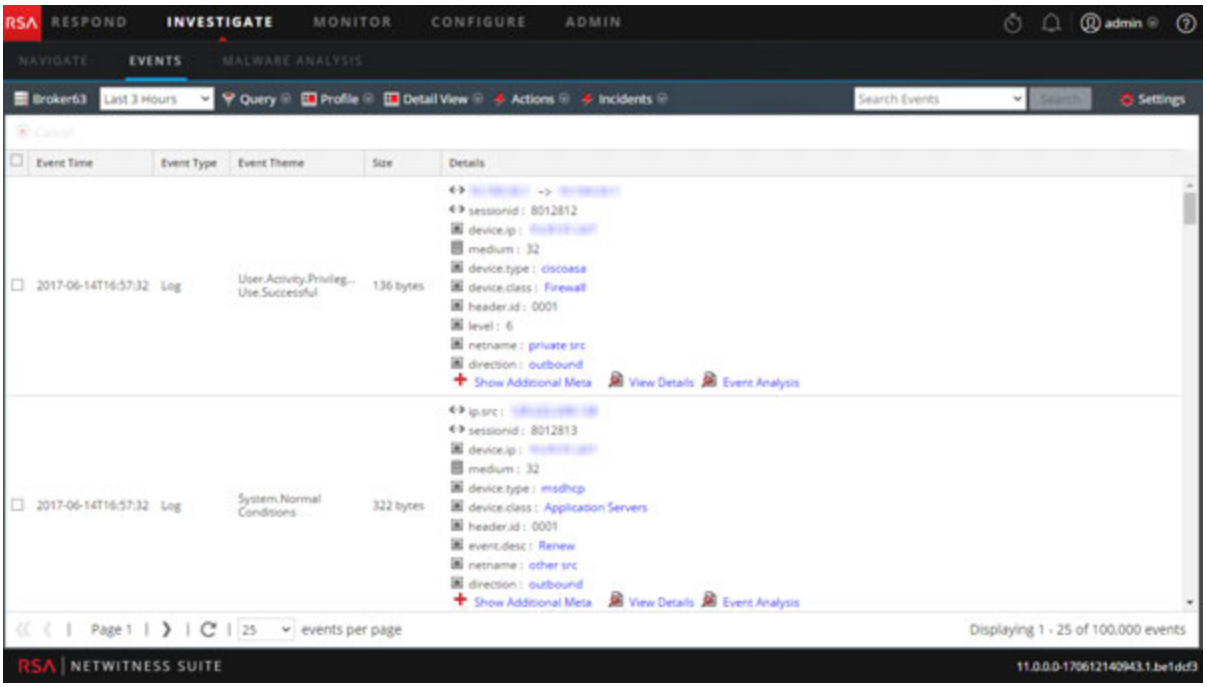
available in Verison 11.1 and later.)



The Events view displays the events for the selected meta value.

The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view.

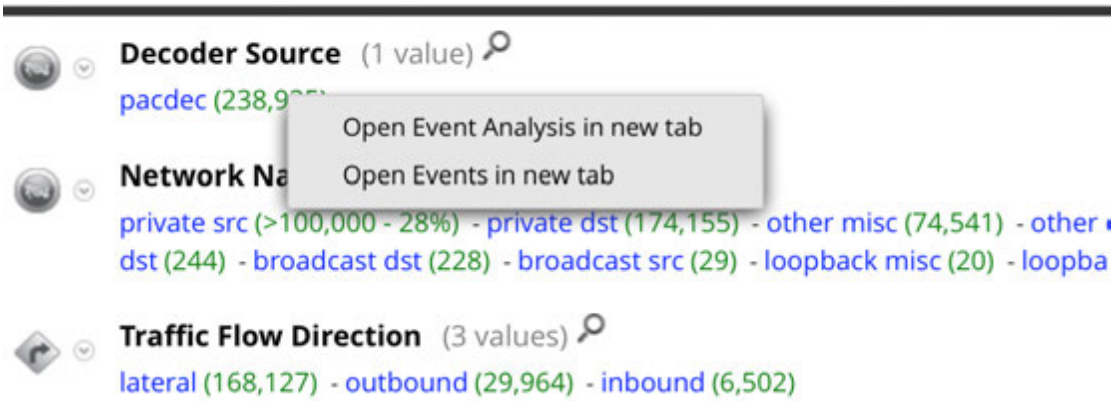
This figure is an example of the Detail view.



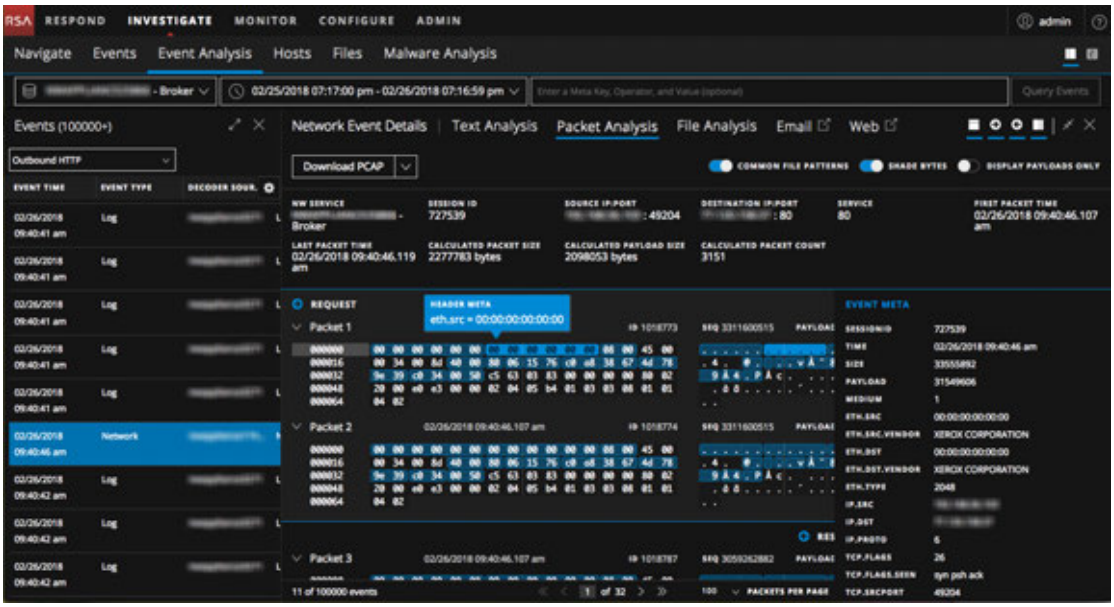
You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can extract files, export events, export logs, and open the Event Reconstruction panel by double-clicking an event. See Examining Raw Events in the Events View for detailed information about these capabilities.

To display events in the Event Analysis view, do one of the following:

1. In Version 11.0.0.x , go to **INVESTIGATE > Navigate**, right-click the meta count for a meta value (the meta count is in green text). When the context menu is displayed, select **Open Event Analysis in new tab.**



The Event Analysis view displays the events for the selected meta value.



For detailed information about the types of analysis that you can use in this view, see Analyze Events in the Event Analysis View .

Export or Print a Drill Point

In NetWitness Investigate, when you have the data for a drill point displayed in the Navigate view, you can:

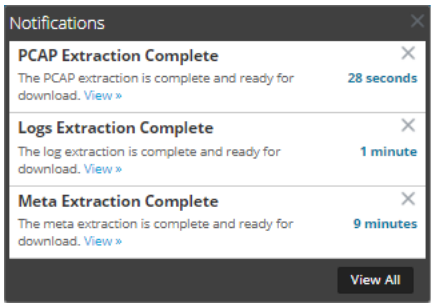
- Extract files from a session and choose the type of files to extract: archives, audio BitTorrent, documents, executable, images, other, video, and web.
- Export the drillpoint as a packet capture (PCAP) file, a log file or a meta data file.
- Print the drillpoint.

The details being exported are affected by both the time range and drill point at the time of exporting.

Note: When you export the drill point as a log file, only the log sessions are exported. The job queue message refers to the total number of sessions in the drill point rather than the number of logs. For example, if the drill point has 505 sessions and only five log sessions, the job queue message states that NetWitness Suite is extracting logs for 505 sessions.

To export a drill point from the Navigate view:

1. Conduct an investigation until you reach the desired drillpoint.
2. For Version 11.0, In the toolbar, select **Actions > Export** and select one of the export options: **PCAP**, **Logs**, or **Meta**.
   The drill point is extracted, and a message advises that the job is scheduled. You can check the jobs page for the status.
3. For Version 11.1, in the toolbar, select Save Events > and selecto one of the export options: PCAP, Logs, Files, Meta.
   A dialog gives you an opportunity to edit the default filename for the file. The default is in the form `investigation-Feb-21-15-44-33`
4. A dialog allows you to select the export log format: Text, XML, CSV, JSON. A dialog selects file types. A dilaog selecte Meta format: Text, CSV, TSV, JSON.
5. When the scheduled file extraction is complete, it is displayed in the Job Notifications tray.



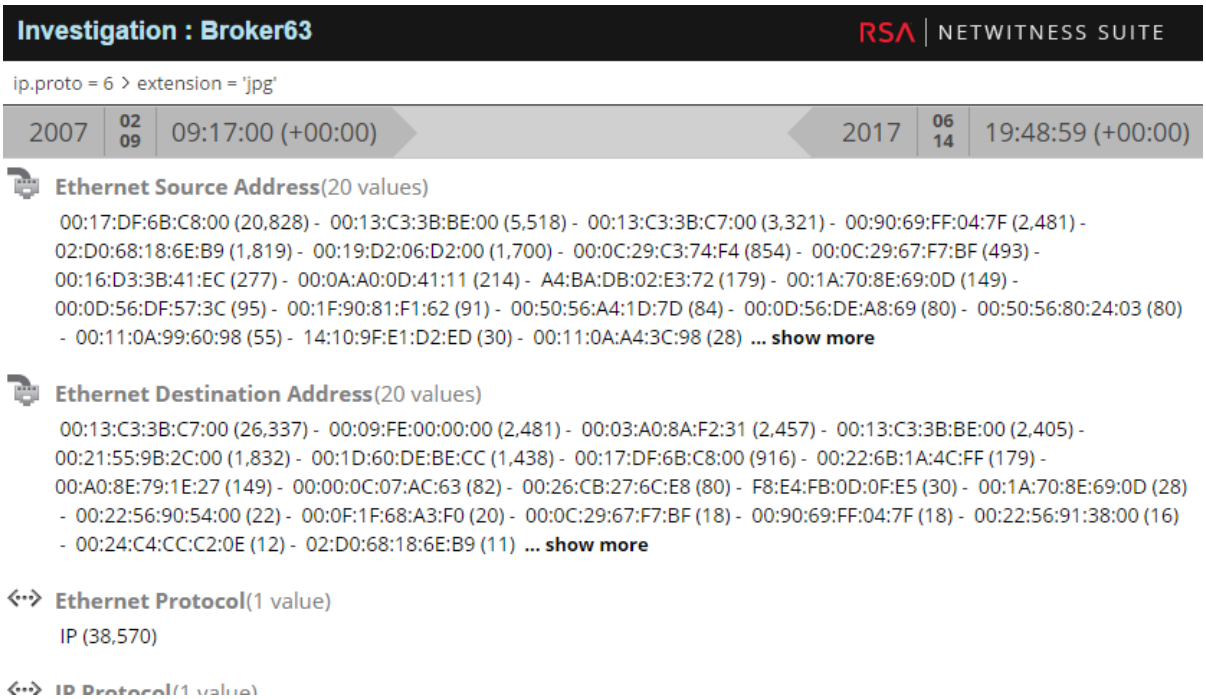
6. Click the **View** link in the Jobs tray sand download the specific extraction file requested.

To print the current drill point:

In the Navigate view, you can display the contents of the current drill point in printer friendly format in the browser window.

To display the current drill point in a print view:

1. With a drill point open in the **Navigate** view, select **Actions > Print** in the toolbar.
   A new tab is created with the print view of the current drill point.



2. Use the print option in your browser to send the printable view to the printer.

Launch an External Lookup of a Meta Key

This topic provides instructions for using out-of-the-box Investigate plugins to launch an external lookup of specific meta keys using tools external to NetWitness Suite while investigating data in the Navigate view or Events view.

Analysts can use out-of-the-box NetWitness Suite Investigation external lookups to save time during investigations. The out-of-the-box lookups are available by right-clicking one of the these meta keys: IP address (`ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`), `host` (`alias-host`, `domain.dst`), `client`, and `file-hash`.

For all `IP` and `host` meta keys, the following lookups are built in to NetWitness Suite:

- Google Malware: Opens a Google Malware search in a new tab.
- McAfee SiteAdvisor: Opens a McAfee SiteAdvisor search in a new tab.

- BFK Passive DNS Collection: Opens a BFK Passive DNS collection search in a new tab
- CentralOps Whois for IPs and Hostnames: Opens a CentralOps Whois search for IPs and hostnames
- Malwaredomainlist.com Search: Opens a Malwaredomainlist.com search in a new tab
- Malwaredomains.com Search: Opens a Malwaredomains.com search for in a new tab
- Robtex IP Search: Opens a RobtexIP search in a new tab
- SamSpade Search: Opens a SamSpade search in a new tab
- ThreatExpert Search: Opens a ThreatExpert search in a new tab
- UrlVoid Search: Opens a UrlVoid Search in a new tab n a new tab

For the `file-hash` and `alias-host` meta keys, the Google lookup opens a Google search in a new tab.

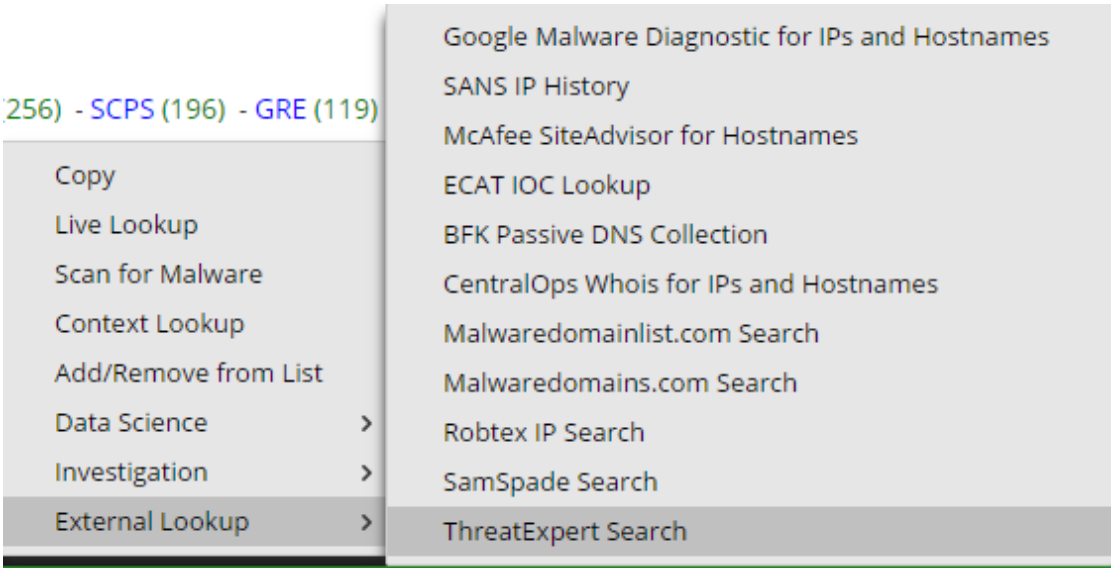
For the `client` meta key, the ECAT Lookup option opens an ECAT client in a new tab if the ECAT client is installed on the same system on which the browser is being used.

Administrators can add additional external lookups and other custom actions as described in "Add Custom Context Menu Actions" in the *System Configuration Guide*.

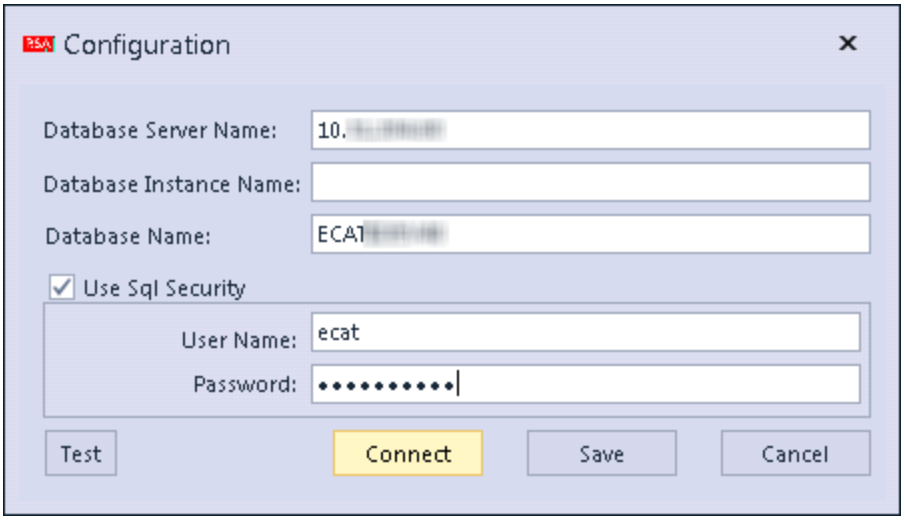
Launch an ECAT IOC Lookup

To launch an ECAT lookup of data from the Navigate view:

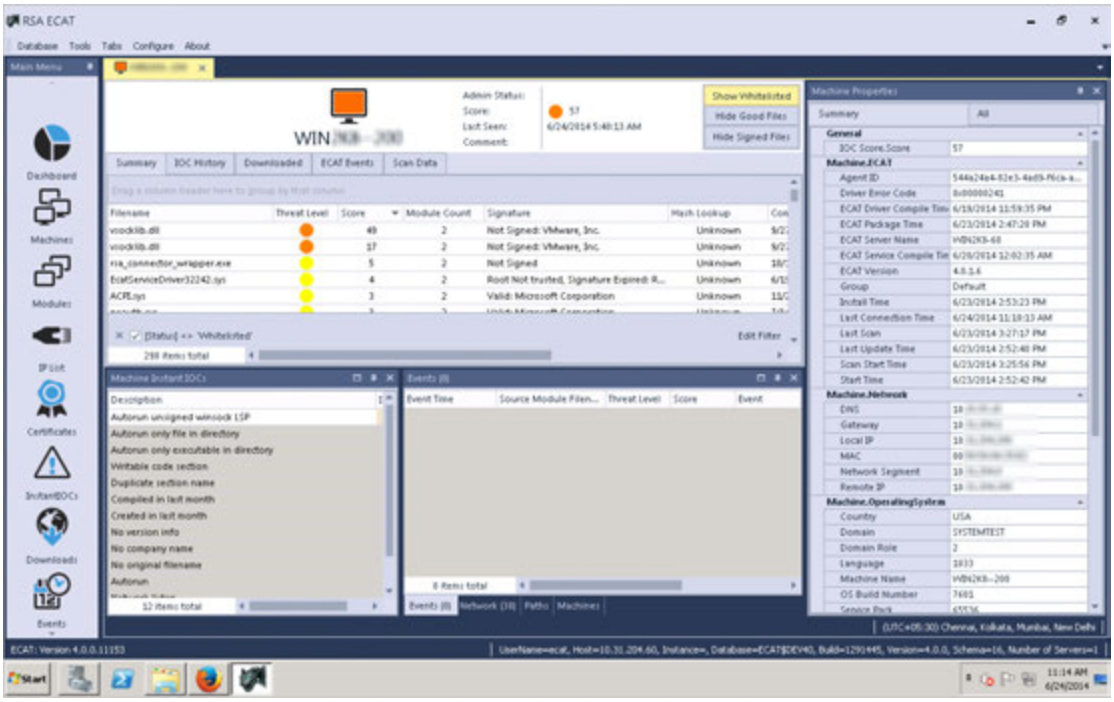
1. Right-click a meta value for one of the following meta keys: `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst`, `client.`
2. Select **External Lookup** in the context menu.
   A submenu of external lookup options is displayed.



3. Select **ECAT IOC Lookup**.
   A dialog asks you to choose an application.
4. Select ECAT and click **OK**.
   The RSA ECAT Configuration dialog is displayed.



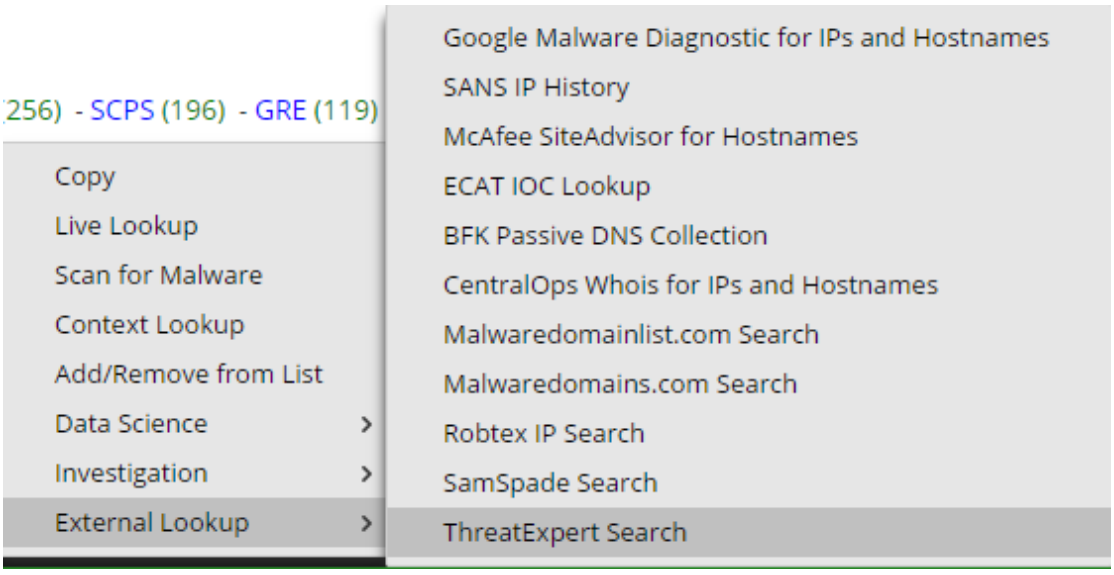
5. Enter the user name and password required to log on to the ECAT client, and click **Connect.**
   The drill point opens in RSA ECAT.



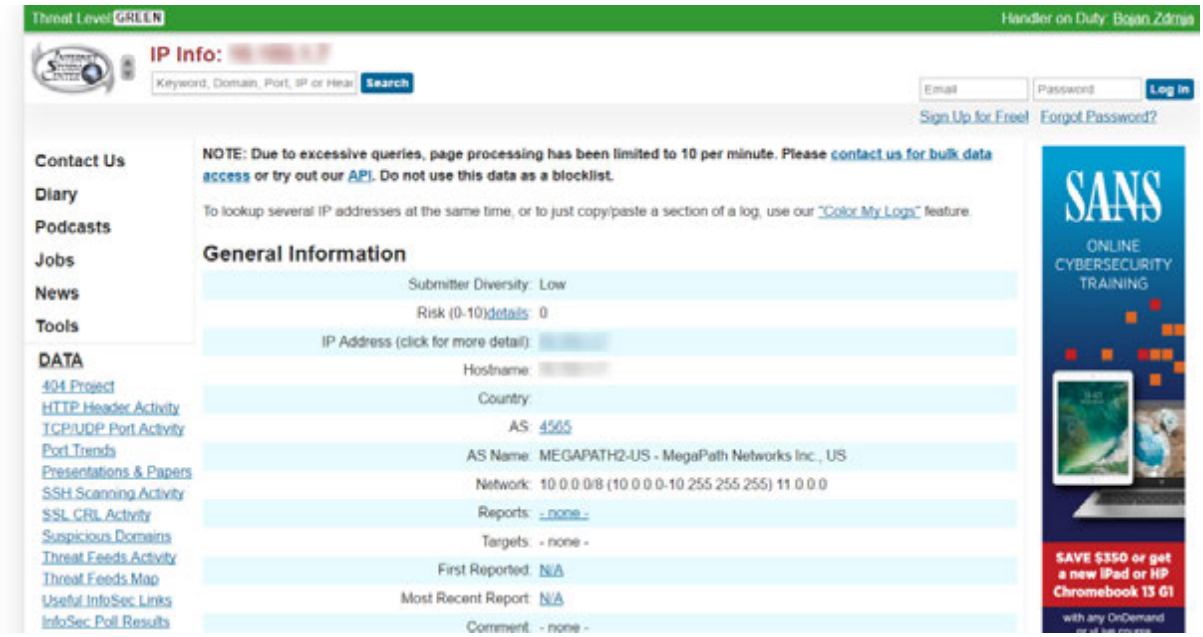
Lauch Other External Lookups

To launch an external lookup (other than ECAT IOC) of data from the Navigate view:

1. Right-click a meta value for one of the following meta keys: `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`
2. Select **External Lookup** in the context menu.
   A submenu of external lookup options is displayed.



3. Select one of the lookup options.
   The selected meta value opens in the selected lookup, for example, if you selected SANS IP History, the drill point information is displayed in SANS Internet Storm Center.

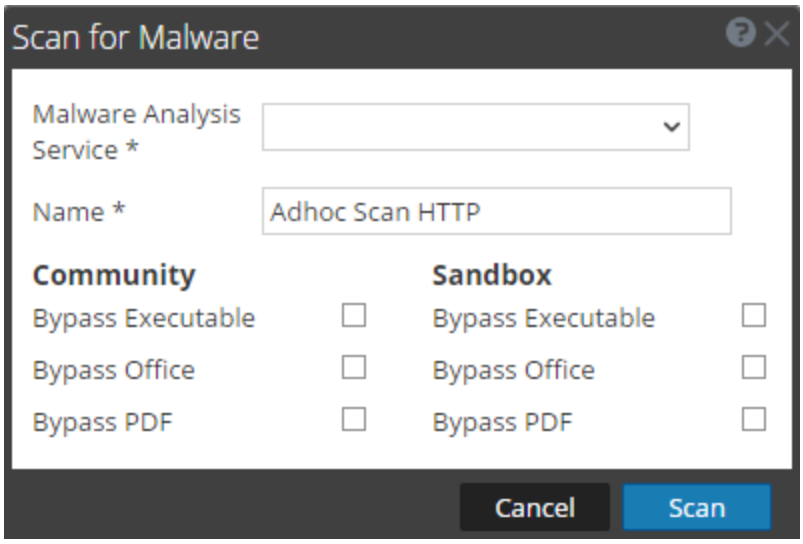


Launch a Malware Analysis Scan from the Navigate View

From within Investigate, analysts can launch an on-demand Malware Analysis scan by selecting a service and meta value, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis.

To launch a Malware Analysis scan of data from the Investigate > Navigate view:

1. Right-click a meta value (for example, OTHER, DNS, or FTP) and select **Scan for Malware** in the context menu.
   The Scan for Malware dialog is displayed with a suggested name for the on-demand scan and no service selected.
2. In the Scan for Malware dialog, select a service to perform the scan, edit the name, and select the types of files to bypass under community and sandbox.

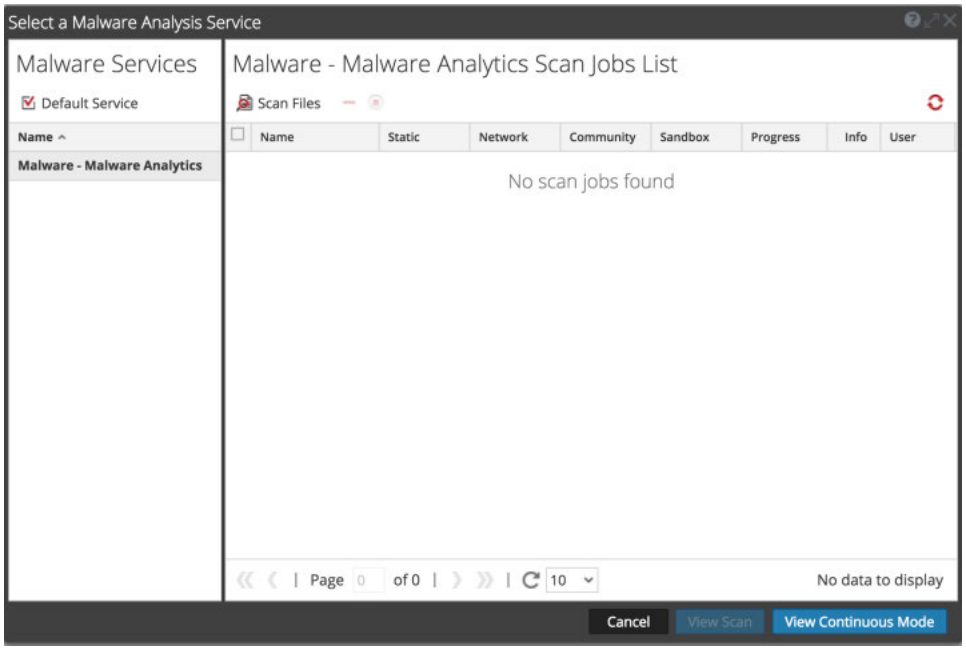


3. Click **Scan**.

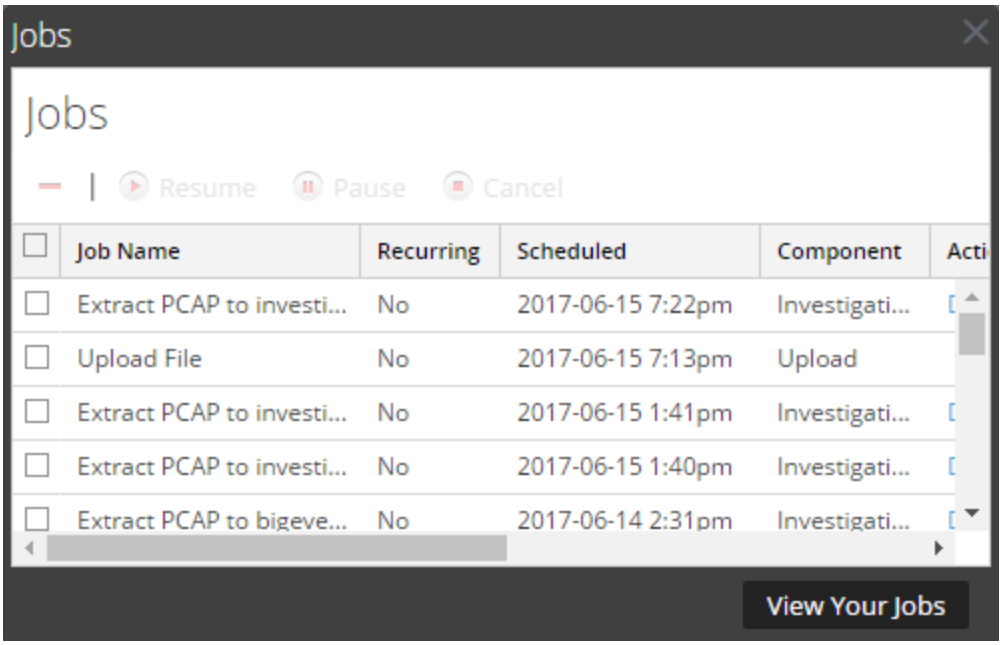
   The scan request is added to the Scan Jobs List dashlet and the Jobs Tray. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.

4. To view the jobs, do one of the following:

   a. Go to the Scan Jobs List in the Malware Analysis view or in the Unified dashboard. Double-click a scan to view the scan.



b. To view the job in the Jobs tray, click in the NetWitness Suite toolbar. When the job is complete, scroll to the left and click **View**.



The Malware Summary of Events for the selected scan is displayed. The scan is also added to the list of available scans in the dialog for selecting scans in the Investigation > Malware tab.

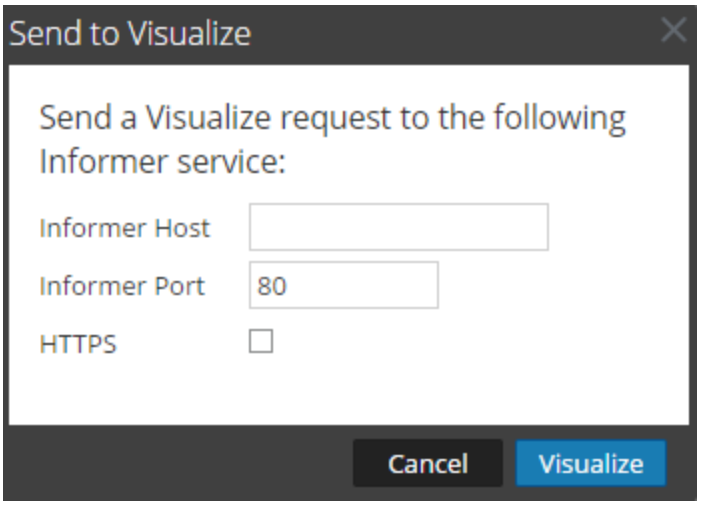
Visualize the Current Drill Point in Informer

This topic provides instructions for sending a drill point in the Navigate view to an Informer visualization.

Informer must be installed in your network and accessible by the service being investigated. You need to supply the host name and the port used on the Informer host to communicate with NetWitness Suite.

To display a visualization in Informer of the current drill point:

1. With a drill point open in the Navigate view, click **Actions > Visualize**.
   The Send to Visualize dialog is displayed.



2. Type the Informer hostname or IP address, and verify the NetWitness Suite server port used to communicate with the Informer host.
3. (Optional) Select the HTTPS option if the Informer host uses secured communications.
4. Click **Visualize**.
   The visualization is displayed in a new tab.

Examining Raw Events in the Events View

Analysts who are investigating data in Investigate can view and reconstruct events associated with a session.

- Analysts who conduct analysis using NetWitness Suite Investigate, and have the appropriate system roles and permissions set up for their user accounts, can go from a Navigate view drill point to the Events view.
- Analysts who do not have access to the Navigate view or want to go directly to the Events view, can open sessions and examine the events that make up the session in the Events view.
- Analysts can select queries from their "query history" window.

Separate topics describe methods of working in the Events view:

- Add Events to an Incident for Response
- Manage Column Groups in the Events View
- Export Events in the Events View
- Add Events to an Incident for Response
- Combine Events from Split Sessions

In addition, you can use these methods of querying data and acting on results that are common to the Navigate view and the Events view.

- Search for Text Patterns
- Create a Custom Query
- View and Modify Queries Using URL Integration
- Use Profiles to Encapsulate Custom Views
- Manage Context Hub Lists and List Values in Investigate
- View Additional Context for a Data Point
- Reconstruct an Event

Filter and Search Results in the Events View

Analysts can filter the results in the Events view and, by searching for events or selecting the service on which to view events, set the time range, and query meta data.

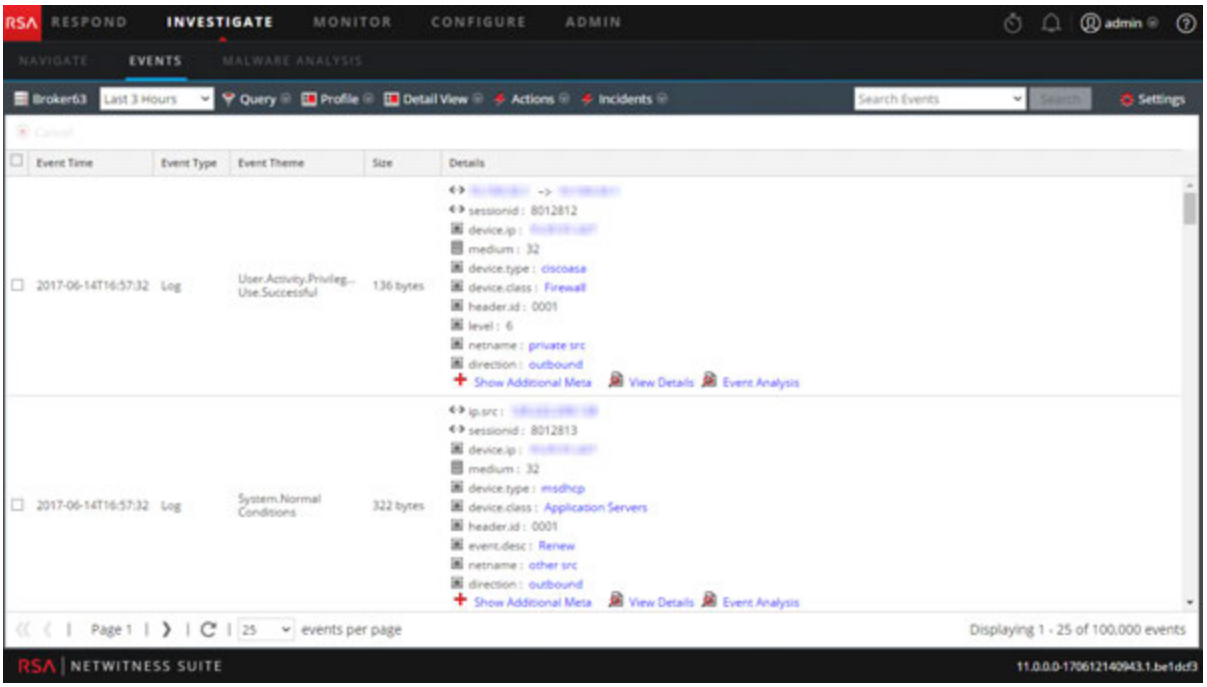
If you opened the Events view from a Navigate view drill point, the view opens to the Detail view of events by default. Analysts who do not have permissions to use the Navigate view can query services directly from the Events view. There are several configuration options to filter the information displayed in the Events view.

Note: When an Archiver is the currently selected service in the Events view and you are searching against a Broker or Concentrator, the search is slower than if searching against a Broker or Concentrator because the data on the Archiver is compressed and there is typically more data.

Filter Events Displayed in the Events View

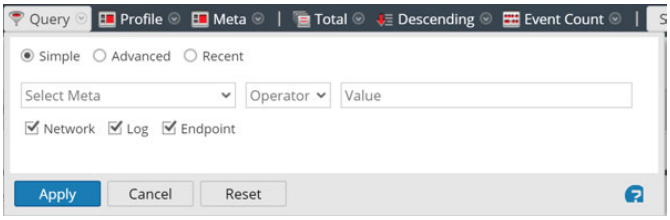
To filter the data displayed in the Events view:

1. In the **Investigate** view, select the **Events** view.
   The Events view is displayed.

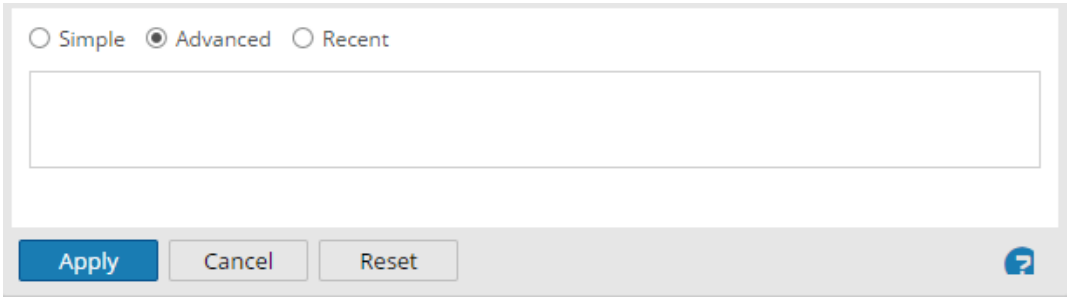


2. To select a time range other than the default (**Last 3 Hours**), in the toolbar, click the time range field and select a value. For example, **Last Hour**.
   The Events view is refreshed with the selected time range.

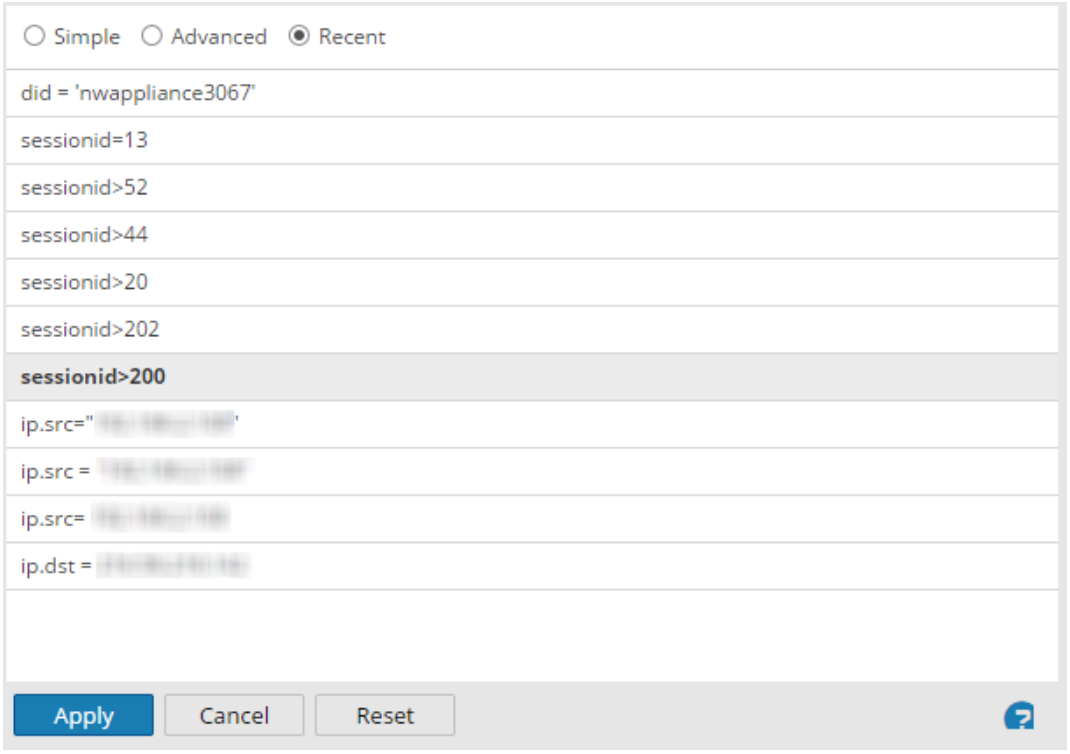
3. To enter a query for the selected service and time range, in the toolbar, click **Query**.
   The Simple Query dialog is displayed.



4. If you want to enter a simple query using the auto-complete feature to select meta and operators, do one of the following:
   a. Click in the **Select Meta** field and select a meta key from the drop-down list.
   b. Select an operator from the drop-down list in the **Operator** field.
   c. Type a value to match in the **Value** field.
   d. Select **Network, Log**, or **Endpoint** data, and click **Apply**.
      The matching data is displayed in the Events view.
5. If you want to enter a more complex query based on your knowledge of the meta and operators:
   a. Click **Advanced**.
      The Advanced Query dialog is displayed.



   b. Type a query. As you type the query, beginning with the meta key, drop-down lists of available meta keys and operators are displayed. When finished, click **Apply**.
6. If you want to select a query from a list of recent queries:
   a. Select **Recent**.
      The Recent Query dialog is displayed.



b. Select a query and click **Apply**.
The matching results for the query are displayed in the Detail View in the Events view. The breadcrumb reflects the query.

c. In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, NetWitness Suite refreshes the results.

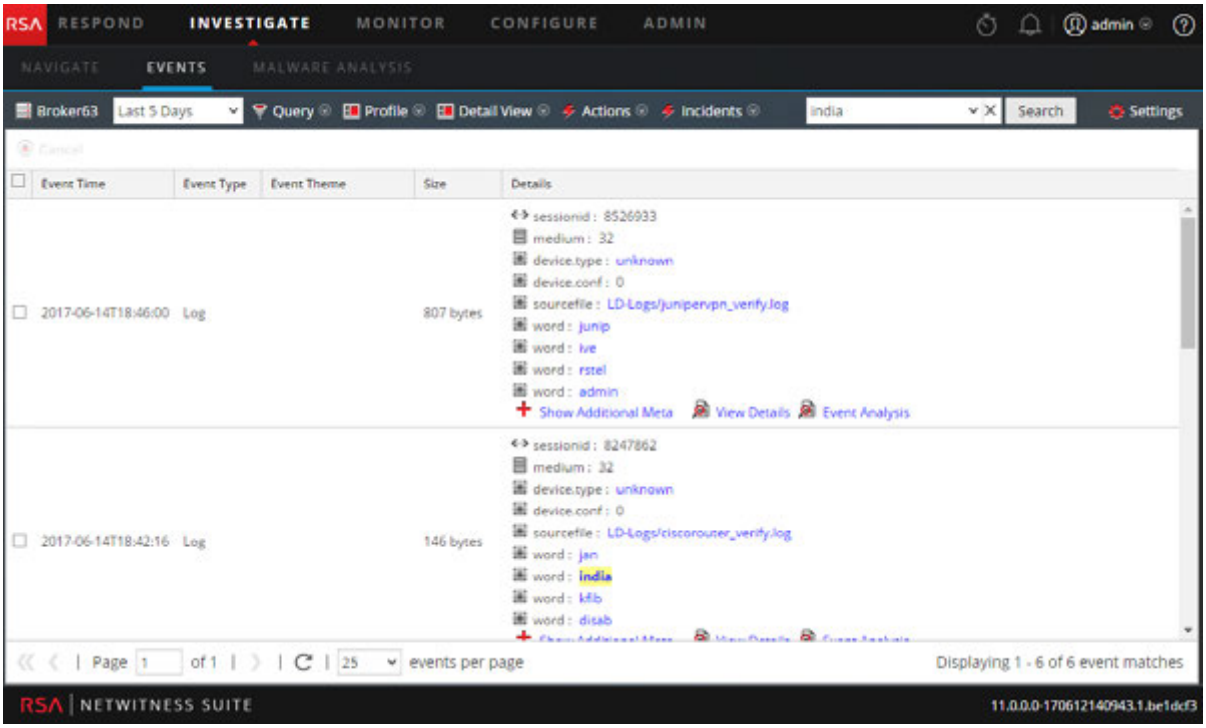
Search for Events in the Events View

You can search the currently displayed data in the Events view by entering a search string in the Search field. The search string can be a regex (Regular Expression) or it can be a simple text search. provides detailed information on these search types.

To search within the currently displayed data in the Events view:

1. To execute the search, place the cursor in the Search box, type a search string, and press **Enter** or click **Search**.
The search results are displayed in the Events view. Events that match the search criteria are displayed in the Event view grid. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column. Below is an example of the search results for the search term **India** in the Events Detail view. Note that search matches are not highlighted in

any Event Reconstruction.



2. If you want to narrow the search, change the query and time as described above in Filter Events Displayed in the Events View.
3. If you want to stop the search and return to the Events view, click **Cancel**.
   Any results that are displayed remain.
4. To clear the search box and return to the normal Events view, click **X** in the search box.

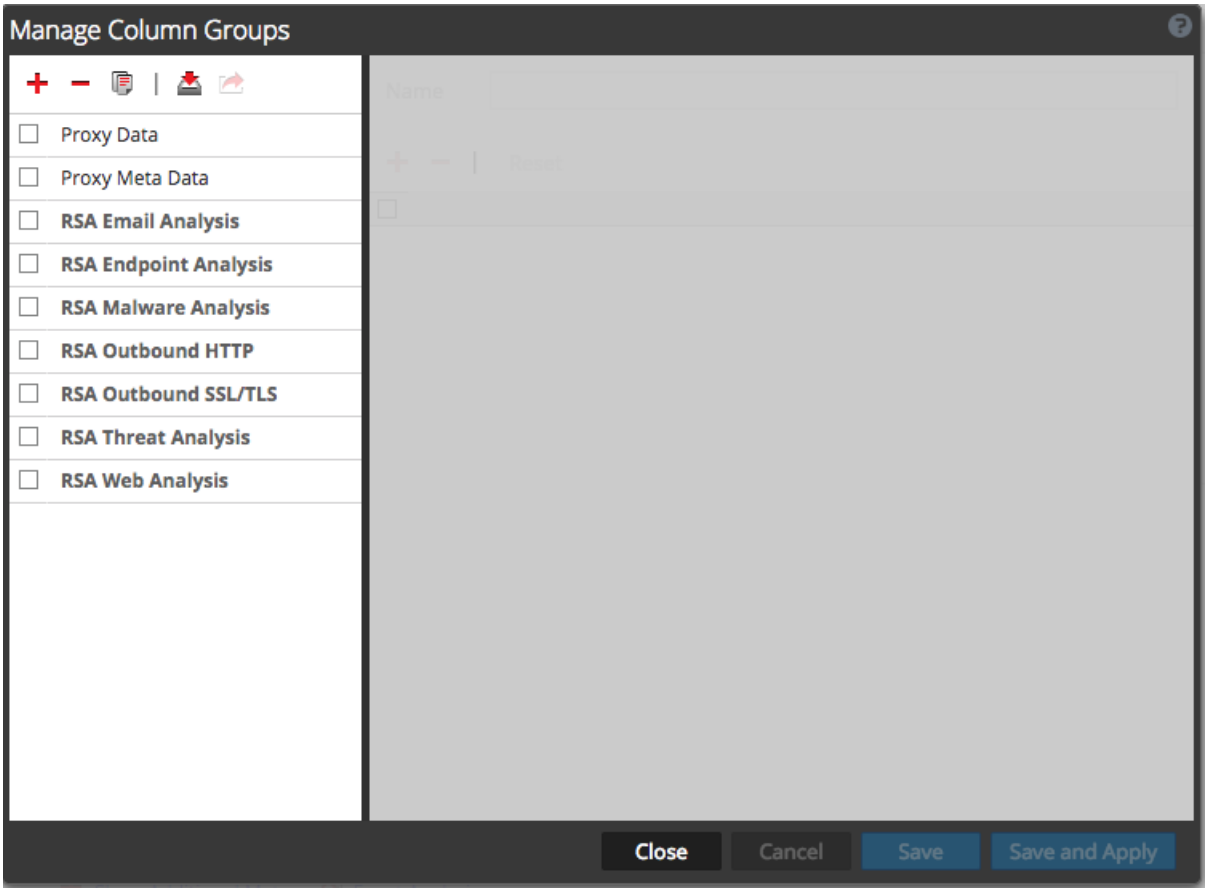
Manage Column Groups in the Events View

When viewing a list of events in Events view, you can customize the way data is displayed by defining the meta key to display in a column, the position of the column in the grid, and the default width of the column.

Note: In Version 11.1 and later, wherever meta keys are used, you can also use configured meta entities.
Investigate profiles can include custom column groups. If a custom column group is used in a profile and you are viewing events in the Events view using a custom column group, you cannot change the view type (Detail, List, or Log).

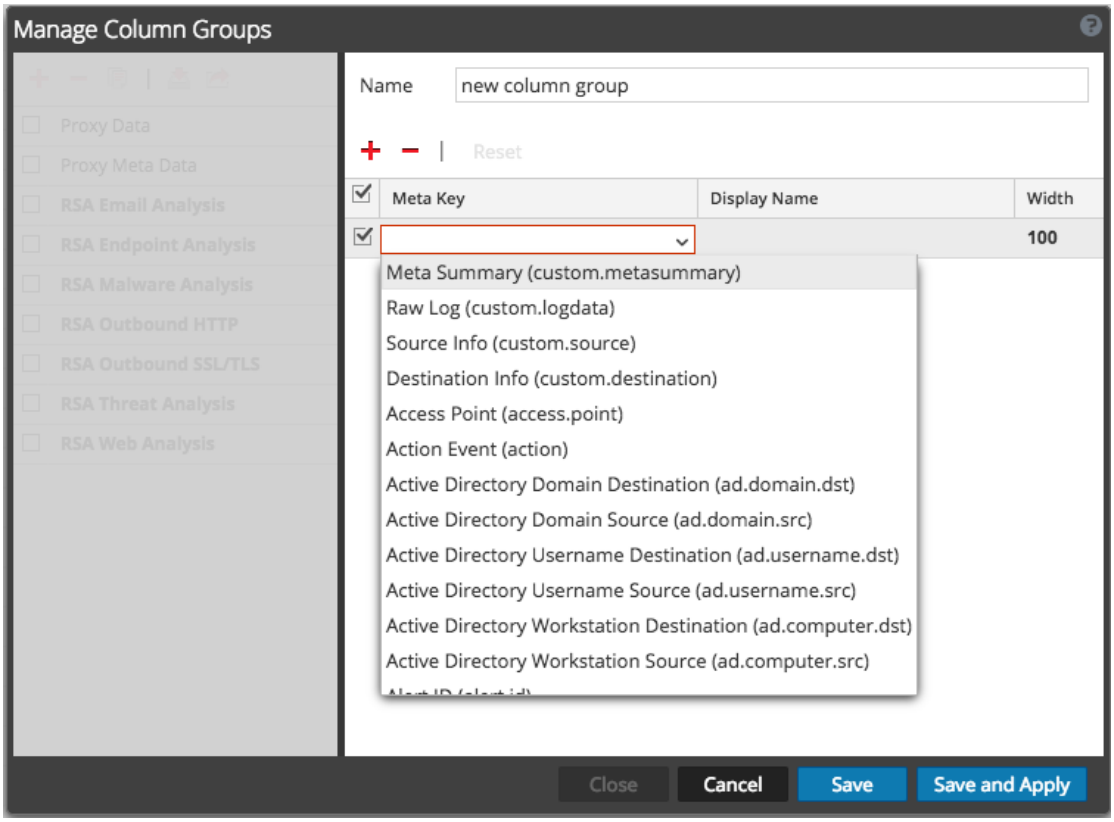
Create Custom Column Group

1. Go to **NAVIGATE > Events**.
2. Select **Manage Column Groups** in the **View** drop-down menu. The View option is named for the current value, for example, Detail View, List View, Log View, or the currently selected column group.
   The Manage Column Groups dialog is displayed.



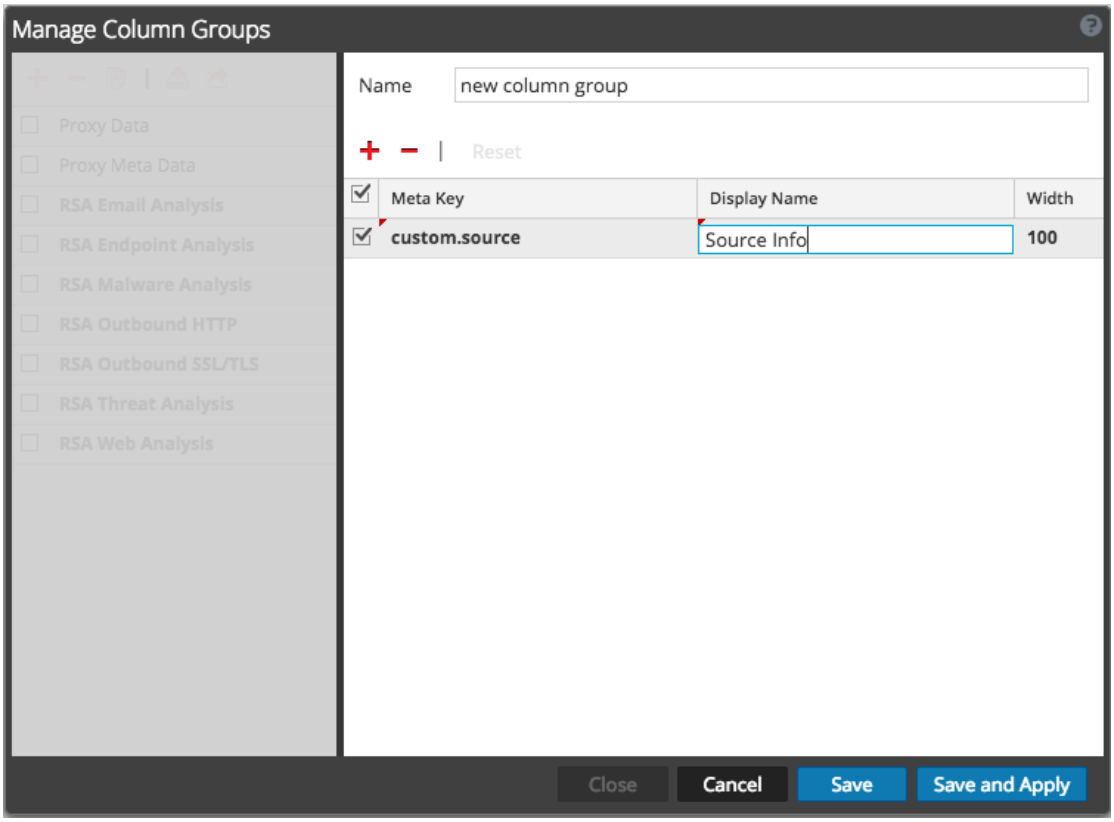
3. To add a new column group in the column group panel, click + and type the name of the new group in the resulting field.
   The column definition panel opens on the right with the group name filled in. You can edit the group name.
4. To add a column to the group, click +, and click in the empty **Meta Key** field to display the **Meta Key** drop-down list. Select a meta key field from the list, and repeat this step until the

column set is complete.



5. (Optional) To delete a meta key from the column group, click −.
6. (Optional) To rearrange the sequence in which the columns appear in the Events list, drag meta keys to the desired position.

7. (Optional) To set the default width for a column, click in the corresponding value in the **Width** column, and type a new column width.

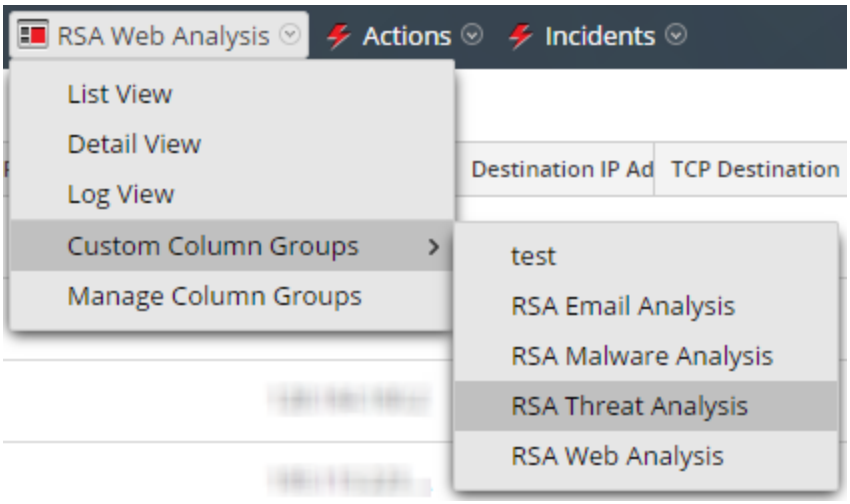


8. (Optional) To revert to the previous settings for the column group, and undo all of your changes, click **Reset**.
9. When ready to save, do one of the following:
   a. To save the edited column group and refresh the Events view with the column group settings, click **Save and Apply**.
   b. To save the edited column group without refreshing the Events view, click **Save**.

Select a Column Group

To select a column group:

1. With the Events view open, select **Custom Column Groups** in the **View** drop-down menu. The option name is the default value (Detail View or the current value).



2. Select one of the column groups from the submenu.
   The Events view is refreshed to reflect the custom column group.

Export Events in the Events View

In the Events view, the Actions menu has an option to export events from the event being viewed to an archive.

Note: You can only export files that you have permission to view or access.

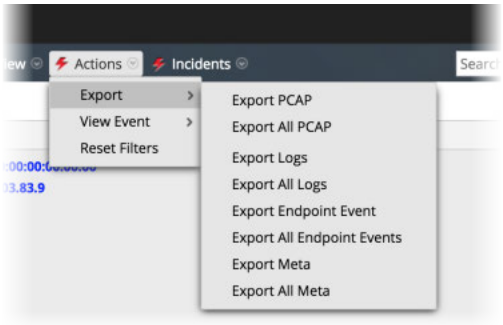
The export function queries the service for all sessions inside the selected time range and drill point to extract the content of each session. The details being exported are affected by both the time range and drill point at the time of exporting. In the File Extraction dialog, you can choose to export:

- PCAPs
- Logs
- NetWitness Endpoint event
- Meta values

The format of the exported archive: ZIP or GZIP file. After you send the request, a job is scheduled and you can track the job in in the Jobs tray. If there is an error retrieving the log or PCAP from the service, NetWitness Suite displays an error notification.

To extract files from an event:

1. While in the **Event view**, click an event.
2. Click **Actions > Export.**.



3. Select the export option.

   A message informs you that the PCAP is being downloaded.

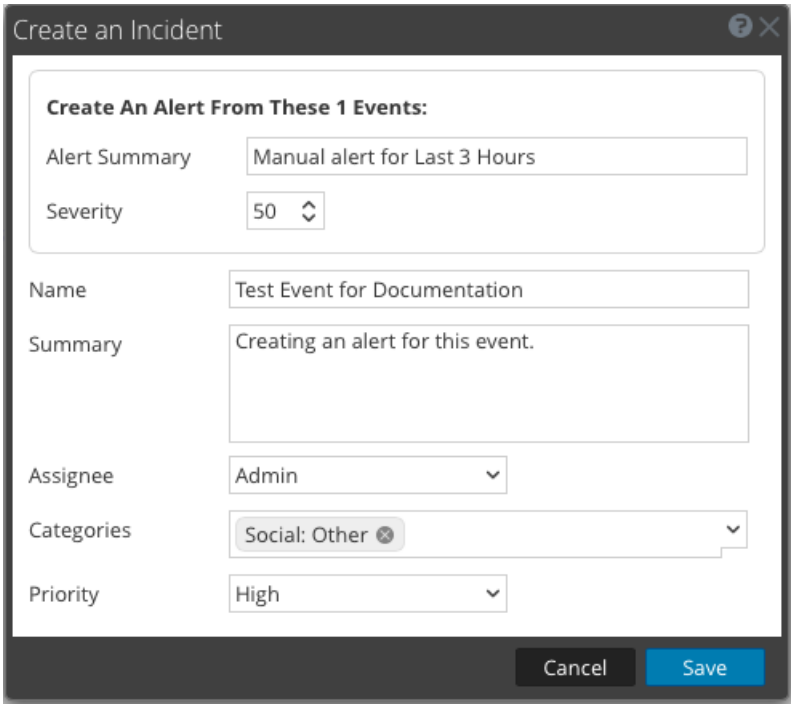
Add Events to an Incident for Response

When conducting an investigation in the Events view , you can select one or more events and create an incident that is available for incident responders in Respond. You can also add events to an existing incident in Respond to which you have access.

Note: An administrator must configure the required roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

1. Go to **INVESTIGATE > Events**.
2. In the Events view, select one or more events, and then **Incidents > Create New Incident**.

3. Complete the information in the Create an Incident dialog.



   a. Select the severity, an integer between 1 and 100, with 100 being the most severe.

   b. Type a name for the incident and describe the incident in the **Summary** field.

   c. Select an assignee for the incident from the drop-down list. This list includes the built-in roles that have access to Respond as well as any custom roles that have been added to

your system. For example, this list might include roles for admin, analyst, dpo, operator and roles for incident responsers.

d. From the **Categories** drop-down list, select one of more categories of alerts that apply to this incident.

e. From the **Priorities** drop-down list, select a category for the incident. For example, an incident may be critical, high, medium, or low priority.

f. Click **Save**.
The new incident is created and is available immediately in the incident queues for the selected role in Respond.

4. To add one or more events to an incident, select one or more events, and then **Incidents > Add to Existing Incident**.

5. In the Add Events to an Incident dialog, select the severity, and select one or more incidents to which the events will be added. You can Search for an existing incident by Incident-ID or Incident Name. When ready, click **Add to Incident**.
The events are added to the selected incidents and updated in Respond.

Combine Events from Split Sessions

Analysts can identify sessions that have been split due to session size in the Events view, and combine the fragmented sessions so that the complete session is viewable as a single query result in the Events view. When split sessions are recombined, a single packet export of the session in the Events view includes all of the session fragments.

Version 10.4 and earlier Decoders are configured with a default session size of 32 MB. When a session exceeds the 32 MB limit, the Decoder splits the session and all subsequent packets become part of a new session, fragmenting the actual network session across multiple Decoder sessions. Split sessions are parsed without the context that it is a fragment of the larger network session, sometimes resulting in session fragments with source and destination addresses and ports reversed and with unidentified application protocols. Another result of split sessions can be difficulty viewing all of the session fragments as a single query result or creating a single packet export of all the session fragments.

Decoder enhancements in NetWitness Suite 10.5 provide improved processing of fragmented sessions:

- Contextual fragment parsing.
- Session fragments highlighting.
- Finding session fragments.
- Exporting all packets to a single PCAP.

Contextual Fragment Parsing

In NetWitness Suite 10.5 and later, the Decoder completes session parsing before splitting the session based on the configured maximum session size (32 MB) or the configured timeout (60 seconds). When parsing is complete, the parsed results include the proper address directionality and application protocol, which are propagated to each subsequent session fragment to ensure consistency with the logical network session they represent.

Note: All of the necessary Decoder configuration changes are made when upgrading to 10.5. However, Find Session Fragments requires that the tcp and udp source port meta keys (tcp.srcport and udp.srcport) be fully indexed, which was not the default configuration prior to 10.5. This functionally limits the ability to find session fragments to sessions captured after the Decoder was upgraded to 10.5.

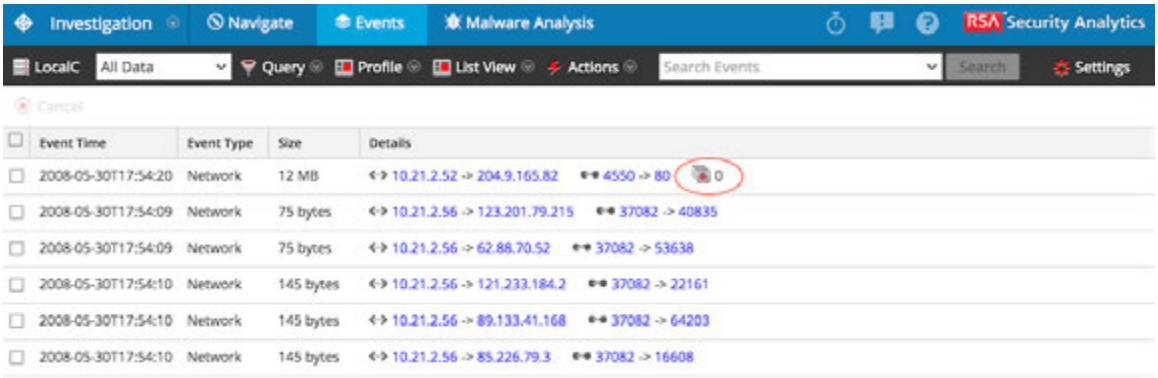
Session Fragments Highlighting

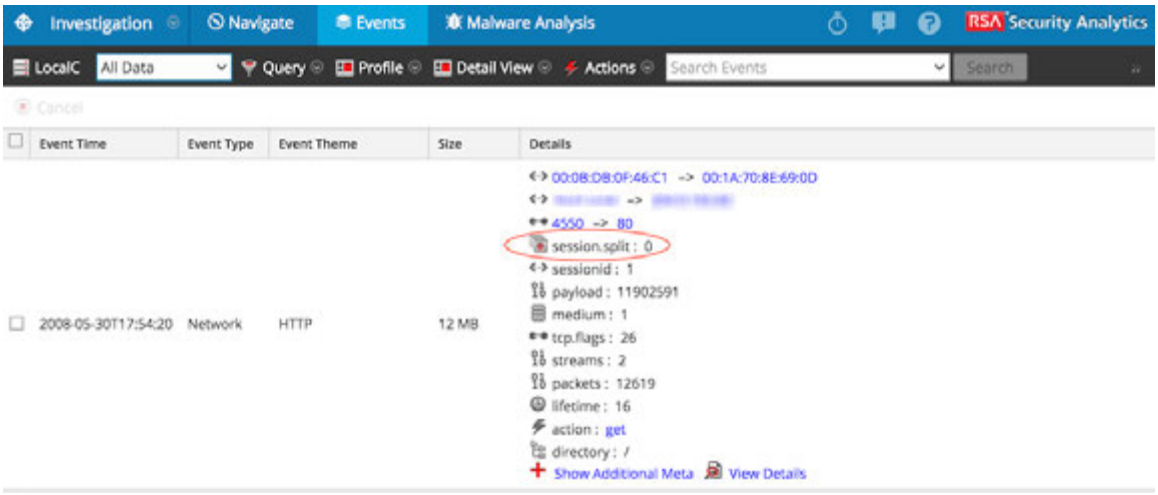
Each session fragment has an additional meta, `session.split`. The value of the `session.split` meta for a particular session fragment indicates how many fragments precede that fragment. When viewing sessions in the Events view, the `session.split` meta clearly identifies sessions that are fragments in the Events List view and the Events Detail view.

The session split happens when the configured Decoder `assembler.size.max` or `assembler.timeout.session` (latency between sessions) is reached. The earliest fragment is session 0 and sessions with a later time stamp are incrementally numbered 1, 2, 3, and so on. The `session.split` meta indicates the number of preceding sessions fragments; however, it does not always indicate that there are subsequent session fragments, even with a value of 0. It is also possible for the first fragment of the session to not have `session.split` meta if the session is parsed before exceeding the maximum session size.

Once you view the session fragments, you can determine the maximum session size or session timeout necessary for parsing to combine the split sessions into one again. For example, if you have four fragments at 32 MB, you need to configure your test Decoder (usually a virtual machine set up separate from main production service) with a maximum session size greater than 128 MB. The steps are the same to find all fragments based on a session timeout. The figures below show the Events List view and the Events Detail view with fragmented session information highlighted.

Note: A maximum session size of 12 MB was configured at the time the screen captures below were created.





The `session.split` metadata is always displayed immediately following the address and port metadata in the details view. It is never hidden as additional metadata. These enhancements make it possible to quickly:

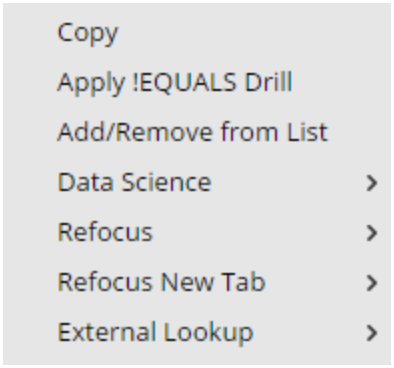
- Identify sessions that are fragments of a network sessions.
- View all of the session fragments of a network session given a single session fragment.
- Export the packets for the entire network session as a single PCAP file.

Find and Combine Fragments

From within the Events view, you can find fragments of a session using the Refocus > Find Session Fragments context menu option. NetWitness Suite composes a query using the source and destination addresses and ports of the selected session and displays all sessions that match that query within the current time window.

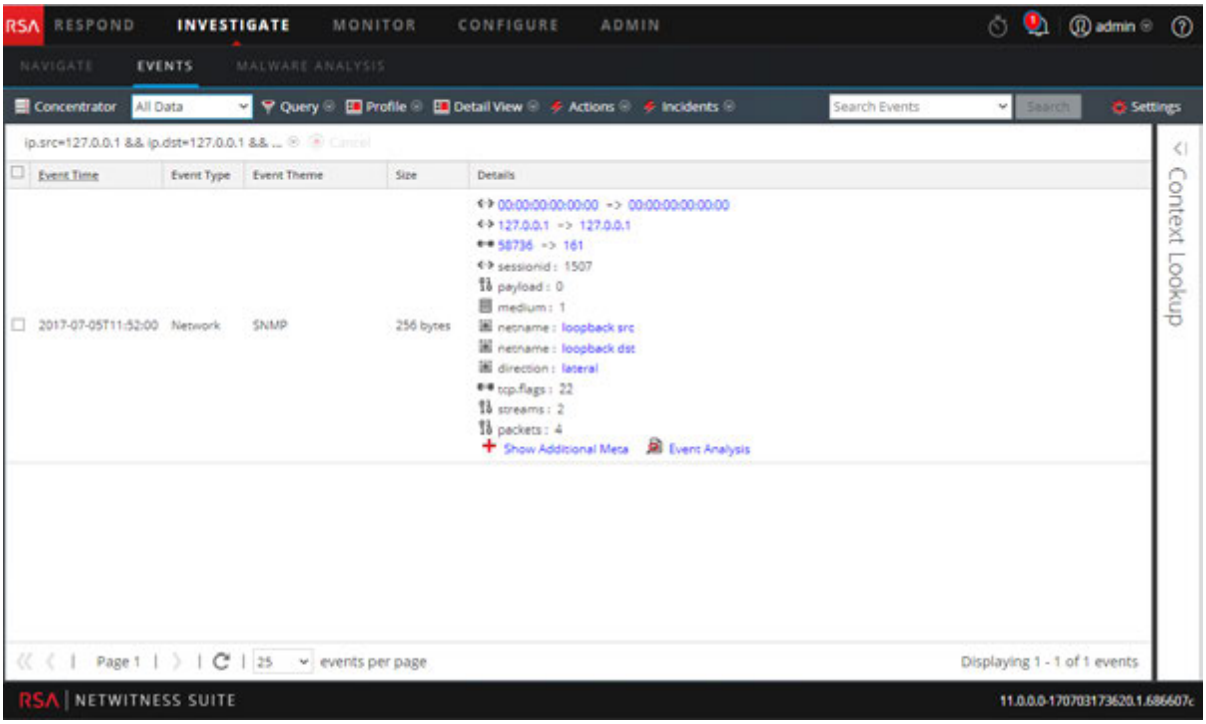
To find session fragments:

1. In the **Events** view, right-click any of the source and destination address and port values: `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport`, and `udp.dstport`) as well as `session.split` values.
   The context menu is displayed.



2. Select **Refocus > Find Session Fragments** or **Refocus New Tab > Find Session Fragments**.

   NetWitness Suite repopulates the Events list with session fragments for a single session within the current time range. Depending on the option you selected, the refocus replaces the current view or opens in a new tab. (All data is used in these examples but is not recommended on production systems).



3. If necessary, adjust the time range to include any session fragments that may precede or follow the current time window. You can tell that the time range needs to be expanded if the fragments occur near the time boundary, especially if the first visible fragment does not have a split value of 0 (or none). Alternately, inspecting the packets of the last visible session may lead you to believe that the session continues. Here is an example:

   a. If you are looking at fragments that are obviously not the first fragment, for example, 1, 2, 3, and 4 in time range 10:30 to 10:35, there should be a fragment 0. You can increase the time range to start earlier (for this example, 10:25) to find the additional fragment.

   b. If the session size of last fragment is close to maximum session size (12 MB in this example), look for additional fragments by increasing the time window to include a later time (for this example, 10:40).

      When all of the session fragments of a network session are included within a single Events list, the list can span multiple pages.

4. (Optional) To export the packets for every session fragment to a single PCAP file, select **Actions > Export All PCAP**.
   A message informs you that the PCAP is being downloaded. When download is complete, PCAP file includes the entire network session that was fragmented.

Querying and Acting on Data in the Navigate and Events Views

This topic describes methods of querying data and acting on results that are common to the Navigate view and the Events view. Analysts can:

- Search for Text Patterns
- Create a Custom Query
- View and Modify Queries Using URL Integration
- Use Profiles to Encapsulate Custom Views
- Manage Context Hub Lists and List Values in Investigate
- View Additional Context for a Data Point
- Reconstruct an Event

Create a Custom Query

In the Investigate > Navigate view or the Events view, you can create a query rather than clicking through the meta keys and values to drill down into the meta data. The dialogs for creating a query offer syntax help with drop-down lists of applicable meta keys and operators. When viewing the drop-down list, you can expand and collapse each meta group to view or hide the individual meta keys in that group.

Note: In Version 11.1 and later, you can query meta entities as well as meta keys.

When you select a meta group, NetWitness Suite generates the complex query equal to a query with all of the meta keys in that group ORed together. So if a meta group contains `ip.src` and `ip.dst`, the query generated is `ip.src = <value> OR ip.dst = <value>`. If the meta group contains meta keys that have different meta value types, the value input is disabled and the query uses `exists` statements. For example, a meta group that contains `ip.src`, `ip.dst`, and `alias.host` includes meta keys that have different value types; `ip.src` and `ip.dst` are ip addresses and `alias.host` is text. The generated query is `ip.src exists OR ip.dst exists OR alias.host exists`.

A basic query is in the following form:

```
<metakey> <operator> [<metavalue>]
```

These are a few examples:

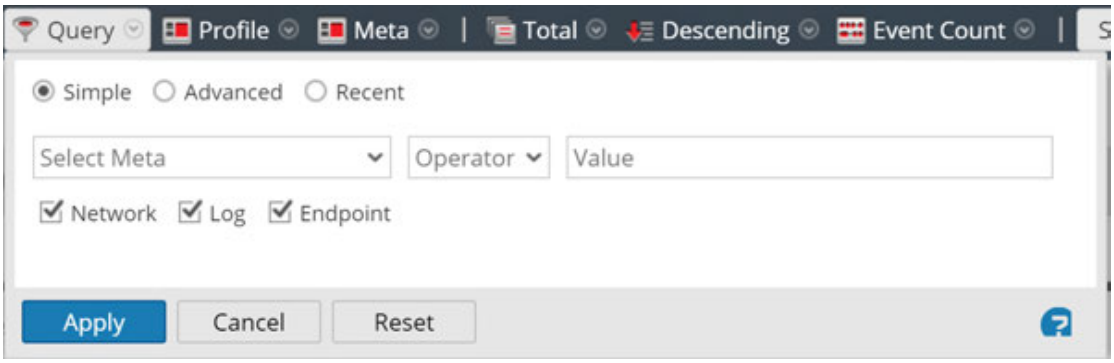
```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Create a Query Using the Basic Method

When you create a query using the basic method, NetWitness Suite provides drop-down lists of meta and operators.

1. In the **Navigate view** or the Events view toolbar, select **Query.**

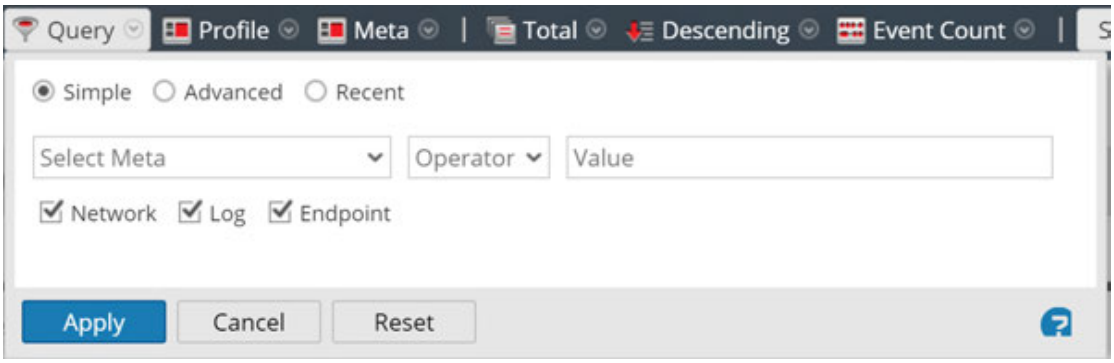
   The Query dialog is displayed, with the Simple option selected.



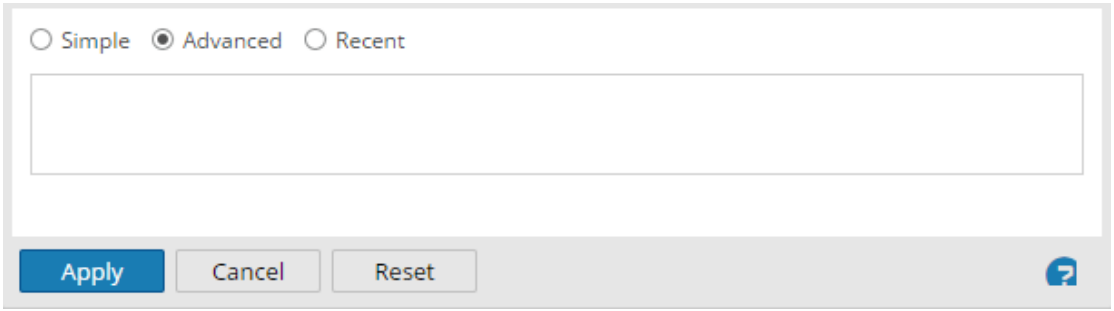
2. In the **Select Meta** field, click to display the drop-down list. The drop-down list has two sections: Meta Groups and All Meta.
3. Select a single meta key under **All Meta** or select a meta group under **Meta Groups**. You can also type in a meta key or meta group in the field.
4. In the **Operator** field, type an operator or click on the drop-down list to select a valid operator.
5. (Optional) If you selected an operator that requires a value, for example, begins, in the third field type the value for the meta key.
6. In the Network, Log, and Endpoint checkboxes, choose the type of data to query. Do one of the following:
   a. To limit the query to packets select **Network** and de-select **Log** and **Endpoint**.
   b. To limit the query to logs, select **Log** and de-select **Network** and **Endpoint**.
   c. To limit the query to endpoint events, select **Endpoint** and de-select **Network** and **Log**.
   d. To apply the query to packets, logs, and endpoints, select **Network**, **Log**, and **Endpoint**.
7. Do one of the following:
   a. Click **Apply**.
      The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   b. Click **Cancel**.
      The window is closed and no changes are made to the view or current query.

Create a Query Using the Advanced Method

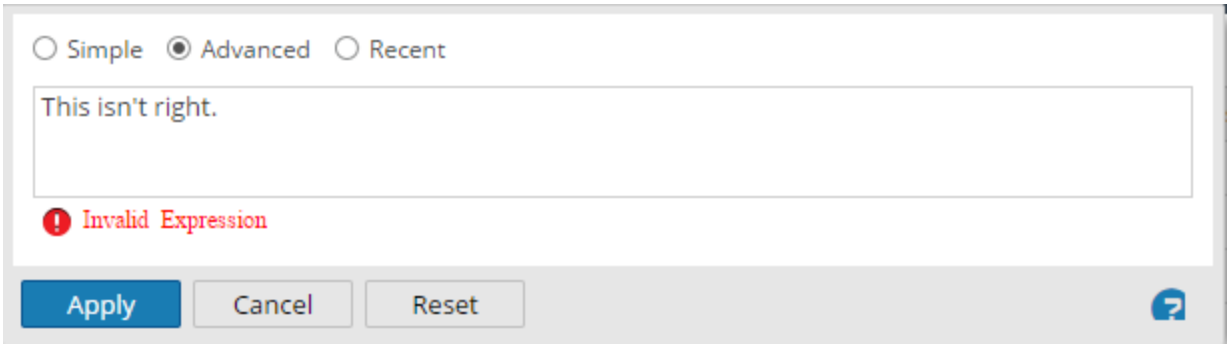
1. In the **Navigate view** or the Events view toolbar, select **Query.**
   The Query dialog is displayed.



2. Select **Advanced**.
   The advanced query field is displayed.



3. In the field, create a query, which can include the meta key, operator, and value. When you begin typing a meta key in the field a drop-down list of available meta keys for the selected service is displayed.
4. Select the meta key for your query.
   The display is updated. If the expression is not yet complete, the status indicates that the query is invalid.
5. Continue with an operator, from the drop-down list, then a value if necessary. The display is updated as you continue to enter the query. If you enter an operator, such as **exists** or **!exists**, which does not use the value field, the value field is disabled and the invalid status is cleared. If you enter an operator, such as =, which requires the value field, the invalid status remains until you enter a value. When the query is valid the invalid status is no longer displayed.



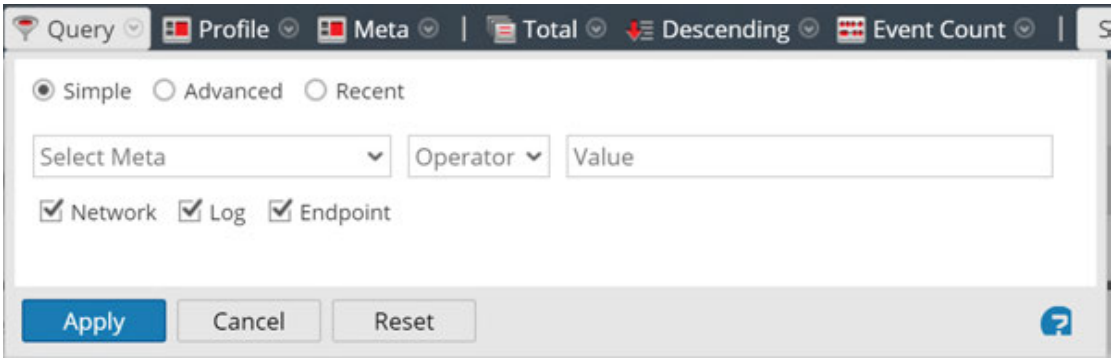
6. Do one of the following:

   - Click **Apply**.
     The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   - Click **Cancel**.
     The window is closed and no changes are made to the view or current query.

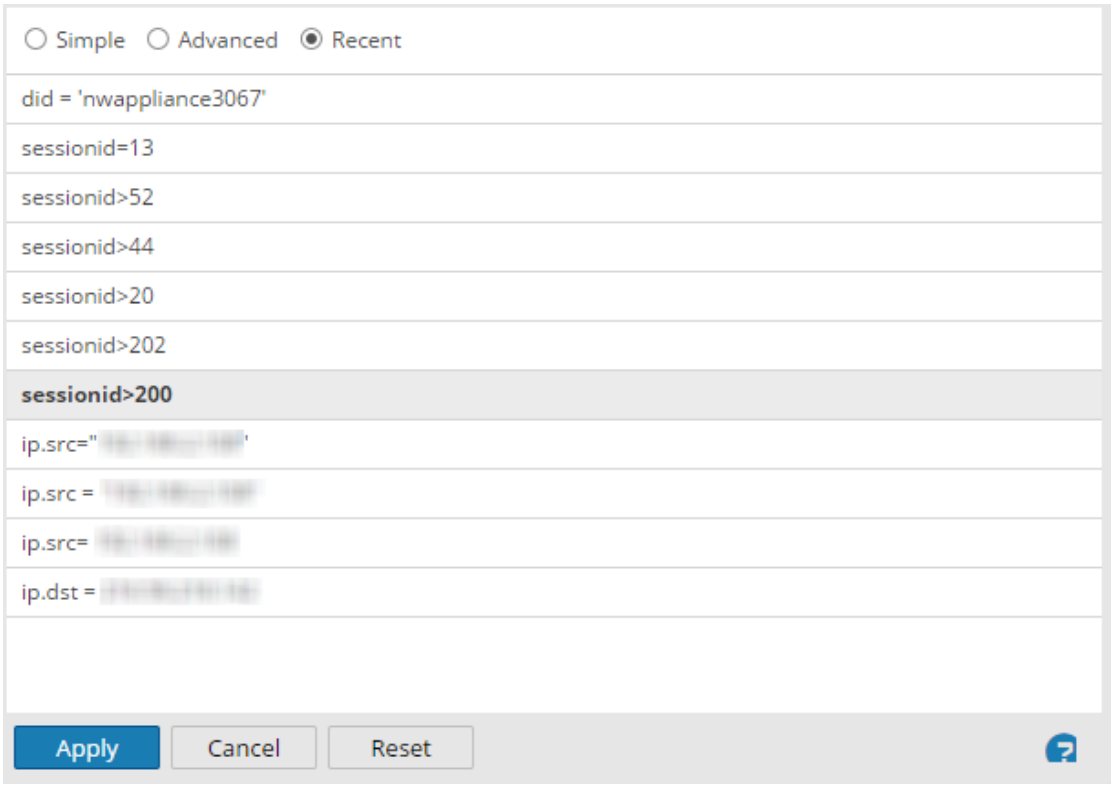
Apply a Recent Query

You can view recent queries and select one to apply to the current service being investigated. To select a recent query:

1. In the **Navigate view** or the Events view toolbar, select **Query.**
   The Query dialog is displayed, with the Simple option selected.



2. Select the **Recent** option.
   The list of recent queries is displayed in the bottom portion of the dialog.



3. In the list of recent queries, click to select a query.
4. Do one of the following:
   - Double-click a query.
   - Select a query and click **Apply**.
     The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   - Click **Cancel**.
     The window is closed and no changes are made to the view or current query.

Manage Context Hub Lists and List Values in Investigate

Analysts can add lists and list values for Context Hub enrichment in the Navigate view and the Events view. When the Context Hub service is enabled and configured, NetWitness Suite provides enrichment data from Incident Management, custom lists, and NetWitness Endpoint directly in the Navigate view and Events view. A visual cue highlights meta values for which enrichment data is available in the Investigate views, and you can click on the highlighted value to look up the contextual information and intelligence.

In addition, from the Values panel in the Navigate view and from the Events view, you can view lists, edit meta values in an existing list, or create a new list. When you add meta values to a list, you can investigate the meta values using the context lookup option.

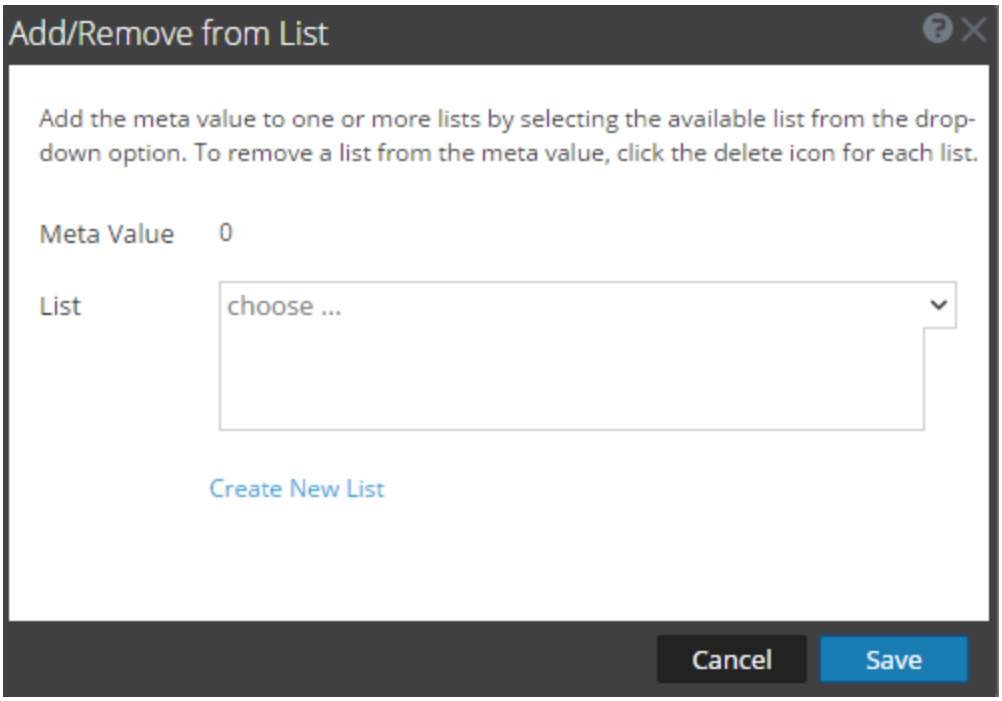
For an analyst to manage lists in Investigate, the administrator must:

- Enable the Context Hub service.
- Assign an analyst role with permission `Manage List from Investigation` to the user who will perform Context Lookup from Investigation views.
- Configure appropriate roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Add Meta Values to an Existing List

To add meta value to an existing list in Context Hub:

1. While investigating a service in the **Navigate** view or the **Events** view, right-click a meta value (for example, values under Source IP, Destination IP, or Username) and select **Add/Remove from List** in the context menu.
   The Add/Remove from List dialog is displayed.



2. In the **List** field, select one or more lists from the drop-down option to which the meta value must be added.
3. Click **Save**.
   The meta value is added to the selected lists.

Remove a Meta Value from a Context Hub List

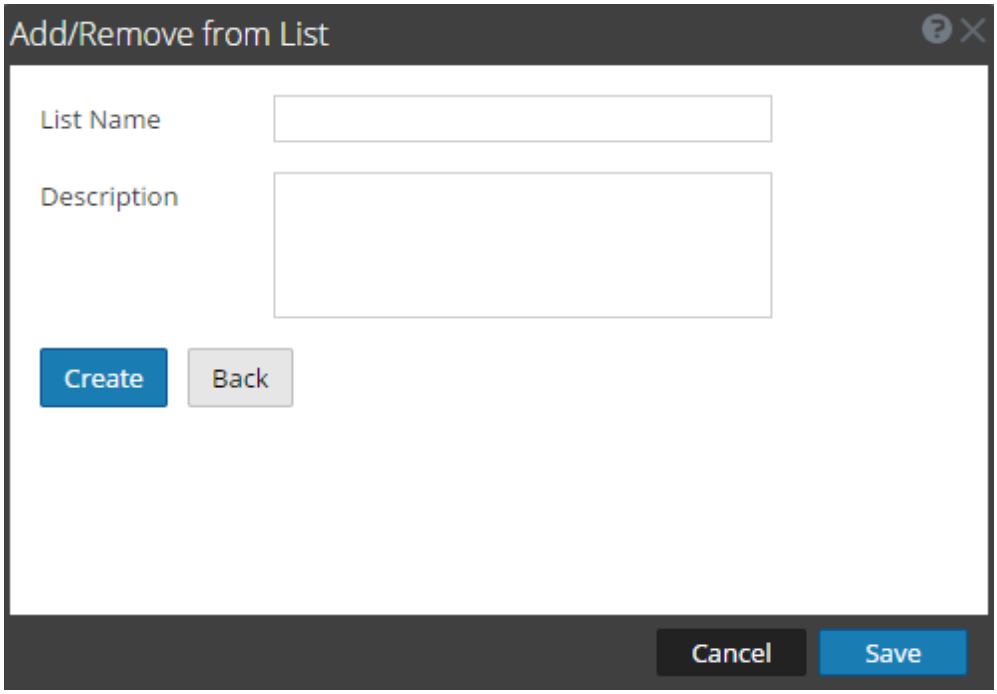
To remove a meta value from list:

1. In the **Add/Remove from List** dialog, in the **List** field, view the lists which include the meta value.
2. Click the delete icon (x) for each list that should not include the meta value.
3. Click **Save**.
   The meta value is removed from the deleted list.

Create a New List

To create a Context Hub list in Investigate:

1. In the **Add/Remove from List** dialog, click **Create New List**.



2. In the **List Name** field, enter an unique name for the list.
3. In the **Description** field, enter the description of the list.
4. Click **Create** to create the list.
5. Click **Save** to add the meta value to the created list.
   These lists are considered as data sources for retrieving context information.

View Additional Context for a Data Point

From the Events view or the Navigate view, you can look up details and intelligence about elements associated with an event in the Context Hub. The data from configured sources, such as RSA NetWitness Endpoint, can help you understand what is happening.

These elements, or entities, are identifiers, such as an IP address, a user name, a host name, a domain name, a file name or file hash. To look up external information about a given entity, NetWitness Suite uses the Context Hub. The Context Hub is a centralized service that aggregates data about entities from multiple configurable data sources. This data can extend your investigation with additional context beyond the immediate results of a specific query. For example, the Context Hub can tell you if a given entity has been mentioned in any incidents, alerts, feeds, or community intelligence publications.

When you right-click the entity in Investigate, the Context Hub queries the configured data sources for relevant information. The Context Lookup panel opens from the right side of the browser window. The Context Lookup panel is populated with the information from the Context Hub as it becomes available.

To perform another lookup, right-click on another entity, and the Context Lookup panel is updated with that entity's information.

To close the Context Lookup panel, click ■ in the panel.

In the Context Lookup panel, you can view and explore individual data sources for further investigation. For example, when you click on a particular Incident's value, the specific incident details are displayed in the Respond view.

For a detailed description of the information displayed for each data source on the Context Lookup panel, see Context Lookup Panel.

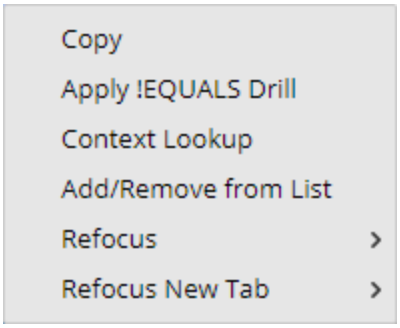
Before an analyst can view contextual information, the administrator must:

- Ensure that the Analyst has a role with the permission `Context Lookup` as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.
- Add the Context Hub service in RSA NetWitness Suite.
- Configure data sources for the Context Hub service as described in the *Context Hub Configuration Guide*.

Note: Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

To view information in the Context Summary panel:

1. In the Navigate view or the Events view, identify a meta value for which you want to view additional context and hover over the meta value.
   The **Context Highlights** panel is displayed with a quick summary of the type of context data is available for the data source: NetWitness Endpoint, Incidents, Alerts, Hosts, Files, Feeds, and Live Connect.
2. Right-click a meta value , and click **Context Lookup** in the drop-down menu to open the Context Lookup panel.



   The Context Summary panel opens from the right side of the browser window. The Context Summary panel is populated with the information from the Context Hub as it becomes available.
3. To perform actions from the Context panel, click an entity such as IP address and right-click. The following options are available: Open Link in New tab, Query in Investigate, Copy Link, Paste, Google Lookup, Virus Total Lookup, and Query in Endpoint.

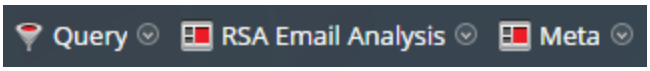
Use Profiles to Encapsulate Custom Views

Using profiles is a quick and easy way to customize which data is displayed in the Navigate view and the Events view. In the Manage Profiles dialog, you can use a profile to specify which meta groups and column groups are displayed by default, to append queries to an investigation, and to import or export profiles.

Note: Profiles are shared across users in the same NetWitness Suite network. If one user modifies or deletes a profile it has an affect on what is available to the other users.

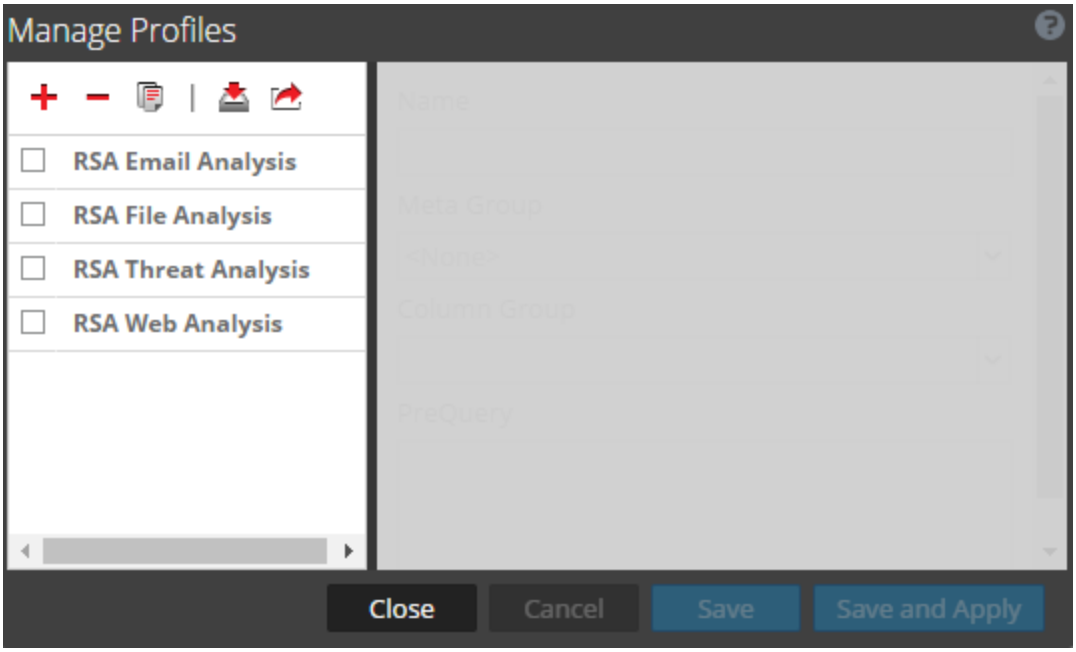
If you have multiple profiles, you can switch between them to quickly change to the selected profile's preferences. If a profile is currently active, the title of the Profile menu is replaced with the profile name.

The following figure illustrates this in the Navigate view. The profile name is displayed between Query and Meta. In the Events view, the profile name is displayed between Query and View.



Navigate to the Manage Profiles Dialog

1. Go to **INVESTIGATE > Navigate** or INVESTIGATE > **Events**.
2. If the **Investigate** dialog is displayed, select a service and click **Navigate**.
3. In the toolbar, select **Profile > Manage Profiles**.
   The Manage Profiles dialog is displayed.



Create and Edit Profiles

1. In the **Manage Profiles** dialog, either select an existing profile by clicking the checkbox beside the name, or click + to create a new profile.

   The right panel is available.

2. Edit or enter the profile name by typing in the **Name** field. The name must be between 2 and 80 characters.

3. Select a meta group from the **Meta Group** drop-down list. You can add custom meta groups as described in Manage Meta Groups.

4. Select a column group for the **Column Group** drop-down list. You can add custom column groups as described in Manage Column Groups in the Events View.

5. Type queries to filter results in the **PreQuery** field. PreQuery follows the same syntax as the Query builder. The PreQuery in the figure uses a meta group called **crypto exists**.

6. Click **Save** to save the profile without using it, or click **Save and Apply** to save the profile and use it immediately.

   If you click **Save and Apply**, a confirmation dialog is displayed before setting the selected profile as active.

Change Active Profile

If you do not see enough results or the right results in the Navigate or Events views, you may have a profile active. If you do not want to use any profiles, you can click **Deactivate Profiles** in the **Profiles** drop-down menu.

To use a different profile:

1. In the **Navigate** or **Events** view toolbar, open the **Profiles** drop-down menu.

2. Hover over the **Profile** option to display a drop-down list of available profiles.

3. Select the profile you want to use.

   The profile settings are applied immediately.

If you want to change the active profile from the Manage Profile dialog:

1. In the **Navigate** or **Events** view toolbar, select **Profiles > Manage Profiles**.

   The Manage Profiles dialog is displayed.

2. Select a profile from the left panel and click **Save and Apply**.

   A confirmation dialog is displayed.

3. Click **Yes**.

   The profile settings are applied immediately.

Import Profiles

You can upload or import .jsn files that have been downloaded from another service.

1. In the **Manage Profiles** dialog, click in the left panel toolbar.
   The Profile Import dialog is displayed.
2. Click **Browse** or the **Upload File** field to select a file from your computer.
3. When the file is selected, click **Upload**.
   The profile is displayed in the left panel.

Download Profiles

Profiles are downloaded as .jsn files.

1. In the **Manage Profiles** dialog, select one or more profiles from the left panel.
2. In the left panel toolbar, click .
   The download begins immediately.

Search for Text Patterns

You can search for text patterns withing the current set of events in both the Navigate view and the Events view. You can perform a keyword text search or do regex (Regular Expression) matching. In the Navigate view, you can click a meta value, such as HTTP, to drill into the data and then enter a search string in the Search field to search for events within that subset of data. The search opens a tab in the Events view, brings your drill and time range forward, and shows your search results. You can also drill into the data using queries before starting a search. To execute the search, enter a search string in the Search box, and press **Enter** or click **Search**.

Keyword Text Search

The text search provides these capabilities:

- Each white space delimited word is ANDed, so that every word must be found, but the order or location position in relation to the other words is irrelevant. For example, if you search on `Mark Albert`, both Mark and Albert must be found in the session, but they need not be together or in any specific order.
- The word OR is special. If you search `Mark OR Albert`, either Mark or Albert must be found in the session to match; both are not required.
- You can mix or match implicit ANDs and ORs together in the search string. The explicit OR has higher precedence than the implicit (whitespace) AND. The following examples make the same logical statement, which requires that both the terms cheese and dumplings be present in a match and one of toaster bread:

  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```

- You can exclude words from search results using the - operator. For example, searching for `cheese -toast` would return any result that has the word cheese, unless the word toast is also present.
- The keyword search can match metadata stored in the following patterns:
  - **IPv4 and IPv6 addresses**. Any term that can be recognized as an IP address will be converted to the native metadata format so that it can be found in indexed metadata.
  - **IPv4 CIDR ranges**. You can use CIDR notation to locate IPv4 addresses within a range.
  - **Timestamps**. Timestamps are matched against the native time meta, and any additional time meta fields stored with the Time type.

- **Numbers**. The search function will attempt to automatically identify decimal search terms and match them against numeric meta data fields.

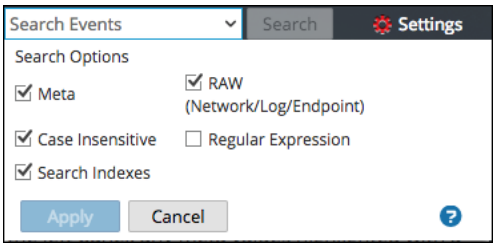
Options Controlling Search Behavior

To access the Search box and search options in the Navigate or Events views:

1. You can see the Search Events field in the toolbar.

   Troubleshooting: If you cannot see the Search Events field in the toolbar, click on the right side of the toolbar.

2. Click in the Search field to view the Search Options drop-down menu.

The options selected in this box change how the search is executed. The default search mode is to use the search indexes for text keywords within meta and raw.

Note: Because the Search Indexes checkbox is selected by default, the search returns results based on data that is indexed. If you want to search for a complete set of metadata or raw data, select those checkboxes and clear the Search Indexes checkbox. The search will take longer, but it will contain a more complete set of data.

The following table describes the Investigation search options.

Feature	Description
Search Indexes	Searches the indexes first, before scanning the meta data or any raw data. Searching the index is the fastest way to locate keywords within a large data set. The index search utilizes any relevant indexes present within your data collection. **Caution:** - The index search only returns results on indexed data. - Substring matches will not be located by index searches. If you require substring matches, clear this checkbox and use a non-index search mode.

Feature	Description
Meta	Searches the metadata. Your keyword or regex pattern will be matched against any parsed meta data.
RAW (Network/Log/Endpoint)	Searches the log or event text. Every event is decoded and content is searched for matches on the keyword or regex pattern. If you select all data with no filters on an Archiver, execution time may be excessive and a warning may be displayed. **Caution:** Searching raw network sessions causes sessions to be decoded, which is very time intensive. You may want to disable raw searches when looking at network-only collections.
Case Insensitive	Ignores case when searching.
Regular Expression	Searches using a Perl regular expression, rather than text. By default executes a text search. To execute a regular expression search, select the Regular Expression option. **Caution:** - Regular expression searches can be very slow. - When combining regular expressions and index search options, the regular expression pattern is matched against unique index values instead of meta values. This produces results faster, but it is not an exhaustive search of all the meta data or raw data.
Apply	Sets the default search options to apply to a search in the Navigate and Events views. This also updates your Investigation preferences in your Profile (Profile > Preferences > Investigation tab). The preferences are saved and effective immediately. You can select search options to use for a particular search without changing your default search preferences.

Regular Expression Search Syntax

A regular expression search uses Perl regular expression syntax, which is documented in detail in http://perldoc.perl.org/perlre.html.

Raw Text Keyword Search

The Log Decoder has the capability to create a raw text index for unparsed log events. This functionality creates metadata items that form a full-text index on downstream services such as Concentrators and Archivers. When you enable the Search Indexes option in your search preferences, your search automatically utilizes the text index. Note that the text index produces meta items that have a coarse granularity. For example, the default text indexer configuration truncates text terms. By comparing the index matches against raw data, the search engine will find accurate results for your search. However, you can improve search times by disabling the raw search checkbox. If you do so, results will be returned faster, but you may see false positive hits in your search results.

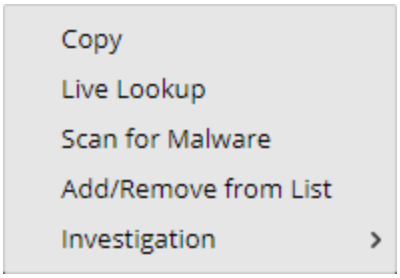
Search Examples

The following examples show searches from the Navigate and Events views.

Search in the Navigate View

To search within the currently displayed data in the Navigate view:

1. To drill into the data, click a meta value, such as HTTP, in the Navigate panel.



2. Type a search string in the Search field and press **Enter** or click **Search**.
3. To clear the search box and return to the normal Events view, click the **X** in the search box.

Search in the Events View

To search within the currently displayed data in the Events view:

1. Type a search string in the Search box, and press **Enter** or click **Search**.
   The search results are displayed in the Events view. Events that match the search criteria are displayed in the Event view grid. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column.
2. If you want to narrow the search, change the query and time.
3. If you want to stop the search and return to the Events view, click **Cancel**.

Any results that are displayed remain.

4. To clear the search box and return to the normal Events view, click **X** in the search box.

View and Modify Queries Using URL Integration

NetWitness Investigate includes an External URL Integration that facilitates integration with third-party products by allowing a search against the NetWitness Suite architecture. By using a query in a URI, you can pivot directly from any product that allows custom links, into a specific drill point in the Investigate view. This integration provides an internal presentation of the user's query.

URL Integration allows the user to identify the service either by the host id or by the service and port, as defined in NetWitness Suite. If NetWitness Suite is unable to resolve the service, the analyst is redirected to the Navigate view, showing the Service selection dialog. Once the service is selected, the Navigate view is loaded with the drill point, defined by the query.

Service Id Known

When the ID of the service to use for an investigation is known, the format for entering a URI using a URL-encoded query is:

http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>

where

- <sa host: port> is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- <deviceId> is the internal Service ID in the NetWitness Suite instance for the service to query against. The service ID can be represented only as an integer. You can see the relevant service ID from the URL when accessing the Investigation view within NetWitness Suite. This value changes based on the service being connected to for analysis.
- <encoded query> is the URL-encoded NetWitness Suite query. The length of query is limited by the HTML URL limitations.
- <start date> and <end date> define the date range for the query. The format is <yyyy-mm-dd>T<hh:mm:ss>Z. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported. All times are run as UTC.
  For example:
  http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z

Host and Port Known

When the host and port of the service to use for investigation is known, the format for entering a URI using a URL-encoded query is:

```
http://<sa host:port>/investigation/<device
host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

where

- `<sa host: port>` is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- `<device host:port>` is the host and port of a service defined in NetWitness Suite instance for the service to query against. NetWitness Suite attempts to resolve the host and port as a service ID defined in NetWitness Suite.
- `<encoded query>` is the URL-encoded NetWitness Suite query. The length of query is limited by the HTML URL limitations.
- `<start date> and <end date>` define the date range for the query. The format is `<yyyy-mm-dd>T<hh:mm:ss>Z`. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.
  For example:
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Examples

These are query examples where the NetWitness Server is 192.168.1.10 and the deviceID is identified as 2.

All activity on 03/12/2013 between 5:00 and 6:00 AM with a hostname registered

- Custom Pivot: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

All activity on 3/12/2013 between 5:00 and 5:10 PM with http traffic to and from IP address 10.10.10.3

- Custom Pivot: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Encoded Pivot Dissected:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Additional Notes

Some values may not need to be encoded as part of the query. For example, commonly the IP src and dst is used for this integration point. If leveraging a third-party application for integration of this feature, it is possible to reference those without encoding applied.

Reconstruct an Event

When viewing a list of events in Events view, you can safely create a reconstruction of the event in a readable form that matches the original. By default, the initial view of a reconstructed event is the most suitable format (Best Reconstruction); for example, web content is reconstructed as a web page; an IM conversation is displayed with both parts of the conversation. Each user can select a different default reconstruction in the Profile > Preferences view.

You can also open a reconstruction from the Navigate view if you know the Event ID of the event.

In the reconstruction, you can:

- Select event information to view. Possible values are: request data, response data, both request and response data.
- Select the reconstruction type: details, text, hex, packets, web, mail, or IM.
- Export raw logs.
- Export the event as a PCAP file.
- Extract any files available in the event.
- Extract all the meta data associated with the event.

  Caution: Be careful when clicking a link to a file in the Reconstruction. If your system has an application associated with the file, or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

- Display the event in a separate window or tab (depending on your browser configuration).
- If you are viewing the reconstruction as a preview in the current view, you can page forward to the next event and back to the previous using the navigation buttons in the bottom left corner.

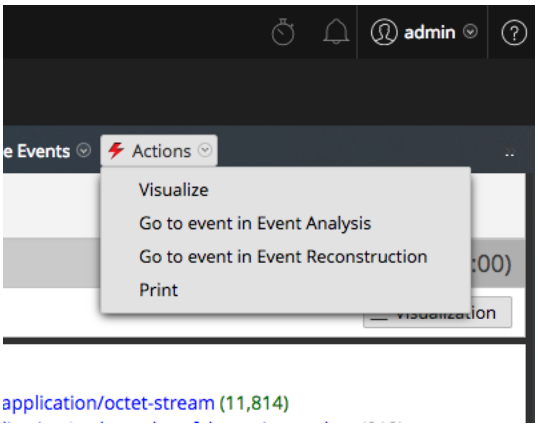
Note: Reconstruction Settings and Reconstruction Cache Settings allow an administrator to manage application performance for Investigation. As analysts reconstruct sessions that they are investigating, two situations can affect performance and results.
-Some events can be very large and contain many thousands of source packets. Reconstructing these types of sessions can degrade application performance.
- In some cases, the reconstruction cache can present incorrect content; for this reason, NetWitness Suite cleans cache that is older than a day every 24 hours. Between the daily cache cleanings, certain actions my result in stale cache being used for a reconstruction, and if the need arises, administrators can manually clear cache for one or more services that are connected to the current NetWitness Server.

Reconstruct an Event from the Navigate View

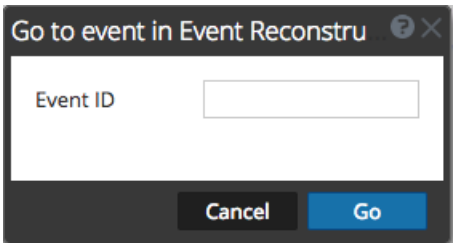
You can reconstruct an event directly from the Navigate view given a known Event ID. You can use this option without executing a query as you usually do when beginning an investigation. A service and time range must be selected to be able to jump directly to an event using just its `eventid`.

To view a reconstruction or event analysis directly from the Navigate view:

1. Go to **INVESTIGATE > Navigate** and select **Actions > Go to event in Event Analysis** or **Go to event in Event Reconstruction**.



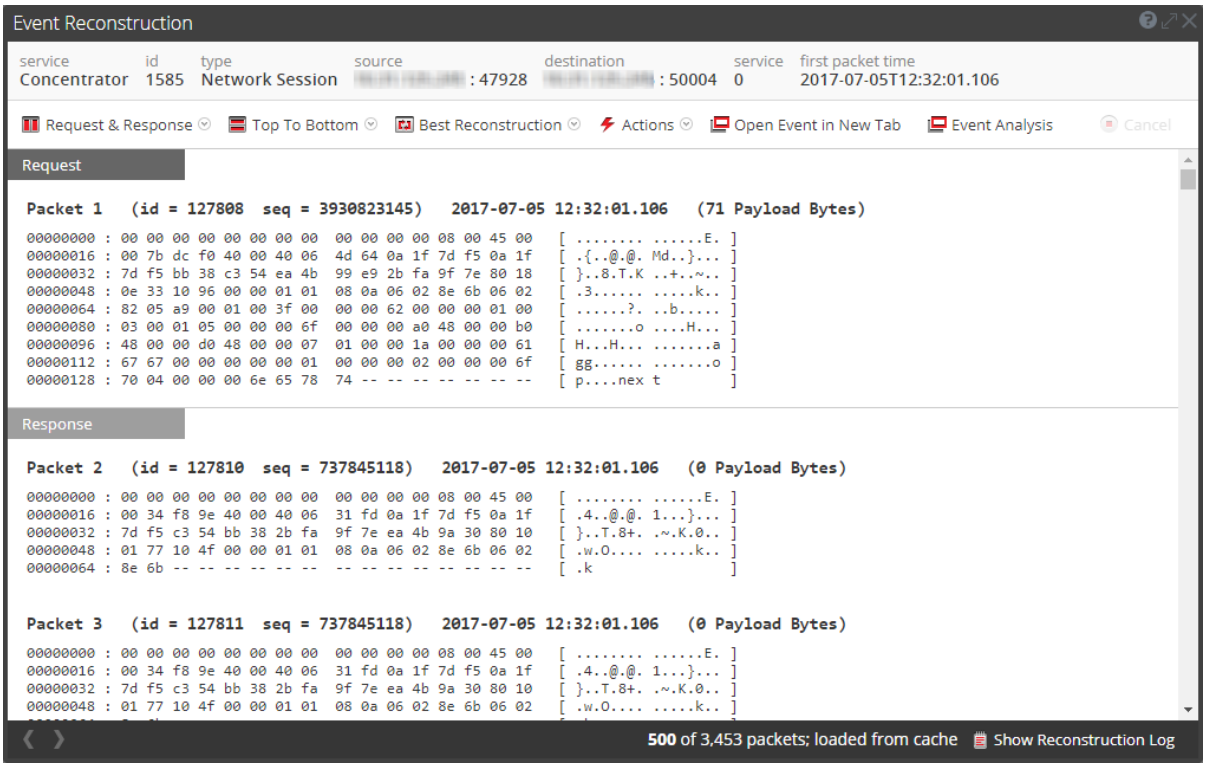
The Go to event dialog is displayed. There are two dialogs, one for Event Analysis and one for Event reconstruction. Both ask for the Event ID.



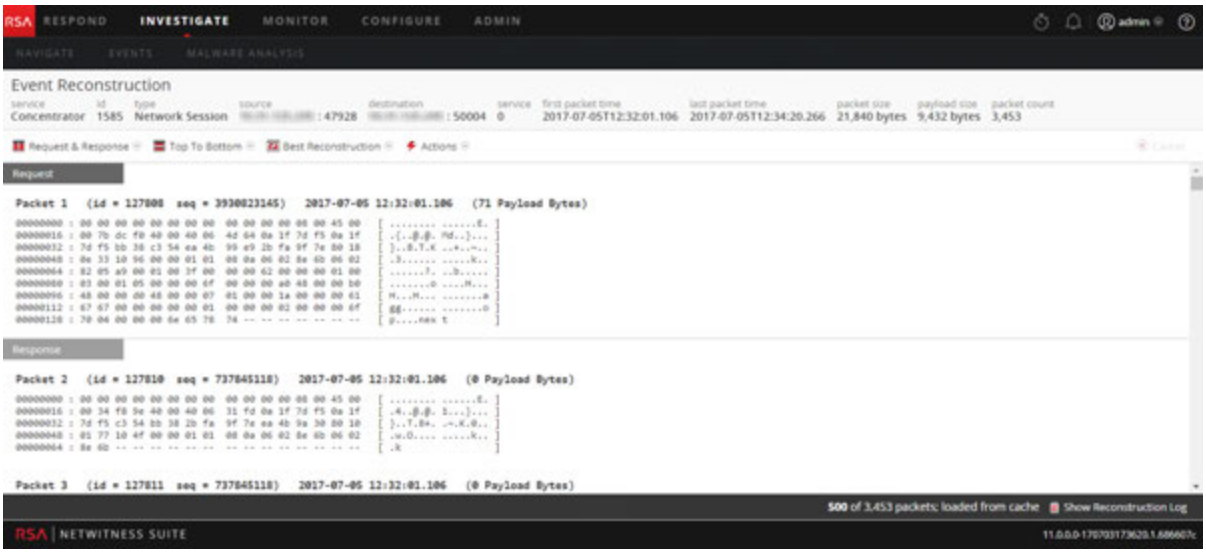
2. In the **Event ID** field, type the ID and click **Go**.
   The specified event is reconstructed in the Event Reconstruction view or the Event Analysis view.

Reconstruct an Event

1. Open a drill point in the **Events** view.
2. To show all meta data, click + Show Additional Meta .
3. To open an event reconstruction in the current view, select an event to reconstruct and select **Actions > View Event > Preview Inline**.
   The Event Reconstruction opens in a popup window in the same view. By default, NetWitness Suite displays the best reconstruction for the event determined by the event content or the reconstruction that you have selected in the Default Session View setting for Investigation. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view side-by-side results, export an event, open an email attachment, extract files, and open the event in a new tab. The toolbar options vary depending on the type of event being reconstructed (network event, log event, or endpoint event). This is an example of the reconstruction for a network event.



4. To preview a reconstruction of the next event, click or to preview a reconstruction of the previous event, click .
5. To open an event reconstruction in a new tab, do one of the following:
   a. In the **Events** view, select an event to reconstruct and select **Actions > View Event> Open in New Tab**.
   b. In the **Event Reconstruction** toolbar of previewed reconstruction, click **Open Event in New Tab** in the toolbar.
   The Event Reconstruction opens in a new tab.



View Side by Side or Top to Bottom

To select the way requests and responses for an event are displayed:

1. In the **Event Reconstruction** toolbar, click **Top to Bottom** or **Side by Side**.
2. In the drop-down menu, select the information you want to see in the event: **Side by Side** or **Top to Bottom.**
   The reconstruction is refreshed with the selected information.

Select Event Information to View

To select what event information to view:

1. In the **Event Reconstruction** toolbar, click **Request & Response**.
2. In the drop-down menu, select the information you want to see in the event: **Request & Response**, **Request**, or **Response**.
   The reconstruction is refreshed with the selected information.

Select Event Reconstruction Type

To select the reconstruction type for an event:

1. In the **Event Reconstruction** toolbar, click **Best Reconstruction**.
2. In the drop-down menu, select the reconstruction type to view: **meta**, **text**, **hex**, **packets**, **web**, **mail**, or **files**.
   The reconstruction is refreshed with the selected reconstruction type.

Open or Download an Email Attachment

When viewing a reconstruction of an email that has attachments, you can open supported file types or download the files to the local system.

Caution: Be careful when selecting file attachments. If your system has an application associated with the file attachments, or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

To open or download email attachments:

1. In the **Event Reconstruction** toolbar, select the **View** drop-down and select **View Mail**.
   The Event Reconstruction is displayed.
2. In the **Event Reconstruction** section of the email, click the Attachment.
   If the file type is supported by the browser, the attachment will open in a new tab.
   If the file type is not supported, the Download dialog is displayed so that you can download the attachment.

Export an Event as a PCAP File

The PCAP export option downloads the sessions for the current time range and drill point to a PCAP file. To export an event as a pcap file:

1. In the **Event Reconstruction** toolbar, click **Actions**.
2. Click **Export PCAP**.
3. A confirmation dialog is displayed.
4. Click **OK**.
   The job is scheduled and when complete the PCAP is downloaded to the local file system.
   In the Profile > Jobs tab, you can download the PCAP.

Extract Files from a Reconstructed Event

The Extract Files option extracts and downloads the files associated with the event. To extract files:

1. In the **Event Reconstruction** toolbar, click **Actions**.
2. Click **Extract Files**.
   The File Extraction dialog is displayed.
3. Select the types of files to extract, and click **OK**.
4. The job is scheduled and when complete the selected file types are downloaded to the local file system. In the Profile > Jobs tab, you can download the files.

Analyzing Raw Events and Metadata in the Event Analysis View

Analyzing raw events and data in the same view is possible when working in the Event Analysis view. After you understand Recontruction Types in the Event Analysis View, you can:

- Filter Results in the Event Analysis View
- Examine Events in the Event Analysis View
- Download Data in the Event Analysis View
- Act on Data in the Event Analysis View

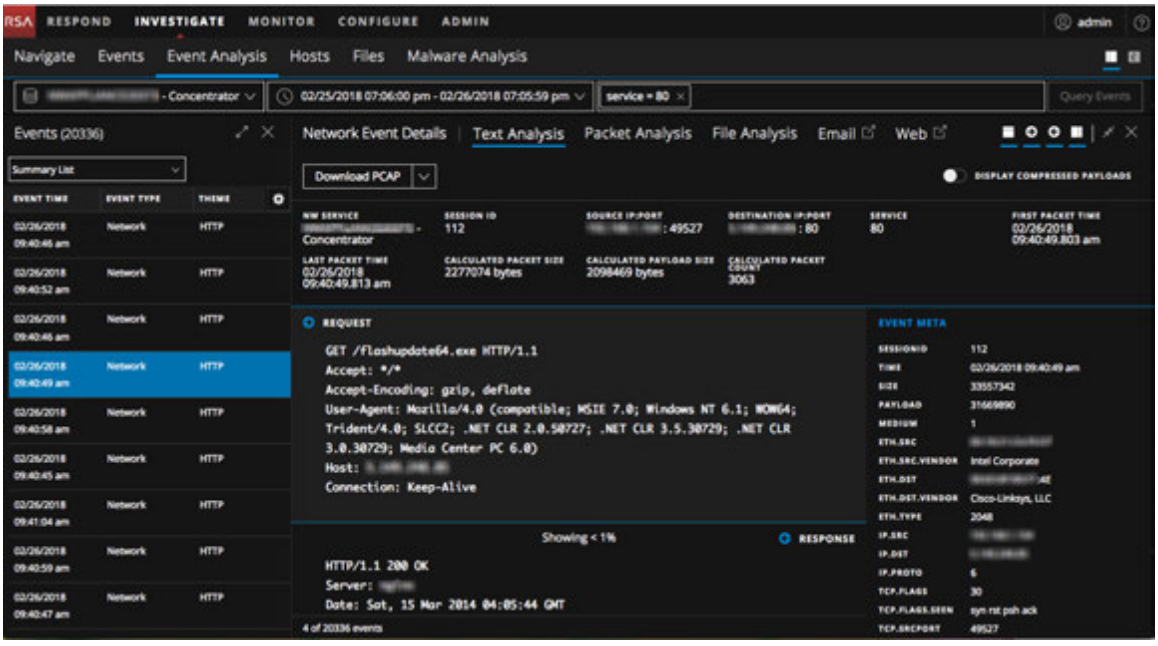
Recontruction Types in the Event Analysis View

When hunting for possible threats in captured network data, you can drill into different points of interest in the data. If a particular session contains suspicious events, you can examine the list of events for the session and you can also safely view a reconstruction of the event with features that help to identify patterns. (See Beginning an Investigation for the different methods to access the Event Analysis view.)

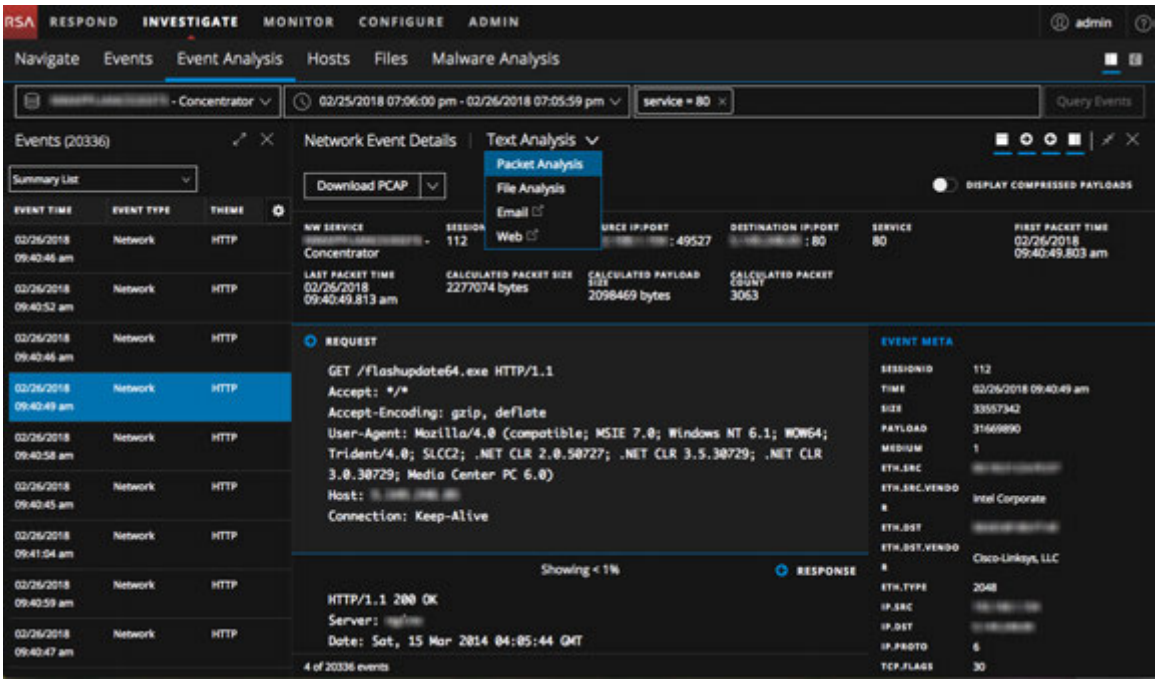
Note: If you are analyzing events on a 10.6.x or 11.0.0.x service from an 11.1 NetWitness Server, the download behavior in the Event Analysis view varies for files, PCAPs, logs, payloads, and meta values. You may see an event payload on a 10.6.x or 11.0.0.x service to which you do not have permission, but you will not be able to download files or payloads.

In the Event Analysis view, you can select the format for the reconstruction: Packet Analysis, File Analysis, or Text Analysis, **Email** (Version 11.1 and later), and **Web** (Version 11.1 and later). When the `medium` meta key tags an event as a log event or endpoint event , only the Text Analysis is available. The default reconstruction for network events is Text Analysis; however, for a network event the last reconstruction format that was open overrides the default. The Email and Web reconstructions open the event in the Events view and are described in

This figure is an example of the Network Event Details: Text Analysis panel in a web browser window that is wide enough to display the reconstruction format options in a row.



When the browser window is too narrow to display all the view options horizontally, the options are presented in a drop-down list.



Within each type of analysis, settings are available to enhance your analysis. If you change a setting, the setting is preserved between browser refreshes and logins within the same browser. These are the preserved settings:

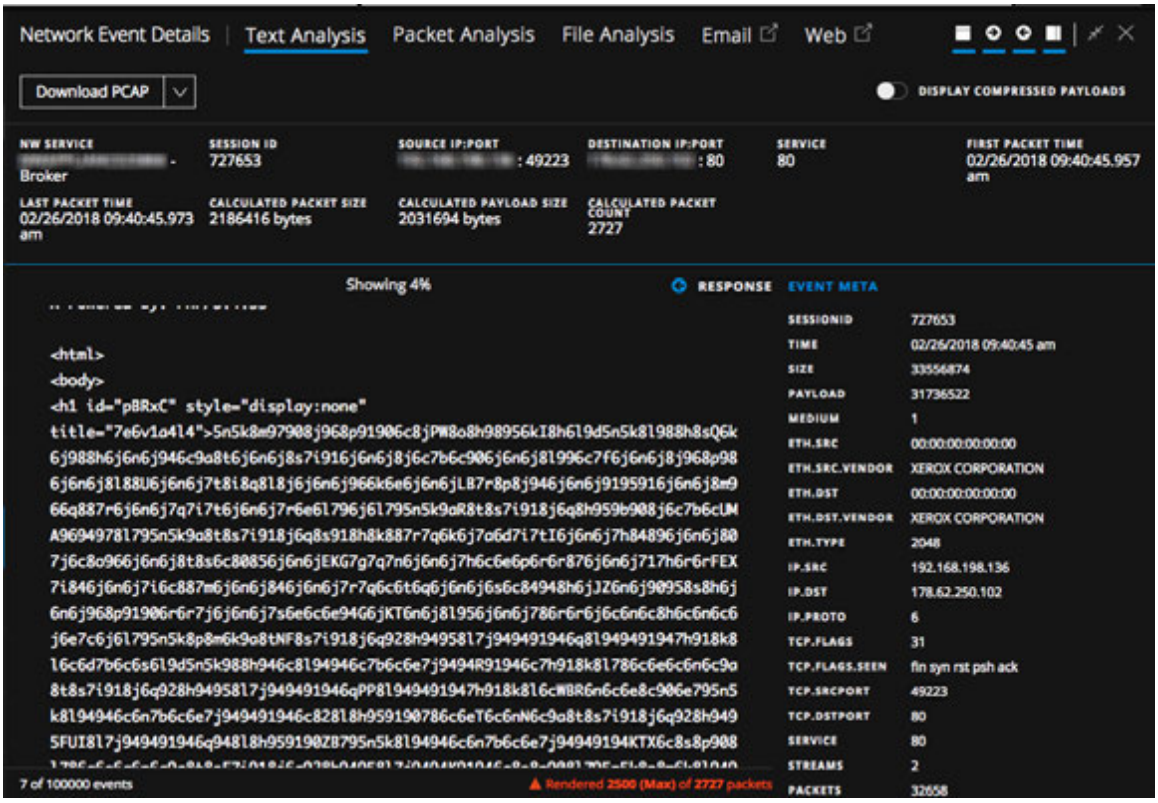
- The currently selected reconstruction: Text Analysis, Packet Analysis, or File Analysis.
- Whether the Event Meta panel is open or closed.
- Whether the Event header is open or closed.
- Whether the Request or Response, or both are displayed.
- Whether packet payloads are displayed in the Packet Analysis panel.
- Whether shaded bytes are displayed in the Packet Analysis panel.
- Whether other common file types are highlighted in the Packet Analysis panel.
- The number of packets per page in the Packet Analysis panel.
- Whether compressed or uncompressed text is displayed in the Text Analysis panel.
- The text decode setting in the Text Analysis panel of a network event.

The Text Analysis Panel

You can view all types of events (network events, log events, and endpoint events) in their original text format in the Text Analysis panel.

Note: Endpoint events are available for investigation in Version 11.1 and later.

The Text Analysis panel for some network events can be quite large. To ensure the best rendering, the number of packets that can be rendered in a single event is limited to 2500. If the Text Analysis panel is not showing all packets, the footer indicates that the limit of 2500 packets has been reached; no additional packets will be rendered for this event. This figure illustrates a reconstruction that has 2727 packets with only 2500 packets rendered; no more packets will be rendered for this reconstruction.



Note: Some network events have a large number of packets but very small payload. In this case, if the entire payload is contained within the first 2500 packets this meets the definition of showing all packets. No message indicating that you are not viewing all of the packets is displayed.

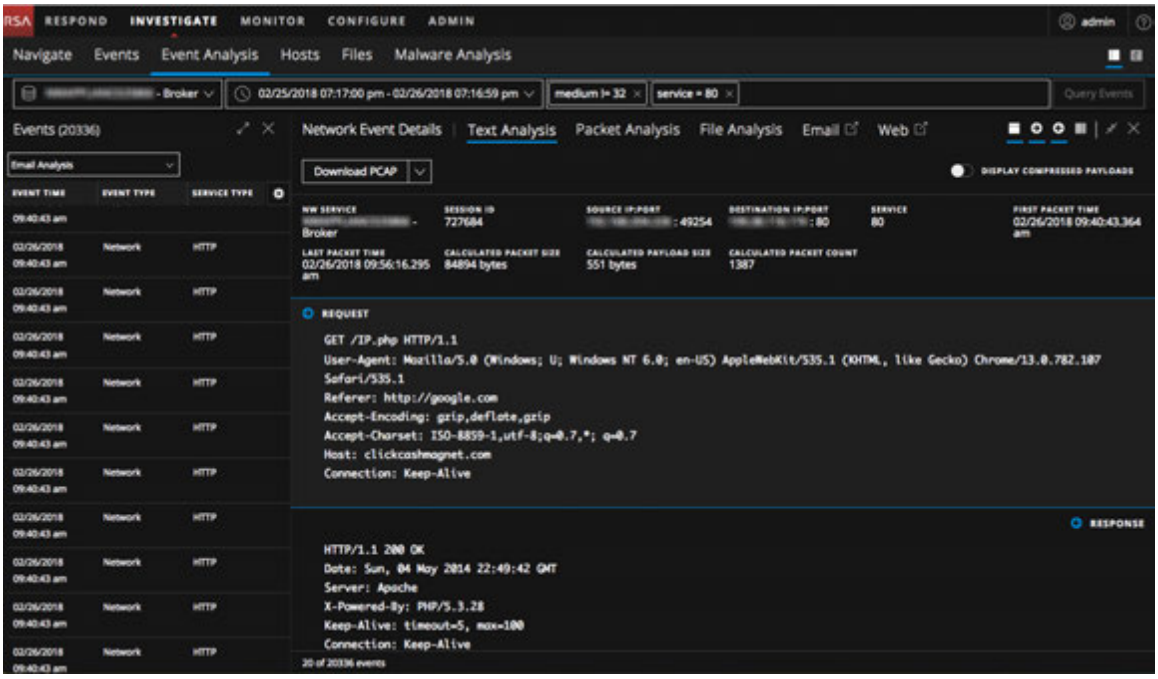
In the Text Analysis panel, network events, log events, and endpoint events are presented differently.

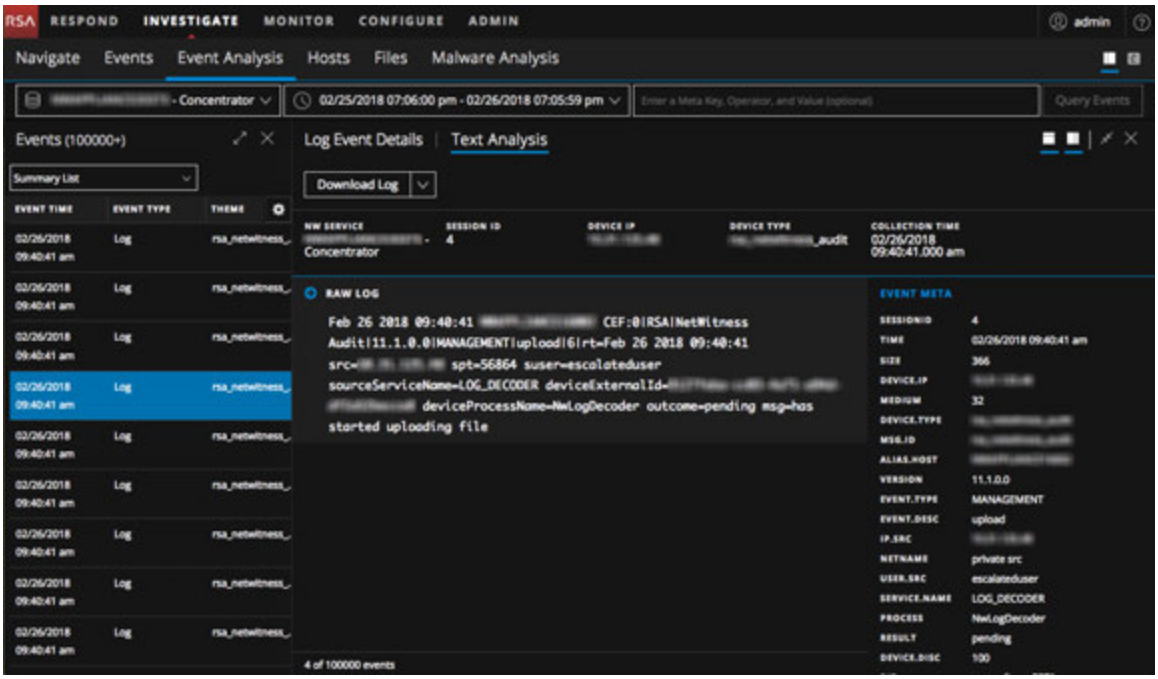
- For network events, Investigate provides the direction of the packet (Request or Response) and contents of each packet in text format. If you are reconstructing a network event, the Text Analysis panel is scrollable. When you scroll, the text identification information as well as the Request and Response labels remain visible rather than scrolling out of view.
- Log events and endpoint events have no request or response; only the raw event is displayed in the Text Analysis panel.

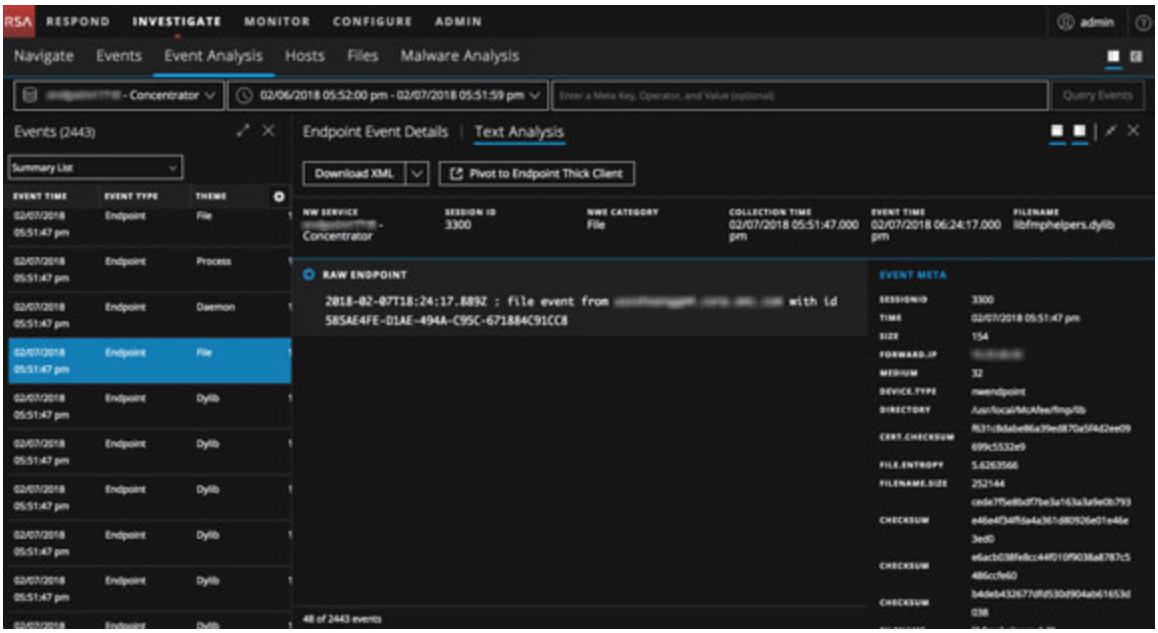
For each type of event (network, log, or endpoint), there are several differences:

- The Event header includes information relevant to each type of event.
- There are different options for exporting.

Below is an example of the Text Analysis panel for each type of event, a network event, a log event, and an endpoint event.



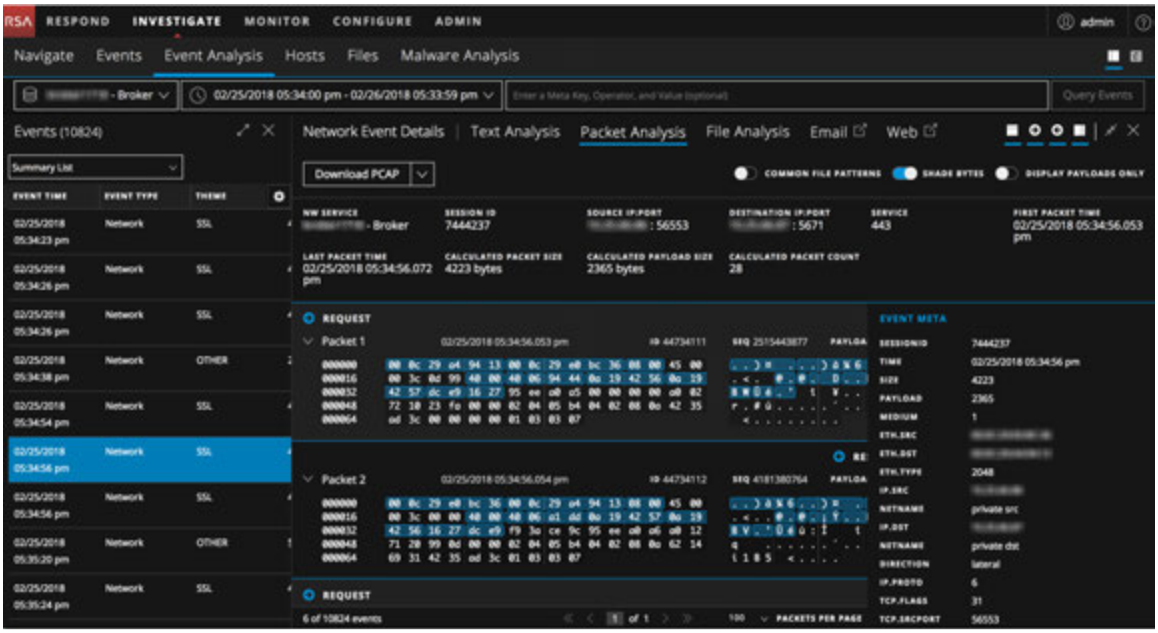




Note: The calculated packet count, calculated packet size, and calculated payload size in the Event header may be different than the same statistics in the Event Meta panel because the metadata is sometimes written before event parsing completes and may include packet duplicates.

The Packet Analysis Panel

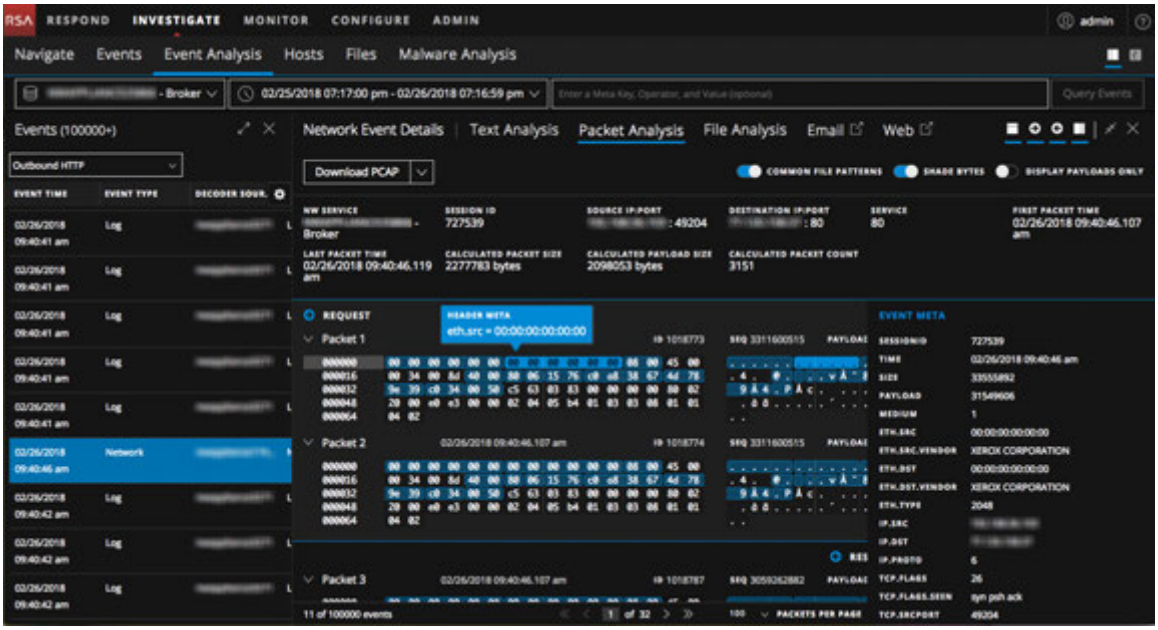
The Packet Analysis panel is for network events only. The Packet Analysis panel is scrollable, and the packet identification information as well as the Request and Response labels remain visible rather than scrolling out of view.



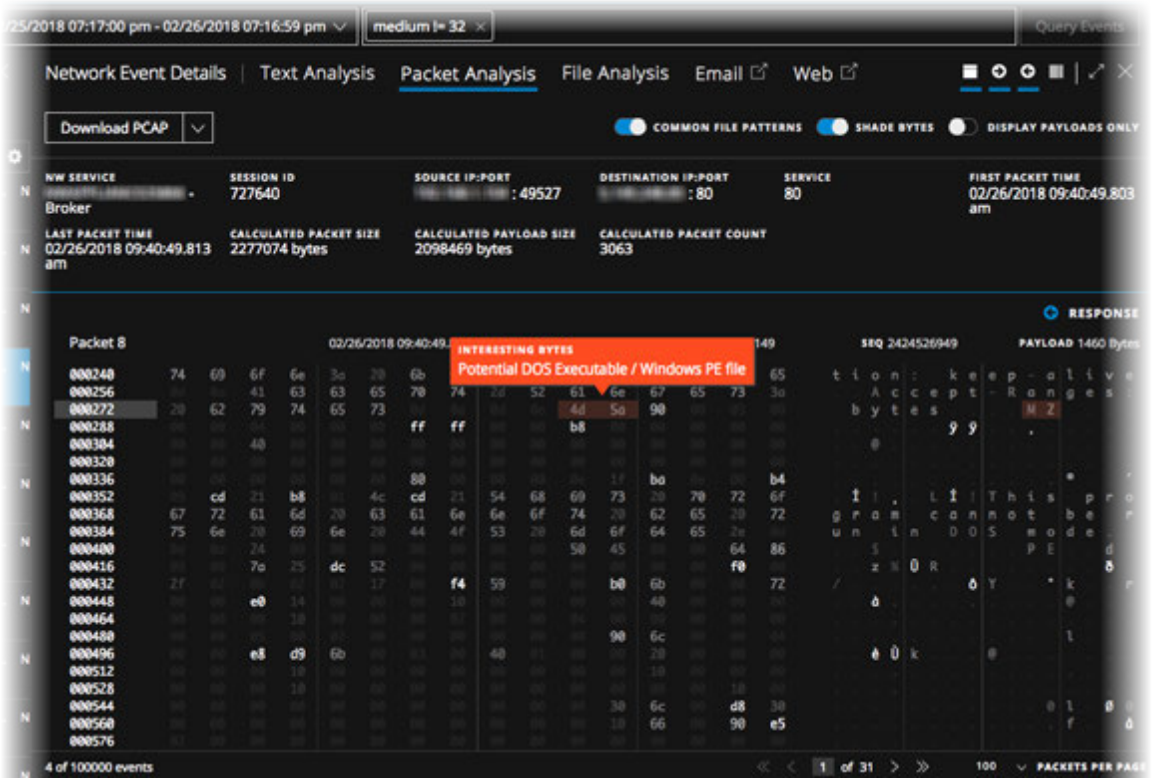
In the Packet Analysis panel, the headings provide the direction of the packet (Request or Response), the packet number, the packet start time, the packet ID and the sequence, and the payload size. All packets begin with a header, and some packets have a footer. Some packets have a payload.

In Version 11.1 pagination controls add flexibility when paging through packets.

The metadata in the hexadecimal and ASCII data is highlighted in blue; when you place the cursor over the highlighted metadata, the meta key/meta value information is displayed in a hover box.

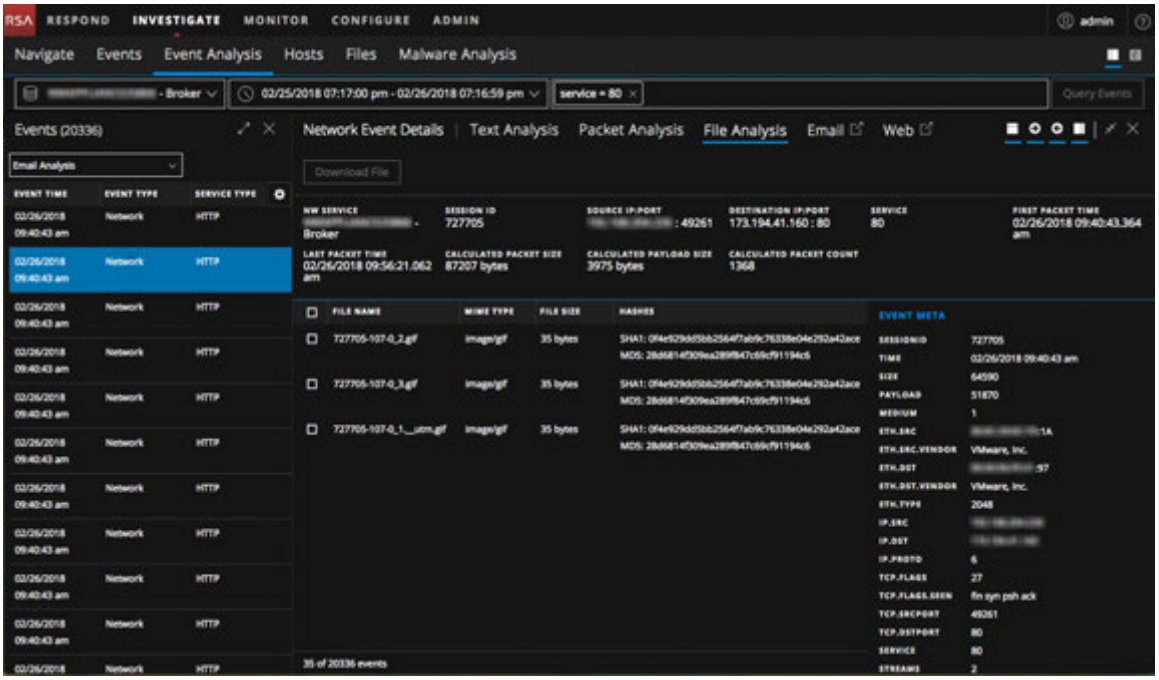


Common file signatures are highlighted with an orange background. When you place the cursor over the highlighted text, the description of the file type is displayed in a hover box.

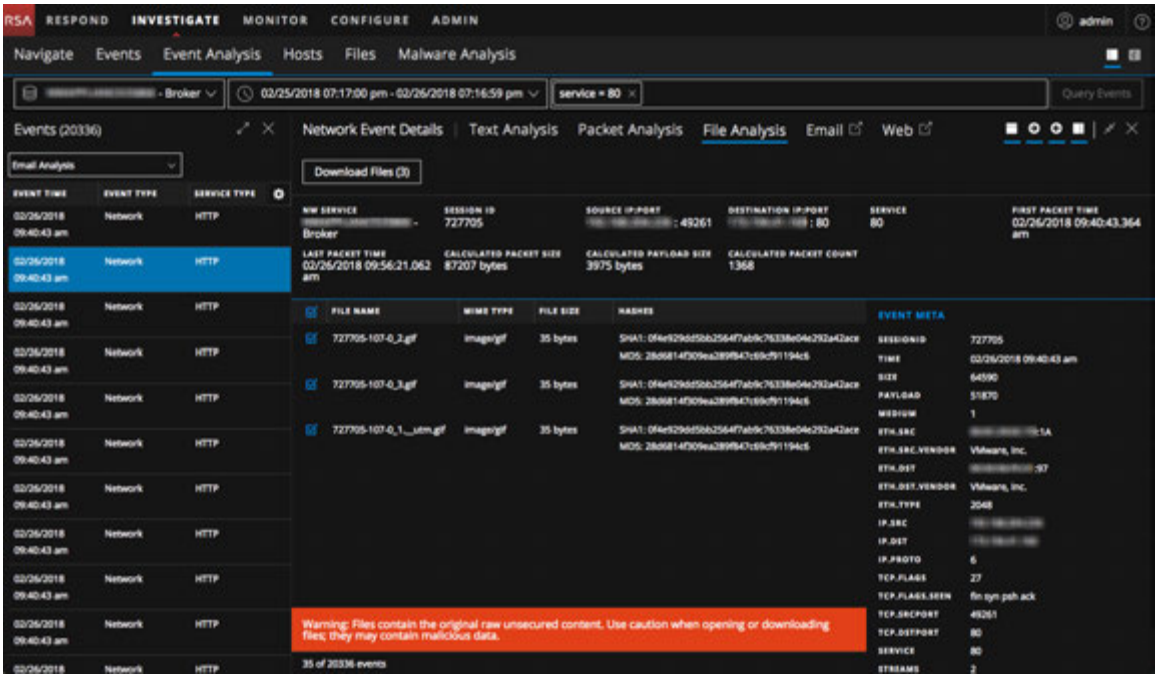


The File Analysis Panel

The File Analysis panel shows a list of files associated with the selected network event. This is an example of the File Analysis panel.



You can select one file, one or more files, or all files to export to your local file system. When files are selected, the Export Files button becomes active and reflects the number of files selected.



Caution: Caution is advised when unzipping and opening files that are associated with a default application; for example, an Excel spreadsheet may automatically open in Excel before you have a chance to verify it is safe.

Analytical Tools for Each Type of Event Analysis

The analytical tools in the Event Analysis view are designed to help analysts find the relevant information for different types of events (network event, log event, and endpoint event). This table lists the actions you can take by event type. The rest of this section provides procedures for performing the actions.

Action	Network Event	Log Event	Endpoint Event
View the Text Analysis panel	✓	✓	✓
View the File Analysis panel	✓		
View the Packet Analysis panel	✓		

Action	Network Event	Log Event	Endpoint Event
Open, close, and adjust the size of panels	✓	✓	✓
Adjust the display of requests and responses	✓		
Show or hide the Event Header in the Text Analysis panel	✓	✓	✓
Expand truncated text entries in the Text Analysis panel	✓		
Switch between a compressed and decompressed view of payloads in the Text Analysis panel	✓		
View highlighted bytes in the Packet Analysis panel	✓		
Highlight common file types in the Packet Analysis panel	✓		
Display only the payload in the Packet Analysis panel	✓		
Shade bytes in the Packet Analysis panel when viewing payload only	✓		
Perform URL and Base64 encoding and decoding in the Text Analysis panel	✓		
View decompressed text for an HTTP network session in the Text Analysis panel	✓		
View event metadata for an event in the Text Analysis panel	✓	✓	✓
Download a network event (as a PCAP file, payload only, request only, or response only) in the Packet Analysis panel or the Text Analysis panel	✓		
Export files from a network event in the File Analysis panel	✓		

Action	Network Event	Log Event	Endpoint Event
Download the file for a log event in the Text Analysis panel		✓	
Download the file for an endpoint event in the Text Analysis panel			✓
Open the current endpoint event in Text Analysis panel			✓

Filter Results in the Event Analysis View

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

In NetWitness SuiteVersion 11.0, you submit a query in the Navigate view or the Events view, and when you go to the Event Analysis view, a read-only breadcrumb shows the submitted query. You need to go to back to the Events view or Navigate view if you want to enter a different query.

In Version 11.1 and later, a query builder populates the interactive breadcrumb in the Event Analysis view so that you can create and edit each `<meta key> <operator> <meta value>` filter in the breadcrumb. In addition, you can select a different service and time range without going back to the Navigate view or the Events view. The remainder of this section provides information about using the Version 11.1 query builder features.

How the Breadcrumb Works

When you click the Event Analysis option in Investigate to open the view, the service and time range selector is displayed. By default, the first service is auto selected (unless you previously selected a service and the selected service is in localstorage). If you do not select a time range, the default time range is used. The query builder field is an empty field to the right of the time range. The following figure illustrates the breadcrumb with only a service and time range selected.

When you open the Event Analysis view from the Events view or the Navigate view, the service, time range, and any filters that were selected in the Events view or Navigate view are displayed in the breadcrumb. The service, time range, and individual filters can be modified.

Note: The query builder supports only simple filters in the form `<meta key><operator><meta value>`. If the Events view or Navigate view has a filter with more than one operator, ||,&&, (), REGEX, or LENGTH, the filter is added, but editing is not supported in the Event Analysis view.

As you create filters in the query builder, the breadcrumb is updated with each filter in an editable field. When you submit the query, all of the filters are AND'd to generate results. The query is not submitted until you click Query Events. Filters line up from left to right, representing the sequence in which the filters were created. Each filter is a simple expression of the form `<meta key> <operator> <optional value>`. As more filters are added and they cannot be displayed in a single line, they wrap to another line and the input area expands vertically so that all filters are visible without scrolling to the right.

As you create and edit filters, you are assisted with suggestions for auto-complete that show only valid meta keys and operators in the drop-down list. You can type or select from the drop-down list. Invalid filters are marked by a red outline, and if you hover the mouse over the filter, a message that explains the error is displayed.

The Query Events button is on the right side of the breadcrumb input, and is visible as needed to input a query. New filters are applied when you click Query Events.

Note: If you change the service, a network call for data for reconstructions or the Events panel (for example, Load More) uses the previous service/time range/metadata filters. It will continue to use these previous query parameters until you submit the new query. When you have a set of results loaded and you change the service, time range, or a filter, the Query Events button turns blue as an indicator that the data in the view is stale. Even if you start to edit any one of the parameters, and then decide not to, the Query Events button turns blue as an indicator that you need to resubmit the query.

The following figure illustrates a breadcrumb with a filter.

Keyboard Actions to Use in the Breadcrumb

The breadcrumb is designed to allow entry, editing, and deletion of filters from the keyboard without having to use a pointer. Although you can use the pointer, you have the option to keep your fingers on the keyboard. This table identifies the available keyboard actions when the cursor is located in the Query Builder portion of the breadcrumb; these do not apply to the service selector and time range.

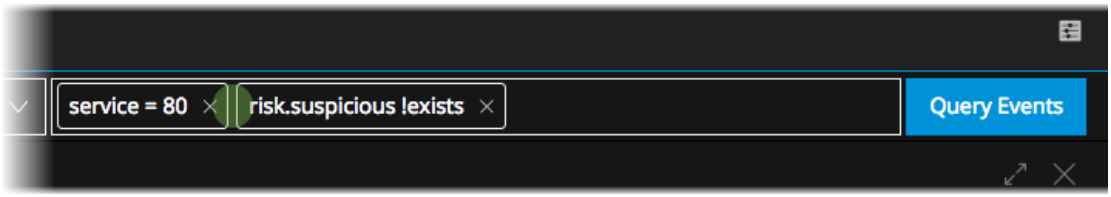
Action	Keyboard Entry
Update the URL and resubmit the query.	With focus on the Query Builder, press **Enter.**
Select the filter to the immediate left if one exists.	With no selection in the Query Builder, press the **Left Arrow** key.
Select the filter to the immediate right if one exists.	With no selection in the Query Builder, press the **Right Arrow** key
Insert a new filter to the immediate left of the selected filter.	With a filter selected, press the **Left Arrow key**

Action	Keyboard Entry
Insert a new filter to the immediate right of the selected filter.	With a filter selected, press the**Right Arrow** key.
Insert a new filter to the immediate left of the selected filter, and open for editing.	With a filter selected, press the **Shift + Left Arrow** keys.
Insert a new filter to the immediate left of the selected filter, and open for editing.	With a filter selected, press the **Shift + Right Arrow** keys.
Select all filters to the right of the current filter.	With a filter selected, press the **Shift + Down Arrow** keys.
Select all filters to the left of the current filter.	With a filter selected, press the **Shift + Up Arrow** keys.
Deselect all filters.	With a filter selected, press the **Escape** key.
Delete all selected filters.	With filters selected, choose the **right-click > Delete selected filters** option, press **Delete**, or press **Backspace**.
Update query with only the selected filters.	With filters selected, choose the **right-click > query with selected filters** option.
Open a new tab with the selected filters.	With filters selected, choose the **right-click > query with selected filters in a new tab** option.

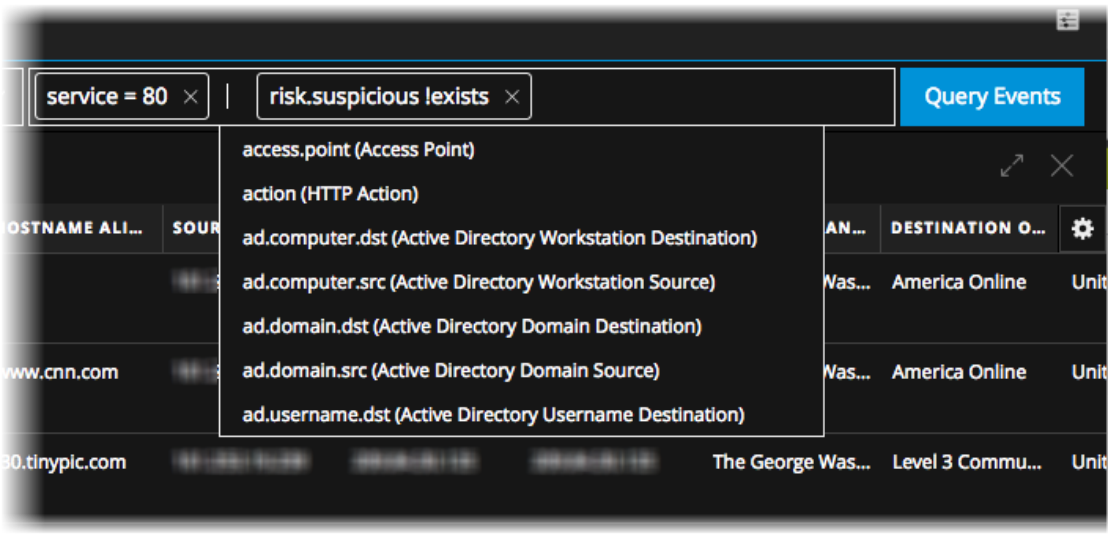
Add a Filter to the Breadcrumb

To filter the data displayed in the Event Analysis view:

1. Navigate to the **Event Analysis** view.
2. To insert a filter, click in the query builder field, or before or after an existing filter.
   If the insertion point is between two filters, a green dot marks the insertion point. If the insertion point is at the end of the existing breadcrumb, the filter entry field opens.

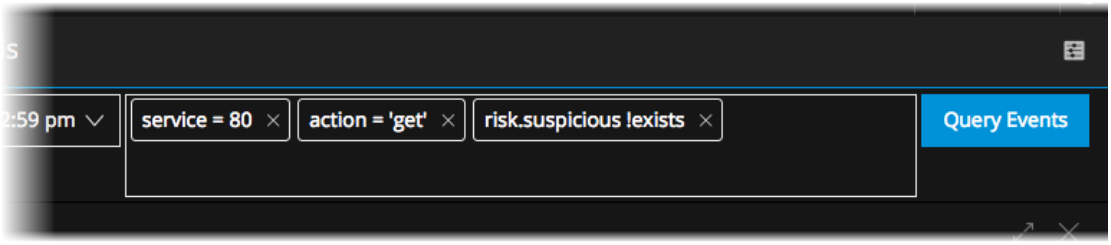


3. Click on the insertion point and a drop-down menu lists available meta keys to use in the new filter. The available meta keys are passed from the service being investigated.



4. To select a meta key do one of the following:
   a. If there is only one option in the drop-down menu, press the **Space** bar.
   b. If there are two or more options in the drop-down menu, click on the meta key or use the up/down arrow and press **Enter**.
   c. Type the meta key and a space. As you type the meta key, the list is further updated. With a meta key selected, a list of valid operators for the selected meta key is displayed.
5. To select an operator do one of the following:
   a. If there is only one option in the drop-down menu, press the **Space** bar.
   b. If there are two or more options in the drop-down menu, click on the operator or use the up/down arrow and press **Return**.
   c. Type the operator and press **Enter**.
   The drop-down list closes and you can add a value if the operator accepts a value.
6. (Optional) Type a value and press **Enter**.
7. To create the filter, press **Enter**. If you click anywhere outside the box before pressing **Enter**, the filter is not created.
   The new filter is inserted, and the cursor is refocused after the last filter.
   If there is an error in the filter, it is outlined in red. You can hover over the filter to see a tool

tip explaining the error.



8. Fix any filters that have errors.
9. When you are ready to execute the query in the breadcrumb, click **Query Events**.
10. The Events List is refreshed to reflect the query.

Edit a Filter in the Breadcrumb

To edit a filter in the Query Builder:

1. Navigate to the **Event Analysis** view.
2. To edit a filter, double-click it, or click the filter and press **Enter**.
3. When finished editing, press **Enter** to update the filter.
4. To deselect the filter, click another filter.
5. If you want to execute the query again, click the **Query** button.
   The Events List is refreshed to reflect the updated filter.

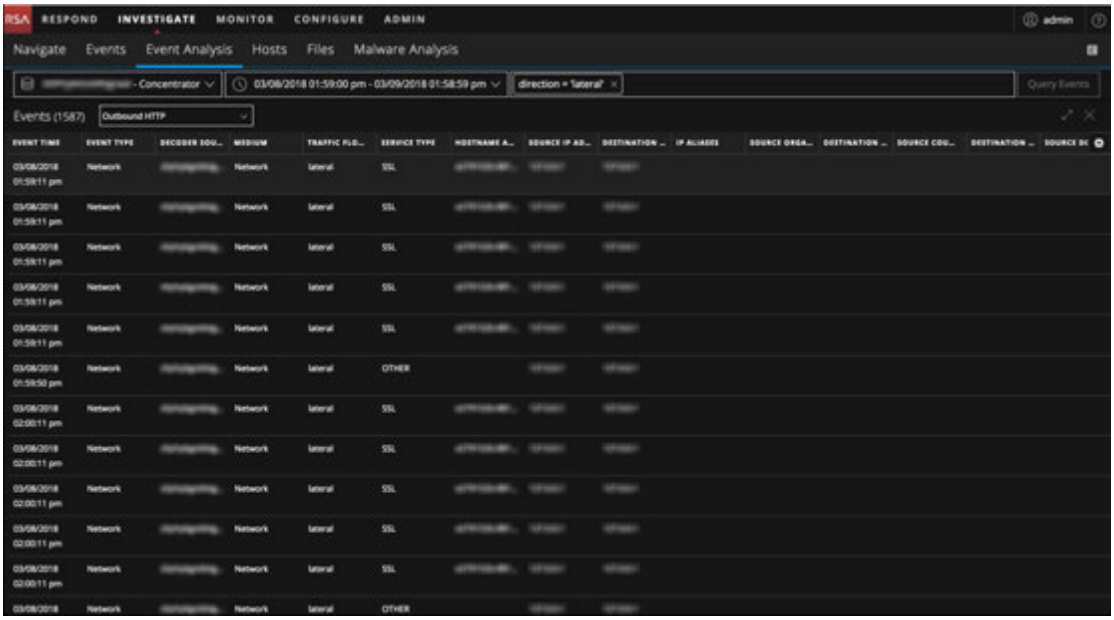
Query Using Selected Filters in the Breadcrumb

With two or more filters in the breadcrumb, you can refocus the same query to include only selected filters. The results are displayed in the current browser tab or a new browser tab.

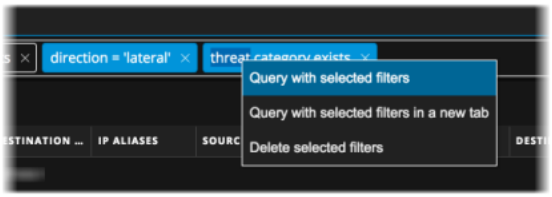
To update the query using only selected filters:

1. Begin with a breadcrumb that includes at least two filters, for example a query has three filters: `risk.info = exists`, `direction ="lateral"`, and `threat.category exists`.
2. To open a new tab with the selected filters, right-click the `query direction = "lateral"` filter and select **query with selected filters in a new tab** in the drop-down menu.

A new tab opens with the results for the selected filter.



3. To query the selected filters in the same tab, click `direction = "lateral"` and `threat.category exists`. Then right-click and select **query with selected filters** in the drop-down menu.



Delete a Filter in the Breadcrumb

To delete a filter:

1. Click **X** in a filter, click on the filter to select it and press **Delete** , or right-click one or more filters and select **Delete selected filters** in the drop-down menu.
2. If you want to execute the query again, click the **Query** button.
   The selected filter is deleted and the Events List is refreshed.

Examine Events in the Event Analysis View

When examining raw events and meta data in the Event Analysis view, you can make simple adjustments in the visibility and size of the panels. Within the Packet Analysis panel and the Text Analysis panel, you use additional features to adjust the way the reconstruction is displayed and bring interesting data into focus.

Select the Event Analysis Type

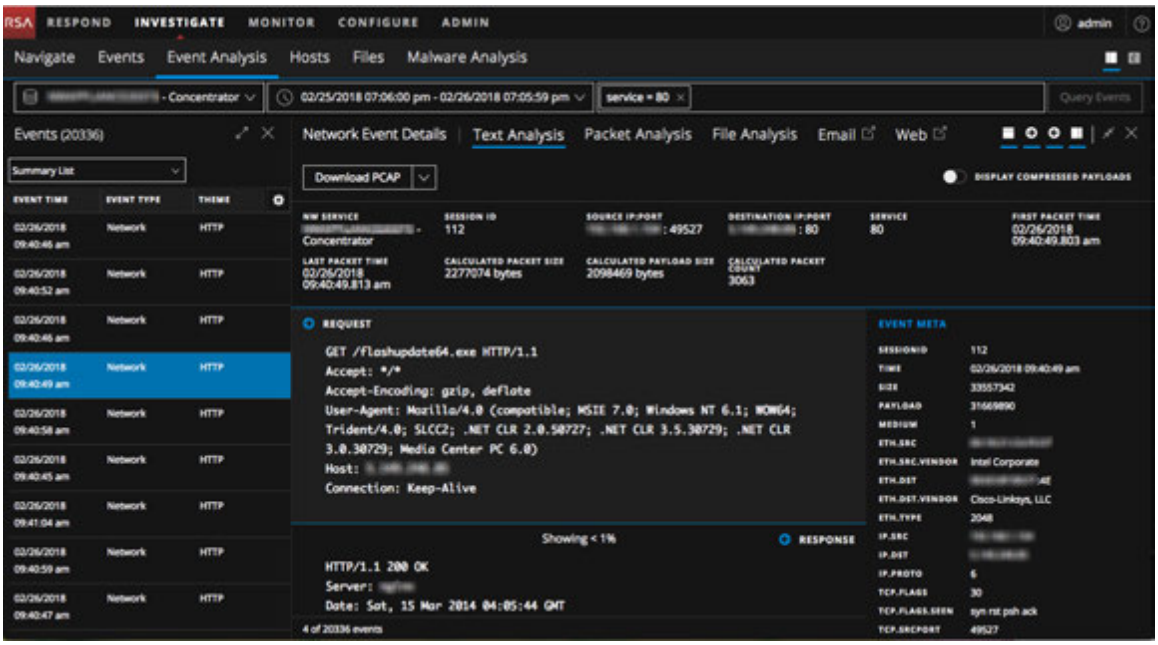
To select the event analysis type for an event, do one of the following:

1. In the **Event Analysis view** toolbar, click the analysis type in the toolbar.
2. In the drop-down menu, select the analysis type: **File Analysis**, **Text Analysis**, **Packet Analysis**, **Email** (Version 11.1 and later), or **Web** (Version 11.1 and later).
   If you chose **File Analysis**, **Text Analysis**, or **Packet Analysis**, the view is refreshed with the Packet Analysis panel, File Analysis panel, or Text Analysis panel open.
   If you chose **Email** or **Web**, the Events view email or web recontruction of the single event opens in a new tab. This is the same reconstruction of an email or web session used in the Events view. The Events view provides more functionality when viewing an email or web reconstruction, allowing you to page through events in that view instead of viewing only one event (see Reconstruct an Event).

Note: The Packet Analysis panel is only available for network events.

Open, Close, and Adjust the Size of the Panels in the Event Analysis View

The Event Analysis view opens with the Event list and no event selected or reconstructed. When you select an event, the Network Event Details, Log Event Details, or Endpoint Event Details panel opens on the right. Initially, the Network Event Details, Log Event Details, or Endpoint Event Details panel occupies 75% of the window width by default.



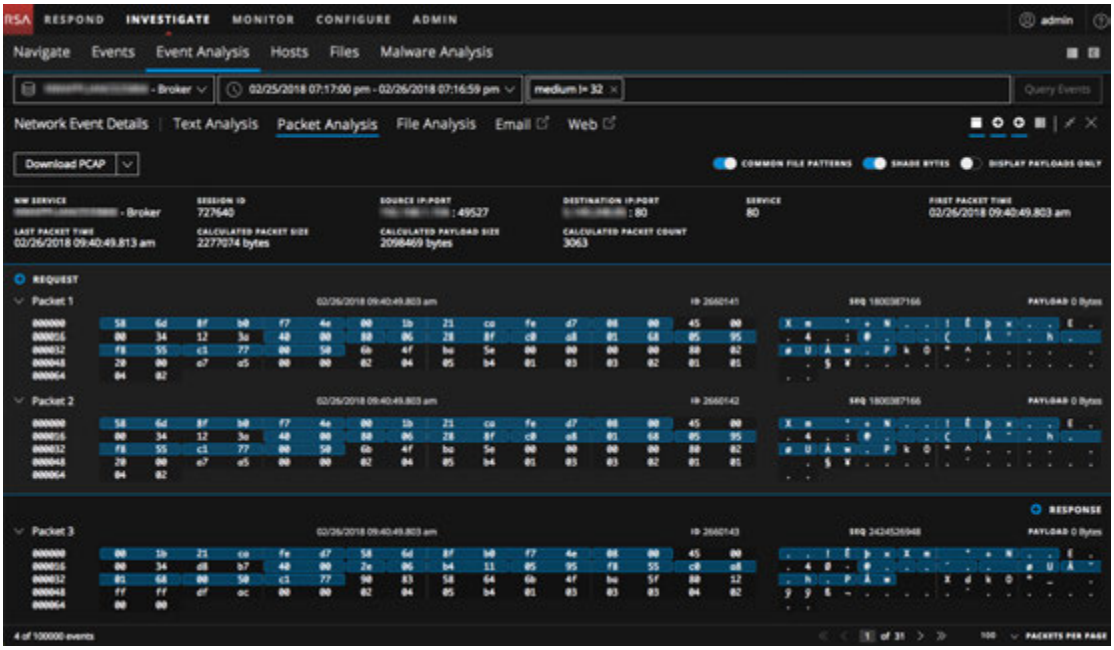
You can adjust the size ratio of the two panels to improve readability by expanding one of the panels, contracting one of the panels, and closing one of the panels. After closing either panel you can reopen it. The ratio you select persists until you change it or refresh the browser.

- To reopen the Events panel, click ◫ in the upper right corner.

To optimize your view:

1. To adjust the size ratio of the two panels, do any of the following:
   a. Click ◪ in the tool bar of the panel that you want to expand.
   b. Click ◪ in the tool bar of the panel that you want to contract.
2. To close either panel, restoring the open panel to its full width, click ◪.
   This is an example of the reconstruction displayed using the full width of the browser

window.



3. To reopen the Events panel after closing, click ◫ in the top right corner of the Navigate view.

   The Events panel opens to the last state (25%:75% or 50%:50%).

4. To reopen the Event Details panel, click an event in the Events panel.

Select a Column Group and Columns in Event Analysis

In Version 11.1 and later, you can use built-in or custom column groups in the Events panel. The column groups are created and managed in the Events view (see Manage Column Groups in the Events View); these groups are reflected in the Event Analysis view. When you change the column group, the changes you make to a column group are for the current view only. When you navigate away and come back to the Event Analysis view, the column changes do not persist in the Events panel.

These are the built-in column groups.

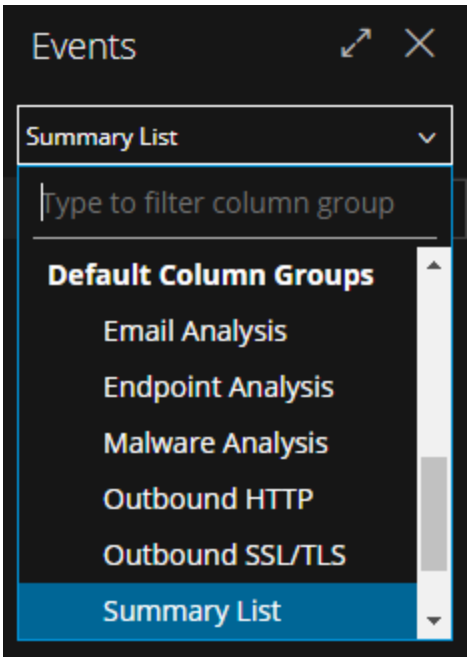
- **Email Analysis**: Includes meta keys that are useful when investigating email-related metadata.
- **Endpoint Analysis**: Includes meta keys that are useful when investigating endpoint-related metadata.
- **Malware Analysis**: Includes meta keys that are useful when investigating malware-related metadata.

- **Outbound HTTP**: Includes meta keys that are useful when investigating Outbound HTTP-related metadata.
- **Outbound SSL/TLS**: Includes meta keys that are useful when investigating Outbound SSL/TTS analysis-related metadata.
- **Summary List**: Includes meta keys that are useful in a general investigation. **This is the default column group.**
- **Threat Analysis**: Includes meta keys that mark potential threats in the data set.
- **Web Analysis**: Includes meta keys that mark anomalies in web traffic.

A column group may contain more columns than are visible without scrolling to the right. In Version 11.1, you can select the columns that appear in Event Analysis view. The order of the columns reflects the order in the Events view of the default column group. By default, the first 15 columns are displayed when you select a column group. For optimized viewing, it is advised to view only 15 columns at a time; however, you can select additional columns to display and remove columns displayed.

To select a column group:

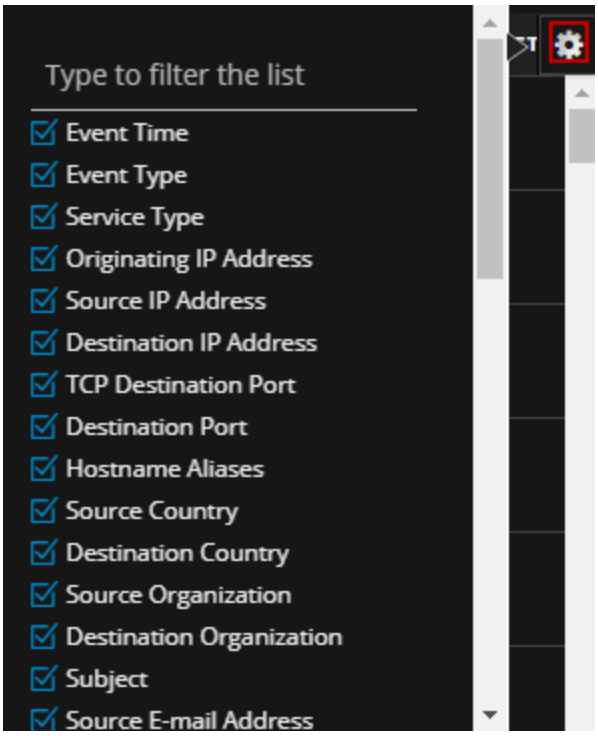
1. From the drop-down menu next to Events, select a column group (for example, **Summary List**). You can also start typing the name of the column group and select a group as the groups appear in the drop-down menu.



The Events panel displays data in the columns that belong to the selected column group.

To select columns to display:

1. While working in the Event Analysis view, with a column group selected, click ⚙ to display the column selector.



2. Select the meta keys or enter the name of a meta key that you want to display in additional columns.
3. If you do not want to see a meta key displayed in a column, de-select the meta key.
   The data is re-displayed using the selected columns.

Adjust the Display of Requests and Responses

For Event types that have requests and responses in them, you can make several adjustments.

Note: If the analysis type does not have requests and responses, the option is not selectable. The File Analysis panel is an example of a reconstruction type without requests and responses. A reconstructed log event in the Text View is another example.

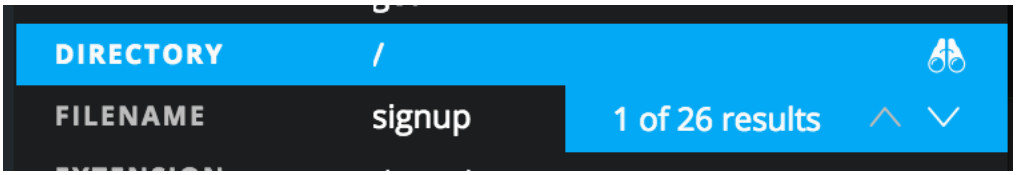
To select which side of the conversation to show--Request, Response, or both--click one or both of the direction icons. The reconstruction is refreshed with the selected information.

Note: If you do not see any data, you may have deselected both Request and Response. You must select one of the two to see data displayed.

View Event Metadata for an Event

When examining events in the Text Analysis panel, Packet Analysis panel, or File Analysis panel, you can click to show the associated metadata in an adjacent panel, the Event Meta panel.

When viewing Text Analysis and the Event Meta panel, hovering over the meta key/meta value pairs reveals a pair of binoculars if the meta value is searchable in the raw text. This is an example of the binoculars icon when hovering over the **Directory** and / meta key/meta value pair.



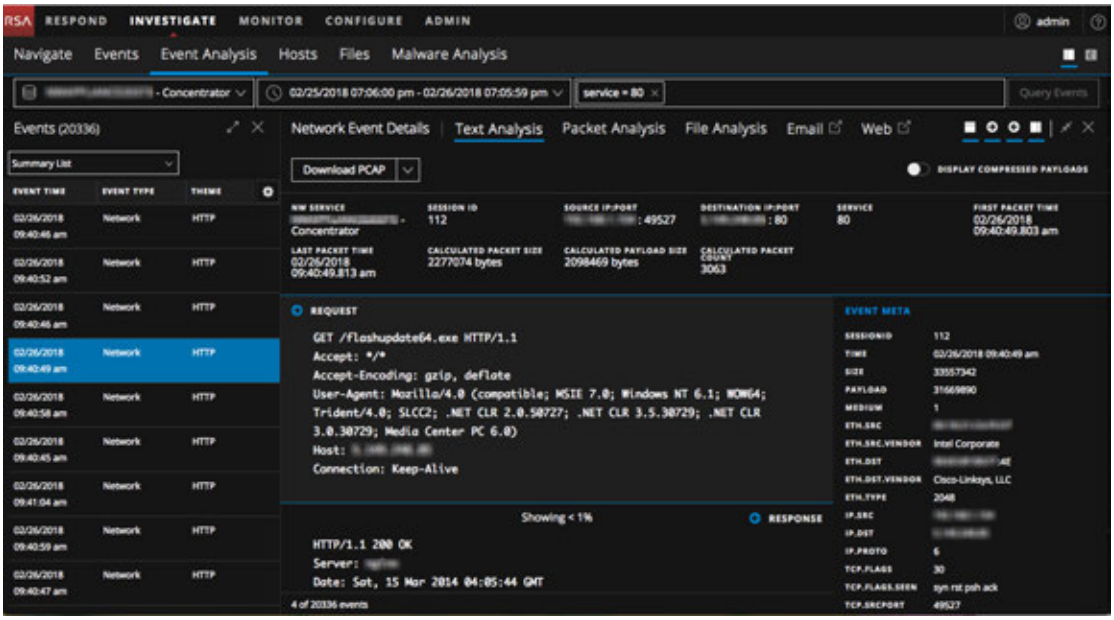
Clicking on the icon triggers a search for the meta key/meta value pair (case-insensitive) in the Text Analysis panel and each instance is highlighted. In the Event Meta panel, the highlighted row has a count of the results and a scroller that you can use to quickly find each result in the Text Analysis panel. You can view each highlighted location of the data that triggered generation of the meta key, going forward to view the next, and back to view the previous.

Only meta keys that have relevant values inside the RAW text are searchable. You can search only one meta key at a time. If the value is currently hidden due to truncation of a text entry with more than 3000 characters, the text entry is expanded to reveal the found meta value.

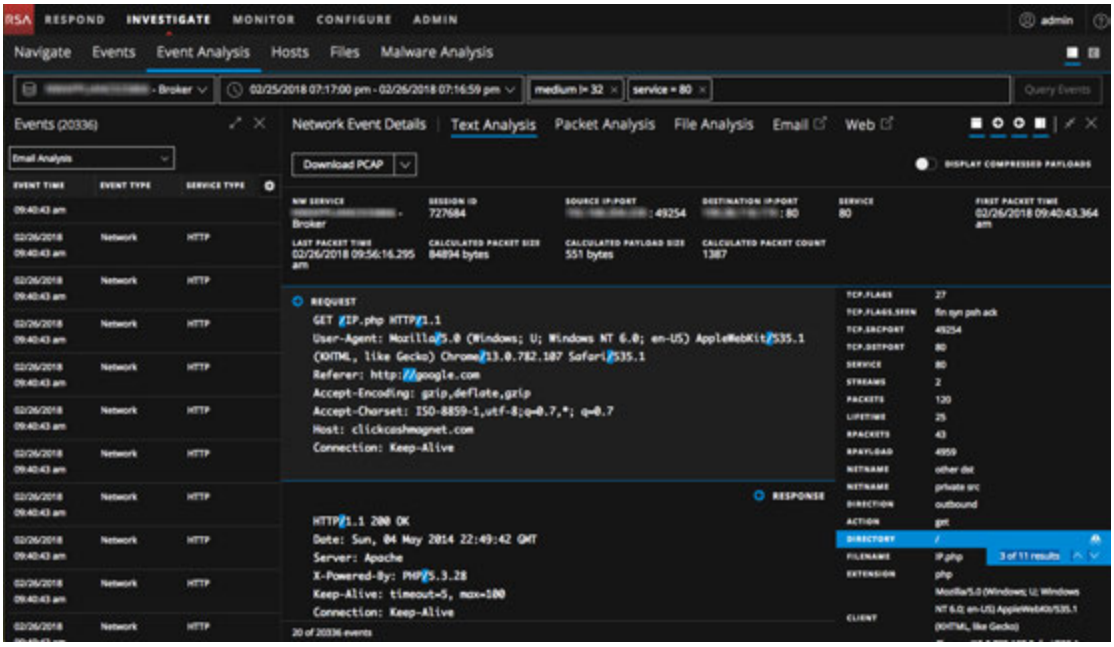
Clicking on the same meta key/meta value pair or a different meta key:value pair in the Event Meta panel removes the highlighting from the raw text. The highlighting is also removed if you close the Event Meta panel.

To search the raw text for meta values that triggered a meta key:

1. Open a network event in the Text Analysis panel.



2. In the toolbar, click to open the Event Meta panel. As you hover over the meta key:value pairs in the list, a binoculars icon identifies values that are searchable in the Text Analysis panel.
3. To search for the value in the raw text, click a row that has the binoculars icon, indicating it is searchable.
   If no relevant occurrence of the value is in the text, the value that you are searching for is highlighted in the Event Meta panel and nothing is highlighted in the Text Analysis panel.
   If one or more relevant instances of the value is found in the Text Analysis panel, each occurrence is highlighted. The value that you are searching for is highlighted in the Event Meta panel and the scroller is visible.



4. To remove the highlighting, close the Event Meta panel, click the same meta key/meta value pair in the Event Meta panel, or click a different meta key/meta value pair in the Event Meta panel.
   The highlighting is removed from the raw text.

Show or Hide the Event Header

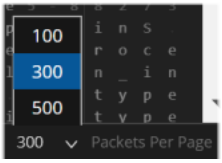
To hide the Event Header in the Packet Analysis panel, Text Analysis panel, or File Analysis panel, providing more vertical space for the data, click .

Page Through Events in the Packet Analysis Panel

In Version 11.1 and later, packet pagination controls allow more flexibility in paging through a list of packets. You can select the number of packets to display per page, and your selection is saved across logins to the NetWitness application. When a control is unavailable, the control is dimmed; for example, when you are viewing page 1, the and controls are dimmed.

To use pagination controls:

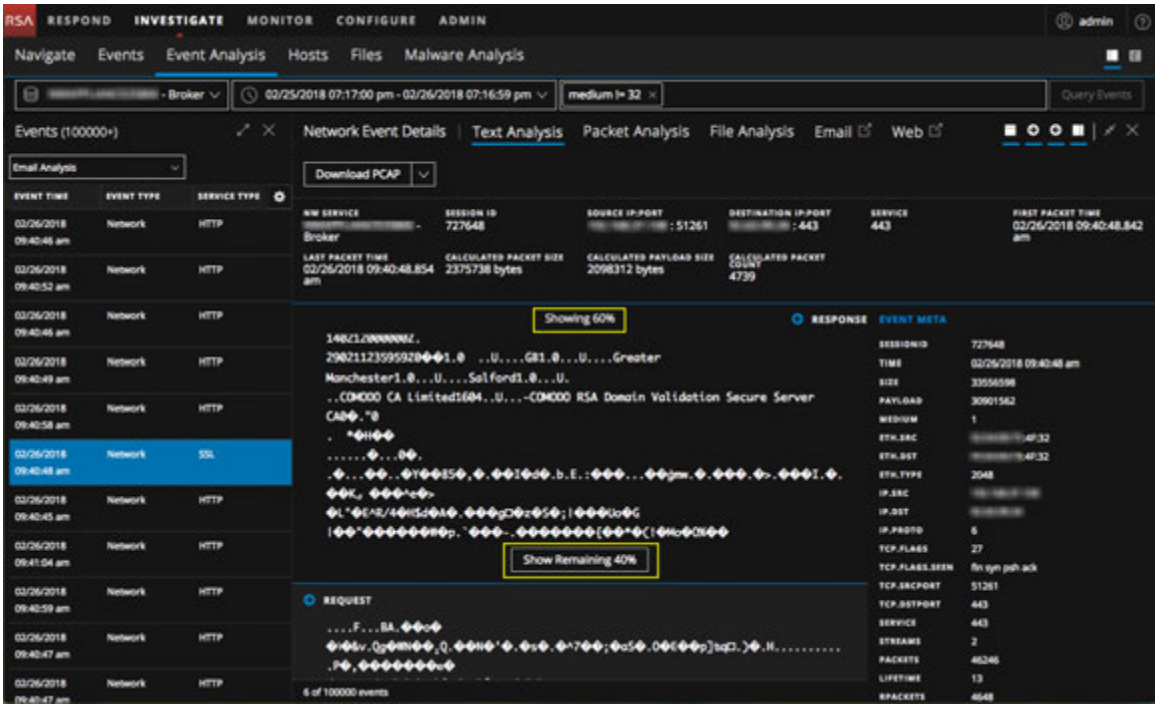
1. With an event open in the Event Analysis view, click the current number of packets per page (**100**, **300**, or **500**), and select the new number of packets per page from the drop-down menu.



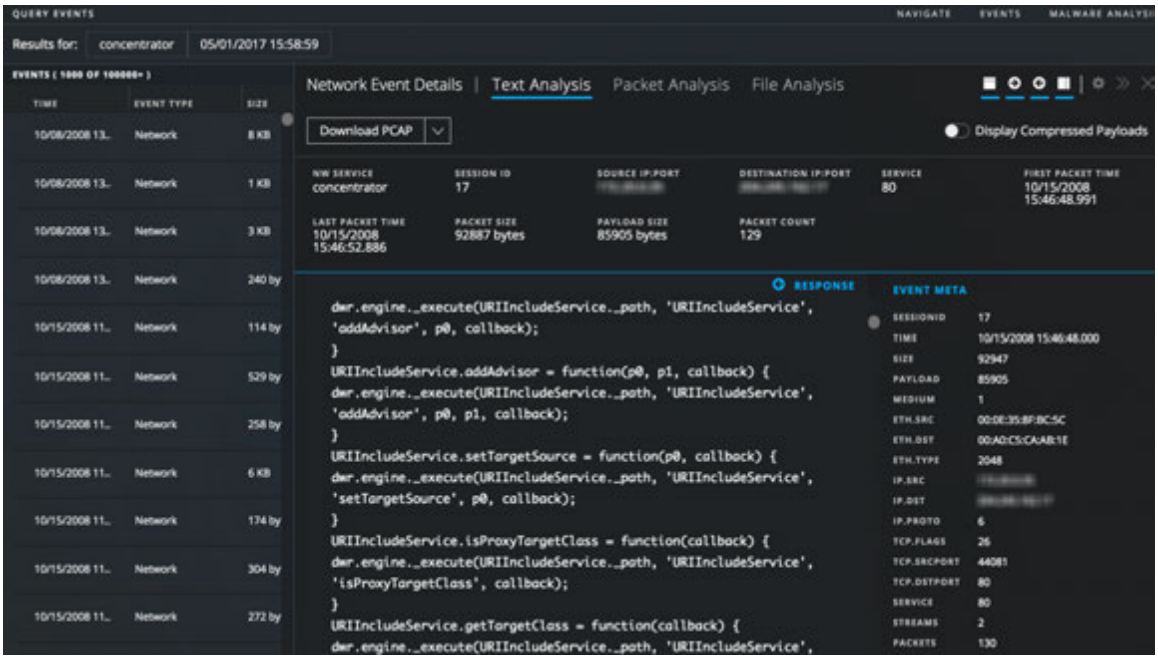
2. To page forward or back, use the page control icons:
   Click ▶ to go to the next page.
   Click ⏭ to go to the last page.
   Click ◀ to go the previous page.
   Click ⏮ to go to the first page.
3. To go to a specific page, type a page number in the page number field 1 of 226.

Expand Truncated Text Entries in the Text Analysis Panel

A reconstruction of a network event in the Text Analysis panel may include requests and responses of many hundred thousands of characters and scrolling through a long entry of more than 6000 characters that is not of interest can waste time. To improve the experience for analysts, all text entries that have more than 6000 characters are truncated to show only the first 2000 characters. This example shows an entry that has more than 2000 characters and a message in the header indicates the percentage of total characters that is being displayed.



You can see that 60% of the characters (the first 2000) are displayed, and click **Show Remaining 40%** to reveal the rest of the entry.



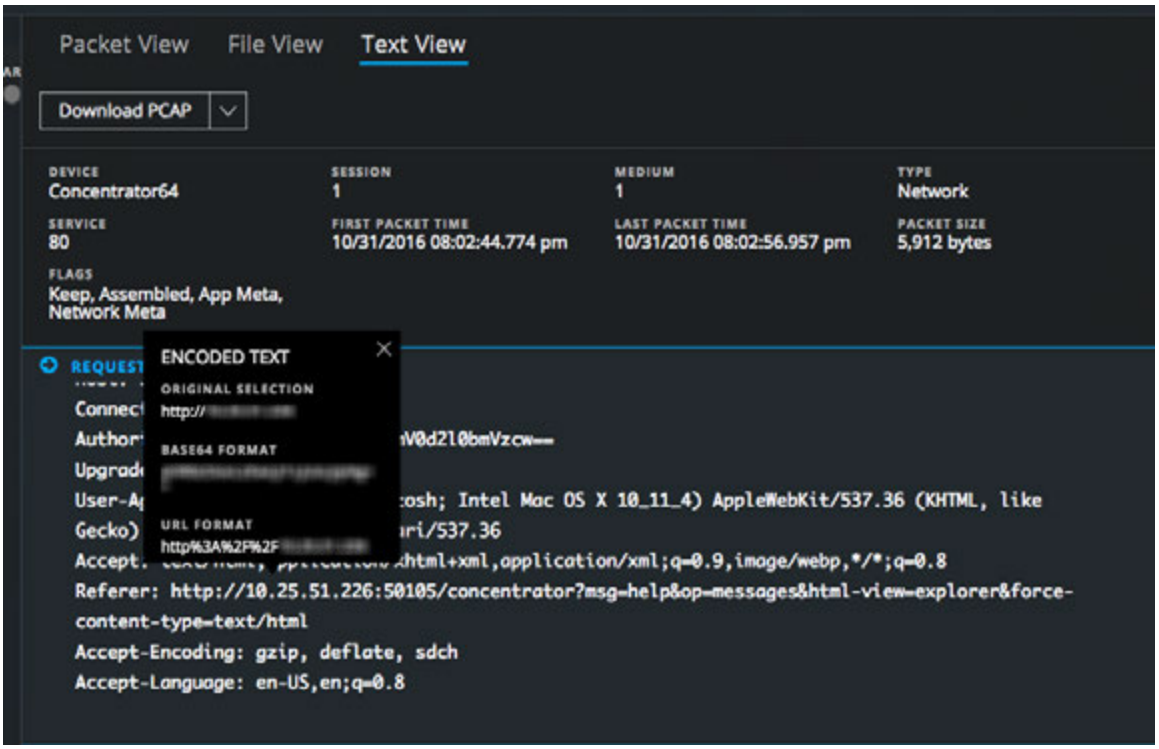
If you search for metadata seen in the Event Meta panel while text is truncated in the Text Analysis panel, the truncated text is searched. If the metadata exists inside hidden text, the text entry expands to reveal the text with the found metadata.

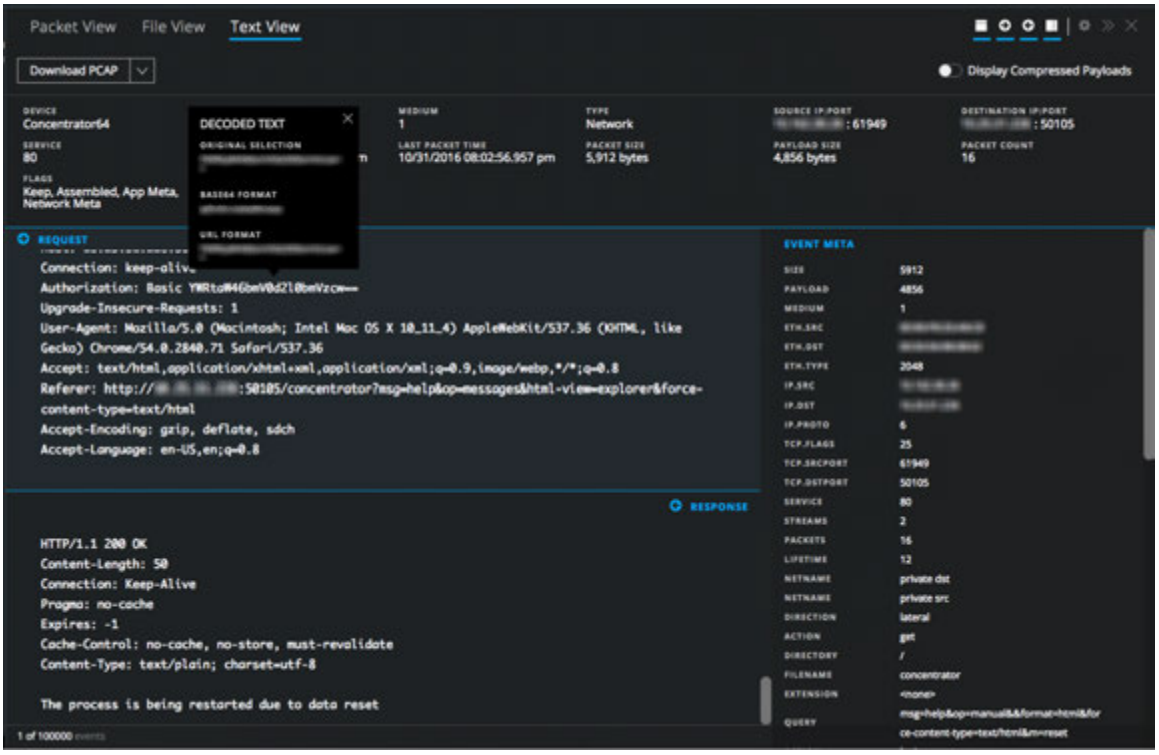
Perform URL and Base64 Encoding and Decoding in the Text Analysis Panel

If a network session being reconstructed in the Text Analysis panel contains Base64 or URL encoded strings, you can decode a string to better understand the session. If the session contains decoded strings for Base64 or URL, you can view a string in its encoded form in order to search for additional instances of the encoded text in other sessions.

When viewing any network session that contains encoded text in the Text Analysis panel, you can select a subset of the text within a single Request or Response to view in either encoded or decoded form. Depending on the content loaded on the Decoder, there may be additional metadata outlining that Base64 or URL encoded data is contained within the session.

Below are examples of a hover box that is displaying URL encoding and Base 64 encoded text.

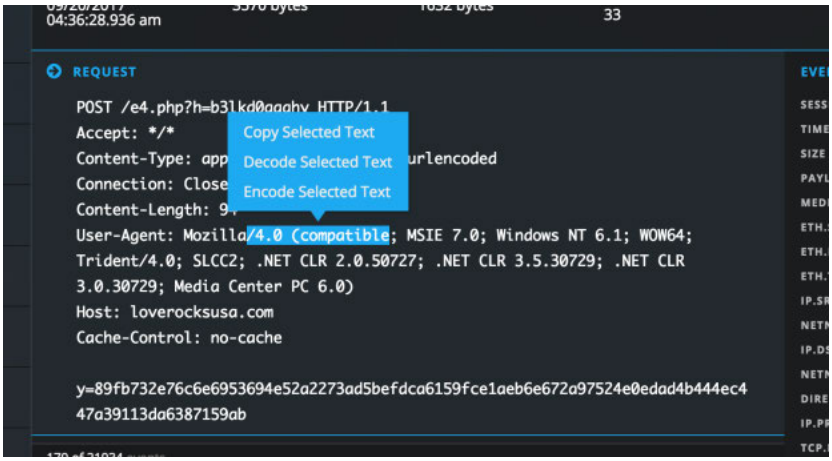




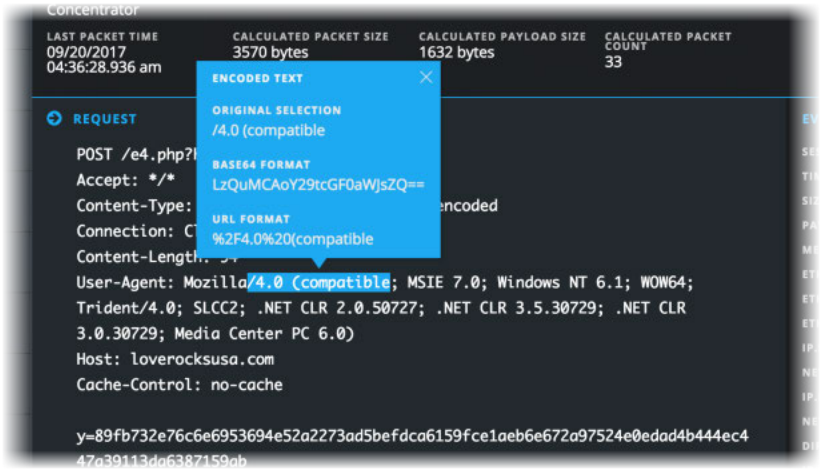
To perform encoding and decoding in the Text Analysis panel:

1. In the **Event Analysis view**, go to the Text Analysis panel of a session that contains encoded or decoded content.

2. To view some decoded text in encoded form, drag to select the text within a single Request or Response.
   A menu offers options to encode and decode.



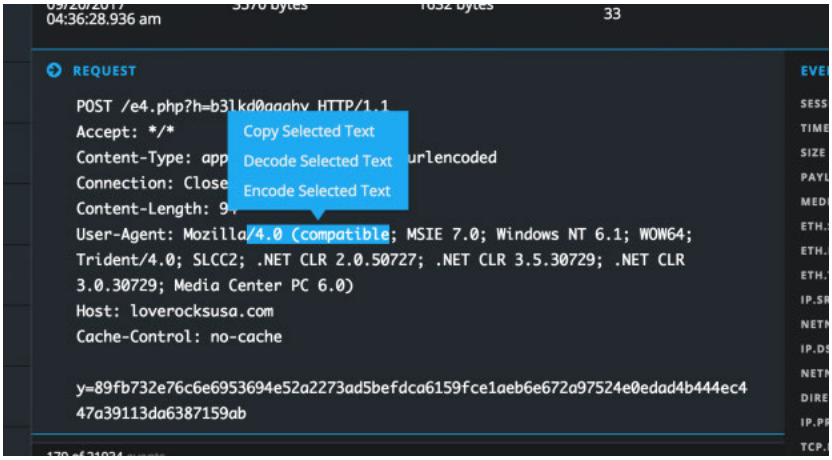
3. Click **Encode Selected Text.**
   The encoded text is displayed in a hover box, which remains in place until you click the ✕, select different text in the Text Analysis panel, close the Events panel, select another event for reconstruction, or switch to a different reconstruction view.



   When a longer text is selected, the hover box is scrollable and large enough to fit the entire selected text as well as the decoded text.

4. If the session contains encoded text that you want to see in decoded form, drag to select the text within a single Request or Response.
   A menu offers options to encode and decode.

5. Click **Decode Selected Text.**
   The decoded text is displayed in a hover box, which remains in place until you click ■, select different text in the Text Analysis panel, close the Events panel, select another event for reconstruction, or switch to a different reconstruction view.
6. If you want to copy some text from the text reconstruction do one of the following:
   a. Drag to select some text, right-click, and select **Copy Selected Text** from the popup menu.



   b. Drag to select some text, then select either **Decode Selected Text** or **Encode Selected Text**. Within the popup, select the desired text and type **Control-C**.
   The selected text is copied to the clipboard and available to paste in a query.
7. When finished, click ■ to close the hover box.

View Decompressed Text in an HTTP Network Session in the Text Analysis Panel

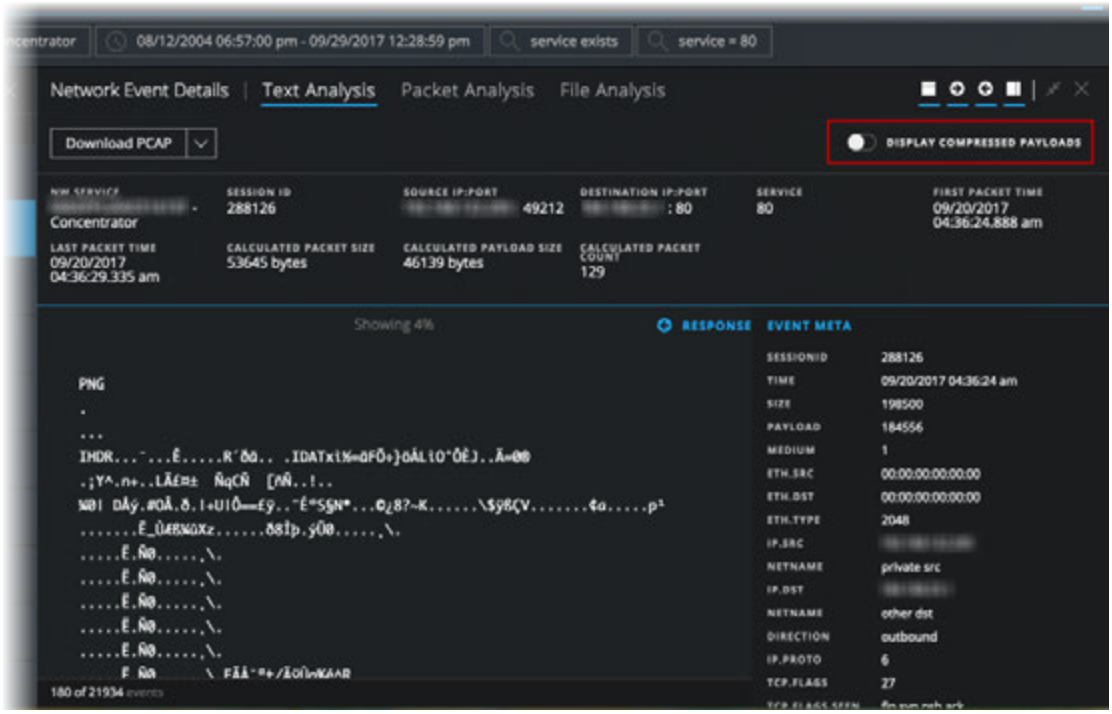
When the content of an HTTP network session is compressed and you are viewing the Text Analysis panel, NetWitness Suite displays decompressed content by default. This helps you to determine if there are any patterns and view the readable characters. You can switch between a compressed and decompressed view of compressed text.

Note: Decompressed text is not available for the Packet Analysis panel, the File Analysis panel, non-HTTP network sessions, and log data.

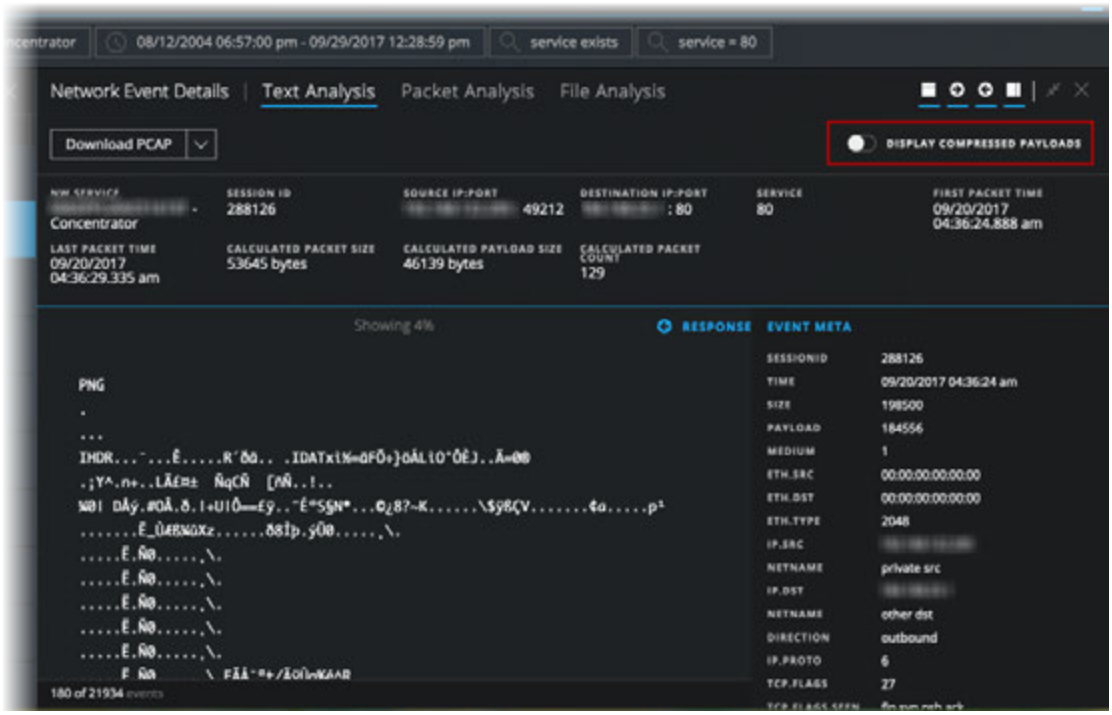
The toggle for changing between compressed and decompressed text is only displayed in the Text Analysis panel, and is enabled only if there is compressed text content.

1. Open the Text Analysis panel of an HTTP session that contains compressed content.
   By default the session is reconstructed with the text decompressed, and above the

reconstruction, is the **Display Compressed Payloads** toggle switch.



2. To view the same text in its compressed form, click the toggle switch.
   The view changes so that the compressed text is no longer readable, and the switch indicates the Display Compressed Packets is on.



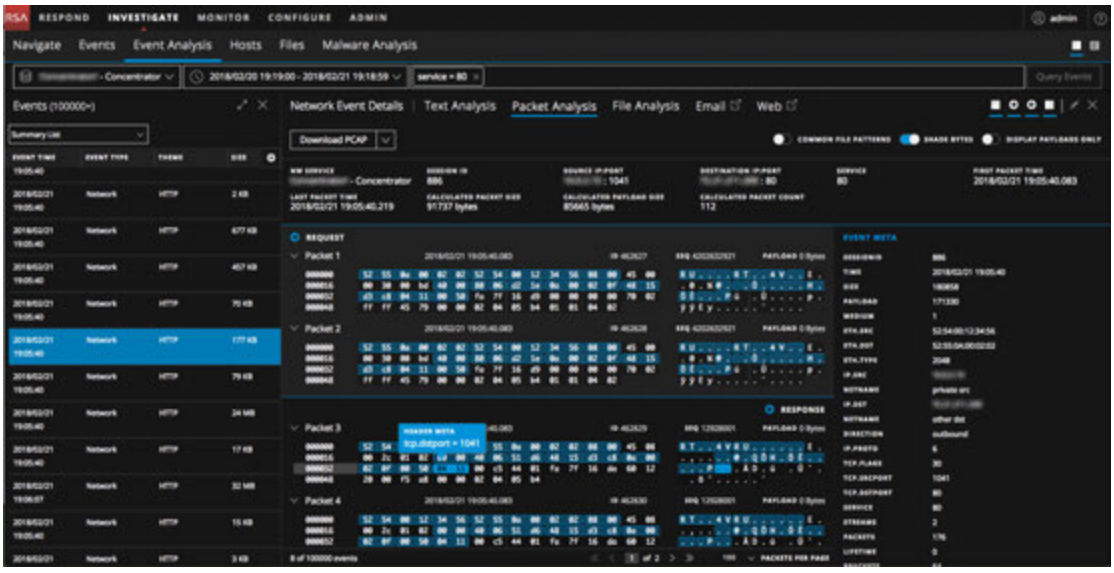
3. To return to the view of decompressed text, click the switch again.

Use the Payload Only Option in the Packet Analysis Panel of a Network Session

When viewing a reconstruction of a network session in the Packet Analysis panel, you can choose to view only the main payload for each packet. By default, packet header and footer bytes are displayed for each packet. You can hide these by clicking the Display Payloads Only toggle switch. If you are viewing only the payload bytes, you can revert to the default setting by setting the Display Payloads Only toggle switch to on. This setting persists until you change it or refresh the browser.

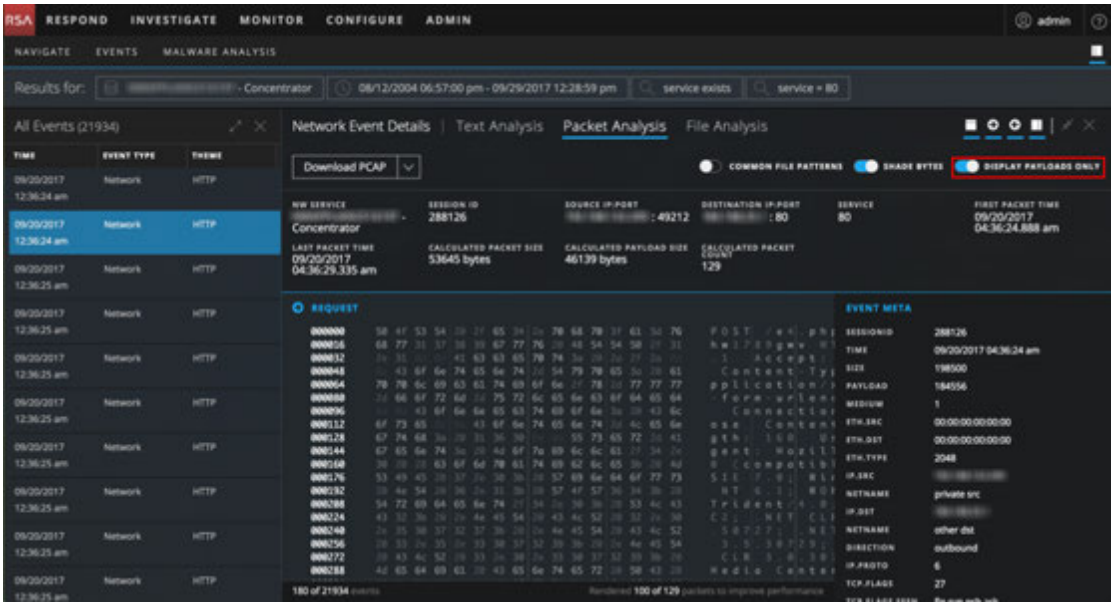
- With the Display Payloads Only option off, the number of packets, packet header, packet footer, and payload are displayed.
- With the Display Payloads Only option on, no packet header and footer bytes are displayed. Only the packet content of 16 hexadecimal bytes per line and the corresponding ASCII per line is displayed.

1. In the **Event Analysis** view, go to the Packet Analysis panel of a network session.
   By default the session is reconstructed with the packet header, footer, and payload displayed.



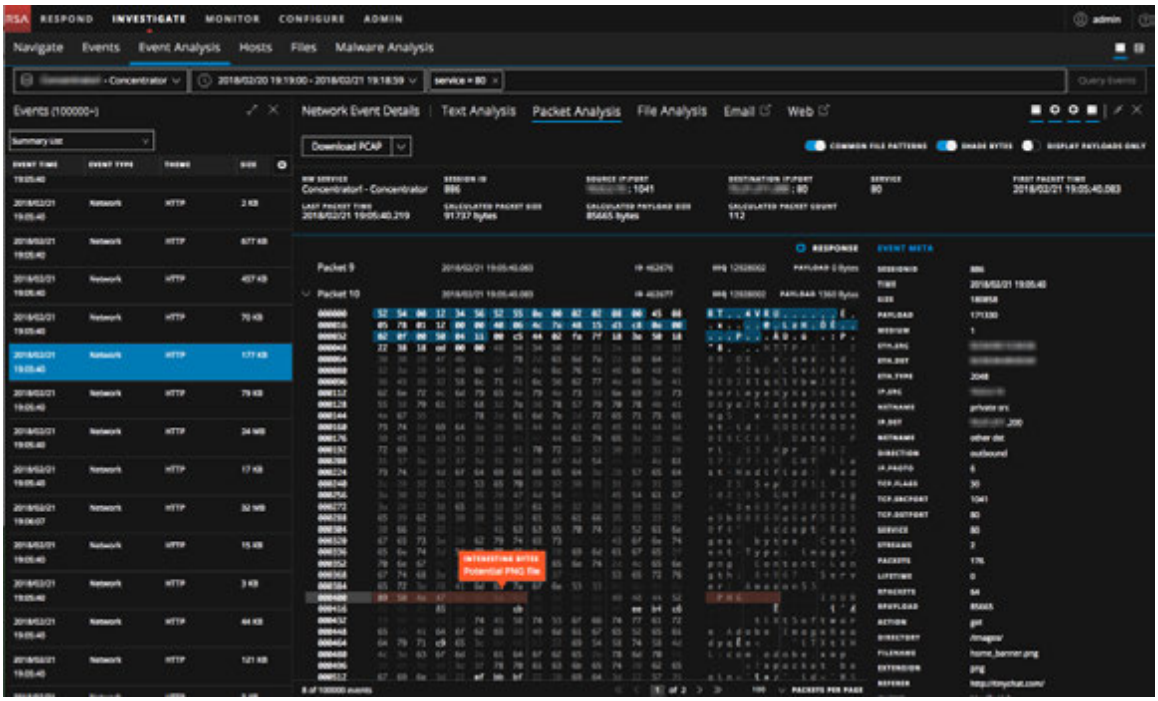
2. To change the view to show only the payload for each packet, click the **Display Payloads Only** toggle switch.
   The view changes to that only the payload is visible and contiguous same-side packets are

concatenated together to make the payload more readable and understandable.

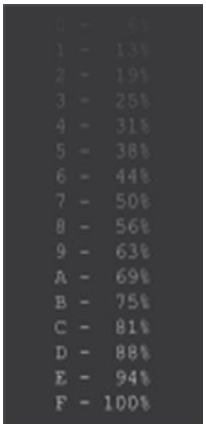


View Highlighted Bytes in the Packet Analysis Panel

When you first open a reconstruction in the Packet Analysis panel, the significant header bytes in each packet are highlighted in blue, and the payload bytes are distinguished using shading to help you understand the contents of the packet. This figure shows the default Packet Analysis with highlighting and byte shading.



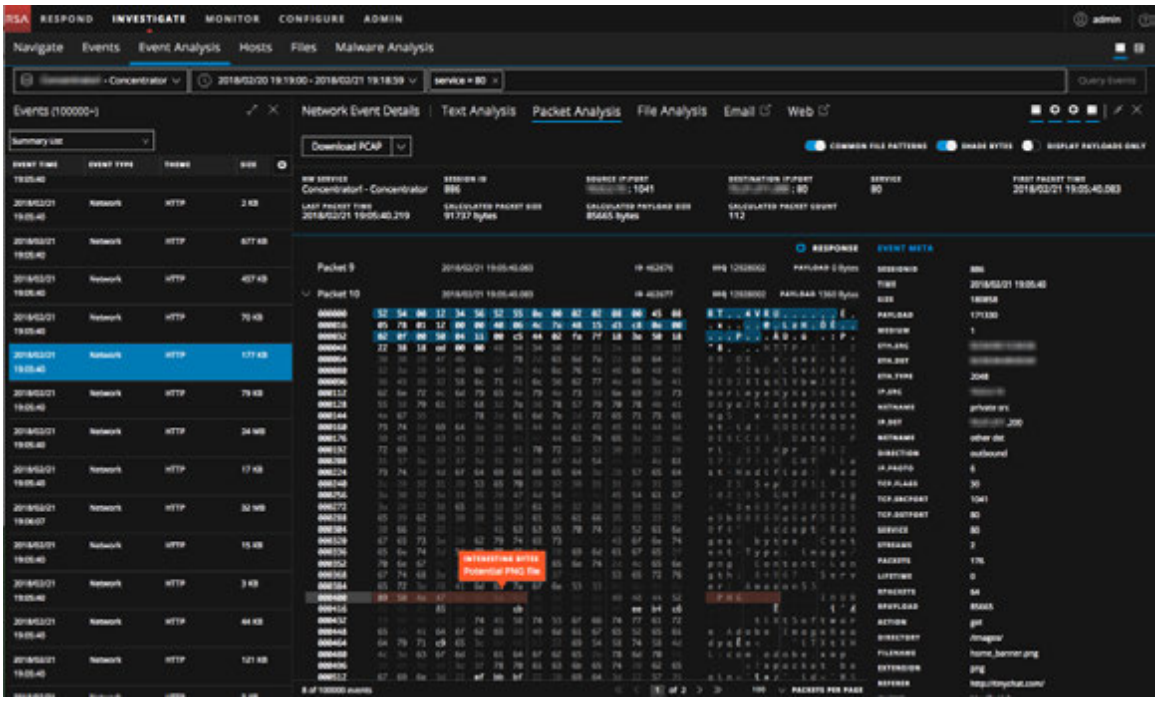
The Shade Bytes option adds shading to identify the different hexadecimal bytes (00 to FF) using degrees of highlighting. Bytes near the lower range are more transparent, and bytes near 255 are more opaque. Both hexadecimal and ASCII bytes are shaded. This is an example of the shading applied to each hexadecimal byte.



The Shade Bytes switch controls the shading of bytes. When you set Shade Bytes on or off, your setting persists until you change it or refresh the browser.

Highlight Common File Types in the Packet Analysis Panel

In the Packet Analysis panel, analysts can show or hide highlighting of certain common file types based on the file signature. When the Common File Patterns feature is turned on, the magic number bytes in the file signature are highlighted in the payload and you can hover over the highlighting to see the potential type of file. In this example, `89 50 4e 47` is highlighted in the hexadecimal payload and `PNG` is highlighted in the ASCII payload. When you hover over the highlighted bytes, the potential file type associated with the magic number is provided in a hover box.



These are the files types and corresponding magic numbers that are highlighted if present in the payload:

File Type	Hexadecimal Signature	ASCII Encoding
DOS Executable / Windows PE	4D 5A	MZ
Portable Network Graphics (PNG)	89 50 4E 47 0D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
Non-portable Executable	5A 4D	ZM
BMP	42 4D	BM

File Type	Hexadecimal Signature	ASCII Encoding
PDF	25 50 44 46	%PDF
Old Office Document (doc, xls, ppt, msg, and other)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
ZIP file formats and formats based on it, such as JAR, ODF, OOXML	50 4B	PK..
7-Zip File Format (7z)	37 7A BC AF 27 1C	7z¼¯'
Java Class File, Mach-O Fat Binary	CA FE BA BE	Êþº¾
Postscript	25 21 50 53	%!PS
Unix/Linux Shell script	23 21	#!
Executable and Linkable Format (ELF) executables	7F 45 4C 46	.ELF

To view common file signatures in the Packet Analysis panel:

1. Go to the Packet Analysis panel, and turn on the **Common File Patterns** option.
   If there is more then one highlight in view, all are shown.
2. To view the hover box, place the cursor over the highlighting.

Download Data in the Event Analysis View

In the Event Analysis view, you can download events, logs, and files.

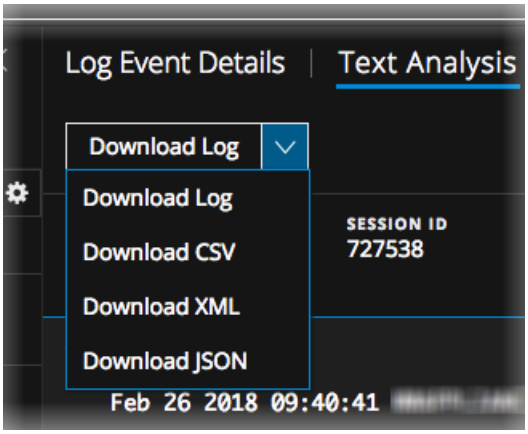
Download a Log in the Text Analysis Panel

When viewing a log reconstruction in the Text Analysis panel, you can download a log file in the following formats using options in the Download Log drop-down menu:

- Raw log (log) using the **Download Log** option
- Comma-separated values (CSV) using the **Download CSV** option
- Extensible Markup Language (XML) using the **Download XML** option
- JavaScript Object Notation (JSON) using the **Download JSON** option

Note: If you initiate a download and move away from the view while the log is being extracted and before the log starts to download, the log is not downloaded in your browser. A message notifies you that you can find the downloaded log in the job queue.

This is an example of a log reconstruction with the Download Log menu options displayed.



The downloaded log file contains the log and is named to help identify the service on which the log was collected, the session ID, and the file type.

Note: Long running or historically downloaded files are not downloadable.

This is an example of the filename for a raw log: **Concentrator_SID2.log**. The exported log file is named using the following convention:

`<service-ID or host name>_SID<n>.<filetype>`

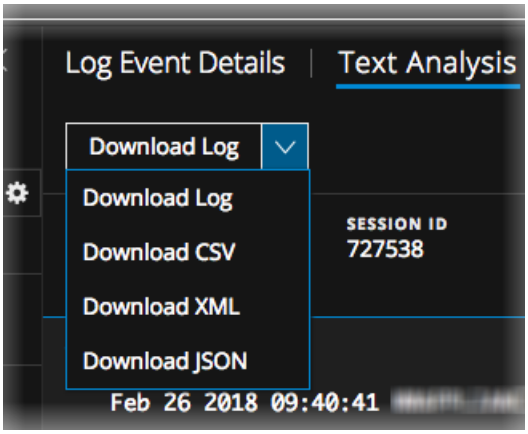
where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.
- `<filetype>` identifies the format of the downloaded log. These are the possible log types: raw log, CSV, XML, and JSON. By default the format is a raw log.

Note: Some formats do not have time stamps or the device IP where the event was generated, so a log downloaded in CSV, XML, or JSON format has an extra value called `timestamp` along with the raw log content. The additional information inside the log is in this form: `Log timestamp="1490824512" source="10.12.35.65"`.

To download the log for a session:

In the Text Analysis panel of a log event, select one of the file formats for the downloaded log.
-To download the log as a raw log (the default format), click **Download Log**.
-To download the log in one of the other formats, click the downward arrow on the **Download Log** button, and select one of the file formats for the downloaded log.



The log file is downloaded to your local file system in the format specified.

Download Network Event Data in the Text Analysis Panel or the Packet Analysis Panel

When viewing a reconstructed network event in the Packet Analysis panel or the Text Analysis panel, you can export network data files for further analysis. The download includes events for the current time range and drill point. You can download the data in these forms:

- The entire event as a packet capture (`*.pcap`) file using the **Download PCAP** option.
- The payload as a `*.payload` file using the **Download All Payloads** option.
- The request payload as a `*.payload1` file using the **Download Request Payload** option.
- The response payload as a `*.payload2` file using the **Download Response Payload** option.

This is an example of the filename for a PCAP file: `C01 - Concentrator_SID1697309.pcap`. The exported network data file is named using the following convention:

`<service-ID or host name>_SID<n>.<filetype>`

where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.
- `<filetype>` is pcap, payload, payload1, or payload2.

The network data is downloaded directly into your browser if the download is quick. If the download takes longer due to network factors or file size, the file is downloaded in the background and the task is tracked in the Jobs queue. In this case, you can check your jobs in the queue and get the file when the download is complete.

Note: If you initiate a download and move away from the view while the file is being extracted and before the file starts to download, the file is not downloaded in your browser. A message notifies you that you can find the downloaded document in the job queue.

To export an event as a network data file:

Go to the Packet Analysis panel of a network event, and select one of the file formats for the downloaded file.
-To download the event as a PCAP file (the default format), click **Download PCAP**.
-To download the event in one of the other formats, click the downward arrow on the **Download PCAP** button, and select one of the file formats for the downloaded event data.

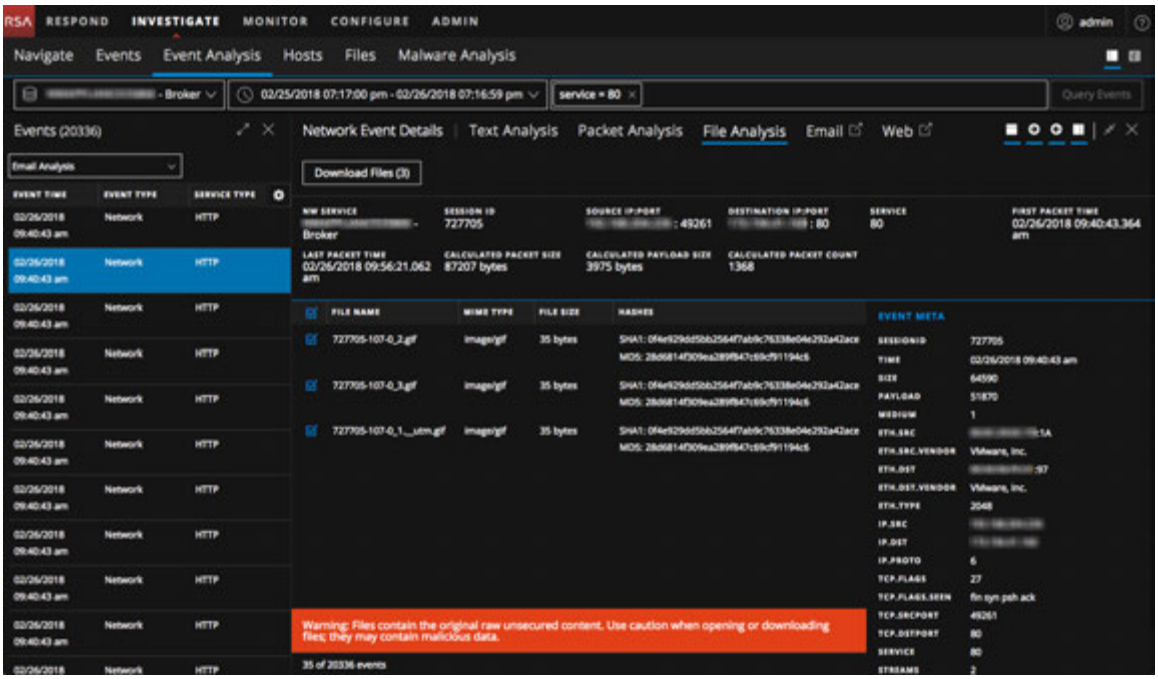
The network data file is downloaded to your local file system in the format specified.

Download Files from a Network Event in the File Analysis Panel

When viewing reconstructed network events that contain files in the File Analysis panel, you can select one file, one or more files, or all files to download to your local file system.

Note: If you initiate a download and move away from the view while the file is being extracted and before the file starts to download, the file is not downloaded in your browser. A message notifies you that you can find the downloaded file in the job queue.

When files are selected, the Download Files button becomes active and reflects the number of files selected.



Clicking the button exports the selected files as a password-protected zip archive. The password to open the exported archive is `netwitness`. Exporting the files in this form ensures that:

- The archive is not quarantined by antivirus software.
- Potentially malicious files are not automatically opened by the default application and executed.

This is an example of the filename for an archive: `C01 - Concentrator_SID1697309_FC1.zip`. The exported archive is named using the following convention:

`<service-ID or host name>_SID<n>_FC<n>.zip`

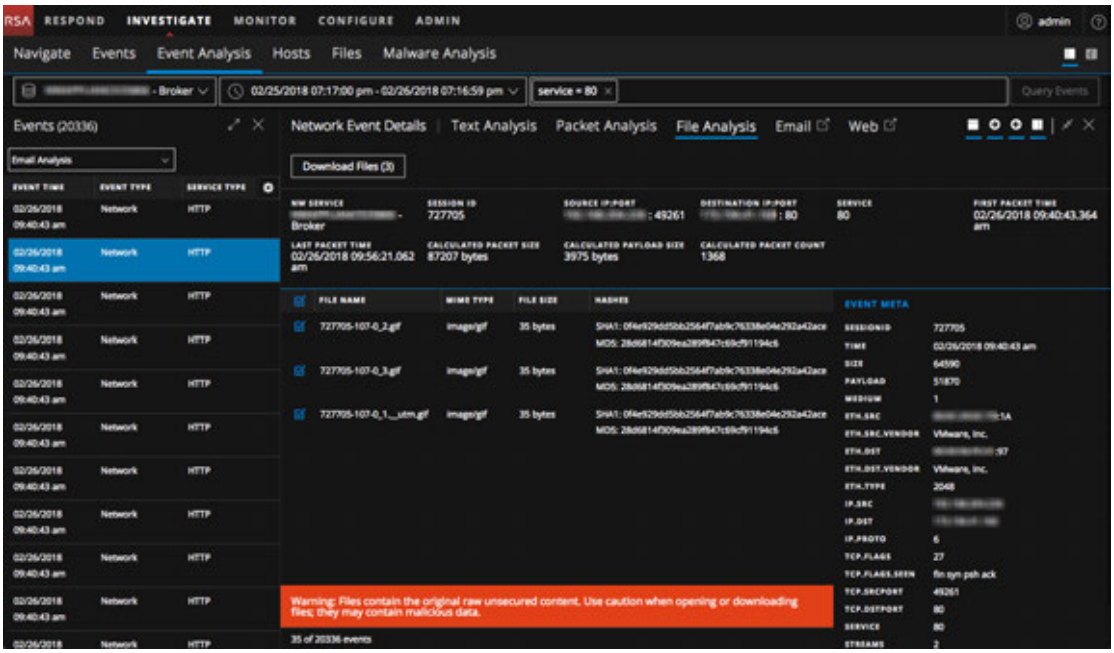
where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.
- `FC<n>` is the file count or number of files in the archive.

Caution: Caution is advised when unzipping and opening files that are associated with a default application; for example, an Excel spreadsheet may automatically open in Excel before you have a chance to verify it is safe.

To export files in a reconstructed event:

1. In the **Event Analysis** view, go to the File Analysis panel of an event that contains files.



2. Click one or more files that you want to extract, and click **Download Files**.
   The job is scheduled and when complete the selected file are downloaded, in the form of a password-protected zip archive, to the local file system.
3. To open the archive on your local file system, enter the following password when prompted: `netwitness`.

Act on Data in the Event Analysis View

When you have found data of interest in the Event Analysis view, you can do internal lookups to NetWitness Endpoint and RSA Live, as well as external lookups of meta values in community resources such as SANS IP History and ThreatExpert Search.

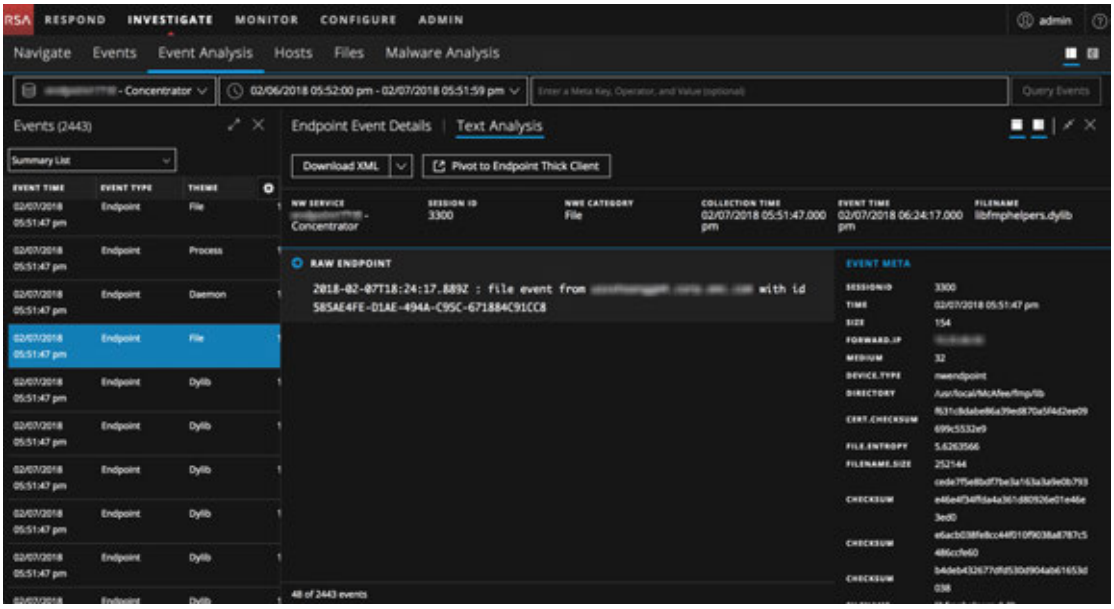
Open an Endpoint Event in the NetWitness Endpoint Thick Client

When viewing an endpoint event in the Text Analysis panel, you can pivot to analyze the same event in NetWitness Endpoint. The NWE thick client offers additional features beyond the built-inbcapabilities in NetWitness Endpoint Insights.

Note: Version 4.4 of the NetWitness Endpoint (NWE) thick client must be installed on the same server, the NWE meta keys must exist in the `table-map.xml` file on the Log Decoder, and the NWE meta keys must exist in the `index-concentrator-custom.xml` file. The NWE thick client is a Windows only application. Complete setup instructions are provided in the *NetWitness Endpoint User Guide* for Version 4.4.

To open an event in NetWitness Endpoint:

1. Starting from the Navigate view:
   a. In the **Query** drop-down, select **Advanced**, and enter one of the following queries: `nwe.callback_id exists` or `device.type='nwendpoint'`
      Endpoint data is displayed in the Values panel.
   b. Right-click an event, and select **Event Analysis** in the menu.
2. (Version 11.1 and later) Go to INVESTIGATE > Events Analysis. In **Query** drop-down, select **Advanced**, and enter one of the following queries: `nwe.callback_id exists` or `device.type='nwendpoint'`
   Endpoint data is displayed in the Events panel.
3. Select an event.
   The Event Analysis opens with the selected event displayed in the Text Analysis.



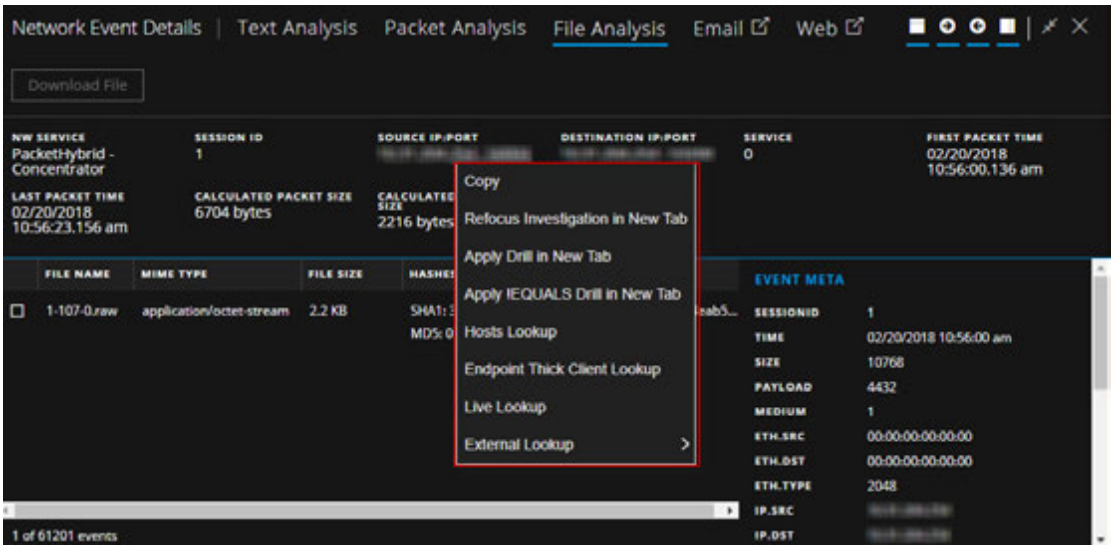
4. In the Event Header click **Pivot to Endpoint.**
   A new browser tab with the url `ecatui://<id>` opens and the NWE Thick Client is launched . If the NetWitness Endpoint Thick Client is not installed, no data is displayed and the following message is displayed: `Applicable for hosts with 4.x Endpoint`

```
agents installed, please install the NetWitness Endpoint Thick
Client.
```

Perform Lookups of Meta Values in Event Analysis

In the Event Analysis view you can further investigate meta values in an event by right-clicking certain meta values and using the options in a drop-down menu. Not all fields have right-click actions. To perform internal and external lookups:

1. In the Event Analysis view, right-click a meta value in the Events List, the Event Meta panel, or the Event Header. Some meta values have a drop-down menu.



2. Select one of the following internal lookups:

   Copy: Copies the meta value to the clipboard.

   Refocus Investigation in New tab: Launches the another investigation in a new tab with the focus on the selected meta value.

   Apply Drill in New Tab: Applies the drill and launches it in a new tab to drill the data in Navigate view.

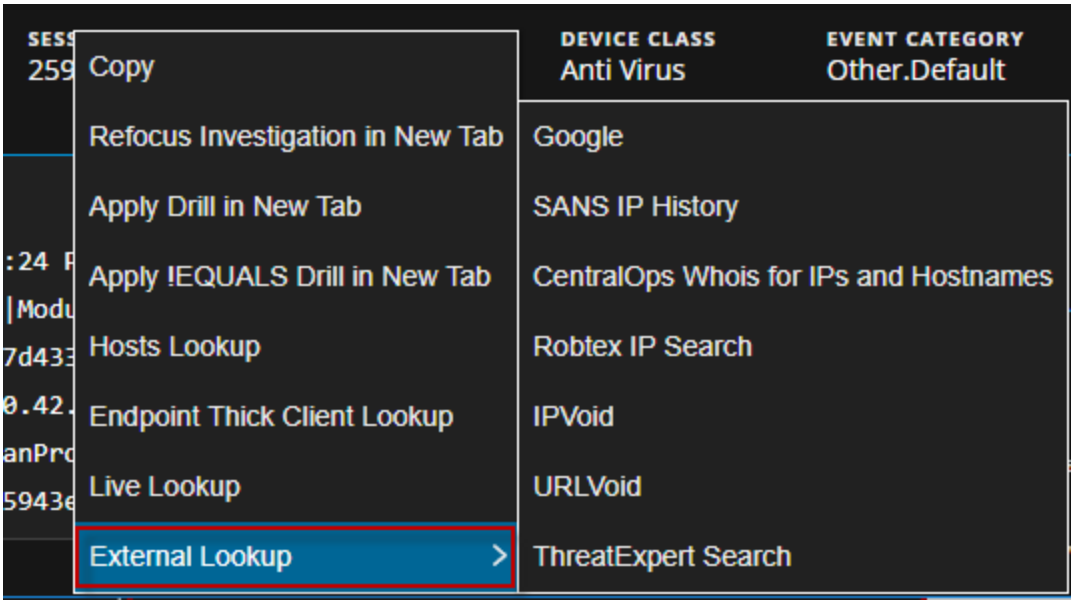
   Apply !EQUALS Drill in New Tab: Applies (!EQUALS) to the meta and launches a new tab, effectively excluding the meta value from the results.

   Hosts Lookup: Looks up the value in the Investigate > Hosts view.

   Endpoint Thick Client Lookup: Analyzes the meta value in the Endpoint Thick Client (for clients which have Endpoint Agent).

   Live Lookup: Looks up a meta value on Live for further analysis.

3. For an external lookup, hover over a meta value, right-click and select **External Lookup**.



4. In the submenu select one of the available external lookups:
   Google: Looks up a meta value on Google.com
   SANS IP History: Looks up a meta value on SANS IP History, domain = http://isc.sans.org/ipinfo.html?ip=ipaddress
   CentralOps Whois for IPs and Hostnames: Looks up a meta value on CentralOps Whois for IPs and Hostnames, domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true
   Robtex IP Search: Looks up a meta value on Robtext IP Search, domain = https://www.robtex.com/cidr/domain.ipaddress
   IPVoid: Looks up a meta value on IPVoid, domain = http://www.ipvoid.com/scan/domain/
   URLVoid: Looks up a meta value on URLVoid, domain = http://www.urlvoid.com/scan/ipaddress/
   ThreatExpert Search: Looks up an IP meta value on ThreatExpert Search, domain = http://www.threatexpert.com/reports.aspx?find=IP address

Investigating Hosts and Files

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

Analysts can use the RSA NetWitness Suite Hosts and Files views to investigate hosts or files.

Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles and permissions as described in Roles and Permissions for Endpoint Analysts. For more information on roles and permissions, see *System Security and User Management Guide*.

Analysts can:

- Investigate Hosts
- Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts
- Investigate Files

Investigate Hosts

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

To conduct an investigation on hosts:

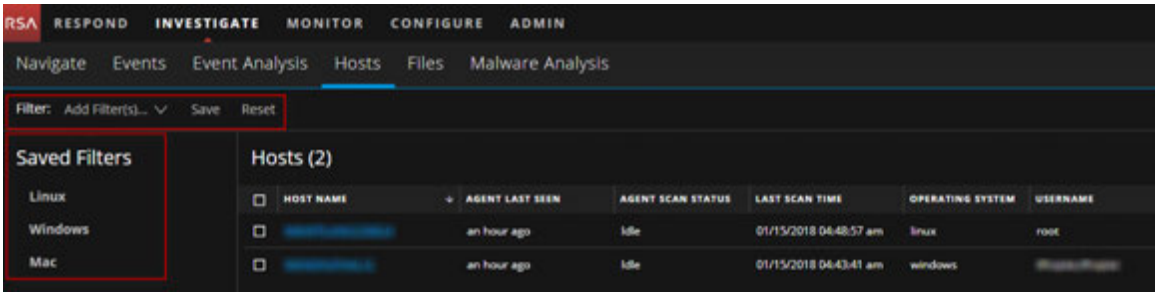
1. Go to **INVESTIGATE > Hosts**.
   A list of hosts is displayed.
2. Select the hosts that you want to scan and click **Start Scan**. For more information, see Investigate Hosts.
3. After completing the process of scanning the hosts, click the host name to investigate the scan results. For more information, see Investigate Hosts.

Note: To investigate NetWitness Endpoint 4.4 hosts, see Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts.

Filter Hosts

You can filter hosts on the operating system or select the fields in the Add Filter drop-down menu.

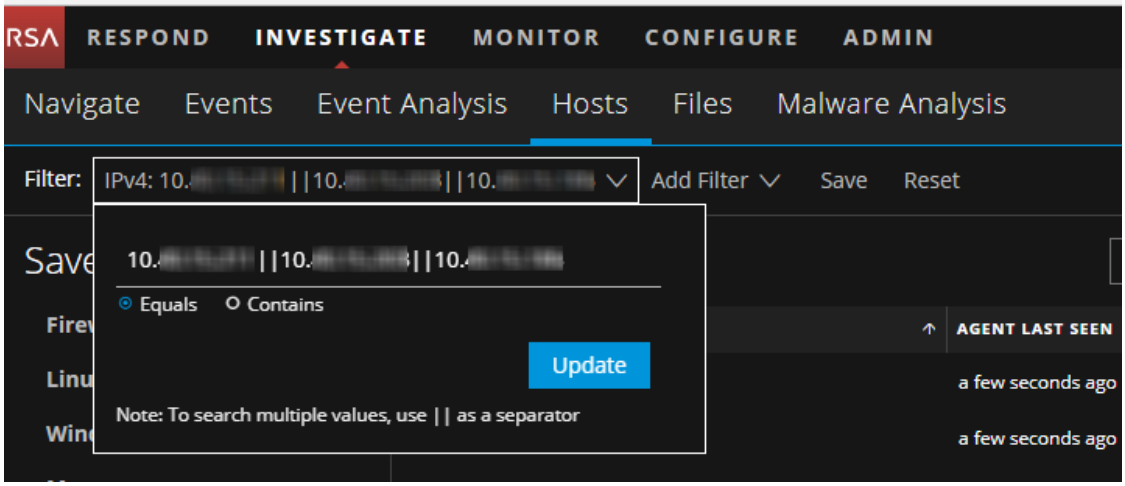
Note: While filtering on a large amount of data, use at least one indexed field with the `Equals` operator for better performance. The following fields are indexed in the database - `Hostname`, `IPV4`, `Operating System`, and `Last Scan Time`.



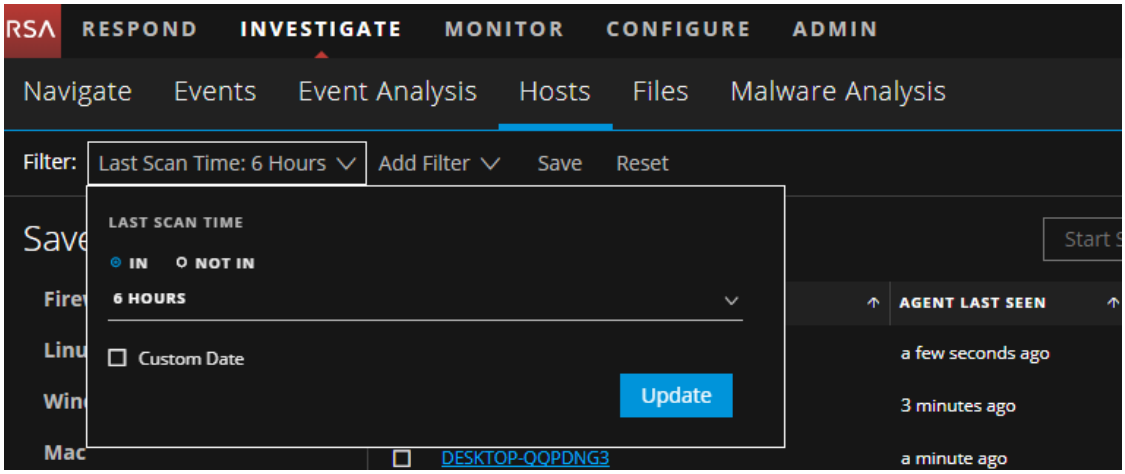
To search multiple values within a field, set the filter option to `Equals`, and use `||` as a separator.

For example,

- Using `Equals` operator for multiple IPV4 values with a separator `||`.



- Using `IN` operator for Last Scan Time to filter agents that are scanned in the last 6 hours.



Click **Save** to save the search and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the name and click .

Note: Special characters are not allowed except underscore (_) and hyphen (-) while saving the filter.

Scan Hosts

You can either perform an on-demand scan or schedule a scan to run daily or weekly. For information on scheduling a scan, see *RSA NetWitness Endpoint Insights Configuration Guide*.

Note: You cannot perform a scan for the NetWitness Endpoint 4.4 agents from the NetWitness Suite user interface.

On-demand Scan

You may want to perform an on-demand scan if:

- A file in the Global Files section is found to be malicious.
- A malicious file is present on different hosts in the network.
- You want to investigate a host that is infected.
- Get the latest snapshot of the host.

When the hosts are scanned, the Endpoint Agent retrieves the following data that can be used for investigation:

- Drivers, processes, DLLs, files (executables), services, and autoruns running on the host.
- Host file entries and scheduled tasks.
- System information such as network share, installed Windows patches, Windows tasks, logged-in users, bash history, and security products installed.

To start a scan:

1. Go to **INVESTIGATE > Hosts**.
2. Select one or more hosts (up to 100) at a time for on-demand scan, and click **Start Scan**.
3. Click **Start Scan** in the dialog.
   This performs a quick scan of all executable modules loaded in memory. It takes approximately 10 minutes.

The following are the scan statuses:

Status	Description
Idle	No scan is in progress.
Scanning	Scan is in progress.
Starting Scan	Scan request is sent to the server but the agent will receive the request the next time it communicates with the server.
Stopping Scan	Stop request is sent to the server but the agent will receive the request the next time it communicates with the server.

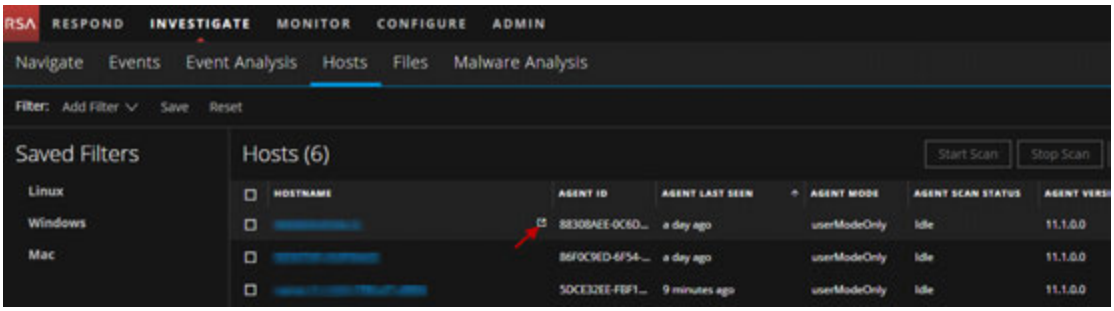
Pivot to the Navigate and Event Analysis Views

If you need to investigate a particular host, IP address (IPV4), or username to look for related activity across a time range, you can pivot to both the Navigate and Event Analysis views to get the entire context of the activity. By default the time range is set to 1 day. You can change the time range accordingly.

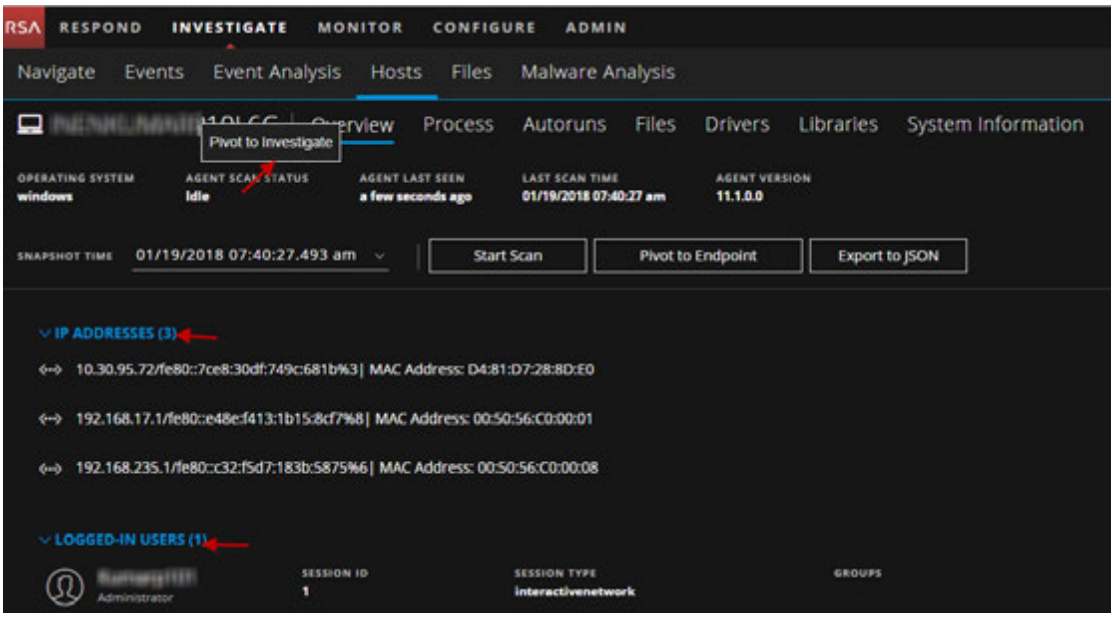
Note: Pivoting to the Navigate or Event Analysis view is not supported for IPV6.

To pivot to the Navigate or Event Analysis view:

1. Go to **INVESTIGATE > Hosts** or **INVESTIGATE > Files**.
2. Click beside the Hostname.



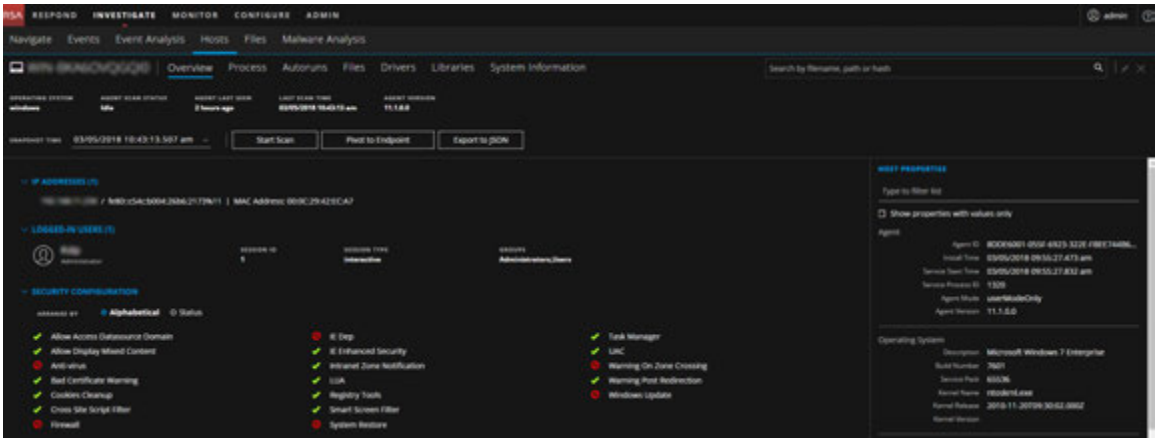
Alternately, in the Overview tab, you can right-click on host name, IP address (IPV4), or logged-in users to pivot.



3. In the Select Service dialog, select any of the services required for investigation.
4. Click **Navigate** or **Event Analysis** to analyze the data.

Investigate Host Details

To look for suspicious files on a host, click the host name and view the details of the host, or start an on-demand scan to get the most recent information.



Search on Snapshots

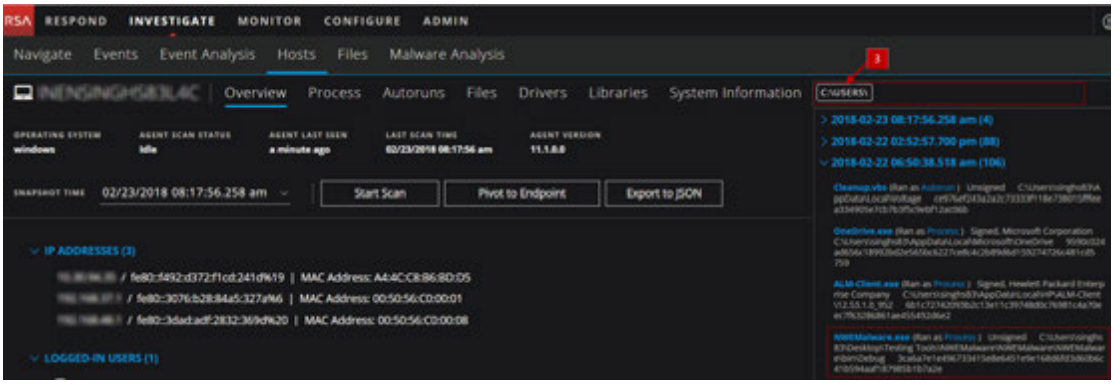
To investigate a host or to check if it is infected with a known malware, you can search for occurrences of the file name, file path, or SHA-256 checksum.

Note: To search for a SHA-256 checksum, provide the entire hash string in the search box.

The result displays details, such as file name, signature information, along with its interaction with the system (ran as process, library, autorun, service, task, or driver). To view more details for these results, click on the category.

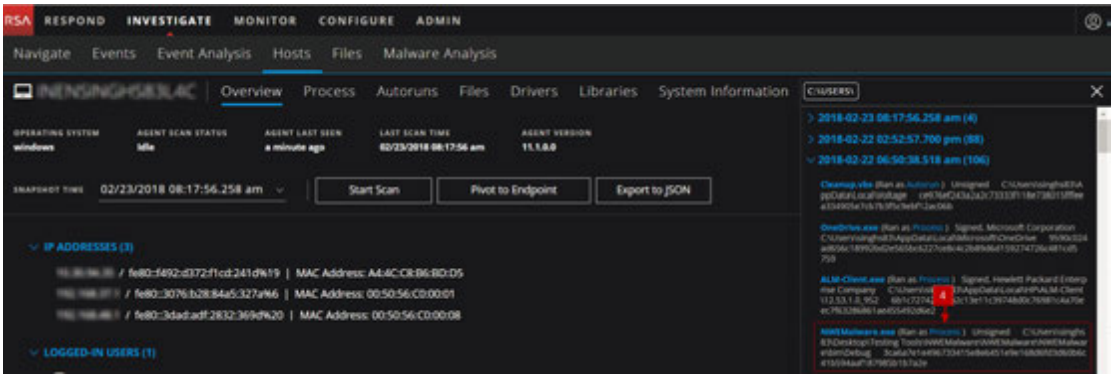
For example, a user has clicked and executed a malicious attachment through a phishing email, and downloaded it to `C:\Users`. To investigate this file:

1. Go to **INVESTIGATE > Hosts**.
2. Select the host that you want to investigate.
3. In the **Overview** tab, enter the file path `C:\Users` in the search box.
   The search displays all the executables in this folder. In this example, the file `NWEMalware.exe`, is an unsigned file that might be malicious.



This file has run as a Process.

4. To view details of this file, click `Process` in the result.
   This opens the Process tab where you can view the process details.



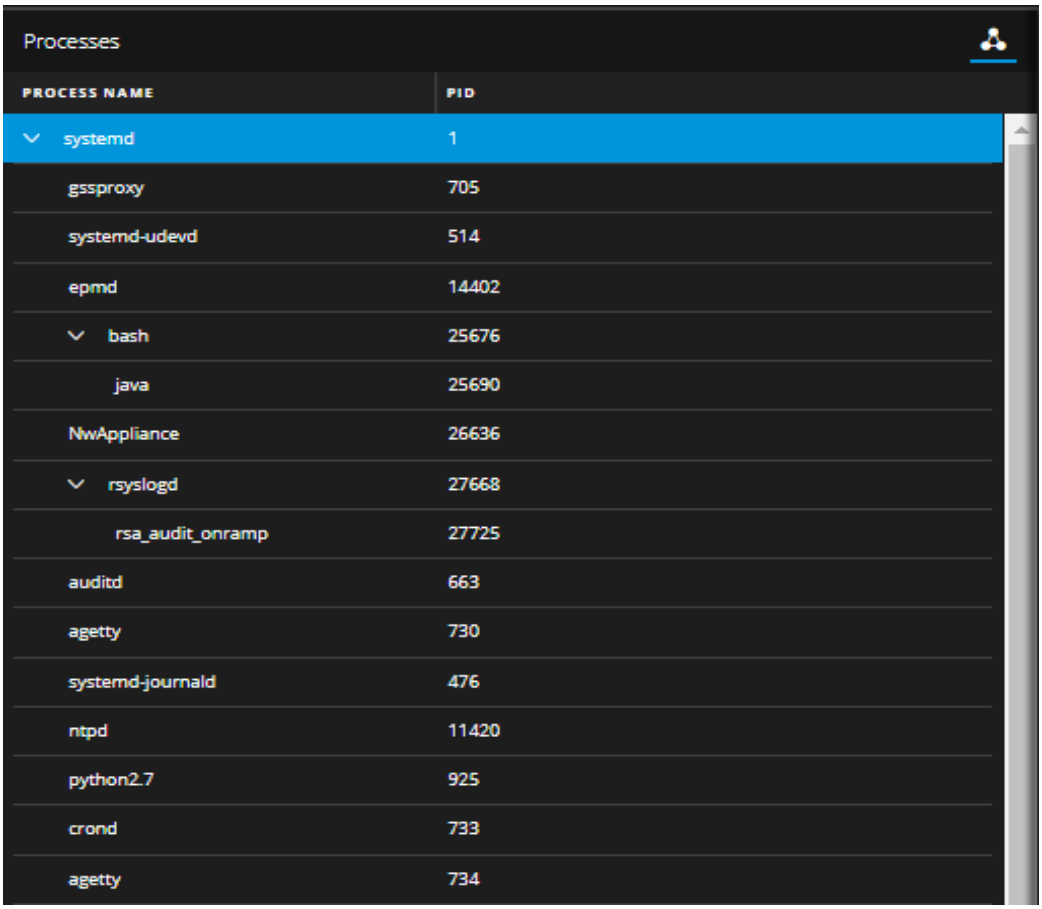
Analyze Processes

In the Hosts view, select the **Process** tab. You can view the processes that were running for the selected host at the time of scan. The process name and process ID (PID) columns are displayed either as a:

- Tree view - You can drill down to each process and view the child or parent process associated with it.
- List view - You can sort the process name and PID columns.

Click ⁂ to switch the views.

The following is an example of the tree view:



When reviewing processes, it is important to see the Launch Arguments. Even legitimate files can be used for malicious purposes, so it is important to view all of them to determine if there is any malicious activity.

For example,

- `rundll32.exe` is a legitimate Windows executable that is categorized as a good file. However, an adversary may use this executable to load a malicious DLL. Therefore, when viewing processes, you must view the arguments of the `rundll32.exe` file.
- `LSASS.EXE` is a child to `WININIT.EXE`. It should not have child processes. Often malware use this executable to dump passwords or mimic to hide on a system (`lass.exe`, `lssass.exe`, `lsasss.exe`, and so on).
- Most legitimate user applications like Adobe, Web browsers, and so on do not spawn child processes like `cmd.exe`. If you encounter this, investigate the processes.

Analyze Autoruns

In the Hosts view, select the **Autoruns** tab. You can view the autoruns, services, tasks, and cron jobs that are running for the selected host.

For example, in the Services tab, you can look for the file creation time. The compile time is found within each portable executable (PE) file in the PE header. The time stamp is rarely tampered with, even though an adversary can easily change it before deploying to a victim's endpoint. This time stamp can indicate if a new file is introduced. You can compare the time stamp of the file against the created time on the system to find the difference. If a file was compiled a few days ago, but the time stamp of this file on the system shows that it was created a few years ago, it indicates that the file is tampered.

Analyze Files

In the Hosts view, select the **Files** tab. You can view the list of files scanned on the host at the time of scan. By default, the table displays 100 files. To display more files, click **Load More** at the bottom of the page.

For example, many trojans write random filenames when dropping their payloads to prevent an easy search across the endpoints in the network based on the filename. If a file is named `svch0st.exe`, `scvhost.exe`, or `svchosts.exe`, it indicates that the legitimate Windows file named `svchost.exe` is being mimicked.

Analyze Libraries

In the Hosts view, select the **Libraries** tab. You can view the list of libraries loaded at the time of scan.

For example, a file with high entropy gets flagged as packed. A packed file means that it is compressed to reduce its size (or to obfuscate malicious strings and configuration information).

Analyze Drivers

In the Hosts view, select the **Drivers** tab. You can view the list of drivers running on the host at the time of scan.

For example, using this panel, you can check if the file is signed or unsigned. A file that is signed by a trusted vendor such as Microsoft and Apple, with the term `valid`, indicates that it is a good file.

Analyze System Information

In the Hosts view, select the **System Information** tab. This panel lists the agent system information. For Windows operating system, the panel displays the host file entries and network shares of that host.

For example, malware might use host file entries to block antivirus updates.

Delete a Host

To delete hosts manually from the UI:

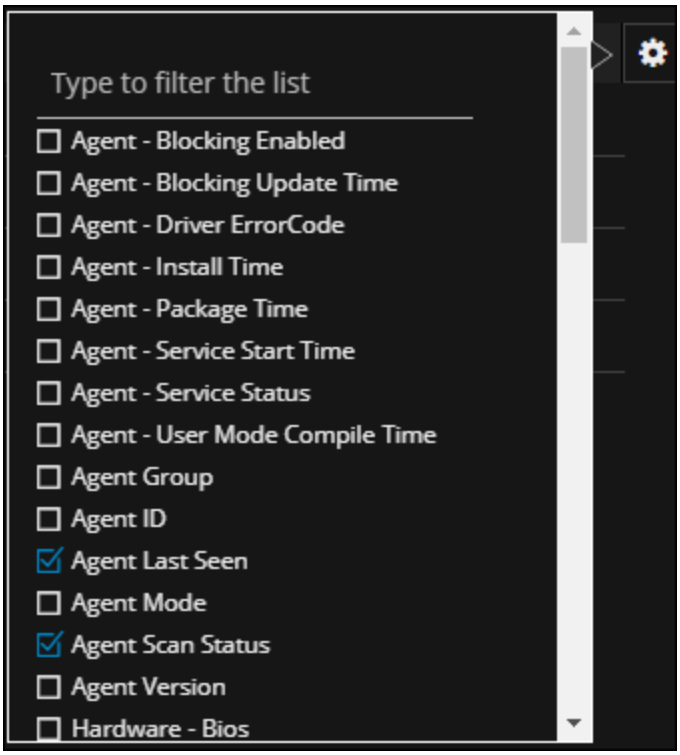
1. Go to **INVESTIGATE > Hosts**.
2. Select the hosts that you want to delete from the Hosts view and click **Delete**.
   This deletes all the collected Endpoint data for the selected hosts.

Note: If you accidentally delete a host from the Hosts view, the Endpoint Server forbids all requests from this agent. The agent must be uninstalled manually from the host and reinstalled for it to appear on the Hosts view.

Set Hosts Preference

By default, the Hosts view displays a few columns and the hosts are sorted based on the last scan time. If you want to view specific columns and sort data on a specific field:

1. Go to **INVESTIGATE > Hosts** view.
2. Select the columns by clicking in the right-hand corner. The following example shows the screen displayed while adding columns:



3. Sort the data on the required column.

Note: This is set as your default view every time you log in to the Hosts view.

Export Host Attributes

You can export up to 100k host attributes at a time. To extract the host attributes to a comma-separate values (csv) file.

1. Go to **INVESTIGATE > Hosts**.
2. Filter the hosts by selecting the required filter options.
3. Add columns by clicking in the right-hand corner.
4. Click **Export to CSV**.

You can either save or open the csv file.

Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

If you have NetWitness Endpoint 4.4.0.2 or later in your deployment, you can view the endpoint data of these hosts in the **INVESTIGATE > Hosts** and **INVESTIGATE > Files** views.

If you do not see the NetWitness Endpoint 4.4.0.2 hosts listed here, see "Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1" in the *RSA NetWitness Endpoint Insights Configuration Guide*.

The NetWitness Endpoint 4.4.0.2 hosts can be identified in the Hosts View using the Agent Version. You cannot perform an on-demand scan on these hosts. To investigate these hosts, you must use the NetWitness Endpoint 4.4.0.2 or later user interface.

Note: To pivot to the thick client from the NetWitness Suite user interface, the NetWitness Endpoint 4.4.0.2 or later must be installed.

To investigate a host in the NetWitness Endpoint user interface:

1. Go to **INVESTIGATE > Hosts**.
2. Select the 4.4 host from the table.
3. Click **Pivot to Endpoint**.

Note: The **Pivot to Endpoint** option is not applicable for the NetWitness Endpoint Insights11.1 hosts.

Investigate Files

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

Analysts can use the Files view (**INVESTIGATE > Files**) to identify suspicious files by examining the file name, file size, entropy, format, company name, signature, and checksum.

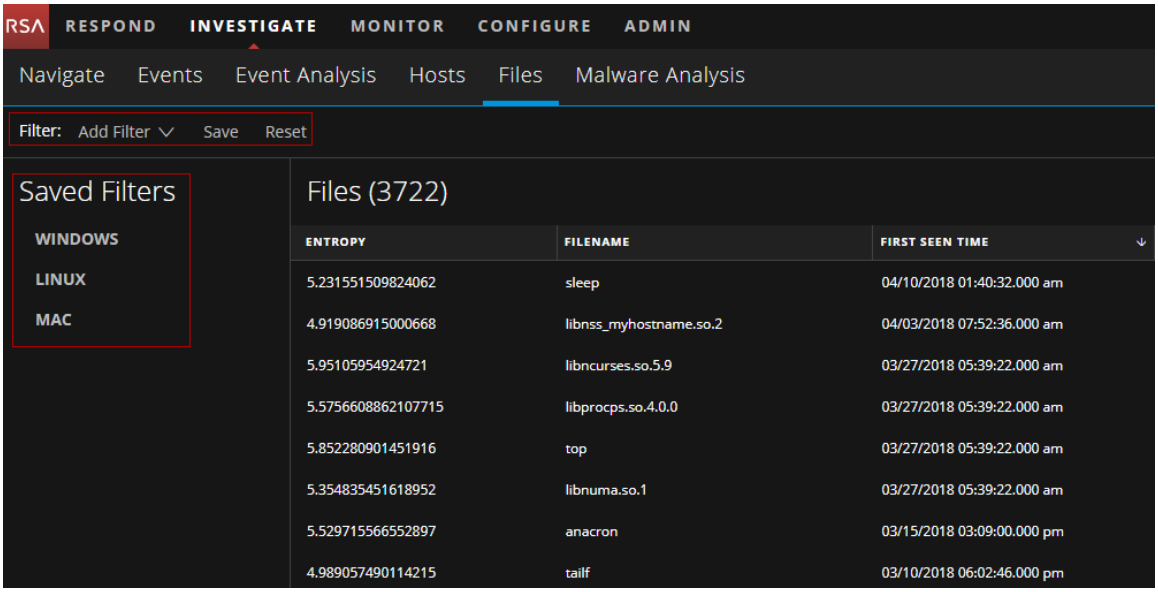
For example, when looking at a file name, if an environment is infected by the WannaCry ransomware, using this file name, the analyst can filter the list. You can also look for this ransomware using the checksum.

The file size can be an indicator when assessing a file. Trojans are usually less than 1 MB, and the majority of them are less than 500 KB.

Filter Files

You can either filter the files on the operating system, or select the fields in the Add Filter drop-down menu.

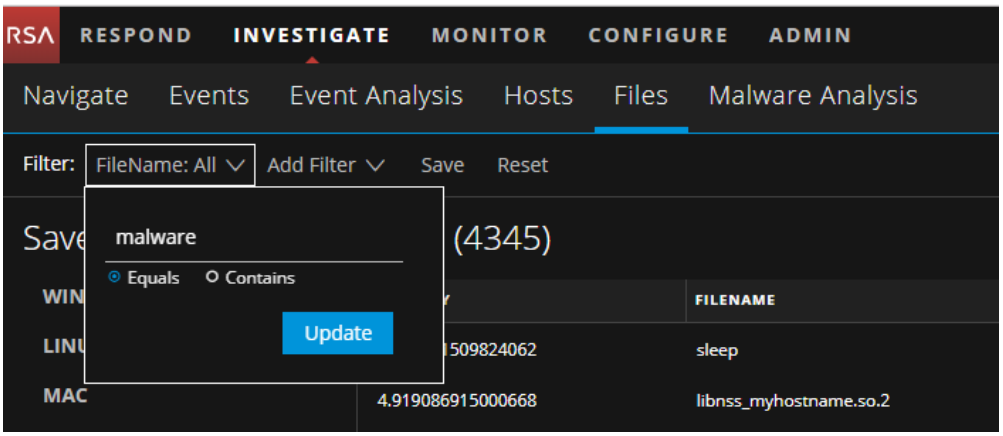
Note: While filtering on a large data set, use at least one indexed field with the `Equals` operator for better performance. The following fields are indexed in the database - Filename, MD5, Operating System, First Seen Time, and Format.



Click **Save** to save the search and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the name and click .

Note: Special characters are not allowed except underscore (_) and hyphen (-) while saving the filter.

For example, filtering files with the filename `malware` using the `Equals` operator.



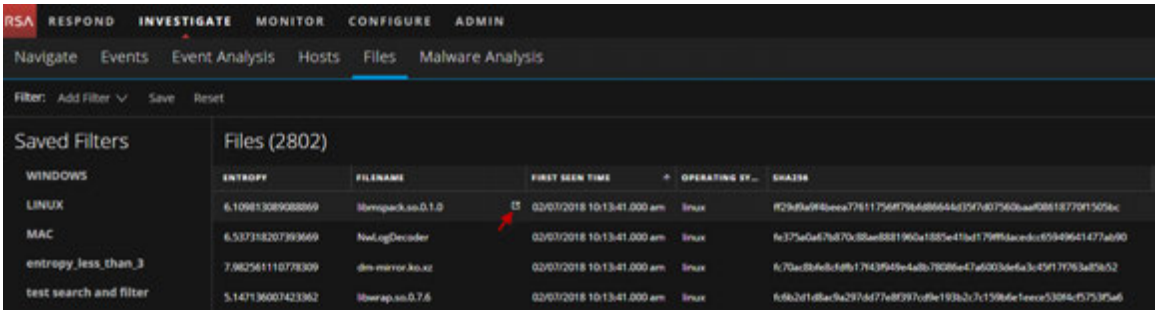
Note: For the file size, 1 KB is calculated as 1024 bytes. For example, if the actual size of the file is 8421 bytes, the UI will display it as 8.2 KB instead of 8.22 KB. It is recommended to search using the bytes format when using the `Equals` operator.

Pivot to Navigate and Event Analysis Views

If you need to investigate a particular filename or hash (SHA256 and MD5) in the global files to look for related activity across a time range, you can pivot to both the Navigate and Event Analysis views to get the entire context of the file. By default the time range is set to 1 day. You can change the time range accordingly.

To pivot to Navigate or Event Analysis view:

1. Go to **INVESTIGATE > Files**.
2. Click beside the Filename or Hash.



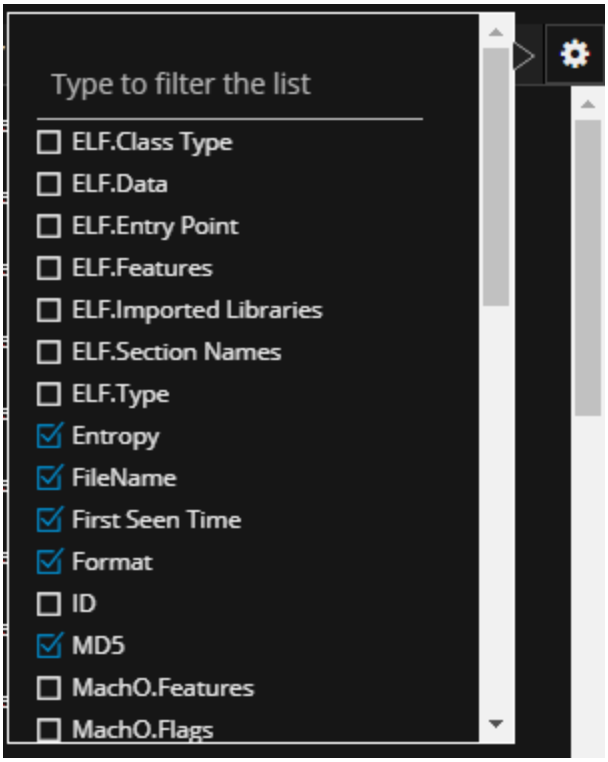
3. In the Select Service dialog, select any of the services required for investigation.
4. Click **Navigate** or **Event Analysis** to analyze the data.

Note: While pivoting to the Navigate or Event Analysis view, if the values are not indexed, the results take time to load. For more information, see Troubleshooting NetWitness Investigate.

Set Files Preference

By default, the Files view displays a few columns and the files are sorted based on the first seen time. If you want to view specific columns and sort data on a specific field:

1. Go to **INVESTIGATE > Files**.
2. Select the columns by clicking in the right-hand corner. The following example shows the screen displayed while adding columns:



3. Sort the data on the required column.

Note: This is set as your default view every time you log in to the Files view.

Export Global Files

To extract the list of global files to a CSV file.

Note: While filtering on a large data set, use at least one indexed field with the `Equals` operator for better performance. You can export up to 100k files at a time.

1. Go to **INVESTIGATE > Files**.
2. Filter the files by selecting the required filter option.
3. Add columns by clicking in the right-hand corner.
4. Click **Export to CSV**.

You can either save or open the CSV file.

Conducting Malware Analysis

Analysts can use the RSA NetWitness Suite Malware Analysis service to detect malware in selected data and files.

Analysts who conduct analyses using NetWitness Suite Malware Analysis need to have the appropriate system roles and permissions set up for their user accounts.

The following procedures provide instructions for using Malware Analysis:

- Begin a Malware Analysis Investigation.
- Upload Files for Malware Analysis Scanning.
- Implement Custom YARA Content.
- Filter Dashlet Data in the Summary of Events View.
- Examine Scan Files and Events in List Form
- View Detailed Malware Analysis of an Event.

Malware Analysis Functions

NetWitness Suite Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows portable executable (PE), PDF, and MS Office) to assess the likelihood that a file is malicious.

Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- Network Session Analysis (network)
- Static File Analysis (static)
- Dynamic File Analysis (sandbox)
- Security Community Analysis (community)

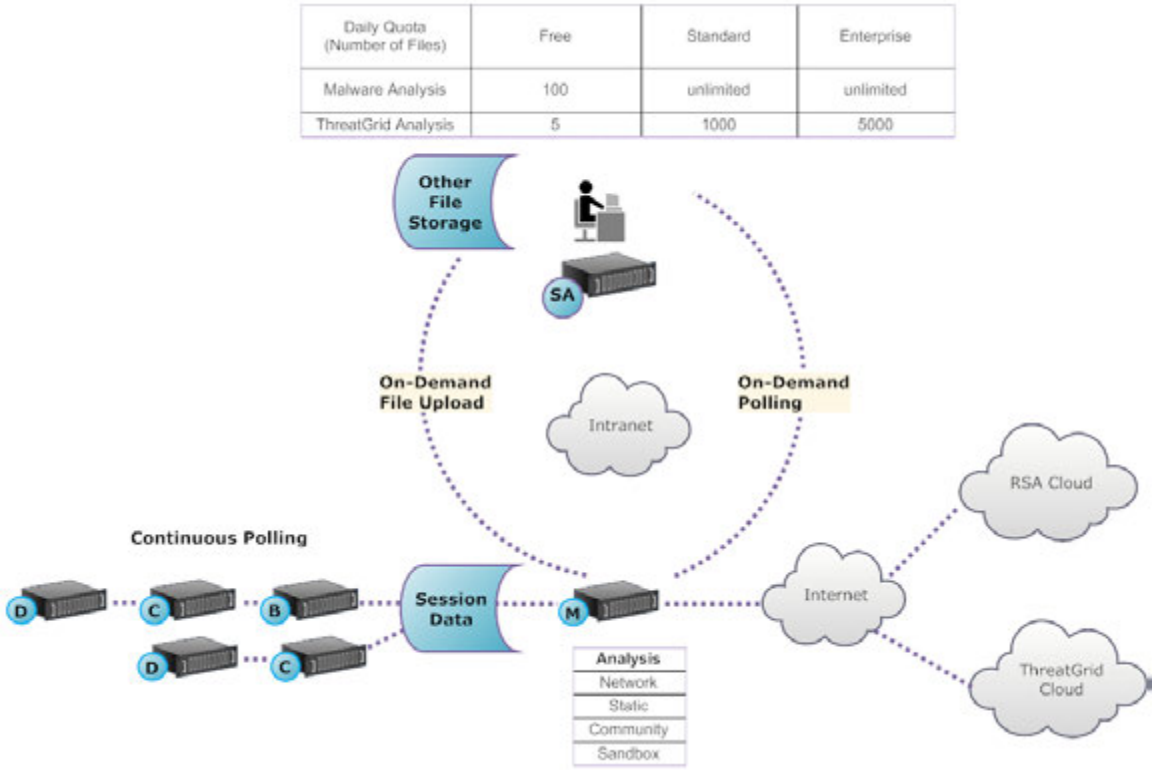
Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language, which allows malware researchers to identify and classify malware samples. This allows IOC authors to add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live. These YARA-based IOCs in RSA Live will automatically be downloaded and activated on the subscribed host, to supplement the existing analysis that is performed in each analyzed file.

Malware Analysis also has features that support alerts for Incident Management.

Functional Description

This figure depicts the functional relationship between the Core services (the Decoder, Concentrator, and Broker), the Malware Analysis service, and the NetWitness Server.



The Malware Analysis service analyzes file objects using any combination of the following methods:

- **Continuous automatic polling of a Concentrator or Broker** to extract sessions identified by a parser as potentially carrying malware content.
- **On-demand polling of a Concentrator or Broker** to extract sessions identified by a malware analyst as potentially carrying malware content.
- **On-demand upload of files** from a user-specified folder.

When automatic polling of a Concentrator or Broker is enabled, the Malware Analysis service continuously extracts and prioritizes executable content, PDF documents, and Microsoft Office documents on your network, directly from data captured and analyzed by your Core service. Because the Malware Analysis service connects to a Concentrator or Broker to extract only those executable files that are flagged as possible malware, the process is both rapid and efficient. This process is continuous and does not require monitoring.

When on-demand polling of a Concentrator or Broker is chosen, the malware analyst uses Investigation to drill into captured data and choose sessions to be analyzed. The Malware Analysis service uses this information to automatically poll the Concentrator or Broker and to download the specified sessions for analysis.

On-demand upload of files provides a method for the analyst to review files captured external to the Core infrastructure. The malware chooses a folder location and identify one or more files to be uploaded and analyzed by Malware Analysis. These files are analyzed using the same methodology as files automatically extracted from network sessions.

Analysis Method

For the Network analysis, the Malware Analysis service looks for characteristics that seem to deviate from the norm, much as an analyst does. By looking at hundreds to thousands of characteristics and combining the results into a weighted scoring system, legitimate sessions that coincidentally have a few abnormal traits are dismissed, while the actual bad ones are highlighted. A user can learn patterns that indicate anomalous activity in the sessions as indicators that warrant further investigation, Indicators of Compromise.

The Malware Analysis service can perform Static analysis against suspicious objects it finds on the network and determine whether those objects contain malicious code. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. For Sandbox analysis, the services can also push data into major security, information and event management (SIEM) hosts (the ThreatGrid Cloud).

Malware Analysis has a unique method for analysis that is partnered with industry leaders and experts, so their technologies can enrich the Malware Analysis scoring system.

NetWitness Server Access to the Malware Analysis Service

The NetWitness Server is configured to connect to the Malware Analysis service and import tagged data for deeper analysis in Investigation. Access is based on three subscription levels.

- Free subscription: All NetWitness Suite customers have a free subscription, with a free trial key for ThreatGrid analysis. The Malware Analysis service is rate-limited to 100 file samples per day. The number of samples (within the set of files from above) submitted to the ThreatGrid Cloud for sandbox analysis is limited to 5 per day. If one network session had 100 files in it, customers would hit the rate limit after processing the one network session. If 100 files were manually uploaded, that would cause the rate limit to be reached.
- Standard subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 1000 per day.
- Enterprise subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 5000 per day.

Scoring Method

By default, the Indicators of Compromise (IOC) are tuned to reflect industry best practices. During analysis, the IOCs that trigger cause the score to move upward or downward to indicate the likelihood that the sample is malicious. The tuning of IOCs is exposed in NetWitness Suite so that the malware analyst can choose to override the assigned score or to disable an IOC from being evaluated. The analyst has the flexibility to either use the default tuning, or to completely customize the tuning to specific needs.

YARA-based IOCs are interleaved with the built-in IOCs within each built-in category and are not distinguished from native IOCs. When viewing IOCs in the Service Configuration view, administrators can select YARA from the Module selection list to see a list of YARA rules.

After a session is imported into NetWitness Suite, all of the viewing and analysis capabilities in Investigation are available to further analyze Indicators of Compromise. When viewed in Investigation, YARA IOCs are distinguished from the built-in native IOCs by the tag `Yara rule`.

Deployment

The Malware Analysis service is deployed as a separate RSA Malware Analysis host. The dedicated Malware Analysis host has an onboard Broker which connects to the Core infrastructure (either another Broker or a Concentrator). Prior to this connection, a collection of parsers and feeds must be added to the Decoders that are connected to the Concentrators and Brokers from which the Malware Analysis service pulls data. This allows suspicious data files to be marked for extraction. These files are `malware analysis` tagged content available through the RSA Live content management system.

Malware Scoring Modules

RSA NetWitness Suite Malware Analysis analyzes and scores sessions and the embedded files within these sessions by scoring four categories: Network, Static Analysis, Community, and Sandbox. Each category comprises many individual rules and checks that are used to calculate a score between 1-100. The higher the score, the more likely the session is to be malicious and worthy of more in-depth follow-on investigation.

Malware Analysis can facilitate a historical investigation into events leading up to a network alarm or incident. If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections. You can also modify behavior for each scoring category based on the scoring category or the file type (Windows PE, PDF, and Microsoft Office).

Once you become familiar with data navigation methods, you can explore the data more completely through:

- Searching for specific types of information
- Reviewing specific content in detail.

Category scores for Network, Static Analysis, Community, and Sandbox are maintained and reported independently. When events are viewed based on the independent scores, as long as one category detects malware, it is evident in the Analysis section.

Network

The first category examines each core network session to determine if the delivery of the malware candidates was suspicious. For example, benign software being downloaded from a well-known safe site, using proper ports and protocols, is considered less suspicious than downloading software known to be malicious from a known dubious download site. Sample factors used in the scoring of this criteria set may include sessions that:

- Contain threat feed information
- Connect to well-known bad sites
- Connect to high-risk domains/countries (for example, .cc domain)
- Use well-known protocols on non-standard ports
- Contain obfuscated JavaScript

Static Analysis

The second category analyzes each file in the session for signs of obfuscation in order to predict the likelihood of the file behaving maliciously if allowed to run. For example, software that links to networking libraries is more likely to perform suspicious network activity. Sample factors used in the scoring of this criteria set may include:

- Files found to be XOR encoded
- Files found embedded within non-EXE formats (for example, PE file found embedded in a GIF format)
- Files linking to higher risk import libraries
- Files highly deviating from the PE Format

Community

The third category scores the session and files based on the collective knowledge of the security community. For example, files whose fingerprint/hash is already known to be good or bad by respected anti-virus (AV) vendors is scored accordingly. Files are also scored based on knowledge that a file was delivered from a site known to be good or bad by the security community.

Community scoring also indicates whether the AV on your network flagged the files as malicious. It does not indicate that the resident AV product acted to protect your system.

Sandbox

The fourth category examines the behavior of the software by actually running it in a sandbox environment. By running the software to watch its behavior, a score can be calculated by identifying well-known malicious activity. For example, software that configures itself to autostart on each reboot and make IRC connections would score higher than a file with no known bad behavior.

Begin a Malware Analysis Investigation

You can investigate data that has been scanned, flagged, and rated by Malware Analysis as containing Indicators of Compromise. This includes all types of Malware Analysis scans: continuous mode polling, on-demand polling, and on-demand uploaded files. Continuous mode polling must be enabled when the administrator configures basic settings for the Malware Analysis service.

NetWitness Suite provides several methods of launching a Malware Analysis investigation.

Fastest: Instant Launch from Malware Analysis Dashlets

The fastest way to begin a Malware Analysis investigation is an Instant launch from the NetWitness Suite Dashboard using one of the Malware Analysis dashlets that lists events or files that are likely to contain malware. The dashlets are described as part of the RSA NetWitness Content in Dashlets. From one of these dashlets, you can go directly to the Analysis Results for a specific event that has been listed as worthy of investigation:

- Top Listing of Highly Suspicious Malware
- Top Listing of Possible Zero Day Malware
- Malware with High Confidence IOCs and High Scores Dashlet

On-Demand Polling from a Meta Value in the Navigate View

You can initiate on-demand polling from within an investigation by right-clicking a meta value in the Navigate view, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis (see Launch a Malware Analysis Scan from the Navigate View).

Investigate a Specific RSA Service

You can also begin a Malware Analysis investigation of a service in the Investigate > Malware Analysis view. For Malware Analysis investigation on a service basis, a service must be specified in the Investigate > Malware Analysis view:Inve

1. Investigate opens the Malware Analysis view with the user-specified default service selected.
2. If no default service is currently specified, a dialog allows you to select the Malware Analysis service to investigate.
3. When a service has been selected in the Malware Analysis view, the Summary of Events for the selected service and continuous scan data for the service is displayed.

This topic provides instructions for all methods of launching a Malware Analysis investigation.

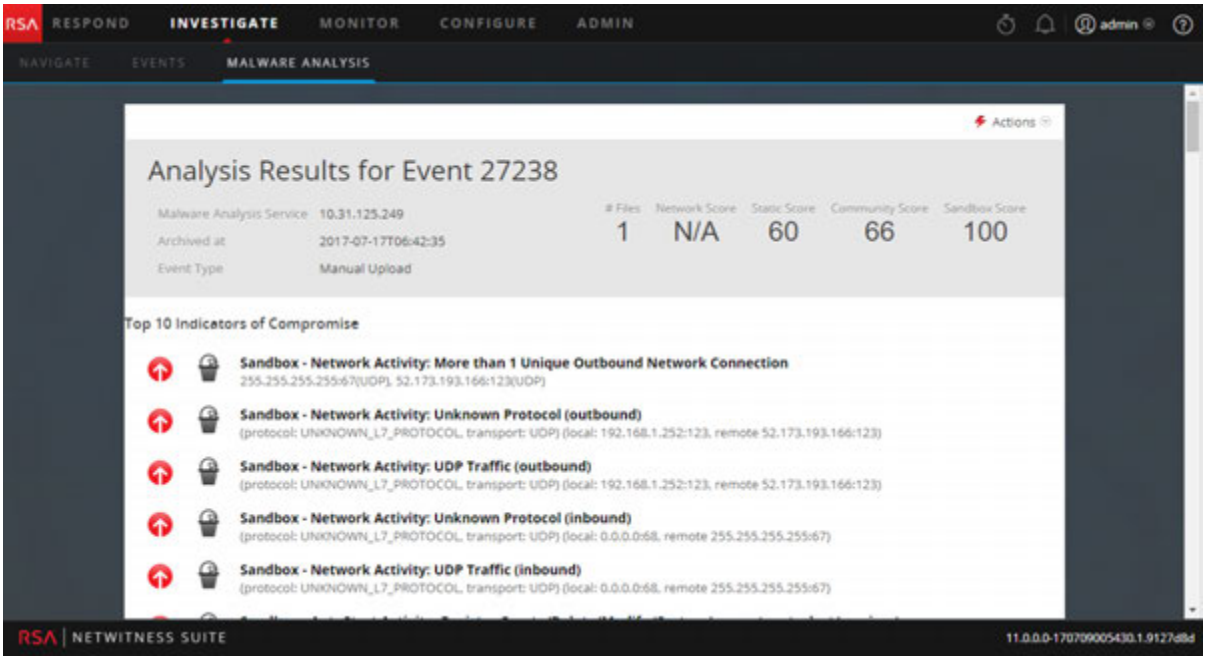
Launch a Malware Investigation from a Malware Analysis Dashlet

A prerequisite for this procedure is that one of the following dashlets must be visible in the NetWitness Suite dashboard or in the Malware Analysis view, and must be populated with listed events or files. If you do not see the dashlets, add them and configure the dashlets.

- Top Listing of Highly Suspicious Malware
- Top Listing of Possible Zero Day Malware
- Malware with High Confidence IOCs and High Scores Dashlet

To launch a Malware Analysis investigation from a dashlet:

1. Log in to NetWitness Suite and look for one of the above dashlets in the Monitor view or in the Malware Analysis view
2. In the dashlet, double-click an event or file for deeper analysis. A detailed analysis of the event in the Events List or the event with which the file in the File List is associated is displayed in the Malware Analysis view.



To learn more about configuring the Malware Analysis dashlets in the Monitor dashboard, see "Dashlets" in the *Getting Started with NetWitness Suite Guide*.

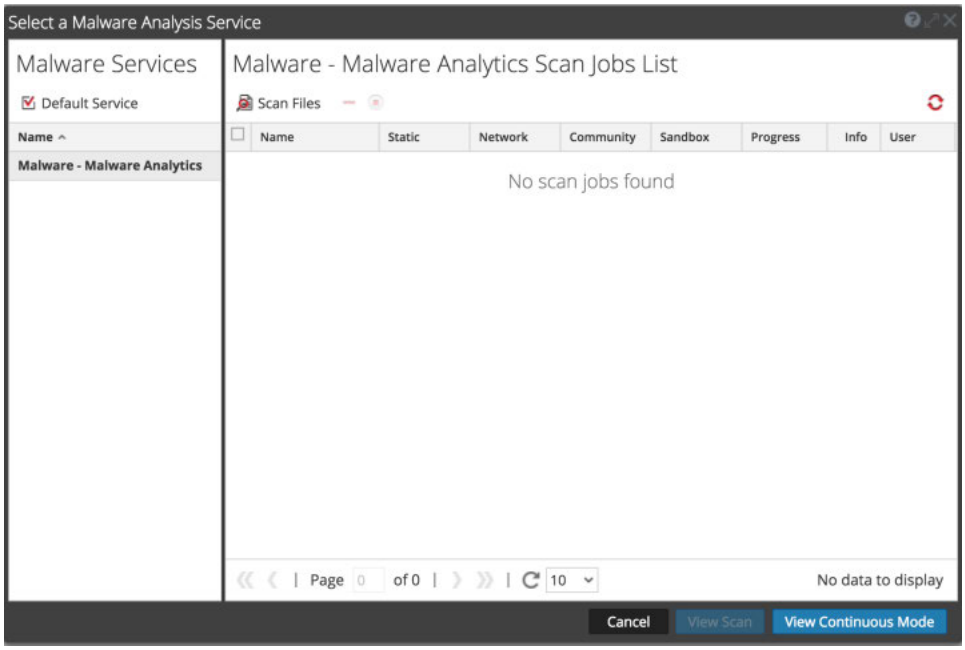
To learn about the ways you can configure and filter information in dashlets in the Malware Analysis view, refer to Filter Dashlet Data in the Summary of Events View.

To learn about the actions you can perform in the Analysis Results, refer to View Detailed Malware Analysis of an Event.

Begin a Malware Analysis Investigation (No Default Service)

To begin an investigation with no default service specified:

1. Select **Investigation > Malware Analysis**.
   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel and available scan jobs in the right panel. This scan jobs panel contains the same columns as the Malware Scan Jobs dashlet in the Unified dashboard. In addition, it has a toolbar and View options, which are described in Select a Malware Analysis Service Dialog.

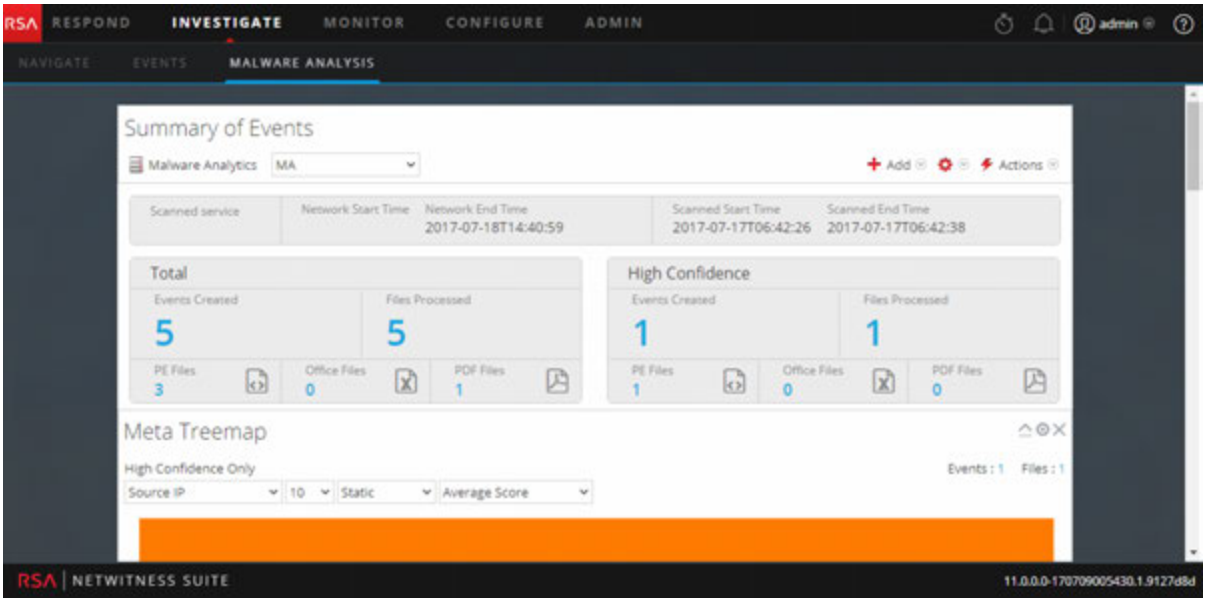


2. In the list of Malware Analysis hosts, select a host and a list of scan jobs is displayed in the right panel. These jobs are created when you scan an event or a file (see Upload Files for Malware Analysis Scanning and Launch a Malware Analysis Scan from the Navigate View.

3. To begin analyzing a scan, do one of the following:

   a. Select a scan and click **View Scan**.

   b. Click **View Continuous Mode**.
      The Summary of Events for the selected scan is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter Dashlet Data in the Summary of Events View.



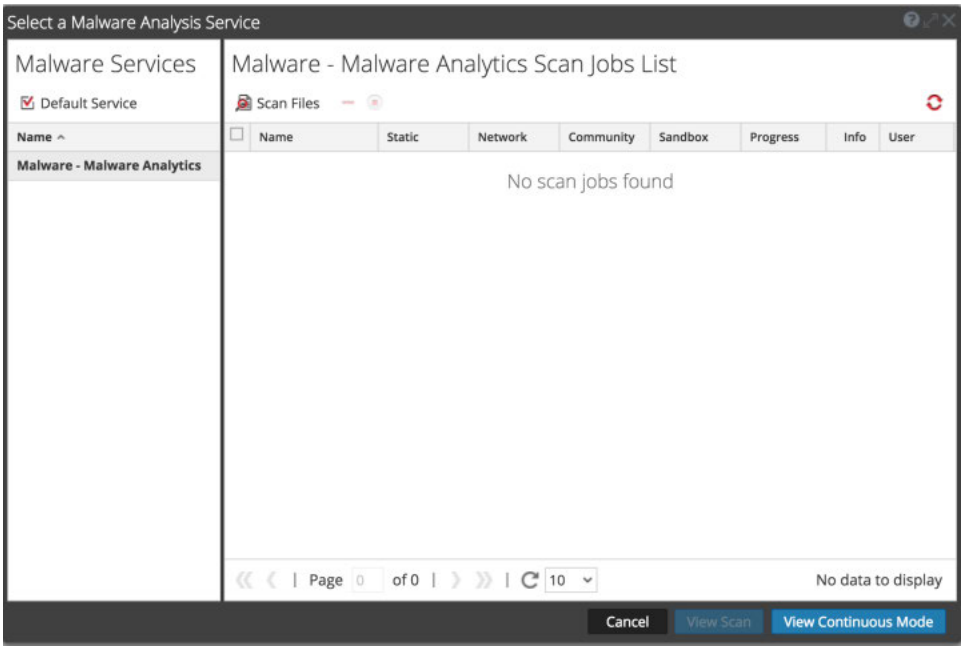
Set or Clear the Default Service

You can set the default service and clear the default service in the Select a Malware Analysis Service dialog.

To set a default service:

1. Click the service name in the Summary of Events toolbar.

   The Select a Malware Analysis Service dialog is displayed.



2. Select a service on the list of available Malware services, and click Default Service.

   The service becomes the default, (indicated by ☑ in front of the host name).

3. To clear the default service, select the default service in the grid, and click Default Service.

   No default service is set.

Upload and Scan Files

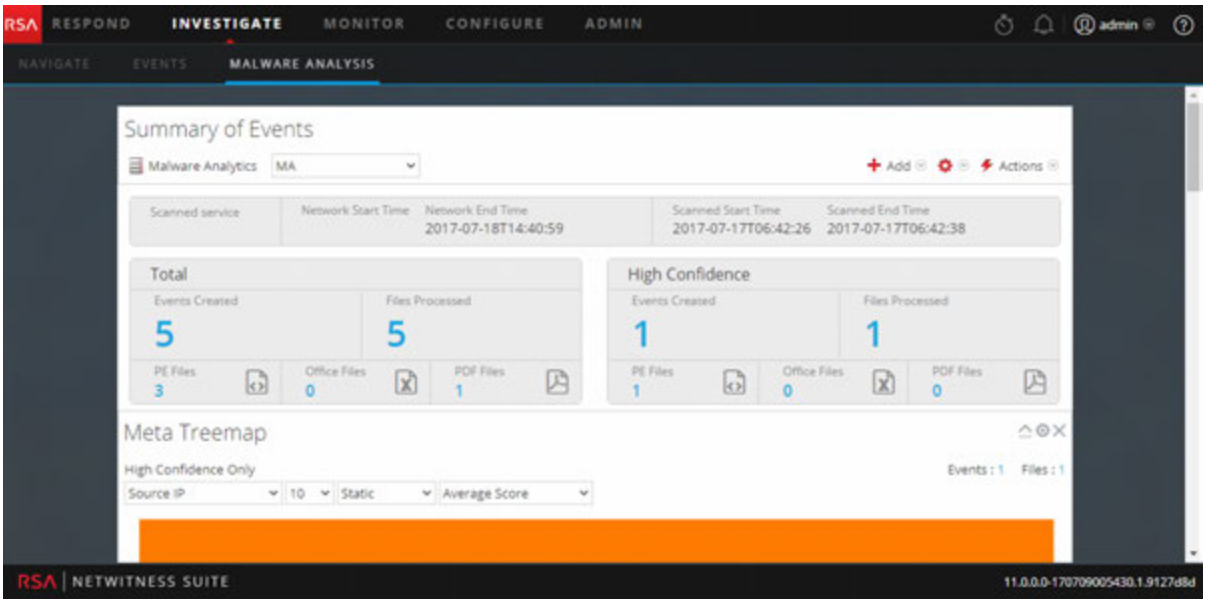
A Malware Analyst with permission to `Initiate Malware Analysis Scan` can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog (see Upload Files for Malware Analysis Scanning. An administrator can upload packet capture files to a Decoder for Malware Analysis in the Services System view as described in "Upload Packet Capture File" in the *Decoder and Log Decoder Configuration Guide*.

Begin an Investigation (Default Service Specified)

To begin an investigation with a default service specified:

1. Select **Investigation > Malware Analysis**.

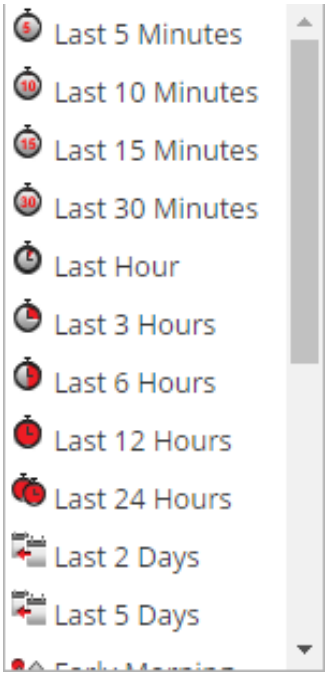
   The Summary of Events for a continuous scan of the selected service is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter Dashlet Data in the Summary of Events View.



Apply Time Parameters Filter for Results

You can apply a Threshold filter to refresh the results of the chosen dashlets.

1. To select a different time range, select either **Continuous Mode** or a different scan from the toolbar.
   The Malware Summary of Events for the selected scan is displayed.
2. To select a new time range for the scan, click in the range selection list in the toolbar.
   Ranges available are: Last 5 minutes, Last 10 minutes, Last 15 minutes, Last 30 minutes, Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 5 Days, Early Morning, Morning, Afternoon, Evening, All Day, Yesterday, This Week, Last Week, or Custom.



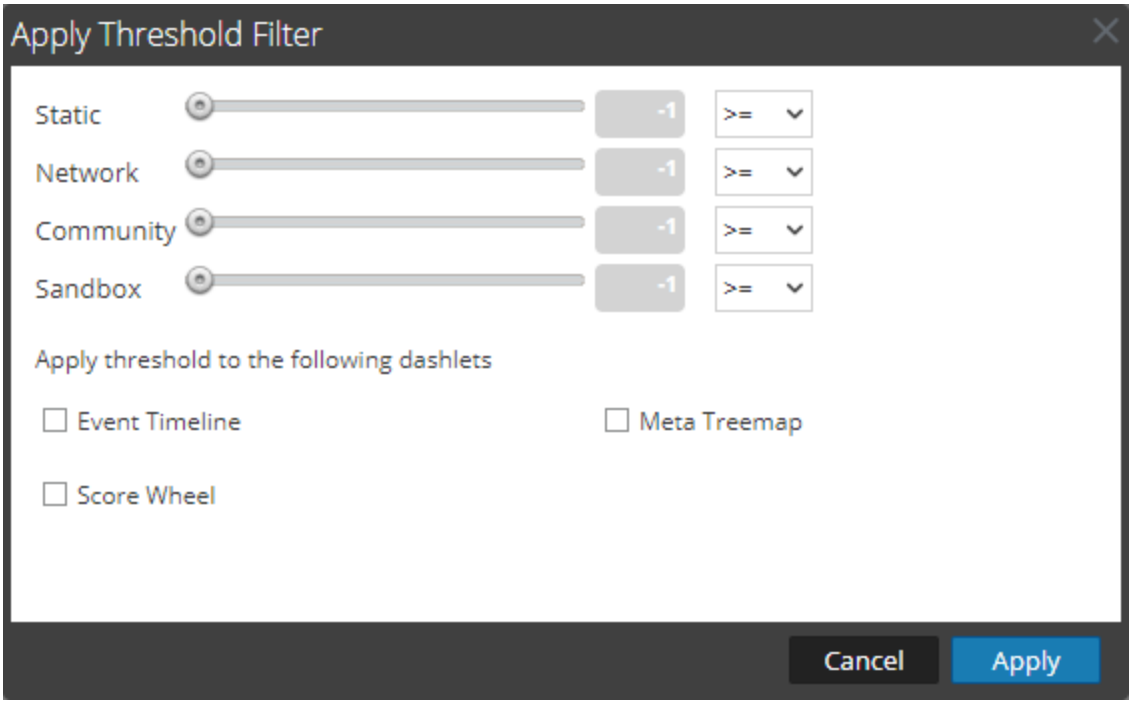
   The results are updated immediately.
3. To refresh a continuous mode scan with new data, click .

Apply a Threshold Filter to Continuous Mode Results

You can apply a new threshold filter to an instance of the Malware with High Confidence IOCs and High Scores dashlet, the Meta Treemap dashlet, the Score Wheel dashlet, and the Event Timeline dashlet.

To customize the scoring applied to the scan, in the toolbar, do the following:

1. Select > **Apply Threshold Filter.**
   The Apply Threshold Filter dialog is displayed.



2. If you want to limit the number of events displayed to events that were given a score above a certain number, do the following:
   a. Drag the slider in the Static, Network, Community, and Sandbox slider bars.
   b. To select the dashlets in which the thresholds apply, select the appropriate checkboxes.
   c. Click **Apply**.

Delete or Resubmit an On-Demand Scan with New Bypass Settings

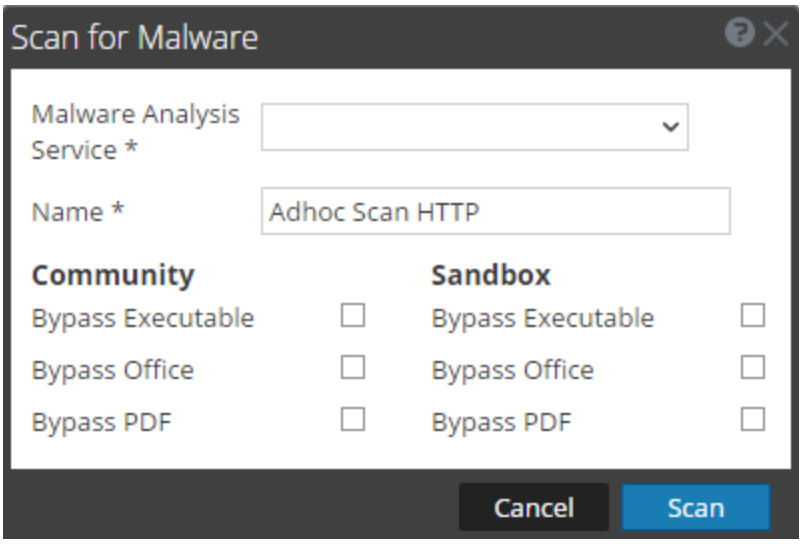
You can delete an on-demand scan or resubmit an on-demand scan with different bypass settings than those specified in the Service Configuration view for a Malware Analysis service.

To delete a scan while viewing an on-demand scan, do the following:

1. Select **Actions > Delete Scan**.
   A dialog asks for confirmation that you want to delete the scan.
2. Click **Yes**.
   The selected scan is deleted.

To apply different bypass settings to the current scan:

1. Select **Actions > Resubmit Scan**.
   The Scan for Malware dialog is displayed.



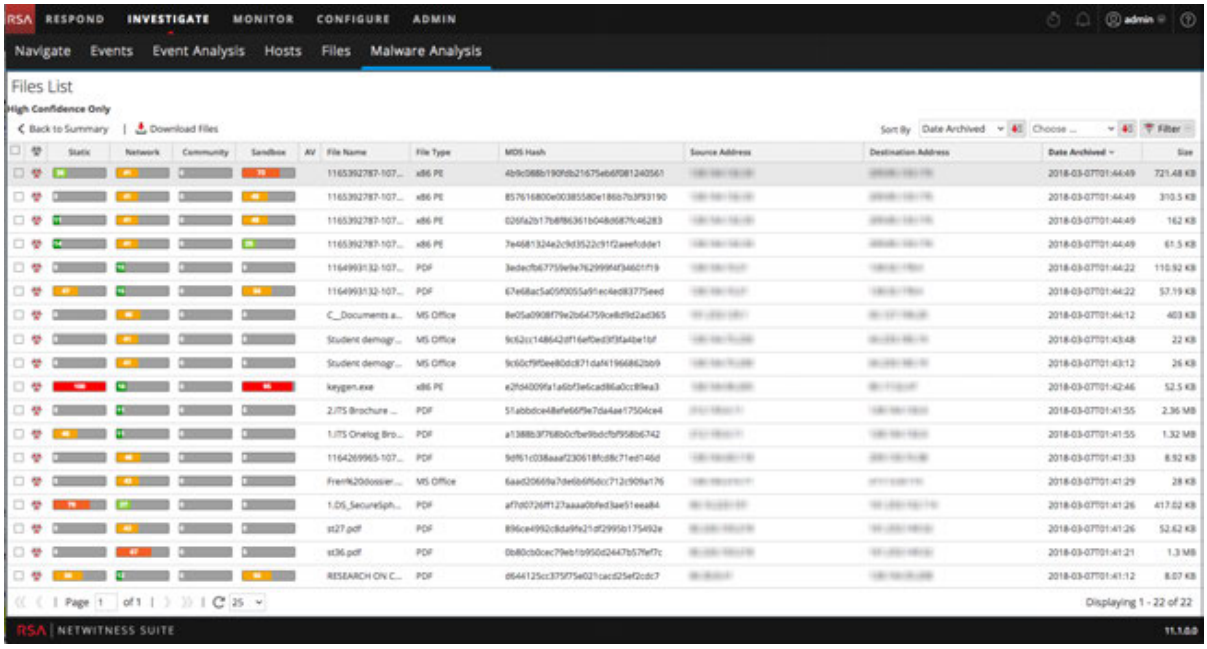
2. Select the bypass settings that you want to use on the new scan, and click **Scan**.
   Malware Analysis resets cache and resubmits the file for a new scan, and the scan jobs are added to the jobs queue.
3. When the job is complete, scroll to the left and select **View**.
   The Malware Summary of Events for the selected scan is displayed.

View the Files List

You can view a list of files for an event from the Malware Analysis Summary of Events and from each of the Visualization charts: Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel.

To view the Files List, do one of the following:

- In the Summary of Events, click on the number of files in the **Total** row or the **High Confidence** row under **Files Processed**, **PE Files**, **Office Files**, or **PDF Files**. The Files List is displayed.
- In any visualization dashlet, click the number next to the **Files** field in the top right corner of the dashlet.
  The Files List for the selected drill point is displayed.



From the Files List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files as described in Examine Scan Files and Events in List Form.

To return to the Summary of Events, click **Back to Summary**.

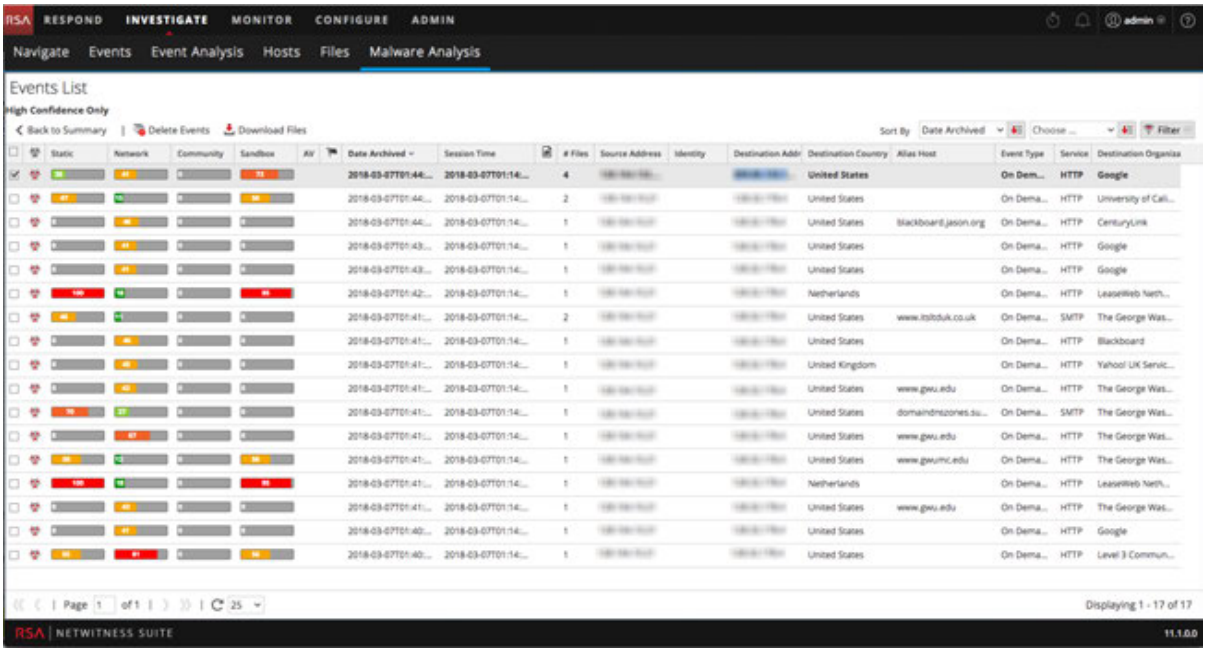
View the Events List

From the Malware Analysis Summary of Events and from each of the visualization charts (Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel), you can select events to view in the Events grid.

To view the Events List, do one of the following:

- In the Summary of Events, click the number of Events Created in the **Total** row or the **High Confidence** row. The Events List is displayed.
- In any visualization dashlet, click the number next to the Events field in the top right corner of the dashlet.

  The Events List for the selected time is displayed.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Navigate
Events
Event Analysis
Hosts
Files
Malware Analysis
Events List
High Confidence Only
Back to Summary
Delete Events
Download Files
Sort By
Date Archived
Choose ...
Filter
Static
Network
Community
Sandbox
AV
Date Archived
Session Time
Files
Source Address
Identity
Destination Addr
Destination Country
Alias Host
Event Type
Service
Destination Organiza
2018-03-07T01:44:...
2018-03-07T01:14:...
4
United States
On Dem...
HTTP
Google
2018-03-07T01:44:...
2018-03-07T01:14:...
2
United States
On Dema...
HTTP
University of Cali...
2018-03-07T01:44:...
2018-03-07T01:14:...
1
United States
blackboard.jason.org
On Dema...
HTTP
CenturyLink
2018-03-07T01:43:...
2018-03-07T01:14:...
1
United States
On Dema...
HTTP
Google
2018-03-07T01:43:...
2018-03-07T01:14:...
1
United States
On Dema...
HTTP
Google
2018-03-07T01:42:...
2018-03-07T01:14:...
1
Netherlands
On Dema...
HTTP
LeaseWeb Neth...
2018-03-07T01:41:...
2018-03-07T01:14:...
2
United States
www.itsltduk.co.uk
On Dema...
SMTP
The George Was...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
On Dema...
HTTP
Blackboard
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United Kingdom
On Dema...
HTTP
Yahoo! UK Servic...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
www.gwu.edu
On Dema...
HTTP
The George Was...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
domaindnszones.su...
On Dema...
SMTP
The George Was...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
www.gwu.edu
On Dema...
HTTP
The George Was...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
www.gwumc.edu
On Dema...
HTTP
The George Was...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
Netherlands
On Dema...
HTTP
LeaseWeb Neth...
2018-03-07T01:41:...
2018-03-07T01:14:...
1
United States
www.gwu.edu
On Dema...
HTTP
The George Was...
2018-03-07T01:40:...
2018-03-07T01:14:...
1
United States
On Dema...
HTTP
Google
2018-03-07T01:40:...
2018-03-07T01:14:...
1
United States
On Dema...
HTTP
Level 3 Commun...
Page
1
of 1
25
Displaying 1 - 17 of 17
RSA | NETWITNESS SUITE
11.1.0.0

Implement Custom YARA Content

In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language that allows malware researchers to identify and classify malware samples. RSA makes built-in YARA-based Indicators of Compromise (IOCs) available in RSA Live; these are automatically downloaded and activated on subscribed hosts.

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the host to consume.

As malware and the threat landscape evolve, it is important to review and examine existing custom rules. Updates are often necessary to incorporate new detection methods. RSA also updates YARA rules in Live from time to time. To receive updates, you can subscribe to the RSA Blog and RSA Live at http://blogs.rsa.com/feed.

This document provides information to help customers implement custom YARA rules in Malware Analysis.

Prerequisites

The host on which you are adding custom rules must be configured to support authoring of YARA rules as described in "Enable Custom YARA Content" in the *Malware Analysis Configuration Guide*.

YARA Version and Resources

RSA Malware Analysis is packaged with YARA version 1.7 (rev:167). To find out the exact version, you can run `yara -v` on the Malware Analysis host as shown in this example:

```
[root@TESTHOST yara] # yara -v
 yara 1.7 (rev:167)
```

Meta Keys in YARA Rules

Malware Analysis is compliant with other sources of YARA rules, and it also consumes additional meta keys that are specific to Malware Analysis. Each YARA rule is equivalent to an Indicator of Compromise (IOC) within Malware Analysis. The example below illustrates the meta definitions in a rule:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Meta Key	Description
iocName	(Required) This is the name that MA uses as the rule name. It is specific to Malware Analysis and is required to add the rule to the IOC list.
fileType	Specifies the files type. Possible values are: WINDOWS_PE, MS_OFFICE, and PDF. If not specified, the default value is WINDOWS_PE.
score	This value that is added to the static score if the YARA rule is triggered. If not specified, the default value is 10.
ceiling	This is the maximum amount that is added to the static scores when a rule is triggered multiple times in one session. For example, if each time a rule is triggered, 20 points are added to the static, and you do not want more that 40 points added when the rule is triggered more than two times, you can specify a ceiling of 40. If not specified, the default value is 100.
highConfidence	This sets the High Confidence flag, which is set on IOCs when there are high confidence indicators that malware is present. If not specified, the default file value is false.

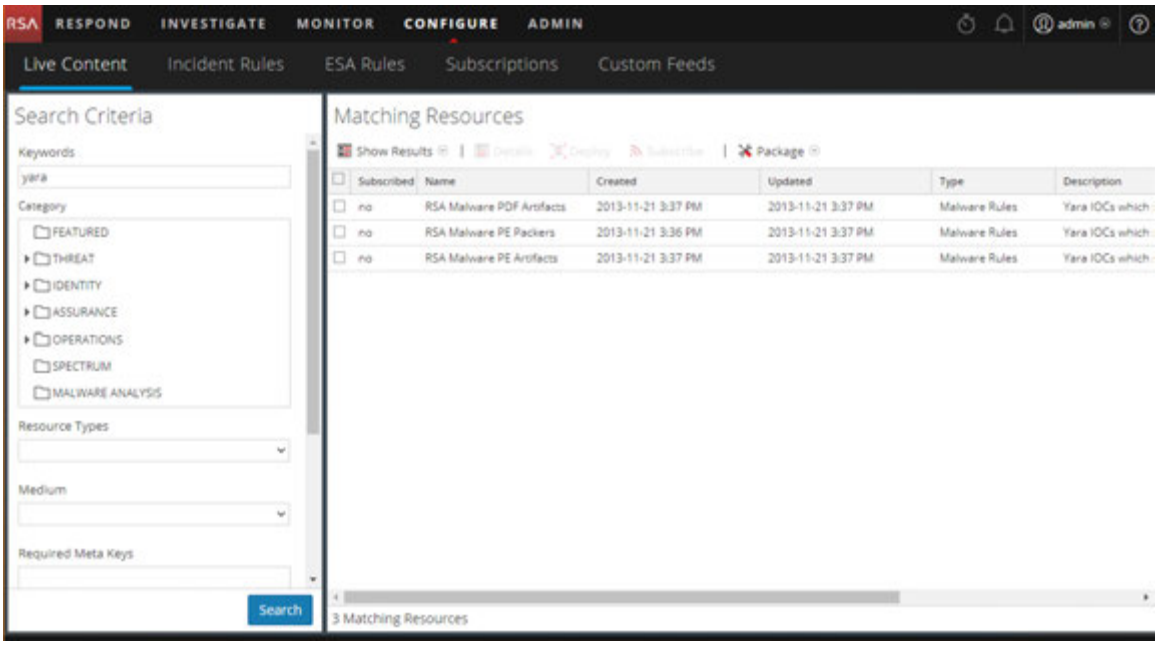
Note: Refer to the following URL for YARA resources: https://code.google.com/p/yara-project/downloads/list. NetWitness Suite uses YARA 1.7, not YARA 2.0.

YARA Content

RSA Live contains 3 sets of Yara rules:

- PE Packers
- PDF Artifacts
- PE Artifacts

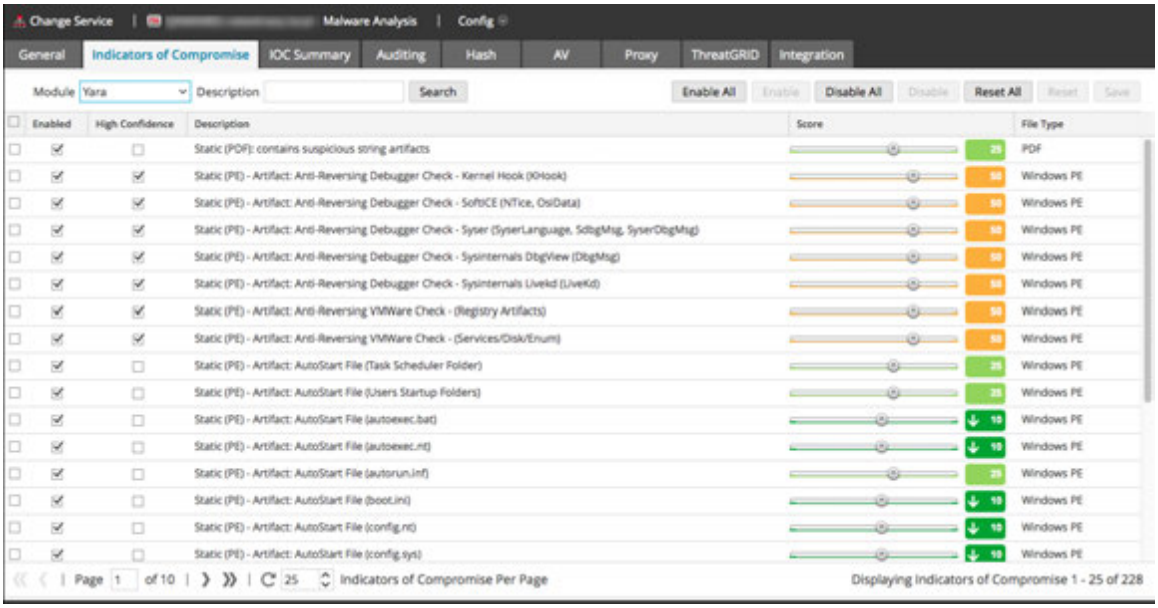
The following figure illustrates YARA content available as YARA rules in NetWitness Suite Live.



On the Malware Analysis host, the YARA rules reside in `/var/lib/rsamalware/spectrum/yara`, as shown in the example below.

```
[root@TESTHOST yara]# pwd
 /var/lib/rsamalware/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_
packers.yara
```

The individual rules are listed as IOCs in the Malware Analysis Service Config view > Indicators of Compromise tab. To view them, use the Yara module as the filter. You can adjust the configuration of an individual in the same way that you configure other IOCs.



Add Custom YARA Rules

To introduce custom YARA rules from other sources:

1. To ensure that the YARA rules follows the correct format and syntax, use the YARA command to compile the YARA rule as shown in the following example. If the rule compiles with no errors, this indicates that the YARA rule has the correct syntax.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
   [root@TESTHOST yara]#
   ```

2. Ensure that custom rules do not duplicate existing YARA rules from RSA or other sources. All YARA rules are in `/var/lib/rsamalware/spectrum/yara`.

3. Ensure that the meta keys that RSA supports are included to organize the YARA rules as part of the configurable IOCs, and name the file with the yara extension (<filename>.yara). For better organization, make sure that the `iocName` meta is included in the meta section as shown in the following example.

   Example:

   ```
   rule HEX_EXAMPLE
   {
       meta:
           author = "RSA"
           info = "HEX Detection"
          iocName = "Hex Example"
        strings:
           $hex1 = { E2 34 A1 C8 23 FB }
           $wide_string = "Ausov" wide ascii
        condition:
           $hex1 or $wide_string
   }
   ```

4. When ready, place the custom YARA file in the folder that the Malware Analysis service watches:

   `/var/lib/rsamalware/spectrum/yara/watch`

   The file is consumed within one minute.

   Once consumed, NetWitness Suite moves the file to the `processed` folder, and the new rule is added to the Malware Analysis Services Config view > Indicators of Compromise tab.

Examine Scan Files and Events in List Form

When viewing the Summary of Events in a Malware Analysis scan, you can click a file count or an event count to view the Files List or the Events List for the scan (see Begin a Malware Analysis Investigation). In the Files List and Events List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files. When you find an event or file of interest in the Events List or Files List, you can view many details about the event in the Event Details view.

For each event in the Events List, NetWitness Suite provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.
- Antivirus vendor scores.
- The Influenced by customized rule flag.
- The date the event was archived.
- The session time.
- The MD5 hash filter.
- The number of files in the event.
- The source IP address of the event.
- The Identity.
- The destination IP address.
- The destination country.
- The name of the alias host.
- The event type, for example, Network.
- The service used by the event.
- The destination organization

For each file in the Files List, NetWitness Suite provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.

- Antivirus vendor scores.
- The filename.
- The file type.
- The MD5 hash filter.
- The source IP address of the event that contained the file.
- The destination IP address.
- The date the event that contained the file was archived.
- The file size.

Sort the Files List or Events List

You can sort the Files List and Events List by column name in ascending and descending order. You can choose one or two columns.

To sort the list:

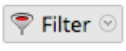
1. In the first **Sort By** drop-down list, choose a column name and sort direction: for descending order or for ascending order.
2. (Optional) In the second **Sort By** drop-down list, choose a column name, and sort direction, for descending order or for ascending order.

   The column titles reflect the selected sort order.

Filter the List by Filename or MD5 File Hash

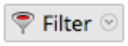
You can filter the Files List and Events List by filename or file hash. With this feature, you can specify a limited subset of the original data based on the search criteria.

Note: When you perform a search, you search the scan that you are currently displaying, not all scans.

1. Click 

   .

   The Filter dialog is displayed.
2. Enter a value in **File Name** or **MD5 Hash** and click **Filter**. The File Name and Hash field are not case sensitive. Wild card or regular expressions are not supported. The filter is based on exact matches. You can drag across a filename or hash to select from the Files list or Events list, then copy and paste it in the dialog.

3. Click **Filter**.
   Malware Analysis filters the list to display only files or events with the selected hash
4. To revert to the unfiltered list, click 

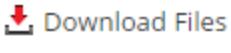
. When the Filter dialog is displayed, click **Reset**.

Download Files from the Files List

NetWitness Suite lets you select and download files from the Files List or the Events List.

Caution: Use caution when downloading files from Malware Analysis; some files may contain harmful code. File Download is a specific permission that can be configured, refer to "Define Roles and Permissions for Malware Analysts" in the *Malware Analysis Configuration Guide* for more details.

To download files from the Files List or Events List:

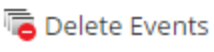
1. In the **Files List** or **Events List**, select the checkbox next to one or more rows.
2. In the toolbar, select 

.
   The Malware File Download dialog is displayed.
3. Do one of the following:
   a. If you decide not to download the file, click **Cancel**.
   b. If you want to download the file, select click the **Download** button.
      The file or files selected are downloaded in a zip archive with the name `Malware_Files.zip`.

Delete Events from the Scan

In the Events List, you select one or more events and delete them from the scan. This is useful for removing events that are not of interest.

To remove an event from the scan being viewed:

1. In the **Events List**, select one or more events.
2. In the toolbar, click 

.
   NetWitness Suite asks for confirmation that you want to delete the events.
3. In the confirmation dialog, click **Yes**.
   The selected events are deleted.

Return to the Summary of Events

To leave the Files List or Events List and return to the Summary of Events, click **Back to Summary**.

Open the Detailed Analysis for an Event

While you examine events or files in the Files List or Events List, you can double-click any event or file to open a detailed analysis of the event in the Events List or the event with which the file in the Files List is associated (see View Detailed Malware Analysis of an Event).

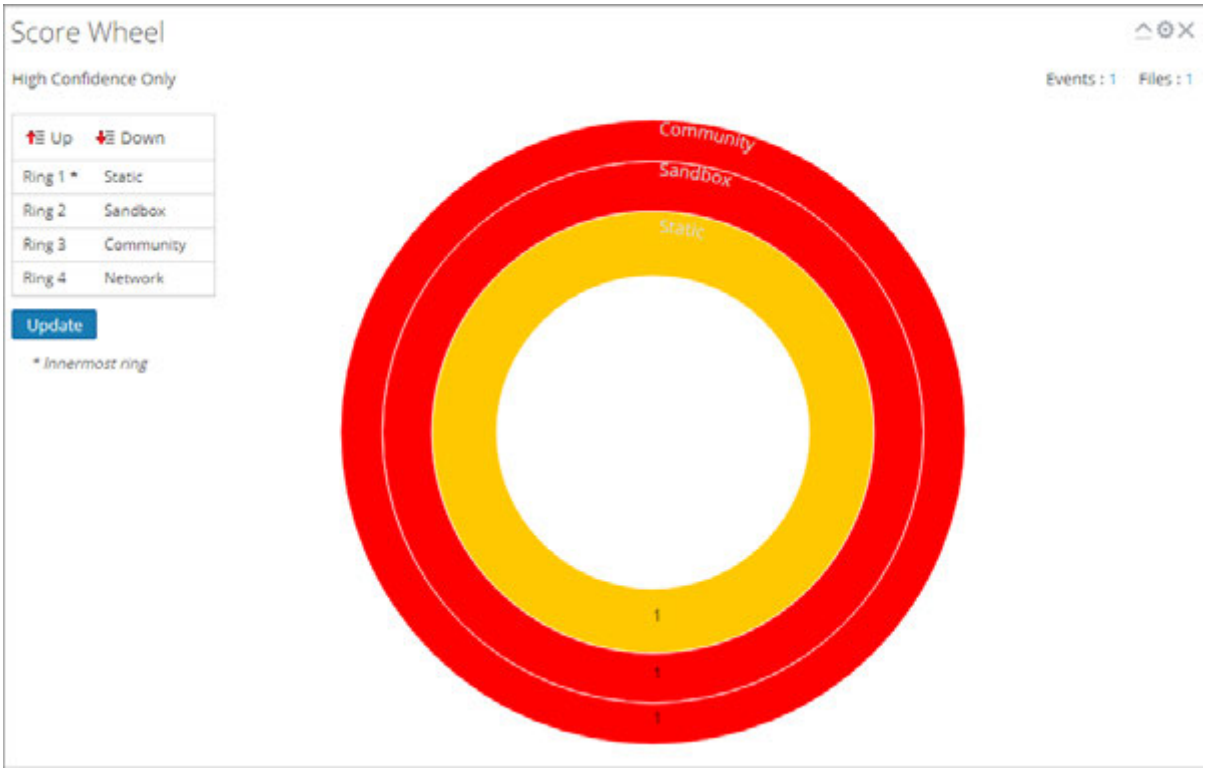
Filter Dashlet Data in the Summary of Events View

The Summary of Events provides a summary of the scan being investigated with selectable dashlets. The Summary of Events is fixed, but Analysts can configure each dashlet to filter out information and drill into the data.

The rest of this topic provides instructions for managing and configuring dashlets.

Configure the Score Wheel Dashlet

The Score Wheel is a high-level visualization of analyzed sessions that scored high, medium, or low in each of the scoring categories: Static, Network, Community, and Sandbox. The Score Wheel is a quick way to drill into sessions to review them. Each ring represents a different scoring category so that you can visually compare results by category.

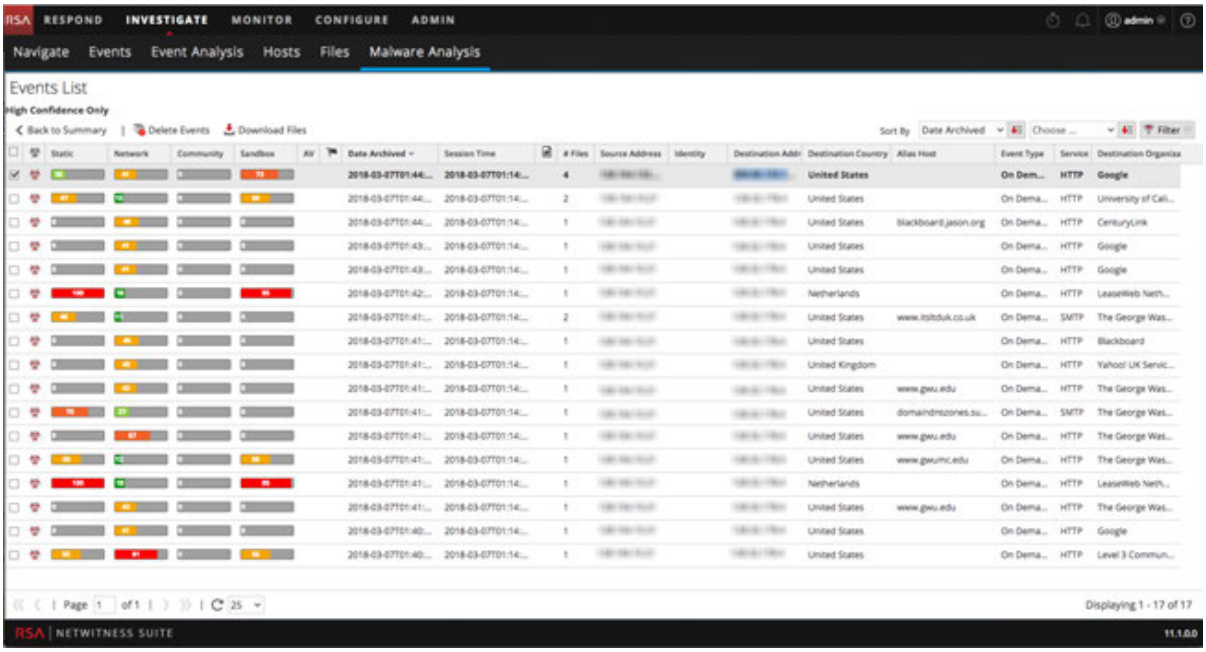


You can change the order of the rings to highlight indicators of compromise that were flagged in one category but not in another category. Comparing the same results in a different sequence of the rings provides visibility into additional vulnerabilities in a session, and you can drill into sessions of interest. The following examples show two possible use cases.

Zero-Day Candidates Example

This example shows how to drill into sessions that the Community did not flag as malicious, but all other scoring categories did. The resulting list of sessions highlights zero-day candidates.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)
2. Click the red slice in the outermost (Sandbox) ring that aligns with a green slice on the innermost ring (Community): green (innermost) -> **Static**: red -> **Network**: red -> **Sandbox**: red (outermost).



Malicious Sessions Example

This example shows how to drill into sessions in which all scoring categories identify the resulting list of sessions as malicious, indicating Malware Analysis has the most confidence that they are malware.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)
2. Click the red slice of the outermost (Sandbox) ring that aligns within a red slice on the innermost ring (Community): red (innermost) -> Static: red -> Network: red -> Sandbox: red (outermost).

Arrange the Ring Sequence by Scoring Module

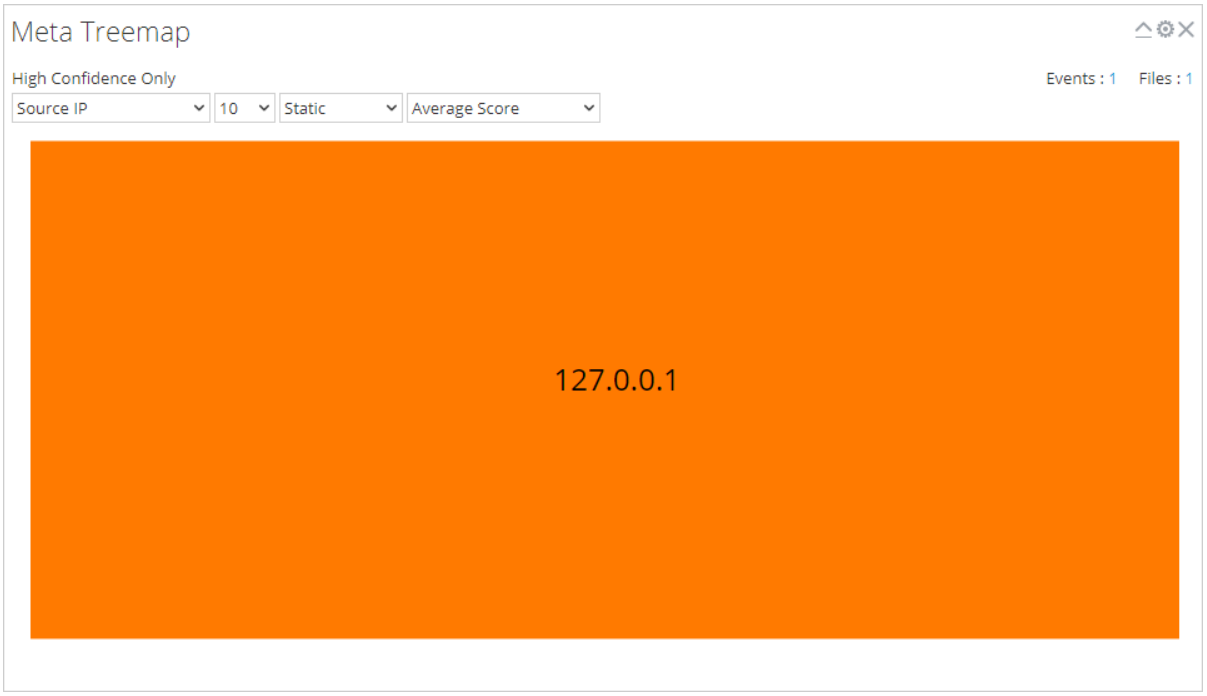
In the Score Wheel, you can arrange the sequence of the rings by scoring module. Initially, the sequence of rings from inside to outside is Static, Network, Community, and Sandbox.

To change the ring sequence:

1. Do one of the following:
   a. Click and drag each scoring module up or down.
   b. Select each scoring module and use the Up and Down buttons to move it.
2. When the ring sequence is the way you want it, click the **Update** button.
   The Score Wheel is refreshed with the new sequence.

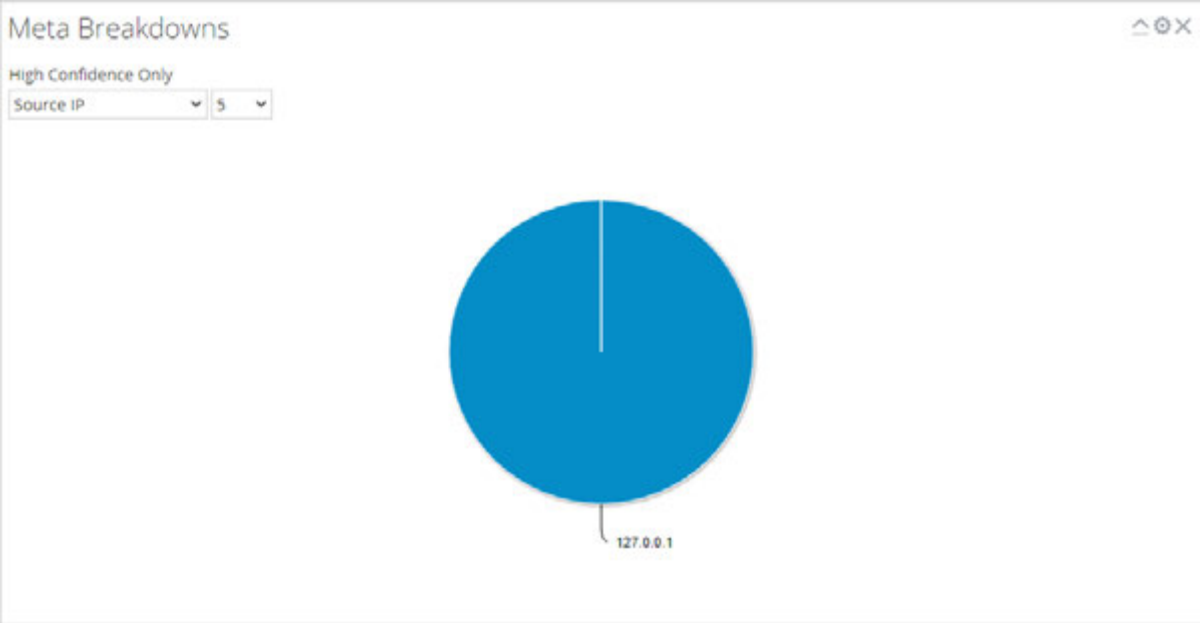
Configure the Meta Treemap Dashlet

In the Meta Treemap chart, you can visualize and filter meta breakdowns by meta type, count, and analysis type. Use the three selection lists to set the filter, and the Meta Treemap chart is refreshed immediately.



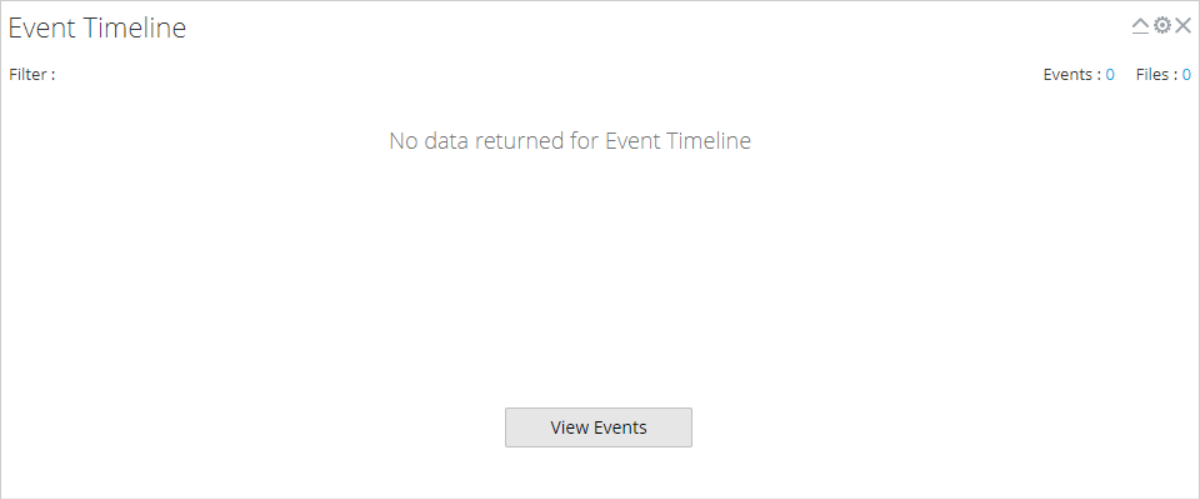
Configure the Meta Breakdowns Dashlet

The Meta Breakdowns dashlet is a visualization of values for a specific meta key in a pie chart. In the Meta Breakdowns chart, you can filter meta breakdowns by meta type and count. Use the two selection lists to set the filter, and the Meta Breakdowns chart is refreshed immediately.



Configure the Events Timeline Dashlet

The Events Timeline dashlet is a visualization of the events along a timeline. No additional filters are available for the Event Timeline.

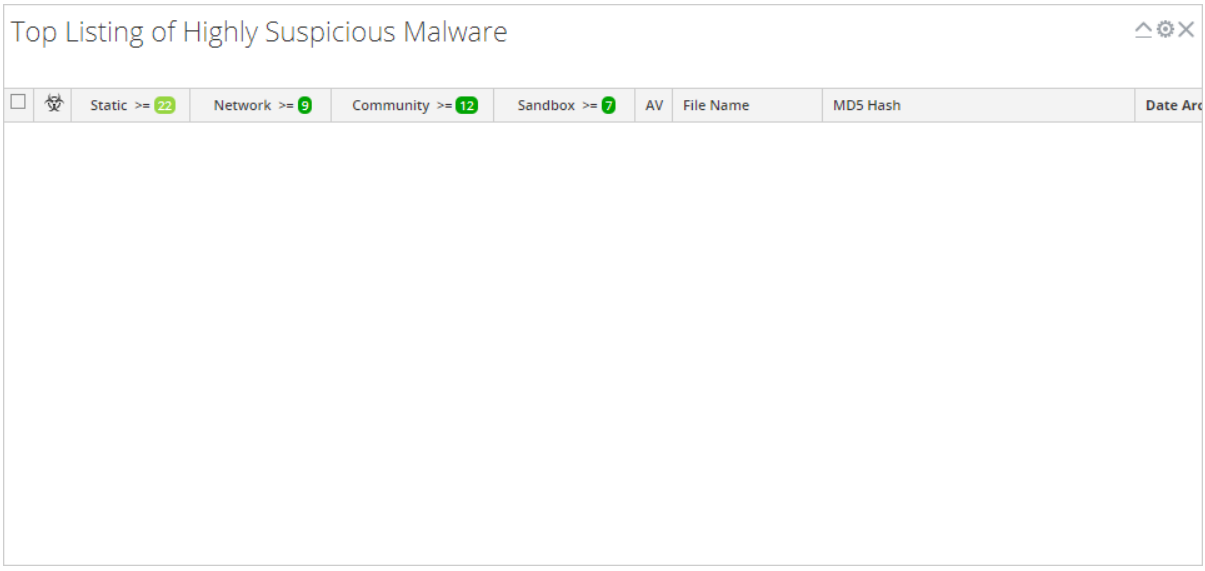


Open All Events in the Events List

From within the Event Timeline, you can open the entire list of events in the Events List. To do so, click View Events. This option is not the same as clicking the count next to Events, which is the same for all visualization charts and opens the current drill point in the Events List.

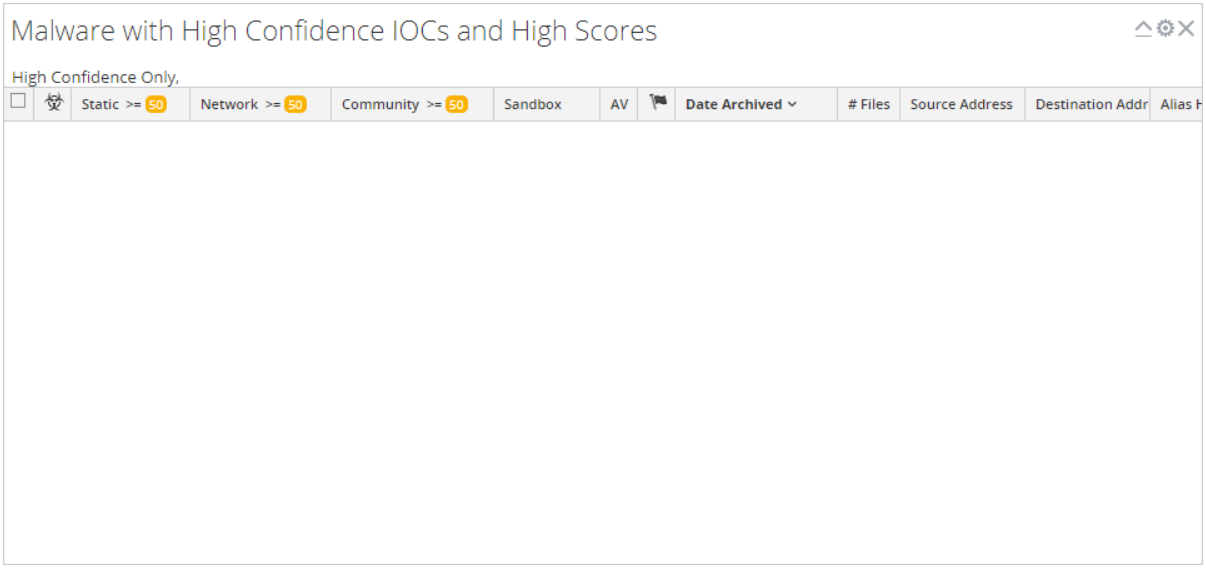
Configure the Top Listing of Highly Suspicious Malware Dashlet

The Top Listing of Highly Suspicious Malware Dashlet presents the Top 10 most suspicious events in the Events List or the Files List. This dashlet is also available in the Monitor dashboard, and the configuration options are described as part of the RSA NetWitness Content in Dashlets..



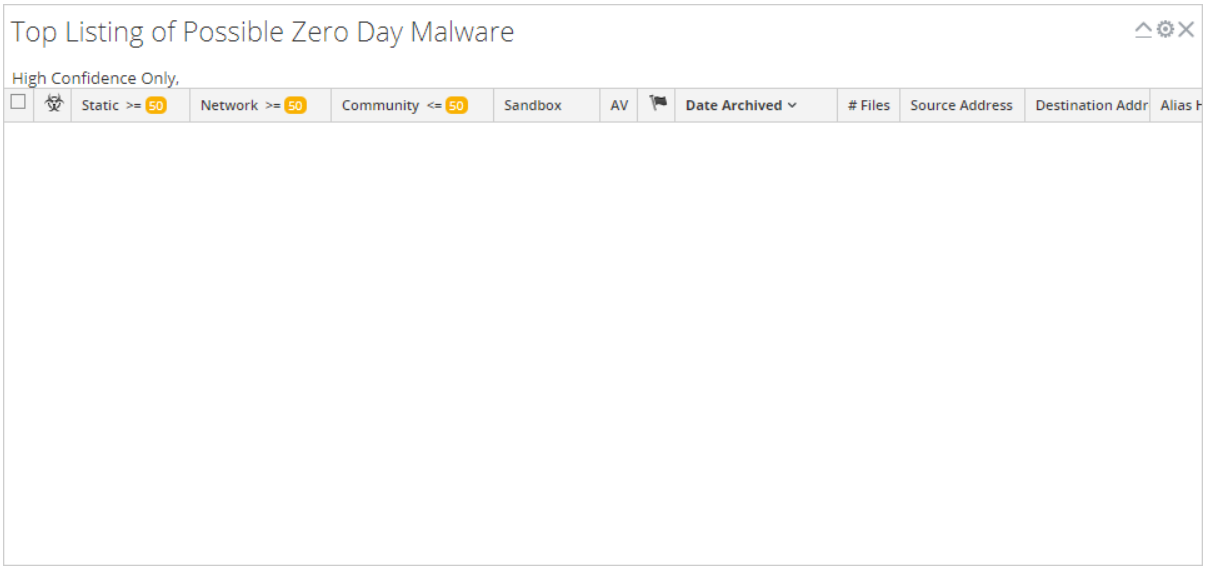
Configure the Malware with High Confidence IOCs and High Scores Dashlet

The Malware with High Confidence IOCs and High Scores dashlet presents Indicators of Compromise that have both high scores and high confidence that the events are likely to contain malware. The dashlet is also available in the Unified dashboard, and the configuration options are described as part of the RSA NetWitness Content in Dashlets..



Configure the Top Listing of Possible Zero Day Malware Dashlet

The Top Listing of Possible Zero Day Malware dashlet presents potential zero day events in the Events List or the Files List. The dashlet is also available in the Unified dashboard, and the configuration options are described as part of the RSA NetWitness Content in Dashlets.



Upload Files for Malware Analysis Scanning

There are two methods for analysts to upload files for Malware Analysis scanning.

A Malware Analyst with permission to Initiate Malware Analysis Scan can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog.

It is also possible to upload a file for scanning using a watched file share.

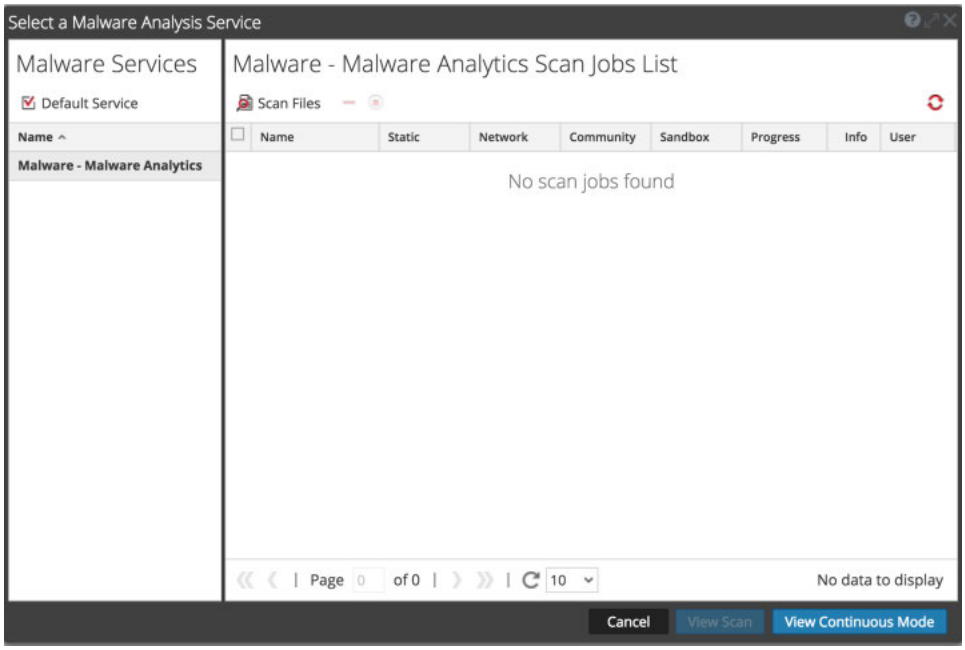
Upload Files Manually

This topic provides instructions for initiating on-demand scanning of an uploaded file. When you upload a file for scanning, NetWitness Suite starts the upload job and adds it to the jobs queue. When the job is complete, you can view the scan in Malware Analysis.

To upload a file to scan:

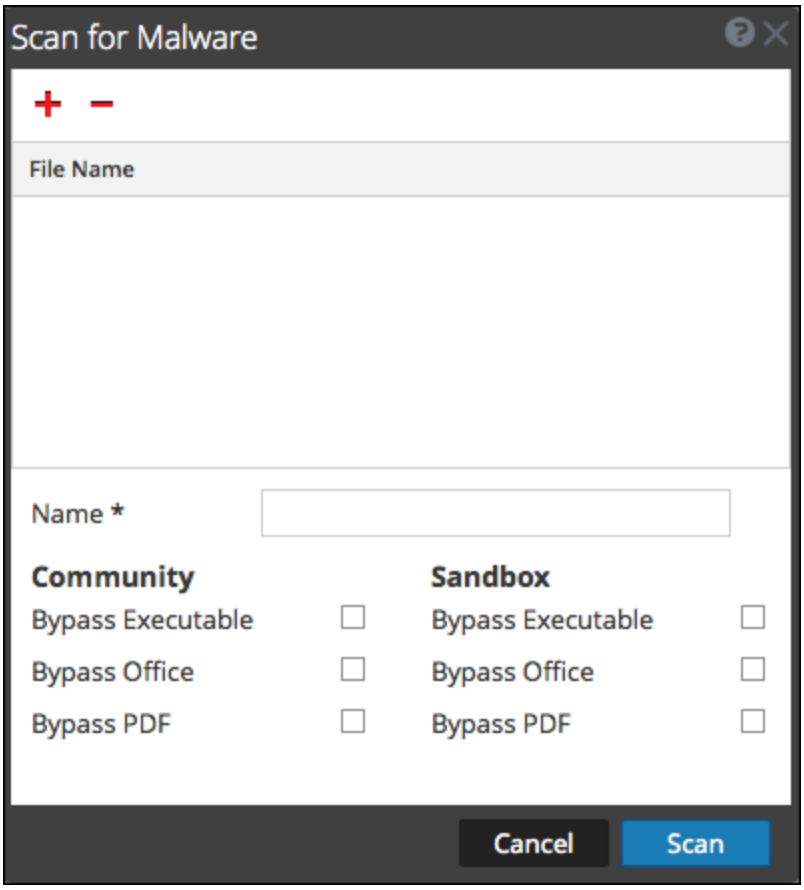
1. Go to **INVESTIGATE > Malware Analysis**.

   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel.



2. Click **View Scan**.

   The Scan for Malware dialog is displayed.



3. Click +
   A view of the files system is displayed so that you can choose files to upload.
4. Select one or more files from the list and click **Open**.
   The file names are added. Malware Analysis escapes the filename characters before processing a file. The maximum number of filename characters after escaping is 200. If the filename is greater than 200 characters, Malware Analysis truncates the filename characters and displays the truncated filename in the NetWitness Suite user interface.
5. Continue adding and deleting files until you have a list of the files that you want to upload.
6. Name the scan and select the types of files to bypass. This is useful for a zip archive that contains different types of files, and overrides the default bypass settings.
7. Click **Scan**.
   The scan job is submitted and NetWitness Suite displays a confirmation message for successful submission. The scan request is added to the Scan Jobs List dashlet. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.

8. The job is added to the Scan Jobs List in the Select a Malware Analysis Service dialog and in the Unified dashboard Scan Jobs List dashlet.
9. To view the scan when complete, double-click the scan.
   The Malware Summary of Events for the selected scan is displayed.

Upload Files from a Watched Folder

To upload files from a watched folder, you can drop files into a watched file share for Malware Analysis. Analysts can share YARA rules, hash files, and infected zip archives with Malware Analysis.

Malware Analysis watches a file share and automatically consumes files placed in specific folders in the file share. This feature is useful for:

- Bulk import of hash files from `/var/lib/rsamalware/spectrum/hashWatch`.
- Addition of custom-YARA rules to the Indicators of Compromise (IOC) list on the host from `/var/lib/rsamalware/spectrum/yara/watch`.
- Creation of on-demand scan jobs from a zip archive of infected zip files from `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Analysts need to prepare the files for consumption in accordance with requirements, the file extension must be correct, and the file must be copied to the correct watched folder in the file share.

Import a Hash List

To import a hash list from the watched directory, the hash list must be in the specified format and must be sorted on md5. You can drop a file formatted into a folder (`/var/lib/rsamalware/spectrum/hashWatch`) on the Malware Analysis host, and it is automatically imported into the local hash database. This is described in "Configure Hash Filter" in the *Malware Analysis Configuration Guide*.

To import a hash list using the watched folder method:

1. Copy the hash lists that you want to import into the **`/var/lib/rsamalware/spectrum/hashWatch`** directory.
   NetWitness Suite Malware Analysis automatically watches this folder and processes files placed there.
   a. Malware Analysis adds every hash found in the hash lists to the hash filter.
   b. If there are processing errors, they are logged in:
      `/var/lib/rsamalware/spectrum/hashWatch/error`

c. Processed files are cataloged
here: `/var/lib/rsamalware/spectrum/hashWatch/processed`

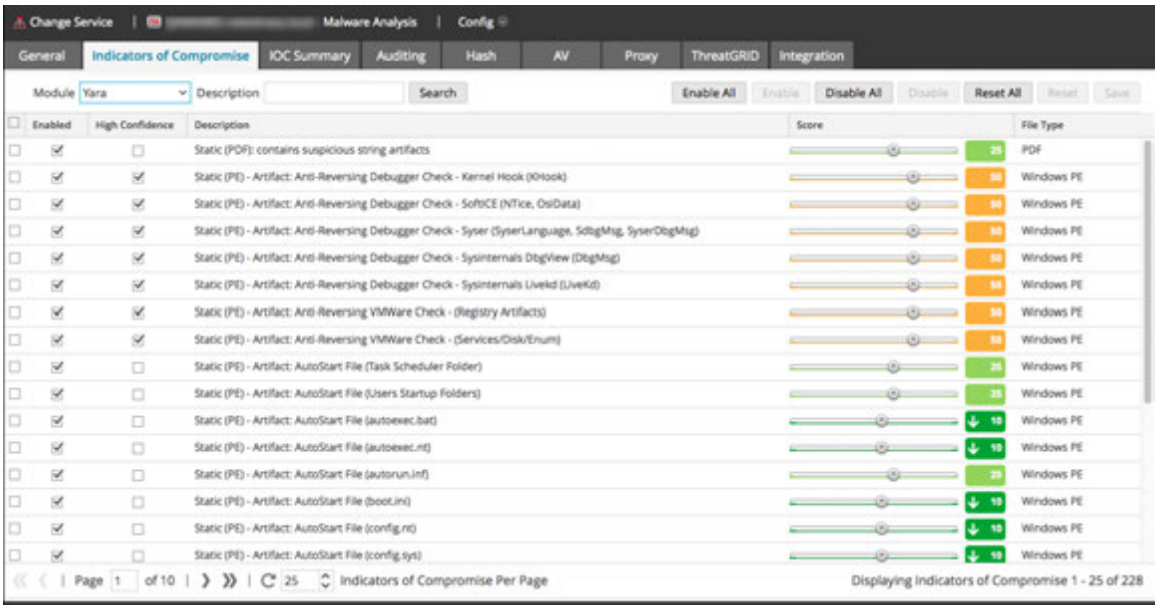
d. Processed files are not removed from the hashWatch directory.

2. After importing hashes in bulk, the System Administrator can use a cronjob to clean up old processed files.

Import YARA rules to the IOC List

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the host to consume. Implement Custom YARA Contentprovides complete information on the prerequisites for using custom YARA content and authoring rules.

When the rules are ready, place the custom YARA files in the folder that the Malware Analysis service watches:
`/var/lib/rsamalware/spectrum/yara/watch`
The file is consumed within one minute.
Once consumed, NetWitness Suite moves the file to the `processed` folder, and the new rule is added to the Malware Analysis Service Config view > Indicators of Compromise tab.



Import Files into the Scan Jobs List

When you obtain samples from perimeter security solutions and would like to perform further analysis on the files, you can zip the files and password protect the archive with `infected`, then add to the watched folder for consumption by Malware Analysis. This zipped archive is ready to be placed in the watched folder:
`/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Note: The maximum size of the archive is 100 MB.

To analyze infected, password-protected zip files, Malware Analysis consumes archives place in a watched folder and creates an on-demand job that is added to the Scan Jobs List.

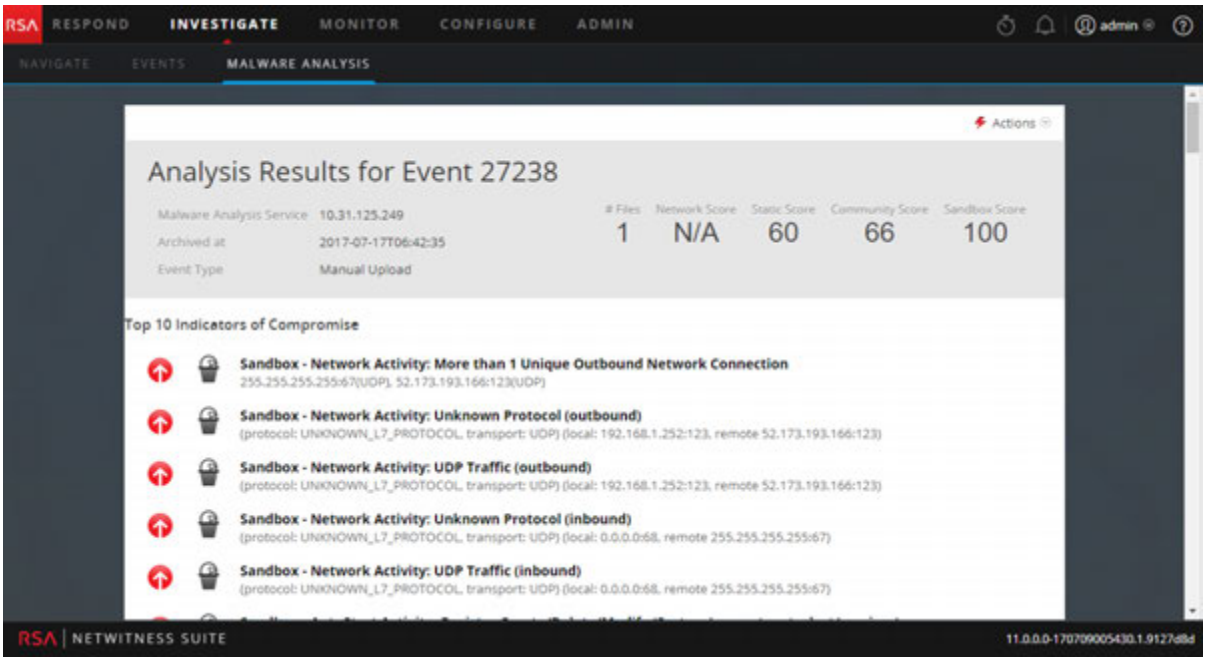
1. While logged on as administrator, place the files to be processed in a zip file with password `infected` at `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   In a minute or two Malware Analysis consumes the archive and creates an on-demand job in the Scan Jobs List. The scan job name is the name of the file, the user is **file share**, and the Event Type is 1. The archive is moved to `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`
2. After the job is added to the Scan Job List, run a script or cronjob to clean up the zip file in `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

View Detailed Malware Analysis of an Event

When viewing the list of individual events in a Malware Analysis scan in the Malware Analysis Events grid, you can double-click an event to view the detailed analysis results for the event.

View Malware Analysis Details for an Event

1. Start an investigation in the **Malware Analysis** tab.
   The Malware Summary of Events is displayed, and includes four charts, including the Event Timeline.
2. Do one of the following:
   a. To view all events in the Event Timeline, click the **View Events** button.
   b. Double-click data in the **Meta Breakdown**, **Meta Treemap Chart**, or **Score Wheel**.
   The Events List is displayed.
3. Double-click an event.
   The Analysis Results for the event are displayed.

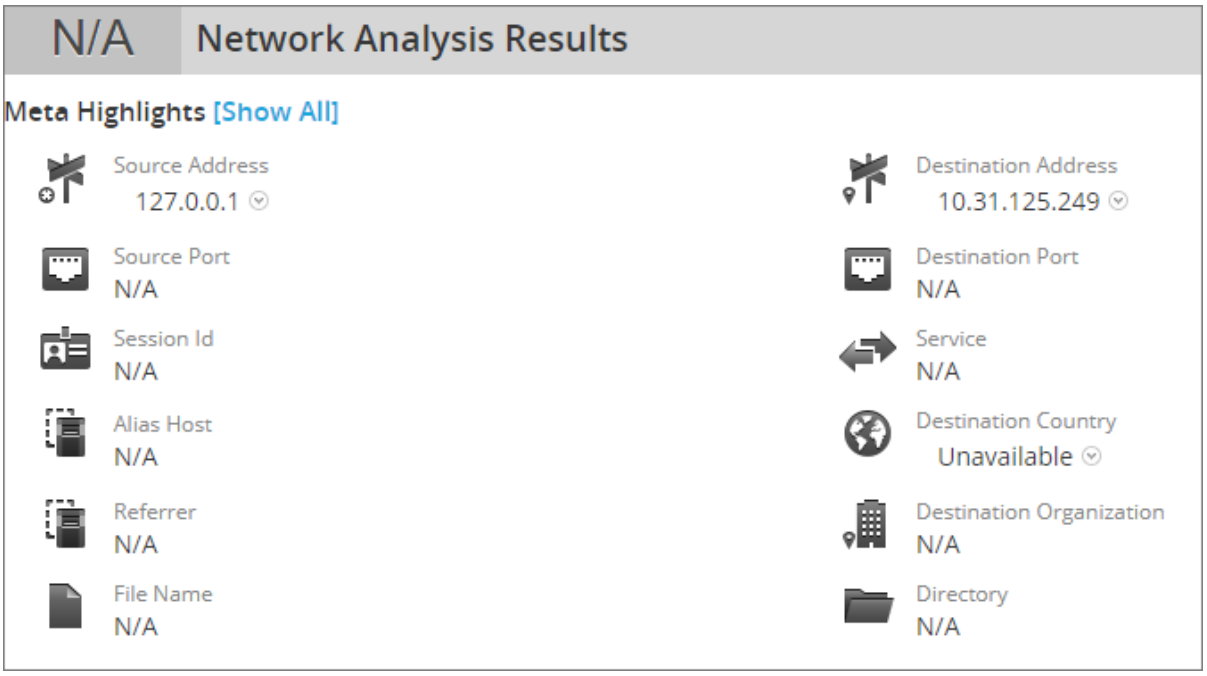


4. (Optional) If you want to delete an event, select **Actions > Delete Event**.
5. If you want to view a reconstruction of the network session, select **Actions > View Network Session**.
   The session opens in the Navigate view > Event Reconstruction.

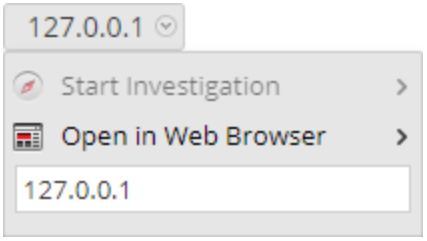
Pivot Network Analysis Results

You can pivot the Network Analysis Results in several ways:

1. Scroll down to the Network Analysis Results.



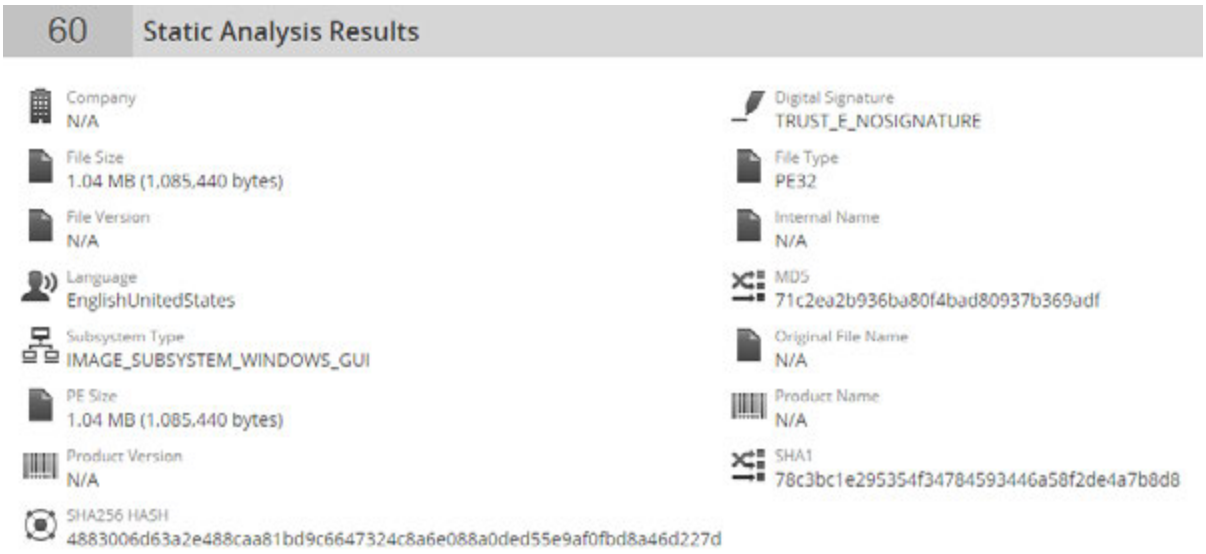
2. Hover over a meta value and left-click.
   The context menu is displayed.



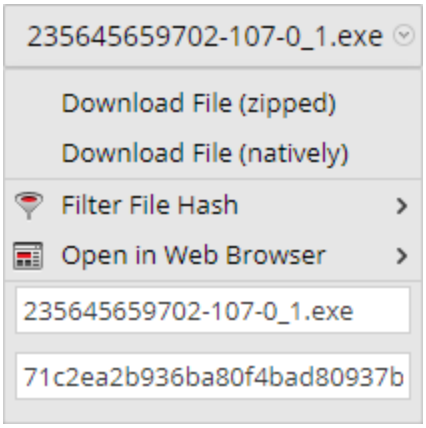
3. To view the selected meta value in the **Navigate** view, select **Start Investigation** and a time option.
4. To view the selected meta value in a browser, select **Open in Web Browser > Open in Google**.

Use File Actions in the Static Analysis Results

1. Scroll down to the Static Analysis Results.



2. If you want to download a file, select the file name and either **Download File (zipped)** or **Download File (natively)** in the drop-down menu. It is safer to download a file in zipped format.



3. If you want to mark the file as safe or unsafe in the hash list, select **Filter File Hash** and **Mark hash as good** or **Mark hash as bad**.

View Community Analysis Results Details

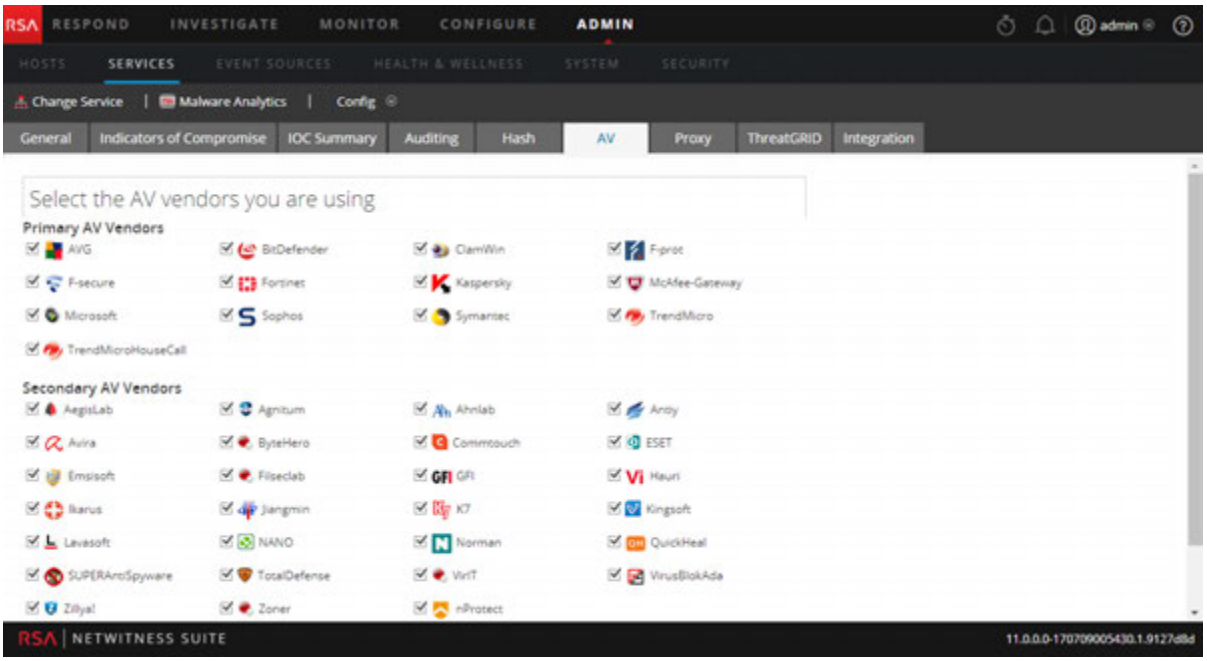
The Community Analysis Results summarizes results from the community, identifying Indicators of Compromise that were flagged as a risk or identified as good.

In addition, this view lists the results from Installed AV Vendors and Not Installed AV Vendors. You can compare results of the installed AV vendors that were configured for the current Malware Analysis service versus Community results. You can also see results from a list of AV vendors that are not configured as installed for the current Malware Analysis service.

Each row of AV vendor results includes the shield icon to show whether the IOC was discovered by a Primary ( ) or Secondary AV ( ) vendor in the community, the name of the Installed or Not Installed vendor, and the name of malware or risk detected by the community and AV vendor. If the AV vendor did not detect a risk, **-- Not detected --** is displayed instead of the name of the risk.

The Not Installed AV Vendors section is expandable to view all entries, but is collapsed by default to minimize the need to scroll. Clicking the + expands the list.

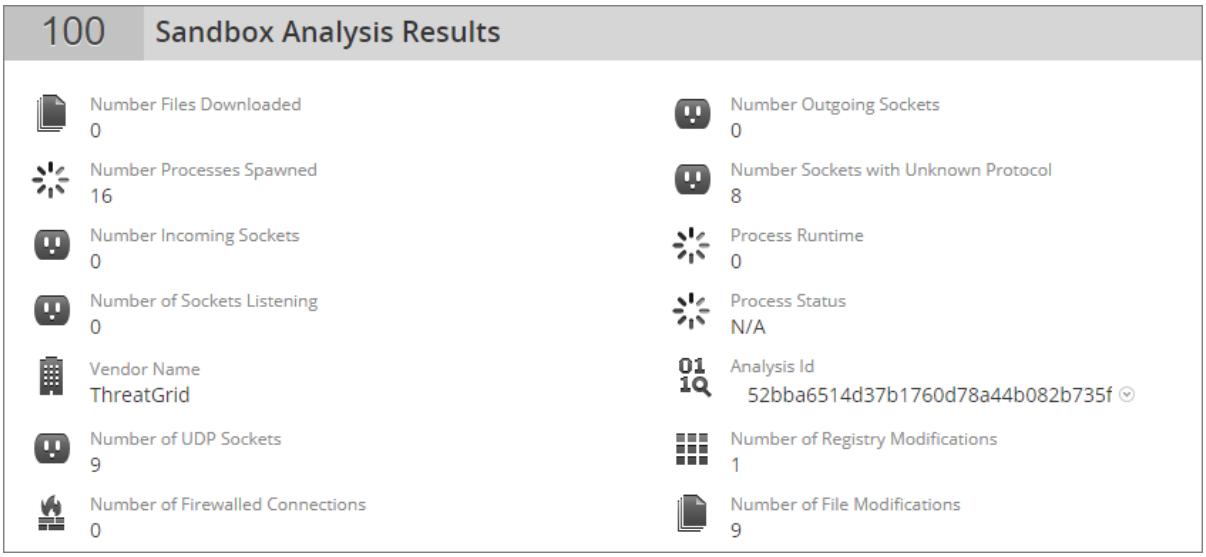
If no installed AV vendors have been configured for the current Malware Analysis service, the following message is displayed: No AV vendors were marked as installed. Please go to the Malware Analysis Service configuration page to identify installed AV vendors.



View Sandbox Analysis Results in the ThreatGrid User Interface

If you have registered with ThreatGrid, you can view the Sandbox results directly in ThreatGrid.

1. Scroll down to the Sandbox Analysis Results.



2. Click the **Analysis ID** and select **Open In ThreatGrid**.
   The analysis report in ThreatGrid is displayed.

Troubleshooting NetWitness Investigate

This section provides information about possible issues when using NetWitness Investigate.

Event Analysis Issues

Message	`Investigation Profiles/OOTB column groups are not present in Event Analysis`
Issue	Post upgrade to RSA NetWitness v11.1, the default column groups - Endpoint Analysis, Outbound SSL and Outbound Http are not added under column groups. Also, few of the Investigation Profiles are missing post upgrade.
Explanation	It is observed that this issue occurs only when you have created a custom column group with the name which is same as one of the new 11.1 OOTB custom column group name. For example, if you create a custom column group in 11.0 with name **RSA Endpoint Analysis** then after upgrade to 11.1. Due to the same name already existing in 11.1, OOTB column groups and OOTB profiles will not be available in the UI. To fix this, change the name of custom column group to something else and restart the jetty server by using the following command on the NetWitness server: `systemctl restart jetty`

Message	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
Issue	When you click **Pivot to Endpoint** in the Event Analysis view, no data is displayed and the message is displayed.
Explanation	Version 4.4 of the NetWitness Endpoint Thick Client must be installed on the same server, the NWE meta keys must exist in the `table-map.xml` file on the Log Decoder, and the NWE meta keys must exist in the `index-concentrator-custom.xml` file. The NWE Thick Client is a Windows only

	application. Complete setup instructions are provided in the *NetWitness Endpoint User Guide* for Version 4.4.

Message	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the *Physical Host Upgrade Guide*).`
Issue	When attempting to investigate a service that has not been updated to Version 11.1 in the Event Analysis view, the informational message is displayed.
Explanation	When an analyst opens the Event Analysis view in mixed mode (that is, some services are upgraded to 11.1 and some are still on 11.0.0.x or 10.6.x), Role-Based Access (RBAC) is not applied uniformly. This affects viewing and downloading content, and validation of filters in the interactive breadcrumb. You will see this informational message when you open Event Analysis. As you select a service, services that are not up to date are displayed in a red box, with the message that the service is not up to date. When your administrator has upgraded all connected services to 11.1, these features work as expected.

Message	`Forbidden. You cannot access the requested page.`
Issue	When attempting to access the Event Analysis view, the view opens with the message.
Explanation	Your administrator has prevented access to the Event Analysis view using role and permissions.

Message	`Insufficient permissions for the requested data.`
Issue	While attempting to access an event in Event Analysis by any means, the reconstruction is not displayed and the message is displayed.

Explanation	You have entered an event ID for an event that you do not have permission to view. The administrator may have placed some restrictions to limit access by role and permissions.

Message	`Invalid session ID: <<eventId>>`
Issue	No `sessionId` matches the `sessionId` that you queried.
Explanation	The reason for an invalid session ID can vary. Perhaps you edited the session ID manually, and no such session exists. Another case may be when you query a Broker, and the aggregated data has not been refreshed, you may see this error for a session that no longer exists.

Message	`No text data was generated during content reconstruction. This could mean that the event data was corrupt/invalid, or that an administrator has disabled the transmission of raw endpoint events in the Endpoint server configuration. Check the other reconstruction views.`
Issue	When you reconstruct an event as text in the Event Analysis view, no data is displayed and the message is displayed.
Explanation	If you do not see the raw text in other Event Analysis views or Events view reconstructions, and you believe the data is not corrupted or invalid, your administrator has likely disabled transmission of raw endpoint events on the NetWitness Endpoint server. Contact your administrator for additional information.

Message	`Session is unavailable for viewing.`
Issue	While querying an event ID, the reconstruction is not displayed and the message is displayed.

Explanation	The query you entered is trying to look at restricted data, for example, if you are allowed to see only log data and you are using a link to network data that you were allowed to see yesterday.

Message	`The session id is too large to be handled:<<eventId>`
Issue	The sessionId integer that you typed in, edited, or got from the Events view or Navigate view is too large.
Explanation	If you manually typed the sessionId or edited a sessionId in the Event Analysis view, you may have created an integer that is too large for Event Analysis to process.

Behavior	While creating a filter in the Event Analysis view, you cannot enter a complex expression using the `AND` or `OR` operator in Query Builder.
Issue	The query builder in the Event Analysis view supports only simple expressions in the form `<meta key><operator><meta value>`.
Explanation	If you want to enter a filter that uses the `AND` or `OR` operator, you need to enter the query it from the Navigate view or Events view and then open it in the Event Analysis view. You can enter some complex expressions as two separate filters in the Event Analysis view. The filters will be AND'd when you execute the query.

Hosts View Issues

Message	`An error has occurred. The Endpoint Server may be offline or inaccessible.`
Issue	When attempting to access the Hosts or Files view, the view opens with the message.
Explanation	Endpoint Server or Nginx Server is not running. Check the status of the Endpoint Server under **Admin > Service** or check if the Endpoint Server host IP address is registered with the Admin Server. For more information, see the *RSA NetWitness Suite Physical Host Installation Guide* or *RSA NetWitness Suite*

	Virtual Host Installation Guide. If the service is not running, start the Endpoint Server.

Issue	The Hosts and Files views do not load in the Safari browser.
Explanation	When you open the Ember pages in the Safari browser with a non-trusted SSL certificate, the Hosts and Files views do not load. To load the views. 1. Click the **Show Certificate** pop-up menu. 2. Enable the **Always trust NetWitness when connecting to <IP Address>** checkbox. 3. Click **Continue**. 4. Enter your username and password. 5. Click **Update Settings**.

Message	`No process information was found.`
Issue	When attempting to access the Process or Libraries tab in the Host Details view, the detailed host information is not available, and the view opens with the message.
Explanation	Scan data is not available due to any of the following reasons: • First time scan is not complete • Data retention policy has deleted all scan snapshots

Files View Issues

Behavior	Meta values will take time to load.
Issue	Meta values are not set to index by values.
Explanation	During investigation, while pivoting to the Navigate or Event Analysis view from the Files view, if the filename or hash (SHA256 and MD5) are not set to index by values, the matching results take time to load as the Concentrator must generate the index by accessing the meta database and retrieving value of the meta for each event. You have to manually index the values before pivoting.

Issue	Filtering files takes a longer time to load results on the UI.
Explanation	In the Files view, while filtering files with the `Contains` operator, the results takes a few seconds to load on the UI. You must use at least one indexed field with the `Equals` operator while filtering the files.

Investigate Reference Materials

This section provides is intended to help you understand the purpose and application of NetWitness Investigate views. For each view, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition some of the reference materials include workflows and Quick Looks to highlight important features in the user interface.

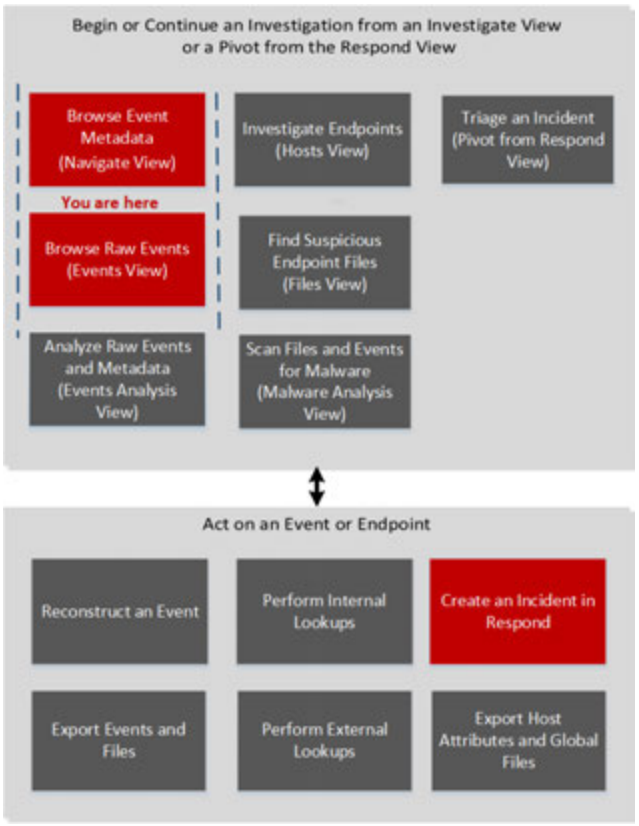
- Investigate View
- Navigate View
- Events View
- Hosts View
- Files View
- Malware Analysis View
- Add/Remove from List Dialog
- Add Events to an Incident Dialog
- Context Lookup Panel
- Create an Incident Dialog
- Event Analysis View
- Event Analysis View - Text Analysis Panel
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - File Analysis Panel
- Event Reconstruction View
- Investigate Dialog
- Investigation Tab - User Preferences Panel
- Manage Default Meta Keys Dialog
- Malware Analysis Events List and Files List
- Manage Column Groups Dialog
- Manage Profiles Dialog
- Navigate View

- Query Dialog
- Scan For Malware Dialog
- Select a Malware Analysis Service Dialog
- Settings Dialogs for Investigate Views
- Hosts View - Overview Tab
- Hosts View - Process Tab
- Hosts View - Autoruns Tab
- Hosts View - Files Tab
- Hosts View - Drivers Tab
- Hosts View - Libraries Tab
- Hosts View - System Information Tab

Add Events to an Incident Dialog

In the Add Events to an Incident dialog, analysts can add alerts to an existing incident so that incident responders look at the associated events as part of an incident response. To access this dialog while investigating a service in the Events view, select **Incidents > Add to Existing Incident** from the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter or Incident Responder	add one or more events to an existing incident or to a new incident*	Add Events to an Incident for Response

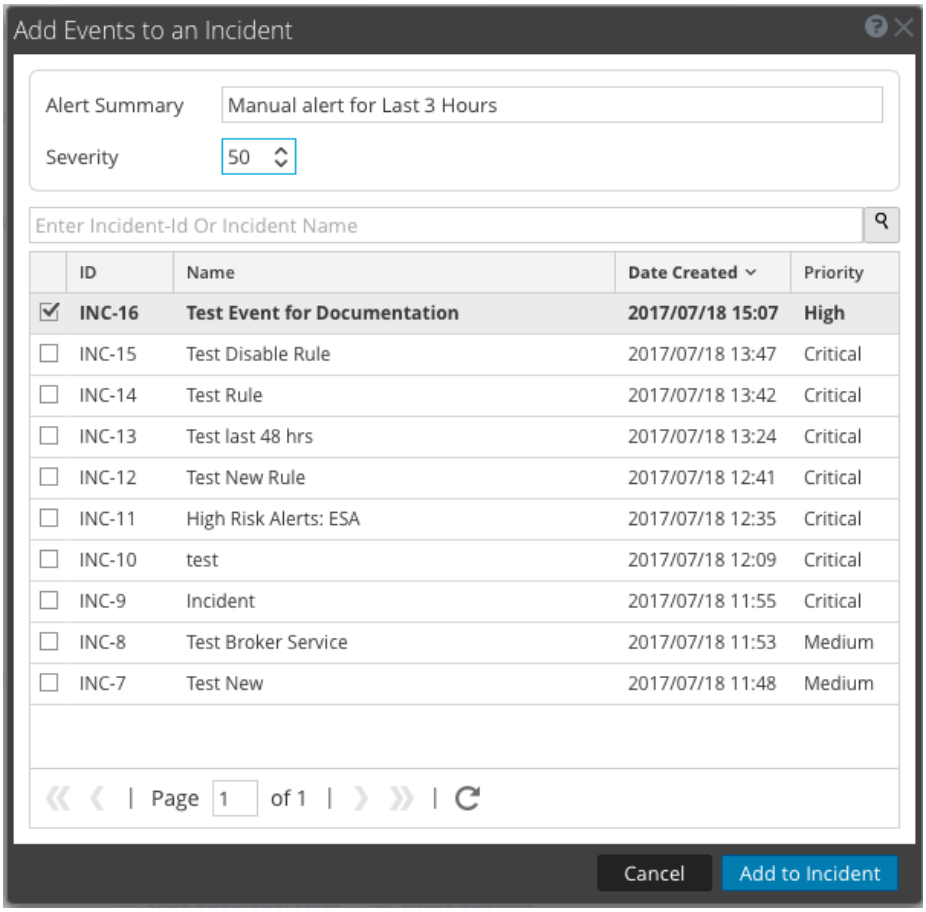
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View

Quick Look

The following figure is an example of the Add Events to an Incident dialog. The table describes the information and options in the Add Alerts to an Incident dialog .



Feature	Description
Alert Summary	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Search	Allows you to search for an existing event.
ID	The ID of the incident. You can sort IDs in ascending or descending order.
Name	The incident name. You can sort the Name in ascending or descending order.

Feature	Description
Date Created	Displays the date and time the incident was created. You can sort the dates in ascending or descending order.
Priority	Displays the priority of the incident: either low or critical.
Cancel	Closes the dialog without saving changes.
Add to Incident	Adds the alerts to the incident. A dialog confirms that alerts are successfully added

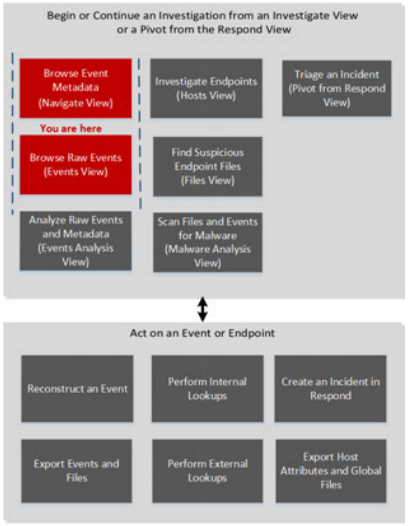
Add/Remove from List Dialog

When working in Investigate, you may find an IP address or user name that you want to watch in the Navigate view or the Events view. In the Add/Remove from List dialog, you can add meta values for the `Source IP`, `Destination IP`, or `Username` meta keys to an existing context hub list or you can create a new list containing the meta values. When you add meta values to a list, you can look up additional context on those meta values.

To display the dialog. right-click a meta value under `Source IP`, `Destination IP`, or `Username`) and select **Add/Remove from List** in the context menu.

Workflow

The following workflow diagram shows the high-level workflow for Investigate with the location of the Add to List task highlighted.



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

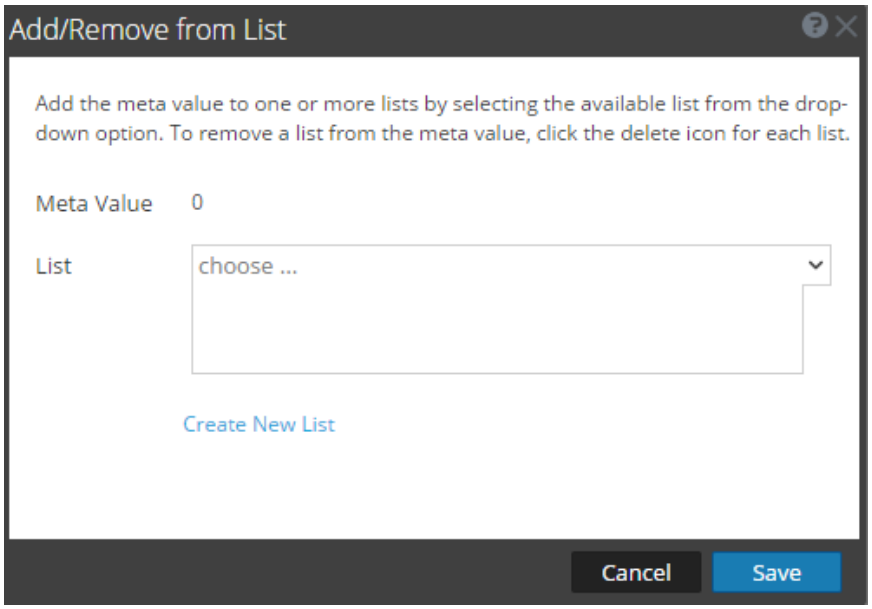
User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	create or add meta values to a Context Hub List*	Manage Context Hub Lists and List Values in Investigate

Related Topics

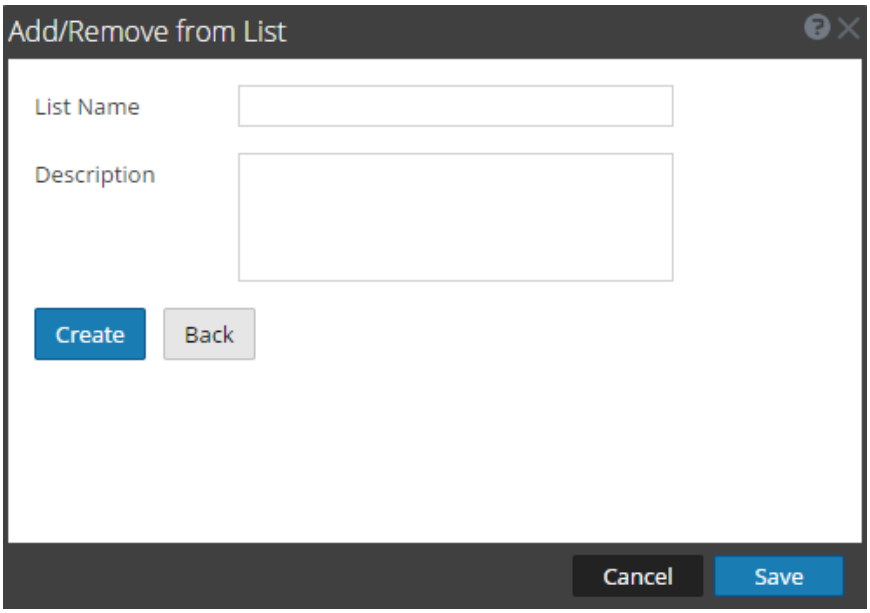
- View Additional Context for a Data Point
- Navigate View
- Events View

Quick Look

The following figure is an example of the dialog when initially opened.



The following figure shows the dialog when you select Create New List.



The following table describes the features of Add/Remove from List and Create New List dialogs.

Feature	Description

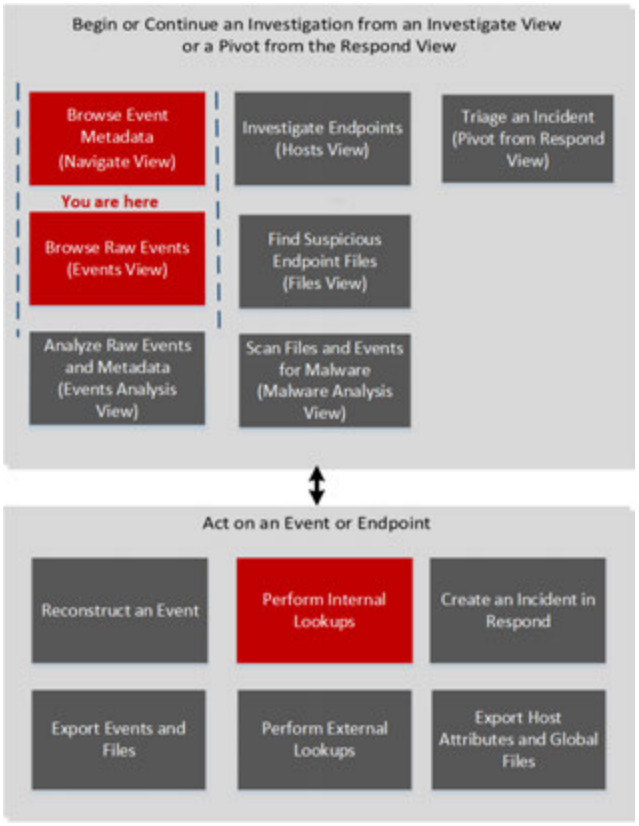
Feature	Description
Meta Value	The selected meta value to be added to the existing or new list.
List	The list to which the selected meta value must be added. A drop-down menu provides a list of available lists to which you can add the meta value.
Create New List	Opens a new dialog in which you can create a new list for the selected meta value.
List Name	The name of the new list.
Description	The description of the new list.
Create	Create a new list after entering the required fields.
Back	In the new list mode, cancels the new list creation and returns to the original dialog.
Cancel	Cancels the addition of the meta value to a list and closes the dialog.
Save	Saves the changes made to the lists and closes the dialog.

Context Lookup Panel

After an administrator configures the Context Hub service, you can view the contextual information for the meta values in the Navigate view and the Events view of the Investigate. The Context Hub service is pre-configured with default meta type and meta key mapping. For information about the mapping of the context hub meta value with investigation meta key, see "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.

The Context Lookup panel is displayed on the right side of the Navigate view and Events view. Meta values that have been added to a Context Hub list are highlighted in gray in the Navigate view or Events view results. When you right-click a highlighted value and select **Context Lookup** in the resulting context menu, the lookup results are displayed in the Context Lookup panel for configured sources for the selected meta value. You can select a source in the Context Lookup panel icon bar to view the contextual information.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	look up additional context for a meta value	View Additional Context for a Data Point

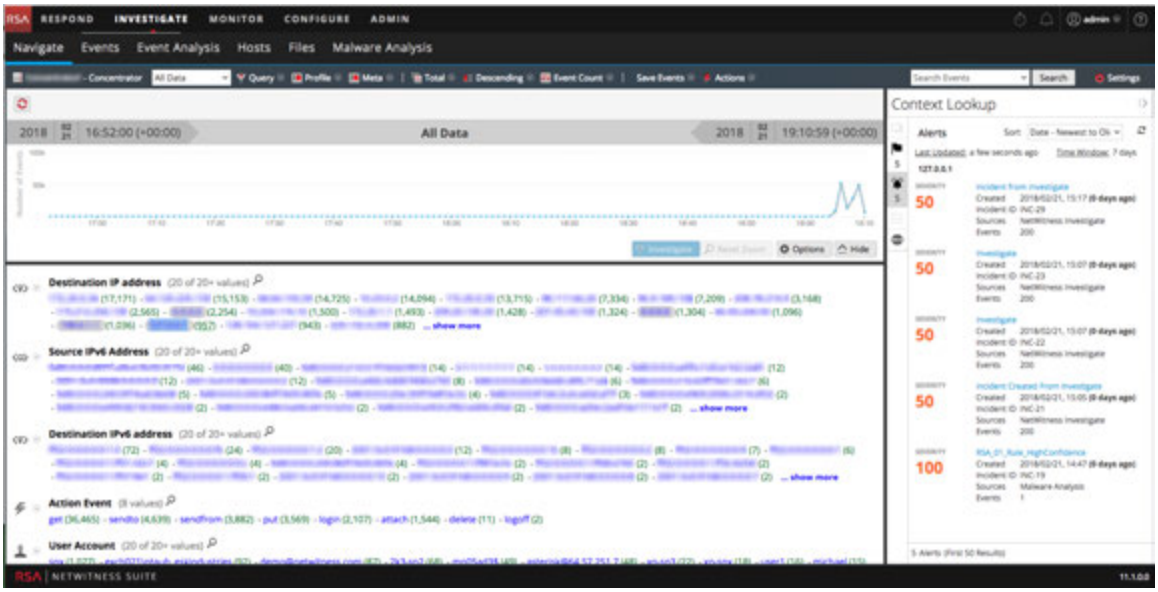
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View
- Navigate View
- "NetWitness Feedback and Data Sharing" in the *Live Services Management Guide*

Quick Look

The following figure is an example of the Context Lookup panel, and controls and features are described in the table.



Feature	Description
Source Options Bar	Displays the icons for the available sources: Endpoint, Incidents, Alerts, and Lists.
Source Name	Displays the source name based on the selected icon: • Endpoint • INCIDENTS • ALERTS • LISTS
Sort	Provides a drop-down of sort options for the listed context information. Possible sort options are Severity - High to Low, Severity Low to High, Date - Oldest to Newest. and Date - Newest to Oldest. The sorting options vary by source type.
	Refreshes the lookup results.

Feature	Description
n items (First n Results)	The footer provides a count of the total number of results, and the count of results currently displayed. For example, 50 Alerts (First 50 Alerts).

Lookup Results

The Context Lookup panel displays the following information when retrieving the context data from the configured sources.

Incidents

Incidents are displayed based on time first (Newest to Oldest) and then priority status. The following information is displayed for incident lookups:

- Incident Name and ID
- Priority status of the incidents
- Risk Score value of the incidents
- Date when the incident was created
- Status of the incident
- Assignee for the incident
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last (Days)" field in the Configure Respond window. For details, see the "Configure Respond as a Data Source" topic in the *Context Hub Configuration Guide*.
- Sort: This drop-down field provides options to change the sorting of result based on time or priority.

Alerts

Alerts are displayed based on the Severity. ;The following information is displayed for alert lookups:

- Alert Name
- Severity value of the alerts
- Date when the alert was created

- Incident ID: This is the ID of the incident that the alert is associated with (If any).
- Sources: Event source name
- Number of events associated with the alert.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last (Days)" field in the Configure Respond window. For details, see the "Configure Respond as a Data Source" topic in the *Context Hub Configuration Guide*
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

Lists

The following information is displayed for list lookups.

- List Name
- Owner who created the list
- Created Date
- Last Updated Date
- Description of the list

Endpoint

The following information is displayed for Endpoint lookups.

- Machine name and IP address of the machine.
  By clicking on the IP or Endpoint machine name, you will be navigated to Endpoint UI to perform further investigation.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Machine Score: A machine IIOC score is aggregated based on the module scores.
- Number of modules: Number of active files for the selected machine.
- Last Updated: Indicates when the scan results were last updated in Endpoint database.
- Last Login User
- Machine MAC Address

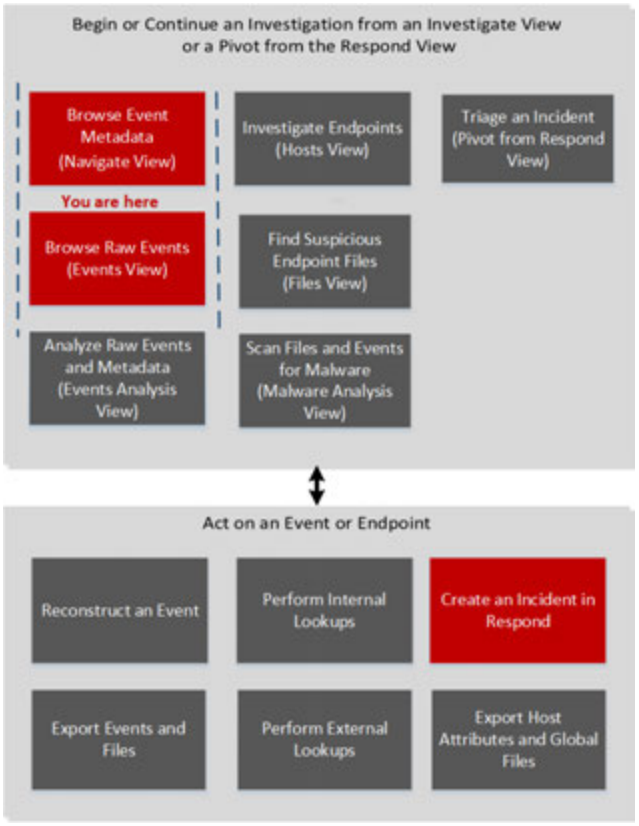
- Operating System Version
- Admin Notes (if any)
- Admin Status (if any)
- Top Suspicious Modules (Modules that have an IIOC score > 500). This is based on the value set for "Minimum IIOC Score" field in the Configure Endpoint window. The default value for "Minimum IIOC Score" is 500.
- Machine IIOC Levels

Create an Incident Dialog

In the Create an Incident dialog, analysts can create an incident from selected events in the Events view. The incident is then available to incident responders working in Respond.

To access this dialog, while investigating a service in the Investigation > Events view, select **Incidents > Create New Incident** from the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

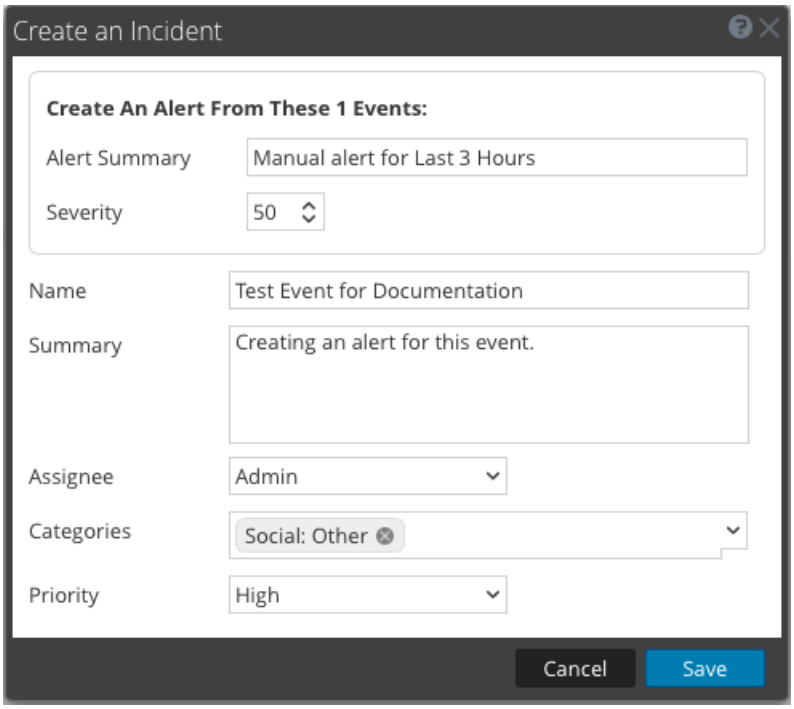
User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter or Incident Responder	add one or more events to an existing incident or to a new incident*	Add Events to an Incident for Response

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

The following figure is an example of the Create an Incident Dialog, and the features are described in the table.



Feature	Description
Create Summary from These Events	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Name	(Required) Specifies a name to identify the incident. In the example, the name is Sample Incident. You can provide a name that clearly identifies the nature of events that will be added to this incident
Summary	(Optional) Specifies a description for the incident. A good summary clearly identifies the incident for other analysts and responders.
Assignee	(Optional) Assigns the incident to a user in the SOC. Clicking Assignee opens a drop-down list showing the user names of SOC personnel who respond to incidents.

Feature	Description
Categories	(Optional) Identifies categories of incidents. Clicking Categories, opens a drop-down list of Incident categories and subcategories. You can select one or more categories to which the incident belongs. Categories fall into these major groups: Environmental, Error, Hacking, Malware, Misuse, and Social.
Priority	Identifies the priority for the incident. Clicking Priority opens a drop-down list of priorities: Critical, High, Medium, or Low displayed in the drop-down list.
Cancel	Closes the dialog without saving changes.
Save	Saves the incident and closes the dialog. A message confirms that the incident was created successfully.

Event Analysis View

In the Event Analysis view analysts can view raw events and meta data with interactive features that enhance the ability to find meaningful patterns in the data. This is an alternative to the static Event Reconstruction view. You can examine network, log, and endpoint events in the Event Analysis view. The Event Analysis view offers packet, text, and log reconstruction, and does not support email and web reconstruction directly. However, in Version 11.1 and later, you can open an email or web reconstruction of the current results in the Events view email or web reconstruction.

Note: The administrator sets permission for analysts to access this view. If your administrator has not given you access, and you navigate to the Event Analysis view by any means, the following message is displayed: `Forbidden. You cannot access the requested page.` For example, if you are viewing a reconstruction from the Events view and attempt to view the same reconstruction in the Event Analysis view, you will see the `Forbidden` message.

The events displayed in the Events Analysis view are for the current drill point in the Navigate view or Events view. Beginning with Version 11.1, the events can be the results of a query entered in the Event Analysis view breadcrumb. Whatever the source of the query, the Event Analysis view lists events in order by time. You can rearrange and resize the columns, In Version 11.1 and later, you can also choose the columns that you want to see and select one of the built-in column groups or a custom column group.

When you click an event, the Network Event Details, Log Event Details, or the Endpoint Event Details panel opens in the same browser window. Each type of event has one or more types of analysis: Text Analysis, Packet Analysis, and File Analysis.

There are multiple access points to this view, which are described in Begin an Investigation in the Event Analysis View.

Workflow

The following figure is a high-level workflow illustrating the tasks you can do in NetWitness Investigate, with the Event Analysis view tasks highlighted in red.

What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata*	Begin an Investigation in the Event Analysis View
Threat Hunter	query events in the Event Analysis view (Version 11.1)*	Filter Results in the Event Analysis View
Threat Hunter	export events and files in the Event Analysis view*	Download Data in the Event Analysis View
Threat Hunter	reconstruct events in Event Analysis view*	Examine Events in the Event Analysis View
Threat Hunter	perform external lookups from the Event Analysis view (Version 11.1)*	Act on Data in the Event Analysis View
Threat Hunter	query events in the Navigate view	Investigating Metadata in the Navigate View
Threat Hunter	query events in the Events view	Examining Raw Events in the Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - Text Analysis Panel
- Event Analysis View - File Analysis Panel

Quick Look

When you first open Investigate, input fields for a query are displayed so that you can select a service and time range, and type an optional query.

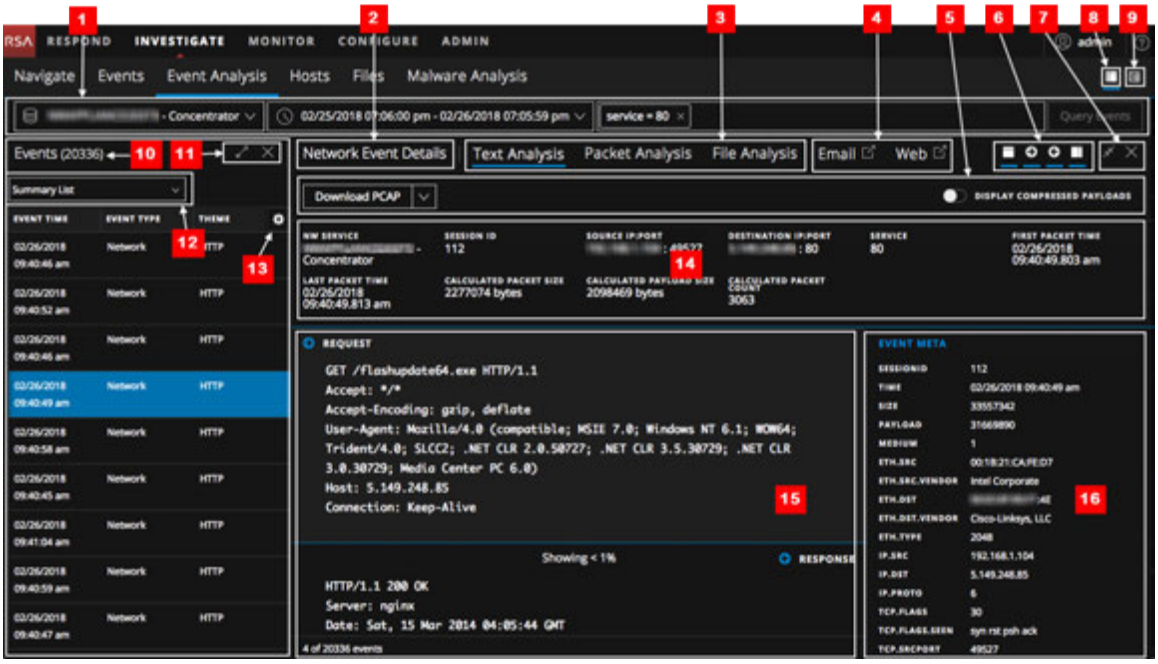
- Version 11.0 has the input fields in the Navigate view and the Events view.
- Version 11.1 has the input fields in the Navigate view, the Events view, and the Event Analysis view.

When you open a drill point in the Event Analysis view, the service being investigated counts the results of the initial query up to a limit of 100,000 events, and the first 100 events (packets, logs, and endpoint) are loaded in the Events panel. The columns in the Events panel are the Event Time, Event Type (Network, Log, or Endpoint), Event Size, and Summary. You can:

- Scroll through the list and click **Load More** to see the next 100 events.
- Select a column group (Version 11.1 and later).
- Select the columns that you want to include (Version 11.1 and later).

- Drag the columns to rearrange the order.
- Make columns wider or narrower.
- View the event analysis of an event.

The following figure highlights the major features of the Event Analysis view for Version 11.1 and later.



1	**Interactive Breadcrumb**: When a service is selected, displays the service selector, time range selector, and the queries you have entered. In Version 11.1 and later, you can select a service as described in Begin an Investigation in the Event Analysis View and refine the filters in the query as described in Filter Results in the Event Analysis View. Clicking the **Submit Query** button submits the query and sends a request to the selected service to load the data.
2	The type of event being analyzed is reflected in the heading: **Network Event Details**, **Log Event Details**, or **Endpoint Event Details**. Each view is discussed in detail in Examine Events in the Event Analysis View.
3	The types of analysis available for the event type. Network events can use all types of analysis: text, packet, and file. Log and endpoint events use only text analysis.
4	The Email and Web analysis types open the current event as an email or web reconstruction in the Events view.

5	These options vary for the different types of analysis. They are discussed in detail in Analyze Events in the Event Analysis View.
6	Controls to show or hide the Event Header, show or hide requests and responses, and open the Event Meta panel (16). These controls are described in Analyze Events in the Event Analysis View.
7, 11	Controls to change the size of the panel and close the panel.
8	Reopens the Events panel or the Event Meta panel if you have closed it.
9	Sets preferences for the Event Analysis view (see Configure the Event Analysis View.
10	The Events panel for Version 11.1 is interactive, displaying query results as you submit updated queries. The Events panel includes a count of the events. You can rearrange and resize columns. You can scroll to the bottom of the list, and load more events (see Analyze Events in the Event Analysis View).
12	The Column Group drop-down lists built-in and custom column groups that you can apply to the Events panel. The built-in column groups are Email Analysis, Endpoint Analysis, Malware Analysis, Outbound HTTP, Outbound SSL/TLS, and Summary List. Summary List is the default column group.
13	Settings to select the columns included in the Events panel.
14	The Event Header provides summary information about the event. This information is different for the different event types (packet, log, and endpoint).
15	The event data (sometimes called a payload for packets). The event data for a log event or endpoint event is typically a line of text from the raw log rather than request and response shown for a packet.
16	The Event Meta panel lists the meta keys and values found in the data. Some meta data are searchable; they have a binoculars icon, which you can click to see the associated data highlighted in the event data (see Analyze Events in the Event Analysis View.

The following figure highlights the major features of the Event Analysis view for Version 11.0.0.x.

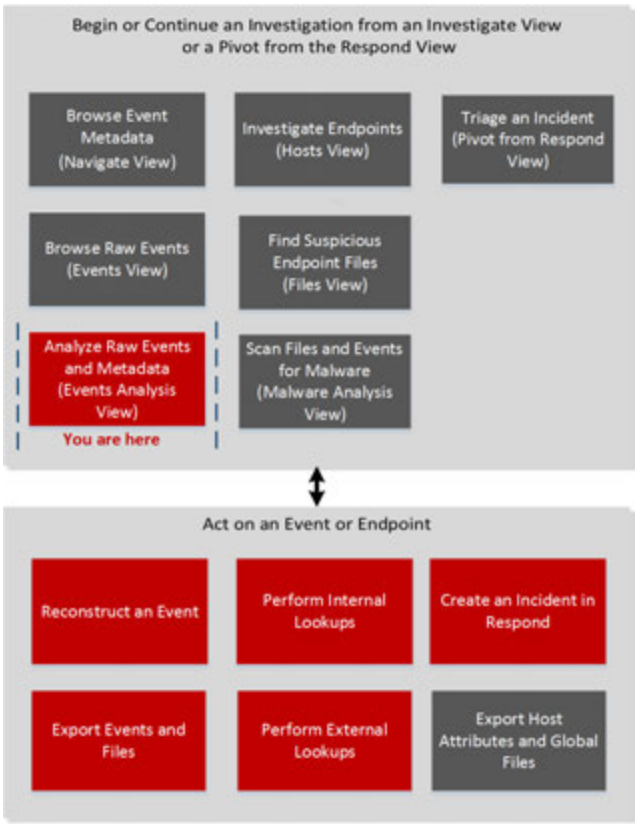
1	The read-only breadcrumb displays the selected service, time range, and query entered in the Navigate view or Events view.
2	This is a read-only list of events based on the query made in the Navigate or Events view. The Events panel includes a count of the events. You can rearrange and resize columns. You can scroll to the bottom of the list, and load more events (see Analyze Events in the Event Analysis View).
3, 8	Controls to change the size of the panel and close the panel.
4	The type of event being analyzed is reflected in the heading: Network Event Details, Log Event Details, or Endpoint Event Details. Each view is discussed in detail in Analyze Events in the Event Analysis View.
5	The types of analysis available for the event type. Network events can use all three types of analysis: text, packet, and file. Log and endpoint events use only text analysis.
6	These options vary for the different types of analysis. They are discussed in detail in Analyze Events in the Event Analysis View.
7	Controls to show or hide the Event Header, show or hide requests and responses, and open the Event Meta panel (12). These controls are described in Analyze Events in the Event Analysis View.

9	Reopens the Events panel or the Event Meta panel if you have closed it.
10	The Event Header provides summary information about the event. This information is different for the different event types (packet, log, and endpoint).
11	The event data (sometimes called a payload for packets). The event data for a log event or endpoint event is typically a line of text from the raw log rather than request and response shown for a packet.
12	The Event Meta panel lists the meta keys and values found in the data. Some meta data are searchable; they have a binoculars icon, which you can click to see the associated data highlighted in the event data (see Analyze Events in the Event Analysis View.

Event Analysis View - File Analysis Panel

In the File Analysis panel (**Event Analysis > File Analysis),** you can safely view a list of files and download one or more files in an event.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	query events in the Event Analysis view (Version 11.1)	Filter Results in the Event Analysis View
Threat Hunter	export events and files in the Event Analysis view*	Download Data in the Event Analysis View
Threat Hunter	reconstruct events in Event Analysis view	Examine Events in the Event Analysis View
Threat Hunter	perform external lookups from the Event Analysis view (Version 11.1)	Act on Data in the Event Analysis View
Threat Hunter	query events in the Navigate view	Investigating Metadata in the Navigate View
Threat Hunter	query events in the Events view	Examining Raw Events in the Events View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis

User Role	I want to ...	11.1 Documentation
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

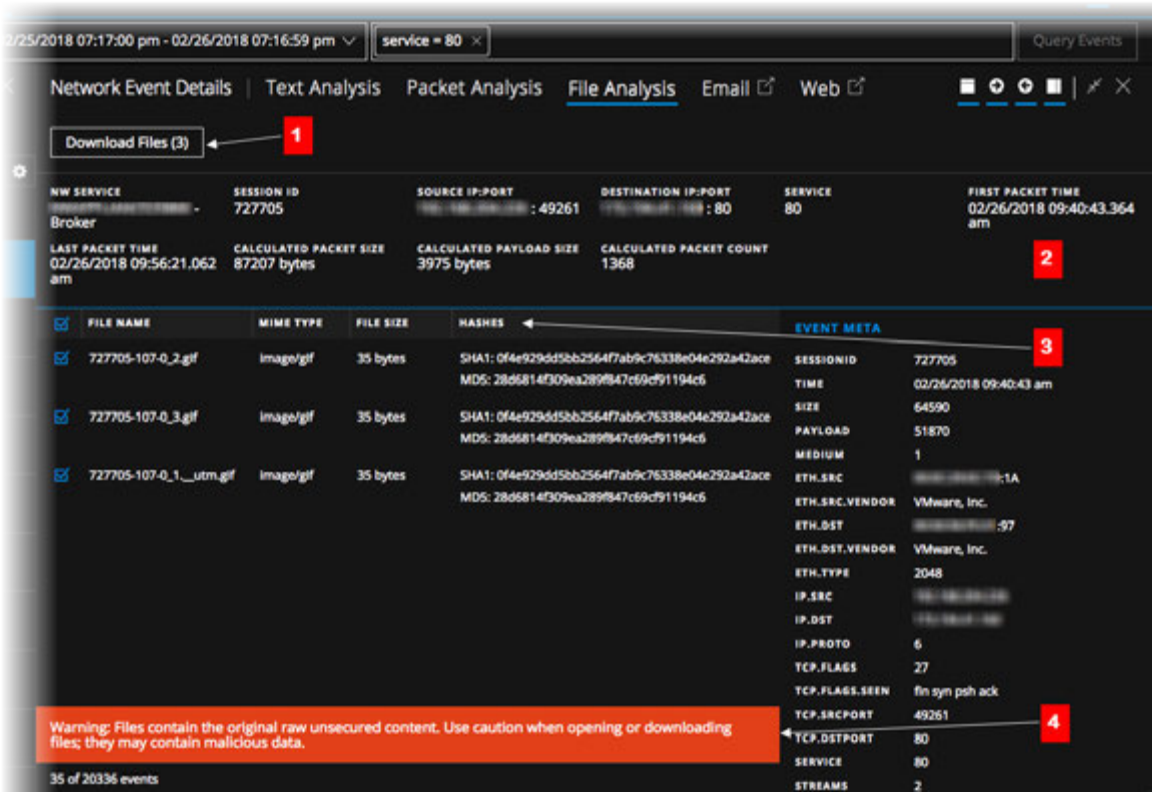
- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Text Analysis Panel
- Event Analysis View - Packet Analysis Panel

Quick Look

The File Analysis panel displays a list of files associated with a network event. You can download files in this view.

Below is an example of the File Analysis panel with labeled features.

Note: The Email and Web reconstruction types at the top of the figure are available in Version 11.1 and later.

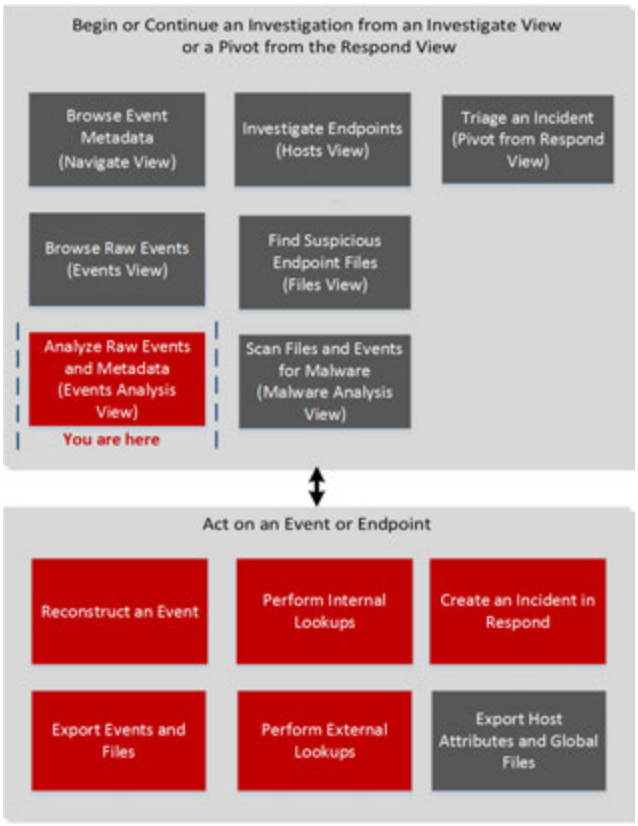


1	Click to download one or more selected files.
2	The Event Header displays summary information for the network event that contains the files.
3	Scrollable list of associated files that you can select and download.
4	Reminder that caution is necessary when downloading potentially malicious files.

Event Analysis View - Packet Analysis Panel

In the Packet Analysis panel (**Event Analysis > Packet Analysis),** you can safely view and interactively analyze the packets and payload of an event.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	query events in the Event Analysis view (Version 11.1)	Filter Results in the Event Analysis View
Threat Hunter	export events and files in the Event Analysis view*	Download Data in the Event Analysis View
Threat Hunter	reconstruct events in the Event Analysis view*	Examine Events in the Event Analysis View
Threat Hunter	perform external lookups from the Event Analysis view (Version 11.1)*	Act on Data in the Event Analysis View
Threat Hunter	query events in the Navigate view	Investigating Metadata in the Navigate View
Threat Hunter	query events in the Events view	Examining Raw Events in the Events View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis

User Role	I want to ...	11.1 Documentation
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Text Analysis Panel
- Event Analysis View - File Analysis Panel

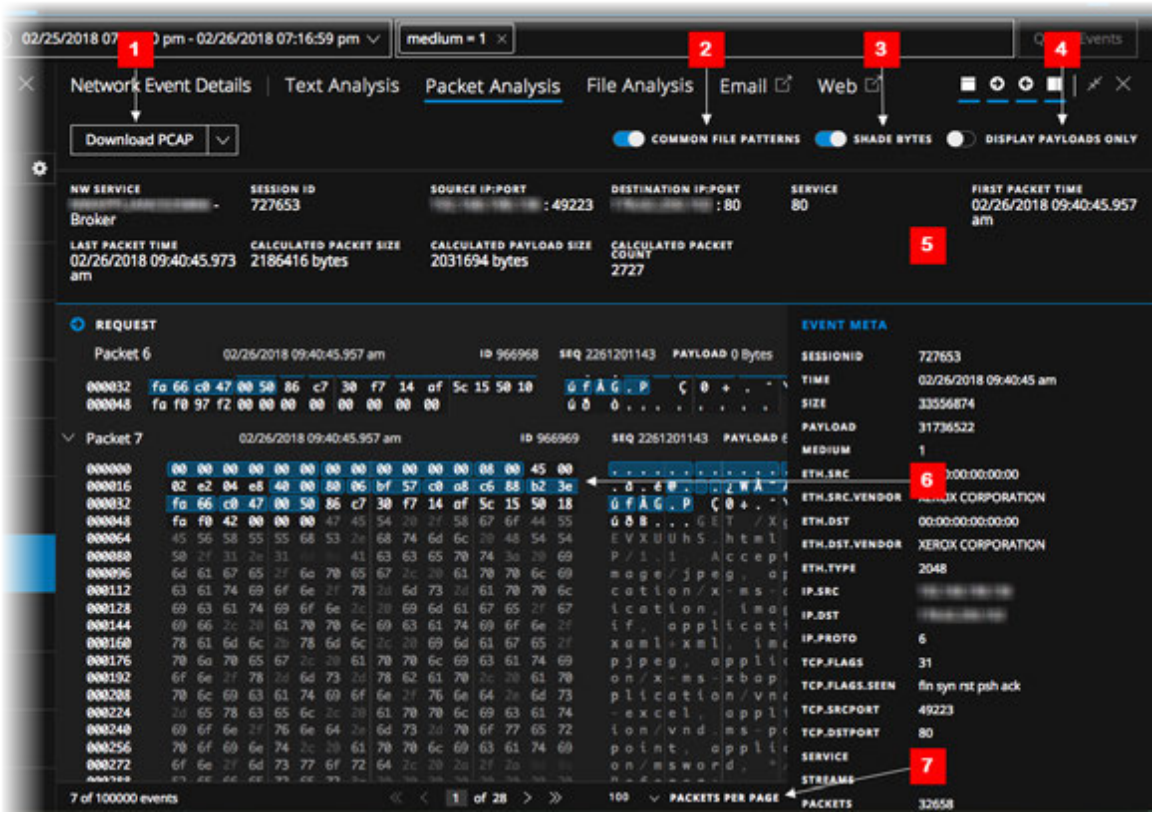
Quick Look

Only network events can be analyzed in the Packet Analysis panel. The Packet Analysis panel lists each packet in the event. The list of packets is scrollable. When you scroll, the packet or text identification information as well as the Request and Response labels remain visible rather than scrolling out of view.

In Version 11.1 and later, you can use pagination controls to go backward and forward through the pages, go to a specific page, and select the number of packets to display per page (100, 300, or 500).

Each packet is displayed with shading and highlighting to help identify common file patterns: significant header and payload bytes, hexadecimal and ascii bytes, and common file signatures. In addition, you can adjust the request/response display, and display or hide the packet summary.

Below is an example of the Packet Analysis panel with labels to identify features. For details and examples of each feature, see Examine Events in the Event Analysis View.

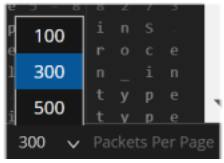


1	Options for exporting a network event. You can export a PCAP, all payloads, request payloads, or response payloads for deeper analysis and to share with others.
2	The option to identify common file signatures is activated by default. Common file signatures are highlighted in orange; hovering over the highlight reveals the file type.
3	The Shade Bytes option adds shading to identify the different hexadecimal bytes (00 to FF) using degrees of highlighting.
4	The option to display payloads only hides the packet headers, leaving more space for the payload.
5	The Event Header.
6	Significant bytes are highlighted in a blue background; as you move the cursor over the highlighting the meta data is displayed in a hover box.
7	(Version 11.1 and later) Packet pagination controls allow more flexibility in paging through a list of packets. When a control is unavailable, the image is dimmed; for example, when you are viewing page 1, the ⏮ and ◀ controls are dimmed. ⏮ - Go to the first page ◀ - Go to the previous page

- Go to a specific page

- Go to the next page

- Go to the last page

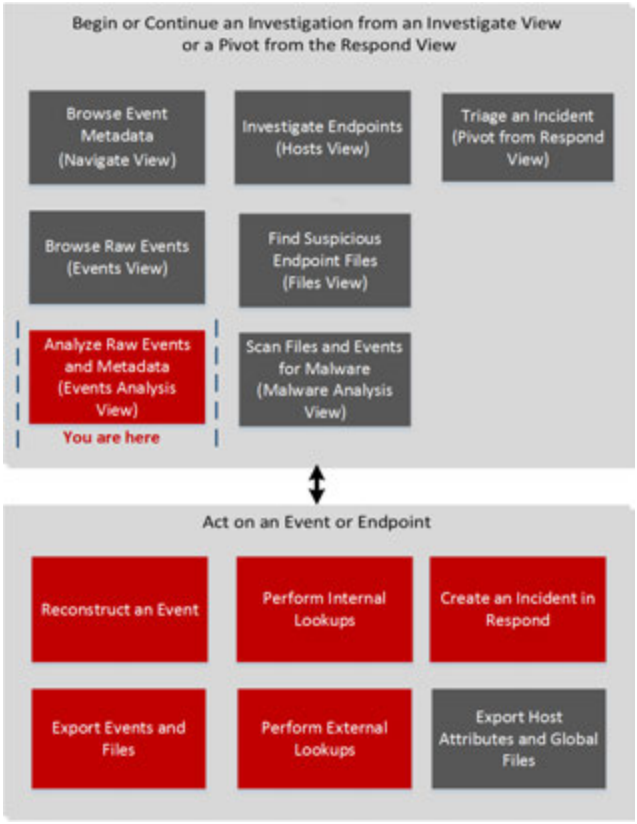


- Select the number of packets per page

Event Analysis View - Text Analysis Panel

In the Text Analysis panel (**Event Analysis > Text Analysis),** you can safely view and analyze the raw text payload of an event. The Text Analysis panel includes features that can show decompressed or compressed text, expand truncated entries, perform URL and Base64 encoding and decoding, and download network events, logs, and endpoint events. The Text Analysis panel is available for all types of events: network, log, and endpoint.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	query events in the Event Analysis view (Version 11.1)	Filter Results in the Event Analysis View
Threat Hunter	export events and files in the Event Analysis view*	Download Data in the Event Analysis View
Threat Hunter	reconstruct events in Event Analysis view*	Examine Events in the Event Analysis View
Threat Hunter	perform external lookups from the Event Analysis view (Version 11.1)*	Act on Data in the Event Analysis View
Threat Hunter	query events in the Navigate view	Investigating Metadata in the Navigate View
Threat Hunter	query events in the Events view	Examining Raw Events in the Events View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis

User Role	I want to ...	11.1 Documentation
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

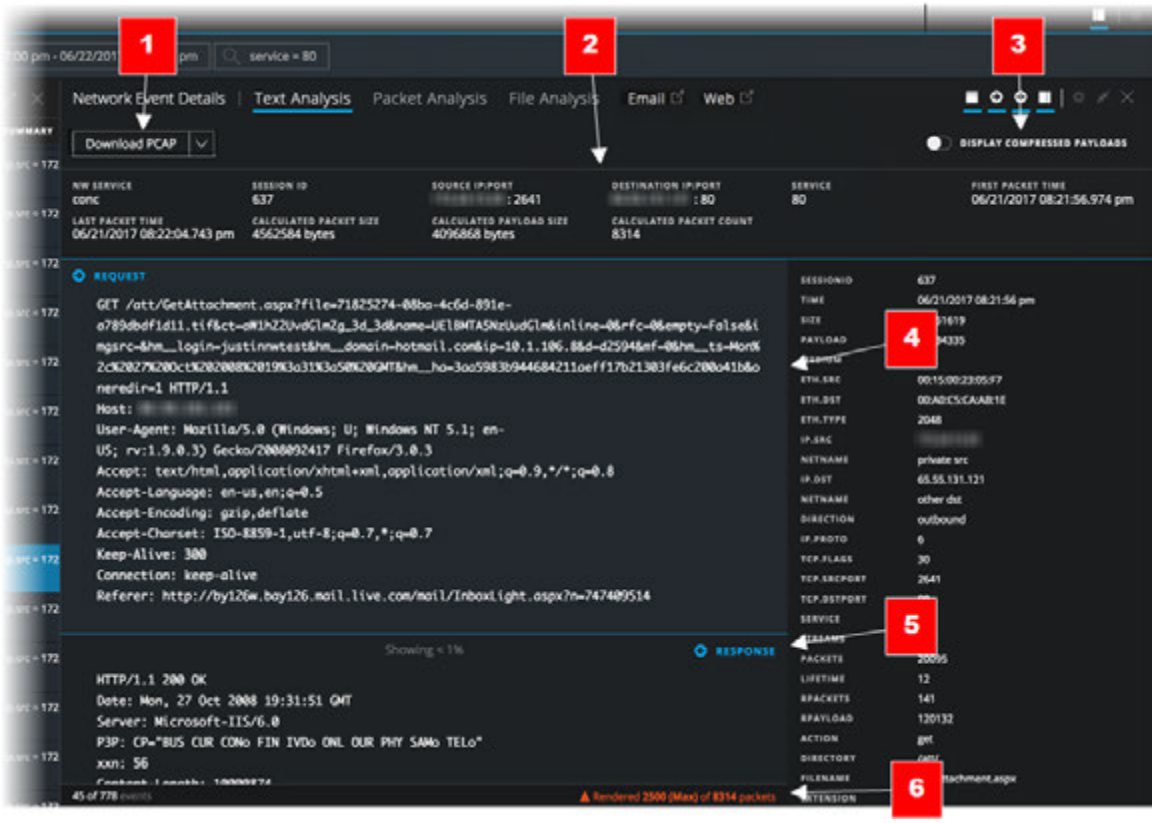
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - File Analysis Panel

Quick Look

The Event Analysis view displays the text of a single event in the Text Analysis panel. When you click an event in the Event list panel, the adjacent panel shows the Text Analysis. Only the raw log for log events and endpoint events is shown in the Text Analysis panel. For network events, the direction of the packet (Request or Response) and contents of each packet are provided in text format. For more examples of the Text Analysis, see Analyzing Raw Events and Metadata in the Event Analysis View. For detailed procedures, see Examine Events in the Event Analysis View.



1	Options for exporting a log, a PCAP, or files for deeper analysis and to share with others. This download menu is for network data.
2	The event header information.
3	Click to view the network payload in compressed or decompressed form.
4	The payload for a network event includes requests and responses. This is the request side of the packet.
5	This is the response side of the packet. Only 1% of the response is displayed because it has been truncated to allow viewing of more packets. When you scroll down, you can click an option to display the rest of the payload.
6	This message is displayed when the threshold of 2500 packets is reached, a measure to optimize performance. Additional packets will not be displayed. You may want to download the event to view all of the packets.

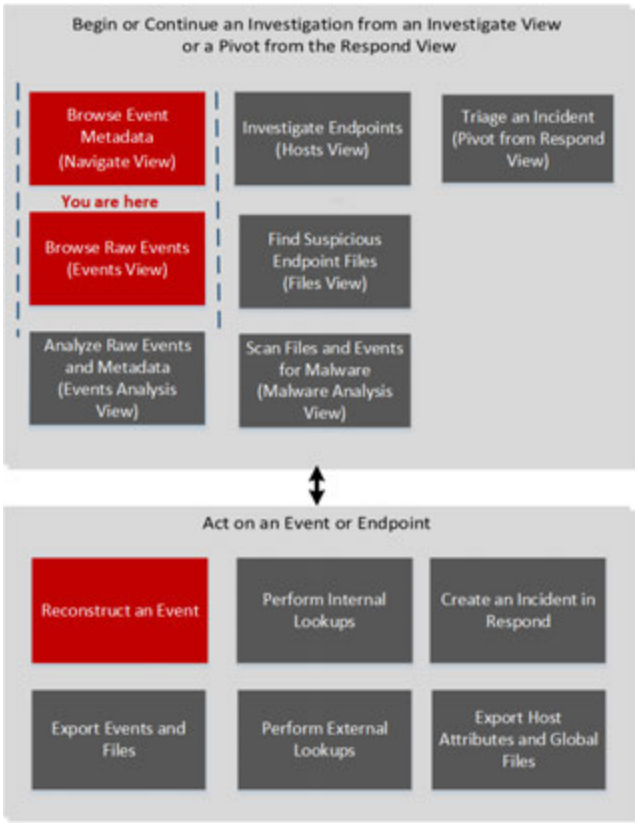
Event Reconstruction View

The Event Reconstruction view provides a reconstruction of a selected event from the Events view. By default, NetWitness Suite displays the best reconstruction for the event determined by the event content, or the default reconstruction that you have selected in the Default Session View setting for Investigate. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view top-to-bottom or side-by-side results, select request and response views, export an event, export meta values, extract files, open an email attachment, and open the event in a new tab.

To access this view, do one of the following:

- In any Events view, double-click an event.
- In the Events view with Detail View selected, right-click **Event Analysis** at the end of the event, and select **Event Reconstruction.**
- In the Event Reconstruction toolbar of previewed reconstruction, click **Open Event in New Tab**.
- In the Navigate view, select **Actions > Go to event in Event Reconstruction**, and enter an event ID.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View

User Role	I want to ...	11.1 Documentation
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	reconstruct an event	Reconstruct an Event
Threat Hunter	extract files from a reconstructed event	Reconstruct an Event

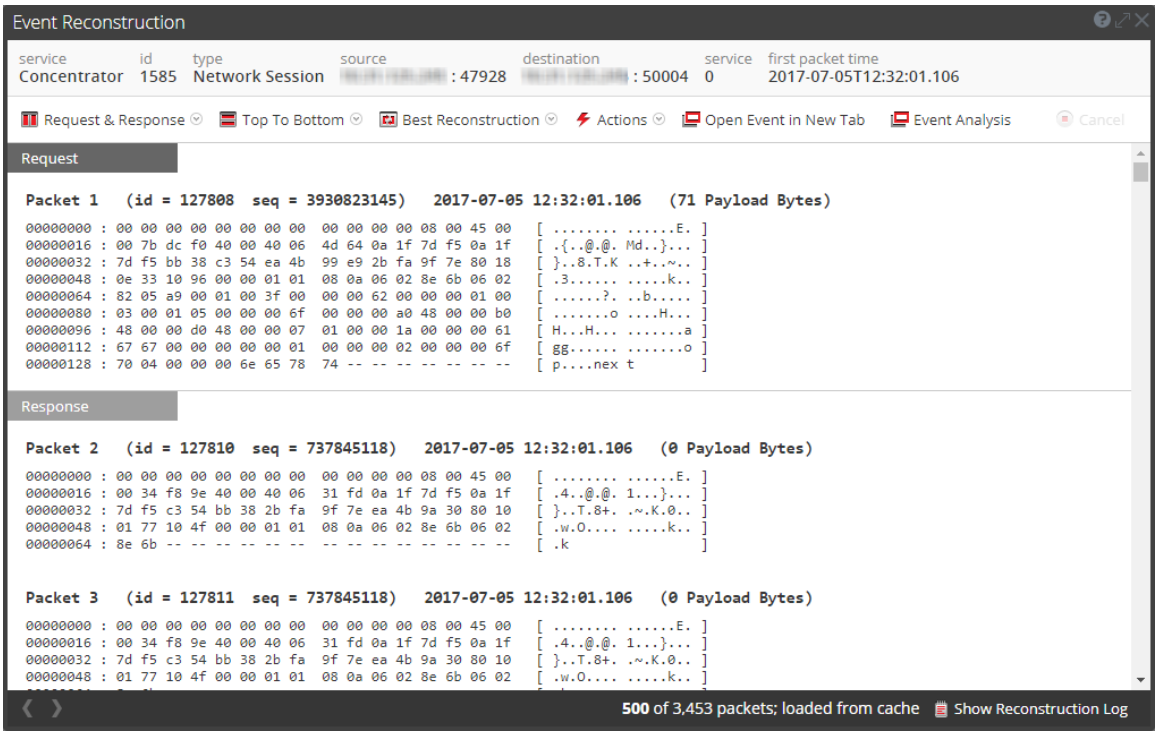
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View

Quick Look

This figure is an example of the Event Reconstruction view. The following table describes the toolbar options.



Feature	Description
Request & Response	Displays a drop-down menu for selecting whether the view displays: • Request & Response • Request • Response
Organization	Displays a drop-down menu for selecting whether the information is displayed top to bottom or side by side.

Feature	Description
View	Displays a drop-down menu for selecting what information is displayed. By default, Best Reconstruction is selected. Other options are: • View Meta • View Text • View Hex • View Packets • View Web • View Mail • View Files
Actions	Displays a drop-down menu with the actions available in the Event Reconstruction view.
Open Event in New Tab	Opens the event in a new browser tab.

Beneath the toolbar is a list of meta keys and values. Some of the keys offer a drop-down menu with available actions.

The bar at the bottom of the view offers several options.

Feature	Description
	Displays the previous event.
	Displays the next event.
Show Reconstruction Log	Displays the reconstruction log at the bottom of the view. Once you click this button, it changes to Hide Reconstruction Log.

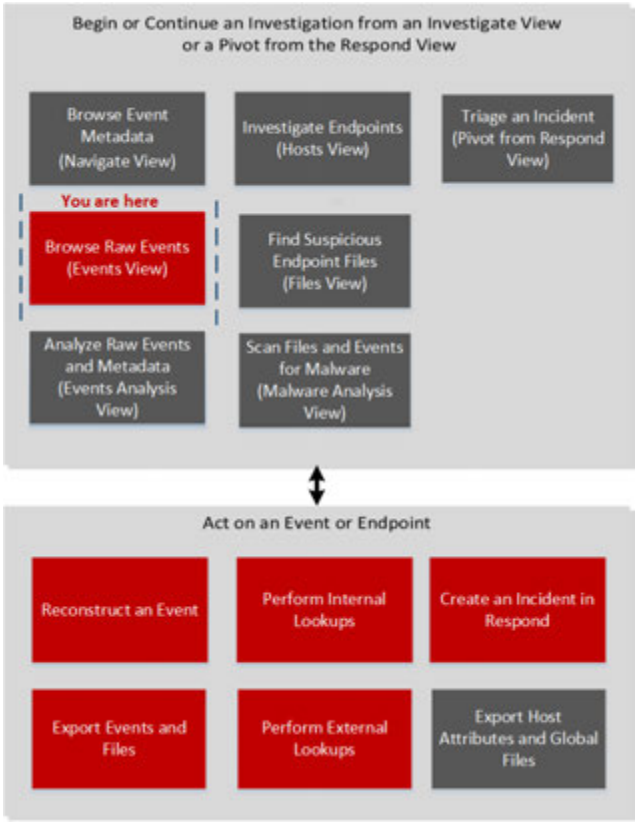
Events View

In the Events view a list of events associated with a session is available; this view is optimized for viewing raw events in sequence by time. You can display the events list in several forms, filter events, search for events, and open a reconstruction of an event.

There are two ways to display the Events view:

- Go to **INVESTIGATE > Events.** NetWitness Suite runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
- From within the **Navigate** view, double-click an event. The Events view displays the events on the selected service based on the drill point in the Navigate view.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events*	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	set user preferences for the Events view*	Configure the Navigate View and Events View
Threat Hunter	reconstruct an event*	Reconstruct an Event
Threat Hunter	export events and Files*	Export Events in the Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	perform internal lookups	View Additional Context for a Data Point
Threat Hunter	perform external lookups	Launch an External Lookup of a Meta Key
Threat Hunter or Incident Responder	add one or more events to an existing incident or to a new incident*	Add Events to an Incident for Response

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Examining Raw Events in the Events View
- Combine Events from Split Sessions
- Filter Results in the Event Analysis View
- Manage Column Groups in the Events View

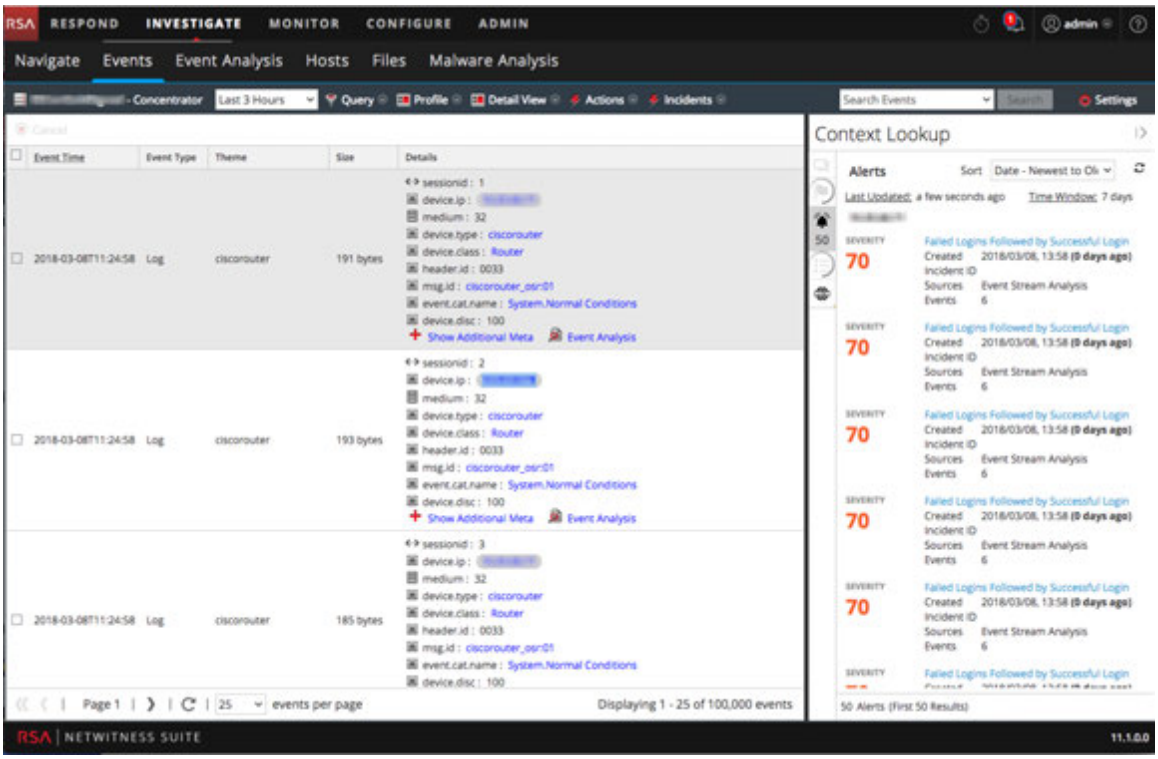
Quick Look

The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view. The List view and Detail view are intended for viewing packet data events, and they provide more information for each event including the timestamp, event type, event theme, and size.

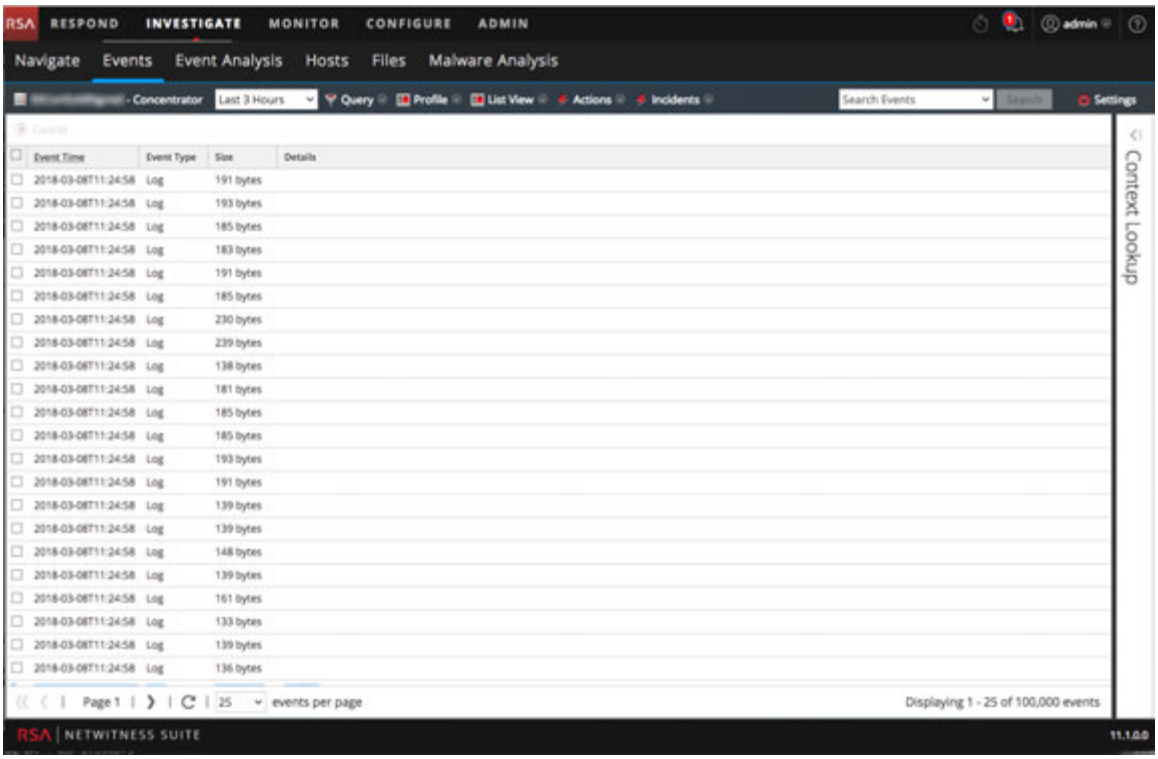
- The List View shows corresponding source and destination address and port information for events in summary form in a grid.
- The Detail View shows all metadata collected for the event in a paged view.
- The Log View is optimized for viewing log information, and provides more information for each log including the timestamp, event type, service type, service class, and the logs.

You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can extract files; export events, logs, and meta values; open the Event Reconstruction panel, and open Event Analysis.

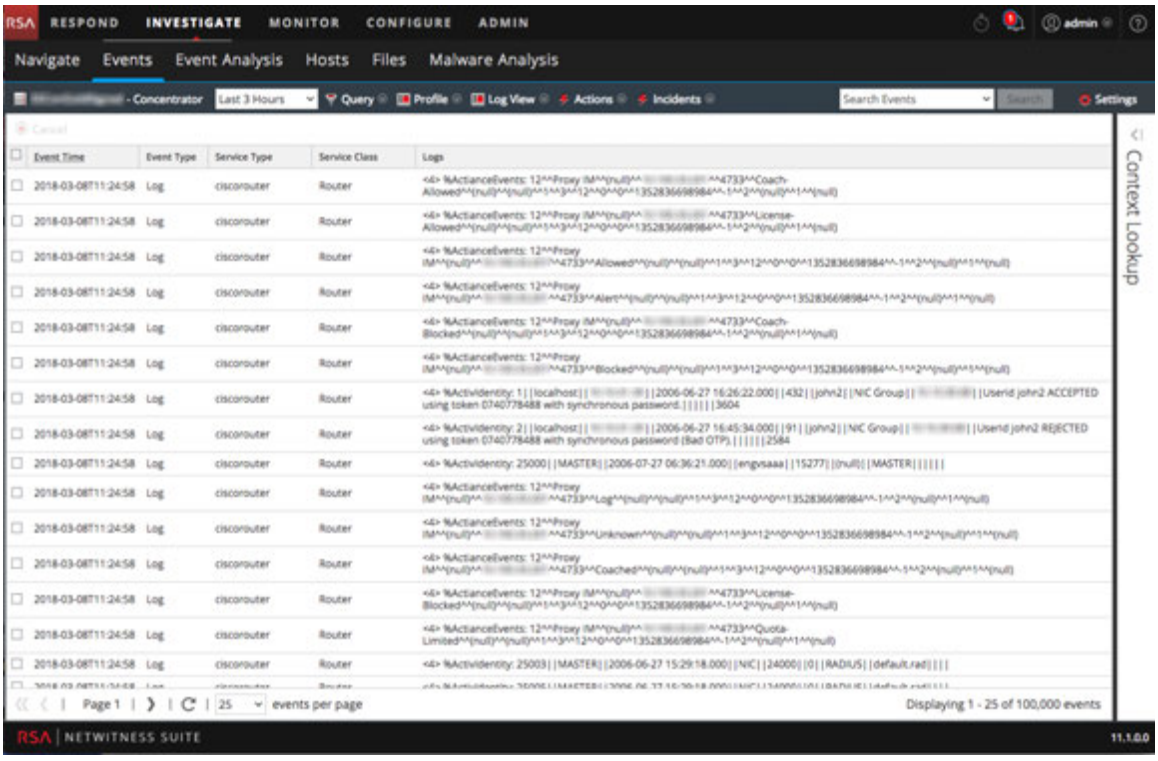
The following figure is an example of events in the Detail View. The Context Lookup panel is visible only if the Context Hub service is configured.



The following figure is an example of events in the List View.



The following figure is an example of the Log View.



Detailed Description

The Events view has a toolbar at the top with the following options.

Feature	Description
Select Service	Displays the selected service name next to the icon. Opens the Select a Service dialog, in which you can select a service for which the event list is displayed.
Time Range	Displays a drop-down menu for selecting the time range to apply to the event list. You can choose one of the standard options or specify a custom time range.
Query	Displays the Create Filter dialog, in which you can enter a custom query directly instead of drilling down the data (see Create a Custom Query)
Profile	Displays the Use Profile menu; the currently selected profile is displayed in the toolbar. A profile allows you to manage and use profiles that can include custom meta groups, a default column group, and a beginning query. The Profiles apply to the Navigate view (meta groups and queries) and the Events view (column groups and queries).

Feature	Description
View Type Drop-down	Displays a drop-down menu for selecting the event view type. • Detail View shows events in a paged format with detailed information for each event. • List view shows the events in grid form with a summary of each event in a separate row. • Log View shows a log-oriented events grid with a summary of each log in a separate row. • Custom Column Groups displays the event list using a column group selected from a drop-down list of custom column groups. • Manage Column Groups displays the dialog for creating and editing custom column groups.
Actions	Displays a drop-down menu with actions in the Events view: • Extract Files, export events as a PCAP file, export logs, or export meta values. • View an event reconstruction in a popup window or in a new tab. • View Event Analysis • Reset all filters in the Events view.
Incidents	Create a new incident in Respond and add the selected events, or add selected events to an existing incident in Respond.
Search	Displays the Search Events options, which allow you to specify the export log and export meta value format with additional options explained in Search for Text Patterns

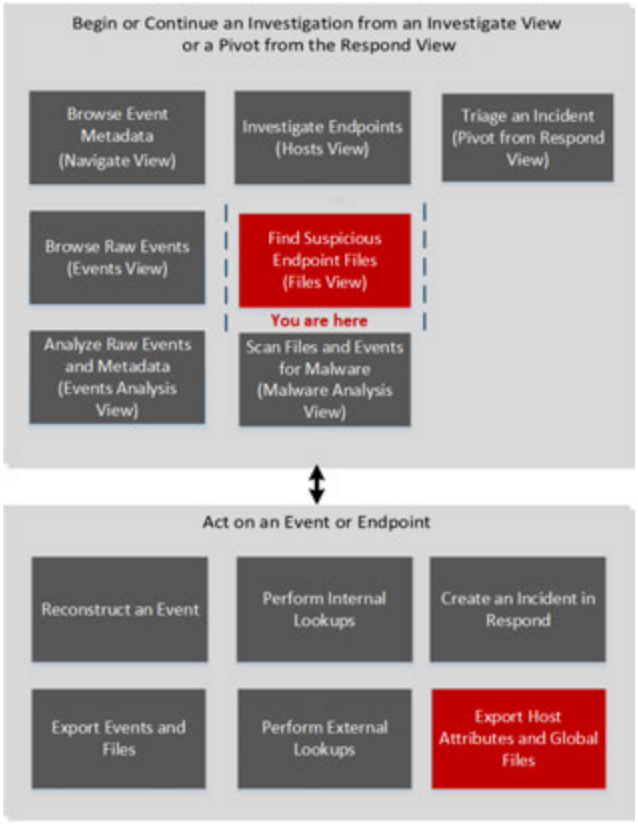
Feature	Description
Settings	Displays the Investigation settings for the Events view (which are also available in the Profile view) so that you can change Investigation settings without navigating away from the Events view. When you change a setting In the Events view the setting is also changed in the Profile view (see Configure the Navigate View and Events View).

Files View

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

In the **Files view**, a list of unique executable files found in the deployment is available. To access this view, go to **INVESTIGATE > Files**. By default, the Files view displays 100 files. To display more files, click **Load More** at the bottom of the page.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)*	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	export host attributes and global files*	Investigate Files

*You can perform this task in the current view

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files

Quick Look

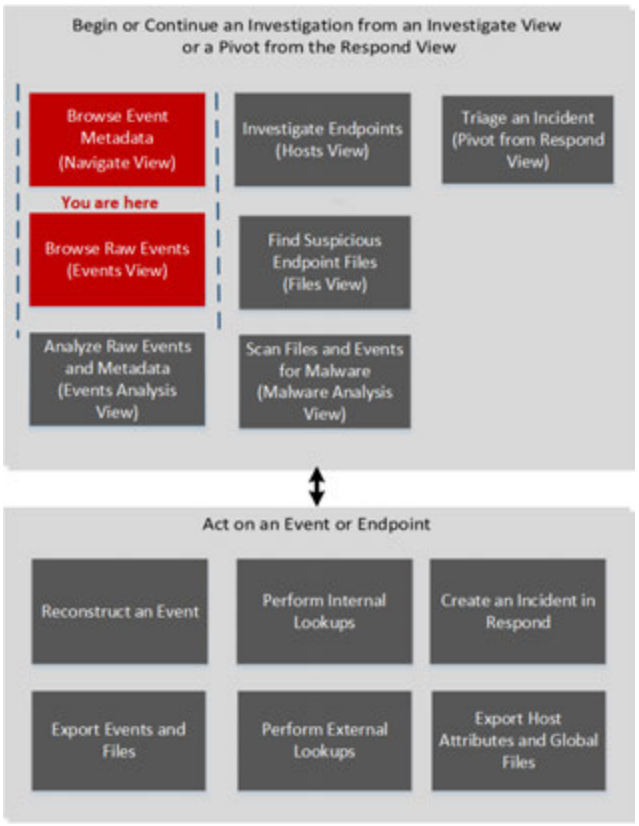
Below is an example of the Files view:

1	**Add Filter Drop-down Menu**. You can filter the files by choosing an operating system (Windows, Linux, or Mac), saved filters, or by selecting the options in the Add Filters drop-down menu. For more information, see Filter Files.
2	**Saved Filters.** The Saved Filters panel lists the saved filters. For more information, see Filter Files.
3	**Sort Columns.** You can sort the list by: **Filename** - Name of the file. **First Seen Time** - First time the hash was seen in the host. **Signature** - Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information. **Size** - Size of the file. **Entropy** - Determines if the contents are compressed or encrypted. **Format** - Format of the file - Windows (PE), Linux (ELF and scripts), and Mac (Macho). **PE.Resources.Company** - Company name.
4	**Settings Menu.** You can set Files view preferences by selecting columns from the Settings menu. For more information, see Set Files Preference.
5	**Export to CSV** - Extracts global files to a CSV file. For more information, see Investigate Files.
6	**Pivot to Navigate and Event Analysis views.** To investigate a particular filename or hash (SHA256 and MD5), you can pivot to both Navigate and Event Analysis views. For more information, see Pivot to Navigate and Event Analysis Views.

Investigate Dialog

In the Investigate dialog, analysts can select a service or a collection to investigate. The dialog is automatically displayed when you first go to the Navigate view or Events view and have not selected a default service to investigate. To access the dialog from a current investigation, select the current service name in the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

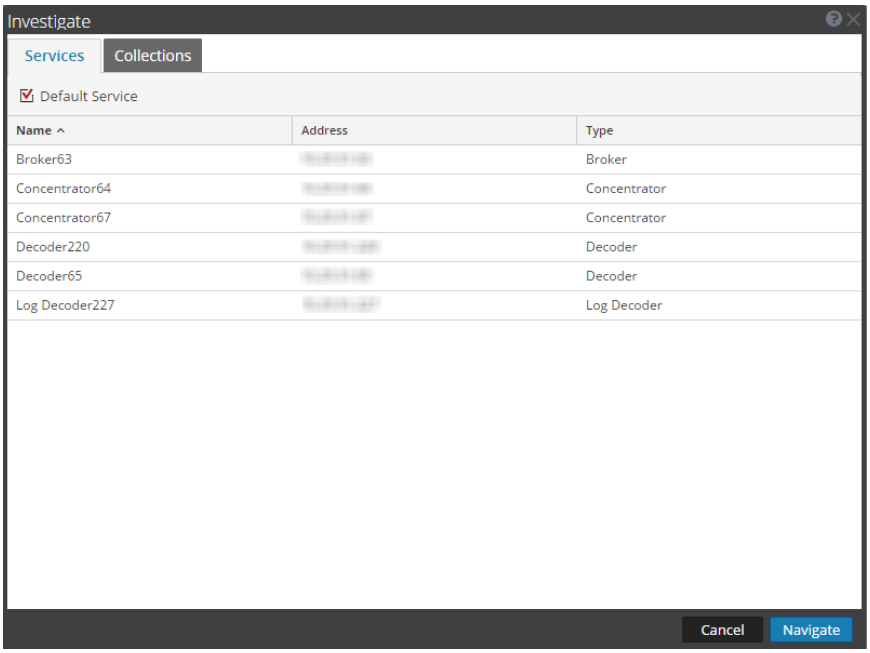
User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	select a service to investigate*	Begin an Investigation in the Navigate or Events View

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look



The Investigate dialog has two tabs: Services and Collections.

Note: Collections are also known as workbench collections. You can only view workbench collections that you have created, and only administrators can create a workbench collection.

The Services tab includes a list of services available for investigation, and three buttons. All features are described in the following table.

Feature	Description
Default Service	Clicking this button sets or clears the default service to investigate. When a service has been set as the default service, the word (Default) is appended to the service name.
Name	The name of the service.
Address	The IP address of the service.
Type	The type of service.
Cancel	Closes the dialog.
Navigate	Opens the selected service in the Navigate or Events view.

The Collections tab has two buttons and two panels: Workbench and Collections.

The Workbench panel lists available Workbench services by name. After a Workbench service is selected, you can select a collection from the Collections panel.

The Collections panel lists available collections to investigate. After a collection is selected, you can click Navigate to view the collection.

The following table describes the features of the Collections panel.

Feature	Description
Name	The name of the collection.
Type	The type of collection.
Size	The size of the collection.
Data Type	The type of data within the collection.
Date Created	The date the collection was created.

Investigation Tab - User Preferences Panel

In the Profile view > Preferences panel > Investigation tab, users can set several preferences that affect the performance and behavior of NetWitness Suite when analyzing data, viewing events, and reconstructing events in NetWitness Investigate. To access this tab, select > Profile. When the Profile view is displayed, select **Preferences > Investigation**. You can change user preferences at any time when you are working in NetWitness Suite.

What do you want to do?

User Role	I want to ...	Documentation
Threat Hunter	view and change user preferences for Investigate*	Configure the Navigate View and Events View

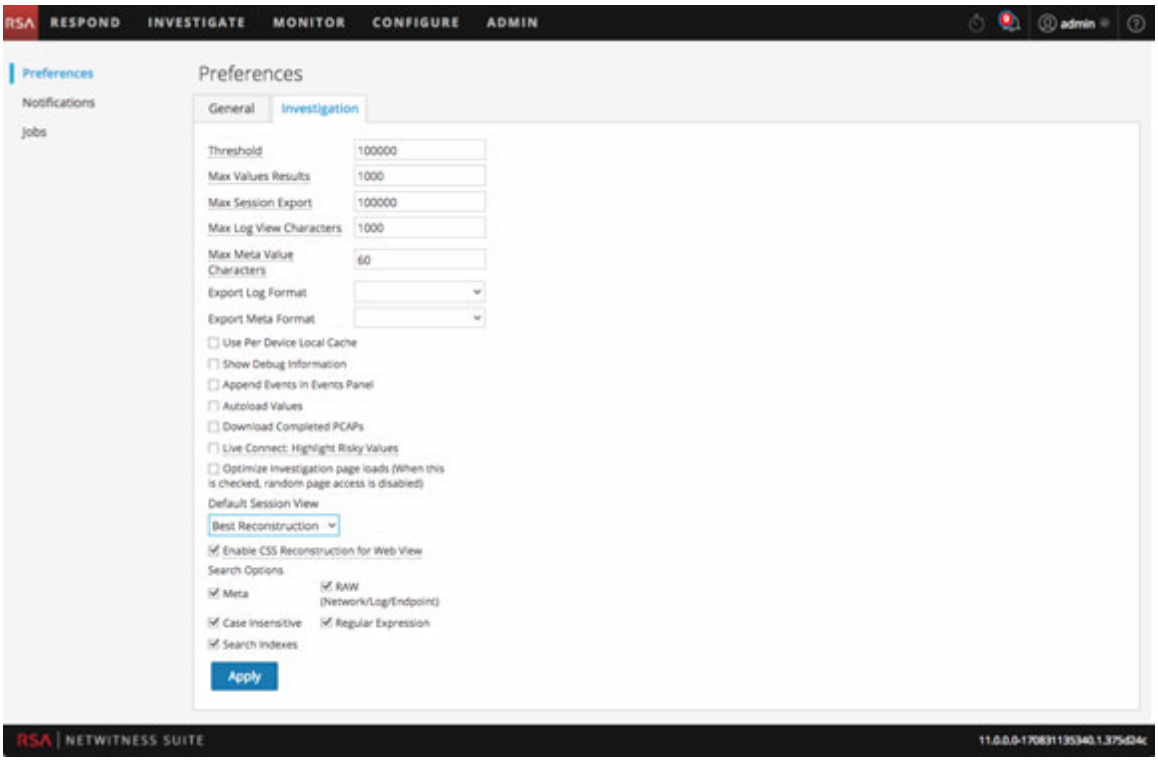
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

This figure is an example of the Investigation tab, and the following table describes the Investigation preferences.



Feature	Description
Threshold	This setting controls the count shown for a Meta Key value in the Navigate view during the load. A higher threshold allows more accurate counts for a value. However, a higher threshold causes longer load times. When the threshold is reached, NetWitness Suite displays the count and the percentage of time used to reach the count in comparison to the time necessary to load all sessions with that value. For example, **(>100000 - 18%)** indicates that the threshold was set at 100000 and this load took only 18% of the time it would have taken with no threshold set. The default value is **100000**.
Max Values Results	This setting controls the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
Max Session Export	This setting controls the maximum number of sessions that can be exported. The default value is **100000**.

Feature	Description
Max Log View Characters	This setting controls the maximum number of characters to be displayed on **Investigation > Events > Log Text**. The default value is **1000**.
Export Log Format	This setting specifies the default format for exporting logs from Investigation. Available options are **Text**, **XML**, **CSV**, and **JSON**. There is no built-in default value for the log export format. If you do not select a format here, NetWitness Suite displays a selection dialog when you invoke export of logs. When you select one of the options from the Export Log Format drop-down menu and click Apply, the setting goes into effect immediately.
Export Meta Format	This setting specifies the default format for exporting meta values from Investigation. Available options are Text, XML, CSV, and JSON. There is no built-in default value for the meta export format. If you do not select a format here, NetWitness Suite displays a selection dialog when you invoke export of meta. When you select one of the options from the Export Meta Format drop-down menu and click Apply, the setting goes into effect immediately.
Use Per Device Local Cache	
Show Debug Information	When this option is selected, NetWitness Suite displays the `where` clause beneath the breadcrumb in the Navigate view. For each meta value load, the load time is displayed. If the service is a Broker, then the elapsed time for each aggregated service is reported. The default value is **Off.**

Feature	Description
Append Events in Events Panel	When this option is selected, the events displayed in the **Events Panel** are added incrementally rather than overwriting the currently displayed events. Each time you click the next page icon, the additional events are appended to the previous events; 1 -25, then 1 -50, then 1 -75 and so on. **Note:** This option is available, only if the Optimize Investigation Page Loads option is enabled
Autoload Values	When this option is selected, the service values are automatically loaded in the Navigate view. When not selected, NetWitness Suite displays a **Load Values** button, allowing the user the opportunity to modify the options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigate so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP format.
Live Connect: Highlight Risky Values	
Optimize Investigation Page Loads	This option is enabled by default (checked) and controls how the Events view retrieves events. When optimized, results are returned as quickly as possible. This sacrifices the original ability to go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). Being able to go to any page in the list sacrifices some speed in returning the results due to additional overhead determining the events in advance.
Default Session View	This setting selects the default reconstruction type for the initial reconstruction view. By default events are reconstructed using the reconstruction type most appropriate to the event.

Feature	Description
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for stylesheets and images used in the target event. The option is enabled by default. Uncheck this option if there are problems viewing specific websites. **Note:** The appearance of the reconstructed content may not match the original web page perfectly if related images and stylesheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically via client side javascript will not render in the reconstruction because all client side javascript is removed for security purposes.
Search Options	This setting sets the default search options to apply to a search in the Navigate and Events views. Search for Text Patterns provides detailed information.
Apply	Saves your preferences and puts them into effect immediately.

Investigate View

The Investigate view (INVESTIGATE) is the primary entry point to NetWitness Investigate. The Investigate view has five submenus, which open different views that allow you to analyze events from different perspectives. The submenus are: Navigate, Events, Event Analysis, Hosts, Files, and Malware Analysis.

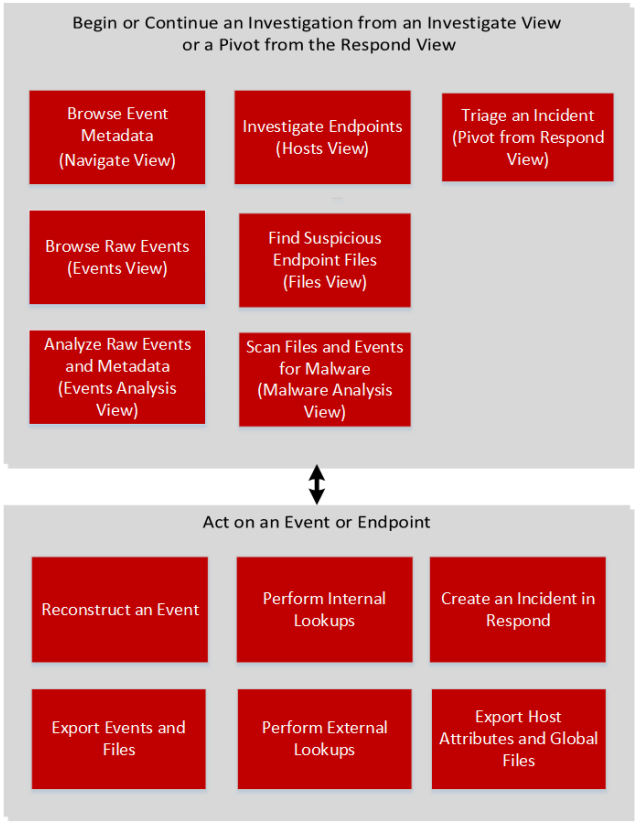
Note: The Event Analysis, Hosts, and Files submenus are available in Version 11.1 and later. Configured permissions per user role and user determine which submenus are displayed .

You can use the submenu options to move between the different views.

- The Navigate view, Events view, and Event Analysis view offer linkages to each other to look at the current results from a different perspective, which provides some continuity for the investigation as you move between views.
- The Hosts view and Files view integrate NetWitness Endpoint into Investigate, and provide a view of all hosts with a NetWitness Endpoint agent installed and a view of unique executable files found in the deployed environment.
- The Malware Analysis view provides the ability to scan files found in one of the other views or collected by continuous scanning of network traffic.

Workflow

The workflow below depicts the high-level tasks when investigating events.



What do you want to do?

Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events*	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata*	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts

Threat Hunter	find suspicious endpoint files (Version 11.1)*	Investigate Files
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis

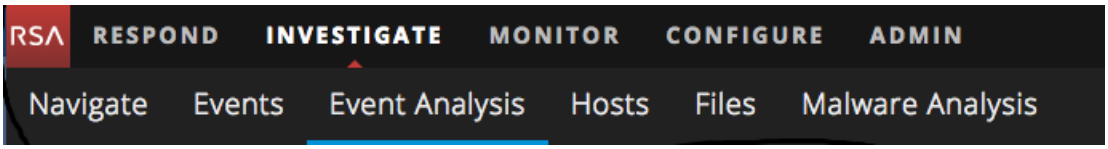
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Beginning an Investigation
- Configuring NetWitness Investigate Views and Preferences
- Navigate View
- Events View
- Event Analysis View
- Hosts View
- Files View
- Malware Analysis View

Quick Look

The Investigate view consists of five views, each representing a different approach to analyzing data. By default, Investigate opens to the Navigate view. You can change the default view to one of the other views. See How NetWitness Investigate Works for an introduction to the uses for each view. The following figure illustrates the submenus under INVESTIGATE.



Hosts View

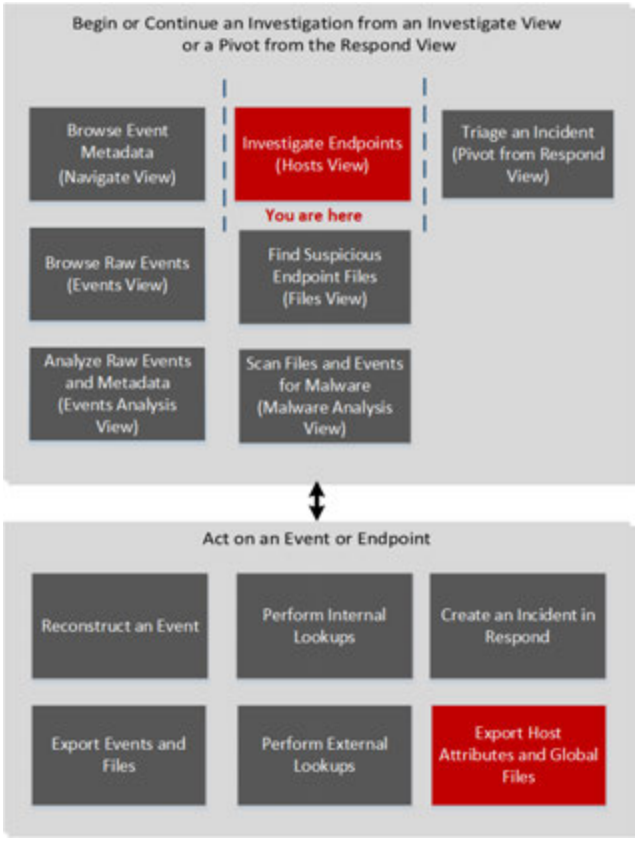
Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

In NetWitness Investigate, the Hosts view provides a list of all hosts with an Endpoint agent installed. The table displays a set of default columns for the host. You can customize this view by setting the Hosts preferences.

To access this view, go to **INVESTIGATE > Hosts**.

Workflow

The following figure shows the high-level Investigate workflow with Investigate Endpoints highlighted.



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	export host attributes and global files*	Investigate Hosts

*You can perform this task in the current view.

Related Topics

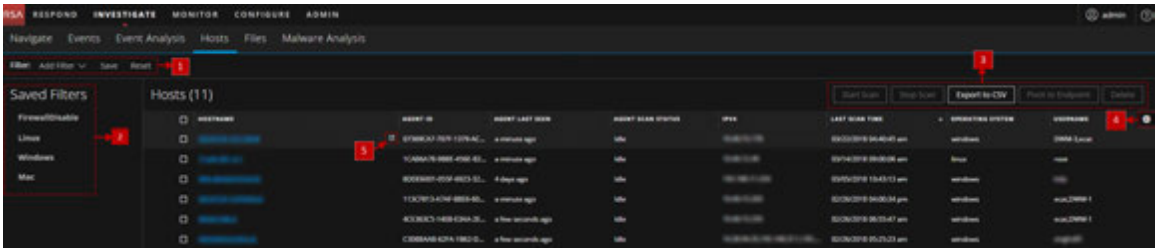
- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View - Overview Tab
- Hosts View - Process Tab

- Hosts View - Autoruns Tab
- Hosts View - Files Tab
- Hosts View - Drivers Tab
- Hosts View - Libraries Tab
- Hosts View - System Information Tab

Quick Look

In the Hosts view, you can export host attributes and global files, perform an on-demand scan, set host preferences, view a list of hosts, and investigate in the Navigate or Events view.

Below is an example of the Hosts view:



1 **Add Filter Drop-down Menu**. You can filter the hosts by choosing an operating system (Windows, Linux, or Mac), saved filters, or by selecting the options in the Add Filters drop-down menu. For more information, see Filter Hosts.

2 **Saved Filters.** The Saved Filters panel lists the saved filters. For more information, see Filter Hosts.

3 **Actions in the toolbar:**

Start Scan - Starts a scan for the selected hosts.

Stop Scan - Stops a scan for the selected hosts.

Export to CSV - Extracts host attributes to a CSV file. For more information, Export Host Attributes.

Pivot to Endpoint - Lets you investigate the NetWitness Endpoint host (version 4.4.0.2 or later). For more information, see Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts.

Delete - Lets you delete hosts manually from the user interface. After deletion, the Endpoint server does not process any request from this host.

> **Note:** Make sure that the agent is uninstalled from the host before deleting it from the user interface. For more information, see Delete a Host.

4 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

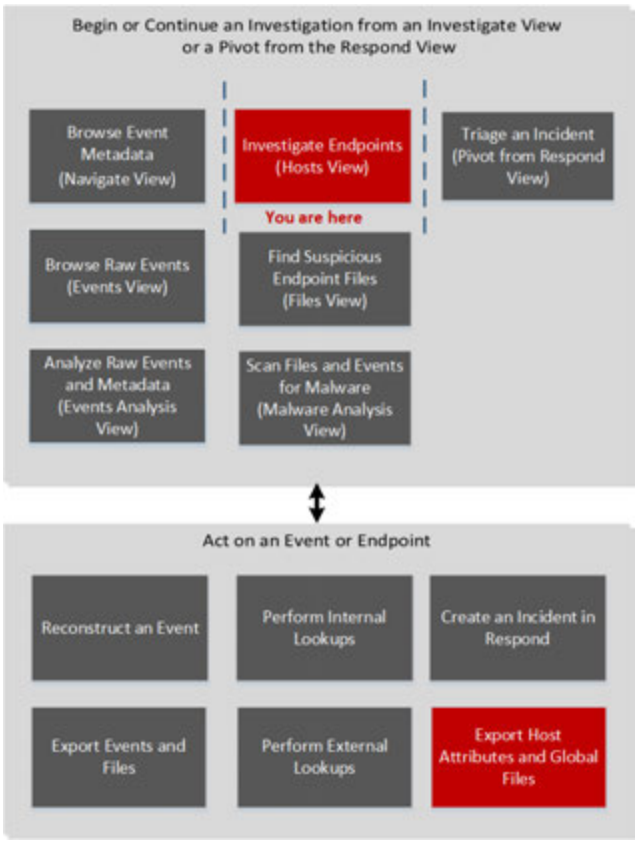
5 **Pivot to Navigate and Event Analysis views**. To investigate a particular host, IP address, or username, you can pivot to both Navigate and Event Analysis views. For more information, see Pivot to the Navigate and Event Analysis Views.

Hosts View - Autoruns Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Autoruns panel provides a list of autoruns, services, tasks, and cron jobs running on the host. To access this tab, select a host from the **Hosts** view and click the **Autoruns** tab.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the autoruns, services, tasks, and cron jobs running on the host*	Analyze Autoruns

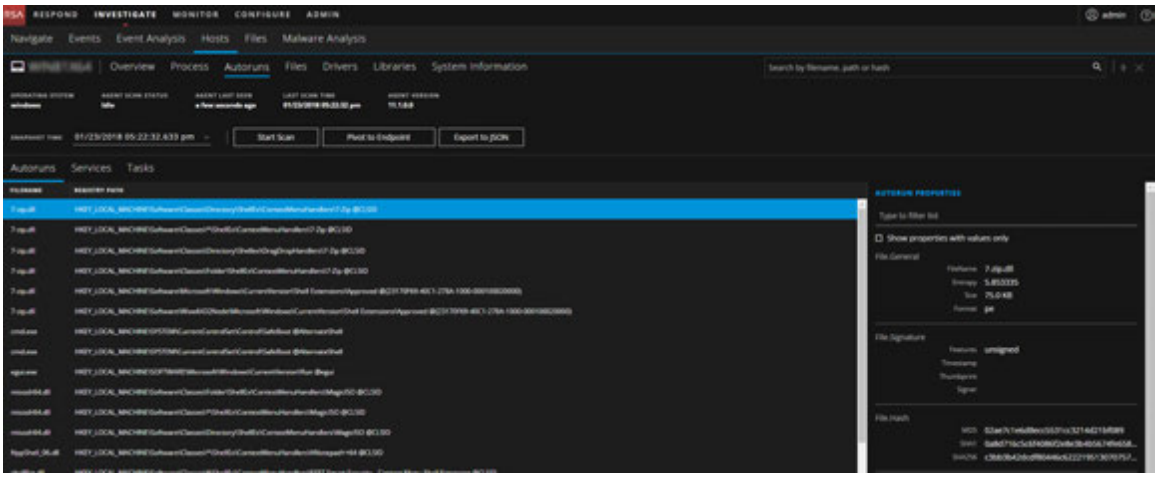
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Autoruns tab:



Category	Description
Autoruns	Files that are executed at start-up. It displays the following columns: • File name - `cmd.exe` • Registry path - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot @AlternateShell`
Services	Files that are running as a service for the selected host. It displays the following columns: • Service name - `acsock` • Running status - `stopped` • File creation time - `07/11/2017 11:47:00 am` • Signature - `Microsoft, signed, valid` • File path - `C:\Windows\System32\drivers`

Category	Description
Tasks/Cron jobs	Files that are configured to run as scheduled tasks along with the trigger. It displays the following columns: • Name - `shell32.dll` • Hash - `cafa6e7b6a9220e7c805ea476a89a78800f48bb48c66fe5f935057940df3909c` • Last run time - `01/19/2018 05:34:50 pm` • Next run time - `12/30/1899 05:30:00 am` • Trigger - `No Trigger`

Autoruns Properties Panel

This panel displays all properties of the selected file. It is grouped as follows:

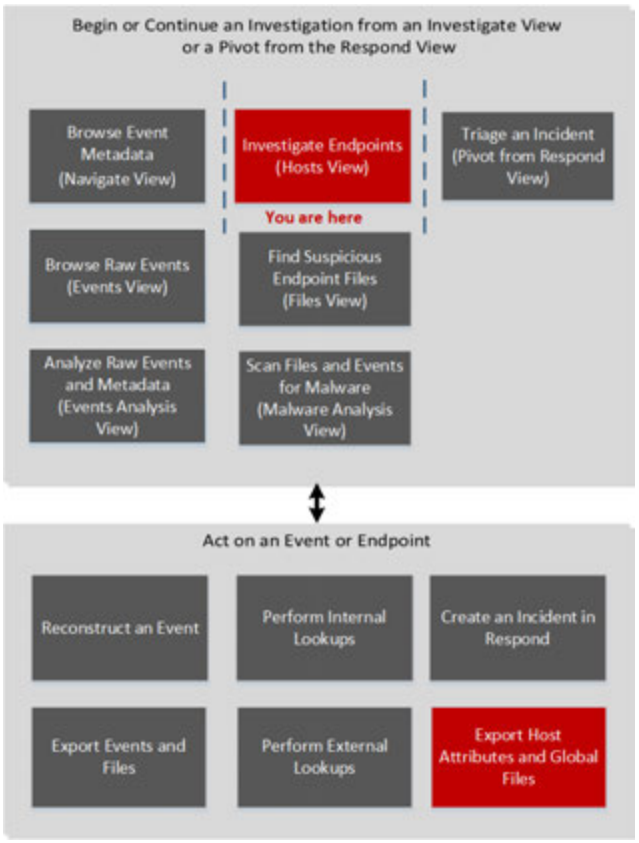
Category	Description
General	General information about the file, such as file name, entropy, size, and format.
Signature	Provides signatory information.
Hash	Hash type of the file (MD5, SHA256, and SHA1).
Time	Time when the file was created, modified, or accessed.
Location	Location of the file.
Image	Loaded image.

Hosts View - Drivers Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Drivers tab lists the drivers running on the hosts at the time of scan. To access this tab, select a host from the **Hosts** view and click the **Drivers** tab.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the drivers running on the host*	Investigate Hosts

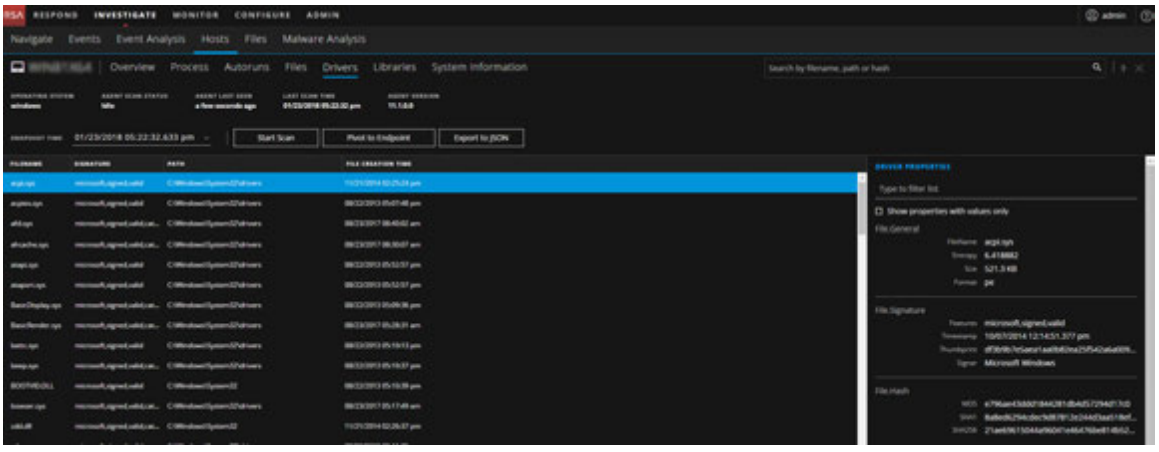
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Drivers tab:



Field	Description
Filename	Name of the file. For example, `acpi.sys`.
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information.
Path	Path of the file. For example, `C:\Windows\System32\drivers`.
File Creation Time	Time when the file was created.

Driver Properties Panel

This panel displays all properties of the selected file. It is grouped as follows:

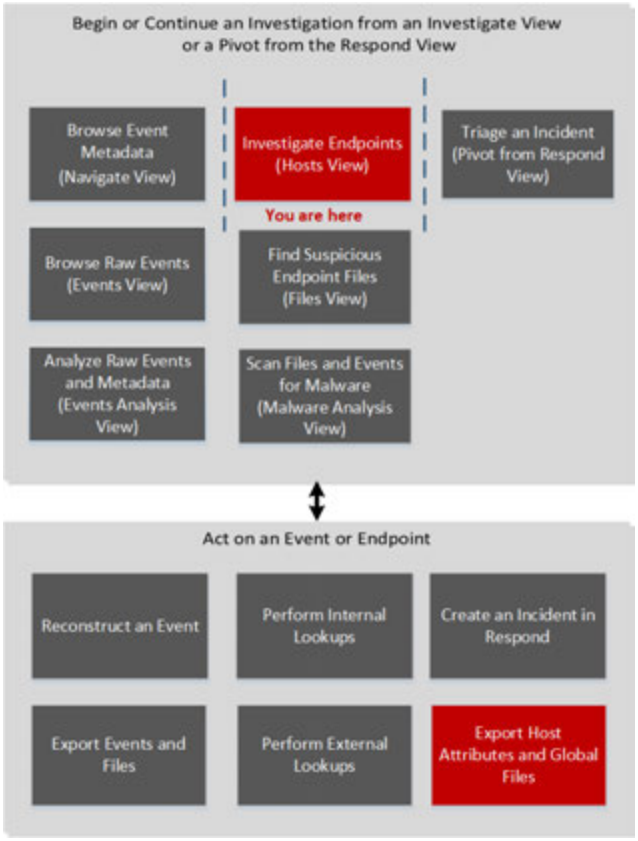
Category	Description
General	General information about the file, such as file name, entropy, size, and format.
Signature	Provides signatory information.
Hash	Hash type of the file (MD5, SHA256, and SHA1).
Time	Time when the file was created, modified, or accessed.
Location	Location of the file.
Image	Loaded image.

Hosts View - Files Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Files tab displays all files scanned on the host. To access this tab, select a host from the **Hosts** view and click the **Files** tab. By default, it displays 100 files. To display more files, click **Load More** at the bottom of the page.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the files scanned on the host*	Analyze Files

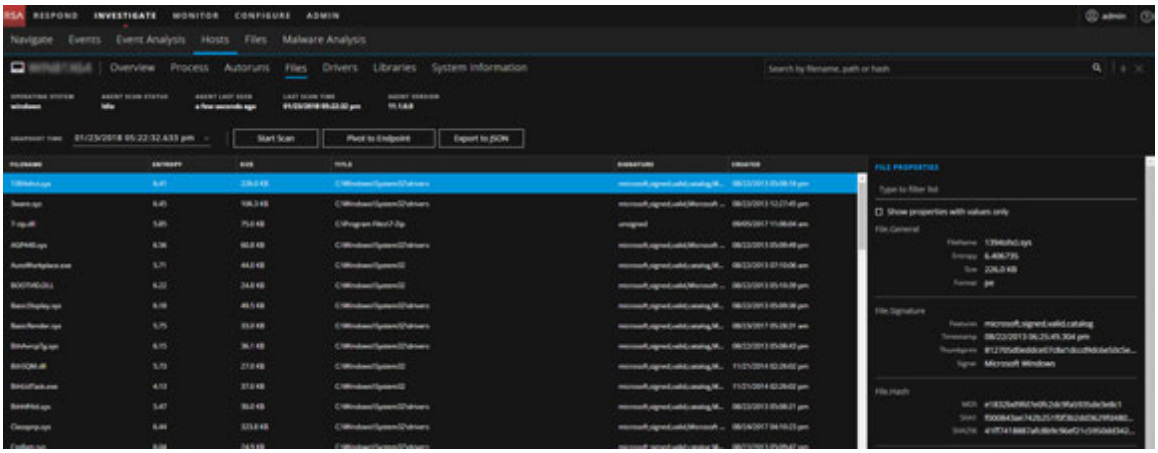
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Files tab:



Field	Description
Filename	Name of the file. For example, `7-zip.dll`.
Entropy	Entropy of the image data, excluding the PE headers. It determines if the contents are packed (compressed or encrypted).
Size	Size of the file. It can be an indicator when assessing a file.
Path	Path of the file. Sometimes malware authors put the file on directories where there are typically no such files. Malicious files are typically standalone files (for example, a file in the root `C:\ProgramData`) versus a group of files in a legitimate folder (for example, files in `C:\Program Files\<folder name>\`).
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information.
Created	Time stamp of the file.
User Name	User of the file (for Linux). For example, `root`.
Group Name	Group to which the user belongs (for Linux). For example, `root (0)`.

File Properties Panel

This panel displays all properties of the selected file. It is grouped as follows:

Category	Description
General	General information about the file, such as file name, entropy, size, and format.

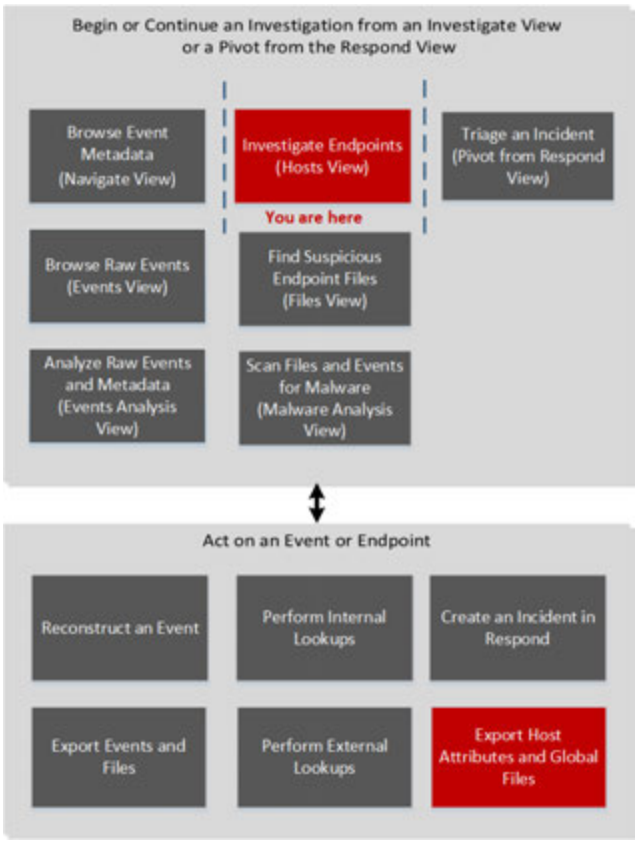
Category	Description
Signature	Provides signatory information.
Hash	Hash type of the file (MD5, SHA256, and SHA1).
Time	Time when the file was created, modified, or accessed.
Location	Location of the file.

Hosts View - Libraries Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Libraries tab lists the libraries loaded at the time of scan. To access this tab, select a host from the **Hosts** view and click the **Libraries** tab.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the libraries loaded*	Analyze Libraries

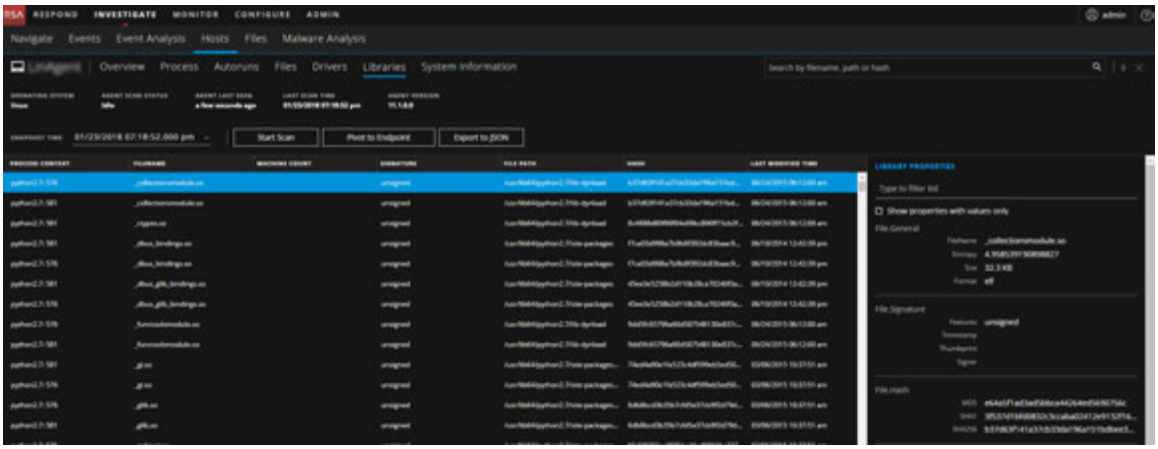
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Libraries tab:



Field	Description
Process Context	Name and PID of the process that has loaded the library in the memory. For example, `explorer.exe: 1916`.
Filename	Name of the file. For example, `7-zip.dll`.
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information. For example, `signed, valid`.
File Path	Path of the file. For example, `C:\Program Files\7-Zip`.
Hash	SHA256 of the file. For example, `c3bb3b42dcdf80446c622219513070757e618c06afd9ee0ac37cbce5befcb897`.
File Creation Time	Time when the file was created.
Last Modified Time	Time when the file was modified.

Library Properties Panel

This panel displays all properties of the selected file. It is grouped as follows:

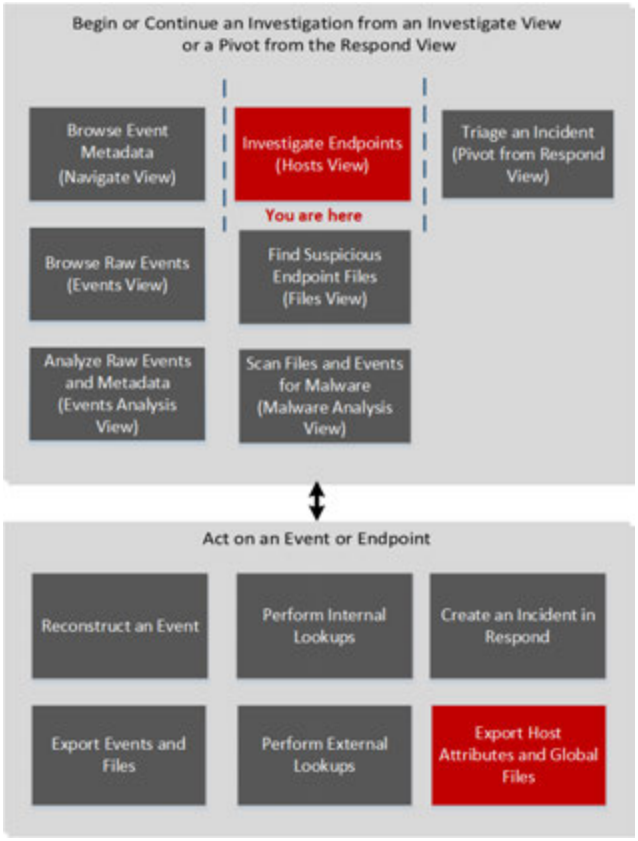
Category	Description
General	General information about the file, such as file name, entropy, size, and format.
Signature	Provides signatory information.
Hash	Hash type of the file (MD5, SHA256, and SHA1).
Time	Time when the file was created, modified, or accessed.
Location	Location of the file.
Process	Details of the process, such as image size and PID.

Hosts View - Overview Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Overview tab provides detailed scan results of the selected host. By default, the latest scan result is displayed. To access this view, go to **INVESTIGATE > Hosts**, and select a host from the **Hosts** view.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view summary of the host*	Investigate Hosts

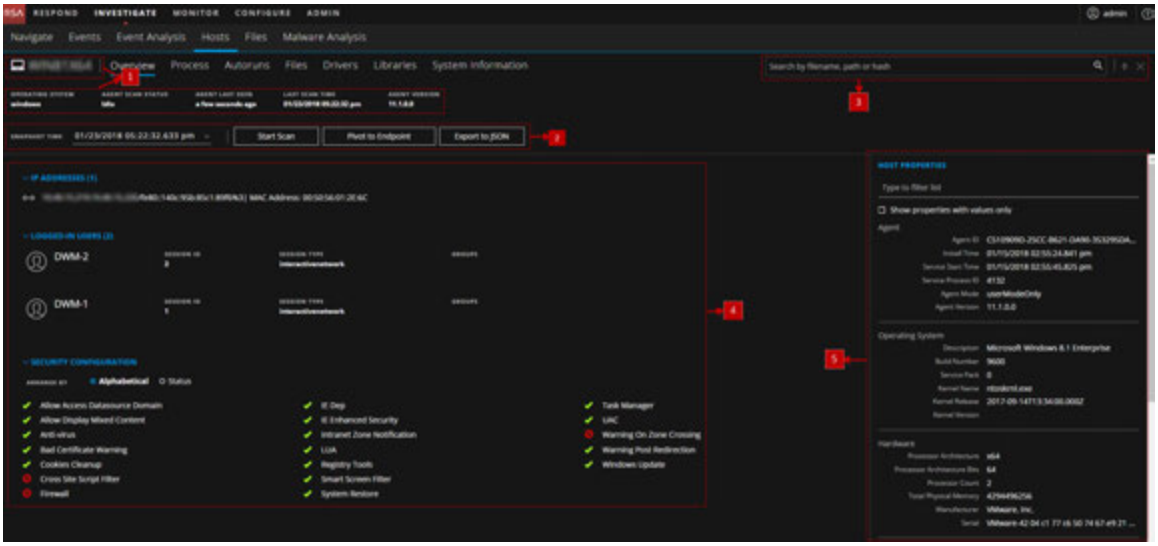
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Overview tab:



1 **Agent and Scan Details**. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, `WIN-ABC`.
Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see Investigate Hosts.

Agent Last Seen - Time when the agent last communicated with the server.

Last Scan Time - Last time the agent was scanned. The date and time is as per the time zone set in the User Preferences and is local to the server.

Agent Version - Version of the agent. For example, `11.1.0.0`.

2 **Actions in the toolbar:**

Snapshot Time - Lists scanned time stamps. To view the scan history, select the snapshot time from the drop-down menu.

Start Scan - Starts scan for the selected hosts. For more information, see Investigate Hosts.

Export to CSV - Extracts host attributes to a CSV file. For more information, see Export Host Attributes.

Pivot to Endpoint - Lets you investigate the NetWitness Endpoint host (version 4.4.0.2 or later). For more information, see Investigate NetWitness Endpoint 4.4.0.2 or Later Hosts.

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot.

3 **Search on Snapshots**. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see Search on Snapshots.

4 **Summary of the selected host**. Displays the following fields:

IP Addresses - IP addresses associated with the host. For example, `10.10.10.3`.

Logged-in users - Users logged in to the host. For example, `abc`.

Security Configuration - Security configuration details on the host. For example, firewall disabled or enabled, smart screen filter disabled or enabled. This field is only applicable for Windows and Mac.

Note: The Agent Version, IP Addresses, Logged-in users, and Security Configuration may change for each scan.

5 **Host Properties Panel**. Displays all properties of the selected host. It is grouped as follows:

Agent - Agent-related information, such as agent ID, driver error code, install time, and agent mode.

Operating System - Operating system version and build information.

Hardware - Information related to the architecture.

Network Interfaces - Network adapter information, such as Mac Address, Gateway.

User - Information related to the user.

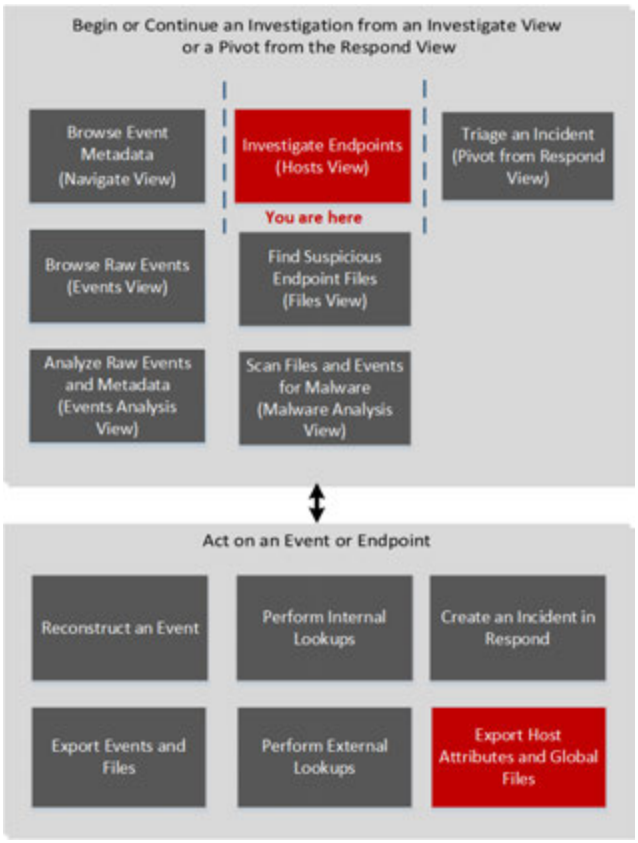
Locale - Time zone and language that is local to the host.

Hosts View - Process Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The Process panel provides a list of processes running on the host. To access this tab, select a host from the **Hosts** view and click the **Process** tab.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the processes running on the host*	Investigate Hosts

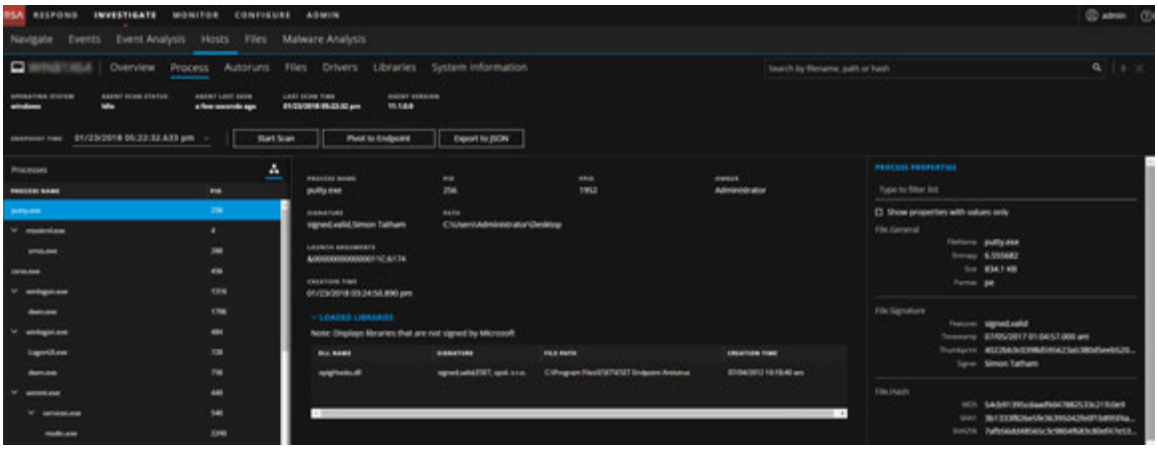
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the Process tab:



The Process panel displays the following information:

• Process Details

Field	Description
Process Name	Name of the process. For example, `server.exe`.
PID	ID of the process. For example, `492`.
Parent Process (PPID)	Name and process ID of the parent. For example, `4`.
Owner	Owner of the process. For example, `SYSTEM`.
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information.
Path	Path of the file associated with the process on the disk. For example, `C:\Windows\System32`.
Launch Arguments	Command line arguments passed to the process when it is launched. For example, `-k LocalServiceNoNetwork`.
Creation Time	Time when the process was created. For example, `01/19/2018 11:32:29.908 am`.

- List of loaded libraries for the selected process, such as DLLs (for Windows), Dylibs (for Mac), or .SO (for Linux).
- List of autoruns (if configured).

Process Properties Panel

This panel displays all properties of the selected process. It is grouped as follows:

Category	Description
General	General information about the file, such as file name, entropy, size, and format.
Signature	Provides signatory information.
Hash	Hash type of the file (MD5, SHA1, and SHA256).
Time	Time when the file was created, modified, or accessed.

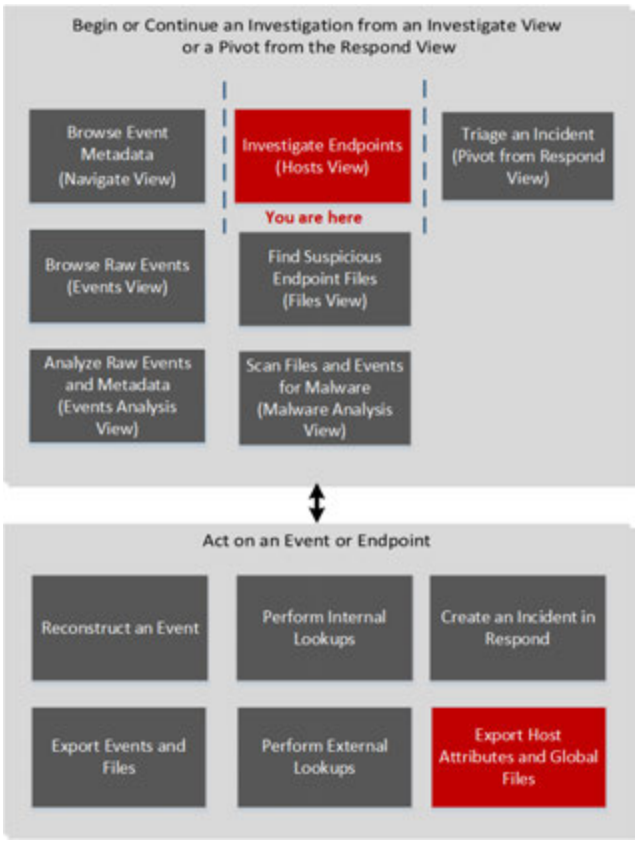
Category	Description
Location	Location of the file.
Process	Details of the process, such as image size and PID.
Image	Image details loaded by the process.

Hosts View - System Information Tab

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

The System Information tab lists the agent system information. To access this tab, select a host from the **Hosts** view and click the **System Information** tab.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View

User Role	I want to...	Documentation
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)*	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	view the agent system information*	Analyze System Information

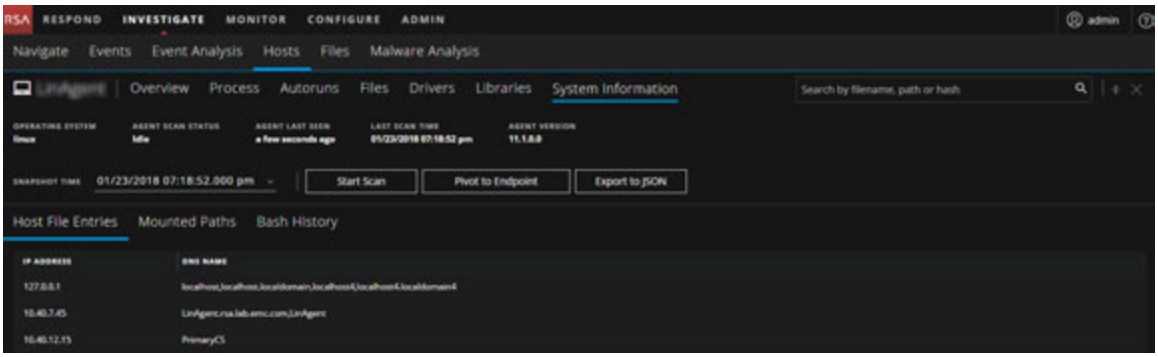
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Investigating Hosts and Files
- Hosts View

Quick Look

Below is an example of the System Information tab:



Field	Description
Host File Entries	All network redirections written in the host file. For example, IP Address - `10.10.10.3` and DNS Name - `localhost,localhost.localdomain,localhost4,localhost4.localdomain4`
Network Shares	Network name of the shared resource (for Windows only). For example, Name - `Admin$`, Description - `Remote Admin`, Path - `C:\`, Permissions - `None`, Type - `disk, special`, Max Users - `4294967295`, Current Users - `0`.
Security Products	Installed security products (for Windows only). For example, Display Name - `Windows Defender`, Instance - `D68DDC3A-831F-4FAE-9E44-DA132C1ACF46`, Features - `Enabled`, Type - `antiVirus`.
Windows Patches	List of patches applied by Windows update (for Windows only). For example, `KB2959936`.
Mounted Paths	Path mounted on. For example, Path - `/`, File System - `rootfs`, Remote Path - `rootfs`, Options - `rw`.
Bash History	User name and command run. For example, User Name - `root` and Command - `ls`.

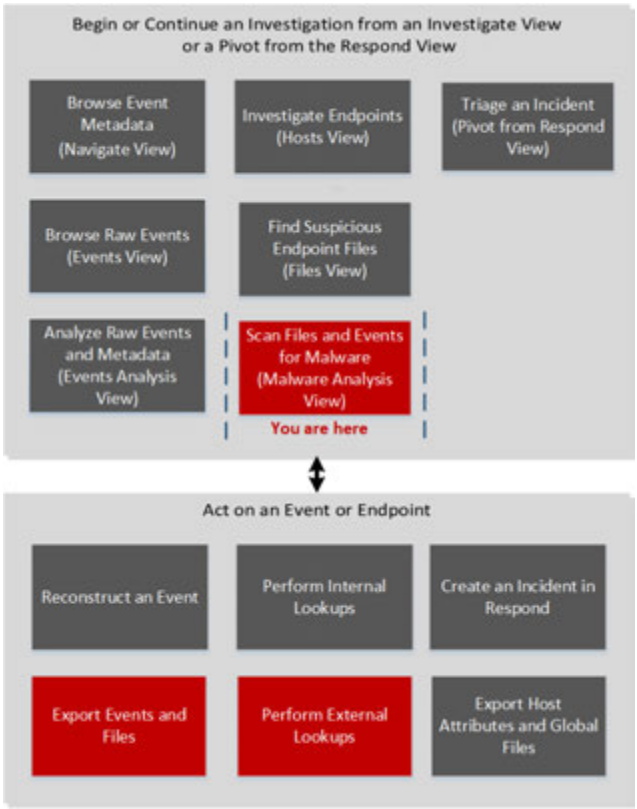
Note: For Mac hosts, the Mounted Paths and Bash History fields are empty.

Malware Analysis View

In NetWitness Investigate, the Malware Analysis view provides the user interface for conducting a malware analysis. The Malware Analysis view is in the form of a customizable dashboard, in which default dashlets in the initial view are based on the user role (Administration or Analyst) and user customizations. Initially, the Summary of Events dashlet is displayed in the Malware Analysis view. Additional dashlets present different visualizations of the events being viewed, and each representation is configurable to further refine your view as you search for Indicators of Compromise. The Malware Analysis dashlets available in the Dashboard are also available in the Malware view.

To access this view, select **INVESTIGATE > Malware Analysis.**. If a default service has not been selected, the Select a Malware Analysis Service dialog is displayed. Select a service, then click **View Continuous Mode**.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	export events and Files*	Examine Scan Files and Events in List Form
Threat Hunter	perform external lookups*	View Detailed Malware Analysis of an Event

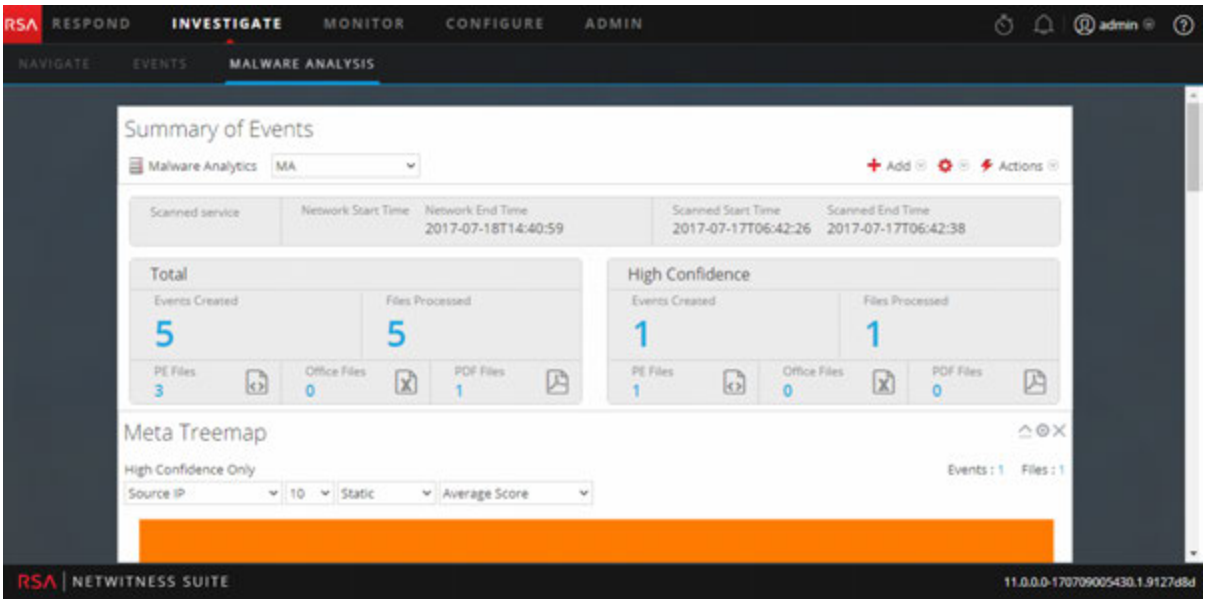
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Launch a Malware Analysis Scan from the Navigate View

Quick Look

Below is an example of the Malware Analysis view.



The Malware Analysis view consists of the Summary of Events panel and four dashlets unique to this view. Each of the unique dashlets have identical Options dialogs. The Malware Analysis dashlets in the MONITOR vieware also available, and are described in the Dashlets topic in the RSA Content for the RSA NetWitness® Suite space.

Summary of Events Panel

In the Summary of Events panel, you can select the service, the scan mode, and the time range. In addition, you can select a data point and view the events associated with the event.

The following table describes all features in the Summary of Events panel.

Feature	Description
	Selects a service to display.
Scan Mode	Displays a drop-down list of available scan modes.

Feature	Description
Time Range	Displays a drop-down list of time ranges to view events.
Start Date	When Time Range is set to custom, offers a calendar from which to choose the start date of the time range.
End Date	When Time Range is set to custom, offers a calendar from which to choose the end date of the time range.
	Displays a drop-down list of dashlets you can add to the view.
	Displays a drop-down list of actions you can perform in this view: • Restore Default Configuration • Order Dashlets • Apply Threshold Filter
	Refreshes the Malware Analysis view.

Options Dialog

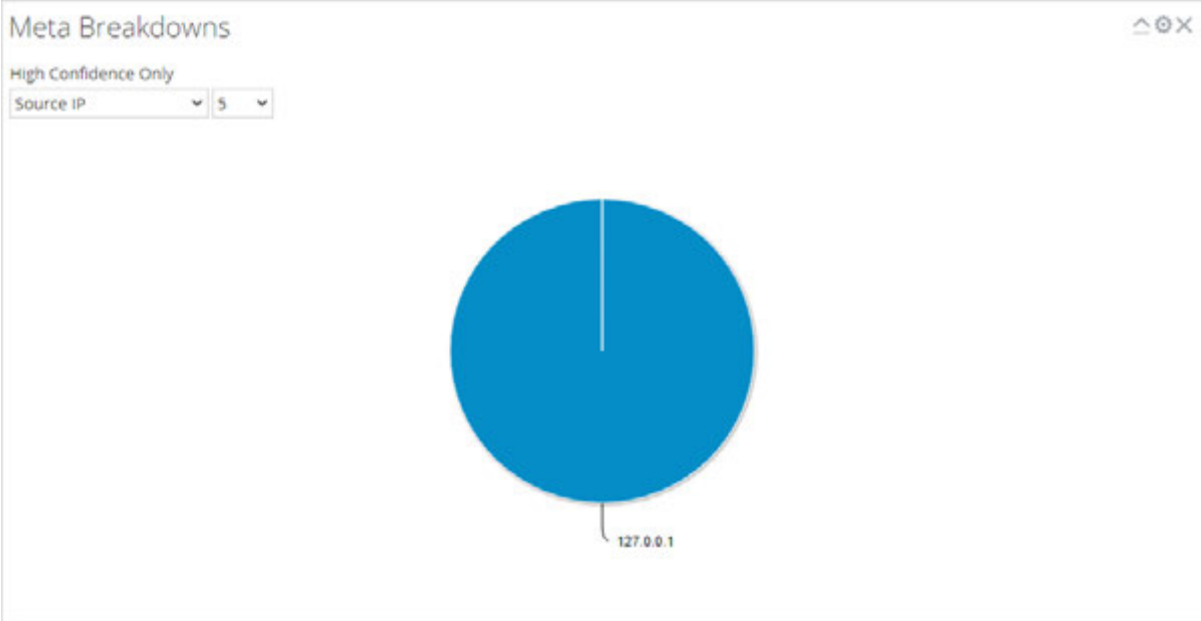
In the Options dialog, you can customize the results displayed in the dashlet. This dialog can be accessed by clicking the icon in the top right corner of each dashlet. The following table describes the features of the Options dialog.

Feature	Description
Title	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Influenced By High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence.

Feature	Description
Static, Network, Community, Sandbox	Allows you to filter results based on the scores in the scoring modules.
Cancel	Closes the dialog without saving any changes.
Apply	Applies changes to the dashlet immediately and closes the dialog.

Meta Breakdowns

Meta Breakdowns presents events in the form of a pie chart, with each slice representing a meta value for the specified meta key. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta value having the most events. Hovering over an event displays the count.



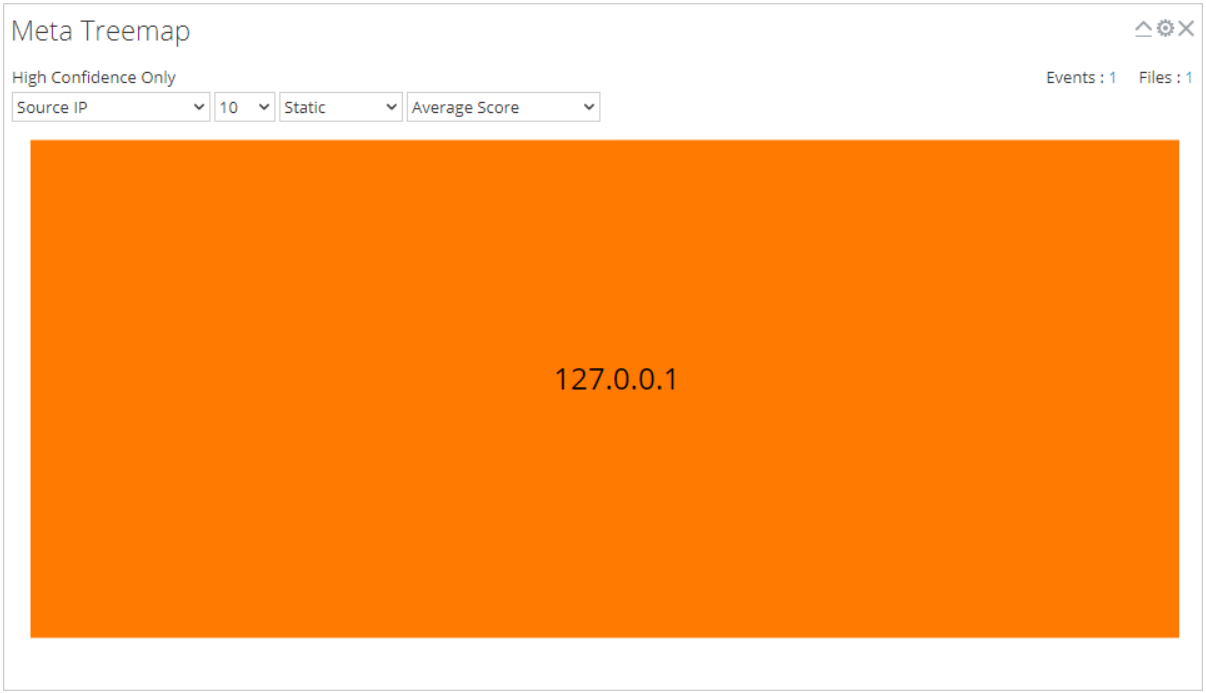
The following table describes the options in the Meta Breakdowns dashlet.

Feature	Description
High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Meta Key	Drop-down list of available meta keys.

Feature	Description
Count	Drop-down list specifying how many of the top results are displayed.

Meta Treemap

Meta Treemap presents events in the form of a heat map. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta values having the most events. In addition, you can select the module that detected the meta value in the events: static, network community, or sandbox.



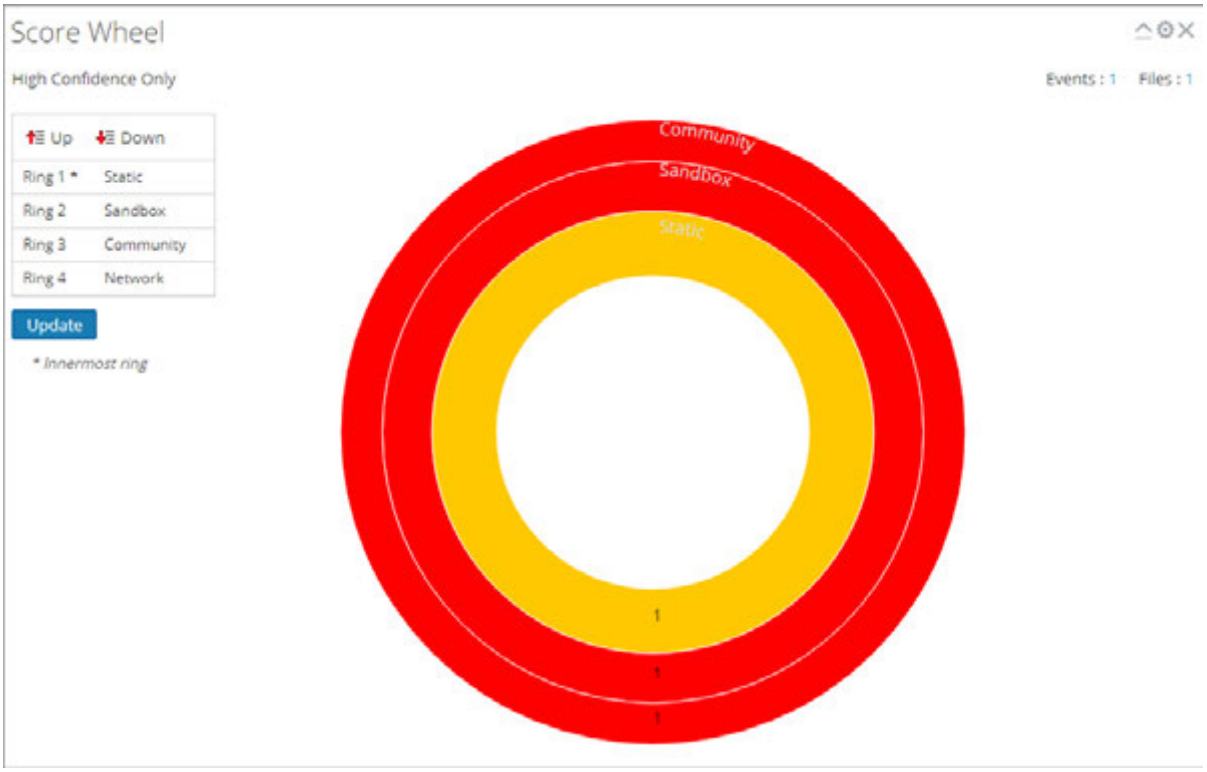
The following table describes the options in the Meta Treemap dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
Meta Key	Drop-down list of available meta keys to select as a filter.
Count	Drop-down list specifying how many of the top results are displayed.
Module	Drop-down list specifying which module results will be pulled from.

Feature	Description
Value	Drop-down list specifying what information will be displayed when the mouse is hovering over a result (for example, Average Score).

Score Wheel

The Score Wheel offers a view of events as concentric rings with colors representing scores for events based on Indicators of Compromise and the scoring module. You can arrange the position of the rings using the Up and Down arrows to obtain a view that highlights events that were detected by one scoring module (red) and not detected by other scoring modules.



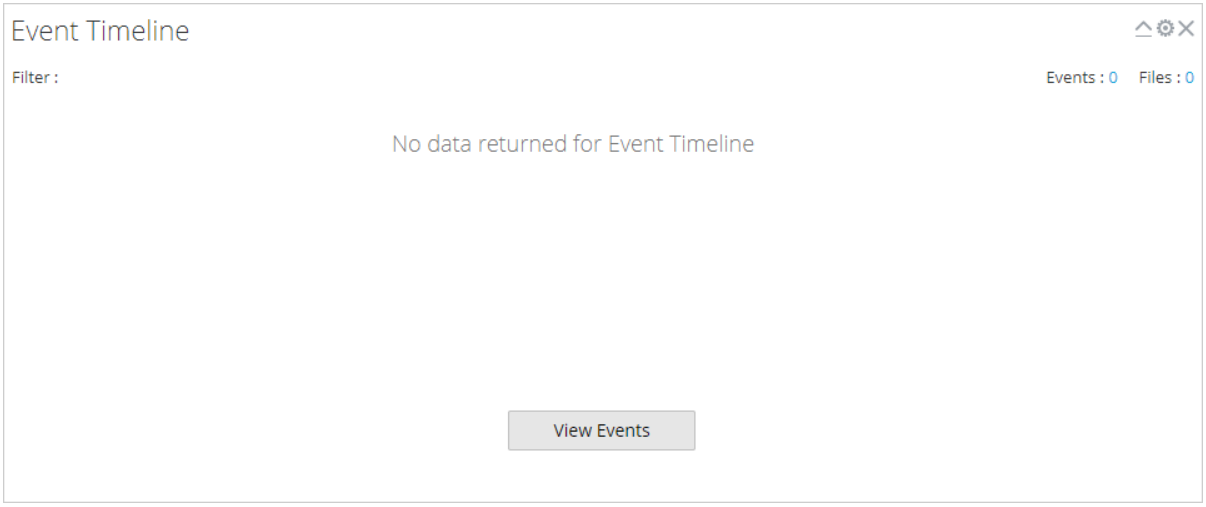
The following table describes the features of the Score Wheel dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.

Feature	Description
Module Order grid	Displays the order of the rings in Score Wheel, Ring 1 being the innermost ring and Ring 4 being the outermost ring. You can click the **Up** and **Down** buttons to reorder the modules, then click **Update** to apply the changes.

Event Timeline

The Event Timeline offers a view of events organized by the time of occurrence in a bar graph. Clicking and dragging to select a time range within the chart zooms in on the selected time.



The following table describes the features of the Event Timeline dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
View Events	Displays the Investigation > Events view.

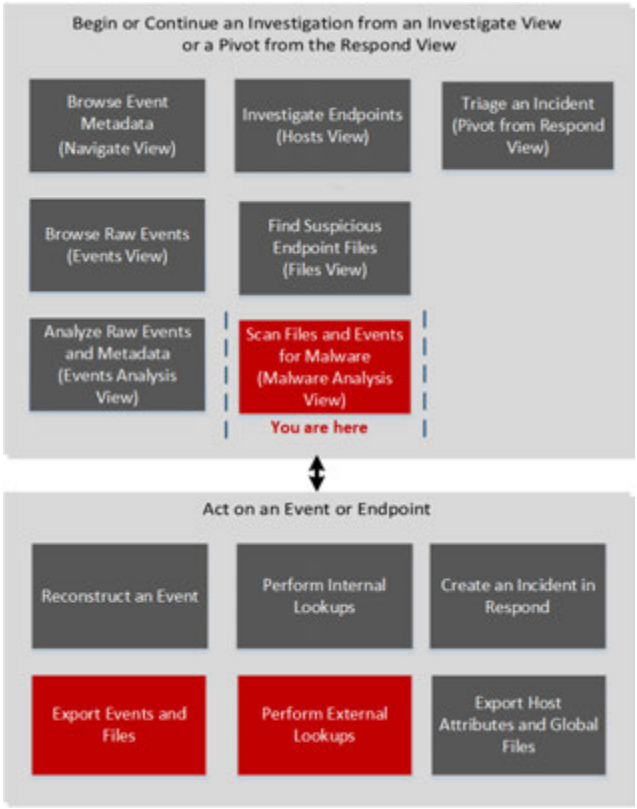
Malware Analysis Events List and Files List

The Malware Analysis Events List and Files List provide a detailed view of events or files. You can double-click on an event or file in either of the lists to display the Analysis Results view in a new browser tab.

To access this view, go to **INVESTIGATE > Malware Analysis** > **Select a Malware Analysis Service** dialog. Select a service from the left panel, then select a job from the right panel, and click **View Scan**. In the Summary of Events view do one of the following:

- In either the **Total** panel or the **High Confidence** panel, click the number in the **Events Created** section.
- If you want to view the Files List, click the number in the **Files Processed** section.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	export events and Files*	Examine Scan Files and Events in List Form
Threat Hunter	perform external lookups*	View Detailed Malware Analysis of an Event

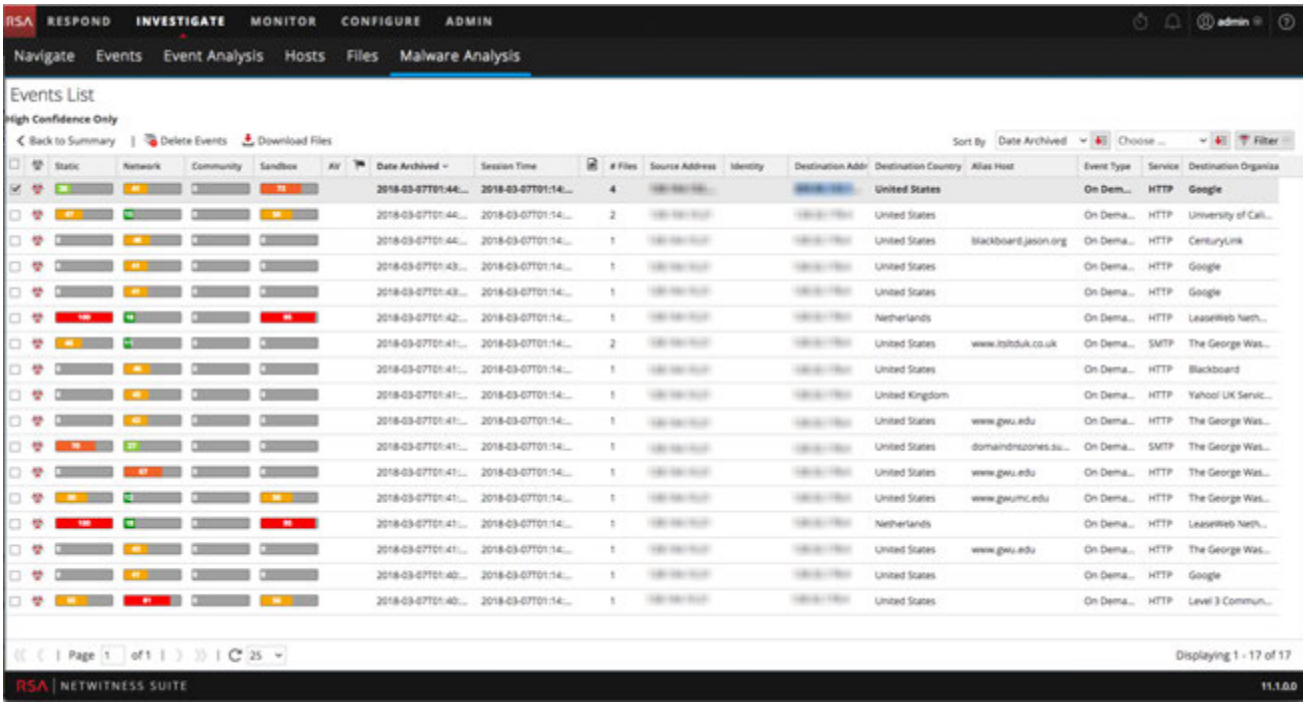
*You can perform this task in the current view.

Related Topics

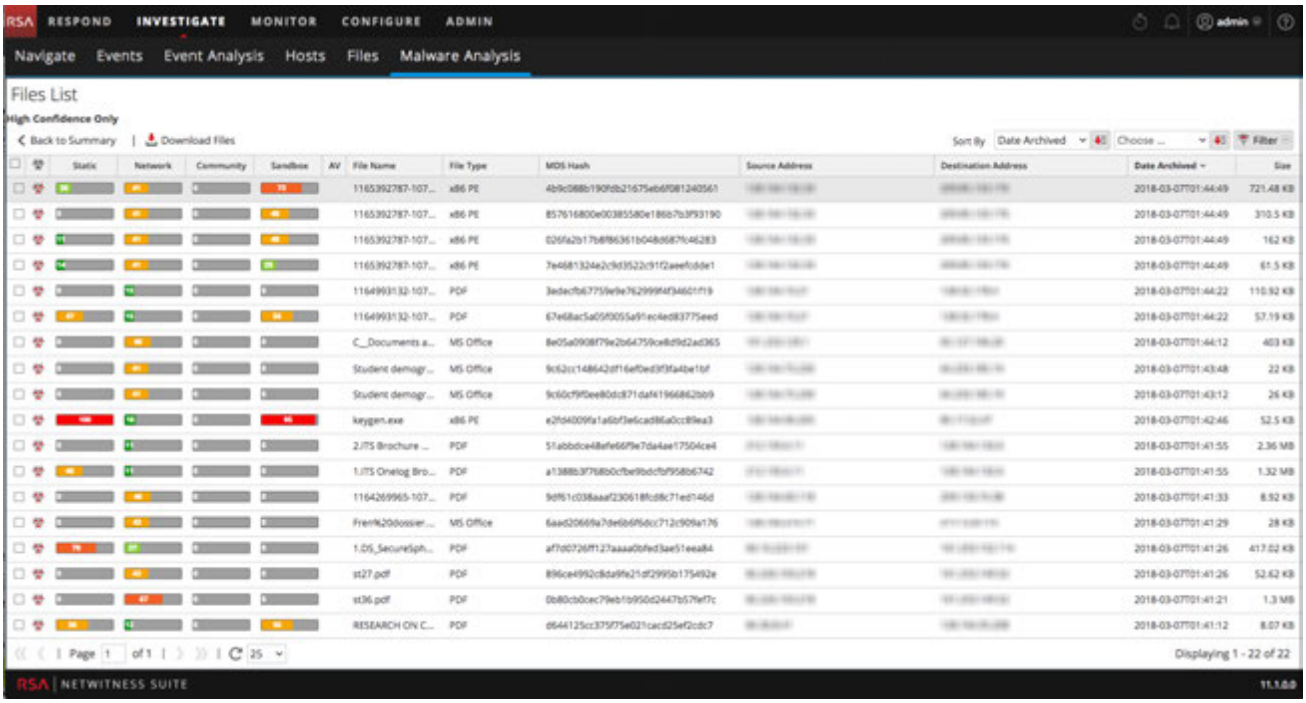
- How NetWitness Investigate Works

Quick Look

This is an example of the Events List view.

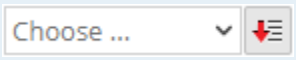
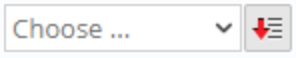
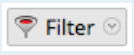


This is an example of the Files List view.



These are the features in the Events List toolbar, and the Files List toolbar is the same, except it has no option to delete events.

Feature	Description
Back to Summary	Returns to the Summary of Events view.
Delete Events	Removes the selected events from the current events list.
Download Files	Displays the Malware File Download dialog, which allows you to download available files.

Feature	Description
	Displays a drop-down menu from which you can decide how to sort the list. These are the options for sorting: • High Confidence • Static • Network • Community • Sandbox • AV • File Name • File Type • Hash • Date Archived • Size The button directly to the right of this drop-down indicates whether the list will be sorted by ascending or descending values.
	Displays a drop-down menu from which you can select a secondary sorting order. This menu includes an option forNetWitness Suite**None**, so selecting a secondary sorting order is not necessary.
	Displays a drop-down window in which you can filter the list by filename or MD5 Hash.

These are the features in the Events List.

Feature	Description
	Indicates whether the event is influenced by the high confidence flag.

Feature	Description
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.
	Indicates whether the event is influenced by a customized rule.
Date Archived	Displays the date and time the event was archived.
Session Time	Displays the time of the event's session.
	Indicates whether the hash value is marked as trusted.
# Files	Displays the number of files included in the event.
Source Address	Displays the address of the event source.
Identity	Displays the identity of the event source.
Destination Address	Displays the address of the event destination.
Destination Country	Displays the country of the event destination.
Alias Host	Displays the hostname of the alias.
Event Type	Displays the type of event. For example, Manual Upload.
Service	Displays the service on which the event occurred.
Destination Organization	Displays the organization of the destination.

These are the features in the Files List grid.

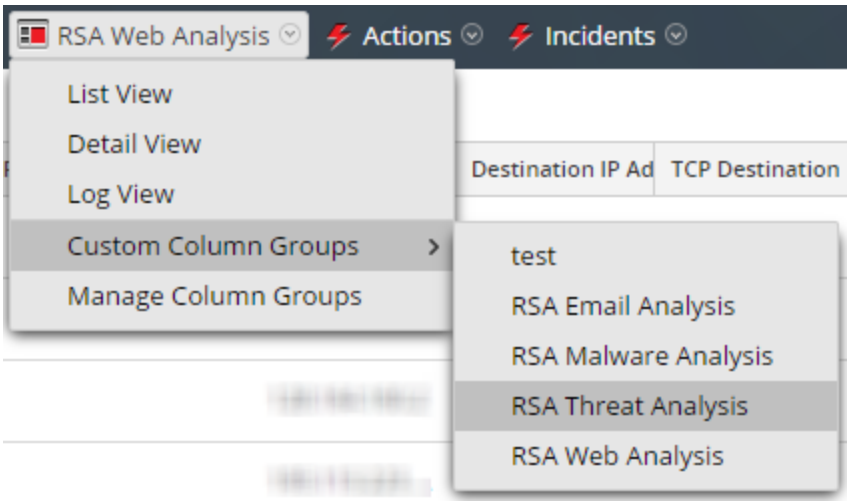
Feature	Description

Feature	Description
	Indicates whether the event is influenced by high confidence flag.
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.
File Name	Displays the name of the file.
File Type	Displays the type of the file (for example, PDF or x86 PE)
MD5 Hash	Displays the MD5 hash.
Source Address	Displays the address of the file source.
Destination Address	Displays the address of the file destination.
Date Archived	Displays the date and time the file was archived.
Size	Indicates the size of the file.

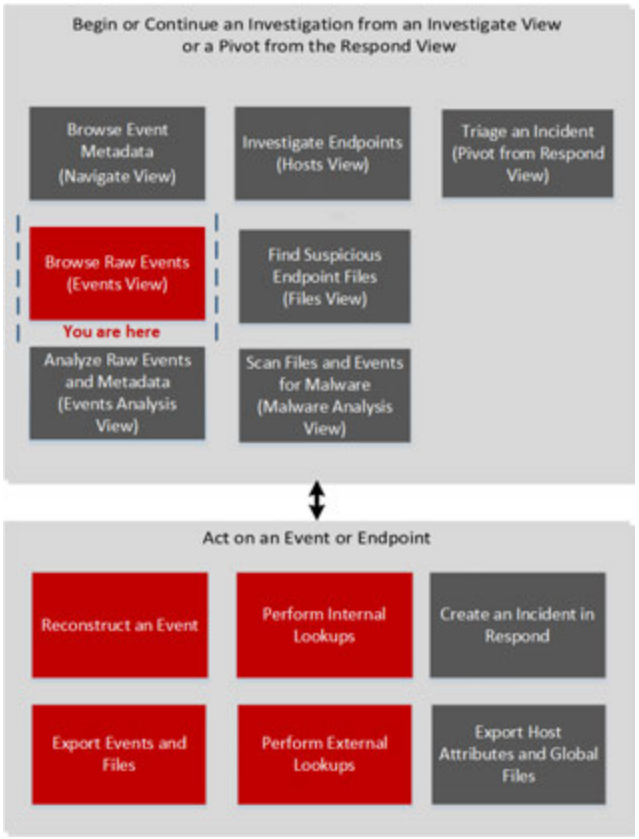
Manage Column Groups Dialog

You can customize the way data is displayed by defining the meta to display in a column, the position of the column in the grid, and the default width of the column. In the Manage Column Groups dialog, you can add, delete, import, export, and edit column groups to display specific meta keys. At fresh installation, out-of-the-box (OOTB) column groups are available for use in the Manage Column Groups dialog. The OOTB column groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. You can also create custom column groups.

To access this dialog, go to **INVESTIGATE > Events** and in the **View** drop-down list select **Manage Column Groups**. The **View** option is named for the current value, for example, Detail View, List View, Log View, or the currently selected column group.



Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View

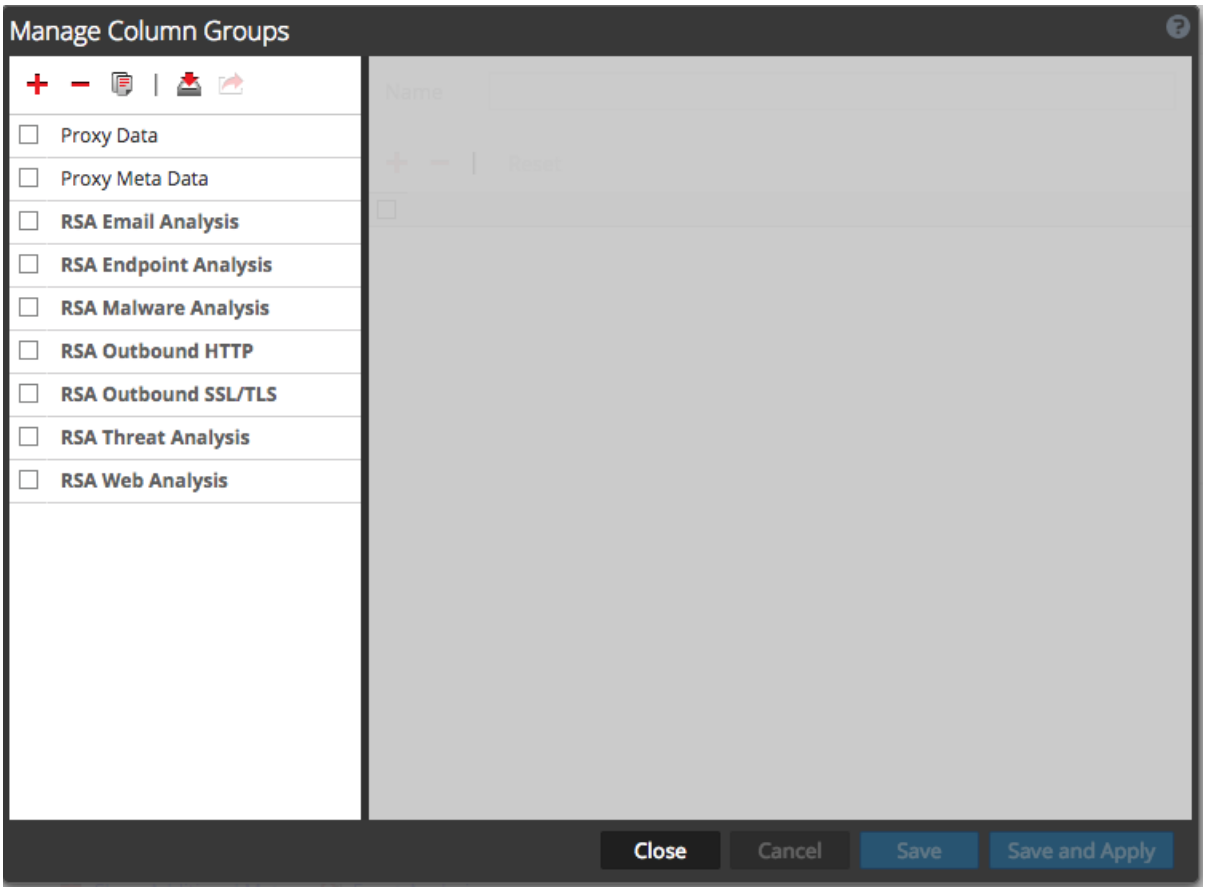
User Role	I want to ...	11.1 Documentation
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	configure column groups	Manage Column Groups in the Events View

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View

Quick Look



The Manage Column Groups dialog has two panels: Groups and Settings.

At the bottom of this dialog are four buttons: Close, Cancel, Save, and Save and Apply. The following table provides descriptions of these buttons.

Feature	Description
Close	Closes the dialog without saving.
Cancel	Cancels all unsaved changes.
Save	Saves all changes without closing the dialog.
Save and Apply	Saves and applies all changes immediately, closing the dialog.

Groups Panel

The left panel is the Groups panel. This is where you can add, delete, import, or export column groups. At the top of the panel is a toolbar which provides actions. Below the toolbar is a list of added column groups, where you can select one or more groups.

The following table lists the actions in the toolbar.

Action	Description
	Adds a column group. Clicking this button highlights the Settings panel on the right, where you can name the column group and add or delete meta keys. At least one meta key is required to add a group.
	Deletes a column group. A confirmation dialog is displayed before the selected group is deleted.
	Displays the Import Column Groups dialog, where you can select a file to upload.
	Exports one or more selected groups to your computer.

Settings Panel

The right panel is the Settings panel. This is where you can create and edit column groups. This panel contains the Name field, a toolbar, and a grid.

The following table describes the features of the Settings panel.

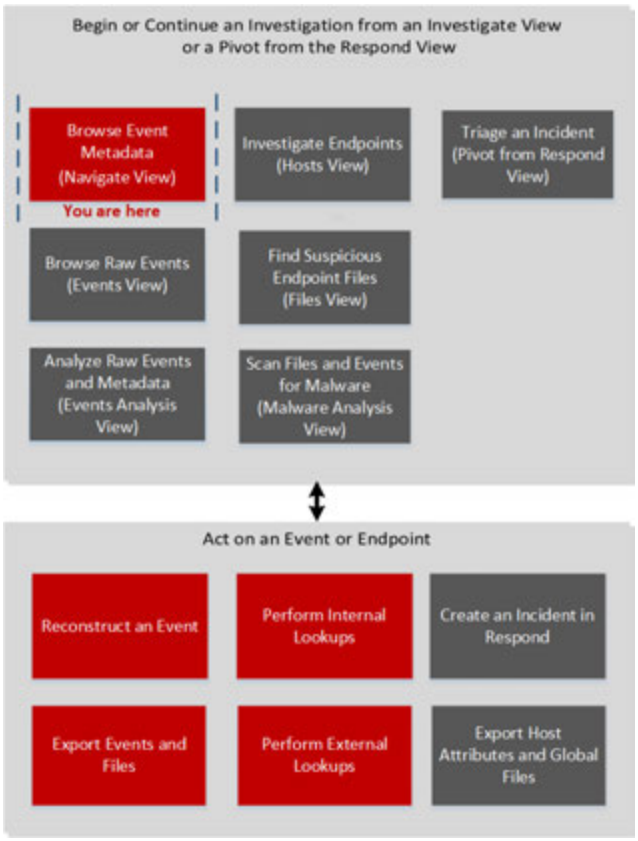
Feature	Description
Name	The name of the selected column group.
	Adds a new row to the list of meta keys, where you can open a drop-down menu to select a new meta key.
	Deletes one or more selected meta keys. Displays a confirmation dialog before deleting.
Reset	Returns column group to its most recently saved settings.
Meta Key	Lists the meta keys added to the selected column group.

Feature	Description
Display Name	Lists the names of the meta keys as they will be displayed in the Events view.
Width	Specifies the width of each meta key's column. The width can be set between **10** and **1000**. The default width is **100**.

Manage Default Meta Keys Dialog

In the Manage Default Meta Keys dialog, analysts can specify the meta keys to be displayed during navigation for a specific service. This can help you find the desired data more quickly and prevents the loading of meta data that is not of interest. To access this dialog, in the **Navigate View** toolbar, select **Meta > Manage Default Meta Keys**.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	configure default meta keys for a service*	Manage and Apply Default Meta Keys in an Investigation

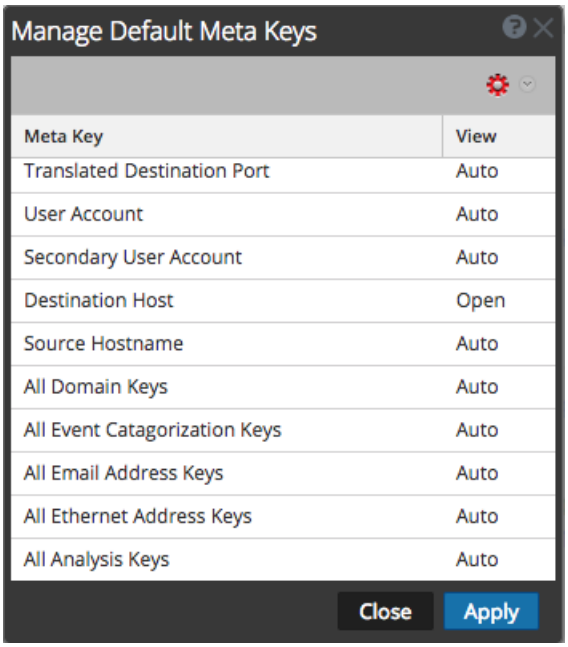
*You can perform this task in the current view.

Related Topics

- Manage Meta Groups
- Manage Meta Groups

Quick Look

The following figure illustrates the Manage Default Meta Keys dialog, which has a list of meta keys, toolbar, Close button, and Apply button. In the list, you can view, sort, and manage default meta keys. If you click and drag meta keys, you can rearrange their order. The following table describes columns in the list.



Column	Description
Meta Key	This column displays the meta keys available for the service. In Version 11.1 and later, default meta entities are also included, for example All Domain Keys and All Email Address Keys.

Column	Description
View	This column displays the type of view assigned to each meta key. By clicking on the view in each row, you can assign the meta key a different default view. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default, and can be opened manually. • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default. When you modify the default meta keys for a non-indexed meta key, you cannot set the key to **Open**. If you change the default view for a group of meta keys to **Open** and some of the meta keys are non-indexed, the non-indexed meta keys revert to **Auto**. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are **Closed** until opened manually.

The following table describes the toolbar options and buttons.

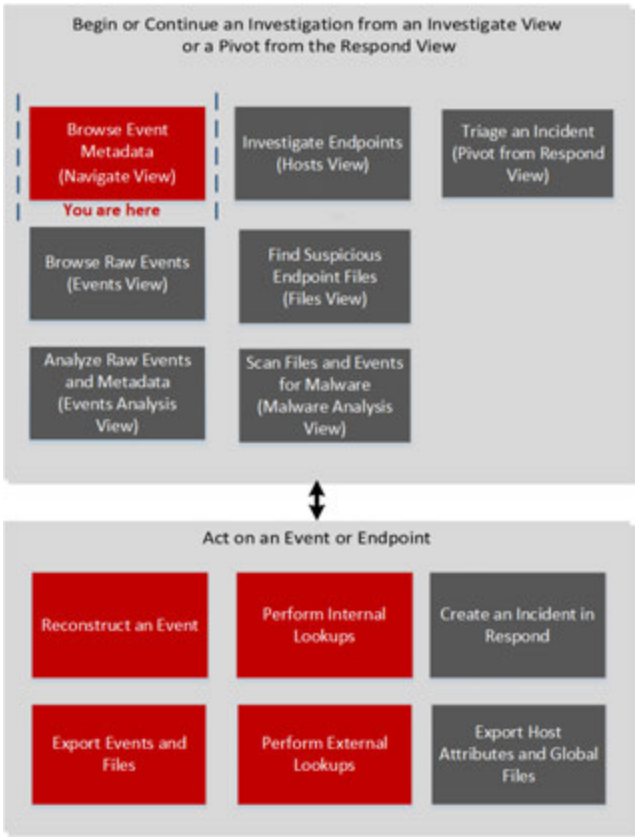
Feature	Description
	Clicking the Actions menu allows you change the default view of all the meta keys. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default. • Hidden: The values of this meta key are hidden by default. • Open: The values of this meta key are displayed by default.
Close	Closes the dialog. Any unsaved changes are lost.
Apply	Applies the changes, and they become effective immediately.

Manage Meta Groups Dialog

At fresh installation, OOTB meta groups are available in the Manage Meta Groups dialog. The OOTB meta groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. In the Manage Meta Groups dialog, you can add, delete, import, and export meta groups.

To access this dialog in the **Investigation > Navigate view** toolbar, select **Meta > Manage Meta Groups**

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	add, edit, and delete meta groups*	Manage Meta Groups

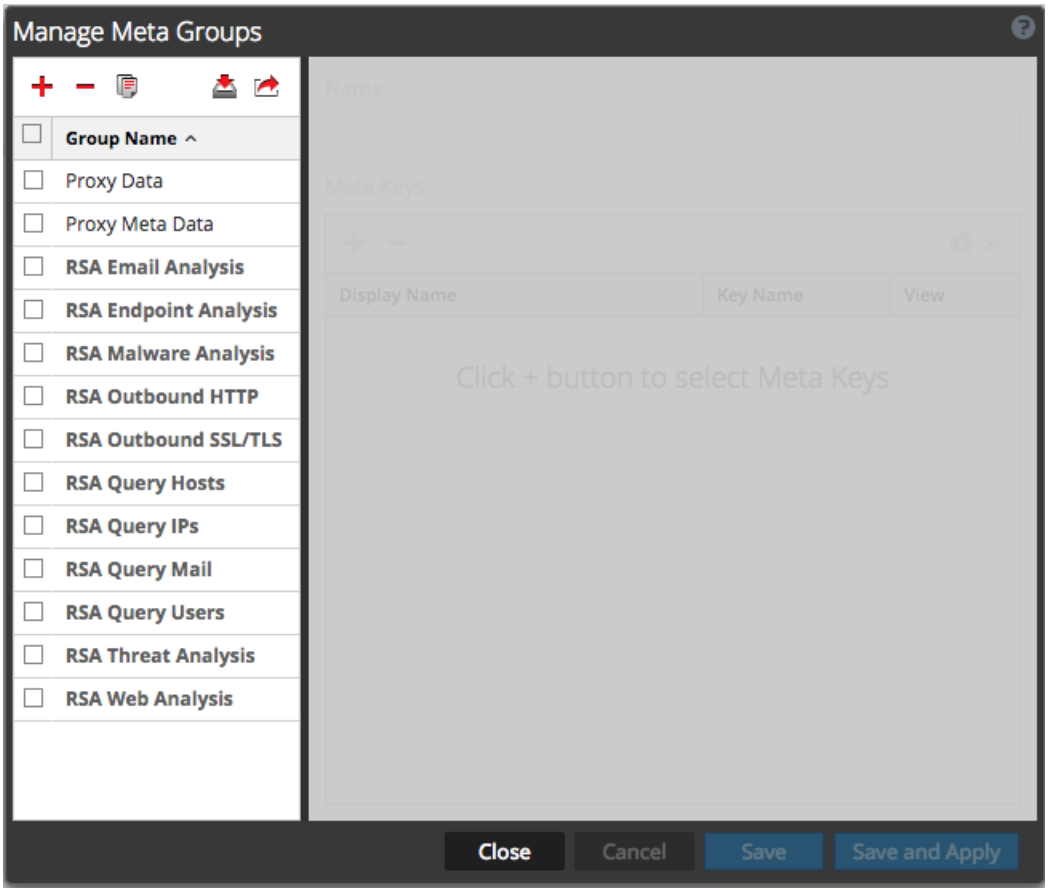
*You can perform this task in the current view.

Related Topics

- Manage and Apply Default Meta Keys in an Investigation
- How NetWitness Investigate Works

Quick Look

Below is an example of the dialog for Version 11.1, in which additional OOTB meta groups are available: RSA Endpoint Analysis, RSA Outbound HTTP, and RSA Outbound SSL/TLS. The Manage Meta Groups dialog has two panels. The following table describes the buttons at the bottom of the dialog.



Feature	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and immediately applies all changes.

The Meta Groups panel is on the left side of the Manage Meta Groups dialog. This is where you can add, delete, import, and export meta groups.

The following table describes the features of the Meta Groups panel.

Feature	Description
+	Adds a meta group using the Settings panel on the right side of the Manage Meta Groups dialog.
−	Deletes the selected meta group. A confirmation dialog is displayed before the meta group is deleted.
	Displays the Meta Group Import dialog, where you can upload a file.
	Exports the selected meta group to your computer.
Group Name	Lists all meta group names.

The Settings panel is on the right side of the Manage Meta Groups dialog. This is where you create and edit meta groups. Below the Name field is the Meta Keys grid.

The following table describes the features of the Settings panel.

Feature	Description
Name	Displays the name of the selected meta group.
+	Displays the Available Meta Keys dialog, where you can select meta keys to add to the group.
−	Deletes the selected meta keys.

Feature	Description
	Displays a drop-down menu, where you can select the view for all meta keys. There are four options based on the possible values for the `defaultAction` property used to define a key in the custom index file for the service: • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default. • Close: The values of this meta key are closed by default, and can be opened manually. • Auto: Reverts to the default view for meta keys as specified in the service index file.
Display Name	Indicates the name that is displayed for the key in Investigation views, and is defined by the `description` property for the key in the custom index file for the service..
Key Name	Indicates the `name` of the meta key as defined in the custom index file for the service.
View	Indicates which view the meta key is set to. You can change this by either: • Clicking **v** in the View column header, then selecting a view in order to change all meta key views. • Clicking a single meta key in the View column, then opening the drop-down menu in which all available views are displayed, in order to change an individual meta key view.

Manage Profiles Dialog

Profiles allow you to set up custom views in the Navigate view and the Events View. At fresh installation, OOTB profiles are available in the Manage Profiles dialog. The OOTB profile groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. In the Manage Profiles dialog, you can configure, add, delete, import, and export profiles.

To access this dialog in the **Investigation > Navigate** or **Events** view toolbar, select **Profile > Manage Profiles**.

What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

User Role	I want to ...	11.1 Documentation
Threat Hunter	configure profiles for the Navigate view or Events view*	Use Profiles to Encapsulate Custom Views

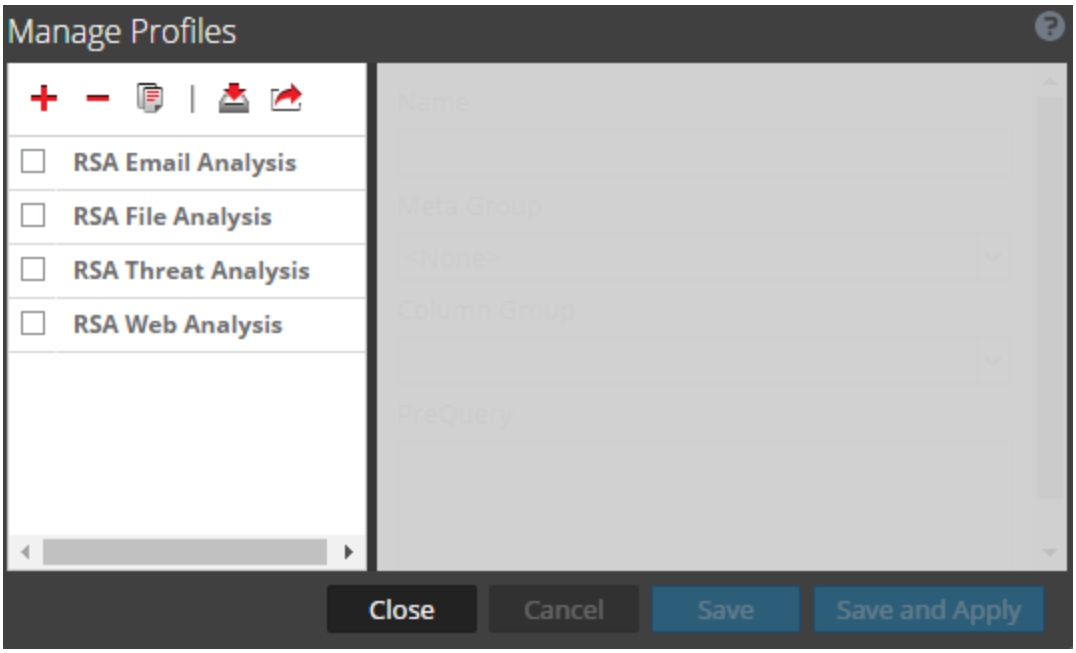
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

This is an example of the Manage Profiles dialog.



The Manage Profiles dialog has two panels. At the bottom of the dialog there is a row of buttons. The following table describes the buttons.

Field	Description
Close	Closes the dialog.

Field	Description
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and applies all changes immediately.

The Profile panel on the left side of the dialog displays available profiles and allows you to add, delete, import, and export profiles. The following table describes the fields in the Profile panel.

Field	Description
	Adds a new profile using the Settings panel on the right side of the Manage Profiles dialog.
	Deletes the selected profile. A confirmation dialog is displayed before the profile is deleted.
	Displays the Profile Import dialog, where you can upload a file.
	Exports the selected profile to your computer.
Profile Name	Lists all profile names.

The Settings panel on the right side of the dialog offers options to configure profiles. It can only be used when one profile is selected. The following table describes the fields in the Settings panel.

Feature	Description
Name	Displays the name of the profile.
Meta Group	Displays a drop-down menu listing available meta groups.

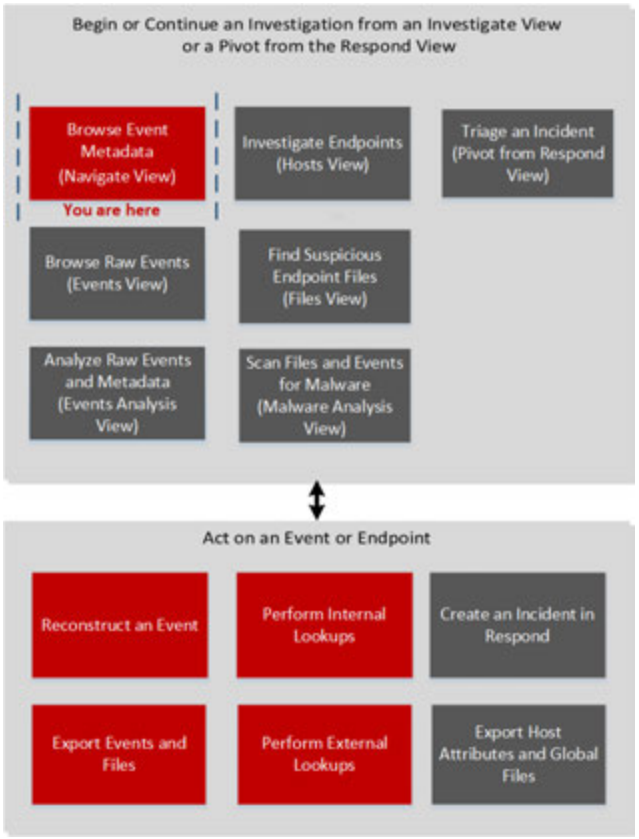
Feature	Description
Column Group	Displays a drop-down menu listing available column groups. Three groups are available by default: • List View • Detail View • Log View
PreQuery	Defines a limiting query for filtering Investigation results. This query is used when the associated profile is activated and the preQuery applies to any queries used in the Investigation Navigate and Events views. This is an example of a preQuery: `'service=80,25,110'`.

Navigate View

The Navigate view (**INVESTIGATE** > Navigate) displays event metadata--the meta keys and meta values-- that were found in captured data for the selected service. The data is filtered and displayed in accordance with the options you set for profile, time range, meta group, and query. You can also drill into the data by clicking meta keys and meta values. The Navigate view is the default entry point to NetWitness Investigate; you can change the default entry point to one of the other views in the User Profile preferences.

Workflow

The figure below depicts the high-level workflow for investigating event metadata.



These are the tasks that you can perform in the Navigate view:

- Select a service to investigate and load data.
- View query results and filter by time range, profile, meta group.
- Sort the results and select a quantification method.
- Save events, go to an event using the event ID, visualize an event, and print the event.

- View additional contextual data for specific meta keys and values.
- Go to the Events view or the Event Analysis view, where you can see a chronological list of events, reconstruct an event, and conduct an interactive analysis of an event. When viewing and analyzing events, you can export events, files, and logs to your local file system.

What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata*	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events*	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	set user preferences for the Navigate view*	Configure the Navigate View and Events View

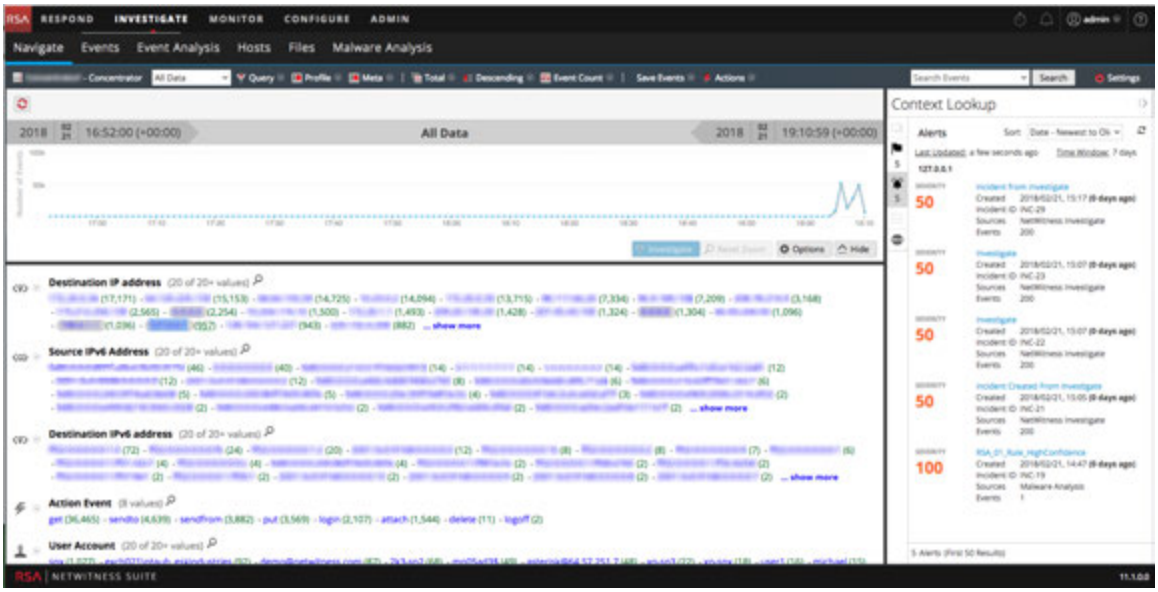
User Role	I want to ...	11.1 Documentation
Threat Hunter	submit a query or drill into the data set*	Investigating Metadata in the Navigate View
Threat Hunter	refine query results*	Querying and Acting on Data in the Navigate and Events Views
Threat Hunter	perform internal lookups*	View Additional Context for a Data Point
Threat Hunter	perform external lookups*	Launch an External Lookup of a Meta Key

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View
- Event Analysis View
- Malware Analysis View

Quick Look



The Navigate view consists of these features:

- Toolbar
- Pause/reload button and breadcrumb
- Time banner
- Optional debug information.
- Collapsible Visualization panel
- Values panel
- Context Lookup panel
- Context menus

Toolbar

The toolbar provides a way to:

- Change the service being investigated.
- Control the range of data displayed: You can select use profiles, set a time range, use meta groups, and create queries to apply to the data.
- Set the quantification method and sorting method for data in the Values panel.

- Perform actions on the results. You can export and print results, open an event for which you have an event ID in the Events view or Event Analysis view, and pass a query to Informer.
- Configure Investigate settings without navigating away from the Investigate views.

Some of the toolbar options are labeled with the default value or the selected value rather than displaying the name of the option. For example, the time range option in the example above is labeled **Last 5 Minutes** to reflect the currently selected value. These are the toolbar options.

Option	Description
	Displays the selected service name next to the icon. Clicking the icon opens the Investigate a Service dialog, in which you can select a service to investigate and set the default service to investigate (see Begin an Investigation in the Navigate or Events View). Changing the service does not cause a reload of the data.

Option	Description
Time Range	Displays the Time Range options; the currently selected option is displayed in the toolbar (see Filter Results in the Navigate View). Possible choices are: • All Data • Last 5, 10, 15, or 30 Minutes • Last Hour, Last 3, 6, 12, or 24 Hours • Last 2 or 5 Days • Early Morning • Morning • Afternoon • Evening • All Day • Yesterday • This Week • Last Week • Custom **Note:** If you specify custom start or end times in seconds, the value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time will be interpreted as `HH:MM:00 - HH:MM:59`. Seconds display in this format in Investigate functions.
Query	Displays the Query dialog, in which you can enter a custom query directly instead of drilling down the data. See Query Dialog for a description of the dialog.

Option	Description
Profile	Displays the Profile menu; the currently selected profile is displayed in the toolbar. A profile allows you to manage and use profiles that can include custom meta groups, a default column group, and a beginning query. The Profiles apply to the Navigate view (meta groups and queries) and the Events view (column groups and queries). See Use Profiles to Encapsulate Custom Views for more information.
Meta	Displays the Meta Group menu. You can use Default Meta Keys or a custom Meta Group. You also have the option to make changes to both group types (see Manage Meta Groups).
Sort Field	Displays the Sort Field menu; the currently selected option is displayed in the toolbar. The menu has two options: Order by Total and Order by Value. The Sort Field is a complement to the Sort Order option; the data for each meta key is ordered based on the total (green number) or the meta value (blue text) (see Filter Results in the Navigate View).
Sort Order	Displays the Sort Order menu; the currently selected option is displayed in the toolbar. The menu has two options: Sort in Ascending Order and Sort in Descending. The Sort Order is a complement to the Sort Field option; the selected field for each meta key is ordered in ascending or descending order (see Filter Results in the Navigate View).

Option	Description
Quantification Method	Displays the Quantification Method menu; the currently selected option is displayed in the toolbar. The Quantification Method only applies to the meta key results in the Values panel. It does not apply to the timeline. The drop-down menu contains three options for calculating the quantity (green number in parentheses) for a meta value: Quantify by Event Count, Quantify by Event Size, and Quantify by Packet Count (see Filter Results in the Navigate View). These are applied differently depending on the type of data in view. For packet data: • Quantify by Event Count shows the number of sessions. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of packets. For log data: • Quantify by Event Count shows the number of logs. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of logs.
Save Events	Displays the Save Events menu, in which you can use options to: extract files associated with an event, export the current drill point as a PCAP file, and export the current drill point as a log file (see Export a Drill Point).
Actions	The Actions menu includes actions that you can perform in the Navigate view (see Investigating Metadata in the Navigate View). In Version 11.0.0.x, the options are: Visualize, Go To Event, and Print. In Version 11.1 and later, the options are Visualize, Go to event in Event Reconstruction, Go to event in Event Analysis, and Print).

Option	Description
Search Events	Enables you to search for text patterns within the current set of events. If you click in the Search field, it shows a drop-down menu with search options. If you click Apply, it saves the selected options and also updates the search options in the Events view and the Investigations profile (see Search for Text Patterns).
Settings	Displays the settings for the Navigate view (which are also editable in the Profile view) so that you can change Investigate settings without navigating away from the Navigate view. When you change a setting In the Navigate view the setting is also changed in the Profile view (see Configure the Navigate View and Events View).

Pause/Reload Button and Breadcrumb

The breadcrumb tracks each query as you drill down through the metadata for the service. Each query is listed with a drop-down menu in a pipe separated string. The last point is the current point, also called the tip. The icon in front of the breadcrumb allows you to pause the loading of meta values and to reload meta values.

The breadcrumb does not include the service name and appears only if a query is in effect. If too many drill points exist for display, the overflow is shown as double angle brackets, >>, at the end of the breadcrumb.

Each drop-down menu in the breadcrumb is the same, with slight variation based on the position of the crumb.

The following table describes the controls and menu options in the breadcrumb.

Feature	Description
	Pause and Reload button. Controls the loading of data in the view. It has three possible functions: pause loading, continue loading, and reload.
Navigate Here	Opens the selected drill point in the current Values panel.
Navigate Here (new tab)	Opens the selected drill point in a new tab.

Feature	Description
Insert Before	Inserts a query before the current drill point. The Create Filter dialog opens and you can define a custom query to insert in the breadcrumb (see Create a Custom Query).
Append	Appends a query after the current drill point. The Create Filter dialog opens and you can define a custom query to append to the end of the breadcrumb (see Create a Custom Query).
Remove	Removes the selected drill point from the breadcrumb.
Edit	Opens the selected drill point in the Create Filter dialog so that you can edit the query.
>>	Clicking the angle brackets displays a drop-down menu of the breadcrumb overflow.

(Optional) Debug Information

If you have activated the Show Debug Information setting and the service you are navigating is a 10.4 or later Broker, NetWitness Suite displays the debug information beneath the breadcrumb.

The debug information is the `where` clause from the current query. The only time there is no `where` clause is when the time range is all data and there are no drill points. If the Broker has at least one aggregate service that is offline, the debug information also lists the offline service.

For example:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info
exists)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment
exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-
04 18:50:00"-"2014-05-09 18:50:59"
```

In addition, the time taken to load is displayed at the end of each meta key in the Values panel.

Time Banner

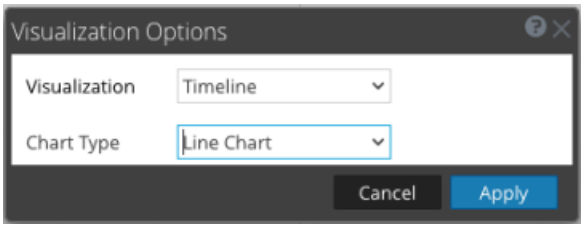
Just below the breadcrumb and debug information (if present), the time banner shows the time range used to create the chart.

Visualizations

At the top of the Navigate view is a visualization of the current drill point. You can use this to drill into data from the Visualization panel (see Filter Results in the Navigate View). You can show or hide the visualization, and choose one of the the visualization options: Timeline or Coordinates. The Visualization opens initially to the last saved Visualization.

Timeline Chart

The timeline is the count of the number of events that occur at a specific instance. The timeline provides event counts so that you can see if the number of events increases drastically at a given point in time. The timeline displays activity for the specified service and time range as a line chart or a bar chart based on your choice in the Options menu. The second figure illustrates a line chart and third figure illustrates a bar chart.



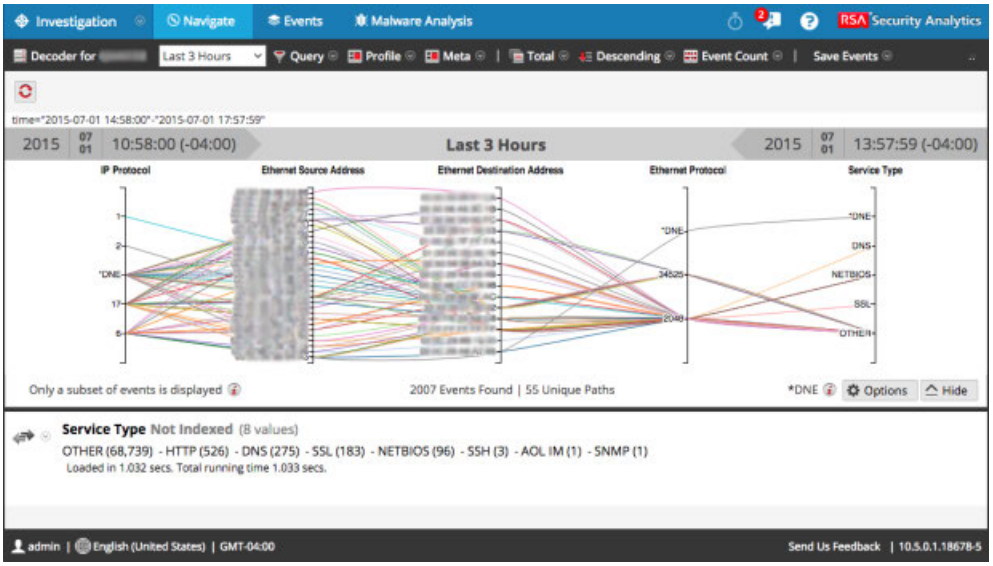
The timeline displays activity for the specified service and time range, as a line chart or a bar chart based on your choice in the Options menu.

Feature	Description
Number of Events (Timeline)	The Y axis of the chart based on thousands of events.
Time Line (Timeline)	The X axis of the chart based on the time the events occurred.
Event point (Timeline)	If you want to explore a specific section, simply select the range from the chart. The new time range will be reflected in the chart.

Feature	Description
Investigate (Timeline)	Displays the meta values for the selected subset.
Reset Zoom (Timeline)	To return to the original time range, click Reset Zoom.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Hide	Collapses the chart.

Parallel Coordinates Chart

The Parallel Coordinates chart is one of the choices in the Options menu for visualizing the current drill point. With Coordinates selected in the Visualization Options dialog, you can select the meta data to be displayed (see Visualize Metadata as Parallel Coordinates).



Feature	Description
Axes	Each axis is a meta key. The number of meta keys affects the load time for the chart. All meta keys are loaded, but it there the number of events per meta key is limited.

Feature	Description
Lines	Lines represent events and they connect values on the axes to show the correlation between multiple meta keys.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Only a subset of events is displayed.	This message is a notification that not all events in the values panel are drawn in the chart. Removing axes or filtering the data in the Values panel can help to display all events.
Events Found | Unique Paths	Displays the total number of events charted versus the number of unique paths charted. Setting the All Meta Keys Must Exist in an Event option redraws the chart so that it is more targeted and legible.
DNE	Indicates that there is no values for this meta key in the event.

In the Visualization Options dialog for Coordinates, you can select the meta keys to chart.

Feature	Description
Visualization selection	Displays a drop-down list of visualization types: Timeline and Coordinates
All Meta Keys Must Exist in an Event	Limits the data represented in the visualization to only those events that include all selected meta keys. This can result in a cleaner, more targeted visualization.
+	Displays the Add Keys to Parallel Coordinates Visualization dialog so that you can add axes to the visualization. This is useful if you are looking for relationships between the default meta keys and some additional ones.
−	Deletes the selected keys so that they do not appear as axes in the visualization. This can help to make the visualization less cluttered and allow for more data points to be included in the visualization.

Feature	Description
	Reverts to the default meta keys for visualization, which consist of all meta keys in the current drill point.
	Controls the display of additional information about the number of selected axes versus the recommended count. This helps to make you aware of possible performance improvements by removing axes.
Axes	Lists the meta keys selected as axes in the visualization.
Cancel	Cancels any changes made to the visualization options.
Apply	Saves the changes made to the visualization options and applies to the current visualization.

In the Add Keys to Parallel Coordinates Visualization dialog, you can select the meta keys or meta groups to use as axes the Parallel Coordinates visualization.

Feature	Description
Visualization selection	Select Keys: Two options for selecting meta keys are: • From Default Meta Keys • From Meta Groups Each option offers a drop-down list from which to select.
With the Selected Meta Keys...	The options for the method of adding meta keys allow you to: • Replace the current list of keys • Append to the current list of keys • Insert at beginning of the current list of keys
Cancel	Closes the dialog and does not add any keys.
Add	Closes the dialog and adds the selected keys as specified.

Values Panel

The major feature of the Navigate view is the Values panel, which you can use to analyze data (see Filter Results in the Navigate View).

The default view is for the last 3 hours of collection, using the default meta keys and non-indexed meta keys closed. The meta keys within the meta groups are displayed in the order that NetWitness Suite queries the keys. As the data loads into the Values panel, NetWitness Suite is optimized to show partial results, loading progress, and service status as the data loads.

The loading behavior is determined by several configuration settings. The highest level settings are configured by the administrator for each user. These are:

- The maximum amount of time allowed for this user to run a query (Query Timeout).
- The limit at which NetWitness Suite stops counting the number of meta values in a session (Session Threshold). If a threshold is set for a session, the Navigate view shows that the threshold was reached and the percentage of results loaded. Any session that does not show a percentage is accurate and was processed to completion. If there is a percentage, that reflects how much processing was completed. The percentage displayed is estimated by extrapolating from the value at the time processing finished, considering the amount of work remaining. Larger percentages are generally more accurate because they require less extrapolating
- The limit at which NetWitness Suite stops counting the number of meta values in a session (Session Threshold). If a threshold is set for a session, the Navigate view shows that the threshold was reached and the percentage of query time used to reach the threshold.

Note: The values for non-indexed meta keys take longer to load in the Values panel. To optimize loading, NetWitness Suite does not open non-indexed meta keys by default. Refer to Manage and Apply Default Meta Keys in an Investigation for a detailed description of non-indexed meta keys in Investigation.

When you have launched an investigation of a service, NetWitness Suite displays results in the Values panel.

1. NetWitness Suite loads meta keys and meta values in the Values panel. For each meta key load, the stages of load are:
    a. **Waiting to Be Loaded** or **Closed**. If Closed, no data for that key is loaded.
    b. **Loading**
        i. **Loading progress**: NetWitness Suite is receiving and displaying progress messages.
        ii. **Partial results**: NetWitness Suite is receiving values messages and partial results are displayed in the Values panel.
    c. **Load Complete**: All results are finished loading.
2. As each meta key load is completed, and final values are displayed, the next meta key is started. The number or values rendered for each meta key is specified by the Render

Threads value in the Investigation Preference settings. Loading continues until all keys to be loaded have finished.

3. If **Show Debug Information** is active and the service you are navigating is a 10.4 or later Broker, NetWitness Suite displays load time information beneath the values for each meta key and displays additional load details for the aggregated services. NetWitness Suite also displays the debug information beneath the breadcrumb.

Iterative results

Iterative results provide feedback on the status of queries within the interfaces to provide additional context for how long the data load will take and if any service data is missing. For example, if you are querying a Broker that is aggregating from two Concentrators, NetWitness Suite starts displaying the results from the first Concentrator as soon as it is available, even if the second Concentrator is still waiting for results.

Iterative results also include a notification that service data is missing because the service is unreachable.

Partial results

When partial values from the Core service are returned but not completed, a message at the end of the meta key listing shows the progress of values loaded. For example, Currently looking at 38 ip.src values 71% indicates that loading of values for the meta key is 71% complete.

Debug Information

If the Show Debug Information setting is in effect, a field at the end of the values displays the status for the different systems against which you are querying within NetWitness Suite. For example, when you are querying against a 10.4 broker pulling from multiple concentrators, NetWitness Suite displays the status of the query on each of the Concentrators, which provides insight into the relative speed of data loading from each of the Concentrators. Each service that participated in the query is listed with the total elapsed time for the query.

Each service that participated in the query is listed with the total elasped time for the query. In the example above, two services returned in 3.207 seconds, localhost:50005 took 2 seconds to return the results. In addition, the where clause of the query is displayed below the breadcrumb. You can copy this syntax directly into an application rule or Reporting where clause of a rule.

Load Complete

For each meta key, there is a list of values (blue text) and counts (green text) found in the current drill point. When you click a value to drill down into a subset of the currently selected data, the display is updated and the new drill point is recorded in the breadcrumb. You can specify the sorting and quantification methods for the values list using the option in the toolbar.

Note: Title, values, and counts for non-indexed meta keys are not drillable; the Values and counts are shown in black.

Feature	Description
Meta Key	The name of the meta that is listed, for example, **Service Type** is a meta key.
Number of values rendered vs number of values available to load	The number or values rendered is specified by the Render Threads value in the Investigation Preference settings. In the example above, the meta key is **Service Type**, and 20 of 20+ values are currently displayed. You can display additional values by clicking **...show more**.
	Clicking on an indexed meta key opens the Search dialog in which you can enter a filter for the current meta key. The search function is not available for non-indexed meta keys, and is based on the actual meta value rather than the alias. Drilling in the Search dialog using aliases is not supported. NOTE: Check with your administrator to obtain a list of aliases used for a meta key in Investigation. When an alias is used, this search dialog does not provide results. Instead, you must query the meta key using the Right-click query capability or the Query dialog.
Offline Services: xxx.xxx.xxx.xxx:50004	Lists offline services queried by a 10.4 Broker.
Meta Count, for example (3)	The number of instances found for a particular meta in the session.
Meta Value, for example other src	The specific name associated with the found meta.
...show more	If the number of meta values has been limited (for example, 20), clicking this displays additional meta values for the selected meta key.

Feature	Description
Loaded in 0.418 secs. Total running time 0.434 secs. (localhost:50005 loaded in 1 secs....	Debug stats display load times based on the Show Debug Information setting.

Meta Key Drop-Down Menus

The Meta Keys in the Values panel have drop-down menus. Next to each meta label, a drop-down arrow displays the options that can apply to that item. You can use these to change the way the results for the meta key are displayed in the current view. Changes made to meta keys are displayed in the current view and persist until you refresh the page or select a new service in the Navigate view toolbar. See Drill into Data in the Values Panel

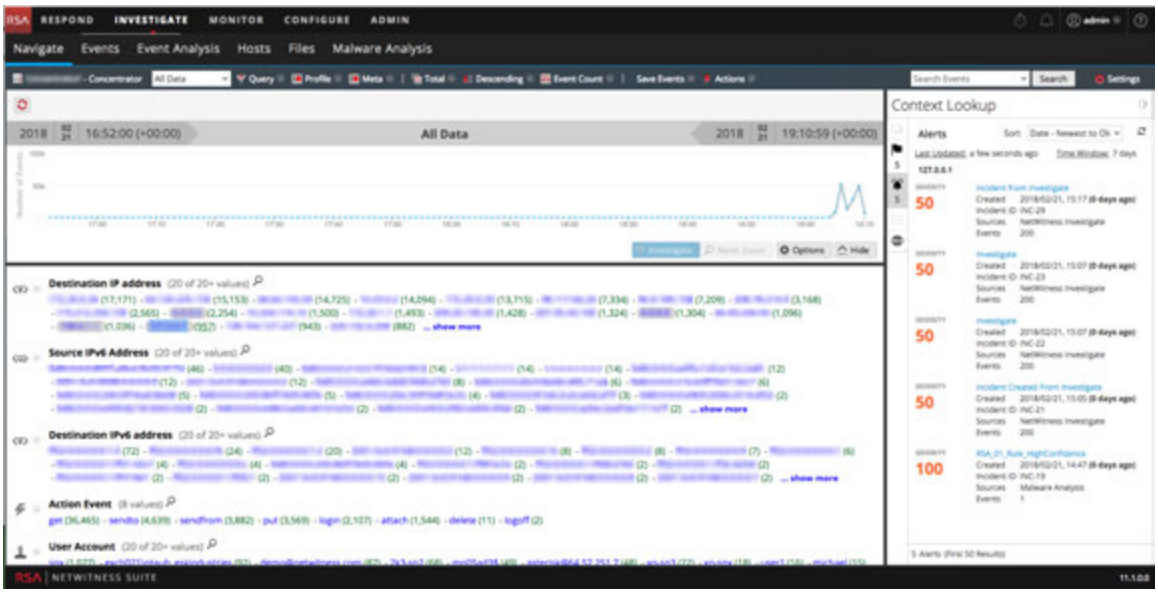
Refresh reverts to the current view of meta keys as defined in the Manage Default Meta Keys dialog (see Manage and Apply Default Meta Keys in an Investigation). If you have never made modifications in the Manage Default Meta Keys dialog, NetWitness Suite restores the default meta keys from the core service.

- More Results
- Max Results
- Hide Results
- Meta Key Info
- View as CSV (Version 11.0.0.x) or Export Values (Version 11.1 and later)

Context Lookup Panel

The Navigate view and the Events view have a Context Lookup panel on the right side. The Context Lookup panel is displayed only if you have installed and configured the Context Hub service. For more information on configuring the Context Hub service, see the *Context Hub Configuration Guide*.

The Context Lookup panel displays relevant data when an analyst looks up contextual data for a meta value in the Values panel.

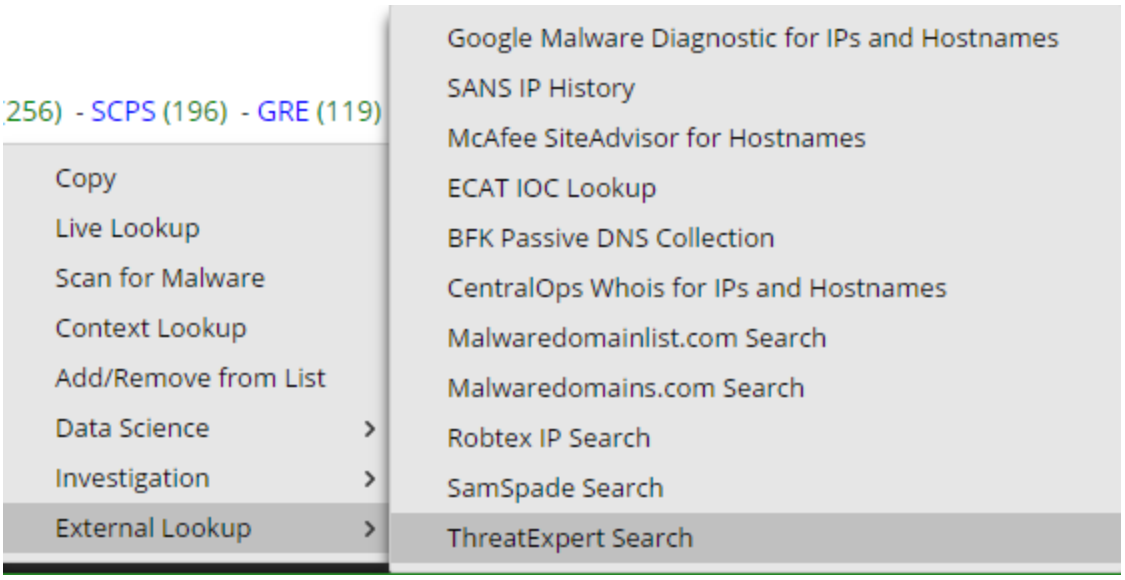


After the administrator configures the Context Hub service, you can view the contextual information for the meta values in the Navigate view and the Events view. For more information on configuring the Context Hub service, see the *Context Hub Configuration Guide*. For information about performing Context Lookup for meta values, see View Additional Context for a Data Point.

The Context Hub service is pre-configured with default meta type and meta key mapping. For information about the mapping of the context hub meta value with investigation meta key, see "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*

You can view the type of context data that is available for a highlighted meta value by hovering the mouse over a highlighted meta value. An inline indicator shows which type of context data is available for the meta: Endpoint, Incidents, Alerts, or Lists.

Right-clicking a meta value opens a menu with the context lookup option. The following figure illustrates the Context Lookup option when you right-click a meta value.



For meta keys such as IP, Host and Mac Address, the details of the values that are flagged are collected from Endpoint, Incident, Alerts, and Lists.

For meta keys such as File, File Hash, Domain, User, the details of the values that are flagged are collected from Incidents, Alerts, and Lists.

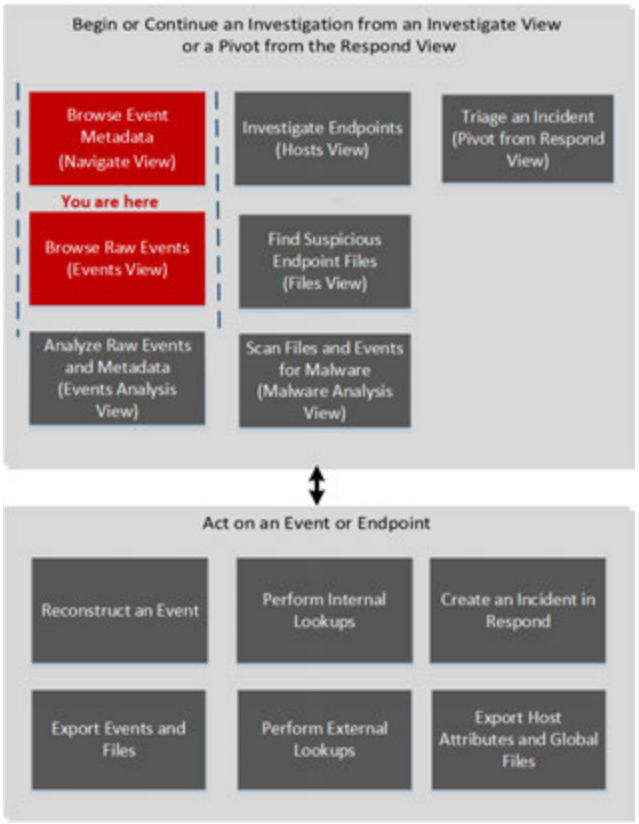
The data is displayed in the context panel, only if there is any data available .

For more information about the lookup results and contextual information for different data sources, see Context Lookup Panel.

Query Dialog

In the Navigate view or Events view, you can create a query rather than clicking through the meta keys and values to drill down into the meta data. The dialogs for creating a query offer syntax help with drop-down lists of applicable meta keys and operators. To access this dialog in the **Navigate** or **Events** view toolbar, select **Query**.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata*	Begin an Investigation in the Navigate or Events View

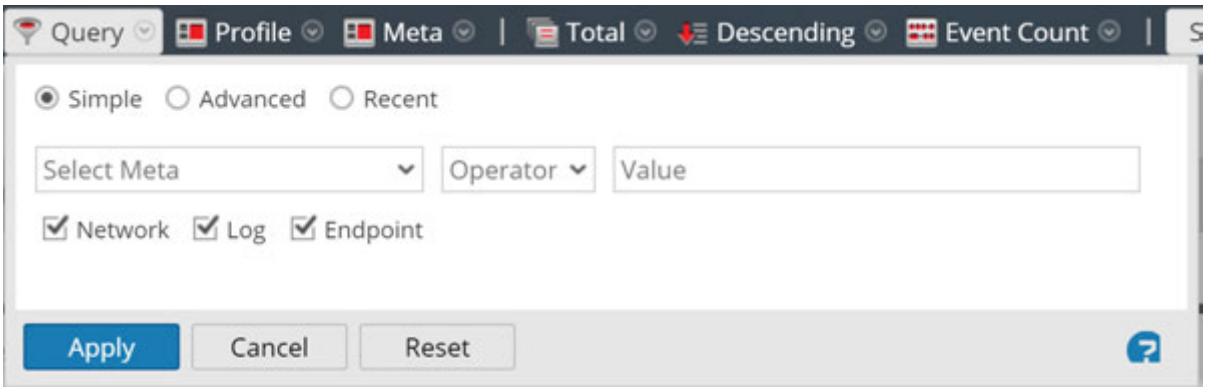
User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events*	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	create a custom query*	Create a Custom Query

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works

Quick Look

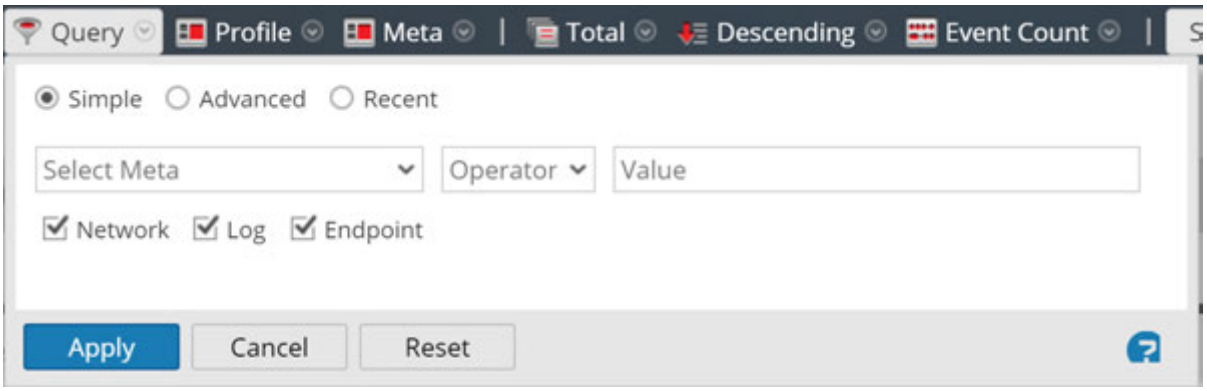


The Query dialog has three views:

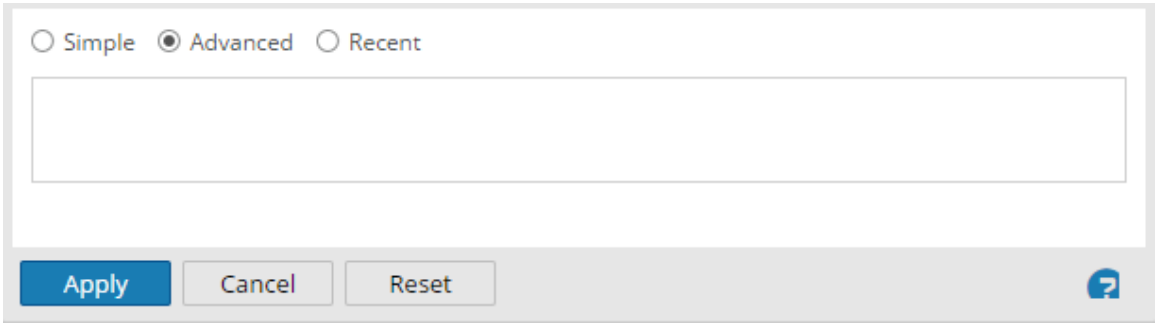
- Simple
- Advanced
- Recent

In the Simple view, you can create a query using the options displayed in the dialog. In the Advanced view, you can create a query without guidance. In the Recent view, you can select a query from a drop-down list of recent queries.

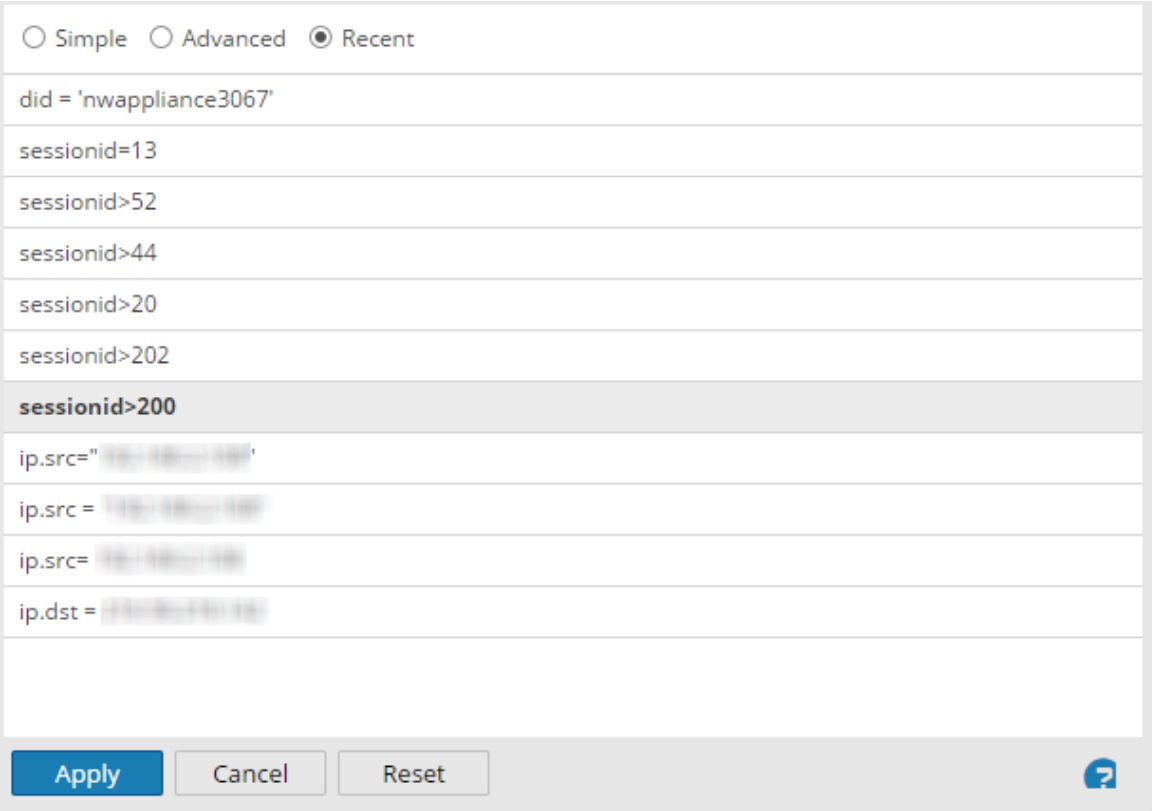
Simple View



Advanced View



Recent View



The following table describes features of the Query dialogs.

Feature	Description
Select Meta	Displays a drop-down list of meta groups.
Operator	Displays a drop-down list of operators (=,NetWitness Suite!=,NetWitness Suiteexists,NetWitness Suite!exists)
Value	Allows you to enter a value to complete the query.
Network	Limits the query to packets if Log is not selected.
Log	Limits the query to logs if Network is not selected.

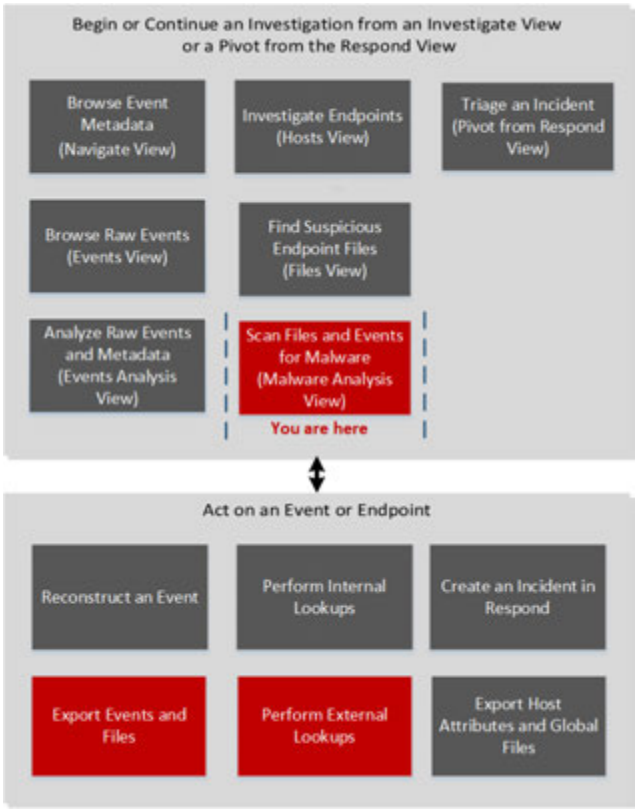
Feature	Description
Query box	Allows you to enter a query in the Advanced view. When you begin typing, a drop-down list of available meta keys for the service is displayed, then a drop-down of operators is displayed as you type. If the expression currently entered in the query box is invalid, a warning appears near the box. When the query is valid, the warning is removed.
Query list	Allows you to select a query from a list of recent queries in the Recent view. Double-clicking a query automatically applies it.
Apply	Applies the new query to the current Investigation view.
Cancel	Closes the dialog without applying changes.
Reset	Resets all fields.

Scan For Malware Dialog

In the Scan for Malware dialog, Malware Analysis analysts can upload files to investigate in Malware Analysis.

To access this dialog go to the **Malware Analysis** view. In the **Select a Malware Analysis Service** dialog, select a service in the left panel, then click Scan Files in the right panel.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

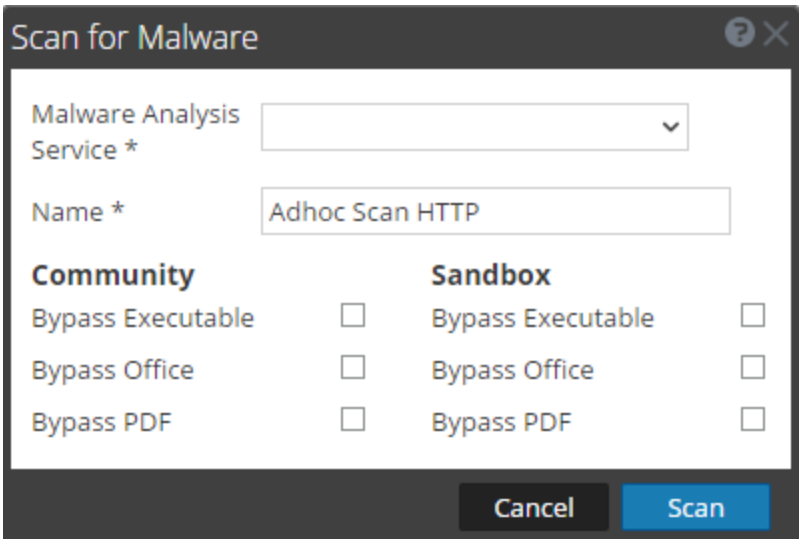
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Begin a Malware Analysis Investigation
- Launch a Malware Analysis Scan from the Navigate View

Quick Look

The figure below illustrates the Scan for Malware dialog, and The following table describes the features available in the dialog.

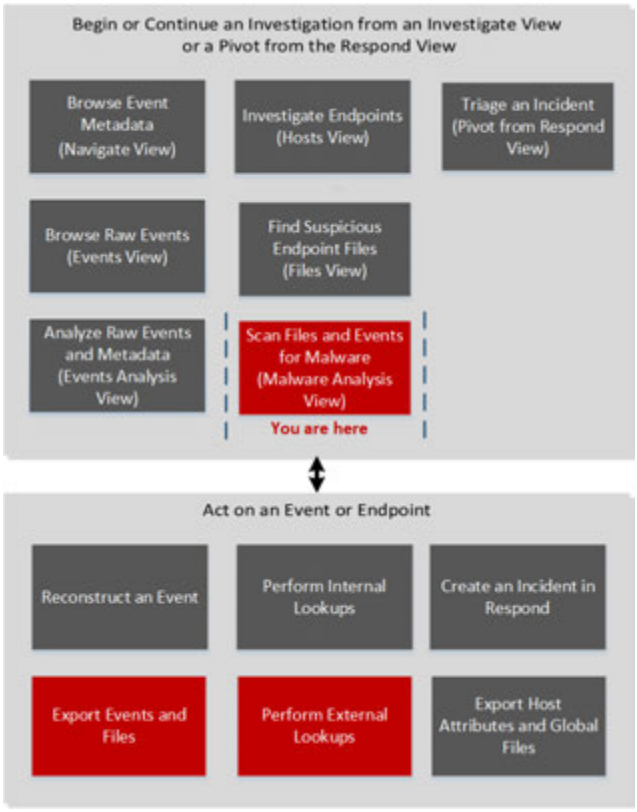


Feature	Description
+	Uploads a file from your computer.
−	Deletes a file from the list.
File Name	Displays the names of the files added to the list.
Name	Allows you to name the scan job.
Community	Displays options for Community to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Sandbox	Displays options for Sandbox to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Cancel	Closes the dialog without performing any actions.
Scan	Scans the uploaded files.

Select a Malware Analysis Service Dialog

The Select a Malware Analysis Service dialog is accessible in the Malware Analysis view. In this dialog, Malware Analysis analysts can select a service to investigate, choose a scan on that service to investigate, upload a file to scan, and begin a continuous scan of the service.

Workflow



What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View

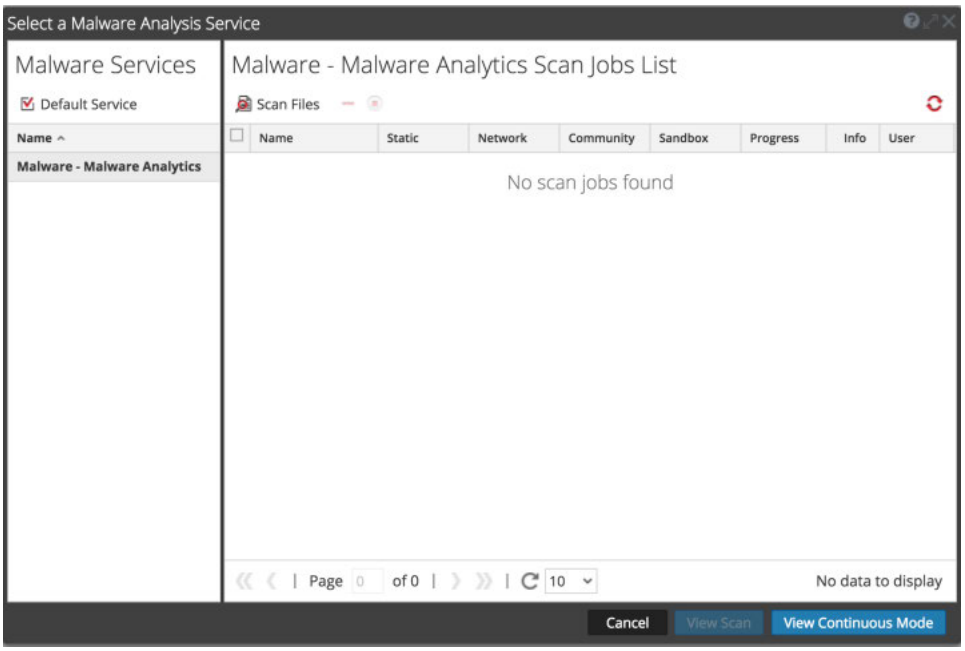
User Role	I want to ...	11.1 Documentation
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware*	Conducting Malware Analysis
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Begin a Malware Analysis Investigation
- Launch a Malware Analysis Scan from the Navigate View

Quick Look



The Select a Malware Analysis Service dialog has a Malware Services panel on the left and a Scan Jobs List on the right. The Scan Jobs List panel has a toolbar, list, and buttons to view scans.

The Malware Services panel is a list of services available for malware analysis. In this panel, you can select the service to investigate and you set a default service using the Default Service icon. When you select a service, the available scan jobs for that service are listed in the Scan Jobs list.

These are the features in the Scan Jobs List toolbar.

Feature	Description
Scan Files	Displays the Scan for Malware dialog, in which you can upload a file to the service for scanning.
Delete scan job ( )	Deletes one or more selected scan jobs, NetWitness Suite displays a confirmation dialog before deleting scan jobs.
Cancel scan job ( )	Pauses or continues one or more scan jobs.
Refresh ( )	Refreshes the list of scan jobs.

These are the columns in the Scan Jobs list. This list is also available in the Malware Scan Jobs dashlet.

Feature	Description
Name	Displays the name of the job.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module.
Progress	Displays the current progress made on the job. • Green: The job is finished. • Black: The job is in progress. • Red: An error occurred.
Info	Provides additional information. Displays the query for the job. If the job is not complete, it also displays more detailed description of the status.
User	Displays the name of the user who created the job.
Events	Counts the number of events for the job.
Dropped	Counts the number of files/events in the job that were dropped because the scores are below their configured threshold.
Event Type	Displays the type of job: Manual Upload, On Demand, or Resubmit.
Scheduled	Displays the date and time when the job was executed.

These are the available actions in the dialog.

Feature	Description
Cancel button	Cancels the selected scan job.
View Scan button	Displays the Summary of Events for the selected scan with the default dashlets displayed.
View Continuous Mode button	Displays the Summary of Events for the selected scan with the default dashlets displayed.

Settings Dialogs for Investigate Views

NetWitness SuiteVersion 11.0 has two settings dialogs, one for the Navigate view and one for the Events view. With the addition of the settings dialog for the Event Analysis view in Version 11.1, Investigate has three settings dialogs.

The settings in the Navigate view and Events view Settings dialogs are a subset of the Investigation settings made in the Profiles > Preferences panel > Investigations tab. By providing the settings within the Investigation view, NetWitness Suite saves time for analysts. If you change a setting here, the same setting is changed in the Profiles view, and if you change a setting in the Profiles view, the same setting is changed here.

To access this dialog, go to the **Navigate** or **Events** view, and select the **Settings** option in the toolbar.

The settings in the Event Analysis view have no corresponding settings in the Profiles > Preferences panel.

What do you want to do?

User Role	I want to ...	11.1 Documentation
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1)	Investigate Hosts
Threat Hunter	find suspicious endpoint files (Version 11.1)	Investigate Files
Threat Hunter	scan files and events for malware	Conducting Malware Analysis

User Role	I want to ...	11.1 Documentation
Incident Responder	triage an incident in Investigate	*NetWitness Respond User Guide*
Threat Hunter	configure preferences for Investigate*	Configuring NetWitness Investigate Views and Preferences

*You can perform this task in the current view.

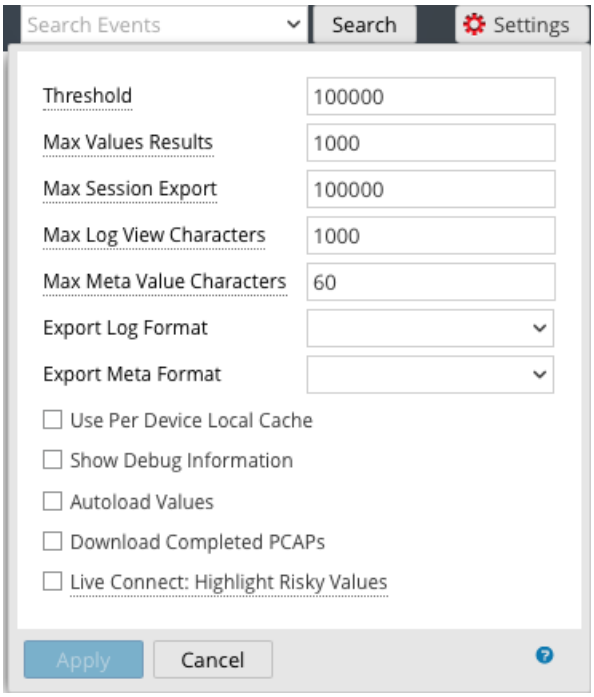
Related Topics

- How NetWitness Investigate Works

Quick Look

The Settings dialogs in the Navigate view and Events view have several features in common.

Several Investigation settings in the Navigate view influence the performance of when loading values in the Values panel. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations. The image below is an example of the dialog, and the following table describes the features.

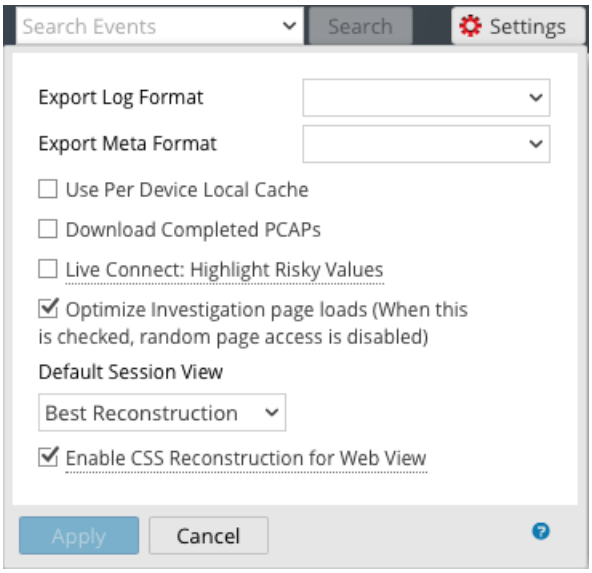


Feature	Description
Threshold	Sets the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.
Max Values Results	Sets the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
Max Session Export	Sets the maximum number of sessions able to be exported. The default value is **100000**.
Export Log Format	Sets the file format of exported logs. There are four formats available: • Text • SML • CSV • JSON
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • Text • SML • CSV • JSON
Use Per Device Local Cache	When unchecked, Investigate sends a fresh query to the database rather than displaying cached data in the Investigate views after the initial load. If checked, Investigate uses the data from local cache.
Show Debug Information	This option controls the display of the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker. When checked the debug information is displayed. The default value is **Off** (unchecked)**.**

Feature	Description
Append Events in Event Panel	This option affects paging in the Events panel. When checked, the next group of events is appended to the already displayed events. When unchecked, the previous page of events is replaced by the next page. The default value is **Off** (unchecked)
Autoload Values	This option controls automati loading of values for the selected service in the Navigate view. When checked, values are automatically loaded when you select a service to investigate. When not checked, Investigate displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigation module so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form.
Live Connect: Highlight Risky IPs	If this option is unchecked, all the meta values that have context available in Live Connect are highlighted in the Navigate view Values panel. If the option is checked, among the values that have context in Live Connect, only those values deemed Risky/Suspicious/Unsafe by the community are highlighted. By default this option is unchecked (**Off**).
Apply	Applies the settings immediately and they are visible the next time you load values. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.

Events View Settings Dialog

The following image is an example of the Settings dialog for the Events view, and the following table describes the features.



Feature	Description
Export Log Format	Sets the file format of exported logs. There are four formats available: • Text • SML • CSV • JSON
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • Text • SML • CSV • JSON
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigation module so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form.

Feature	Description
Live Connect: Highlight Risky IPs	When checked, Investigate uses a filter to fetch only IP addresses that are considered as risky by RSA community. When not selected, NetWitness Suite displays all IP addresses. By default, this option is not selected (**Off**).
Optimize Investigation page loads	Sets a paging option. When optimized, results are returned as quickly as possible, sacrificing the original ability to go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is **enabled**.
Default Session View	Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Uncheck this option if there are problems viewing specific websites.
Apply	Applies the settings immediately and they are visible the next time you view events. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.

Event Analysis View Preferences Panel

Beginning with Version 11.1, the Event Analysis view has user preferences that you can configure in the Event Analysis view > Event Preferences panel. These settings persist so that they are applied each time log in and go to the Event Analysis view. The following table describes the options.

Feature	Description
Default Event Analysis View	Selects the default event analysis view that is displayed every time you open the Event Analysis view. For example, if you select File Analysis, the File Analysis panel is highlighted and displayed every time you investigate an event in the Event Analysis view. These are following options: • **Text Analysis**: View and analyze the raw text payload of an event. • **Packet Analysis**: View and interactively analyze the packets and payload of an event. • **File Analysis**: View a list of files and download one or more files in an event.
Default Log Format	Selects the default format for downloading logs: • **Download Log**: Raw log (log) using this option. • **Download CSV**: Comma-separated values (CSV) using this option. • **Download XML**: The Extensible Markup Language (XML) file using this option. • **Download JSON**: The JavaScript Object Notation (JSON) file using this option.

Feature	Description
Default Packet Format	Selects the default packet format for downloading packets. • **Download PCAP**: To download the entire event as a packet capture (*.pcap) file. • **Download All Payloads**: To download the payload as a *.payload file. • **Download Request Payload**: To download the request payload as a *.payload1 file. • **Download Response Payload**: To download the response payload as a *.payload2 file.
Time Format for Query	The Event Analysis view can display results based on the database time or the current clock time. The default setting for this preference is Database Time, which is the same time format used to display query results in the Navigate view and Events view. When **Database Time** is selected, the start and end time for a query is based on the time that the event was captured. When **Wall Clock Time** is selected, the query is executed using the end time based on the current browser time; the start time is calculated based on that end time and the time range.
Download extracted files automatically	Enables the automatic download of files if they are in the selected default format in the **Default Log Format** and **Default Packet format** fields from the Event Preferences panel. Select the checkbox to enable downloading the selected format automatically to local folder. Otherwise, the download job goes to the job queue, and you can download it manually.

RSA NETWITNESS® SUITE

NetWitness Respond User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Respond Process **7**

NetWitness Respond Workflow 8

Responding to Incidents **9**

Responding to Incidents Workflow 11

Review Prioritized Incident List 11

View the Incidents List 11

Filter the Incident List 13

Remove My Filters from the Incident List View 16

View My Incidents 16

Find an Incident 16

Sort the Incidents List 17

View Unassigned Incidents 18

Assign Incidents to Myself 18

Unassign an Incident 20

Determine which Incidents Require Action **21**

View Incident Details 21

View Basic Summary Information about the Incident 23

View the Indicators and Enrichments 25

View and Study the Events 27

View and Study the Entities Involved in the Events 30

Filter the Data in the Incident Details View 32

View the Tasks associated with an Incident 35

View Incident Notes 35

Find Related Indicators 36

Add Related Indicators to the Incident 38

Investigate the Incident **40**

View Contextual Information 40

Add an Entity to a Whitelist 43

Create a List 43

Pivot to NetWitness Endpoint 44

Pivot to Investigate 44
Document Steps Taken Outside of NetWitness 45
View the Journal Entries for an Incident 46
Add a Note 47
Delete a Note 48

Escalate or Remediate the Incident 49

Update an Incident 49
Change Incident Status 49
Change Incident Priority 52
Assign incidents to other Analysts 55
Rename an Incident 57
View All Incident Tasks 58
Filter the Tasks List 60
Remove My Filters from the Tasks List 62
Create a Task 62
Find a Task 66
Modify a Task 67
Delete a Task 71
Close an Incident 73

Reviewing Alerts 74

View Alerts 74
Filter the Alerts List 76
Remove My Filters from the Alerts List 79
View Alert Summary Information 79
View Event Details for an Alert 80
Investigate Events 84
View Contextual Information 84
Add an Entity to a Whitelist 87
Create a Whitelist 87
Pivot to NetWitness Endpoint 88
Pivot to Investigation 88
Create an Incident Manually 88
Add Alerts to an Incident 90
Delete Alerts 92

NetWitness Respond Reference Information 94

Incidents List View 95
Workflow 95
What do you want to do? 96
Related Topics 96
Quick Look 97
Incidents List View 97
Incidents List 99
Filters Panel 100
Overview Panel 102
Toolbar Actions 104
Incident Details View 105
Workflow 105
What do you want to do? 106
Related Topics 107
Quick Look 107
Overview Panel 109
Indicators Panel 109
Nodal Graph 110
Events Datasheet 113
Journal Panel 116
Tasks Panel 117
Related Indicators Panel 118
Toolbar Actions 120
Alerts List View 122
Workflow 122
What do you want to do? 122
Related Topics 123
Alerts List View 123
Alerts List 124
Filters Panel 127
Overview Panel 129
Toolbar Actions 132
Alert Details View 133
Workflow 133
What do you want to do? 133

Related Topics 134
Alert Details View 134
Overview Panel 135
Events Panel 135
Events List 136
Event Details 136
Event Metadata 137
Event Source or Destination Device Attributes 138
Event Source or Destination User Attributes 139
Toolbar Actions 140
Tasks List View 141
What do you want to do? 141
Related Topics 141
Tasks List 142
Task Overview Panel 146
Toolbar Actions 148
Add/Remove from List Dialog 149
What do you want to do? 149
Add/Remove from List 150
Context Lookup Panel - Respond View 153
What do you want to do? 153
Related Topics 154
Contextual Information Displayed in the Context Lookup Panel 154

NetWitness Respond Process

NetWitness Suite Respond collects alerts from multiple sources and provides the ability to group them logically and start an Incident Respond workflow to investigate and remediate the security issues raised. NetWitness Suite Respond enables you to configure rules that aggregate Alerts into Incidents. Alerts will be normalized by the system to a common format to provide users with a consistent view for the rule criteria regardless of the data source. You can build query criteria based on the alert data with the ability to query on fields that are common as well as specific to data sources.

The rule engine allows you to group similar alerts together into an Incident so that the investigation and remediation workflow can be shared across a set of similar alerts. You can create rules that can group alerts into incidents depending on a common value they share for one or two attributes (for example, source hostname) or if they are reported within a limited time window (for example, alerts that are within four hours of each other).

If an alert matches a rule, an incident is created using the criteria. As new alerts are ingested, if an existing Incident was already created that matched those criteria, and that incident is not "in progress" yet, the new alerts will continue to be added to the same incident. If there is no existing incident for the grouped value (for example, the specific hostname) or the time window, a new incident will be created and the alert will be added to it.

You can have multiple incident rules. The rules can either group alerts into Incidents or suppress alerts from being matched by any rule, hence the rules are ranked top-to-bottom and only the first rule to match an incoming alert is used to include that alert in an incident. The Incidents provide a context for the alerts, provide tools to record the investigation status, and track the progress of associated tasks.

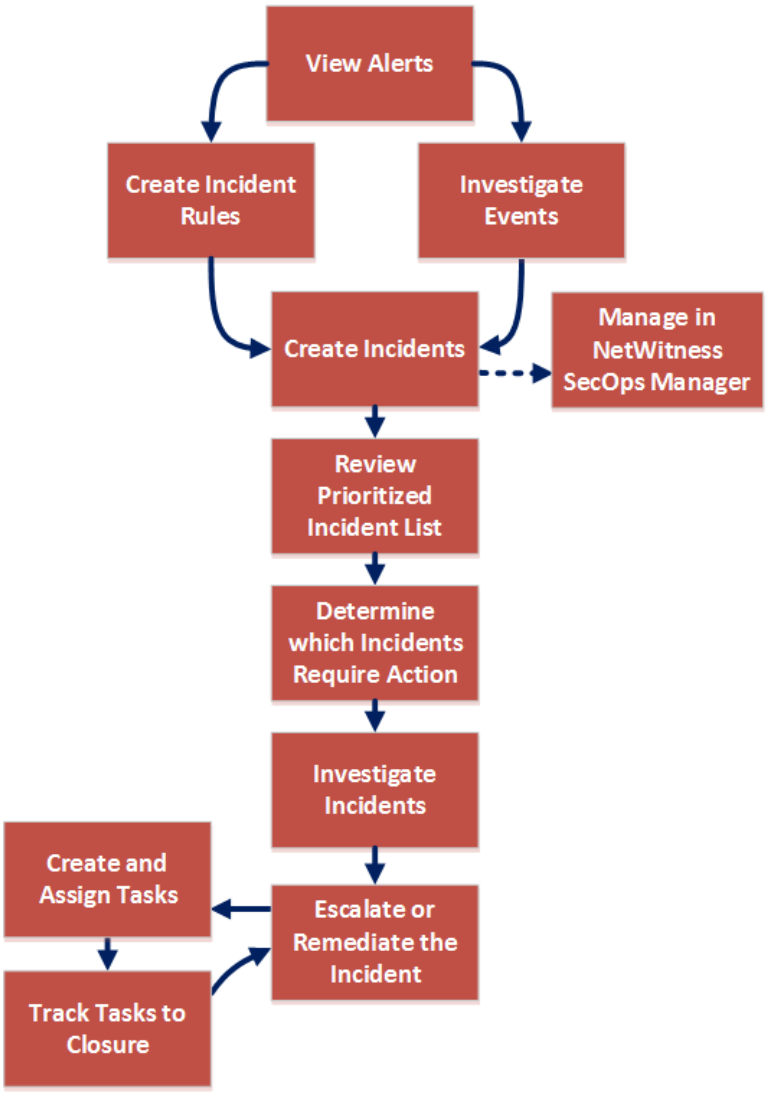
The stages in the NetWitness Respond process are:

- Review Alerts
- Create Incidents
- Respond to Incidents:
  - Review Prioritized Incident List
  - Determine which Incidents Require Action
  - Investigate Incidents
  - Escalate or Remediate the Incident (This includes creating and assigning tasks as well as tracking tasks to closure.)

You also have the option of managing incidents in RSA NetWitness® SecOps Manager instead of NetWitness Respond.

NetWitness Respond Workflow

The following figure shows the high-level NetWitness Respond workflow process.



Responding to Incidents

An *Incident* is a logically grouped set of alerts created automatically by the Incident Aggregation Engine and grouped by a specific criteria. An Incident, available in the Respond view, allows an Analyst to triage, investigate, and remediate these groups of alerts. Incidents can be moved between users, notated, and explored using a nodal graph. Incidents allow users to ensure that they understand the full scope of an attack or event in their NetWitness Suite system and then take action.

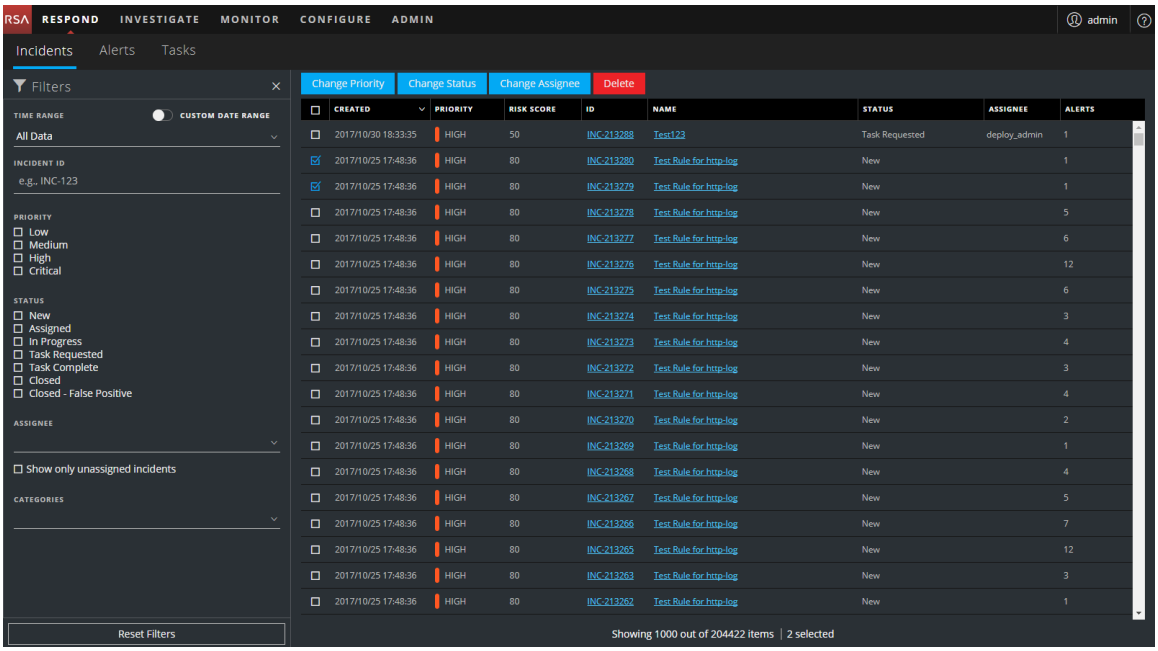
The **Respond** view is designed to help you quickly identify the ongoing issues in your network and work with other Analysts to quickly solve the issues.

The Respond view presents Incident Responders with a queue of incidents in severity order. When you take an incident from the queue, you receive relevant supporting data to help you investigate the incident. This enables you to determine the incident scope so you can escalate or remediate it as appropriate.

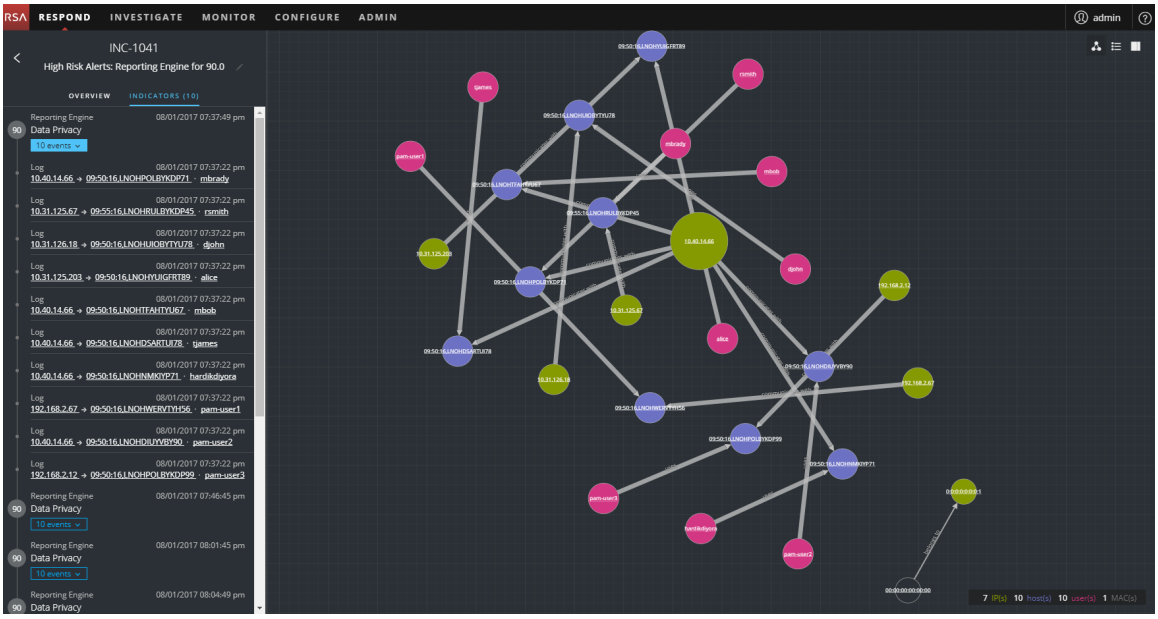
Within the Respond view, you can see Incidents, Alerts, and Tasks:

- **Incidents**: Enables you to respond to and manage incidents from start to finish.
- **Alerts**: Enables you to manage alerts from all sources received by NetWitness Suite and create incidents from selected alerts.
- **Tasks**: Enables you to view and manage the complete list of tasks created for all incidents.

If you navigate to RESPOND > Incidents, you can see the Incidents List view and from there you can access the Incident Details view for a selected incident. These are the main views that you use to respond to incidents. The following figure shows the list of prioritized incidents in the **Incidents List** view.



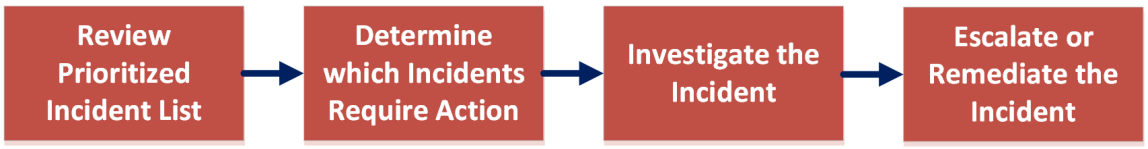
The next figure shows an example of details available in the **Incident Details** view.



The Respond view is designed to make it easy to evaluate incidents, contextualize that data, collaborate with other analysts, and pivot to a deep-dive investigation as needed.

Responding to Incidents Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



First, you review the list of prioritized incidents, which shows basic information about each incident, and determine which incidents require action. You can click a link in an incident to get a clearer picture of the incident with supporting details in the Incident Details view. From there, you can further investigate the incident. You can then determine how to respond to the incident, by escalating or remediating it.

These are the basic steps for responding to an incident:

1. Review Prioritized Incident List
2. Determine which Incidents Require Action
3. Investigate the Incident
4. Escalate or Remediate the Incident

Review Prioritized Incident List

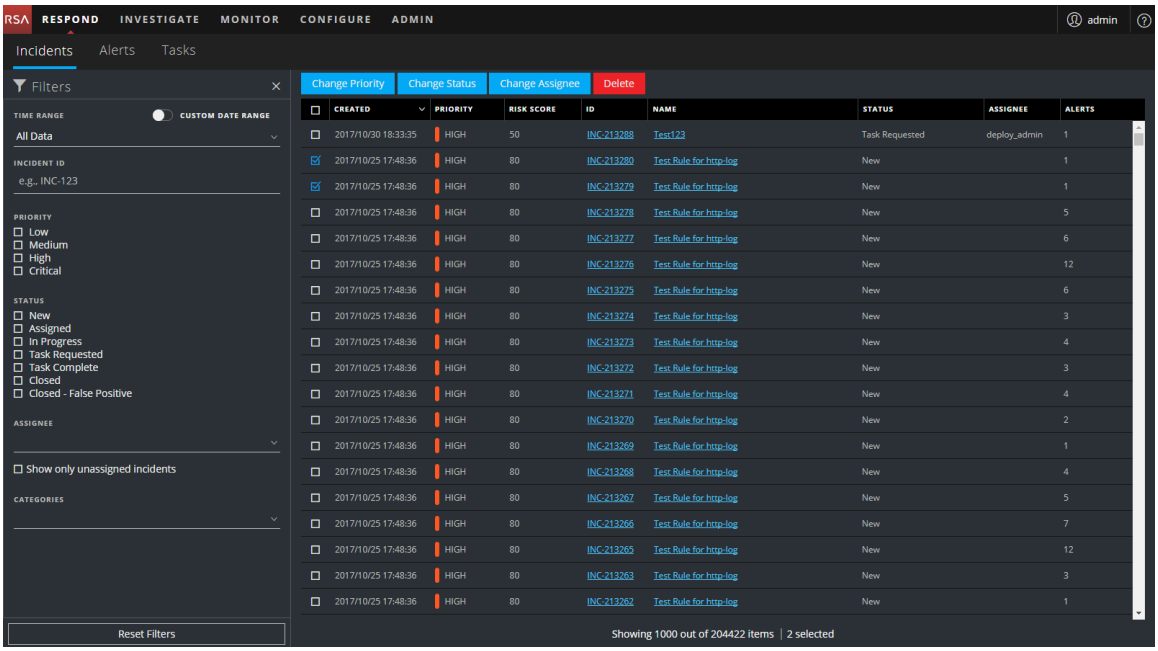
In the Respond view, you can view the list of prioritized incidents. The incident list shows both active and closed incidents.

View the Incidents List

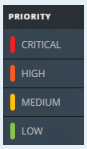
After logging in to NetWitness Suite, most Incident Responders see the Respond view, which is set as the default view. If you have a different initial view, you can navigate to the Respond view.

1. Log in to NetWitness Suite.

   The Respond view shows the list of incidents, also referred to as the Incident List view.



2. If you do not see the incidents list in the Respond view, go to **RESPOND > Incidents**.
3. Scroll through the incidents list, which shows basic information about each incident as described in the following table.

Column	Description
CREATED	Shows the creation date of the incident.
PRIORITY	Shows the incident priority. Priority can be Critical, High, Medium or Low. The Priority is color coded, where red indicates a **Critical** incident, orange represents a **High** risk incident, yellow indicates a **Medium** risk incident, and green represents a **Low** risk incident. For example: 
RISK SCORE	Shows the incident risk score. The risk score indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
ID	Shows the automatically created incident number. Each incident is assigned a unique number that you can use to track the incident.

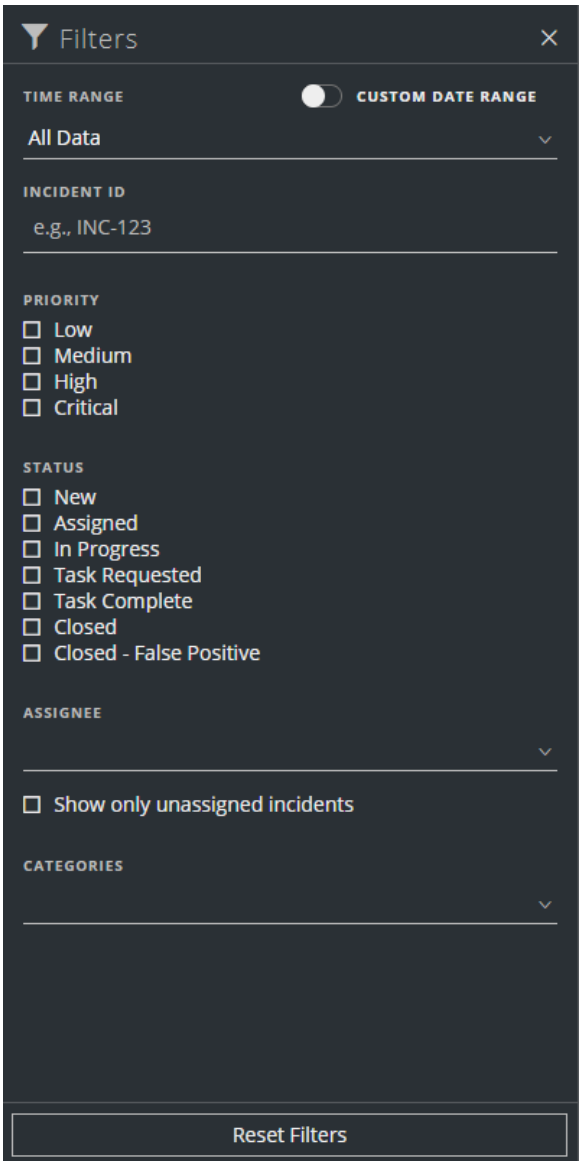
Column	Description
NAME	Shows the incident name. The incident name is derived from the rule used to trigger the incident. Click the link to go to the Incident Details view for the selected incident.
STATUS	Shows the incident status. The status can be: **New**, **Assigned**, **In Progress**, **Task Requested**, **Task Complete, Closed**, and **Closed- False Positive**.
ASSIGNEE	Shows the team member currently assigned to the incident.
ALERTS	Shows the number of alerts associated with the incident. An incident may include many alerts. A large number of alerts might mean that you are experiencing a large-scale attack.

At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number selected. For example: **Showing 1000 out of 1115 items | 3 selected**. The maximum number of incidents that you can view at one time is 1,000.

Filter the Incident List

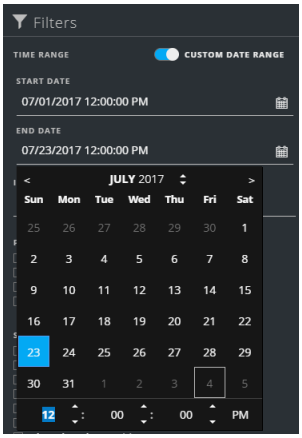
The number of incidents in the Incidents List view can be very large, making it difficult to locate particular incidents. The Filter enables you to specify those incidents that you would like to view. You can also choose the timeframe when those incidents occurred. For example, you may want to view all of the new critical incidents created within the last hour.

1. Verify that the Filters panel appears to the left of the incidents list. If you do not see the Filters panel, in the Incident List view toolbar, click , which opens the Filters panel.



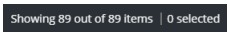
2. In the Filters panel, select one or more options to filter the incidents list:
   - **TIME RANGE**: You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the incidents. For example, if you select Last Hour, you will see incidents that were created within the last 60 minutes.
   - **CUSTOM DATE RANGE**: You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to

view the Start Date and End Date fields. Select the dates and times from the calendar.



- **INCIDENT ID**: Type the Incident ID for an incident you would like to locate, for example INC-1050.
- **PRIORITY**: Select the priorities that you would like to view.
- **STATUS**: Select one or more incident statuses. For example, select Closed - False Positive to view only false positive incidents, which were initially identified as suspicious, but then they were later found to be safe.
- **ASSIGNEE**: Select the assignee or assignees of the incidents that you would like to view. For example, if you only want to view the incidents assigned to Cale or Stanley, select Cale and Stanley from the Assignee drop-down list. If you want to view incidents regardless of the assignee, do not make a selection under Assignee.
  (Available in version 11.1 and Later) To view only unassigned incidents, select **Show only unassigned incidents**.
- **CATEGORIES**: Select one or more categories from the drop-down list. For example, if you only want to view incidents classified with the Backdoor or Privilege abuse categories, select Backdoor and Privilege abuse.

The incidents list shows a list of incidents that meet your selection criteria. You can see the number of incidents in your filtered list at the bottom of the incident list.



3. Click ✕ to close the Filters panel and return to the Incidents List view, which now shows your filtered incidents.

Remove My Filters from the Incident List View

NetWitness Suite remembers your filter selections in the Incident List view. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of incidents that you expect to see or you want to view all of the incidents in your incident list, you can reset your filters.

1. In the Incident List view toolbar, click .
   The Filters panel appears to the left of the incidents list.
2. At the bottom of the Filters panel, click **Reset Filters**.

View My Incidents

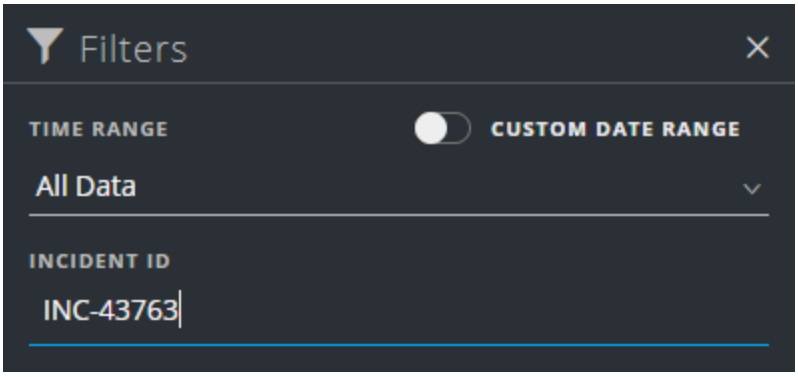
You can view your incidents by filtering the incidents by your username.

1. If you cannot see the Filter panel, in the Incident List view toolbar, click .
2. In the Filter panel, under ASSIGNEE, select your username from the drop-down list.
   The incidents list shows the incidents that are assigned to you.

Find an Incident

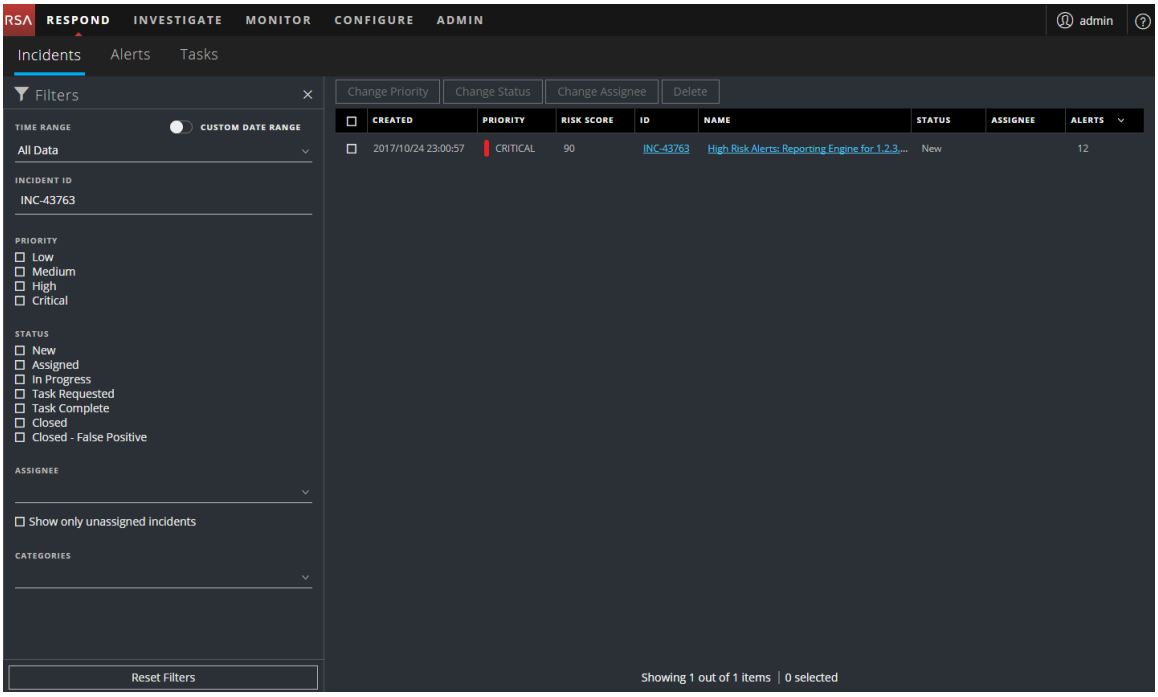
If you know the Incident ID, you can quickly locate an incident using the Filter. For example, you may want to locate a specific incident out of thousands of incidents.

1. Go to **RESPOND > Incidents**.
   The Filters panel appears to the left of the incidents list. If you do not see the Filters panel, in the Incident Lists view toolbar, click , which opens the Filters panel.



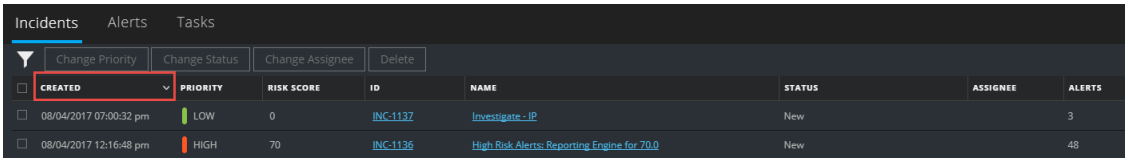
2. In the INCIDENT ID field, type the INCIDENT ID for an incident that you would like to locate, for example INC-43763.

The specified incident appears in your incident list. If you do not see any results, try resetting your filters.



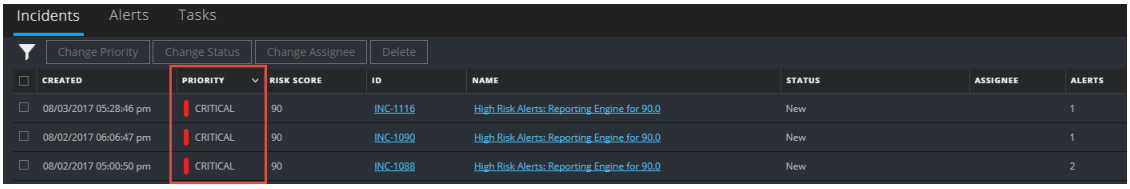
Sort the Incidents List

The default sort for the incidents list is by Created date in descending order (newest on the top).

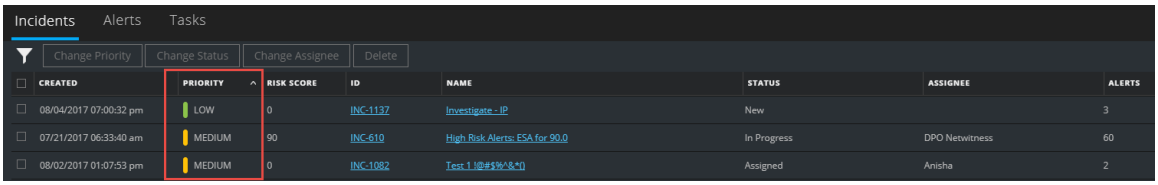


You change the sort order of the incidents list by clicking a column in the list.

For example, to prioritize the incidents, you can sort your view by the Priority column. To do this, hover over the Priority column and click the down arrow ▼. The incident list sorts by Priority in descending order (highest priority on top), as shown in the following figure.



To sort by Priority in ascending order (lowest priority on top), click the up arrow ▲. as shown in the following figure.

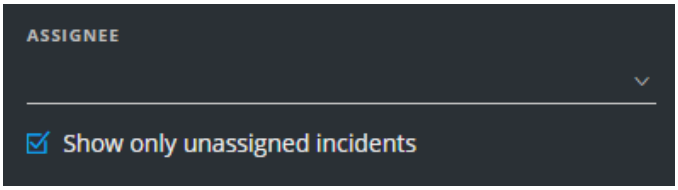


View Unassigned Incidents

This option is available in version 11.1 and later.

You can view unassigned incidents using the Filter.

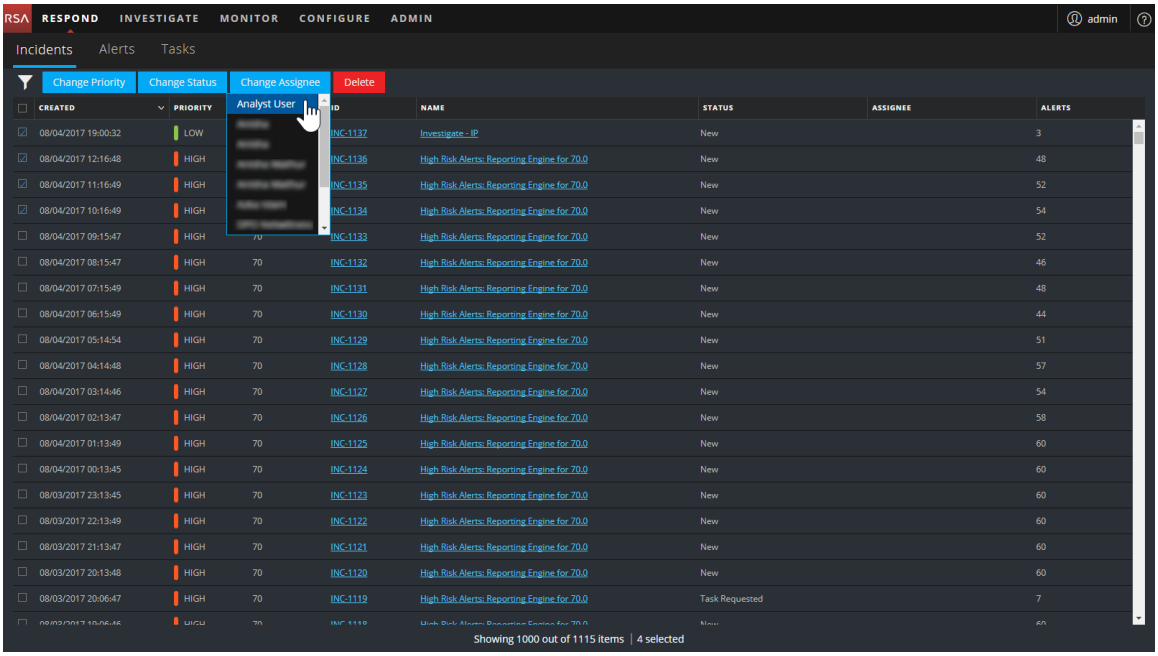
1. If you cannot see the Filter panel, in the Incident List view toolbar, click .
2. In the Filters panel, under ASSIGNEE, select **Show only unassigned incidents**.



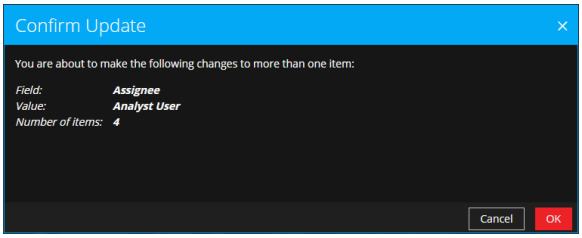
The incidents list will be filtered to show unassigned incidents.

Assign Incidents to Myself

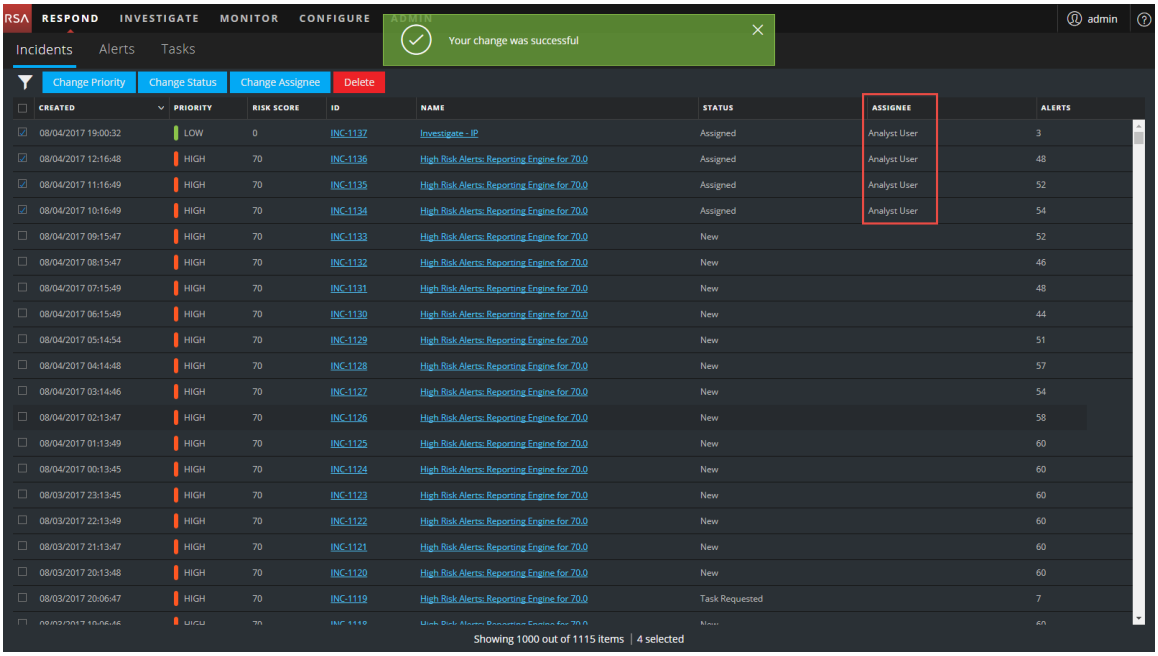
1. In the Incident List view, select one or more incidents that you want to assign to yourself.
2. Click **Change Assignee** and select your username from the drop-down list.



3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.

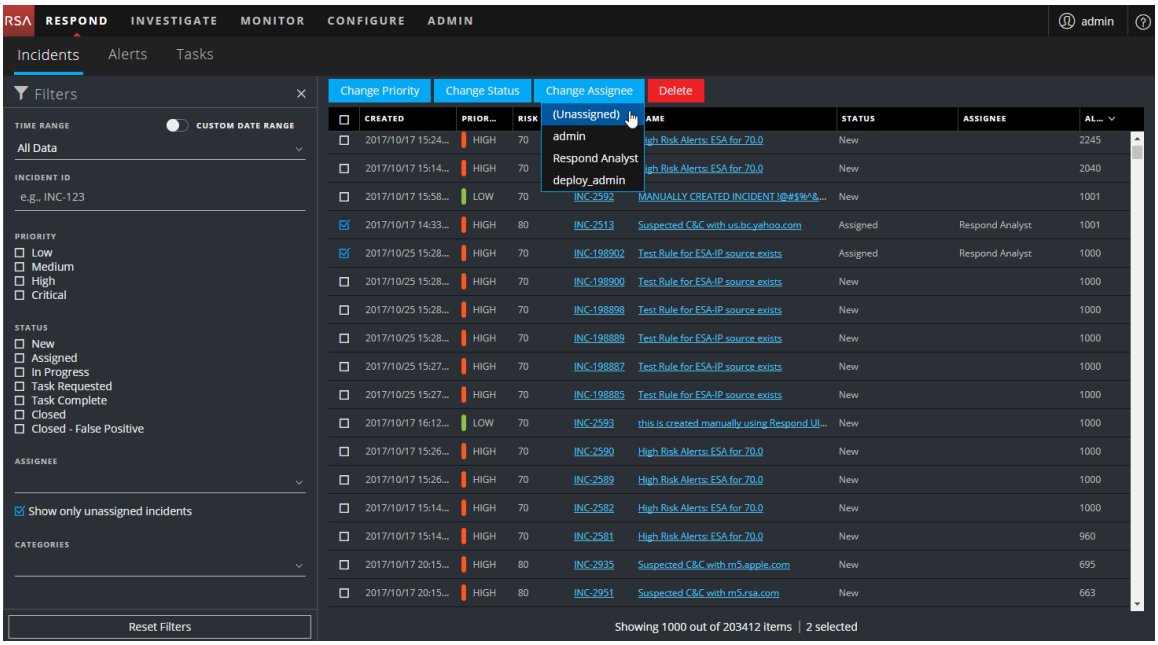


You will see a successful change notification.

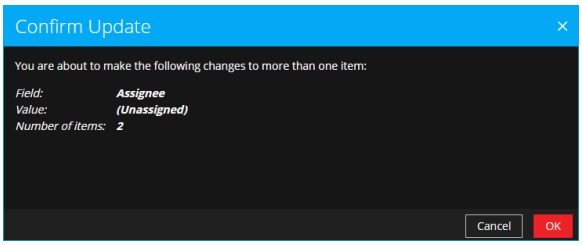


Unassign an Incident

1. In the Incident List view, select one or more incidents that you want to unassign.
2. Click **Change Assignee** and select **(Unassigned)** from the drop-down list.



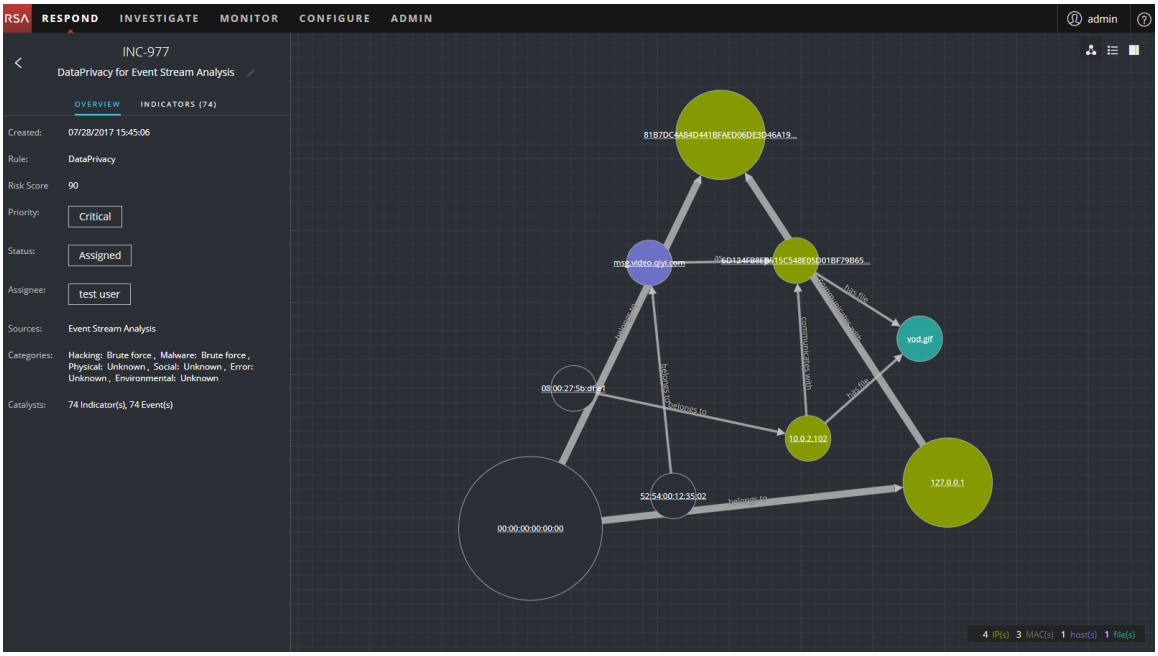
3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.



4. Verify that the Status is still correct and make changes as required. To change the status, select one or more incidents, click **Change Status**, and select a new status.
   For example, if you assigned an incident to yourself by mistake, you can unassign the incident and then change the Status from Assigned back to New.

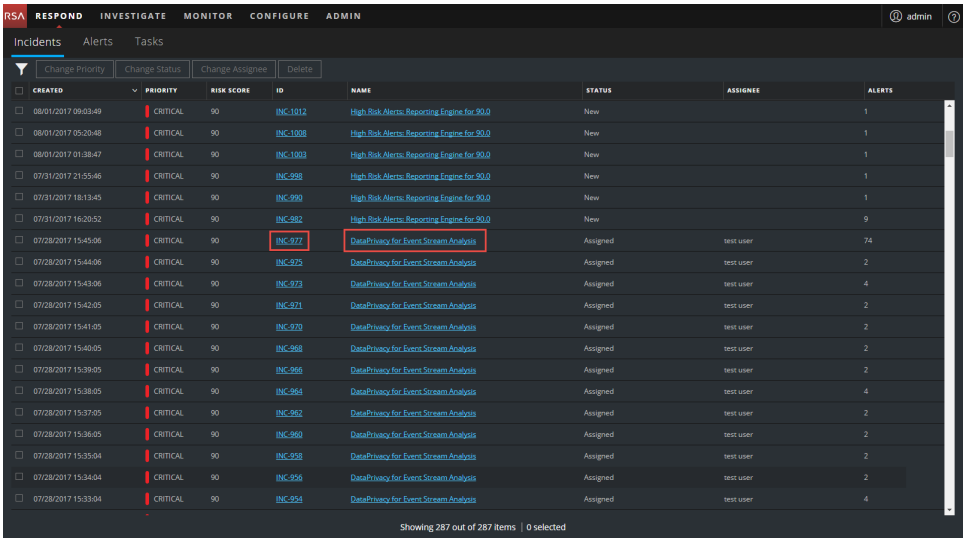
Determine which Incidents Require Action

Once you get the general information about the incident from the Incident List view, you can go to the Incident Details view for more information to determine the action required.

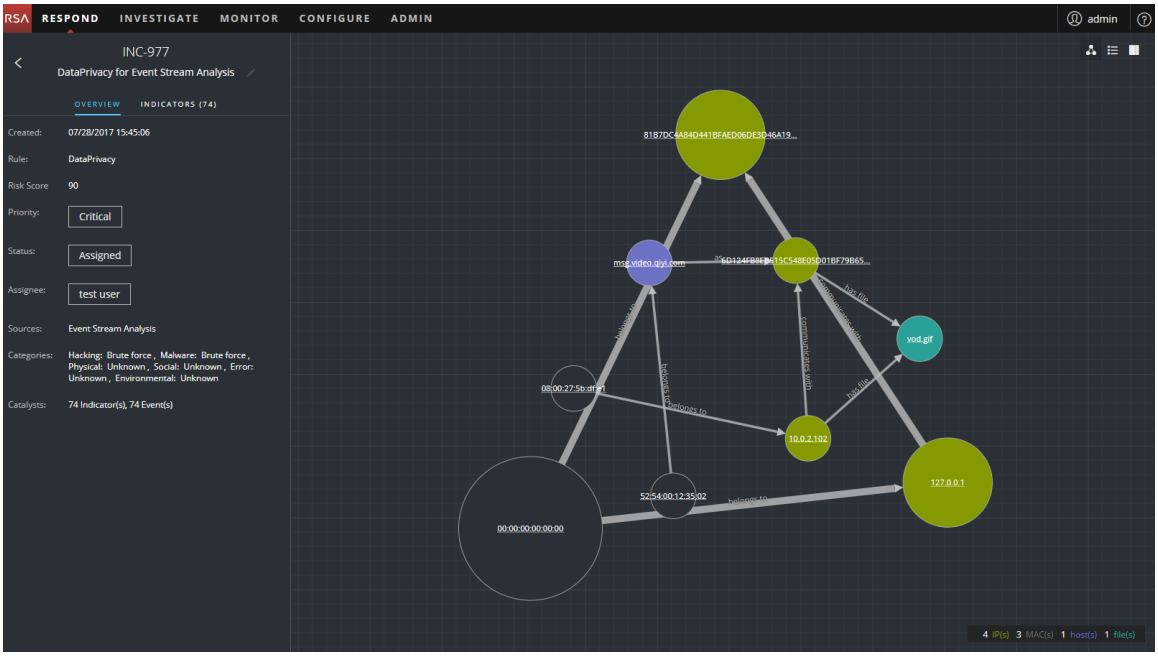


View Incident Details

To view details for an incident, in the Incidents List view, choose an incident to view and then click the link in the ID or NAME column for that incident.



The Incident Details view for the selected incident appears with the Overview panel and Nodal Graph in view.



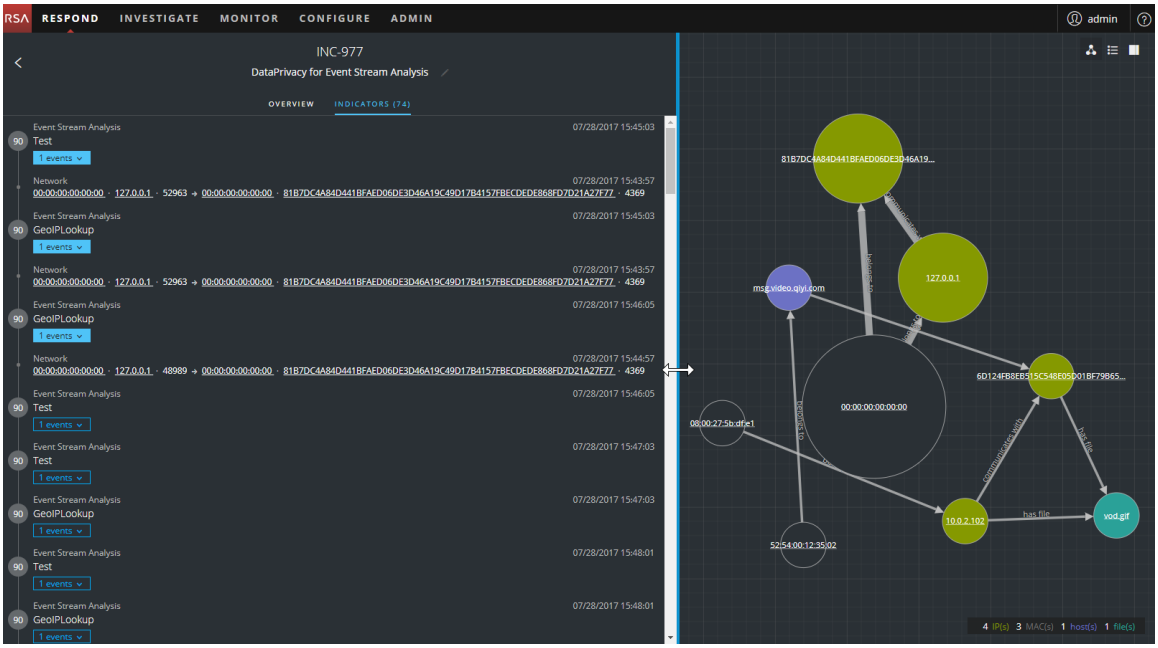
The Incident Details view has the following panels:

- **OVERVIEW**: The incident overview panel contains high-level summary information about the incident, such as the score, priority, alerts, and status. You have the option to change the incident Priority, Status, and Assignee.
- **INDICATORS**: The Indicators panel contains a chronological listing of indicators. ***Indicators*** are alerts, such as an ESA alert or a NetWitness Endpoint alert. This listing helps you to connect indicators and notable data. For example, an IP address connected to a command and communication ESA alert might also have triggered a NetWitness Endpoint alert or other suspicious activities.
- **Nodal Graph**: The nodal graph is an interactive graph that shows the relationship between the entities involved in the incident. An *Entity* is a specified piece of meta, such as IP address, MAC address, user, host, domain, file name, or file hash.
- **Events**: The Events panel, also known as the Events table, lists the events associated with the incident. It also shows event source and destination information along with additional information depending on the event type. You can click an event in the list to view the detailed data for that event.
- **JOURNAL**: The Journal panel enables you to access the Journal for the selected incident, which allows you to communicate and collaborate with other analysts. You can post notes to

a journal, add Investigation Milestone tags (Reconnassance, Delivery, Exploitation, Installation, Command and control), and view the history of activity on your incident.

- **TASKS**: The Tasks panel shows all of the tasks that have been created for the incident. You can also create additional tasks from here.
- **RELATED**: The Related Indicators panel enables you to search the NetWitness Suite alerts database to find alerts that are related to this incident. You can also add related alerts that you find to the incident.

To view more information in the left-side panel without scrolling, you can hover over the right edge and drag the line to resize the panel as shown in the following figure:

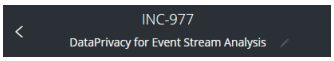


View Basic Summary Information about the Incident

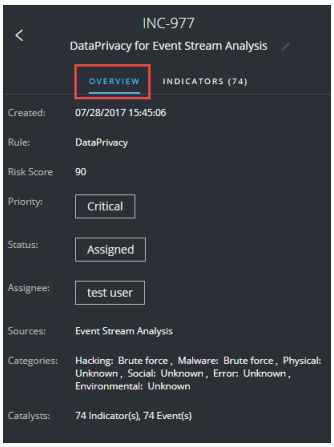
You can view basic summary information about an incident in the Overview panel.

Above the Overview panel, you can see the following information:

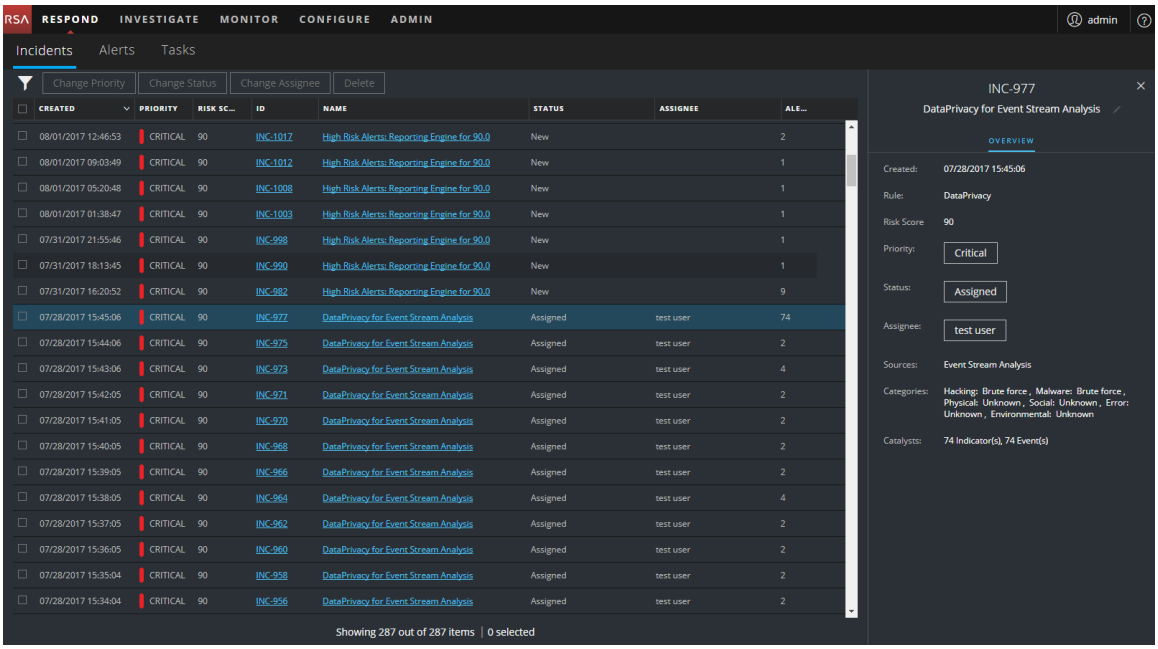
- **Incident ID**: This is an automatically created unique ID assigned to the incident.
- **Name**: The incident name is derived from the rule used to trigger the incident.



To view the Overview panel from the Incident Details view, select **OVERVIEW** in the left panel.



To view the Overview panel from the Incidents List view, click an incident in the list. The Overview panel appears on the right.



The Overview panel contains basic summary information about the selected incident:

- **Created**: Shows the creation date and time of the incident.
- **Rule / By**: Shows the name of the rule that created the incident or the name of the person who created the incident.
- **Risk Score**: Indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
- **Priority**: Shows the incident priority. Priority can be Critical, High, Medium or Low.

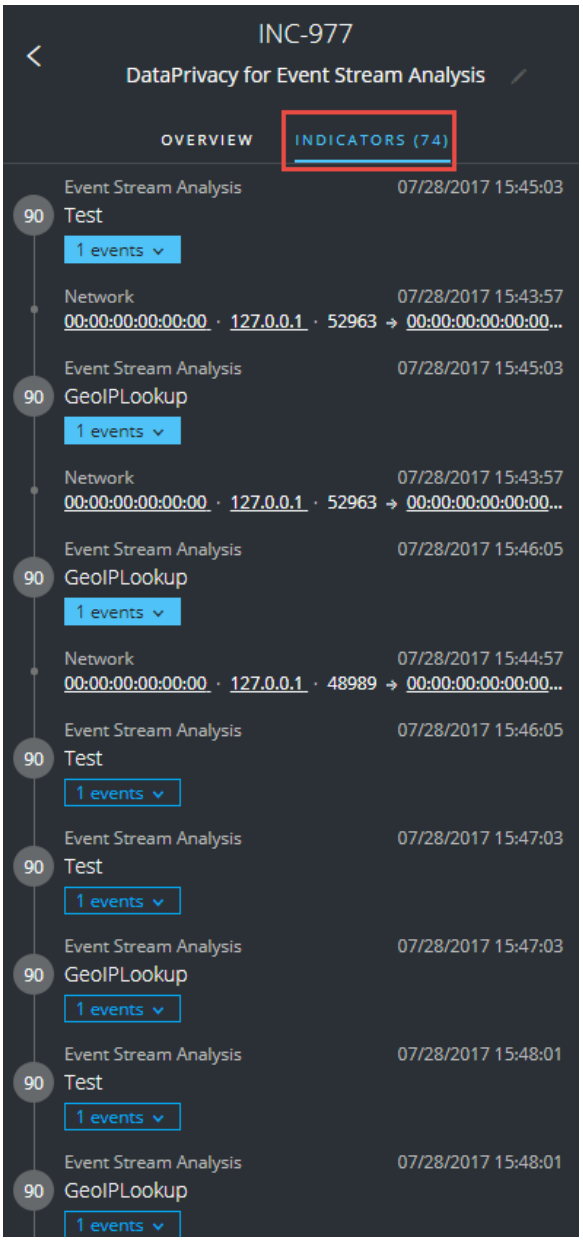
- **Status**: Shows the incident status. The status can be New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive. After you create a task, the status changes to Task Requested.
- **Assignee**: Shows the team member currently assigned to the incident.
- **Sources**: Indicates the data sources used to locate the suspicious activity.
- **Categories**: Shows the categories of the incident events.
- **Catalysts**: Shows the count of indicators that gave rise to the incident.

View the Indicators and Enrichments

Note: *Indicators* are alerts, such as an ESA alert or a NetWitness Endpoint alert.

You can find indicators, events, and enrichments on the Indicators panel. The Indicators panel is a Chronological listing of indicators that helps you to find enrichments and events related to the triggering indicator. For example, an indicator might be a Command and Control alert, a NetWitness Endpoint alert, a Suspicious Domain (C2) alert, or an alert from an Event Stream Analysis (ESA) rule. The Indicators panel helps you to aggregate and order these indicators (alerts) from different systems so that you can see how they are related and also help you develop a timeline of a given attack.

To view the Indicators panel, in the left panel of the Incident Details view, select **INDICATORS**.



Indicators are alerts, such as an ESA alert or a NetWitness Endpoint alert. This listing helps you to connect indicators and notable data. For example, indicators can show the data found by your rules. In the Indicators panel, the risk score for an indicator is shown within a solid-colored circle.

Data source information is shown below the names of the indicators. You can also see the creation date and time of the indicator and the number of events in the indicator. When data is available, you can see the number of enrichments. You can click the event and enrichment buttons to view the details.

View and Study the Events

You can view and study the events associated with the incident from the Events panel. It shows information about the events, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

There are two types of events:

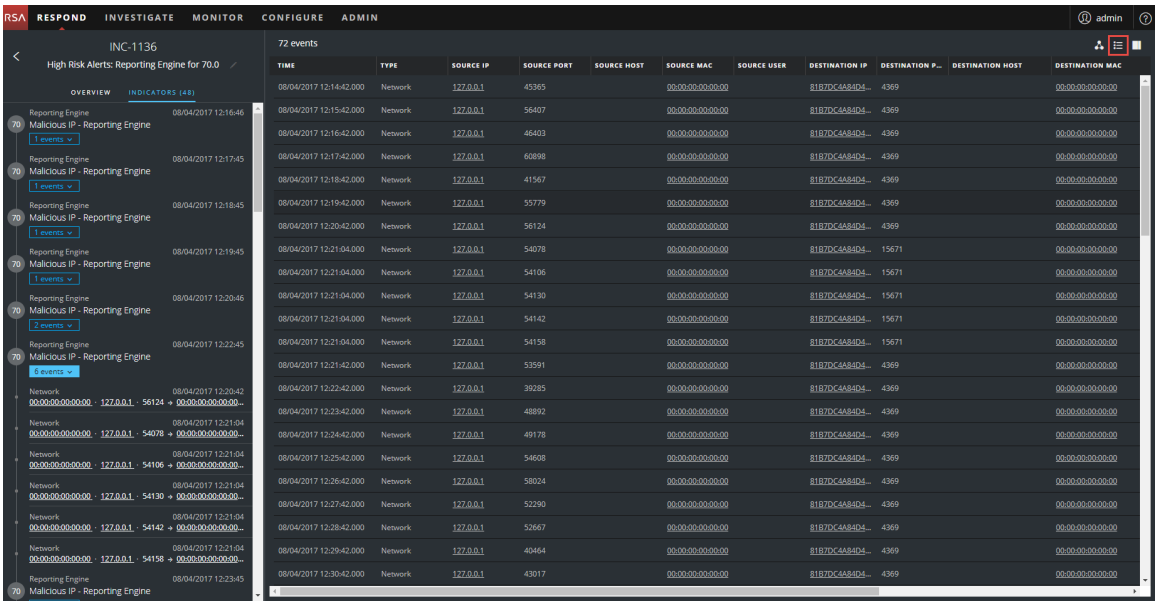
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

Some events will only have a Detector. For example, NetWitness Endpoint finds malware on your machine. Other events will have a Source and Destination. For example, packet data shows communication between your machine and a Command and Control (C2) domain.

You can drill further into an event to get detailed data about the event.

To view and study the events:

1. To view the Events panel, in the Incident Details view toolbar, click .



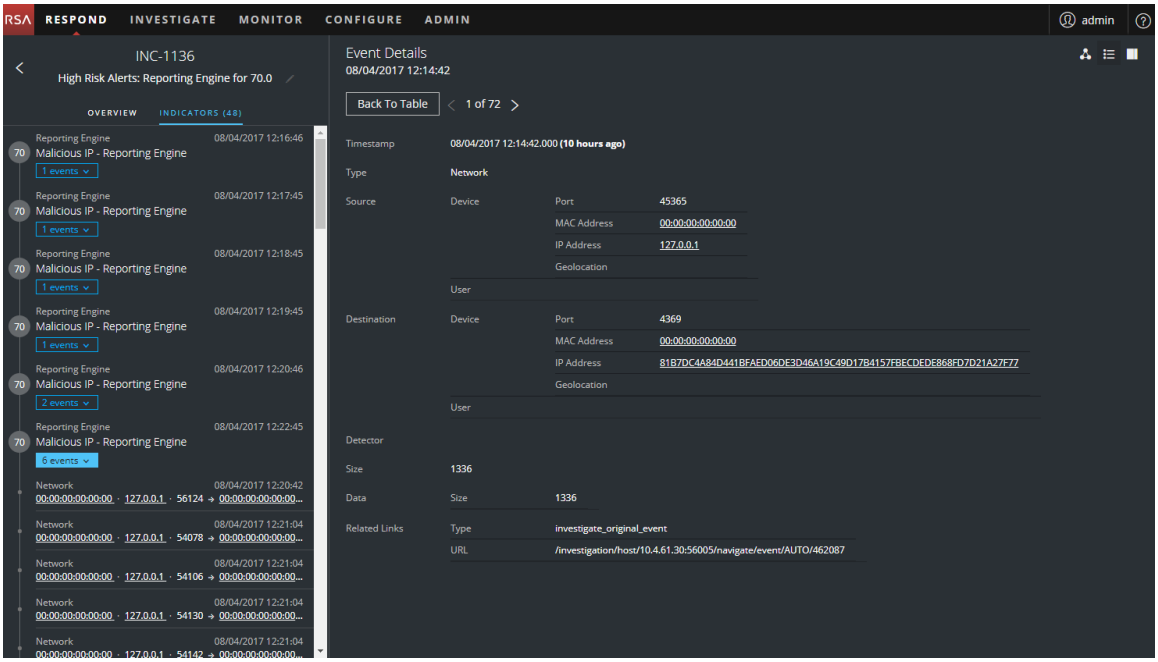
The Events panel shows a list of information about each event as shown in the following table.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
SOURCE PORT	Shows the source port of the transaction. The source and destination ports can be on the same IP address.
SOURCE HOST	Shows the source host where the event took place.
SOURCE MAC	Shows the MAC address of the source machine.
SOURCE USER	Shows the user of the source machine.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DESTINATION PORT	Shows the destination port of the transaction. The source and destination ports can be on the same IP address.
DESTINATION HOST	Shows the destination host where the event took place.
DESTINATION MAC	Shows the MAC address of the destination machine.
DESTINATION USER	Shows the user of the destination machine.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

If there is only one event in the list, you will see the event details for that event instead of a list.

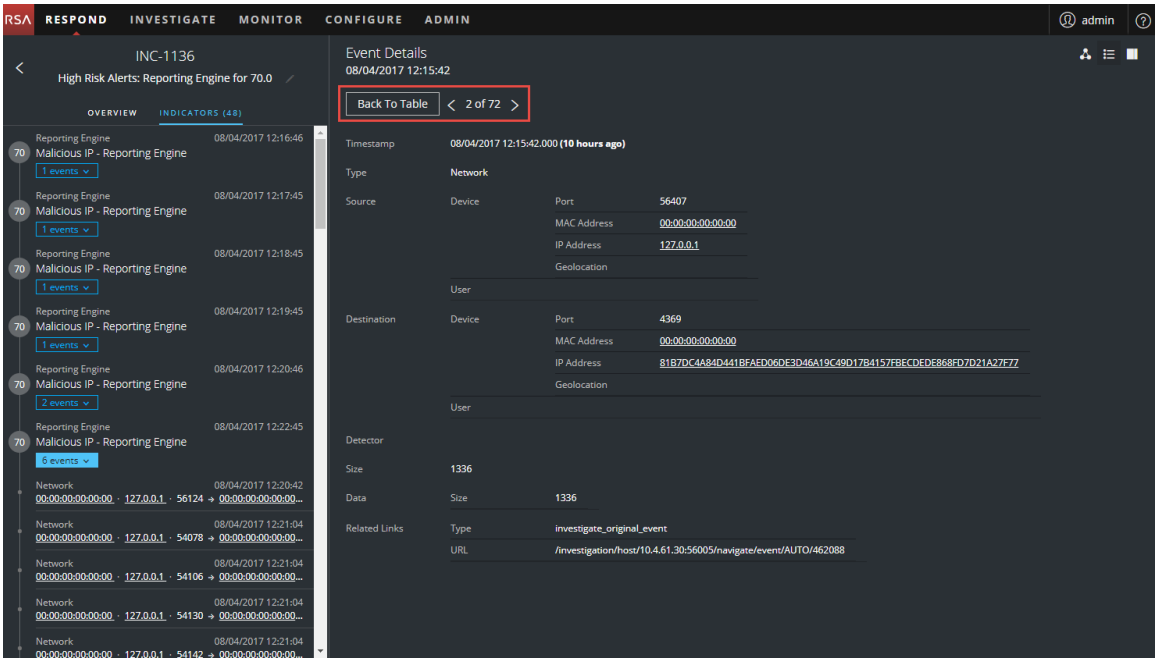
2. Click an event in the Events list to view the Event details.

   This example shows the event details for the first event in the list.



3. Use the Event Details navigation to view details for additional events.

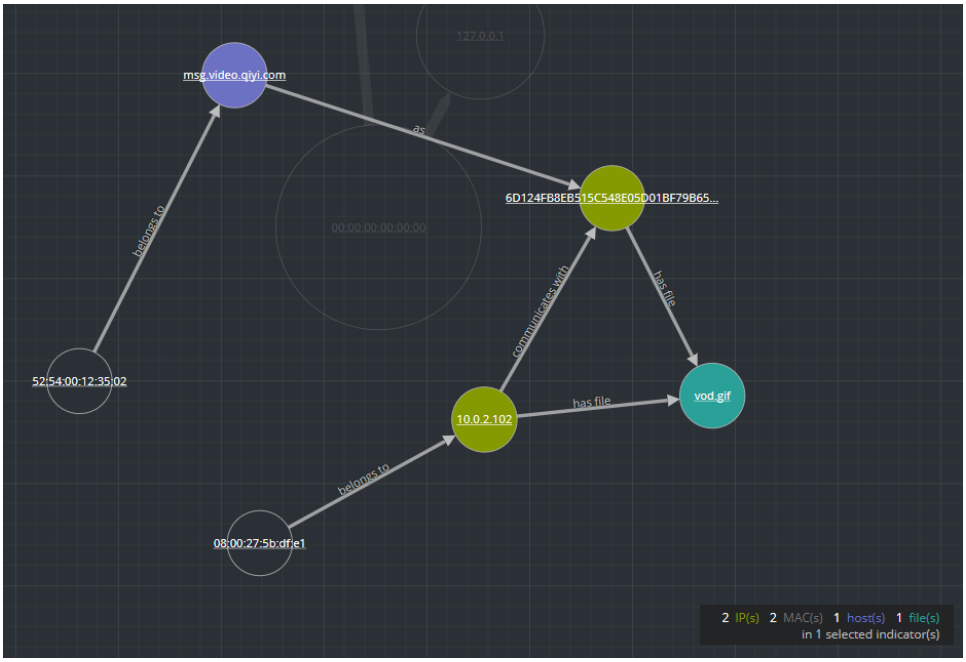
   This example shows the second event in the list.



View and Study the Entities Involved in the Events

An *Entity* is either an IP address, MAC address, user, host, domain, file name, or file hash. The nodal graph is an interactive graph that you can move around to get a better understanding of how the entities involved in the events relate to each other. The nodal graphs look different depending on the type of event, the number of machines involved, whether the machines are associated with users, and if there are files associated with the event.

The following figure shows an example nodal graph with six nodes.



If you look closely at the nodal graph, you can see circles that represent nodes. A nodal graph can contain one or more of the following types of nodes:

- **IP address** (If the event is a detected anomaly, you can see a Detector IP. If the event is a transaction, you can see a Destination IP and a Source IP.)
- **MAC address** (You may see a MAC address for each type of IP address.)
- **User** (If the machine is associated with a user, you can see a user node.)
- **Host**
- **Domain**
- **Filename** (If the event involves files, you can see a filename.)
- **File Hash** (If the event involves files, you may see a file hash.)

The legend at the bottom of the nodal graph shows the number of nodes of each type and the color coding of the nodes.

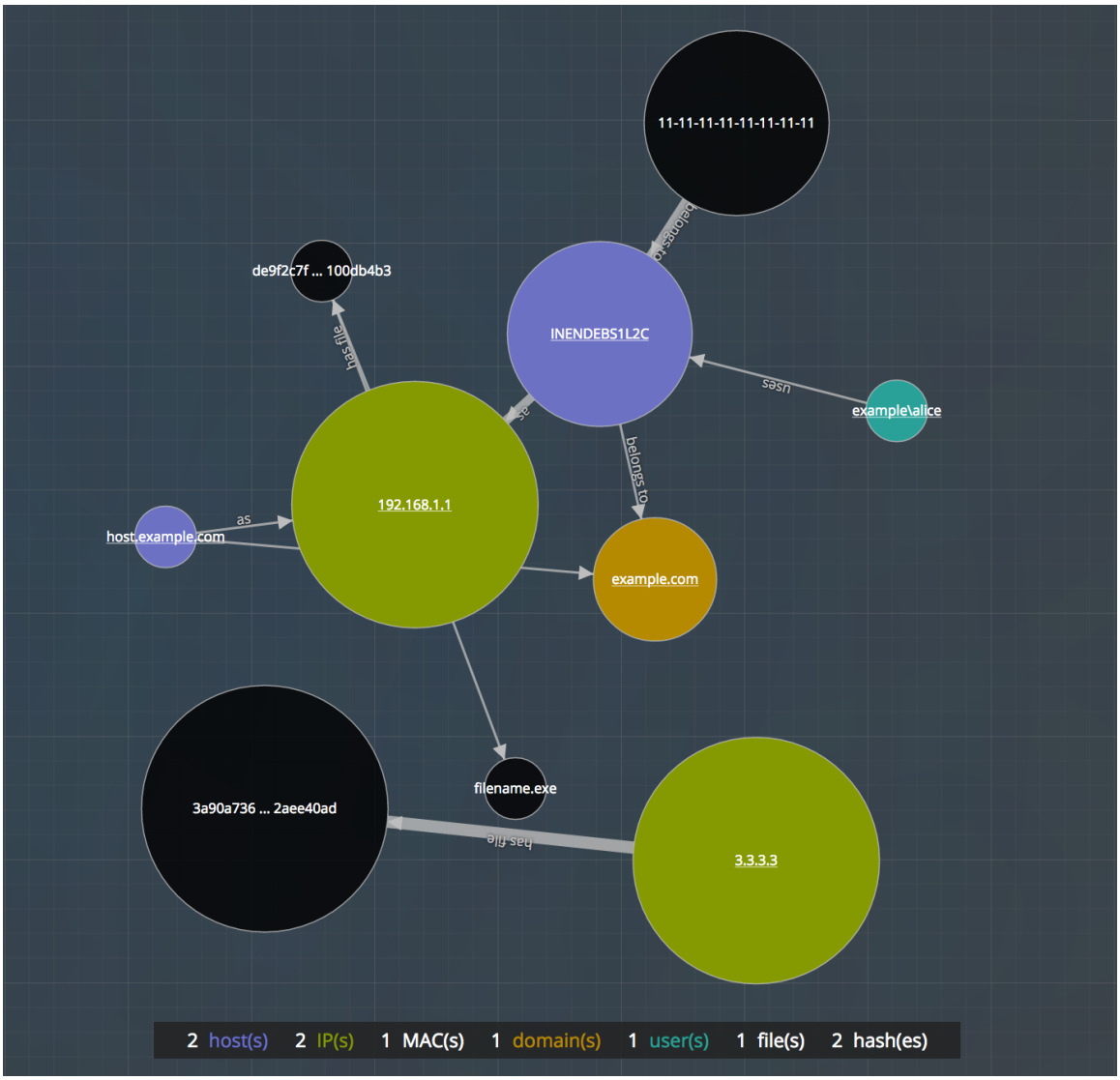
You can click any node and drag it to reposition it.

The arrows between the nodes provide additional information about the entity relationships:

- **Communicates with**: An arrow between a Source machine node (IP address or MAC address) and a Destination machine node labeled with "communicates with" shows the direction of the communication.
- **As**: An arrow between nodes labeled with "as" provides additional information about the IP address that the arrow points to. In the above example, there is an arrow from the host node circle that points to a hashed IP address node that is labeled with "as". This indicates that the name on the host node circle is the hostname of that IP address and is not a different entity.
- **Has file**: An Arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has" indicates that the IP address has that file.
- **Uses**: An arrow between a User node and a machine node (IP address, MAC address, or Host) labeled with "uses" shows the machine that the user was using during the event.
- **Is named**: An arrow from a File Hash node to a File Name node labeled with "is named" indicates that the file hash corresponds to a file with that name.
- **Belongs to**: An arrow between two nodes labeled with "belongs to" indicates that they pertain to the same node. For example, an arrow between a MAC address and a Host labeled with "belongs to" indicates that it is the MAC address for the host.

Larger line size arrows indicate more communication between the nodes. Larger nodes (circles) indicate more activity than smaller nodes. The larger nodes are the most common entities mentioned in the events.

The following nodal graph example has ten nodes.

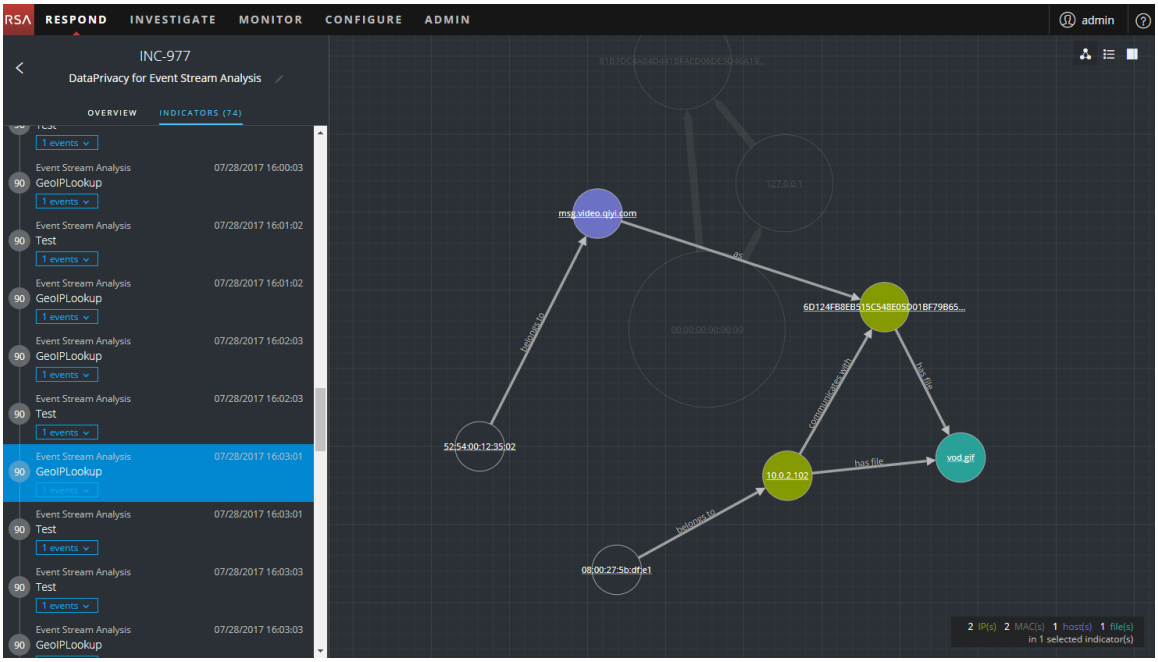


In this example, notice that there are two IP nodes that have a lot of activity. They both have files, but they do not communicate with each other. The IP address at the top (192.168.1.1) represents one machine with two hostnames (host.example.com and INENDEBS1L2C) in the example.com domain. The MAC address of the machine is 11-11-11-11-11-11-11-11-11-11and Alice uses it.

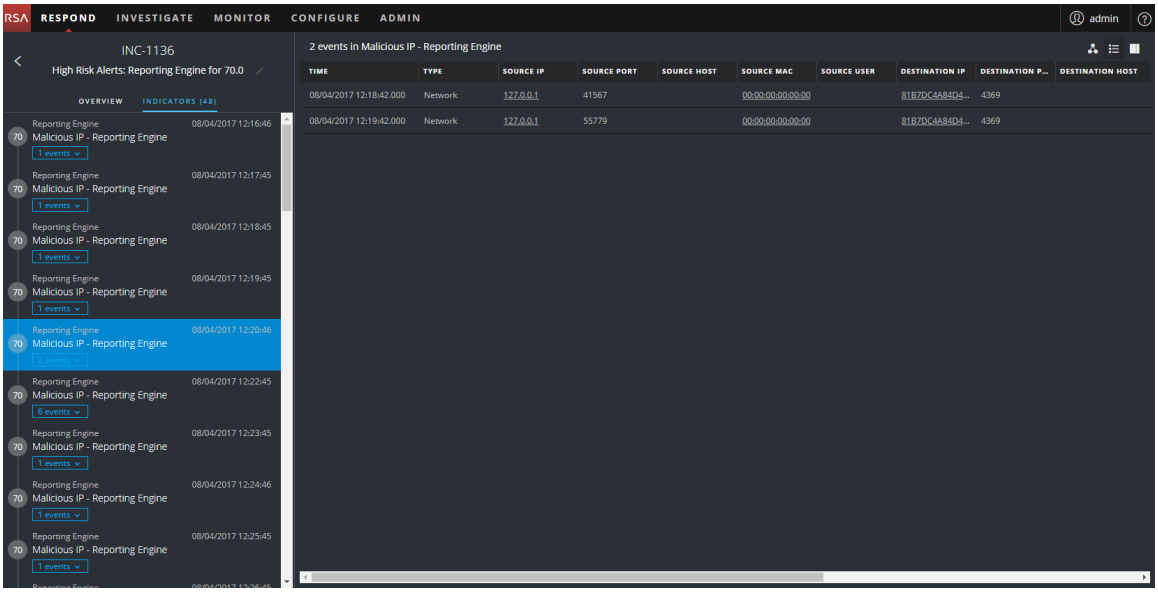
Filter the Data in the Incident Details View

You can click indicators in the Indicators panel to filter what you can see in the nodal graph and the Events list.

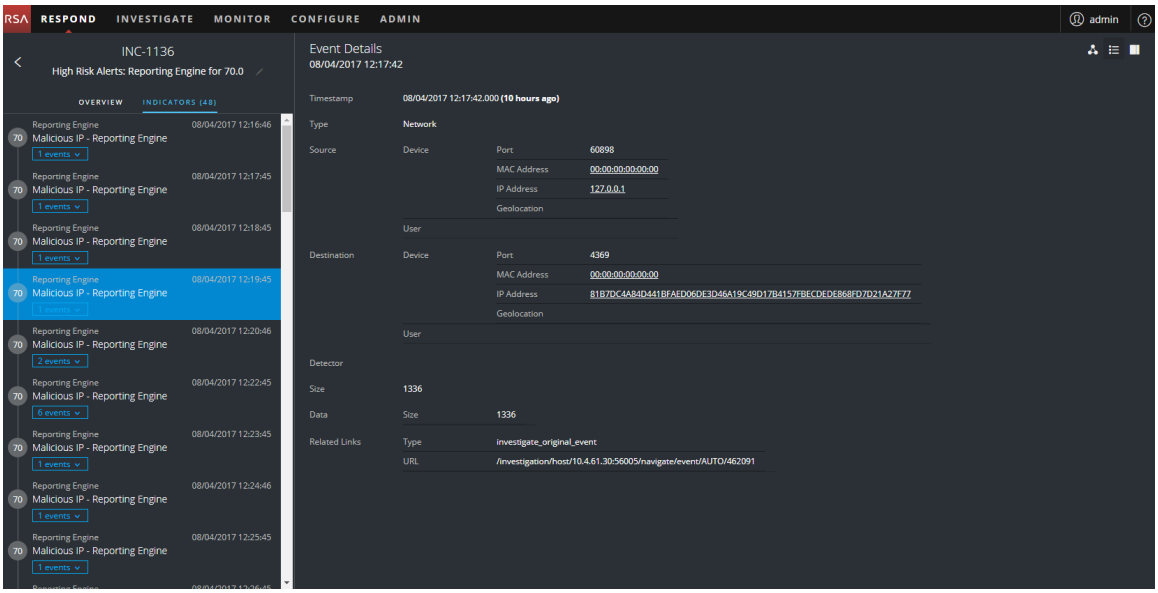
If you select an indicator to filter the nodal graph, data that is not part of your selection is dimmed, but it is still in view as shown in the following figure.



If you select an indicator to filter the events list, only the events for that indicator are shown in the list. The following figure shows an indicator selected that contains two events. The filtered Events list shows those two events.



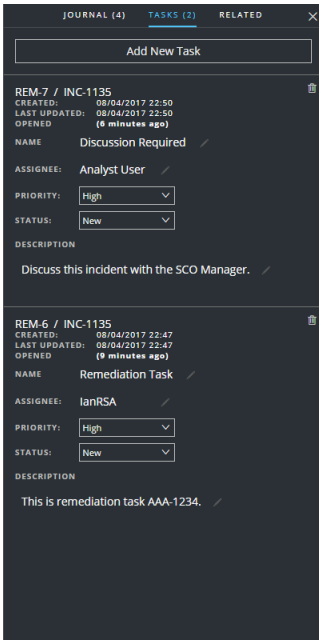
If you select an indicator to filter the events list and there is only one event for that indicator, you can see the event details for that event as shown in the following figure.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
INC-1136
High Risk Alerts: Reporting Engine for 70.0
OVERVIEW
INDICATORS (48)
Reporting Engine
Malicious IP - Reporting Engine
08/04/2017 12:16:46
1 events
08/04/2017 12:17:45
08/04/2017 12:18:45
08/04/2017 12:19:45
08/04/2017 12:20:46
2 events
08/04/2017 12:22:45
6 events
08/04/2017 12:23:45
08/04/2017 12:24:46
08/04/2017 12:25:45
Event Details
08/04/2017 12:17:42
Timestamp
08/04/2017 12:17:42.000 (10 hours ago)
Type
Network
Source
Device
Port
60898
MAC Address
00:00:00:00:00:00
IP Address
127.0.0.1
Geolocation
User
Destination
Device
Port
4369
MAC Address
00:00:00:00:00:00
IP Address
81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBECDEDE868FD7D21A27F77
Geolocation
User
Detector
Size
1336
Data
Size
1336
Related Links
Type
investigate_original_event
URL
/investigation/host/10.4.61.30:56005/navigate/event/AUTO/462091

View the Tasks associated with an Incident

Threat responders and other analysts can create tasks for an incident and track those tasks to completion. This can be very helpful, for example, when you require actions on incidents from teams outside of your security operations. You can view the tasks associated with an incident in the Incident Details view.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.
2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .
   The Journal panel opens.
4. Click the **TASKS** tab.
   The Tasks panel shows all of the tasks for the incident.



For more information about tasks, see Tasks List View, View All Incident Tasks, and Create a Task.

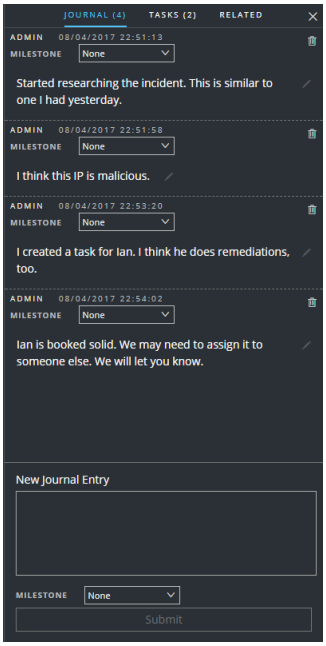
View Incident Notes

The incident Journal enables you to view the history of activity on your incident. You can view journal entries from other analysts and also communicate and collaborate with them.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.

2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .

   The Journal panel shows all of the journal entries for the incident.



Find Related Indicators

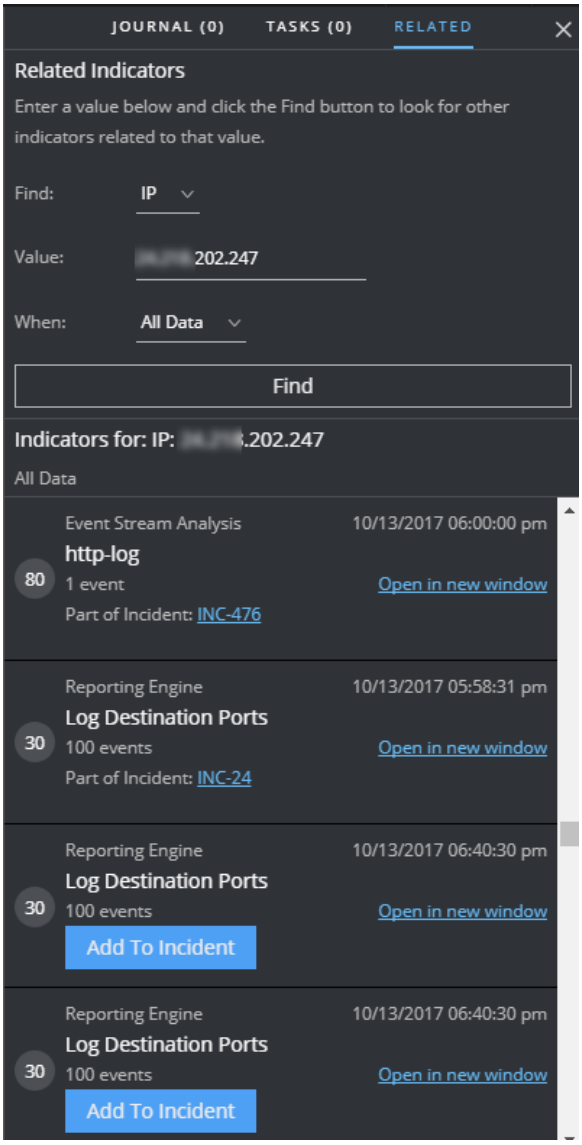
Related Indicators are alerts that were not originally part of the selected incident, but they are related in some way to the incident. The relationship may or may not be obvious. For example, related indicators can involve one or more entities from the incident, but they can also be related due to some intelligence outside of NetWitness Suite.

In the Incident Details view Related panel, you can search for an entity (such as IP, MAC, Host, Domain, User, Filename, or Hash) in other alerts outside of the current incident.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.
2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .

   The Journal panel opens on the right.

4. Click the **RELATED** tab.



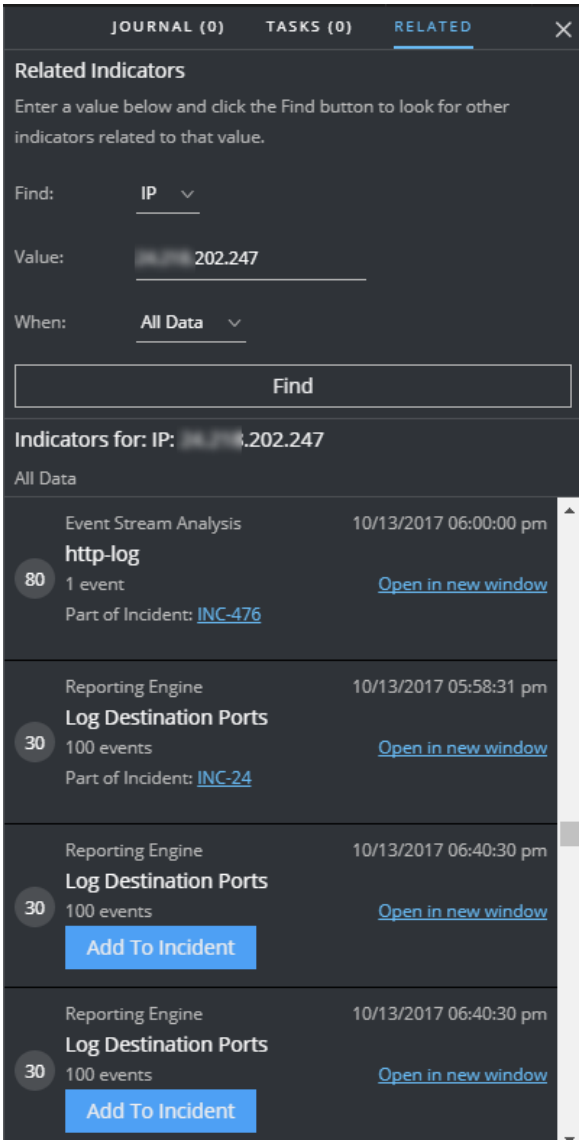
5. Click **Find**.

   A list of related indicators (alerts) appear below the **Find** button in the **Indicators for** section. If an alert is not part of another incident, you can click the **Add to Incident** button to add the related indicator (alert) to the current incident. See Add Related Indicators to the Incident below.

Add Related Indicators to the Incident

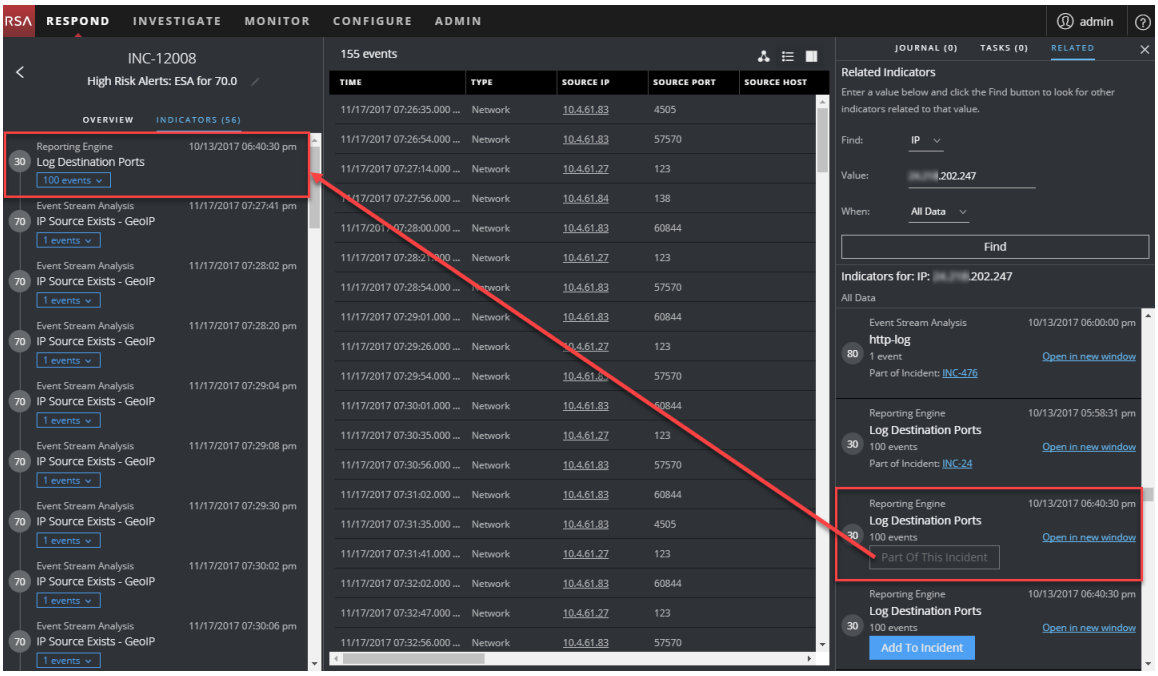
You can add related indicators (alerts) to the current incident from Related Indicators panel. An indicator that is already part of an incident cannot be part of another incident. In the search results, if an alert is not already part of an incident, it has an **Add to Incident** button.

1. In the **RELATED** (Related Indicators) panel, do a search to find related indicators. See Find Related Indicators above.



2. Review the alerts in the search results. The **Indicators for** section (below the Find button) lists the related indicators (alerts).

3. To inspect the details of an alert before adding it as a related indicator to the incident, you can click the **Open in New Window** link to view the alert details for that indicator.
4. For each alert that you want to add to the current incident as a related indicator, click the **Add to Incident** button.
   The selected related indicator adds to the Indicators panel on the left. The button in the Related Indicators panel on the right now shows **Part of This Incident**.



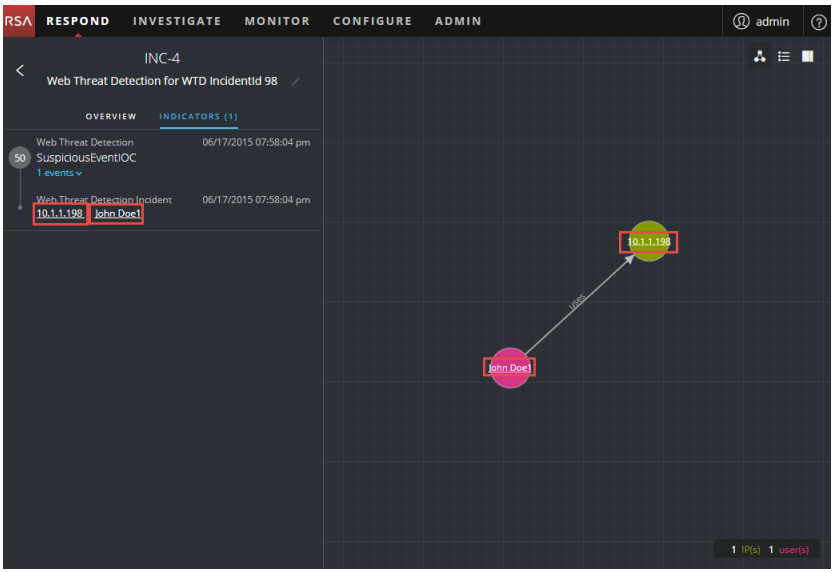
Investigate the Incident

To further investigate an incident within the Incident Details view, you can find links that take you to additional contextual information about the incident when it is available. This additional context can help you understand additional technical context and business context about a specific entity in the incident. It can also provide additional information that you may want to research to ensure that you understand the full scope of the incident.

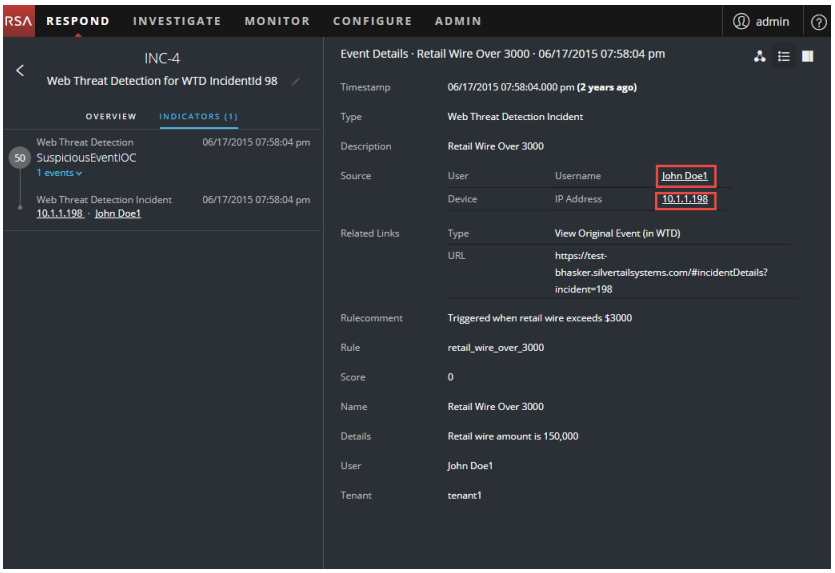
View Contextual Information

In the Indicators panel, Events List panel, Event Details panel, or the Nodal Graph, you can see underlined entities. If an entity is underlined, NetWitness Suite is populating information about that entity type in the Context Hub. There may be additional information available about that entity in the Context Hub.

The following figure shows underlined entities in the Indicators panel and the Nodal Graph.



The following figure shows underlined entities in the Event Details panel.



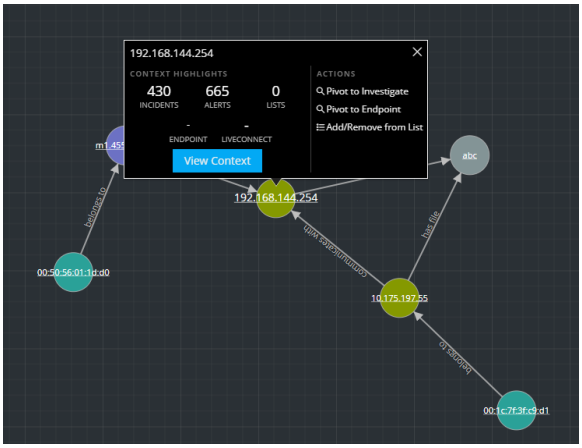
The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and Investigatie use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the **ADMIN > SYSTEM > Investigations > Context Lookup** tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, ip.address is a meta key and ip_address is not a meta key (it is a field in the MongoDB).

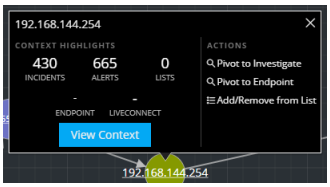
To view contextual information:

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over an underlined entity.

   A context tooltip appears with a quick summary of the type of context data that is available for the selected entity.



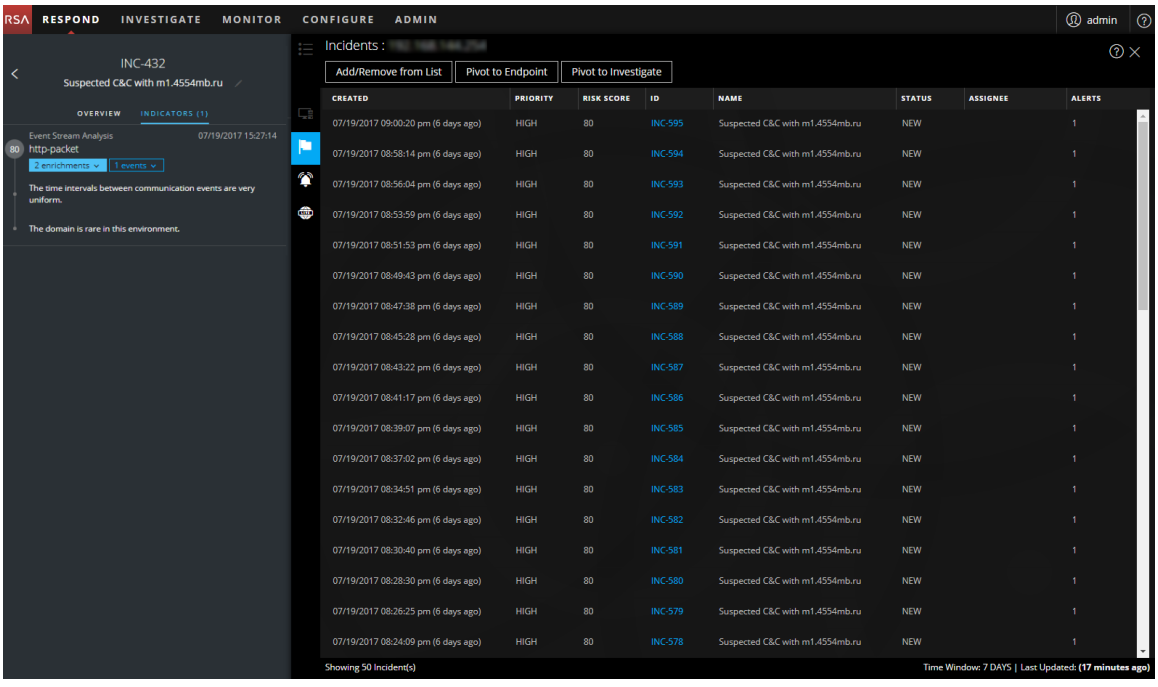
   The context tooltip has two sections: Context Highlights and Actions.



The information in the **Context Highlights** section helps you to determine the actions that you would like to take. It can show related data for Incidents, Alerts, Lists, Endpoint, and Live Connect. Depending on your data, you may be able to click these items for more information. The above example shows 430 related incidents, 665 alerts, 0 lists, and no information in NetWitness Endpoint or Live Connect that mentions the IP address entity, 192.168.144.254.

The **Actions** section lists the available actions. In the above example, the Pivot to Investigate, Pivot to Endpoint, and Add/Remove from List options are available. For more information, see Pivot to Investigate, Pivot to NetWitness Endpoint, and Add an Entity to a Whitelist.

2. To see more details about the selected entity, click the **View Context** button.
   The Context Lookup panel opens and shows all of the information related to the entity.
   The following example shows contextual information for a selected source IP address. It lists all of the incidents that mention the IP address.



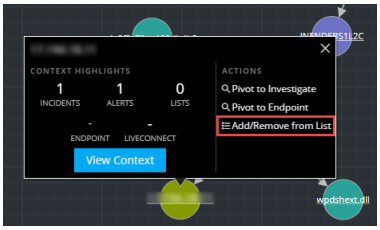
To understand the different views within the Context Hub Lookup panel, see Context Lookup Panel - Respond View .

Add an Entity to a Whitelist

You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

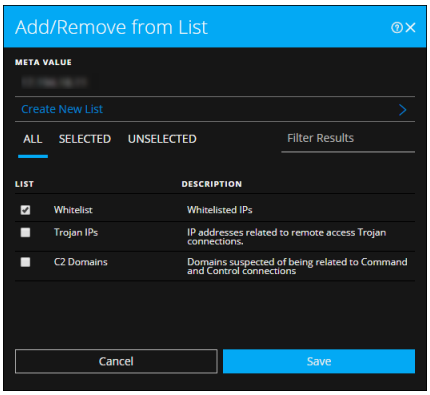
1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over the underlined entity that you would like to add to a Context Hub list.

   A context tooltip appears showing the available actions.



2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.

   The Add/Remove from List dialog shows the available lists.



3. Select one or more lists and click **Save**.

   The entity appears on the selected lists.

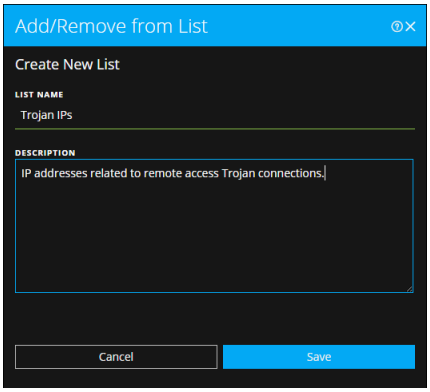
   Add/Remove from List Dialog provides additional information.

Create a List

You can create lists in Context Hub from the Respond view. In addition to using lists to whitelist and blacklist entities, you can use lists to monitor entities for abnormal behavior. For example, to improve the visibility of a suspicious IP address and Domain under investigation, you may want to include them in two separate lists. One list could be for domains suspected of being related to command and control connections, and another list could be for IP addresses related to remote access Trojan connections. You can then identify indicators of compromise using these lists.

To create a list in Context Hub:

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over the underlined entity that you would like to add to a Context Hub list.
   A context tooltip appears showing the available actions.
2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.
3. In the Add/Remove from List dialog, click **Create New List**.



4. Type a unique **List NAME** for the list. The list name is not case sensitive.
5. (Optional) Type a **DESCRIPTION** for the list.
   Analysts with the appropriate permissions can also export lists in CSV format to send to other analysts for further tracking and analysis. The *Context Hub Configuration Guide* provides additional information.

Pivot to NetWitness Endpoint

If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint**.
   The NetWitness Endpoint thick client application opens outside of your web browser.

For more information on the thick client, see the *NetWitness Endpoint User Guide*.

Pivot to Investigate

For a more thorough investigation of the incident, you can access the Investigate view.

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate**.
   The Investigate Navigate view opens, which enables you to perform a deeper dive investigation.

For more information, see the *NetWitness Investigate User Guide*.

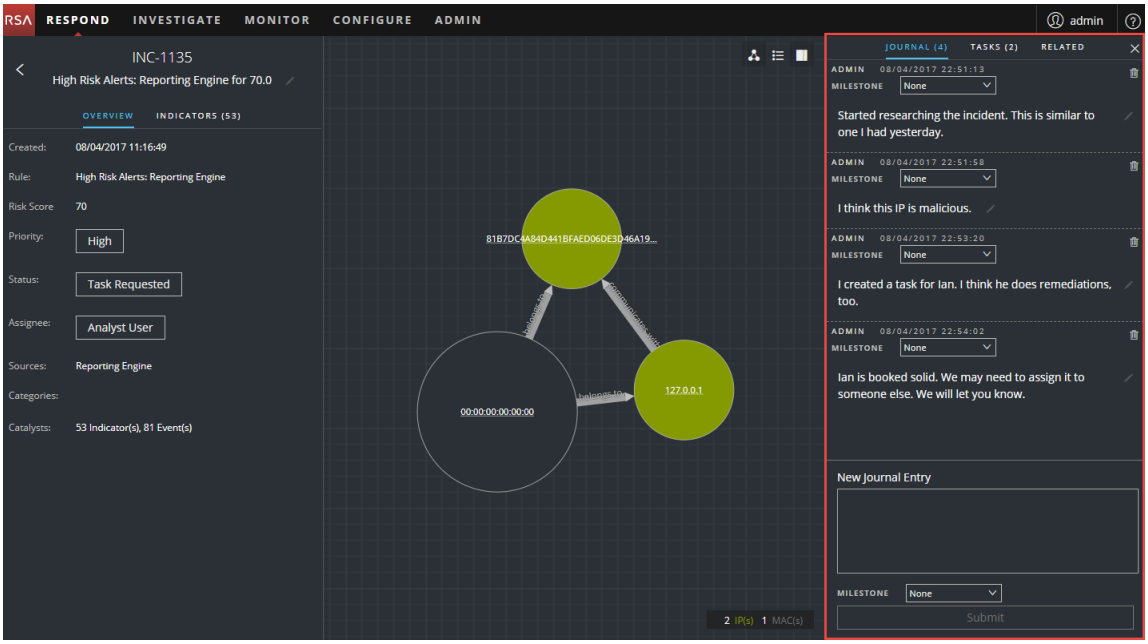
Document Steps Taken Outside of NetWitness

The journal shows notes added by analysts and it enables you to collaborate with your peers. You can post notes to a journal, add Investigation Milestone tags (Reconnaissance, Delivery, Exploitation, Installation, Command and control), and view the history of activity on your incident.

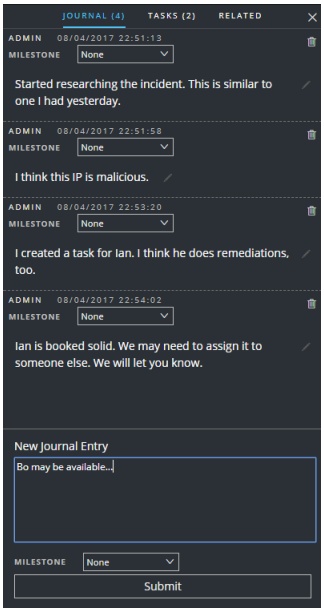
View the Journal Entries for an Incident

In the Incident Details view toolbar, click ■ .

The Journal appears on the right side of the Incident Details view.



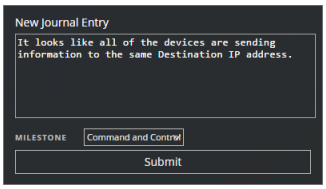
The Journal shows the history of activity on an incident. For each journal entry, you can see the author and time of the entry.



Add a Note

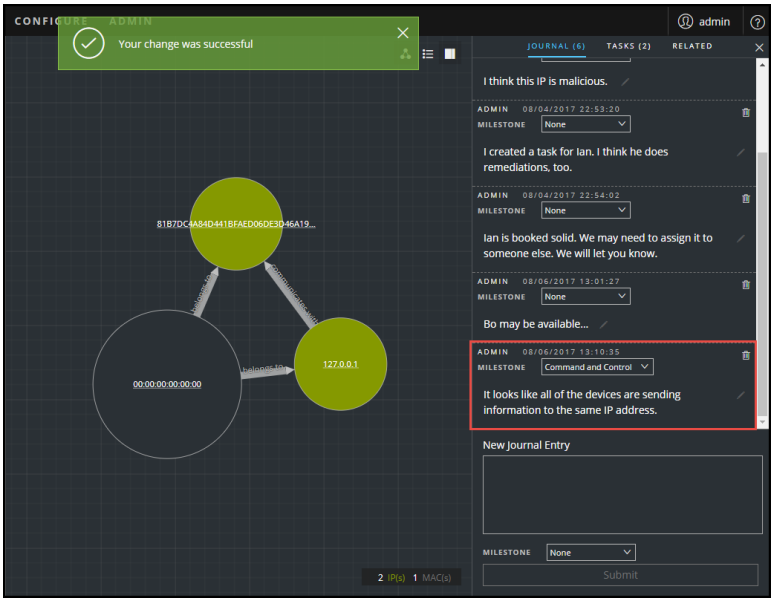
Typically, you will want to add a note to allow another analyst to understand the incident, or add a note for posterity so that your investigative steps are documented.

1. At the bottom of the Journal panel, type your note in the **New Journal Entry** box.



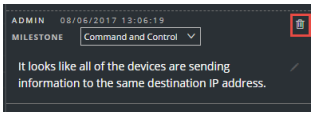
2. (Optional) Select an Investigation Milestone from the drop-down list (Reconnassance, Delivery, Exploitation, Installation, Command and Control, Action On Objective, Containment, Eradication, and Closure).

3. After you finish your note, click, **Submit**.
   Your new journal entry appears in the Journal.



Delete a Note

1. In the Journal panel, locate the journal entry that you would like to delete.
2. Click the trash can (delete) icon next to the journal entry.



3. In the confirmation dialog that appears, click **OK** to confirm that you want to delete the journal entry. This action cannot be reversed.

Escalate or Remediate the Incident

You may want to assign incidents to another Analyst or change the status and priority of an incident as you gather more information about it. This is useful if, for example, you upgrade the priority of an incident from **medium** to **high** after determining that the incident is major breach.

Update an Incident

You can update an incident from several places. You can change the priority, status, or assignee from the Incident List view and the Incident Details view. For example, if you are an Analyst, you may want to assign yourself a case from the Incident List view if you see that it is related to another case you are working on. If you are an SOC Manager or an Administrator, you may want to view unassigned incidents from the Incident List view and assign the incidents as they come in. SOC Managers and Administrators can do bulk updates of the priority, status, or assignee instead of updating them one incident at a time.

From the Details view, you might want to change the status to In Progress once you begin working on an incident, and then update it to Closed or Closed - False Positive after you resolve the issue. Or you might change the priority of the incident to Medium or High as you determine the details of the case.

Change Incident Status

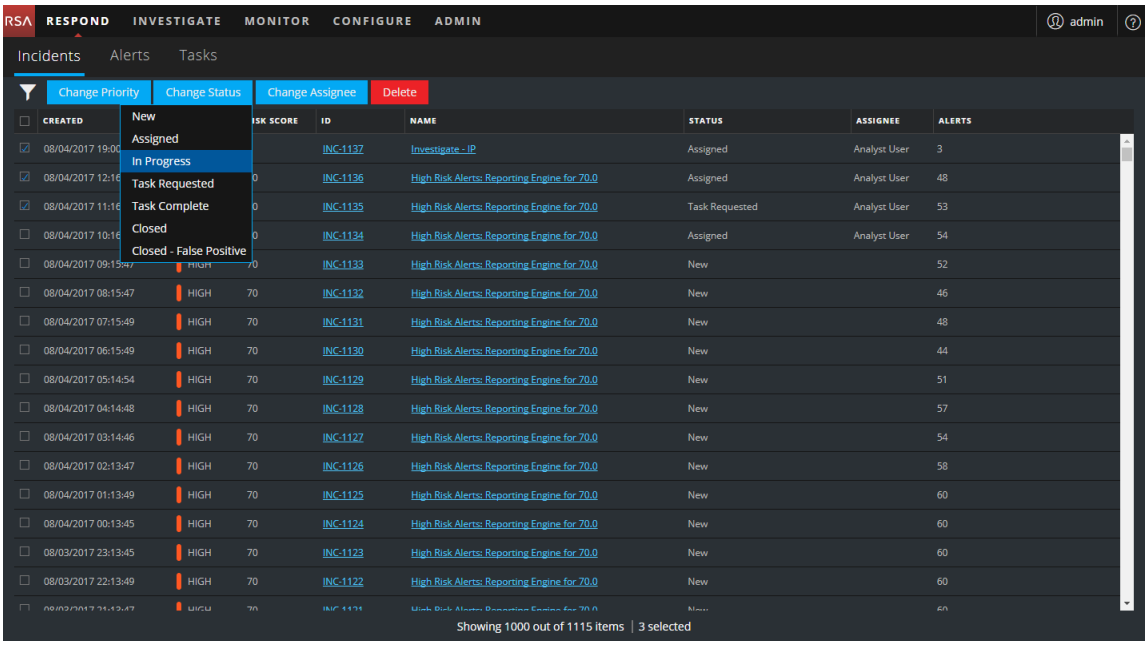
When an incident first appears in the incident list, it has an initial status of New. You can update the status as you complete your work on the incident. The following statuses are available:

- New
- Assigned
- In Progress
- Task Requested
- Task Complete
- Closed
- Closed - False Positive

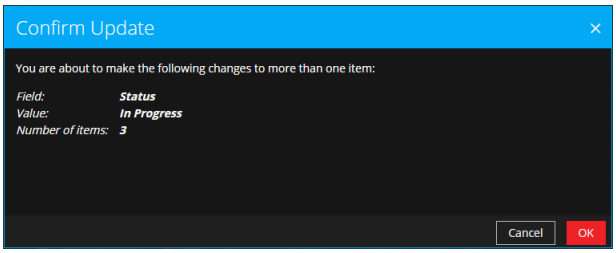
To update the status of multiple incidents:

1. In the Incidents List view, select one or more incidents that you would like to change. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears incidents list footer.

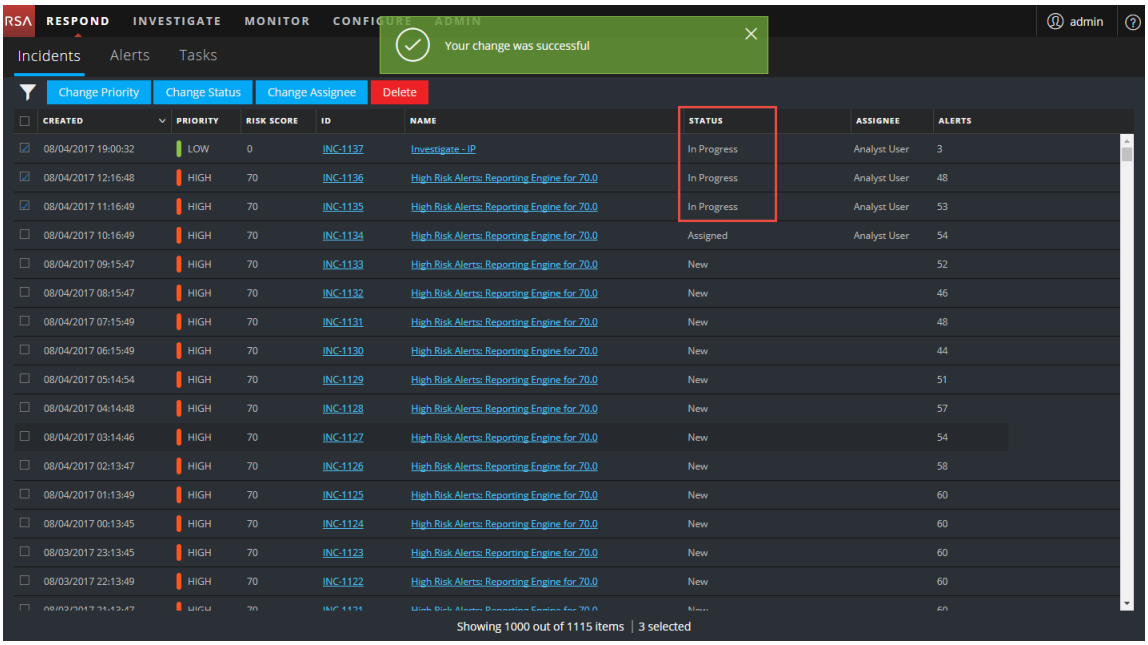
2. Click **Change Status** and select a status from the drop-down list. In this example, the current status is Assigned, but the Analyst would like to change it to In Progress for the selected incidents.



3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.

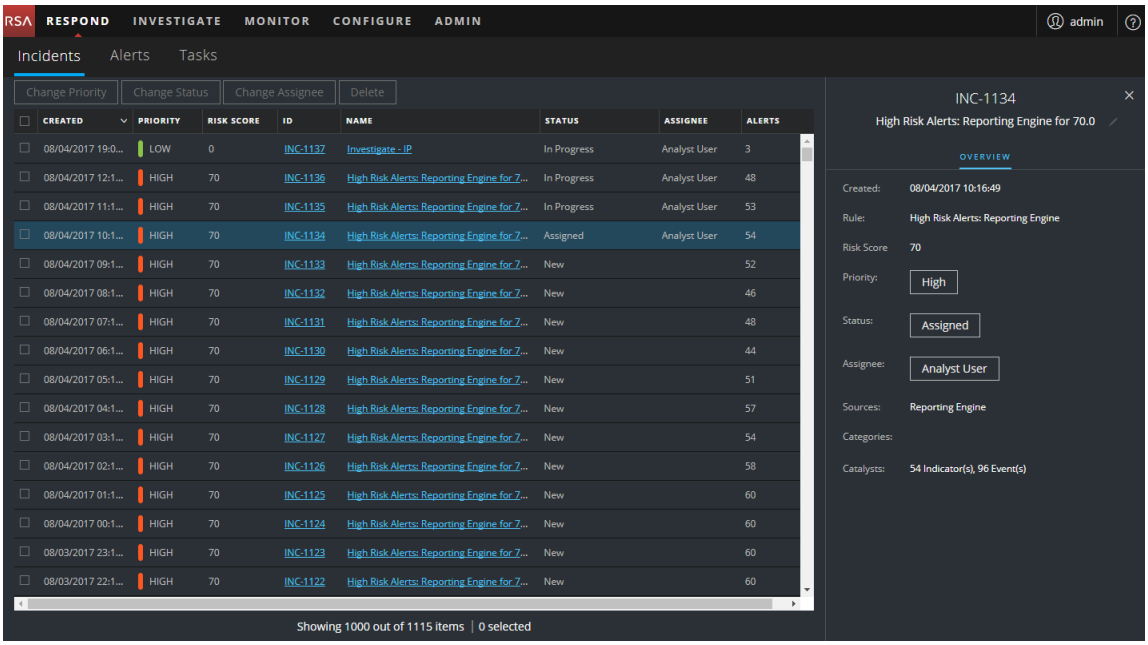


You will see a successful change notification. In this example, the status of the updated incidents now show In Progress.



To change the status of a single incident from the Overview panel:

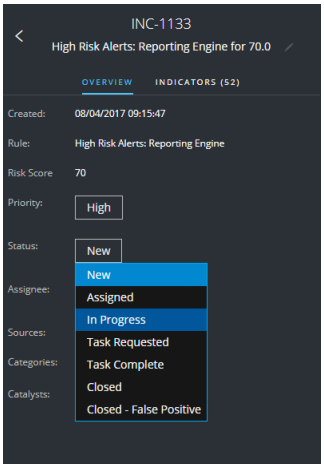
1. To open the Overview panel, do one of the following:
   - From the Incidents List view, click an incident that needs a status update.



- From the Incident Details view, click the **OVERVIEW** tab.

In the Overview panel, the Status button shows the current status of the incident.

2. Click the **Status** button and select a status from the drop-down list.



You will see a successful change notification.

Change Incident Priority

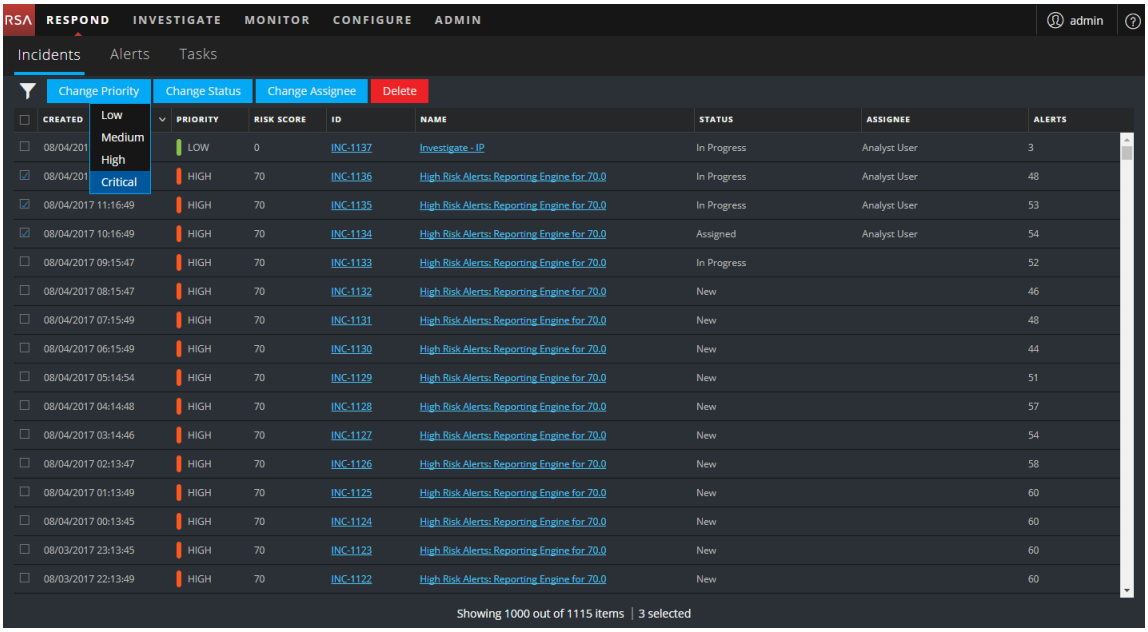
The incident list is sorted by Priority by default. You can update the priority as you study the details of the case. The following priorities are available:

- Critical
- High
- Medium
- Low

Note: You cannot change the priority of a closed incident.

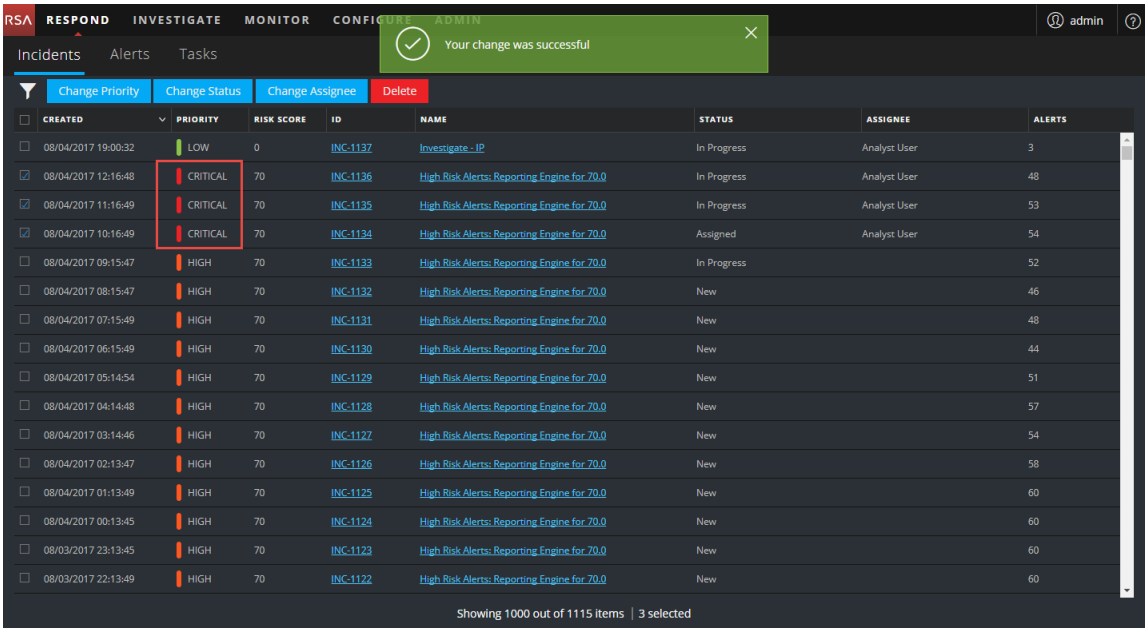
To update the priority of multiple incidents:

1. In the Incidents List view, select one or more incidents that you would like to change. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears in the incidents list footer.
2. Click **Change Priority** and select a priority from the drop-down list. In this example, the current priority is High, but the Analyst would like to change it to Critical for the selected incidents.



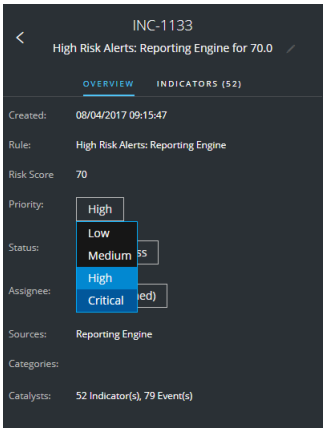
3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.
   You will see a successful change notification. In this example, the status of the updated

incidents now show Critical.



To change the priority of a single incident from the Overview panel

1. To open the Overview panel, do one of the following:
   - From the Incidents List view, click an incident that needs a priority update.
   - From the Incident Details view, click the **OVERVIEW** tab.
     In the Overview panel, the Priority button shows the current priority of the incident.
2. Click the **Priority** button and select a status from the drop-down list.



You will see a successful change notification. The Priority button changes to show the new incident priority.

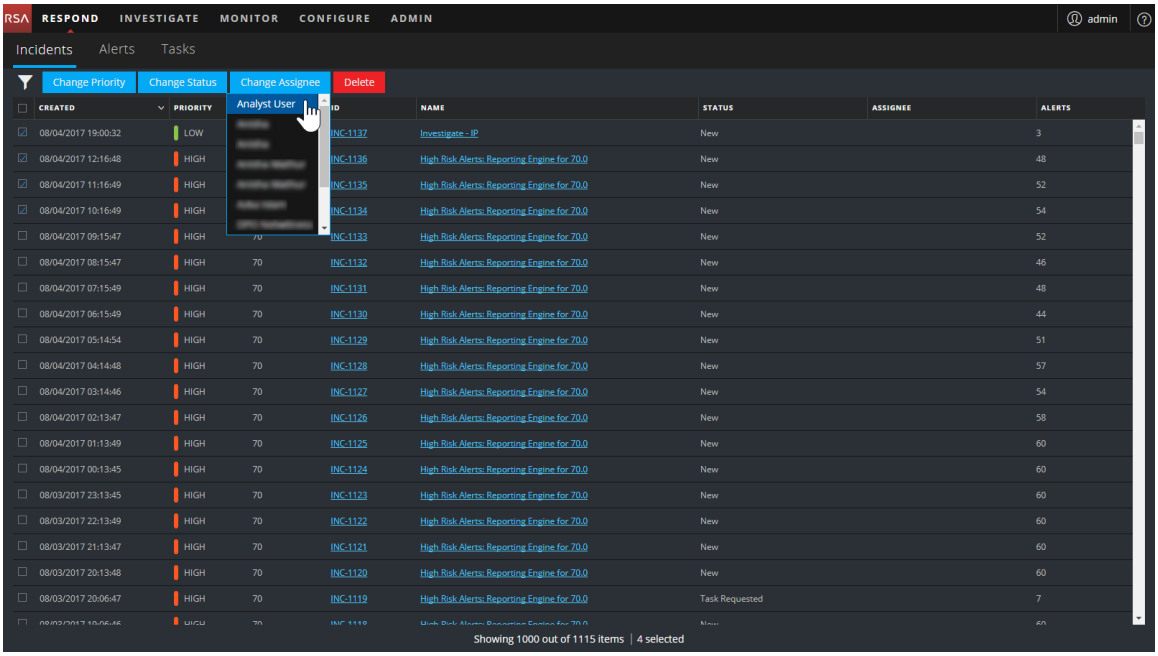
Assign incidents to other Analysts

You can assign incidents to other Analysts in the same way as you assign incidents to yourself. SOC Managers and Administrators can assign multiple incidents to a user at the same time.

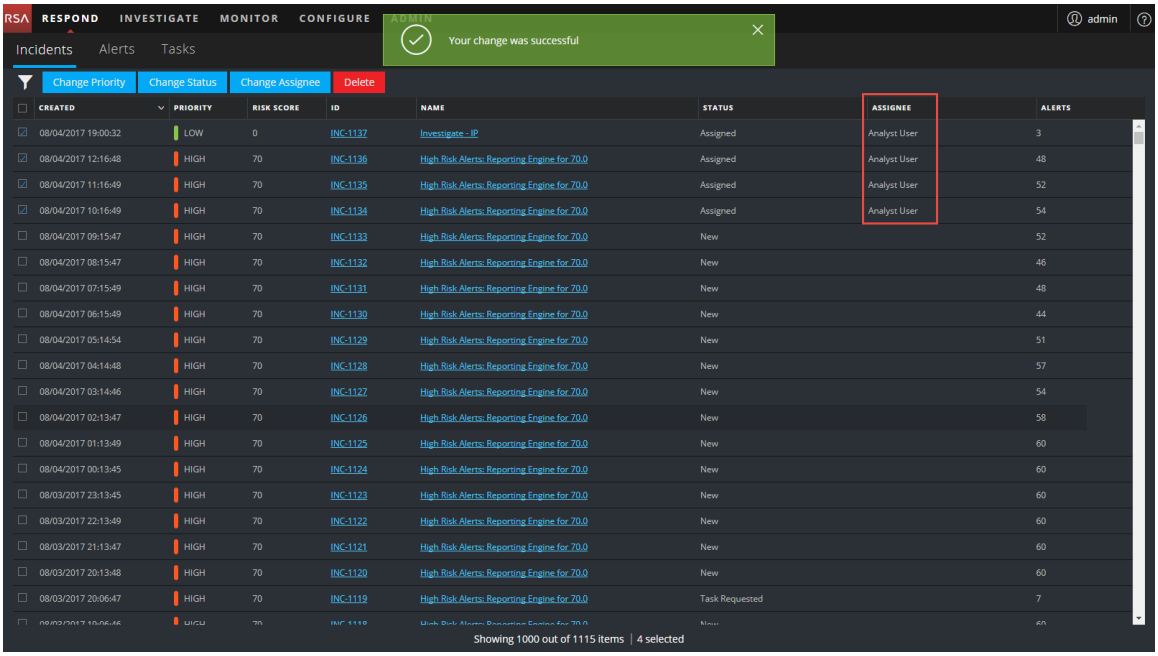
Note: You cannot change the assignee of a closed incident.

To assign multiple incidents to a user:

1. In the Incidents List view, select the incidents that you would like to assign to a user. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears in the incidents list footer.
2. Click **Change Assignee** and select a user from the drop-down list. In this example, the incidents are unassigned, but they should be assigned to an Analyst.

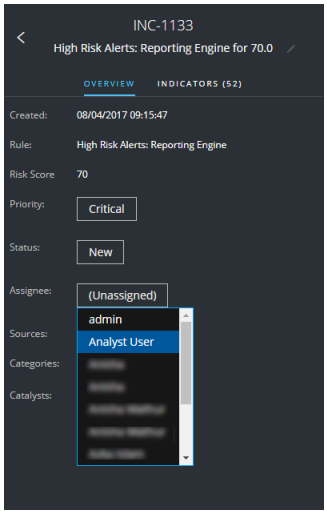


3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.
   You will see a successful change notification. The assignee changes to the selected user.



To assign a user to an incident from the Overview panel:

1. To open the Overview panel, do one of the following:
   - From the Incidents List view, click an incident that needs a priority update.
   - From the Incident Details view, click the **OVERVIEW** tab.
     In the Overview panel, the Priority button shows the current priority of the incident. In the following example, the Assignee button has a current status of Unassigned.



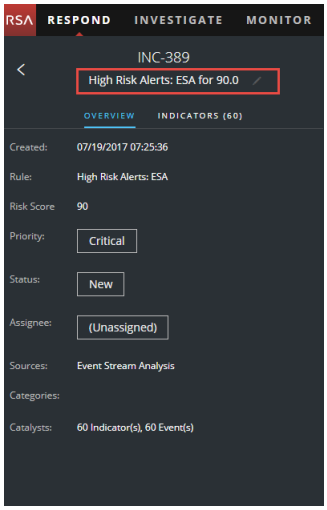
2. Click the **Assignee** button and select a user from the drop-down list.
   You will see a successful change notification. The Assignee button changes to show the assigned user.

Rename an Incident

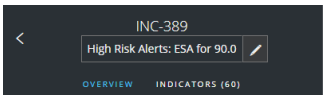
You can rename an incident from the Overview panel in the Incidents List view and the Incident Details view. For example, you may want to rename an incident to provide clarification about the issue, especially if multiple incidents have the same name.

1. Go to **RESPOND > Incidents**.
2. To open the Overview panel, do one of the following:
   - From the Incidents List view, click an incident that needs a name change.
     The Overview panel opens.
   - From the Incident Details view, go to the **OVERVIEW** panel.
     In the header above the Overview panel , you can see the Incident ID and the incident

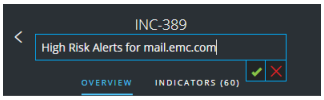
name.



3. Click the incident name in the header to open a text editor.



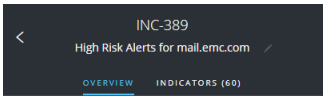
4. Type a new name for the incident in the text editor and click the check mark to confirm the change.



For example, you can change "High Risk Alerts: ESA for 90.0" to "Alerts for mail.emc.com" for more clarification.

You will see a successful change notification.

The incident name field shows the new name.

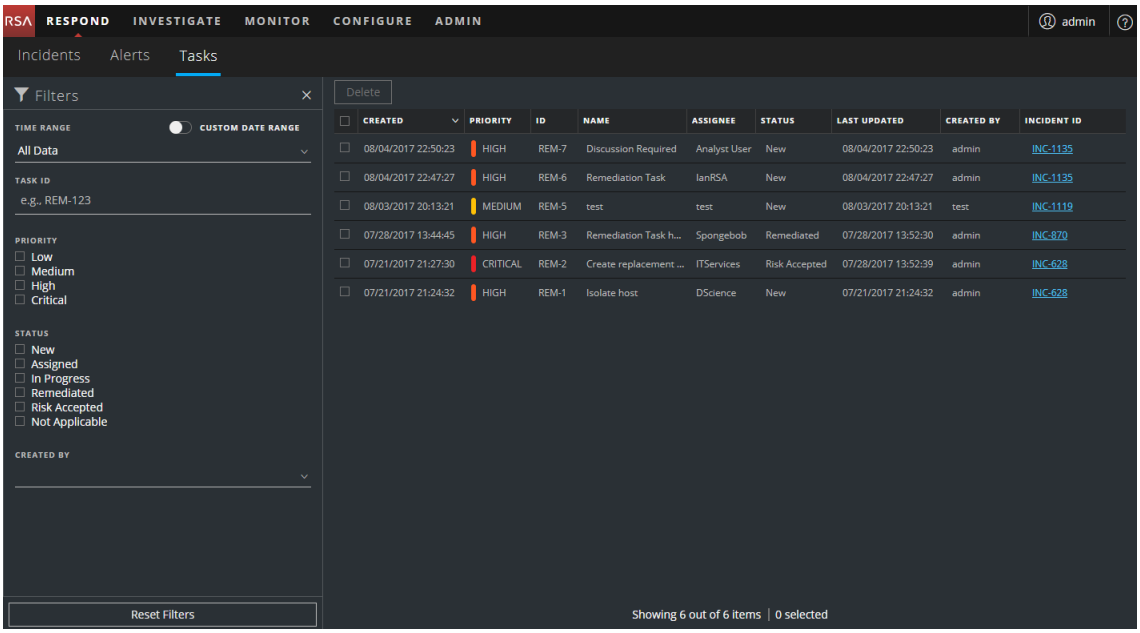


View All Incident Tasks

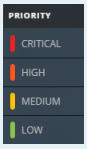
When additional work is required for an incident, you can create tasks for the incident and track the progress on those tasks. This is helpful, for example, when the work being done is outside security operations or you make a request for a computer reimage. In the Tasks List view, you can manage and track the tasks,to closure.

1. Go to **RESPOND > Tasks**.

   The Tasks List view displays a list of all incident tasks.



2. Scroll through the tasks list, which shows basic information about each task as described in the following table.

Column	Description
CREATED	Displays the date when the task was created.
PRIORITY	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates **Critical**, orange represents **High** risk, yellow indicates **Medium** risk, and green represents **Low** risk as shown in the following figure: 
ID	Displays the task ID.
NAME	Displays the task name.
ASSIGNEE	Displays the name of the user assigned to the task.

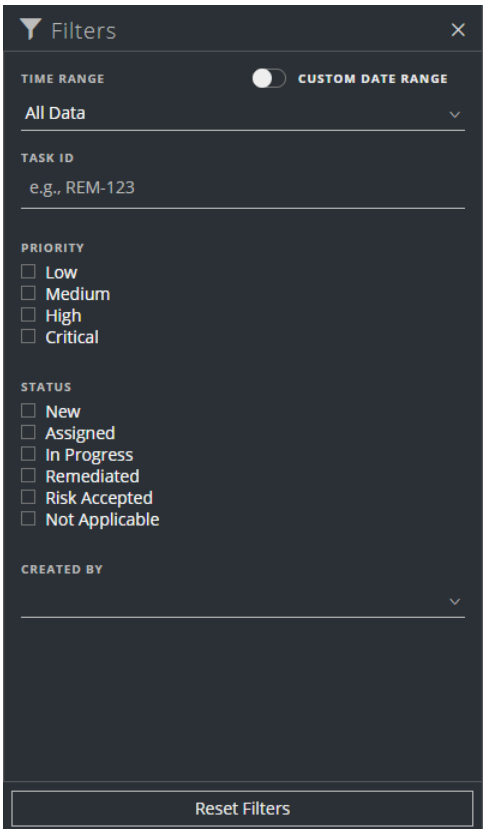
Column	Description
STATUS	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
LAST UPDATED	Displays the date and time when the task was last updated.
CREATED BY	Displays the user who created the task.
INCIDENT ID	Displays the incident ID for which the task was created. Click the ID to display the details of the incident.

At the bottom of the list, you can see the number of tasks on the current page, the total number of tasks, and the number of tasks selected. For example: **Showing 6 out of 6 items | 2 selected**.

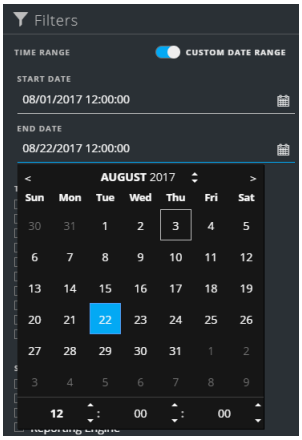
Filter the Tasks List

The number of tasks in the Tasks List can be very large, making it difficult to locate particular tasks. The Filter enables you to specify those tasks that you would like to view, such as tasks created within the last 7 days. You can also search for a specific task.

1. Go to **RESPOND > Tasks**.
   The Filters panel appears to the left of the Tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.



2. In the Filters panel, select one or more options to filter the incidents list:
   - **TIME RANGE**: You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the tasks. For example, if you select Last Hour, you will see tasks that were created within the last 60 minutes.
   - **CUSTOM DATE RANGE**: You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of CUSTOM DATE RANGE to view the Start Date and End Date fields. Select the dates and times from the calendar.



- **TASK ID**: Type the Task ID for a task that you would like to locate, for example REM-123.
- **PRIORITY**: Select the priorities that you would like to view.
- **STATUS**: Select one or more incident statuses. For example, select Remediated to view completed remediation tasks.
- **CREATED BY**: Select the user who created the tasks that you would like to view. For example, if you only want to view the tasks created by Edwardo, select Edwardo from the CREATED BY drop-down list. If you want to view tasks regardless of the person who created the task, do not make a selection under CREATED BY.

The Tasks List shows a list of tasks that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the tasks list.
For example: **Showing 6 out of 6 items**

3. If you want to close the Filters panel, click **X**. Your filters remain in place until you remove them.

Remove My Filters from the Tasks List

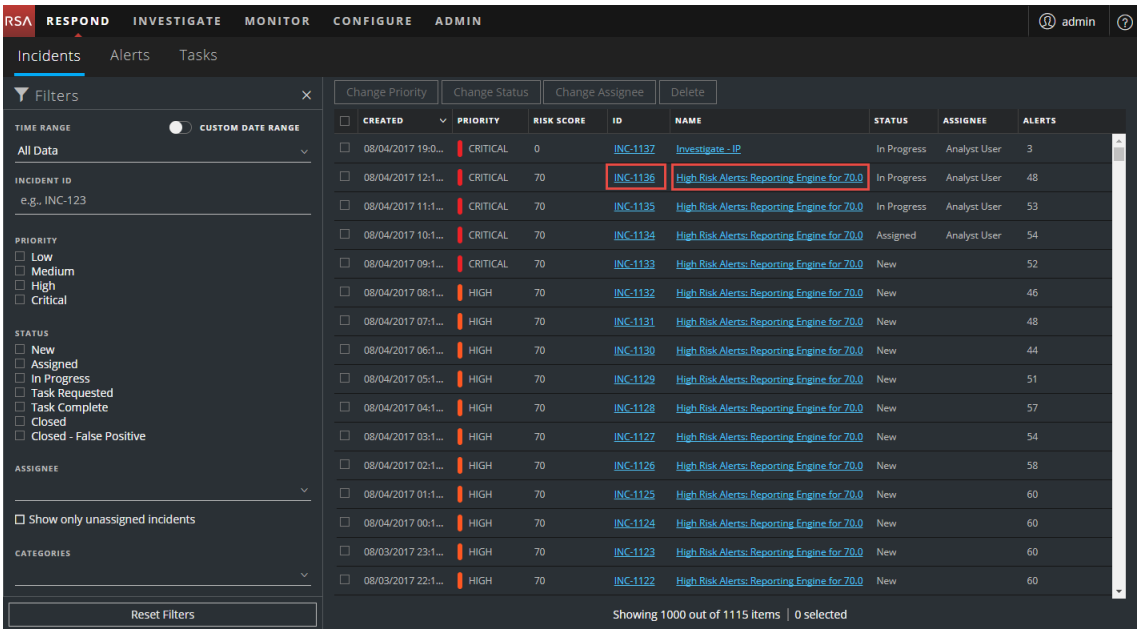
NetWitness Suite remembers your filter selections in the Tasks Listview. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of tasks that you expect to see or you want to view all of the tasks in your tasks list, you can reset your filters.

1. Go to **RESPOND > Tasks**.
   The Filters panel appears to the left of the tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.
2. At the bottom of the Filters panel, click **Reset Filters**.

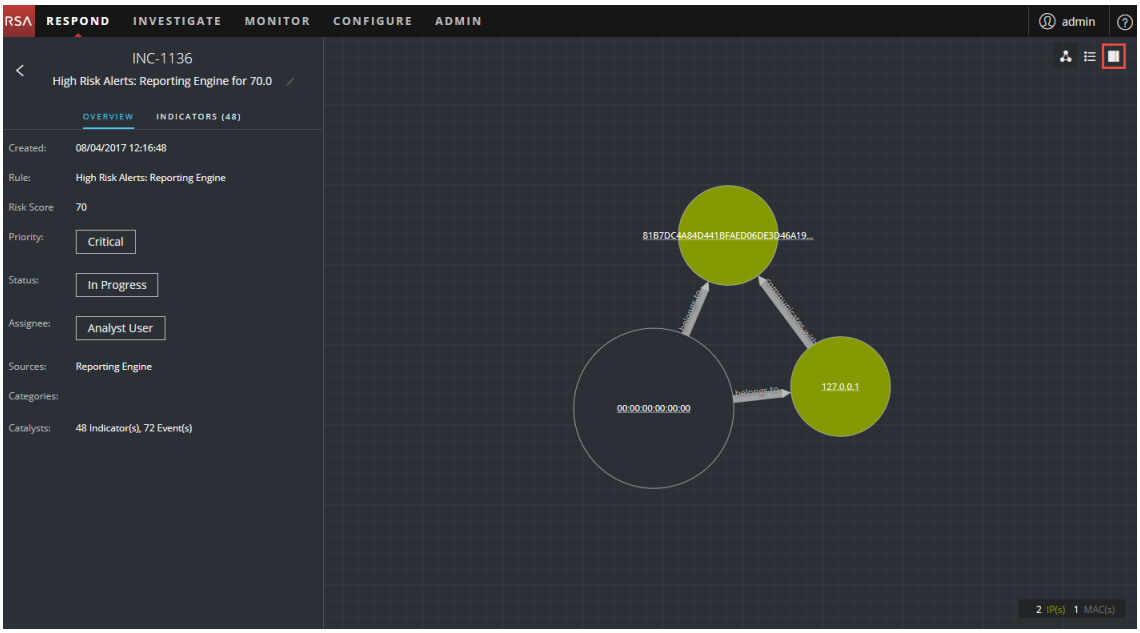
Create a Task

After you investigate an incident and know more about it, you can create a task, assign it to a user, and track it to closure. You create tasks from the Incident Details view.

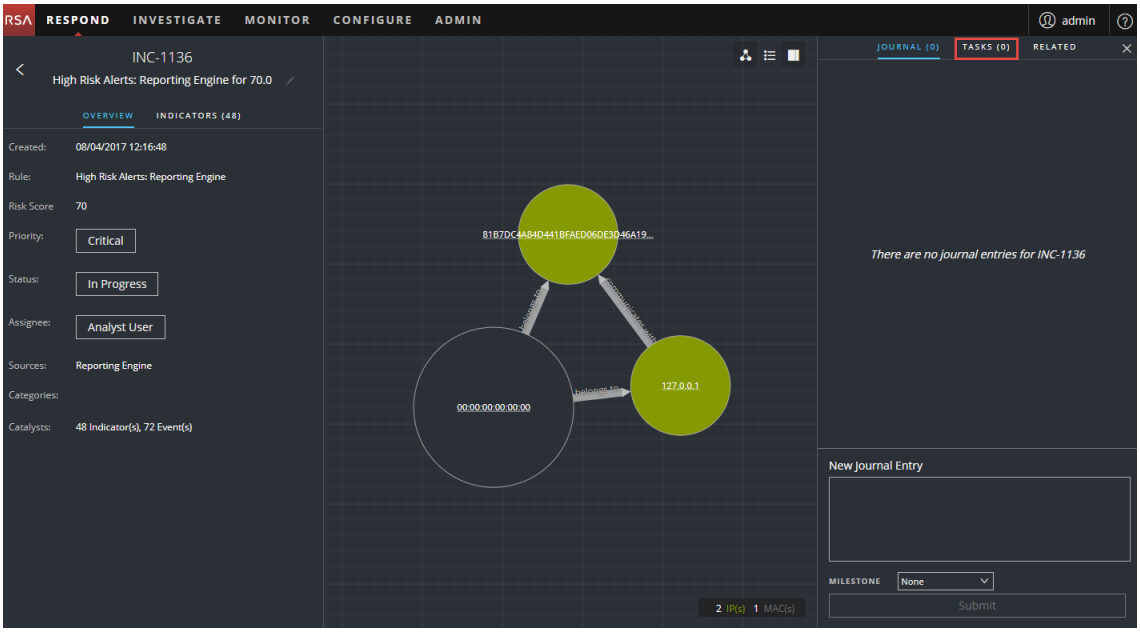
1. Go to **RESPOND > Incidents**.
   The Incidents List view displays a list of all incidents.



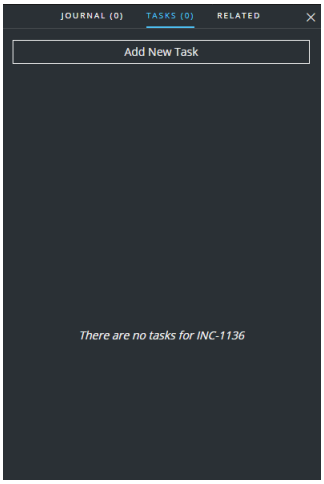
2. Locate the incident that needs a task and click the link in the **ID** or **NAME** field.
   The Incident Details view opens.



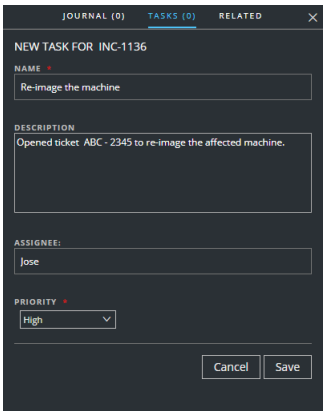
3. In the toolbar at the top right of the Incident Details view, select ▣.
   The Journal panel opens.



4. Select the **TASKS** tab.

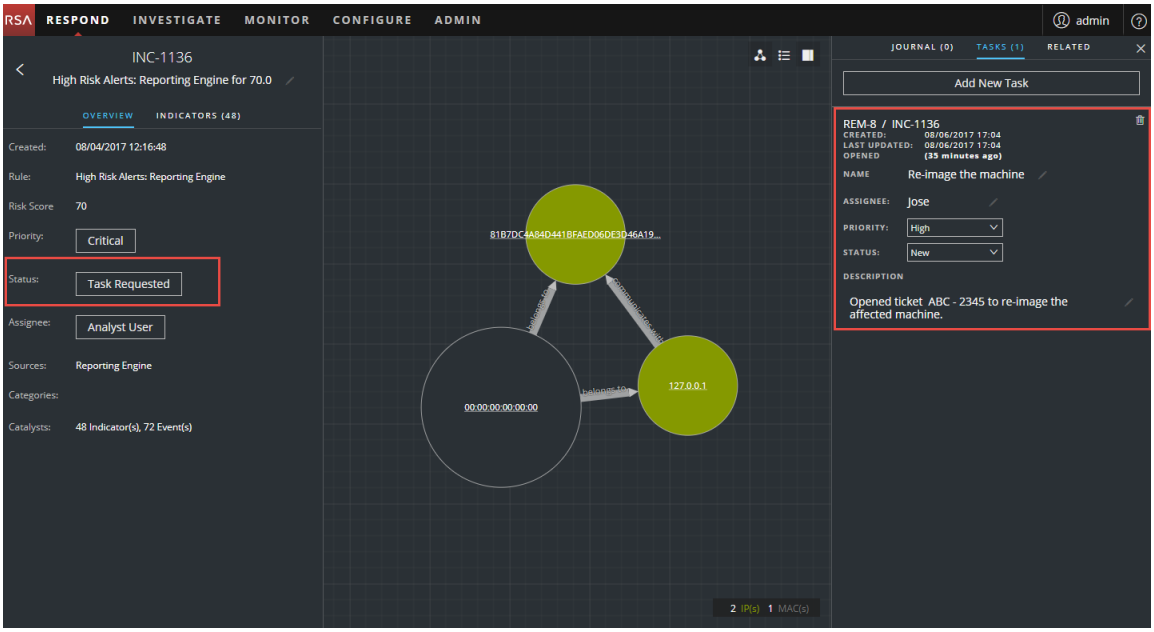


5. In the Tasks panel, click **Add New Task.**
   You will see the new task fields.



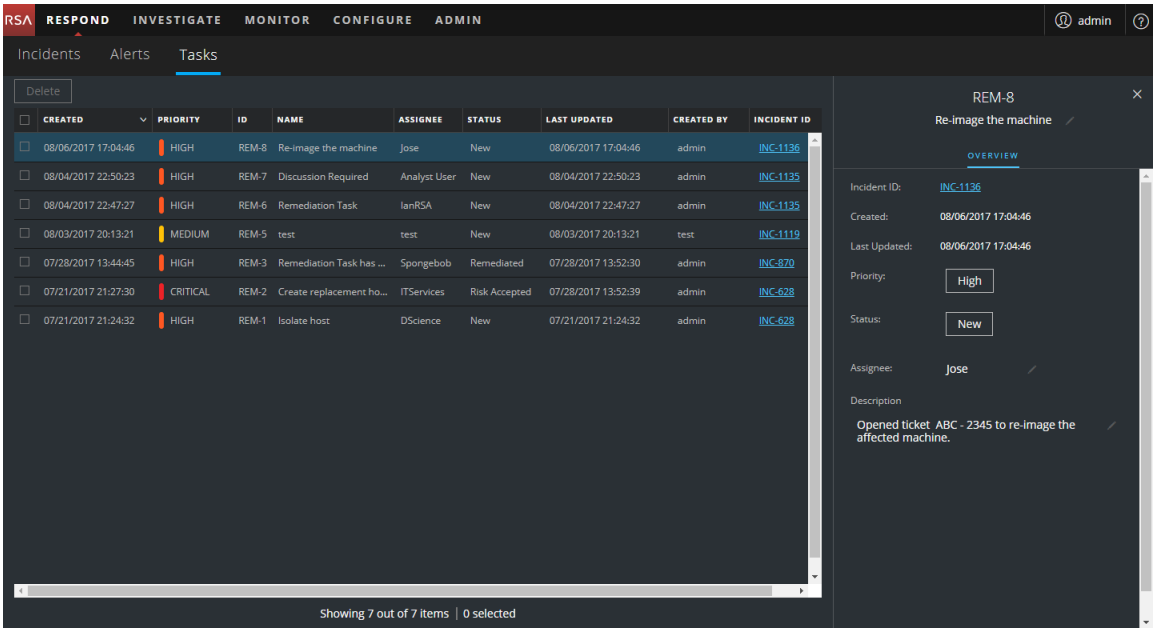
If the incident is in a closed state (Closed or Closed - False Positive), the Add New Task button is disabled.

6. Provide the following information:
   - **Name** - Name of the task. For example: Re-image the machine.
   - **Description** - (Optional) Type information that describes the task. You may want to include any applicable reference numbers.
   - **Assignee** - (Optional) Type the username of the user to whom the task is to be assigned.
   - **Priority** - Click the priority button and select a priority for the tasks from the drop-down list: Low, Medium, High, or Critical.
7. Click **Save**.
   You will see a confirmation that your change was successful. The incident status changes to **Task Requested**. The task appears in the Tasks panel for this incident.



It also appears in the Tasks list (RESPOND > Tasks), which shows a list of all incident

tasks.

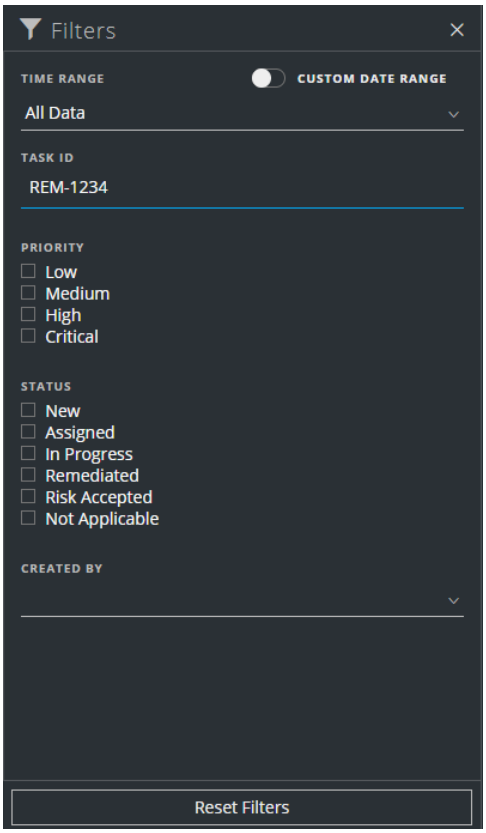


Note: If you do not see the status change, you may need to refresh your internet browser.

Find a Task

If you know the Task ID, you can quickly locate a task using the Filter. For example, you may want to locate a specific task out of thousands of tasks.

1. Go to **RESPOND > Tasks**.
   The Filters panel appears to the left of the Tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.



2. In the TASK ID field, type the Task ID for a task that you would like to locate, for example REM-1234.

   The specified task appears in your task list. If you do not see any results, try resetting your filters.

Modify a Task

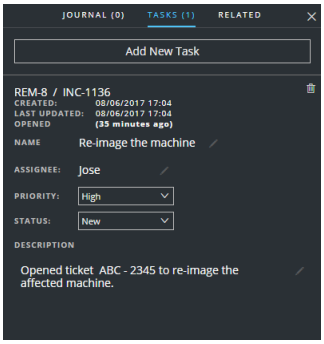
You can modify a task from within an incident and from the Tasks list. For example, you may want to show the status of the task as In Progress and add some additional information to the task. If the task is in a closed state (Not Applicable, Risk Accepted, or Remediated), you cannot modify the Priority or Assignee.

To modify a Task from within an incident:

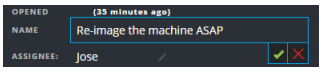
1. Go to **RESPOND > Incidents**.
   The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **NAME** field.
   The Incident Details view opens.
3. In the toolbar at the top right of the view, select ▣.

   The Journal panel opens.

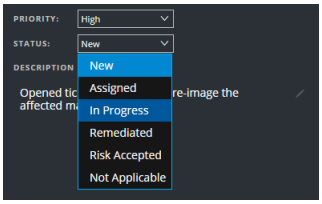
4. Select the **TASKS** tab.
5. In the Tasks panel, a pencil icon indicates a text field that you can change. A button indicates that there is a drop-down list to make a selection.



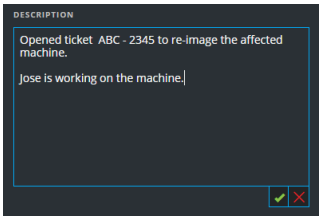
6. You can modify any of the following fields:
   - **NAME** - Click the current task name to open a text editor.

     Click the check mark to confirm the change. For example, you can change "Re-image the machine" to "Re-image the machine ASAP."
   - **ASSIGNEE** - Click (Unassigned) or the name of the previous assignee to open a text editor. Type the username of the user to whom the task is to be assigned.
     Click the check mark to confirm the change.
   - **PRIORITY** - Click the Priority button and select a priority for the task from the drop-down list: Low, Medium, High, or Critical.
   - **STATUS** - Click the Status button and select a status for the task from the drop-down list: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. For example, you can change the status to In Progress.

- **DESCRIPTION** - Click the text underneath the description to open a text editor.

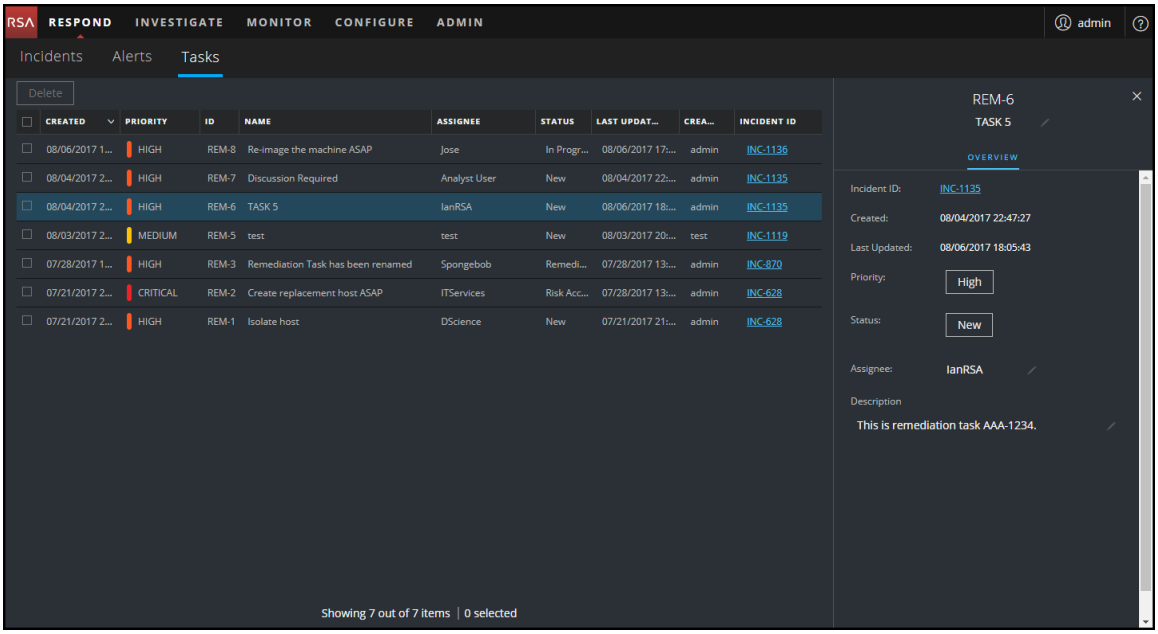


  Modify the text and click the check mark to confirm the change.

For each change that you make, you will see a confirmation that your change was successful.

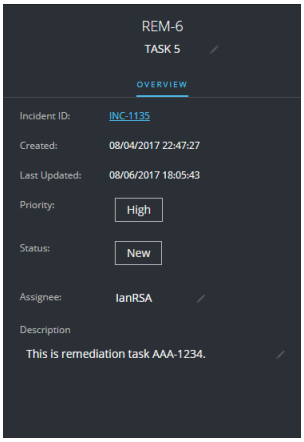
To modify a Task from the Tasks list:

1. Go to **RESPOND > Tasks**.
   The Tasks List view displays a list of all incident tasks.
2. In the Tasks list, click the task that you want to update.
   The Task Overview panel appears to the right of the tasks list.



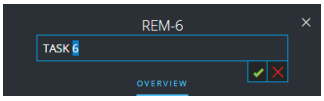
   In the Task Overview panel, a pencil icon indicates a text field that you can change. A

button indicates that there is a drop-down list to make a selection.



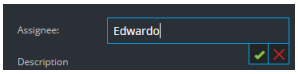
3. You can modify any of the following fields:

- **<Task Name>** - At the top of the Task Overview panel, below the Task ID, click the current task name to open a text editor.

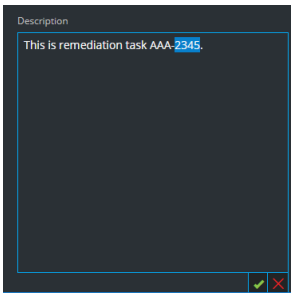
  Click the check mark to confirm the change. For example, you can change TASK 5 to TASK 6.

- **Priority** - Click the Priority button and select a priority for the task from the drop-down list: Low, Medium, High, or Critical.
- **Status** - Click the Status button and select a status for the task from the drop-down list: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
- **Assignee** - Click (Unassigned) or the name of the previous assignee to open a text editor. Type the username of the user to whom the task is to be assigned.

  Click the check mark to confirm the change.

- **Description** - Click the text underneath the description to open a text editor.

  Modify the text and click the check mark to confirm the change.

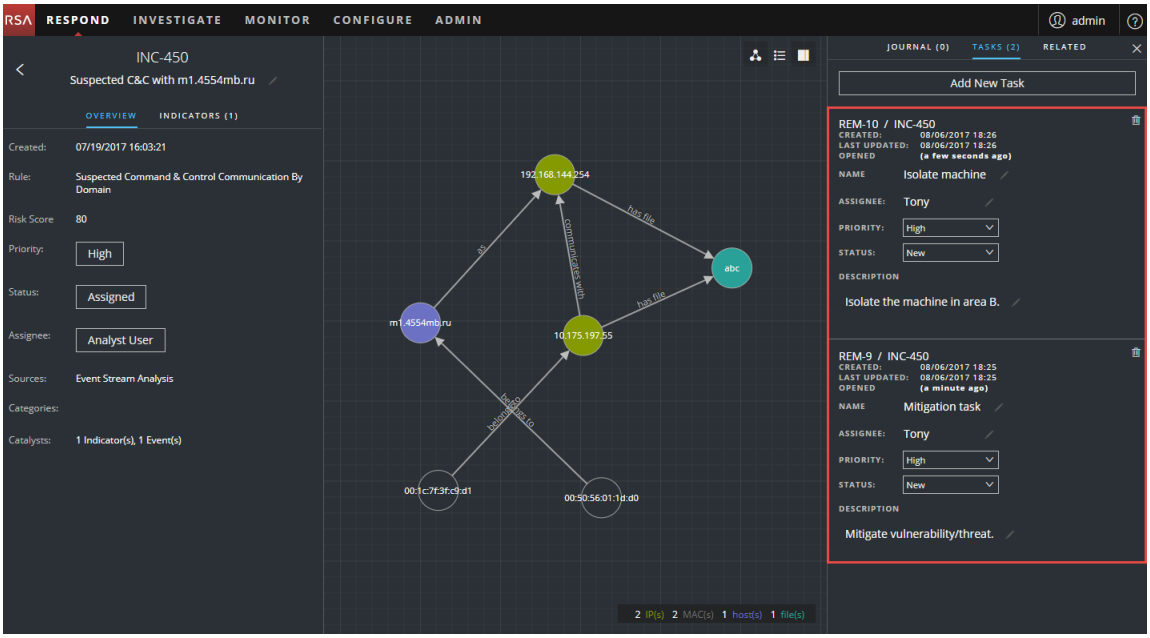
For each change that you make, you will see a confirmation that your change was successful.

Delete a Task

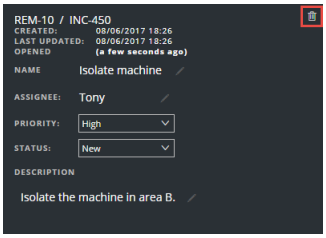
You can delete a task, if, for example, you created it in error or you find that it is not needed. You can delete a task from within an incident and also from the Tasks List view. In the Tasks List view, you can delete multiple tasks at the same time.

To Delete a Task from within an incident:

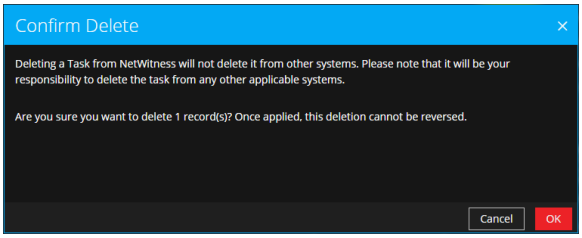
1. Go to **RESPOND > Incidents**.
   The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **NAME** field.
   The Incident Details view opens.
3. In the toolbar at the top right of the view, select ▣.
   The Journal panel opens.
4. Select the TASKS tab.
5. In the Tasks panel, you can see the tasks created for the incident.



6. Click 🗑 to the right of the task that you want to delete.



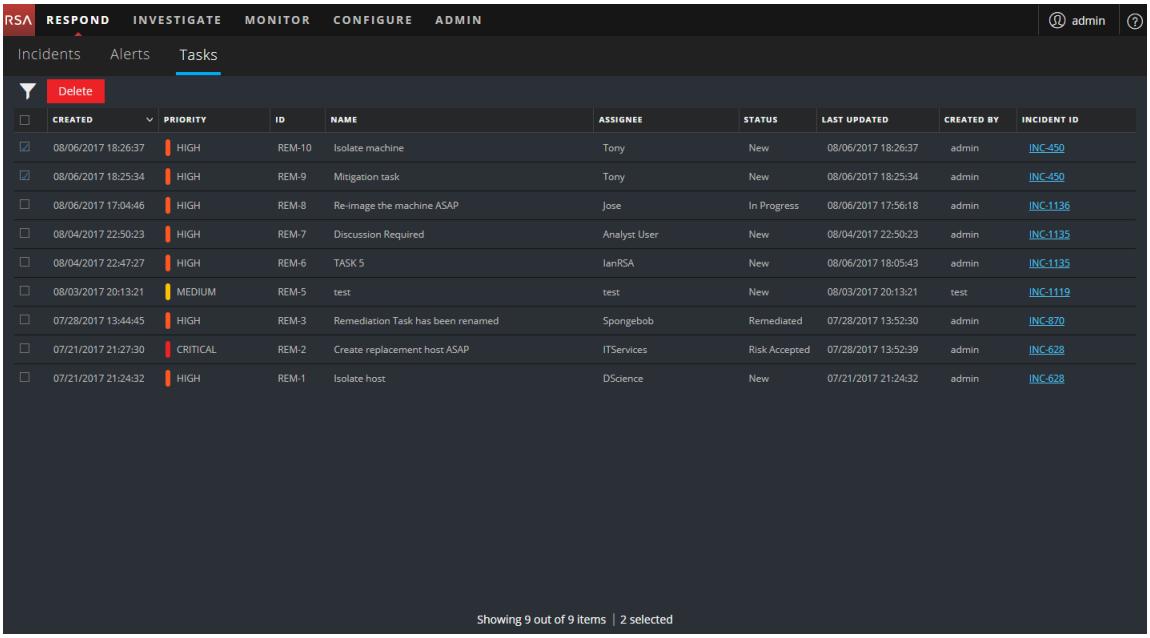
7. Confirm that you want to delete the task and click **OK**.



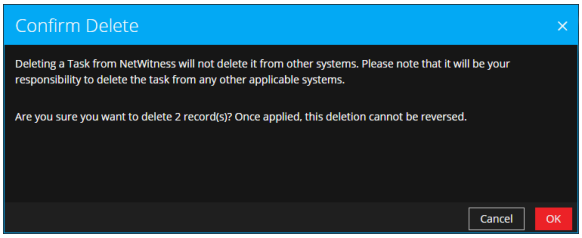
The task is deleted from NetWitness Suite. Deleting tasks from NetWitness Suite does not delete them from other systems.

To Delete Tasks from the Tasks List:

1. Go to **RESPOND > Tasks**.
   The Tasks List view displays a list of all incident tasks.
2. In the Tasks list, select the tasks that you want to delete and click **Delete**.



3. Confirm that you want to delete the tasks and click **OK**.



   The tasks are deleted from NetWitness Suite. Deleting tasks from NetWitness Suite does not delete them from other systems.

Close an Incident

When you have arrived at a solution after investigating an incident and remediating it, you close the incident.

1. Go to **RESPOND > Incidents**.
2. In the Incident List view, select the incident that you want to close and click **Change Status**.
3. Select **Closed** from the drop-down list.
   You will see a successful change notification. The incident is now closed. You cannot change the priority or assignee of a closed incident.

Note: You can also close an incident in the Overview panel. You can close multiple incidents at the same time in the Incident List view. Change Incident Status provides additional details.

Reviewing Alerts

NetWitness Suite enables you to view a consolidated list of threat alerts generated from multiple sources in one location. You can find these alerts in the RESPOND > Alerts view. The source of the alerts can be ESA correlation rules, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine, as well as many others. You can see the original source of the alerts, the alert severity, and additional alert details.

Note: ESA correlation rule alerts can ONLY be found in the RESPOND > Alerts view.

To better manage a large number of alerts, you have the ability to filter the alerts list based criteria that you specify, such as severity, time range, and alert source. For example, you may want to filter the alerts to only show those alerts with a severity between 90 and 100 that are not already part of an incident. You can then select a group of alerts to create an incident or add to an existing incident.

You can perform the following procedures to review and manage alerts:

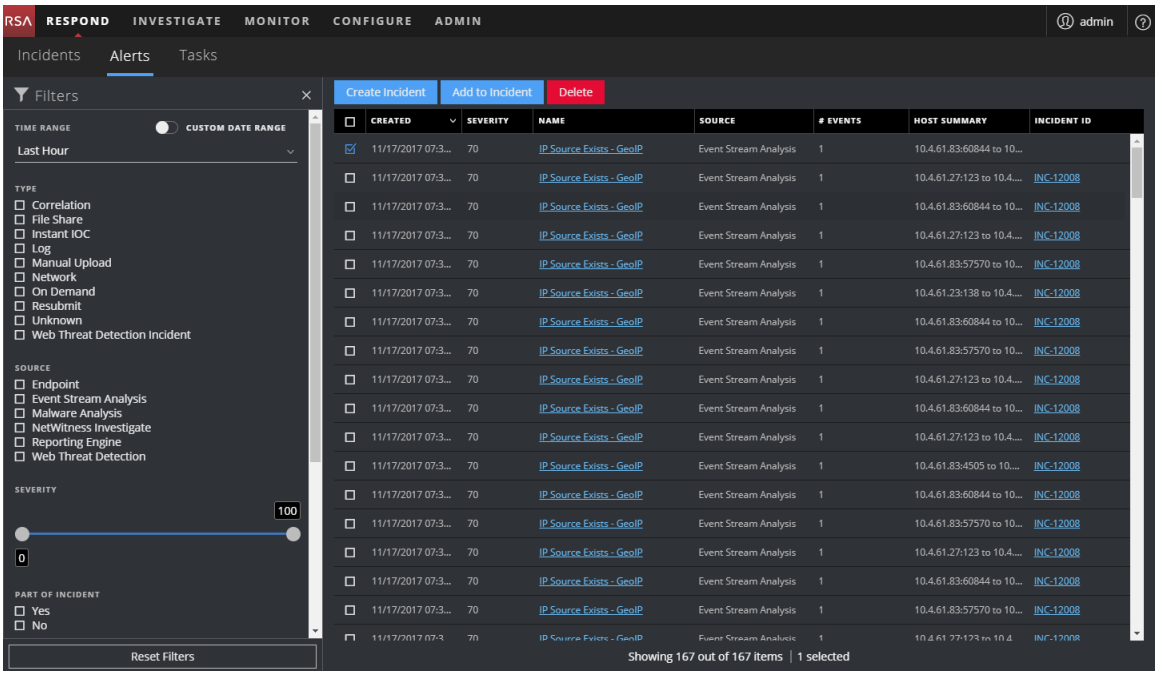
- View Alerts
- Filter the Alerts List
- Remove My Filters from the Alerts List
- View Alert Summary Information
- View Event Details for an Alert
- Investigate Events
- Create an Incident Manually
- Add Alerts to an Incident
- Delete Alerts

View Alerts

In the Alerts List view you can browse through various alerts from multiple sources, filter them, and group them to create incidents. This procedure shows you how to access the alerts list.

1. Go to **RESPOND > Alerts**.

   The Alerts List view displays a list of all NetWitness Suite alerts.



2. Scroll through the alerts list, which shows basic information about each alert as described in the following table.

Column	Description
CREATED	Displays the date and time when the alert was recorded in the source system.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.
NAME	Displays a basic description of the alert.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection, and many others.
# EVENTS	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.

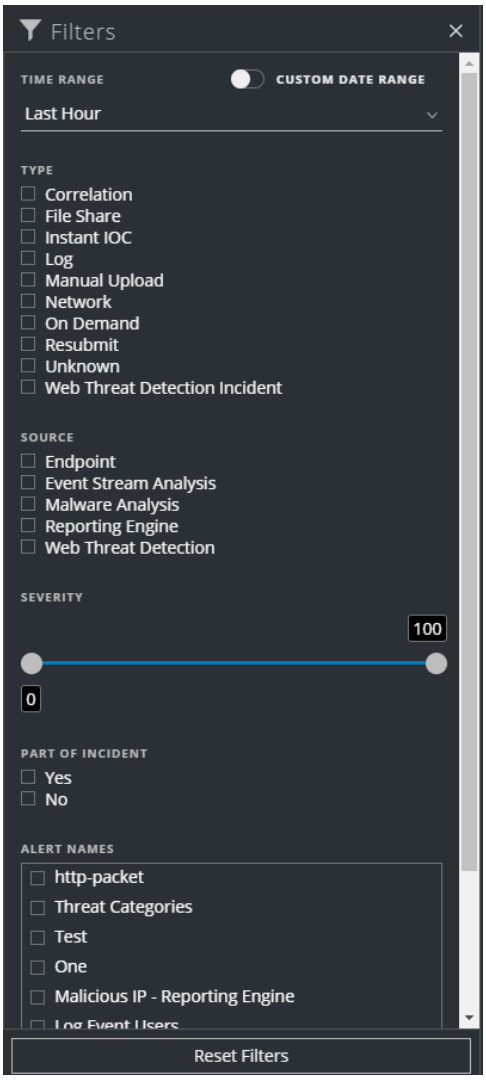
Column	Description
HOST SUMMARY	Displays details of the host like the host name from where the alert was triggered. The details may include information about the source and destination hosts in an Alert. Some alerts may describe events across more than one host .
INCIDENT ID	Shows the Incident ID of the alert. If there is no incident ID, the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.

At the bottom of the list, you can see the number of alerts on the current page and the total number of alerts. For example: **Showing 377 out of 377 items**

Filter the Alerts List

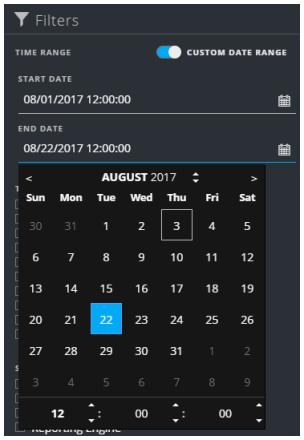
The number of alerts in the Alerts List can be very large, making it difficult to locate particular alerts. The Filter enables you to view the alerts you want to see, for example, alerts from a particular source, alerts of a particular severity, alerts that are not part of an incident, and so on.

1. Go to **RESPOND > Alerts**.
   The Filters panel appears to the left of the Alerts list. If you do not see the Filters panel, in the Alerts List view toolbar, click , which opens the Filters panel.



2. In the Filters panel, select one or more options to filter the alerts list:
   - **TIME RANGE**: You can select a specific time period from the Time Range drop-down list. The time range is based on the date that the alerts were received. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
   - **CUSTOM DATE RANGE**: You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of CUSTOM DATE RANGE to view the Start Date and End Date fields. Select the dates and times from the

calendar.



- **TYPE**: Select the type of events in the alert to view, for example, logs, network sessions, and so on.
- **SOURCE**: Select one or more sources to view alerts triggered by the selected sources. For example, to view NetWitness Endpoint alerts only, select Endpoint as the source.
- **SEVERITY**: Select the the level of severity of the alerts to view. The values are from 1 through 100. For example, to concentrate on the highest severity alerts first, you may want to view only those alerts with a severity from 90 to 100.
- **PART OF INCIDENT**:To view only alerts that are not part of an incident, select **No**. To view only alerts that are part of an incident, select **Yes**. For example, when you are ready to create an incident from a group of alerts, you can select No to view only those alerts that are not currently part of an incident.
- **ALERT NAMES**: Select the name of the alert to view. You can use this filter to search for all alerts generated by a specific rule or source, for example, Malicious IP - Reporting Engine.

The Alerts List shows a list of alerts that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the alerts list.
For example: **Showing 30 out of 30 items**

3. If you want to close the Filters panel, click **X**. Your filters remain in place until you remove them.

Remove My Filters from the Alerts List

NetWitness Suite remembers your filter selections in the Alerts List view. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of alerts that you expect to see or you want to view all of the alerts in your alerts list, you can reset your filters.

1. Go to **RESPOND > Alerts**.

   The Filters panel appears to the left of the alerts list. If you do not see the Filters panel, in the Alerts List view toolbar, click , which opens the Filters panel.

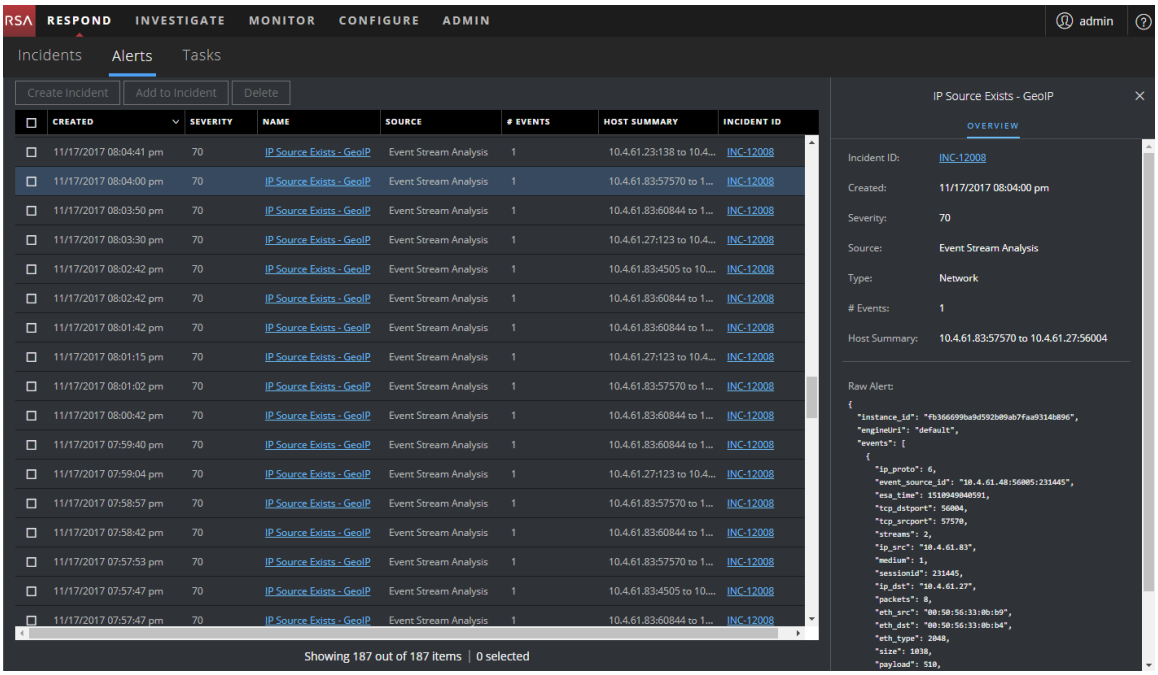
2. At the bottom of the Filters panel, click **Reset Filters**.

View Alert Summary Information

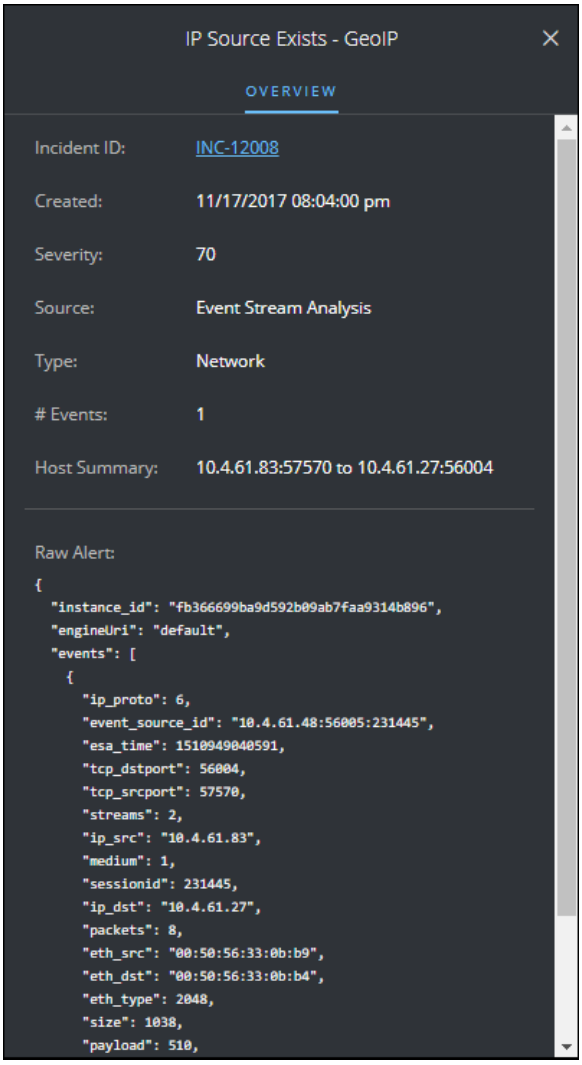
In addition to viewing basic information about an alert, you can also view raw alert metadata in the Overview panel.

1. In the Alerts list, click the alert that you want to view.

   The Alert Overview panel appears to the right of the Alerts list.

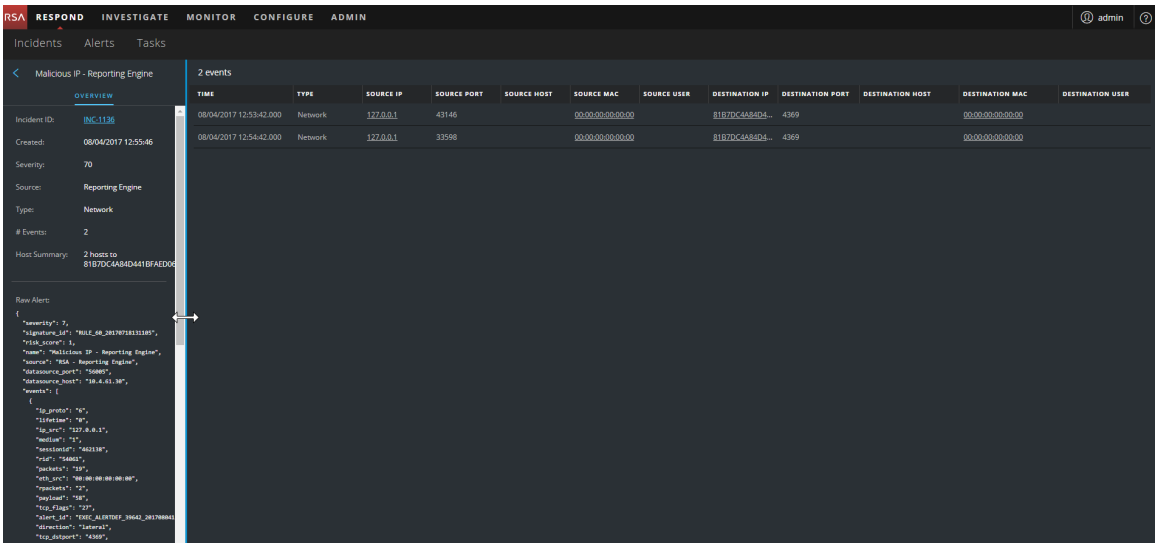


2. In the Raw Alert section, you can scroll to view the raw alert metadata.



View Event Details for an Alert

After you review the general information about the alert in the Alerts List view, you can go to the Alert Details view for more detailed information to determine the action required. An alert contains one or more events. In the Alert Details view, you can drill down into an alert to get additional event details and further investigate the alert. The following figure shows an example of the Alert Details view.



The Overview panel on the left has the same information for an alert as the Overview panel in the Alerts List view.

The Events panel on the right shows information about the events in the alert, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

There are two types of events:

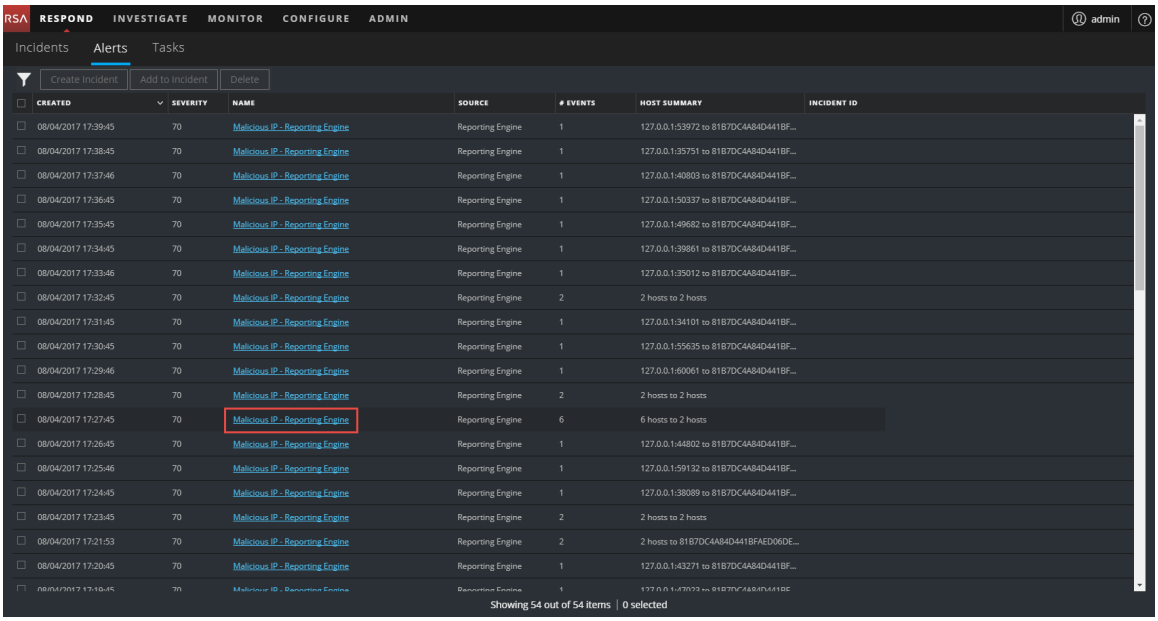
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

Some events will only have a Detector. For example, NetWitness Endpoint finds malware on your machine. Other events will have a Source and Destination. For example, packet data shows communication between your machine and a Command and Control (C2) domain.

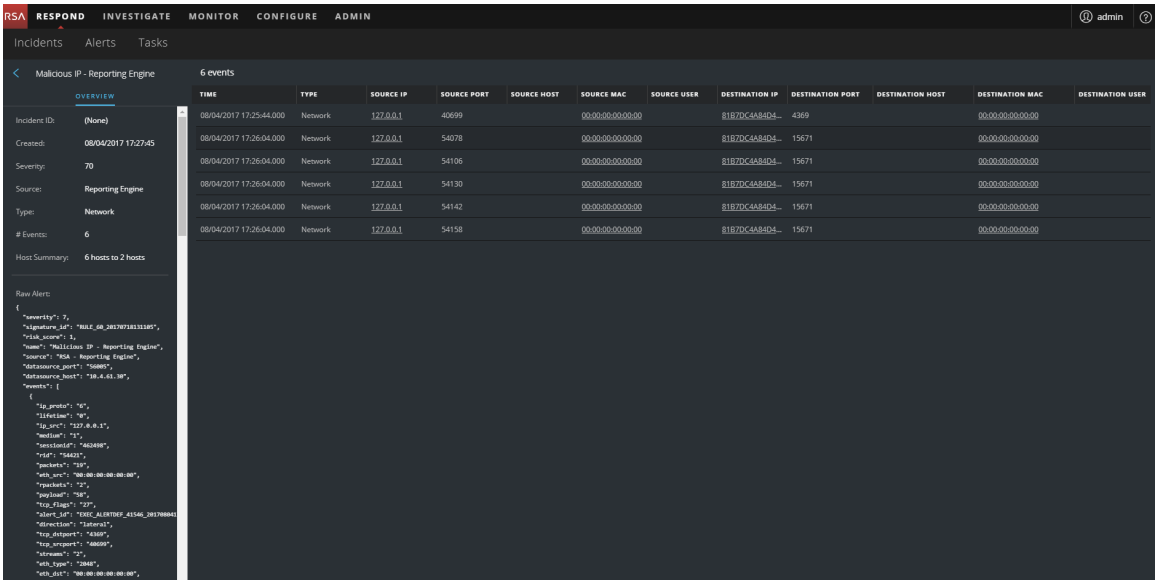
You can drill further into an event to get detailed data about the event.

To View the Event Details for an Alert:

1. To view event details for an alert, in the Alerts List view, choose an alert to view and then click the link in the NAME column for that alert.



The Alerts Details view shows the Overview panel on the left and the Events panel on the right.



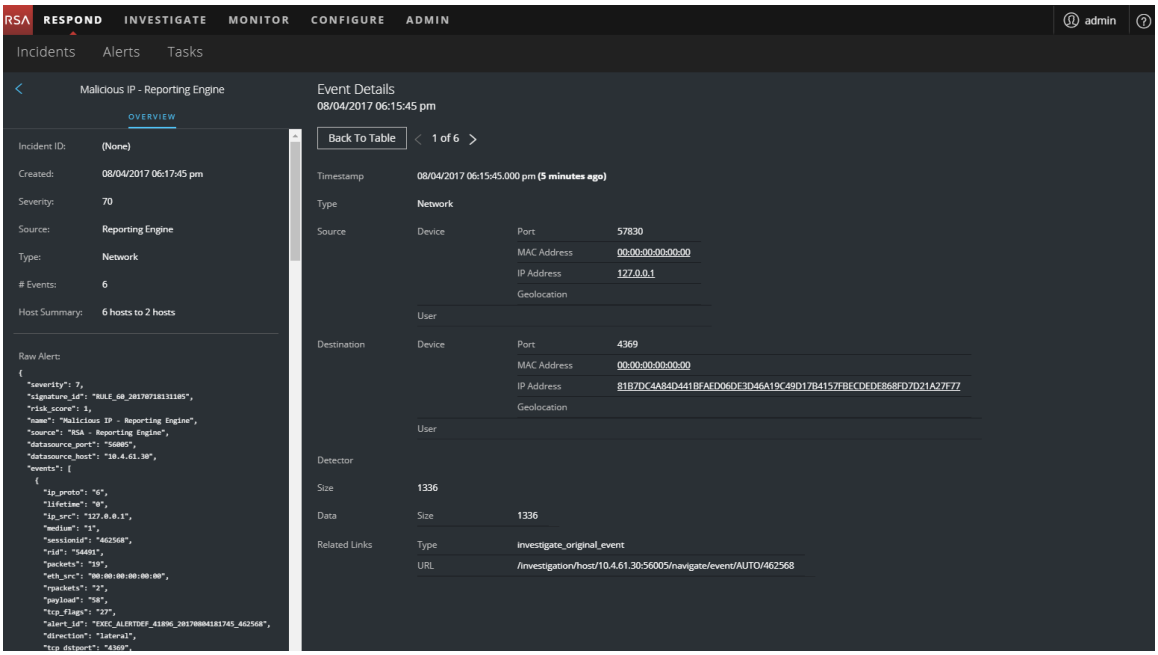
The Events panel shows a list of events with information about each event. The following table shows some of the columns that can appear in the Events List (Events Table).

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.

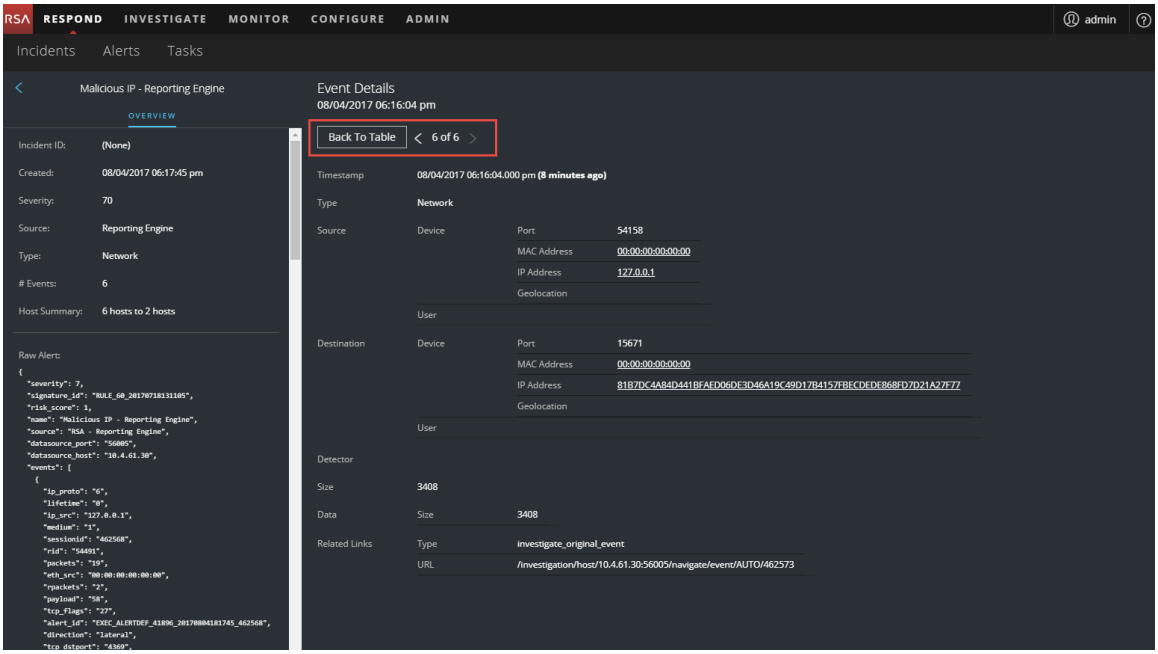
Column	Description
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
SOURCE USER	Shows the user of the source machine.
DESTINATION USER	Shows the user of the destination machine.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

If there is only one event in the list, you will see the event details for that event instead of a list.

2. Click an event in the Events list to view the Event details.
   This example shows the event details for the first event in the list.



3. Use the page navigation to the right of the Back To Table button to view other events. This example shows the event details for the last event in the list.



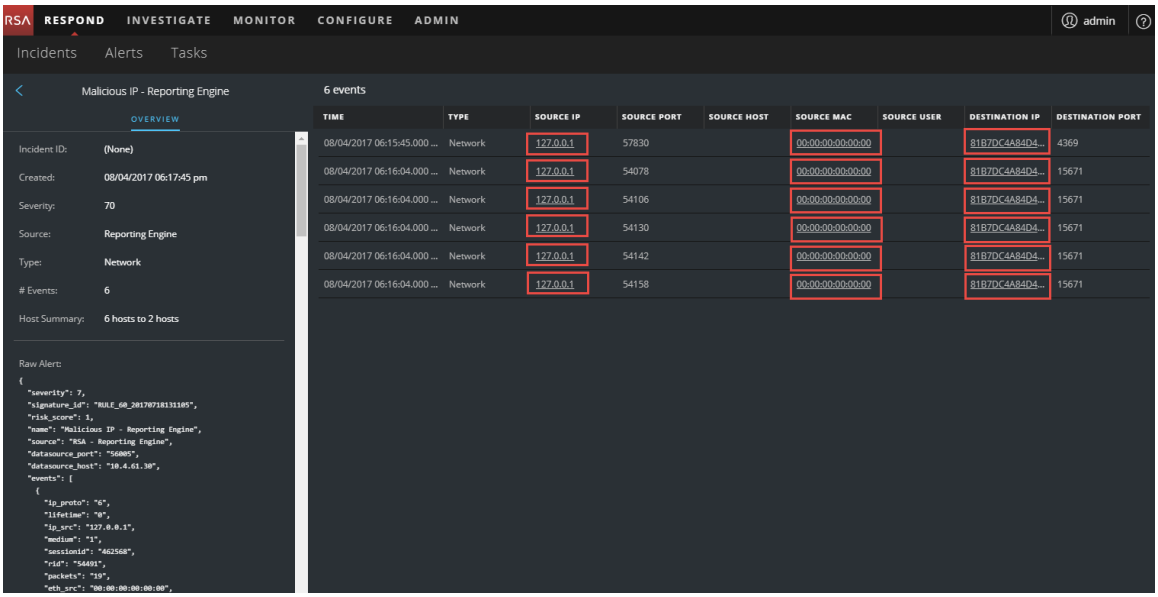
See Alert Details View for detailed information about the event data listed in the Alert Details panel.

Investigate Events

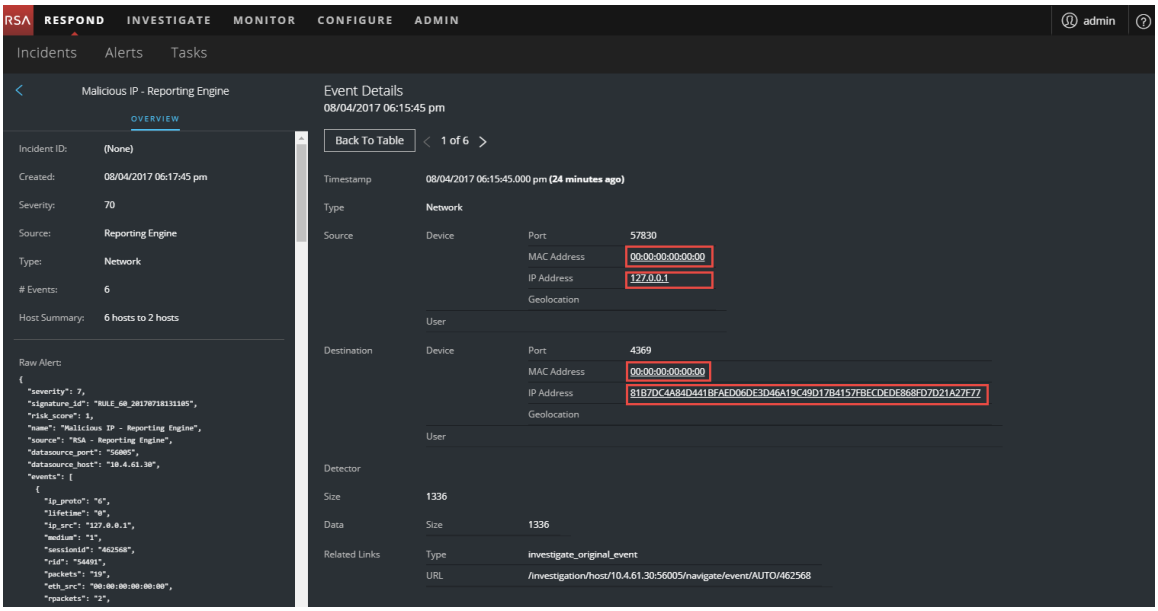
To further investigate the events, you can find links that take you to additional contextual information. From there, you have options available depending on your selection.

View Contextual Information

In the Alert Details view, you can see underlined entities in the Events panel. An underlined entity is considered an entity in the Context Hub and has additional contextual information available. The following figure shows underlined entities in the Events list.



The following figure shows underlined entities in the Events Details.

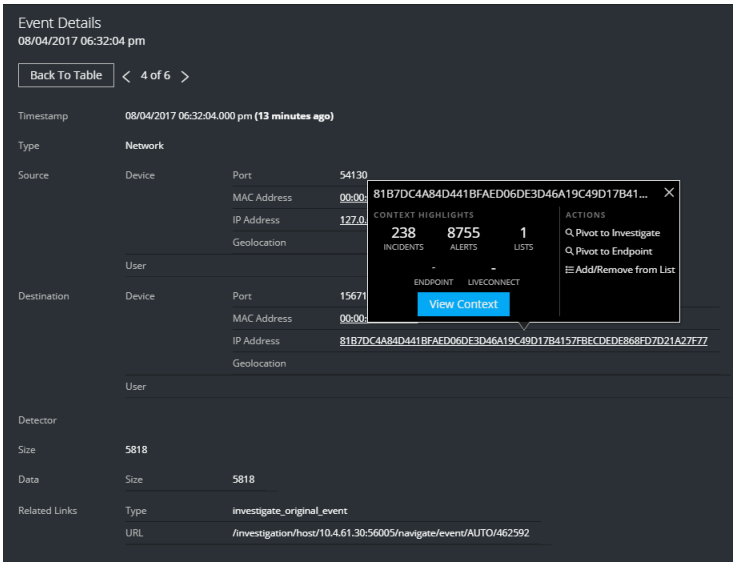


The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and Investigation use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

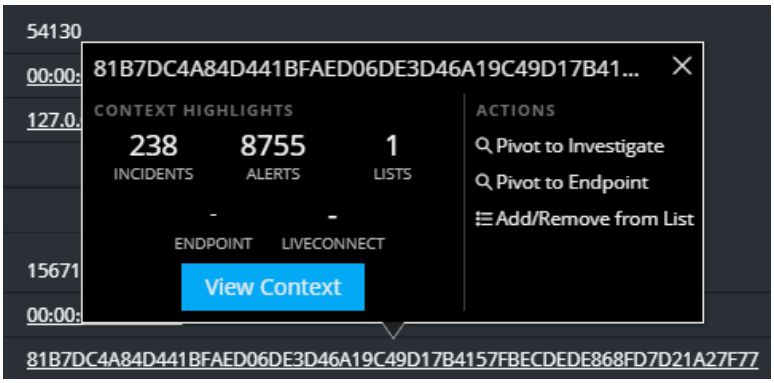
Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the **ADMIN > SYSTEM > Investigations > Context Lookup** tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, ip.address is a meta key and ip_address is not a meta key (it is a field in the MongoDB).

To View Contextual Information:

1. In the Alert Details view Events List or Event Details, hover over an underlined entity.
   A context tooltip appears with a quick summary of the type of context data that is available for the selected entity.



   The context tooltip has two sections: Context Highlights and Actions.



   The information in the **Context Highlights** section helps you to determine the actions that you would like to take. It shows the number of related alerts and incidents. Depending on your data, you may be able to click these numbered items for more information. The above example shows 238 related incidents, and 8,755 related alerts, and 1 related context hub list.

   The **Actions** section lists the available actions. In the above example, the Pivot to Investigate, Pivot to Endpoint, and Add/Remove From List options are available.

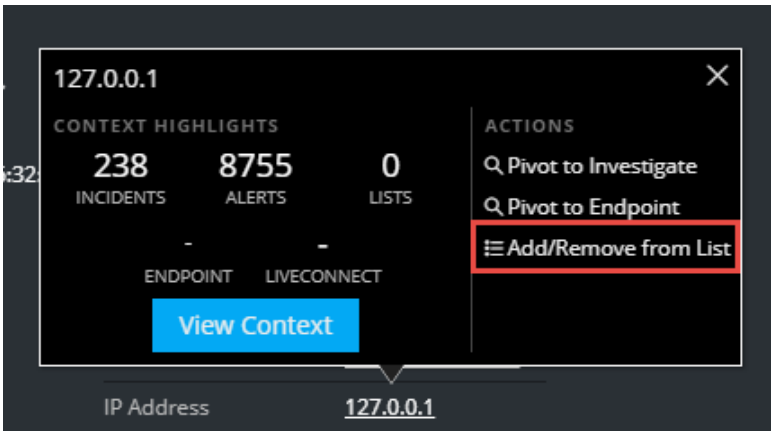
2. To see more details about the selected entity, click the **View Context** button.
   The Context panel opens and shows all of the information related to the entity.
   Context Lookup Panel - Respond View provides additional information.

Add an Entity to a Whitelist

You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

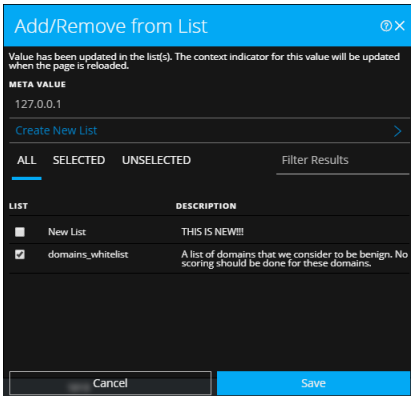
1. In the Alert Details view Events List or Event Details, hover over the underlined entity that you would like to add to a Context Hub list.

   A context tooltip appears showing the available actions.



2. In the **Actions** section of the tooltip, click **Add/Remove from List**.

   The Add/Remove From List dialog shows the available lists.



3. Select one or more lists and click **Save**.

   The entity appears on the selected lists.

   Add/Remove from List Dialog provides additional information.

Create a Whitelist

You can create a whitelist in the Context Hub in the same way as you would create it in the Incident Details view, see Create a List.

Pivot to NetWitness Endpoint

If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint**.
   The NetWitness Endpoint thick client application opens outside of your web browser.

For more information on the thick client, see the *NetWitness Endpoint User Guide*.

Pivot to Investigation

For a more thorough investigation of the incident, you can access the Investigate view.

1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate**.
   The Investigate Navigate view opens, which enables you to perform a deeper dive investigation.

For more information, see the *NetWitness Investigate User Guide*.

Create an Incident Manually

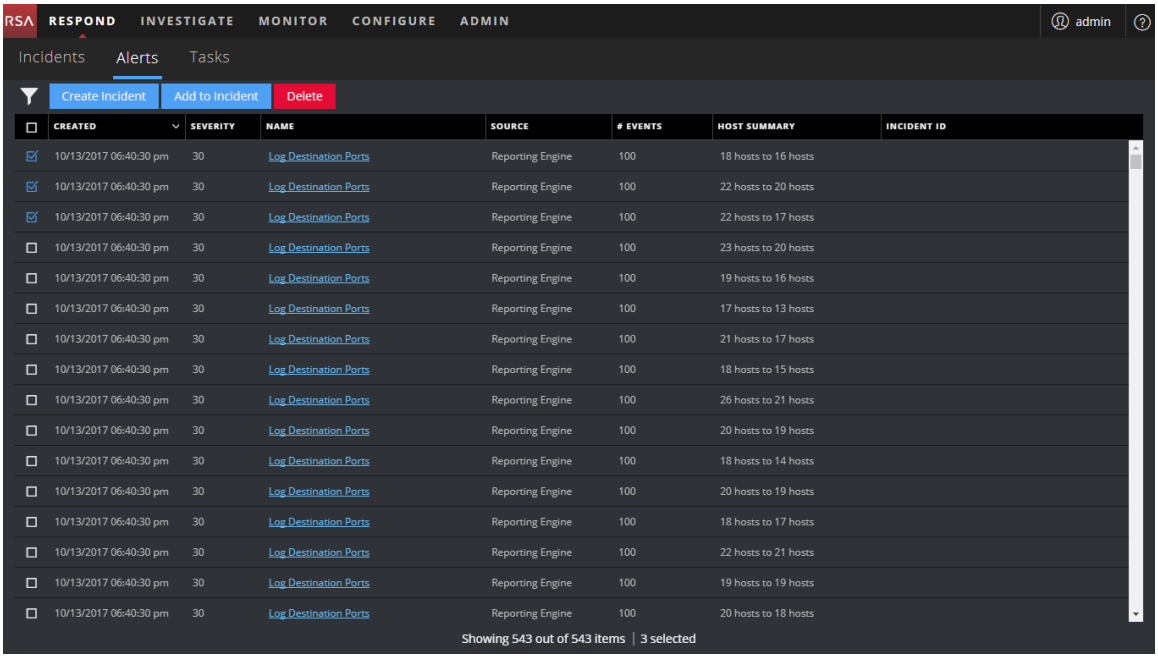
You can create incidents manually from alerts in the Alerts List view. The alerts that you select cannot be part of another incident. Incidents created manually from alerts default to Low priority, but you can change the priority after you create it. You cannot add categories to manually created incidents.

Note: Incidents can be created manually or automatically. An Alert can only be associated with one Incident. You can create incident rules to analyze the alerts collected and group them into incidents depending on which rules they match. For details, see the "Create an Incident Rule for Alerts" topic in the *NetWitness Respond Configuration Guide*.

To Create an Incident Manually:

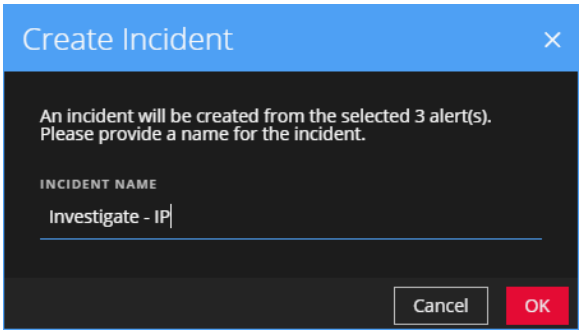
1. Go to **RESPOND > Alerts**.
2. Select one or more alerts in the Alerts List.

Note: Selecting alerts that do not have incident IDs enable the **Create Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **PART OF INCIDENT** as **No** in the Filters panel.

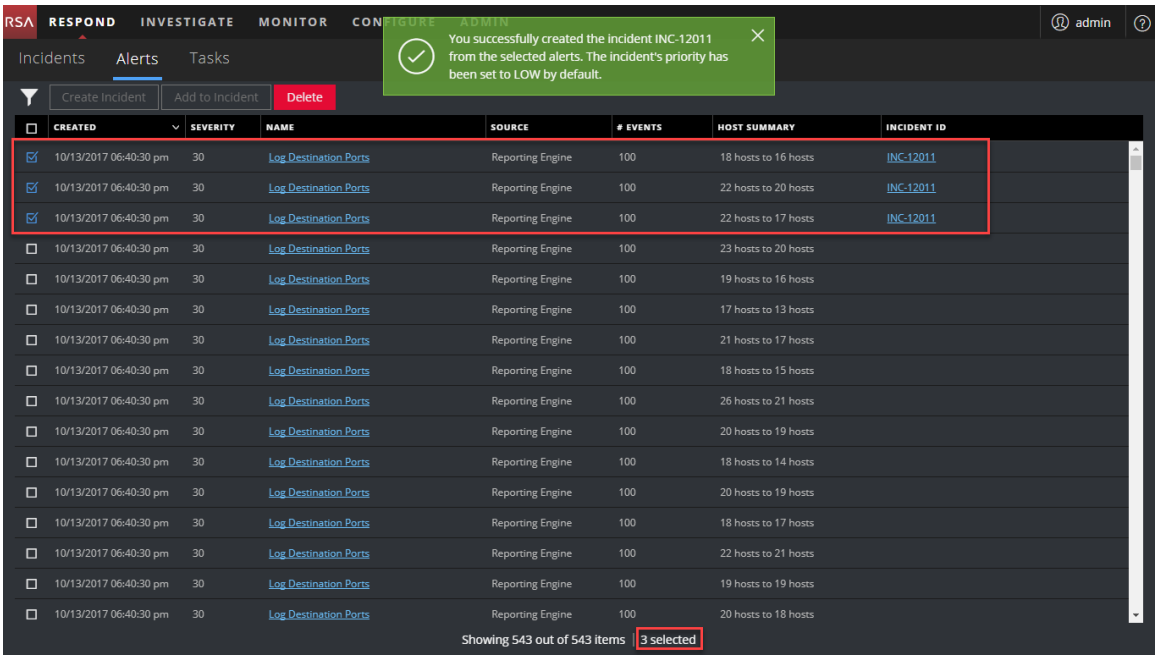


3. Click **Create Incident**.

   The **Create Incident** dialog is displayed.



4. In the **INCIDENT NAME** field, type a name to identify the incident. For example, Investigate - IP.
5. Click **OK**.



You will see a confirmation message that an incident was created from the selected alerts. The new incident ID appears as a link in the INCIDENT ID column of the selected alerts. If you click the link, it takes you to the Incident Details view for that incident, where you can update information, such as changing Priority from low to high.

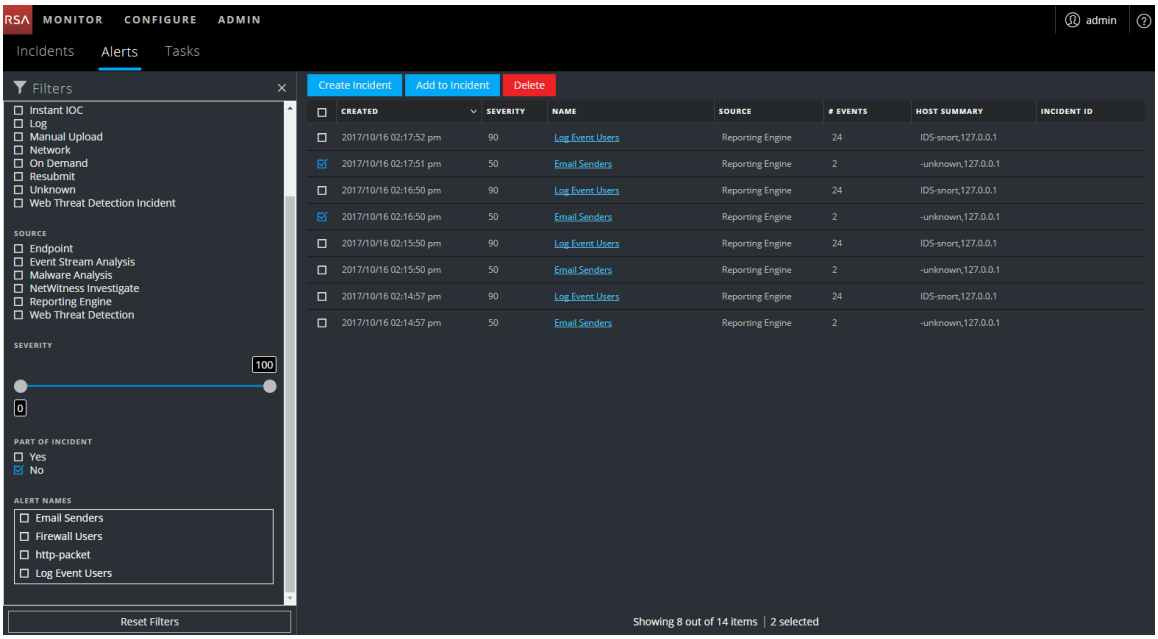
Add Alerts to an Incident

Note: This option is available in version 11.1 and later.

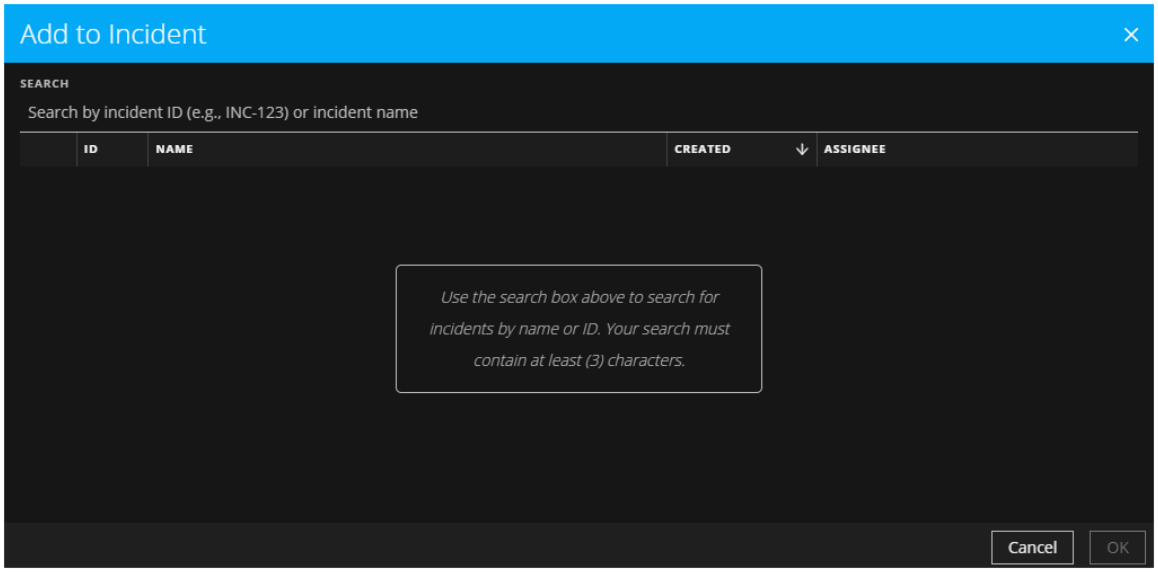
If you have alerts that fit a particular existing incident, you do not have to create a new incident. Instead, you can add alerts to that incident from the Alerts List view. The alerts that you select cannot be part of another incident.

1. Go to **RESPOND > Alerts**.
2. In the Alerts List, select one or more alerts that you want to add to an incident, and click **Add to Incident**.

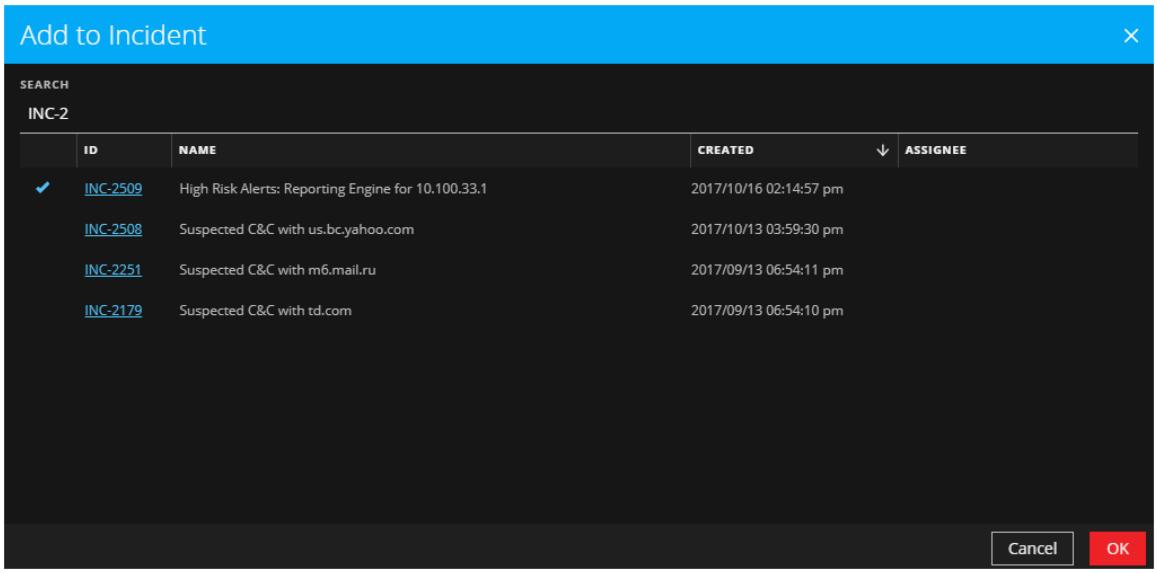
Note: Selecting alerts that do not have incident IDs enable the **Add to Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **PART OF INCIDENT** as **No** in the Filters panel.



3. In the **Add to Incident** dialog, type at least three characters in the **Search** field to search for the incident by **Name** or **Incident ID**.



4. In the results list, select the incident that will receive the selected alerts and click **OK**.



   The selected alert or alerts are now part of the selected incident and will have that incident ID.

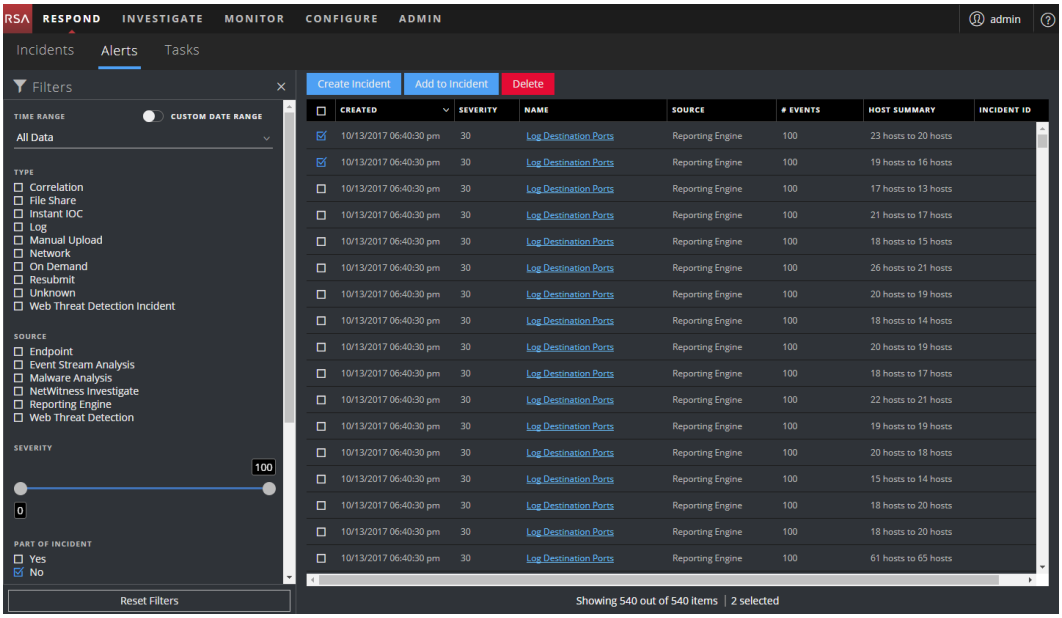
Delete Alerts

Users with the appropriate permissions, such as Administrators and Data Privacy Officers, can delete alerts. This procedure is helpful when you want to remove unnecessary or non-relevant alerts. Deleting these alerts frees up disk space.

1. Go to **RESPOND > Alerts**.

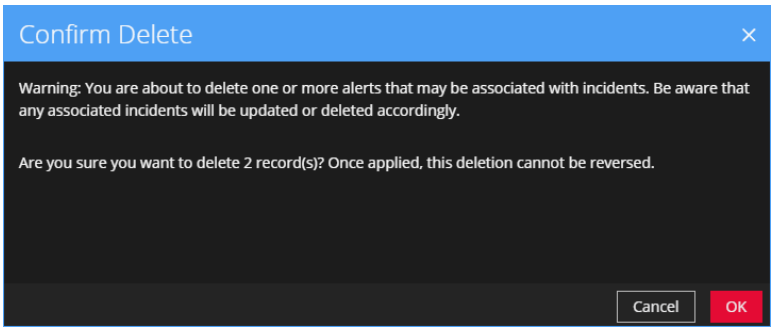
   The Alerts List view displays a list of all NetWitness Suite alerts.

2. In the Alerts list, select the alerts that you want to delete and click **Delete**.



If you do not have permission to delete alerts, you will not see the Delete button.

3. Confirm that you want to delete the alerts and click **OK**.



The alerts are deleted from NetWitness Suite. If a deleted alert is the only alert in an incident, the incident is also deleted. If the deleted alert is not the only alert in an incident, the incident is updated to reflect the deletion.

NetWitness Respond Reference Information

The Respond view user interface provides access to NetWitness Respond functions. This topic contains descriptions of the user interfaces as well as other reference information to help users understand the functions of NetWitness Respond.

Topics

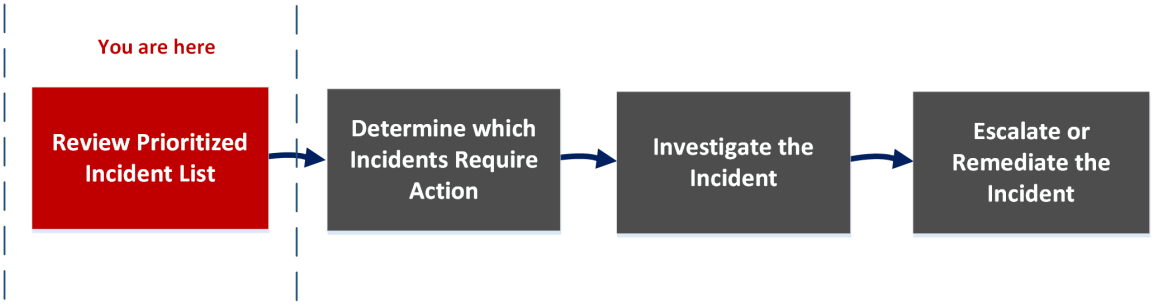
- Incidents List View
- Incident Details View
- Alerts List View
- Alert Details View
- Tasks List View
- Add/Remove from List Dialog
- Context Lookup Panel - Respond View

Incidents List View

The Incidents List view (RESPOND > Incidents) shows Incident Responders and other Analysts a prioritized results list of incidents created from various sources. For example, your results list could show incidents created from ESA rules, NetWitness Endpoint, or ESA Analytics modules for Automated Threat Detection, such as C2 for packets or logs. From the Incidents List view, you have easy access to the information that you need to quickly triage and manage incidents through completion.

Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



In the Incidents List view, you can review the list of prioritized incidents, which shows basic information about each incident. You can also change the assignee, priority, and status of the incidents. Because the results can be large in the incidents list, you have the option to filter those incidents by time range, incident ID, custom date range, priority, status, assignee, and categories.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, and SOC Manager	View prioritized incidents*	Review Prioritized Incident List
Incident Responders, Analysts, and SOC Manager	Filter and sort the incident list*	Filter the Incident List
Incident Responders, Analysts	View my incidents*	View My Incidents
Incident Responders, Analysts	Assign incidents to myself*	Assign Incidents to Myself
Incident Responders, Analysts, and SOC Manager	Find Incidents*	Find an Incident
Incident Responders, Analysts, and SOC Manager	Update an incident.*	Escalate or Remediate the Incident
Incident Responders, Analysts	View incident details.	Determine which Incidents Require Action
Incident Responders, Analysts	Further Investigate an incident.	Investigate the Incident
Incident Responders, Analysts, and SOC Manager	Create a task.	Escalate or Remediate the Incident

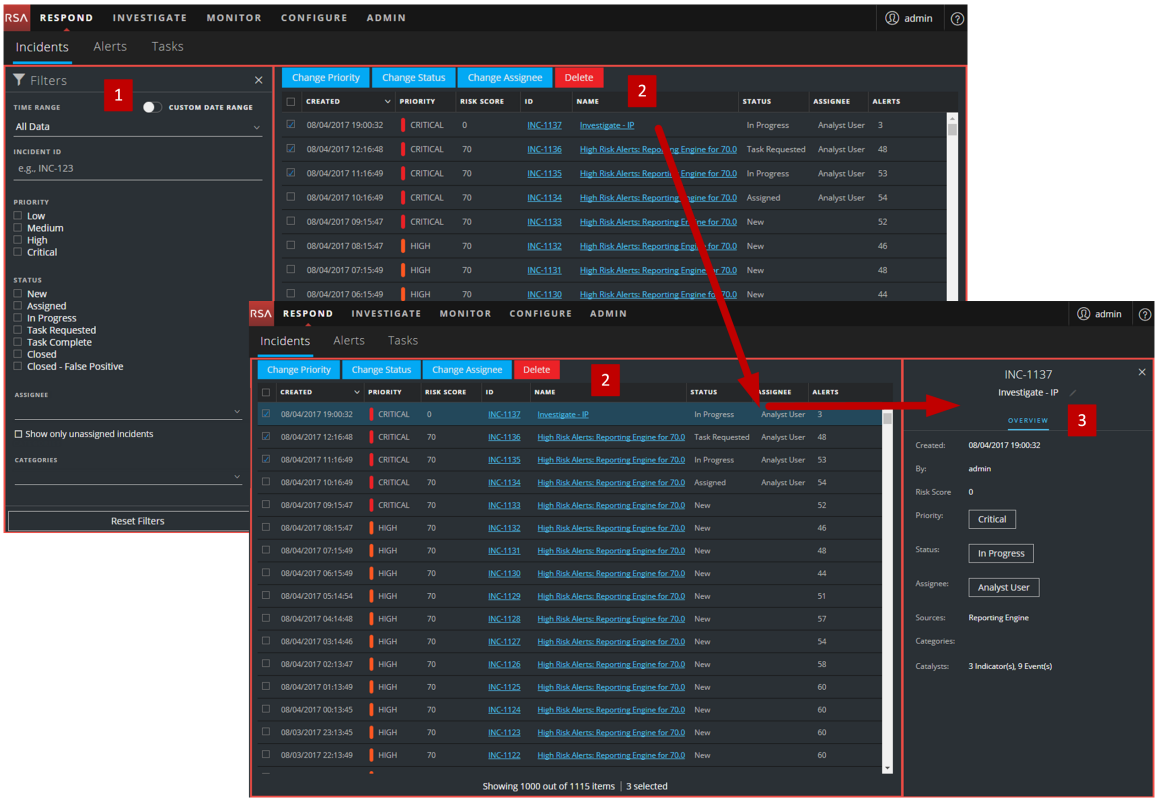
*You can complete these tasks here (that is in the Incidents List view).

Related Topics

- Incident Details View
- Responding to Incidents

Quick Look

The following example shows the initial Incidents List view with the Filter panel. You can open the Overview panel for an incident by clicking an incident in the Incident List.



1 Filters Panel

2 Incidents List

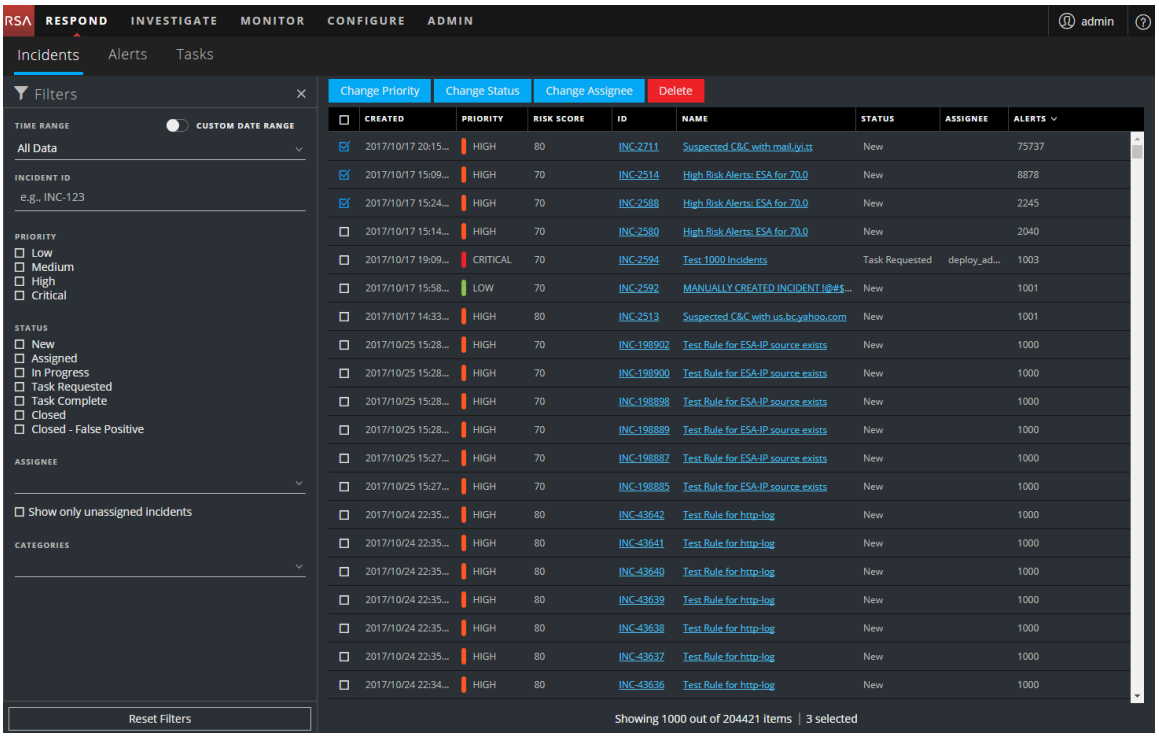
3 Overview Panel

You can go directly to the Incident Details view from the Incidents List by clicking the hyperlinked ID or NAME. The Overview panel is also available in the Incident Details view. For more information about the Incidents Details view, see Incident Details View.

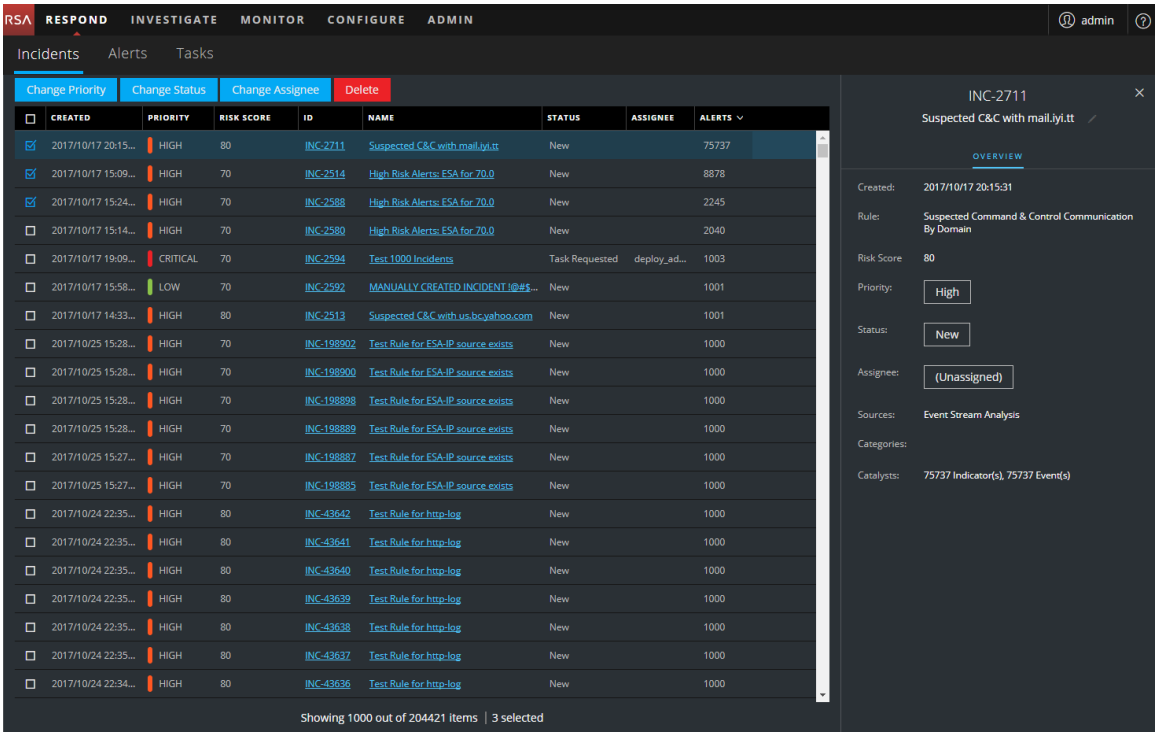
Incidents List View

To access the Incidents List view, go to **RESPOND > Incidents**. The Incidents List view displays a list of all incidents. The Incidents List view consists of a Filters panel, an Incidents List, and an Incidents Overview panel.

The following figure shows the Filter Panel on the left and the Incidents List on the right.

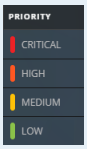


The following figure shows the Incidents List on the left and the Incidents Overview panel on the right.



Incidents List

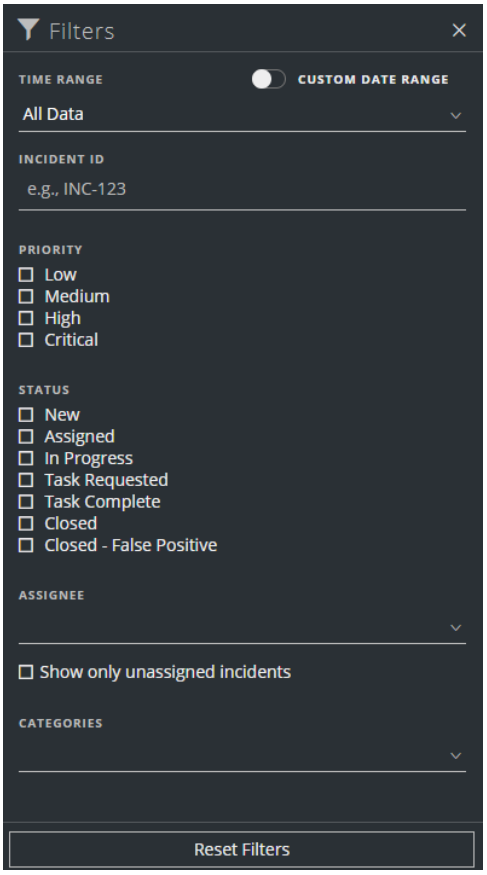
The Incidents List shows a list of all of the prioritized incidents. You can filter this list to show only incidents of interest.

Column	Description
CREATED	Shows the creation date of the incident.
PRIORITY	Shows the incident priority. Priority can be Critical, High, Medium or Low. The Priority is color coded, where red indicates a **Critical** incident, orange represents a **High** risk incident, yellow indicates a **Medium** risk incident, and green represents a **Low** risk incident. For example: 
RISK SCORE	Shows the incident risk score. The risk score indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
ID	Shows the automatically created incident number. Each incident is assigned a unique number that you can use to track the incident.
NAME	Shows the incident name. The incident name is derived from the rule used to trigger the incident. Click the link to go to the Incident Details view for the selected incident.
STATUS	Shows the incident status. The status can be: New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed-False Positive.
ASSIGNEE	Shows the team member currently assigned to the incident.
ALERTS	Shows the number of alerts associated with the incident. An incident may include many alerts. A large number of alerts might mean that you are experiencing a large-scale attack.

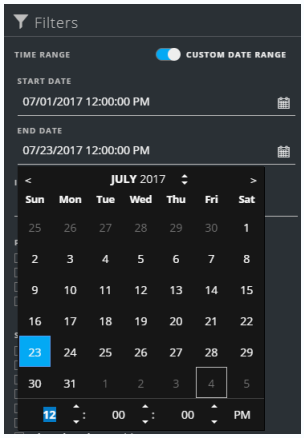
At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number of incidents selected. For example: **Showing 1000 out of 2517 items | 2 selected**. The maximum number of incidents that you can view at one time is 1,000.

Filters Panel

The following figure shows the filters available in the Filters panel.



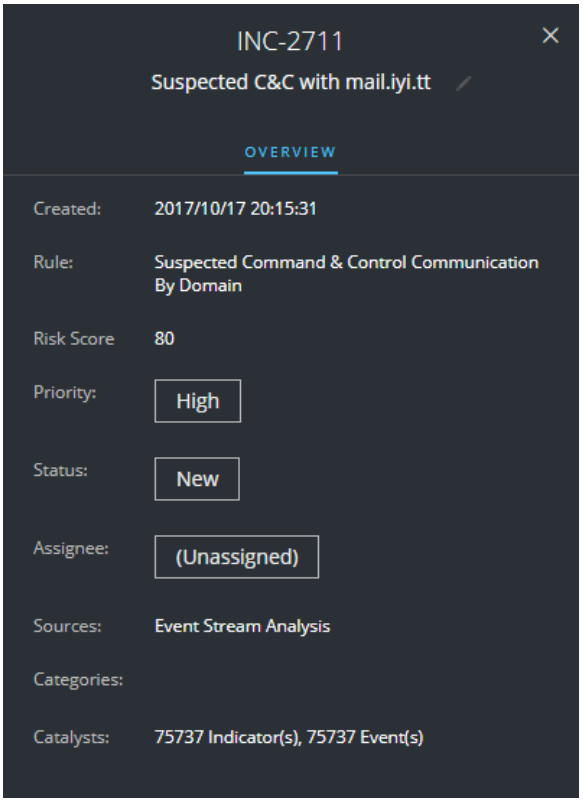
The Filters panel, on the left of the Incidents List view, has options that you can use to filter the incidents list. When you navigate away from the Filters panel, the Incidents List view retains your filter selections.

Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the received date of the alerts. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
CUSTOM DATE RANGE	You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar. 
INCIDENT ID	You can type the Incident ID for an incident you would like to locate, for example INC-1050.
PRIORITY	Select the priorities that you would like to view.
STATUS	Select one or more incident statuses. For example, select Closed - False Positive to view only false positive incidents, which were initially identified as suspicious, but then they were later found to be safe.

Option	Description
ASSIGNEE	Select the assignee or assignees of the incidents that you would like to view. For example, if you only want to view the incidents assigned to Cale or Stanley, select Cale and Stanley from the Assignee drop-down list. If you want to view incidents regardless of the assignee, do not make a selection under Assignee. (Available in version 11.1 and Later) To view only unassigned incidents, select **Show only unassigned incidents**.
CATEGORIES	Select one or more categories from the drop-down list. For example, if you only want to view incidents classified with the Backdoor or Privilege abuse categories, select Backdoor and Privilege abuse.
Reset Filters	Removes your filter selections.

Overview Panel

The Overview panel shows basic summary information about a selected incident. From the Incidents List, you can click an incident to access the Overview panel. The Overview panel in the Incident Details view contains the same information.



The following table lists the fields displayed in the Incident Overview panel.

Field	Description
<Incident ID>	Displays the Incident ID.
<Incident Name>	Displays the name of the incident. You can click the incident name to change it. For example, rules can create many incidents with the same name. You can change the incident names to be more specific.
Created	Shows the creation date and time of the incident.
Rule / By	Shows the name of the rule that created the incident or the name of the person who created the incident.
RiskScore	Indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
Priority	Shows the incident priority. Priority can be Critical, High, Medium or Low. To change the priority, you can click the Priority button and select a new priority from the drop-down list.
Status	Shows the incident status. The status can be New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive. To change the status, you can click the Status button and select a new status from the drop-down list.
Assignee	Shows the team member currently assigned to the incident. To change the assignee you can click the Assignee button and select a new assignee from the drop-down list.
Sources	Displays the data sources used to locate the suspicious activity.
Categories	Displays the categories of the incident events.
Catalysts	Displays the count of indicators that gave rise to the incident.

Toolbar Actions

This table lists the toolbar actions available in the Incidents List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the alerts that you would like to see in the Alerts List.
	Closes the panel.
Change Priority button	Allows you to change the Priority of one or more selected incidents in the Incidents List.
Change Status button	Allows you to change the Status of one or more selected incidents.
Change Assignee button	Allows you to change the Assignee of one or more selected incidents.
Delete button	Allows you to delete the selected incidents if you have the appropriate permissions, such as an Administrator or Data Privacy Officer.

Incident Details View

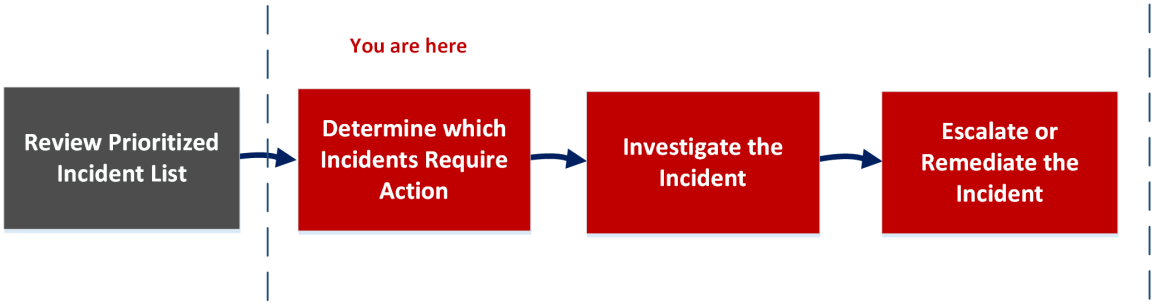
In the Incident Details view (RESPOND > Incidents > click an ID or NAME hyperlink in the Incidents List), you can view and access extensive incident details. The Incident Details view contains multiple panels that provide the following benefits:

- **Overview**: View an incident summary and update the incident.
- **Indicators**: View the indicators (alerts) involved in the incident, the events within those alerts, and available enrichment information.
- **Nodal Graph**: Visualize the size and interactions between entities (IP address, MAC address, user, host, domain, file name, or file hash).
- **Events Datasheet**: Study the events associated with the incident.
- **Journal**: Add notes and collaborate with other analysts.
- **Tasks**: Create incident tasks and track them to closure.
- **Related Indicators**: View indicators (alerts) that are related to the incident and add them to the incident if they are not associated with an incident.

You can also filter the data in the Incident Details view to study indicators and entities of interest.

Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



In the Incident Details view, you can use the extensive information provided about the incidents to determine which incidents require action. You also have the tools and information to investigate the incident, and then escalate or remediate it.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, and SOC Manager	View prioritized incidents, filter and sort the incident list, find incidents, view my incidents, and assign incidents to myself.	Review Prioritized Incident List
Incident Responders, Analysts	View incident details.*	View Incident Details
Incident Responders, Analysts	View alerts and enrichments.*	View the Indicators and Enrichments
Incident Responders, Analysts	View events.*	View and Study the Events
Incident Responders, Analysts	View a graph of the entities involved in the events.*	View and Study the Entities Involved in the Events
Incident Responders, Analysts	Filter the incident data.*	Filter the Data in the Incident Details View
Incident Responders, Analysts	View and add incident notes.*	View Incident Notes and Document Steps Taken Outside of NetWitness
Incident Responders, Analysts	View and create tasks.*	View the Tasks associated with an Incident and Create a Task
Incident Responders, Analysts	Add related alerts and add them to the incident.*	Find Related Indicators and Add Related Indicators to the Incident
Incident Responders, Analysts	View contextual information about an incident from Context Hub.*	View Contextual Information

Role	I want to ...	Show me how
Incident Responders, Analysts	Reduce false positives by adding an entity to the whitelist.*	Add an Entity to a Whitelist
Incident Responders, Analysts	Pivot to Investigation.*	Pivot to Investigate
Incident Responders, Analysts	Pivot to NetWitness Endpoint.*	Pivot to NetWitness Endpoint
Incident Responders, Analysts	Update or close an incident.*	Update an Incident and Close an Incident
Incident Responders, Analysts, and SOC Manager	View all tasks.	Escalate or Remediate the Incident
Incident Responders, Analysts, and SOC Manager	Bulk update incidents and tasks.	Escalate or Remediate the Incident

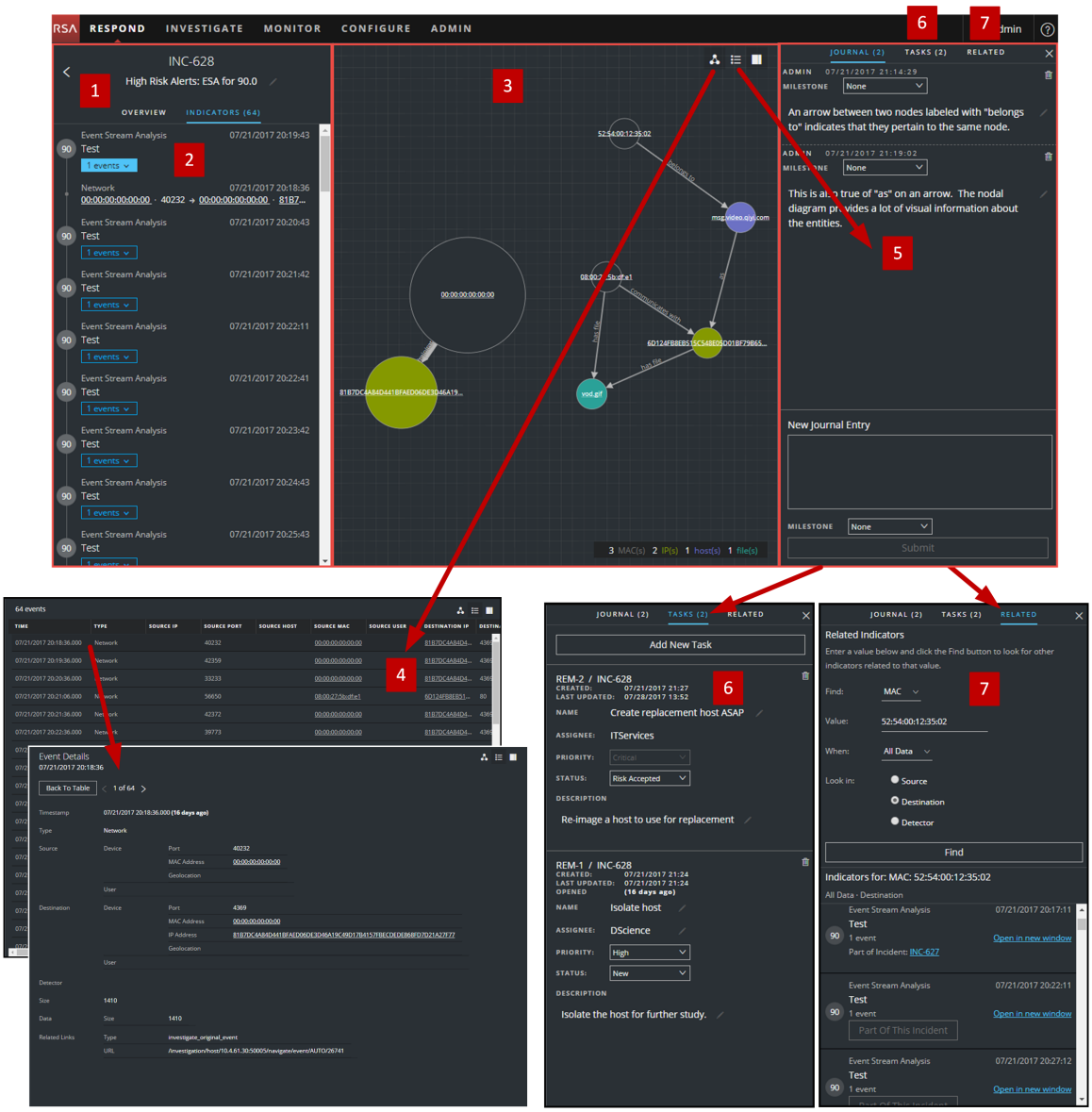
*You can complete these tasks here (that is in the Incident Details view).

Related Topics

- Incidents List View
- Determine which Incidents Require Action
- Investigate the Incident
- Escalate or Remediate the Incident

Quick Look

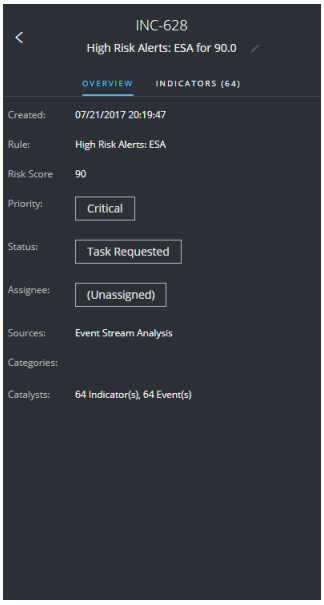
The following example shows the locations of the Incident Details view panels.



1	Overview Panel (Click the OVERVIEW tab to view it.)
2	Indicators Panel
3	Nodal Graph
4	Events Datasheet (Click an event in the Events List to view Event Details.).
5	Journal Panel
6	Tasks Panel (Click the TASKS tab to view it.)
7	Related Indicators Panel (Click the RELATED tab to view it.)

Overview Panel

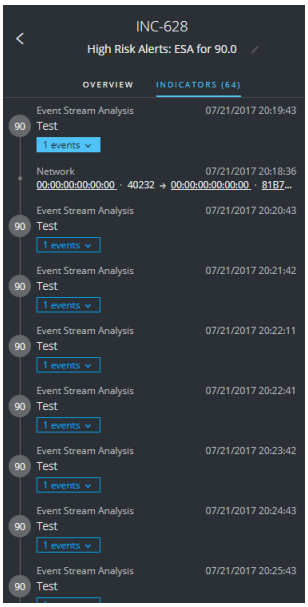
The Overview panel shows basic summary information about a selected incident. It also allows you to change the incident name and update the incident priority, status, and assignee. The Overview panel in the Incidents List view contains the same information. The Incidents List view Overview Panel topic provides details.



Indicators Panel

The Indicators panel contains a chronological listing of indicators. *Indicators* are alerts, such as an ESA alert or a NetWitness Endpoint alert. (This is different than a timeline, which provides a visual representation of the timing of the events in the incident). This listing helps you to connect indicators and notable data. For example, an IP address connected to a command and communication ESA alert might also have triggered a NetWitness Endpoint alert or other suspicious activities.

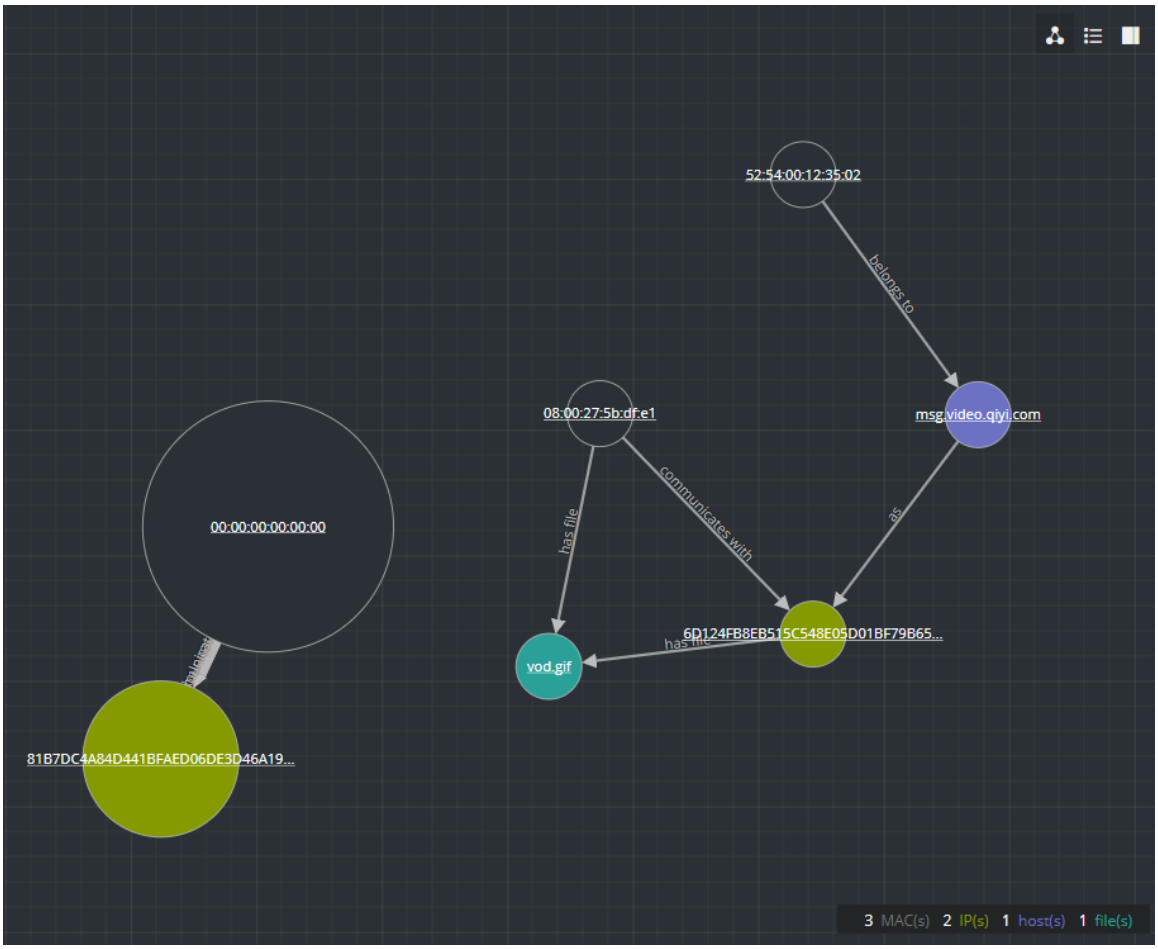
To view the Indicators panel, in the left panel of the Incident Details view, select **INDICATORS**.



Data source information is shown below the names of the indicators. You can also see the creation date and time of the indicator and the number of events in the indicator.

Nodal Graph

The nodal graph is an interactive graph that shows the entities involved in the incident. An *Entity* is a specified piece of meta, such as IP address, MAC address, user, host, domain, file name, or file hash.



Nodes

In the nodal graph, circles represent nodes. The following table describes the nodal graph node types.

Node	Description
IP address	If the event is a detected anomaly, you can see a Detector IP. If the event is a transaction, you can see a Destination IP and a Source IP.
MAC address	You may see a MAC address for each type of IP address.
User	If the machine is associated with a user, you can see a user node.
Host	A host can be physical equipment or a virtual machine, designated by a Fully Qualified Domain Name (FQDN) or IP address, on which any service is installed.

Node	Description
Domain	
Filename	If the event involves files, you can see a filename.
File Hash	If the event involves files, you may see a file hash.

The legend at the bottom of the nodal graph shows the number of nodes of each type and the color coding of the nodes. It also helps you to locate the entities when the values, such as the IP addresses, are hashed.

You can click any node and drag it to reposition it.

Arrows

The arrows between the nodes provide additional information about the entity relationships. The following table describes the nodal graph arrow types.

Arrow	Description
Communicates with	An arrow between a Source machine node (IP address or MAC address) and a Destination machine node labeled with "communicates with" shows the direction of the communication.
As	An arrow between nodes labeled with "as" provides additional information about the IP address that the arrow points to. For example, if there is an arrow from the host node circle that points to an IP address node that is labeled with "as", it indicates that the name on the host node circle is the hostname of that IP address and is not a different entity.
Has file	An Arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has" indicates that the IP address has that file.
Uses	An arrow between a User node and a machine node (IP address, MAC address, or Host) labeled with "uses" shows the machine that the user was using during the event.
Is named	An arrow from a File Hash node to a File Name node labeled with "is named" indicates that the file hash corresponds to a file with that name.

Arrow	Description
Belongs to	An arrow between two nodes labeled with "belongs to" indicates that they pertain to the same node. For example, an arrow between a MAC address and a Host labeled with "belongs to" indicates that it is the MAC address of the host.

Larger line size arrows indicate more communication between the nodes. Larger nodes (circles) indicate more activity than smaller nodes. The larger nodes are the most common entities mentioned in the events.

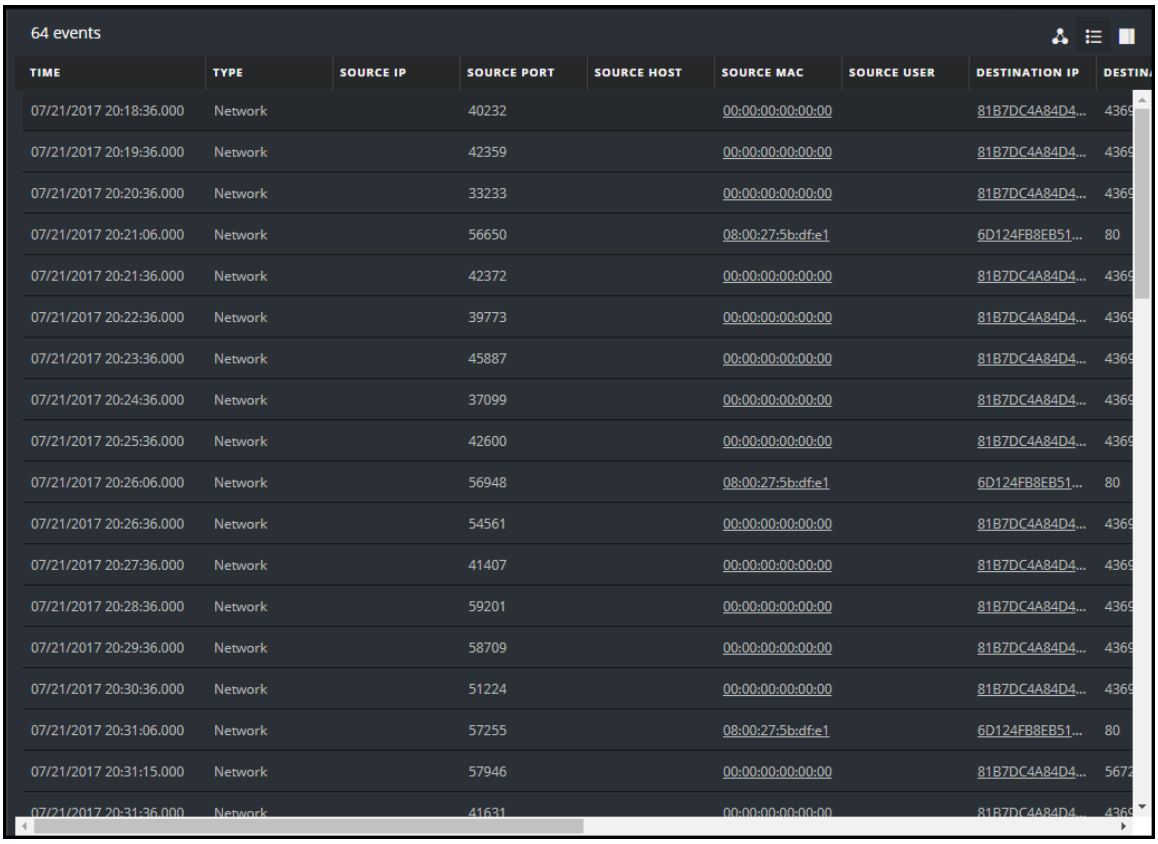
Events Datasheet

The Events datasheet shows the events associated with the incident. It shows information about the events, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

The Events datasheet shows an Events List for multiple events or Event Details for a single event.

Events List

The following figure shows the Events List.



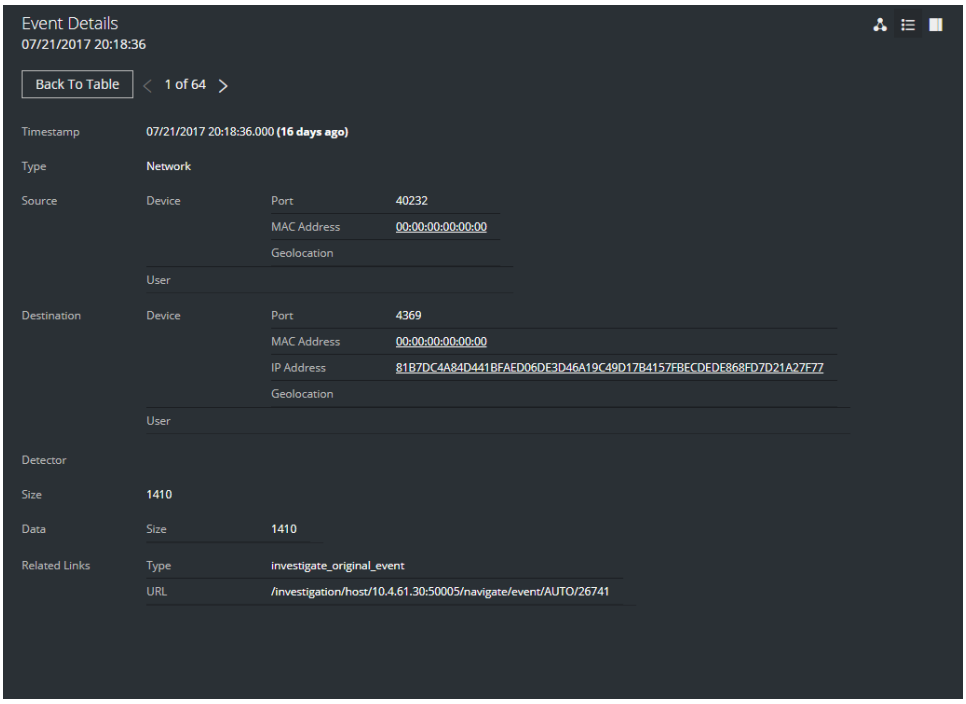
The following table describes the columns in the Events list.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
SOURCE PORT	Shows the source port of the transaction. The source and destination ports can be on the same IP address.
SOURCE HOST	Shows the destination host where the event took place.
SOURCE MAC	Shows the MAC address of the source machine.
SOURCE USER	Shows the user of the source machine.

Column	Description
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DESTINATION PORT	Shows the destination port of the transaction. The source and destination ports can be on the same IP address.
DESTINATION HOST	Shows the HOST name of the destination machine.
DESTINATION MAC	Shows the MAC address of the destination machine.
DESTINATION USER	Shows the user of the destination machine.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

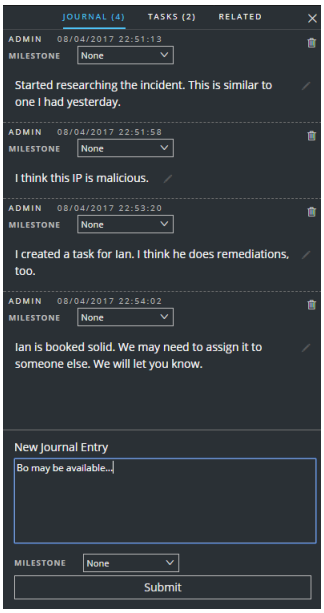
Event Details

To view the event details, you click an event in the event list. If there is only one event in the list, you will see the event details for that event instead of a list.



Journal Panel

The incident Journal shows the history of activity on your incident.

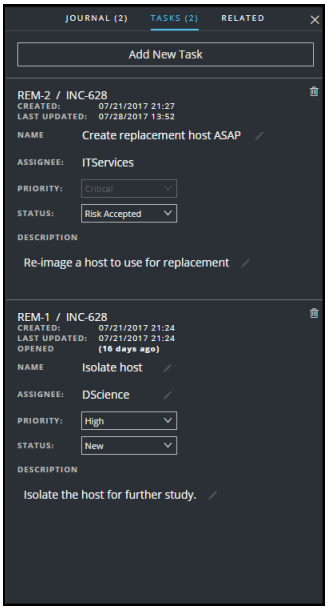


The following table describes the New Journal Entry options.

Field	Description
New Journal Entry	Type your note in the field.
Milestone	(Optional) Select a milestone, if applicable. This field is used to track significant events for the incident.
Submit button	Click submit to add an entry to the journal. You journal entry will be visible to anyone who views the incident.

Tasks Panel

In the Tasks panel, you can manage and track the incident tasks to closure.



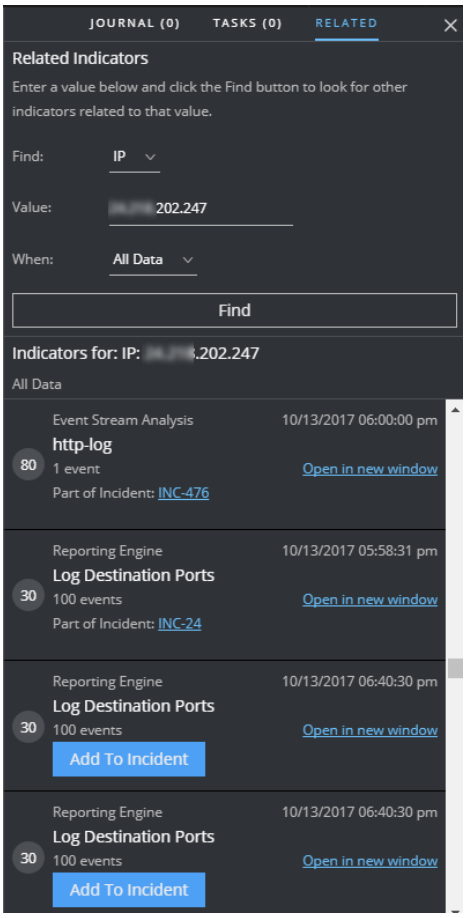
The following table describes the Task fields.

Field	Description
<Task ID / <Incident ID>	The autogenerated Task ID / The incident associated with the task.
CREATED	The created date of the task.
LAST UPDATED	The date that the task was last modified.
OPENED	The time that passed since the task was opened. For example, 3 minutes ago or 2 days ago.

Field	Description
NAME	The name of the task. For example: Re-image the machine. You can click this field to edit it.
ASSIGNEE	The username of the user assigned to the task. You can click this field to edit it.
PRIORITY	The priority of the task: Low, Medium, High, or Critical. You can click the priority button and select a new priority for the task from the drop-down list.
STATUS	The status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. You can click the status button and select a new status for the task from the drop-down list.
DESCRIPTION	Type information that describes the task. You may want to include any applicable reference numbers. You can click this field to edit it.

Related Indicators Panel

The Related Indicators panel enables you to search the NetWitness Suite alerts database to find alerts that are related to this incident. You can add alerts that you find to the incident if they are not already associated with an incident.



The following table describes the fields in the search section at the top of the panel.

Field	Description
Find	Select the entity that you would like to locate in the alerts. For example, IP.
Value	Type the value of the entity. For example, type the actual IP address of the entity.
When	Select a time range to search for the alerts. For example, Last 24 hours.
Find button	Initiates the search. A list of related indicators appear below the **Find** button in the **Indicators for** section.

The following table describes the options in the **Indicators for** (results) section at the bottom of the panel.

Option	Description
Indicators For:	Shows the search results.

Option	Description
Open in new window link	Shows alert details for the indicator.
Add To Incident button	Adds the related indicator to the incident. The related indicator adds to the Indicators panel.
Part Of This Incident button	Shows that the indicator is already part of the incident.

Toolbar Actions

Option	Description
	(Back to Incidents) Enables you to navigate back to the Incidents List view.
	Closes the panel.
	Deletes the entry, such as a journal entry or task.
Priority button	(In the Overview panel) Allows you to change the Priority of one or more selected incidents in the Incidents List.
Status button	(In the Overview panel) Allows you to change the Status of one or more selected incidents.
Assignee button	(In the Overview panel) Allows you to change the Assignee of one or more selected incidents.
(View: Graph)	Enables you to view the Nodal Graph.

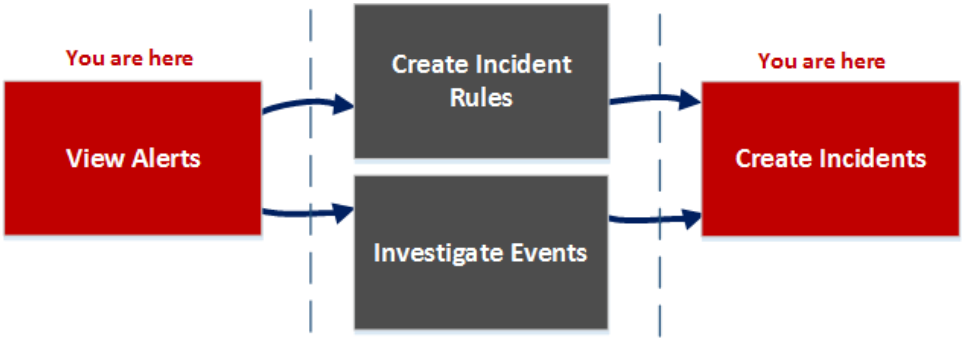
Option	Description
(View: Datasheet)	Enables you to view the Events datasheet, which can appear as an Events List for multiple events or Event Details for a single event.
(Journal, Tasks, and Related)	Enables you to view the Journal, Tasks, and Related Indicators panels.

Alerts List View

The Alerts List view (RESPOND > Alerts) enables you to view all of the threat alerts and indicators received by NetWitness Suite in one location. This can include alerts received from ESA Correlation Rules, ESA Analytics, Malware Analysis, Reporting Engine, NetWitness Endpoint, as well as many others. In the Alerts List view you can browse through various alerts, filter them, and group them to create incidents.

Workflow

This workflow shows the high-level process that Analysts use to review alerts and create incidents.



In the Alerts List view, you can review a list of alerts from all sources received by NetWitness Suite. After that, you can investigate those alerts further and create incidents from the alerts or you can create incident rules to create incidents.

Note: You can use NetWitness Suite Automated Threat Detection to create incidents without manually creating rules.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	View all alerts in NetWitness Suite.*	View Alerts
Incident Responders, Analysts	Filter alerts.*	Filter the Alerts List

Role	I want to ...	Show me how
Incident Responders, Analysts	View alert overview information and raw alert metadata.*	View Alert Summary Information
Incident Responders, Analysts	Create incidents from alerts.*	Create an Incident Manually
Incident Responders, Analysts	(Available in version 11.1 and Later) Add alerts to an existing incident.*	Add Alerts to an Incident
Administrators, Data Privacy Officers	Delete alerts.*	Delete Alerts
SOC Managers, Administrators	Create incident rules.	See "Create an Incident Rule for Alerts" in the *NetWitness Respond Configuration Guide*.
Incident Responders, Analysts	Investigate the events in an alert.	View Event Details for an Alert and Investigate Events
Incident Responders, Analysts	Add related alerts to an existing incident.	Add Related Indicators to the Incident

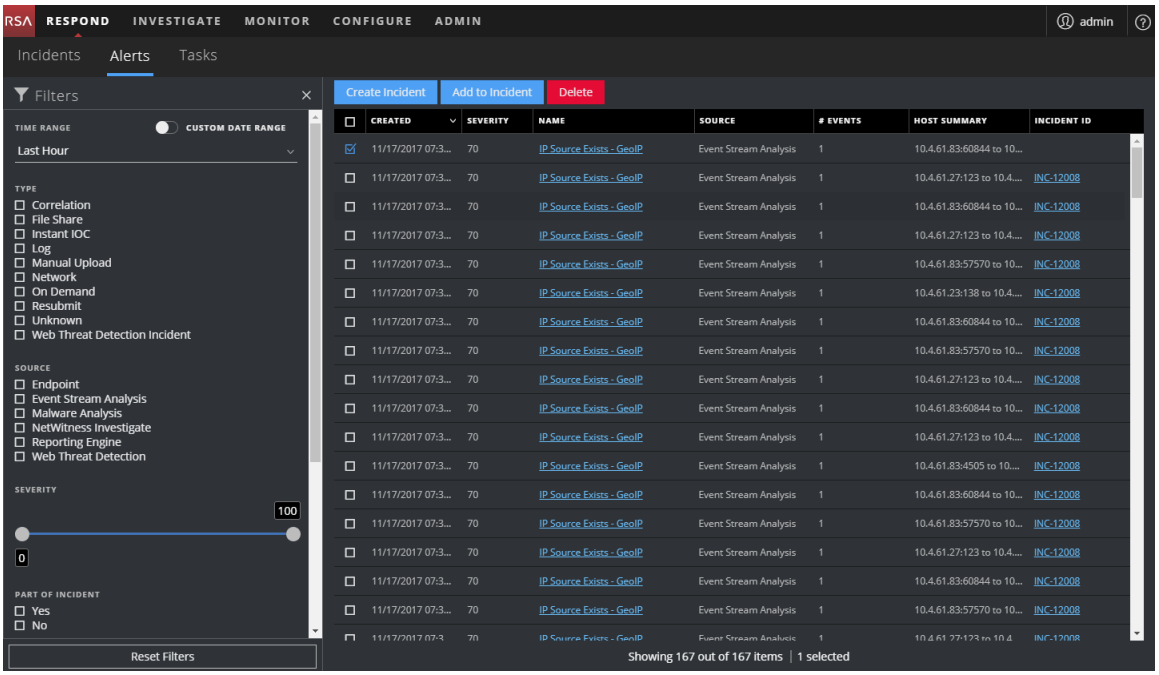
*You can complete these tasks here (that is in the Alerts List view).

Related Topics

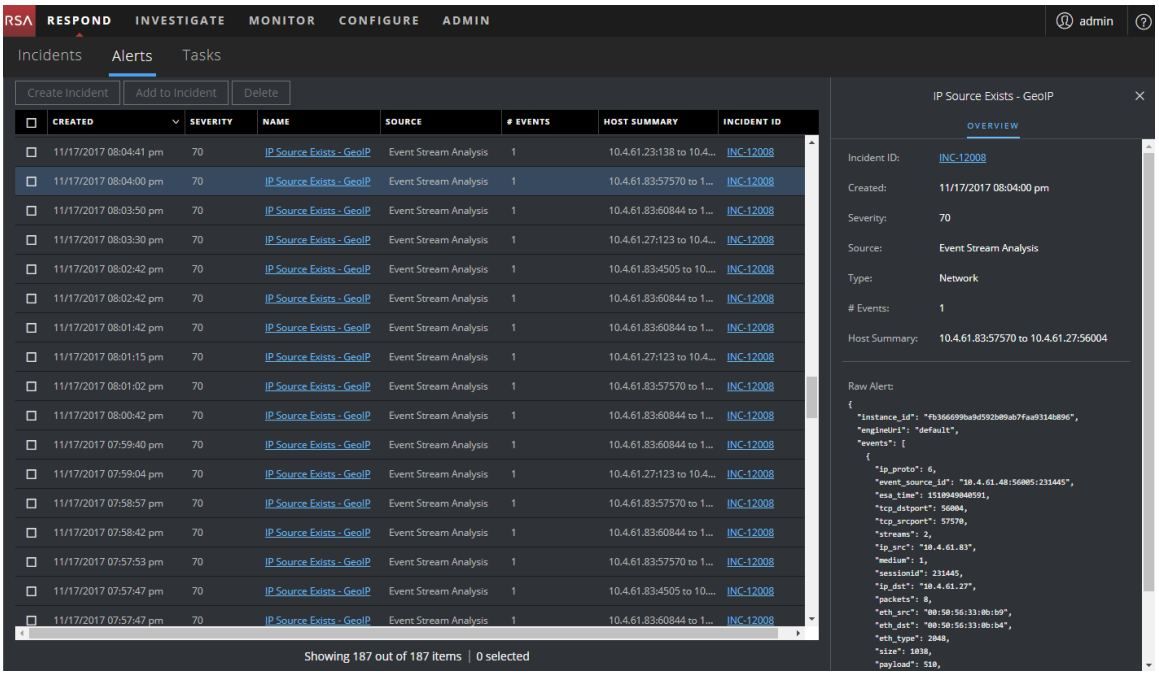
- Alert Details View
- Reviewing Alerts

Alerts List View

To access the Alerts List view, go to **RESPOND > Alerts**. The Alerts List view displays a list of all alerts and indicators received by the Respond Server database in NetWitness Suite. The following figure shows the Filters panel on the left.

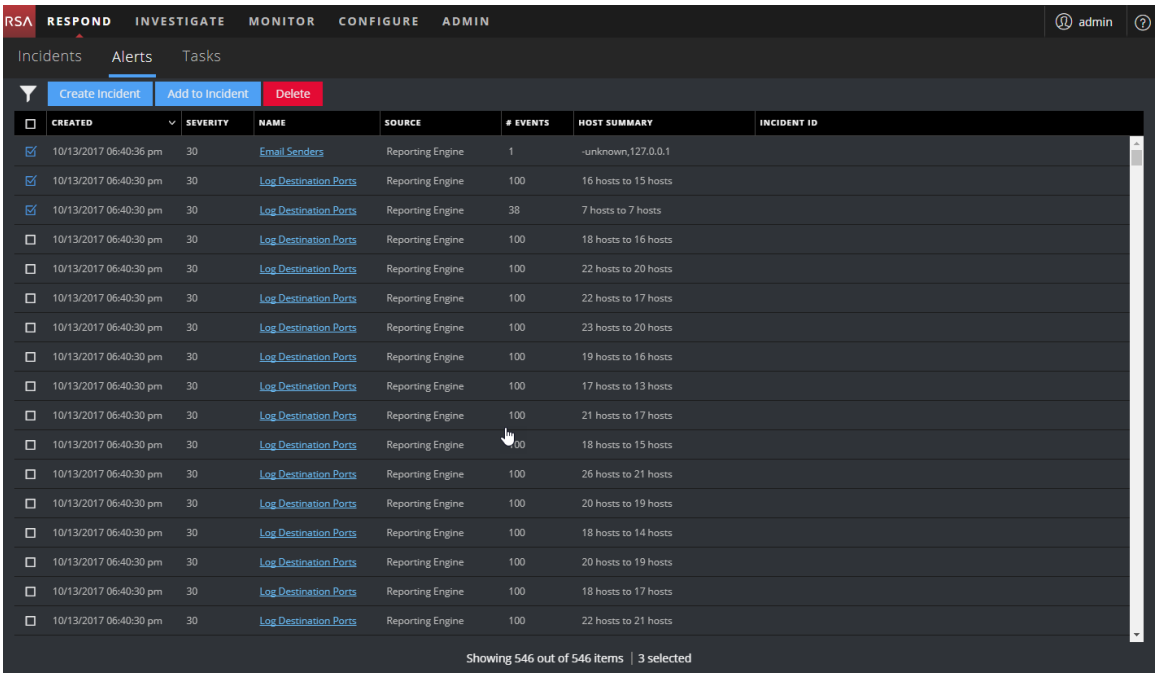


The Alerts List view consists of a Filters panel, an Alerts List, and an Alert Overview panel. You can click an alert in the Alerts list to view the Alert Overview panel on the right.



Alerts List

The Alerts List shows all of the alerts in NetWitness Suite. You can filter this list to only show alerts of interest.



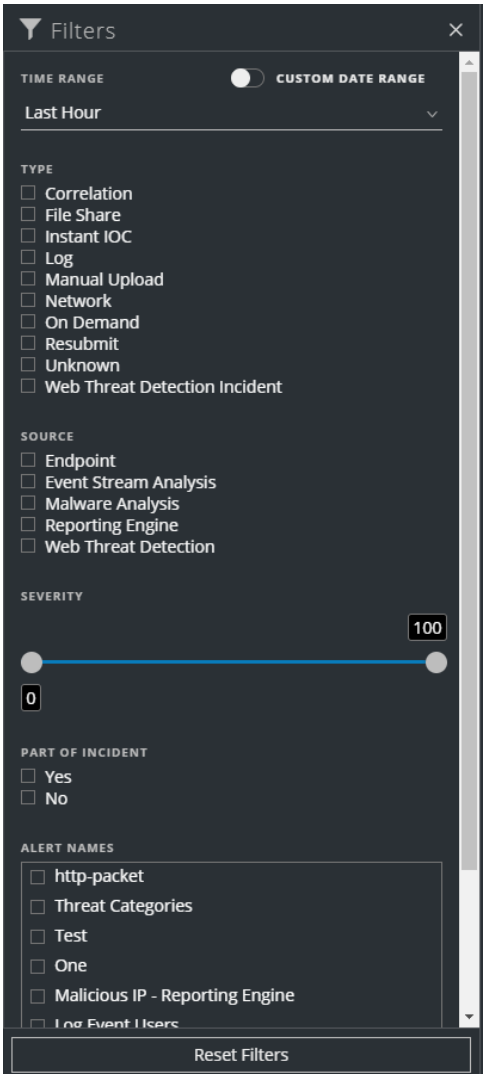
Column	Description
	Enables you to select one or more alerts to delete. Users with the appropriate permissions, such as Administrators and Data Privacy Officers, can delete alerts.
CREATED	Displays the date and time when the alert was recorded in the source system.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.
NAME	Displays a basic description of the alert.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, ESA correlation rules, ESA Analytics, Reporting Engine, and many others.
# EVENTS	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.

Column	Description
HOST SUMMARY	Displays details of the host like the host name from where the alert was triggered. The details may include information about the source and destination hosts in an Alert. Some alerts may describe events across more than one host .
INCIDENT ID	Shows the Incident ID of the alert. If there is no incident ID, the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.

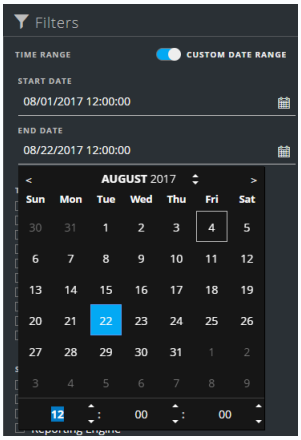
At the bottom of the list, you can see the number of alerts on the current page, the total number of alerts, and the number of alerts selected. For example: **Showing 377 out of 377 items | 3 selected**

Filters Panel

The following figure shows the filters available in the Filters panel.



The Filters panel, on the left of the Alerts List view, has options that you can use to filter the alerts list. When you navigate away from the Filters panel, the Alerts List view retains your filter selections.

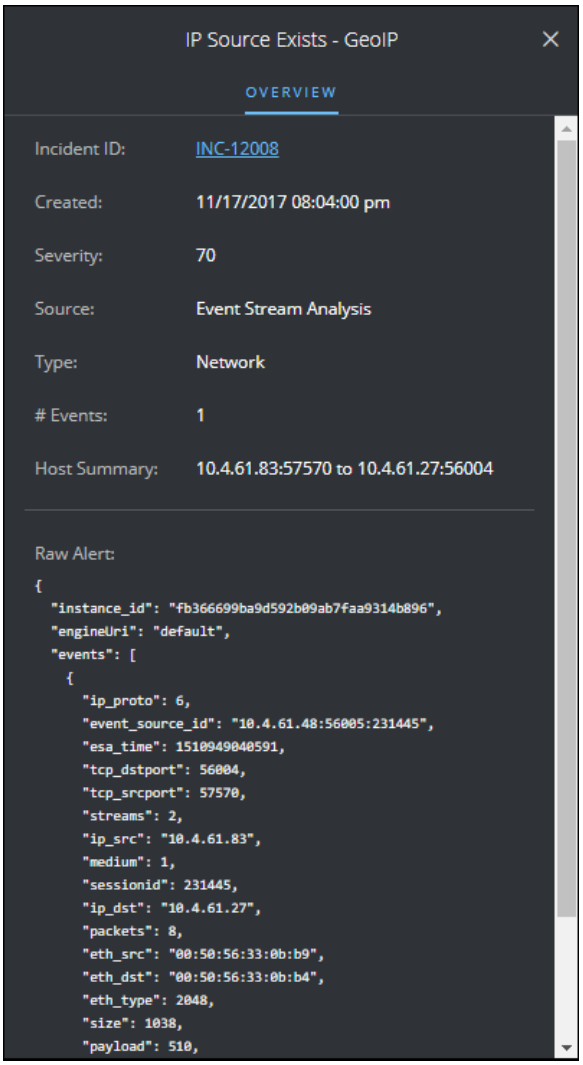
Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the received date of the alerts. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
CUSTOM DATE RANGE	You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar. 
TYPE	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection, and many others.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.

Option	Description
PART OF INCIDENT	Categorizes alerts on whether or not they are associated with an incident. Select **Yes** to view alerts that are part of an incident. Select **No** to view alerts that are not part of an incident. For example, before you create incidents from alerts, you may want to select No to view only those alerts that are not already part of an incident.
ALERT NAMES	Shows the name of the alert. You can use this filter to search for all alerts generated by a specific rule or source, for example, Malicious IP - Reporting Engine.
Reset Filters	Removes your filter selections.

The Alerts List shows a list of alerts that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the alerts list. For example: **Showing 30 out of 30 items**

Overview Panel

The Overview panel shows basic summary information about a selected alert and raw alert metadata. The Overview panel in the Alert Details view contains the same information, but in the Alerts Details view, you can expand the panel to view more information.



The following table lists the fields displayed in the Alert Overview panel.

Field	Description
<Alert Name>	Displays the name of the alert.
Incident ID	Displays the Incident ID associated with the alert. You can click the incident ID link to go to the Incident Details view of the associated incident. If there is no incident ID, the alert does not belong to an incident. You can create an incident for this alert or you can add it to an incident.
Created	Displays the date and time when the alert was created.

Field	Description
Severity	Displays the level of severity of the alert. The values are from 1 through 100.
Source	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, ESA correlation rules, ESA Analytics, Reporting Engine, and many others.
Type	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
# Events	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.
Raw Alert	Shows the raw alert metadata.

Toolbar Actions

This table lists the toolbar actions available in the Alerts List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the alerts that you would like to see in the Alerts List.
	Closes the panel.
Create Incident button	Enables you to create incidents from alerts. The alerts cannot be part of an incident. To get a list of alerts without incidents, you can filter the Alerts List, In the PART OF INCIDENT section, select No.
Add to Incident button	(This option is available in version 11.1 and later.) Enables you to add selected alerts to an incident. The alerts cannot be part of an incident. To get a list of alerts without incidents, you can filter the Alerts List. In the PART OF INCIDENT section, select No.
Delete button	Allows you to delete alerts.

Alert Details View

In the Alert Details view (RESPOND >Alerts > click a NAME hyperlink in the Alerts List), you can view summary information about an alert, such as the source of the alert, the number of events within the alert, and whether it is part of an incident. You can also view detailed information about the events within the alert as well as the event metadata.

Workflow

This workflow shows the high-level process that Analysts use to review alerts and create incidents.

After reviewing the alerts list, in the Alert Details view, you can investigate those alerts further and create incidents from the alerts. In the CONFIGURE > Incident Rules view, you can create incident rules to create incidents.

Note: You can also use NetWitness Suite Automated Threat Detection to create incidents without manually creating rules.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	View all alerts in NetWitness Suite.	View Alerts
SOC Managers, Administrators	Create incident rules.	See "Create an Incident Rule for Alerts" in the *NetWitness Respond Configuration Guide*.

Role	I want to ...	Show me how
Incident Responders, Analysts	View a list of events in the alert.*	View Event Details for an Alert
Incident Responders, Analysts	View event metadata for each event in the alert.*	View Event Details for an Alert
Incident Responders, Analysts	Further investigate the events in the alert.*	Investigate Events
Incident Responders, Analysts	Add alerts to an existing incident.	Add Alerts to an Incident Add Related Indicators to the Incident
Incident Responders, Analysts	Create incidents from alerts.	Create an Incident Manually
Data Privacy Officers, Administrators	Delete alerts.	Delete Alerts

*You can complete these tasks here (that is in the Alerts Details view).

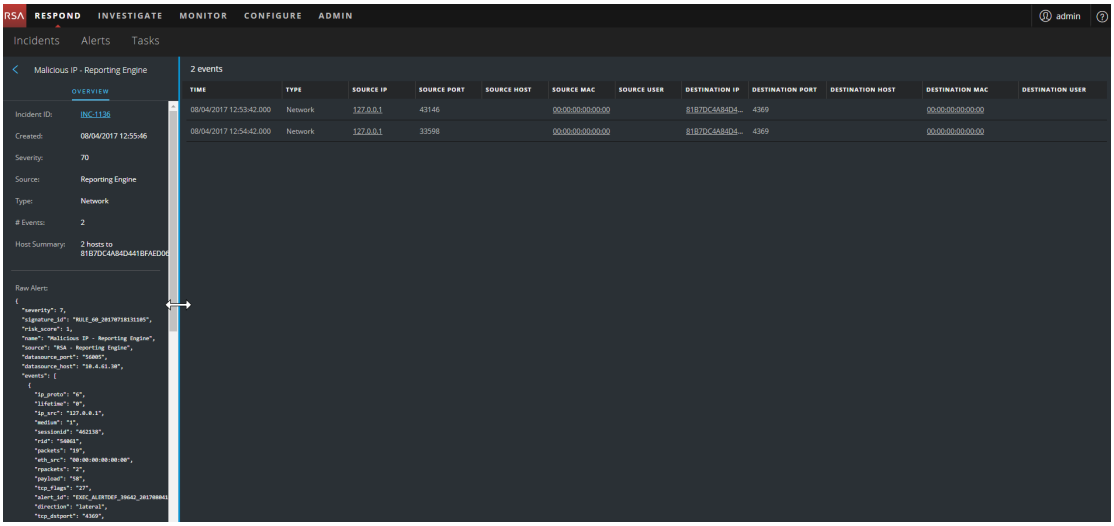
Related Topics

- Alerts List View
- Reviewing Alerts

Alert Details View

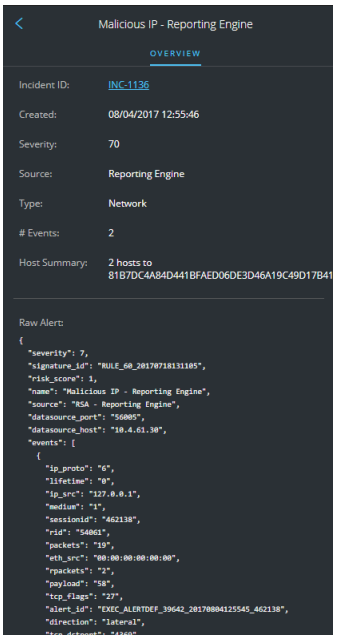
1. To access the Alert Details view, go to **RESPOND > Alerts**.
2. In the Alerts list, choose an alert to view and then click the link in the NAME column for that alert.
   The Alert Details view has an Overview panel on the left and the Events panel on the right.

You can resize the panels to show more information as shown in the following figure.



Overview Panel

The Overview panel shows basic summary information about a selected alert. The Overview panel on the Alerts List view contains the same information. The Alerts List view Overview Panel topic provides details.

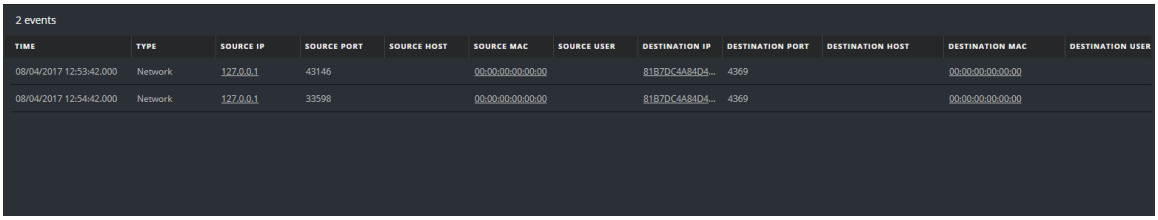


Events Panel

The Events panel can show an Events List if there is more than one event in the alert. If there is only one event in the alert, or you click an event in the Events List, you can see Event Details in the Events panel.

Events List

The Events List for a selected alert shows all of the events contained in that alert.

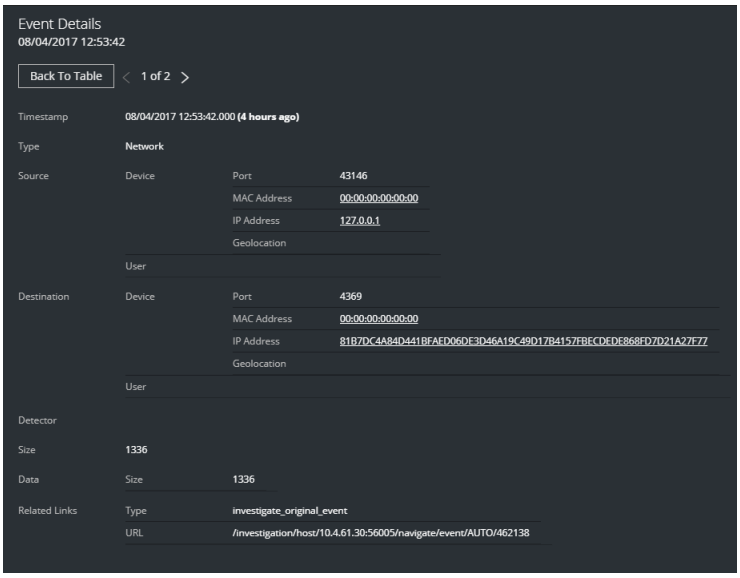


The following table lists some of the columns shown in the Events List, which provide a summary of the listed events.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
SOURCE USER	Shows the user of the source machine.
DESTINATION USER	Shows the user of the destination machine.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

Event Details

The Event Details in the Events panel shows the event metadata for each event in the alert.



Event Metadata

The following table lists some event metadata sections and subsections shown in the first two columns in the Event Details. This is not an extensive list.

Section	Subsection	Description
Data		Shows information about the data involved with the event, such as the files involved. There may be 0 or more per event.
	Filename	Shows the file name if a file is involved with the event.
	Hash	Shows a hash of the file contents, for example, MD5 or SHA1.
	Size	Shows the size of the transmission or file involved with the event.
Description		Displays a general description of the event.
Destination		Shows the destination device and user.
	Device	Shows information about the destination device. See Event Source or Destination Device Attributes below.
	User	Shows information about the user or users of the destinationSee Event Source or Destination User Attributes below.

Section	Subsection	Description
Detector		Shows the host or software product that detected the issue. This is most relevant for malware scanners and logs
	Device Class	Shows the device class of the product that detected the alert.
	IP Address	Shows the IP address of the product that detected the alert.
	Product Name	Shows the name of the product that detected the alert.
Domain		Shows the domain associated with the event.
Enrichment		Shows available enrichment information.
Related Links		If available, it shows a link back to the user interface (UI) of the source product.
	Type	Shows the type of event, such as investigate_original_event.
	URL	Shows the URL link back to the UI of the source product.
Size		Shows the size of the transmission or file involved.
Source		Shows the source device and user.
	Device	Shows information about the source machine. See Event Source or Destination Device Attributes below.
	User	Shows information about the user or users of the source machine. See Event Source or Destination User Attributes below.
Timestamp		Shows the time that the event occurred.
Type		Shows the type of the alert, such as log, network, correlation, Resubmit, Manual Upload, On Demand, File Share, or Instant IOC.

Event Source or Destination Device Attributes

The following table lists attributes for an event source or destination device that can be shown in the Events Details.

Name	Description
Asset Type	Displays the type of device, for example, desktop, laptop, server, network equipment, tablet, and so on.
BusinessUnit	Shows the business unit associated with the .
Compliance Rating	Shows the compliance rating of the device. It can be Low, Medium, or High.
Criticality	Shows how critical the device is to the business (business criticality).
Facility	Shows the location of the device.
Geolocation	Shows the geographic location for the host. It can contain the following attibutes: city, country, latitude, longitude, organization, and domain.
IP Address	Shows the IP address of the device.
MAC Address	Shows the MAC address of the device.
Netbios Name	Shows the NetBIOS name for the device.
Port	Displays the TCP port, UDP port, or the IP Src port (the first one available) used to connect to and from the host.

Event Source or Destination User Attributes

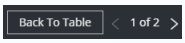
The following table lists attributes for an an event source or destination user that can be shown in the Events Details.

Attribute Name	Description
AD Domain	Shows the Active Directory domain.
AD Username	Shows the Active Directory username.

Attribute Name	Description
Email Address	Shows the email address of the user.
Username	Shows a general name if you do not know the source of the username, such as UNIX or a username in a particular system.

Toolbar Actions

This table lists the toolbar actions available in the Alert Details view.

Option	Description
	(Back to Alerts) Enables you to navigate back to the Alerts List .view.
	Click the arrows to navigate through the event meta details for each event in the alert. The numbers, such as "1 of 2" show the number of the event that you are currently viewing. Click **Back to Table** to go back to the Events List view, which is also known as the Events Table.

Tasks List View

After investigating incidents, in the Tasks List view (RESPOND > Tasks), you can create and track incident tasks. For example, you can create remediation tasks when you require actions on incidents from teams outside of your security operations. You can reference external ticket numbers within the tasks and then track those tasks to completion. You can also modify and delete tasks as required, depending on your user permissions.

What do you want to do?

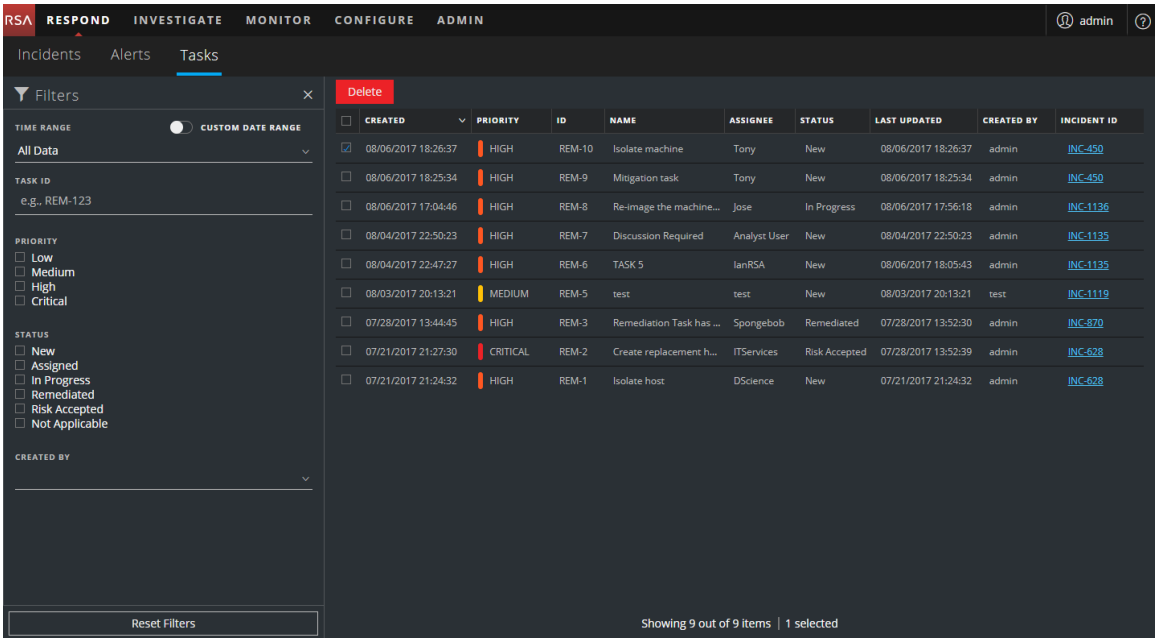
Role	I want to ...	Show me how
Incident Responders, Analysts	View tasks	View All Incident Tasks and View the Tasks associated with an Incident
Incident Responders, Analysts	Filter tasks.	Filter the Tasks List
Incident Responders, Analysts	Create a task.	Create a Task
Incident Responders, Analysts	Find and modify tasks.	Find a Task and Modify a Task
Incident Responders, Analysts	Close a task (Change the Status to Remediated, Risk Accepted, or Not Applicable).	Modify a Task
Incident Responders, Analysts, SOC Managers	Delete a task.	Delete a Task

Related Topics

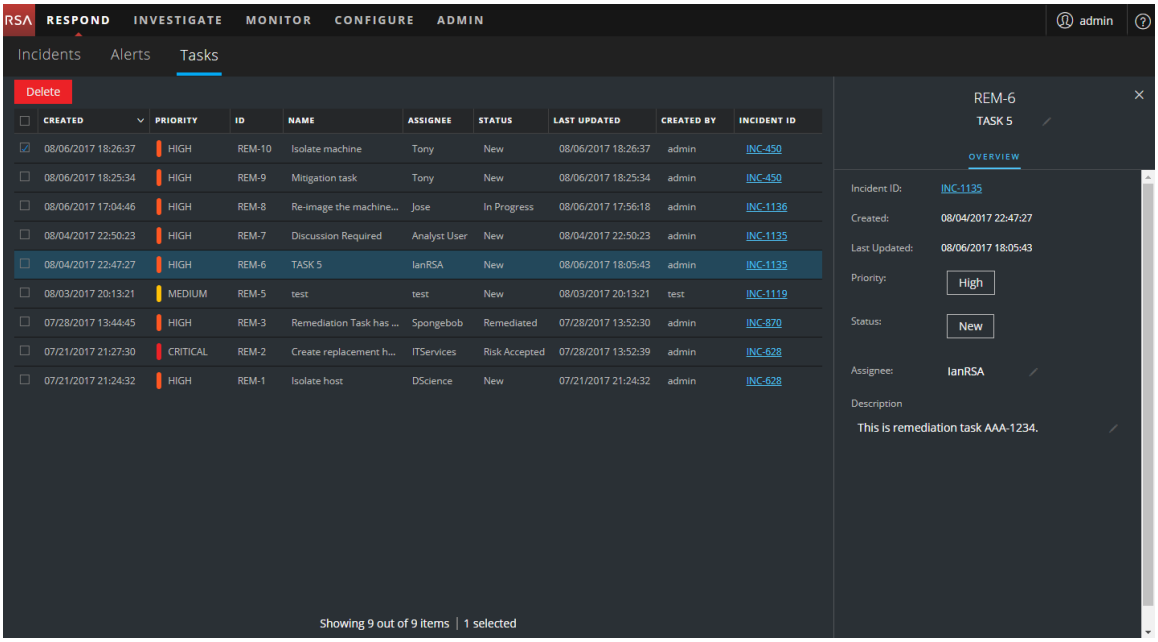
- Incident Details View
- Escalate or Remediate the Incident

Tasks List

To access the Tasks List view, go to **RESPOND > Tasks**. The Tasks List view displays a list of all incident tasks.

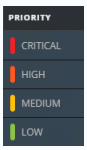


The Tasks List view consists of a Filters panel, a Tasks List, and a Task Overview panel. The following figure shows the Tasks List and the Overview panel.



Tasks List

The Tasks List shows all of the incident tasks. You can filter this list to show only tasks of interest.

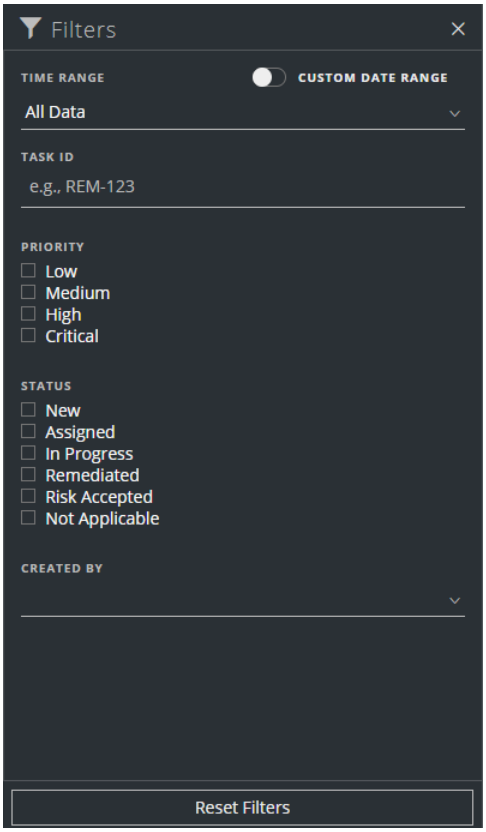
Column	Description
	Enables you to select one or more tasks to modify or delete. Users with the appropriate permissions can make bulk updates and delete tasks, such as SOC Managers. For example, an SOC Manager may want to assign multiple tasks to a user at the same time.
CREATED	Displays the date when the task was created.
PRIORITY	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates **Critical**, orange represents **High** risk, yellow indicates **Medium** risk, and green represents **Low** risk as shown in the following figure: 
ID	Displays the task ID.
NAME	Displays the task name.
ASSIGNEE	Displays the name of the user assigned to the task.
STATUS	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
LAST UPDATED	Displays the date and time when the task was last updated.
CREATED BY	Displays the user who created the task.

Column	Description
INCIDENT ID	Displays the incident ID for which the task was created. Click the ID to display the details of the incident.

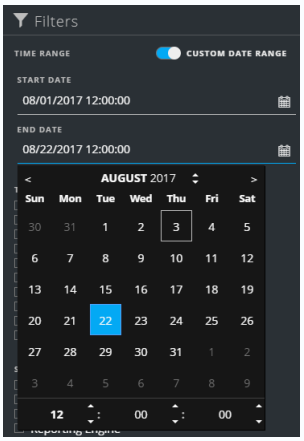
At the bottom of the list, you can see the number of tasks on the current page and the total number of tasks. For example: **Showing 23 out of 23 items**

Filters Panel

The following figure shows the filters available in the Filters panel.



The Filters panel, on the left of the Tasks List view, has options that you can use to filter the incident tasks.

Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the tasks. For example, if you select Last Hour, you will see tasks that were created within the last 60 minutes.
CUSTOM DATE RANGE	You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar. 
TASK ID	You can type the Task ID for a task that you would like to locate, for example REM-123.
PRIORITY	You can select the priorities that you would like to view. If you make one or more selections, the Tasks list shows only those tasks with the selected priorities. For example: If you select Critical, the Tasks list shows only the tasks with a priority set to Critical.
STATUS	You can select the statuses that you would like to view. If you make one or more selections, the Tasks list shows only those tasks with the selected statuses. For example: If you select Assigned, the Tasks panel shows only the tasks that are assigned to users.

Option	Description
CREATED BY	You can select the user who created the tasks that you would like to view. For example, if you only want to view the tasks created by Edwardo, select Edwardo from the CREATED BY drop-down list. If you want to view tasks regardless of the person who created the task, do not make a selection under CREATED BY.
Reset Filters	Removes your filter selections.

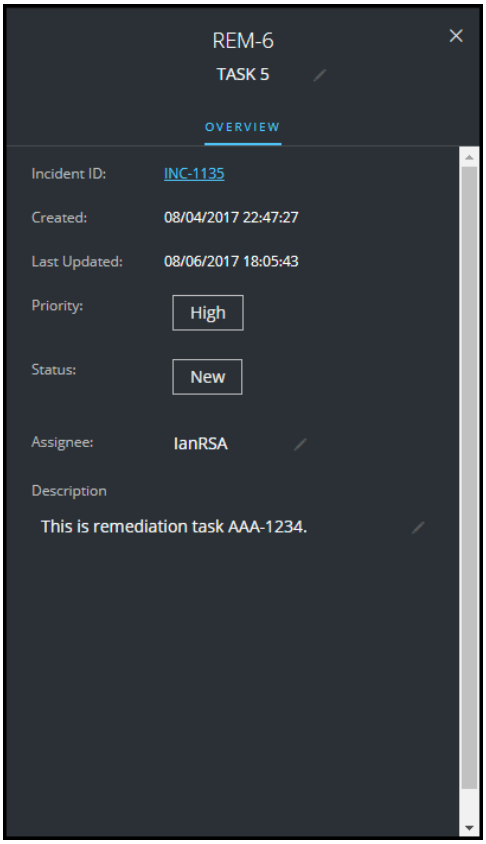
The Tasks List shows a list of tasks that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the tasks list. For example: **Showing 18 out of 18 items**

Task Overview Panel

To access the Task Overview panel:

1. Go to **RESPOND > Tasks**.

2. In the Task list, click the task that you want to view.
   The Task Overview panel appears to the right of the Tasks list.



The following table lists the fields displayed in the Task Overview panel.

Field	Description
<Task ID>	Displays the automatically assigned task ID.
<Task Name>	Displays the task name. This is an editable field. To change the task name, you can click the current task name to open a text editor. For example, you can change a task name from "Reimage a Laptop" to "Reimage a Server".
Incident ID	Displays the Incident ID for which the task was created. Click the ID to display the details of the Incident.
Created	Displays details about the date and time when the task was created.

Field	Description
Last Updated	Displays the date and time when the task was last updated.
Priority	Displays the priority of the task: Low, Medium, High, or Critical. To change the priority, you can click the priority button and select a priority for the task from the drop-down list.
Status	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. To change the status, you can click the status button and select a status for the task from the drop-down list.
Assignee	Displays the user assigned to the task. To change the user assigned to the task, you can click (Unassigned) or the name of the previous assignee to open a text editor.
Description	Shows task details. To modify the description, you can click the text underneath the description to open a text editor.

Toolbar Actions

This table lists the toolbar actions available in the Tasks List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the tasks that you would like to see in the Tasks List.
	Closes the panel.
Delete button	Allows you to delete the selected tasks.

Add/Remove from List Dialog

The Add/Remove from List dialog allows you to add or remove an entity or meta value to an existing list or create a new list. For example, when you look up an IP address and you find it suspicious or interesting, you can add it to a relevant list, which has been added a data source. This improves the visibility of the suspicious IP addresses. You can also add entities or meta values to different lists. For example, you can add them to one list for suspected domains related to command and control connections and to another list for Trojan connections IP addresses related to remote access. If a list is not available, you can create a list. You can also remove the entity or meta value from a list.

Note: From the Add/Remove from List dialog, you can only add or remove entities or meta values from single column lists added as a datasource, not multi-column lists. And when you edit a list or a value in a list from the nodal view or the context lookup view, ensure to refresh the web page to view the updated data.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	Add an entity to a list.	From the Incident Details view, see Add an Entity to a Whitelist. From the Alert Details view, Add an Entity to a Whitelist.
Incident Responders, Analysts	Create a whitelist, blacklist, or other list.	Create a List
Administrators	Add a Context Hub list as a data source.	See "Configure Lists as a Data Source" in the *Context Hub Configuration Guide*.
Administrators	Import or export a list for Context Hub.	See "Import or Export Lists for Context Hub" in the *Context Hub Configuration Guide*.

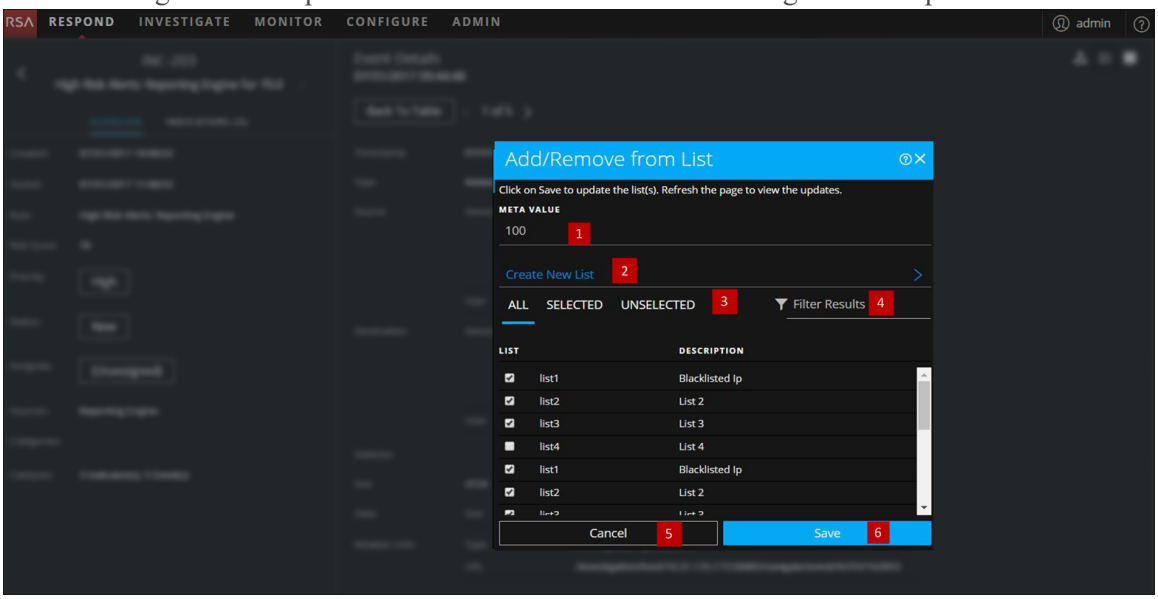
Related Topics

- Investigate the Incident
- Reviewing Alerts
- View Contextual Information (Incident Details view)
- View Contextual Information (Alert Details view)

Note: You cannot delete a list, but you can delete values within a list.

Quick Look

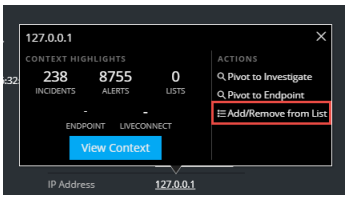
The following is an example of the **Add/Remove from List** dialog in the Respond view.



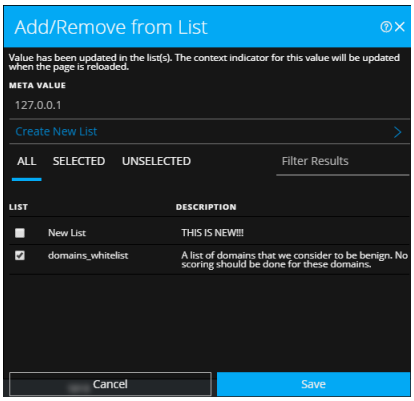
1. Entities or meta values to be added or removed.
2. Create a new list using the selected meta.
3. Select any of the tabs: All, Selected, or Unselected.
4. Search using the list name or description.
5. Cancel the action.
6. Save to update lists or create a new list.

Add/Remove from List

To access the Add/Remove from List dialog, in the Incident Details view or the Alert Details view, hover over the underlined entity that you would like to add or remove from a Context Hub list. A context tooltip appears showing the available actions.



In the Actions section of the tooltip, click Add/Remove from List. The Add/Remove From List dialog shows the available lists.



The following table shows the options in the Add/Remove from List dialog.

Option	Description
META VALUE	Displays the selected entity or meta value that needs to be added to or removed from one or more lists. You can also a create a new list using the selected value.
Create New List	When clicked, it displays a dialog to create a new list using the selected meta value.
ALL	Shows all of the available Context Hub lists. The lists that contain the selected entity or meta value are selected. Select a checkbox to add an entity or meta value to a list. Clear a checkbox to remove it from the list.
SELECTED	Shows only the lists that contain the selected entity or meta value. (All lists are selected.)
UNSELECTED	Shows only the lists that do not contain the selected entity or meta value. (All lists are unselected.)
Filter Results	Enter the name or description of a specific list to search from multiple lists.
LIST	Displays the name of all the lists.

Option	Description
DESCRIPTION	Displays information about the selected list. The description that you provide when creating a list appears in this dialog. For example: This list contains all of the blacklisted IP addresses.
Cancel	Cancels the operation.
Save	Saves the changes.

Context Lookup Panel - Respond View

The Context Hub service brings together contextual information from several data sources into the Respond view so that analysts can make better decisions during their analysis and take appropriate action. Seeing the entities, meta values, and contextual information in a single interface helps analysts to prioritize and identify areas of interest. For example, recently created incidents and alerts from the Respond view involving a given entity or meta value will be displayed when the analyst queries for additional information for that entity or meta value. The Context Lookup panel displays contextual information for the selected entities or meta values such as IP address, User, Host, Domain, File Name, or File Hash. The data available depends on the configured sources in the Context Hub.

The Context Lookup panel displays the contextual information based on the data available on the configured sources in the Context Hub.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, Threat Hunters	Navigate to the Context Lookup panel.	From the Incident Details view, see View Contextual Information . From the Alert Details view, see View Contextual Information .
Incident Responders, Analysts, Threat Hunters	Understand the information in the Context Lookup panel for a selected entity.	See the information in this topic.
Administrator	Configure Data Sources for Context Hub.	See "Configure Data Sources for Context Hub" in the *Context Hub Configuration Guide*.
Administrator	Configure Context Hub settings.	See "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.

Related Topics

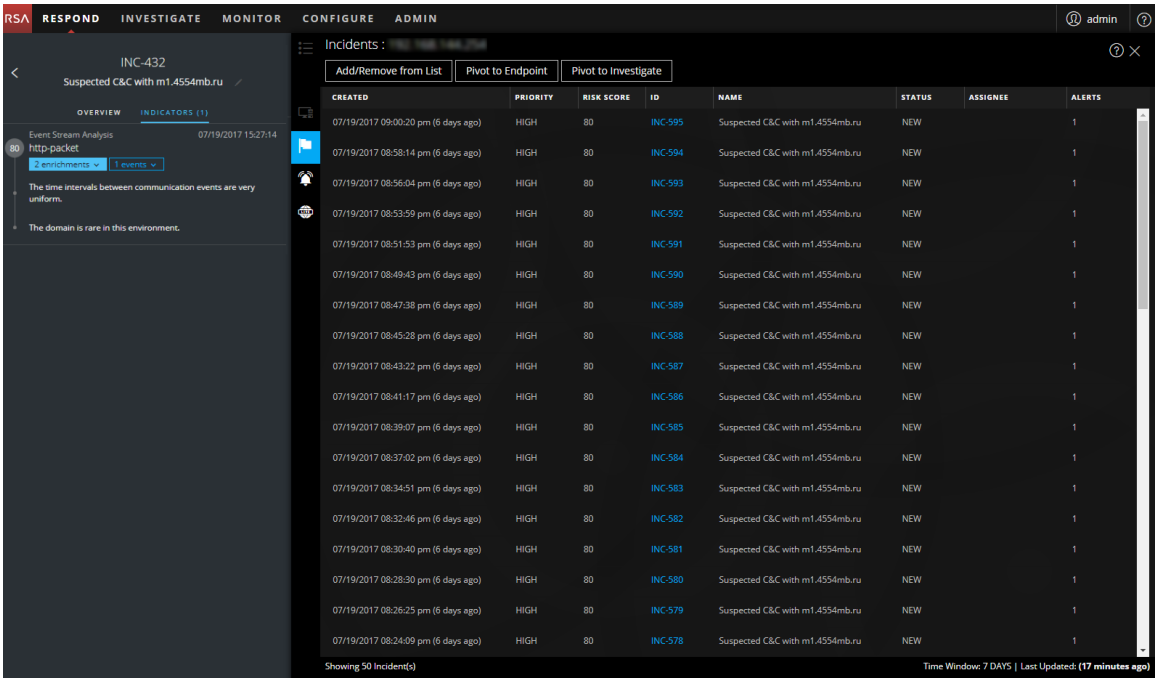
- Investigate the Incident
- Reviewing Alerts

Contextual Information Displayed in the Context Lookup Panel

The contextual information or query results displayed in the Context Lookup panel depends on the selected entity and the associated data sources.

The Context Lookup panel has separate tabs for each of the data sources. The List data source tab is the first in the context panel followed by Archer, Endpoint, Incidents, Alerts and Live Connect.

The following figure displays the Context Lookup panel for a selected entity in the Incident Details view. The Context Lookup panel Incidents tab is in view.



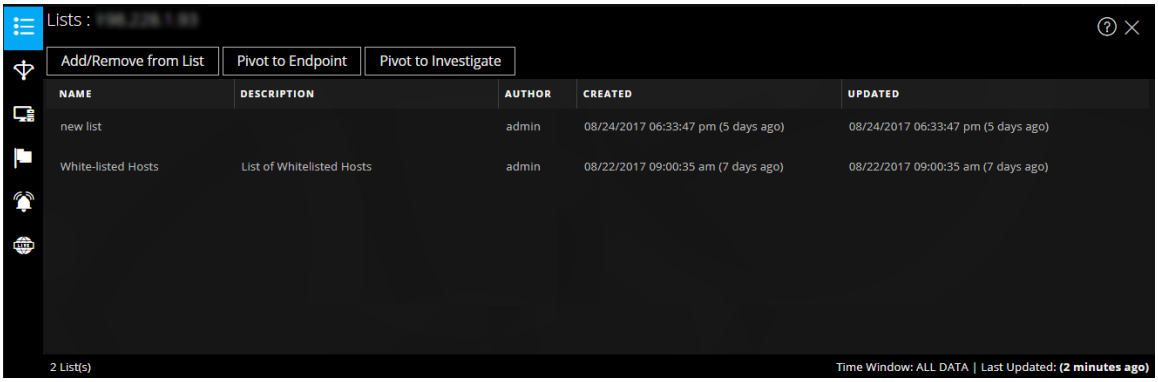
The following table describes the data available on each tab and the supported entities.

Tab	Description	Supported Entities
(Lists)	Displays all of the list data associated with the selected entity or meta value. The result is sorted by the last updated list.	All entities
(Archer)	Displays asset information along with criticality ratings using the Archer data source.	IP and Host
(Active Directory)	Displays all user information for the selected user.	User

Tab	Description	Supported Entities
(NetWitness Endpoint)	Displays the NetWitness Endpoint data source information for the selected entity or meta value, which includes the Machines, Modules, and IIOC levels. Modules are by highest IOC score to lowest IIOC score and IIOC levels are sorted by highest IOC levels to lowest IOC levels.	IP, MAC address, and Host
(Incidents)	Displays the list of incidents associated with the selected entity or meta value. The result is sorted by newest incidents to oldest incidents.	All entities
(Alerts)	Displays the list of alerts associated with the selected entity or meta value. The result is sorted by newest alerts to oldest alerts.	All entities
(Live Connect)	Displays information related to Live Connect.	IP, Domain, and Filehash

Lists

The Context Lookup panel for Lists shows one or more lists associated with the selected entity or meta value. The following figure is an example of the Context Panel for Lists.

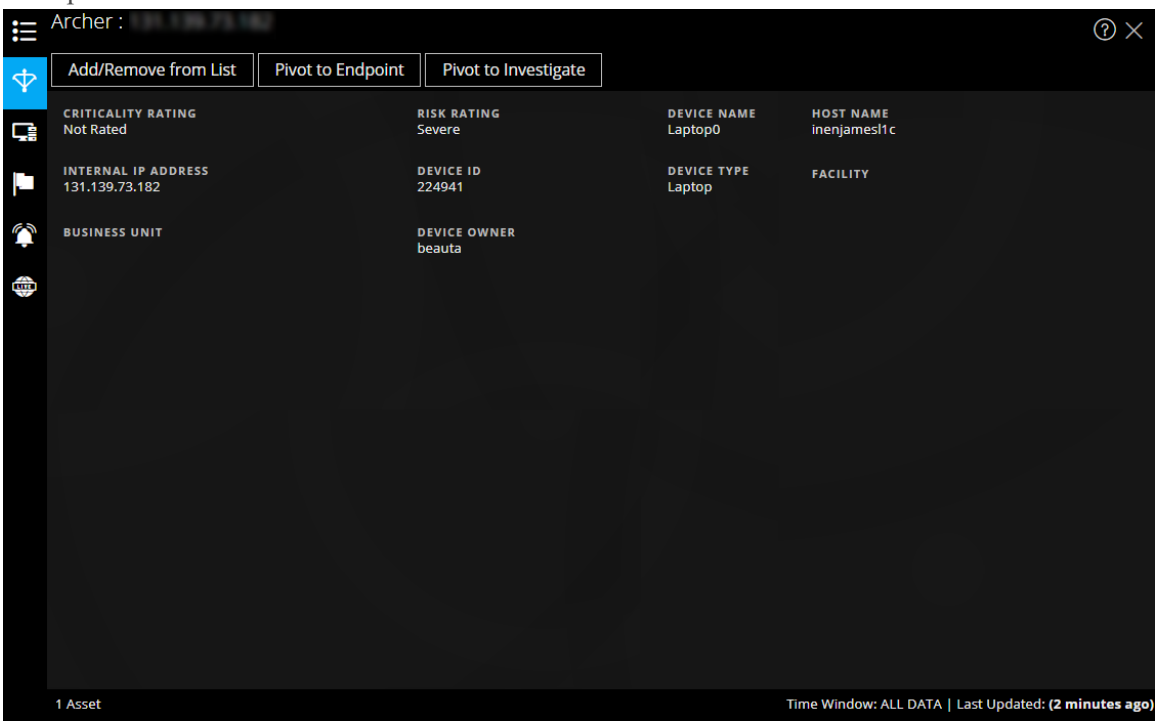


The following information is displayed for Lists.

Field	Description
Name	The name of the list (defined while creating the list).
Description	The description of the list (defined while creating the list).
Author	The owner who created the list.
Created	The date when the list was created.
Updated	The date when the list was last updated or modifed.
Count	The number of lists in which the selected entity or meta value is available.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Responses dialog. By default, all Lists data is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Archer

The Context Lookup panel for Archer displays asset information along with criticality ratings using the Archer data source for IP and Host entities and meta values. The following figure is an example of the Context Panel for Archer.



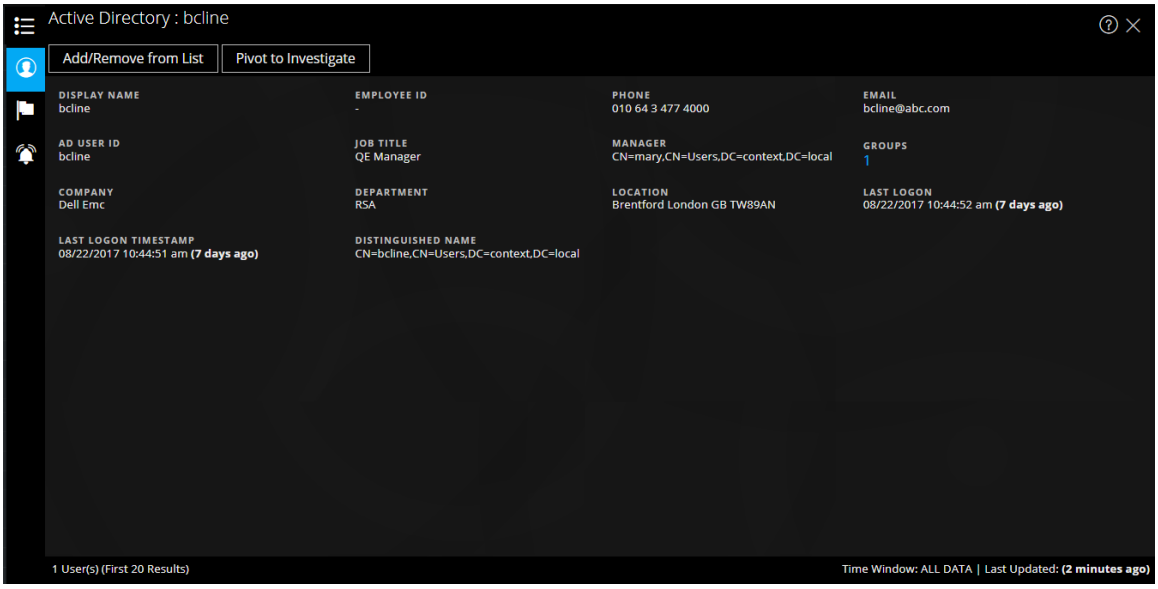
The following information is displayed for Archer.

Field	Description
Criticality Rating	Displays the device operational Criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High .
Device ID	Displays the automatically populated value that uniquely identifies the record across all applications within the system.
Device Name	Displays the unique name of the device.
Device Owner	Displays the owner(s) of the device who is responsible for the device and receives read and update rights of the record.
Host Name	Displays the host name of the device.

Field	Description
Facilities	Provides links to records in the Facilities application that are related to this device.
Business Unit	Provides links to records in the Business Unit application that are related to this device.
Risk Rating	Calculates the risk rating for the device based on the most recent assessment and the average risk rating of facilities using the device. The risk rating can be set as Severe, High, Medium, Low, or Minimal.
Type	Displays the device type such as Server, laptop, desktop etc.
IP Address	Displays the primary internal IP address of the device.
Count	Displays the number of assets available.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Responses Dialog. By default, all data for Archer is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Active Directory

The following figure is an example of a Context Panel for Active Directory.



The Context Lookup panel for Active Directory displays all the related information, incidents, and alerts for a user. You can perform a look up using the following formats:

- userPrincipalName
- Domain\UserName
- sAMAccountName

If the user exists in multi-domain or multi-forest, all the related context information is displayed for the specific user.

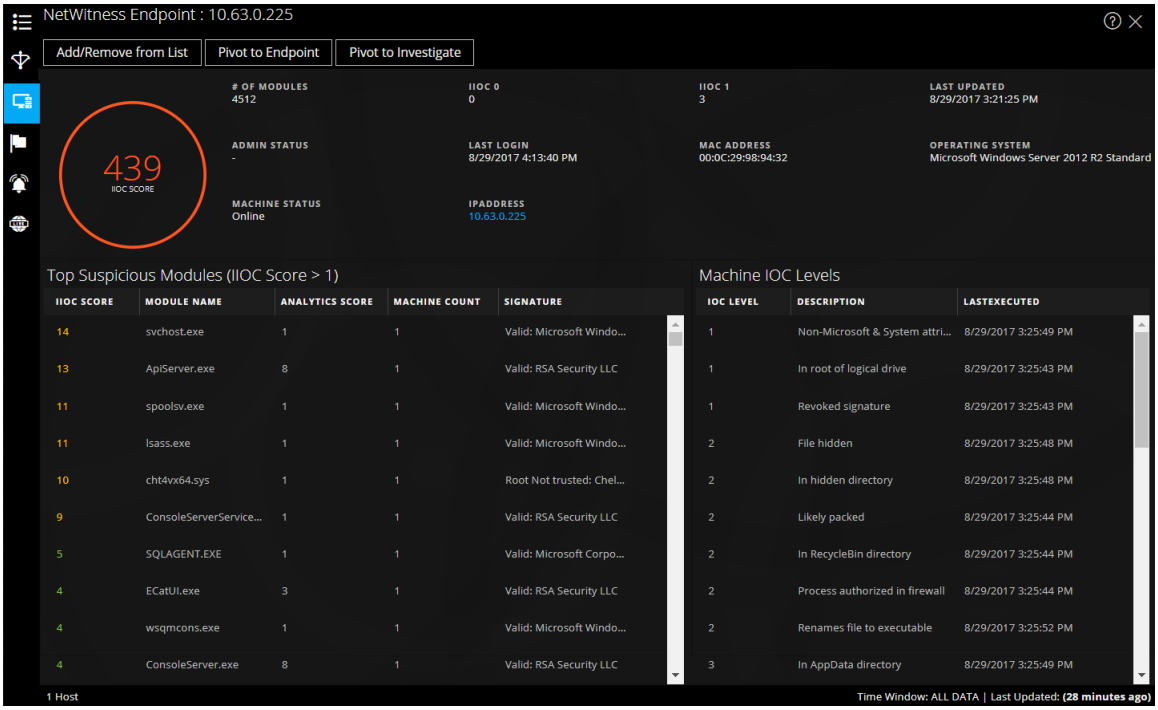
The following information is displayed for Active Directory.

Field	Description
Display Name	Displays the name of the specific user.
Employee ID	Displays the employee ID of the specific user.
Phone	Displays the phone number of the specific user.
Email	Displays the email ID of the specific user.
AD User ID	Displays the unique identification of the specific user within an organization.
Job Title	Displays the designation of the specific user.
Manager	Displays the manager's name of the
Groups	Displays the list of groups the specific user is a member.
Company	Displays the name of the company the specific user belongs to.
Department	Displays the department name within the organization that the specific user belongs to.
Location	Displays the location of the specific user.
Last Logon	Displays the time when the specific user logged into to the system only if the Global Catalogue is defined.
Last Logon TimeStamp	Displays the time when the specific user logged into to the system.
Distinguished Name	Displays the unique name assigned to the user.
Count	Displays the number of users.

Field	Description
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, all data for Active Directory is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

NetWitness Endpoint

The following information is displayed in the Context Lookup panel for NetWitness Endpoint.



The following information is displayed for IIOC.

Field	Description
# Of Modules	Displays the number modules that are looked up.
Admin Status	Displays the admin status (if any).
Last Updated	Displays the time when the data was last refreshed.
Last Login	Displays the time when the user last logged in.
MAC Address	Machine MAC Address.

Field	Description
Operating System	Version of the Operating System used by the NetWitness Endpoint machine.
Machine Status	Displays if the looked you module is Online, Offline, Active, or Inacive.
IP Address	Displays the IP address of the specific Module.

The following information is displayed for Modules.

Field	Description
IIOC Score	A machine IIOC score is an aggregated score based on the module scores. This is based on the value set for "Minimum IIOC Score" field in the Context Hub Data Source Settings The default value for "Minimum IIOC Score" is 500. See the "Configure Context Hub Data Source Settings" topic in the *Context Hub Configuration Guide*.
Module Name	Name of the module that is looked up.
Analystic Score	Number of active files for the selected machine.
Machine Count	Indicates when the scan results were last updated in NetWitness Endpoint database.
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information. For example, Google, Apple, and so on.

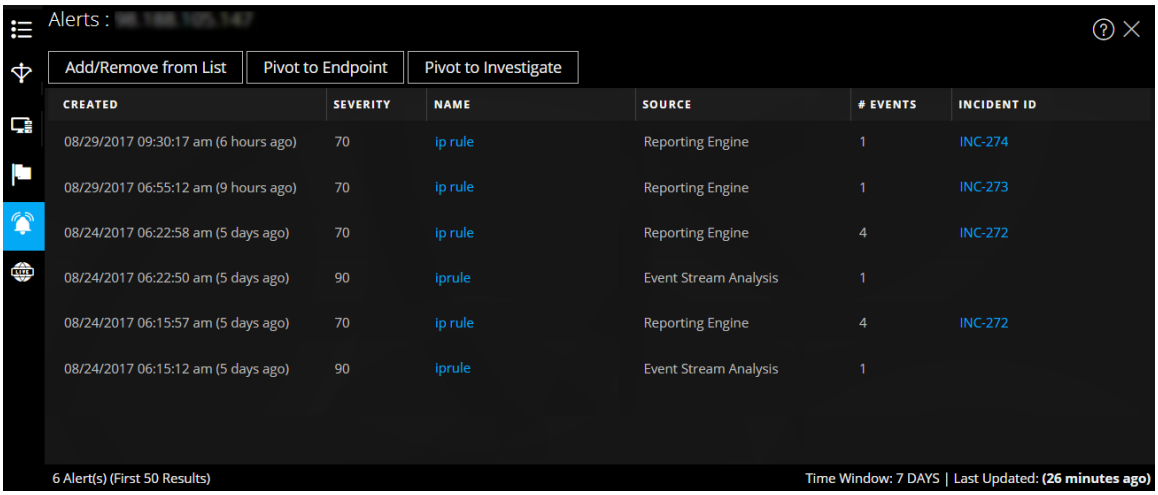
The following information is displayed for Machines.

Field	Description
IOC Levels	Displays the IOC levels.
Description	Displays the description for he IOC level if available.
Last executed	Displays the time when the action was executed.
Count	Displays the number of hosts that are looked up.

Field	Description
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, all data for NetWitness Endpointis fetched.
Last Updated	Indicates when the scan results were last updated in NetWitness Endpoint database.

Alerts

The following figure is an example of Context Panel for Alerts that is displayed based on time first (Newest to Oldest) and then severity.



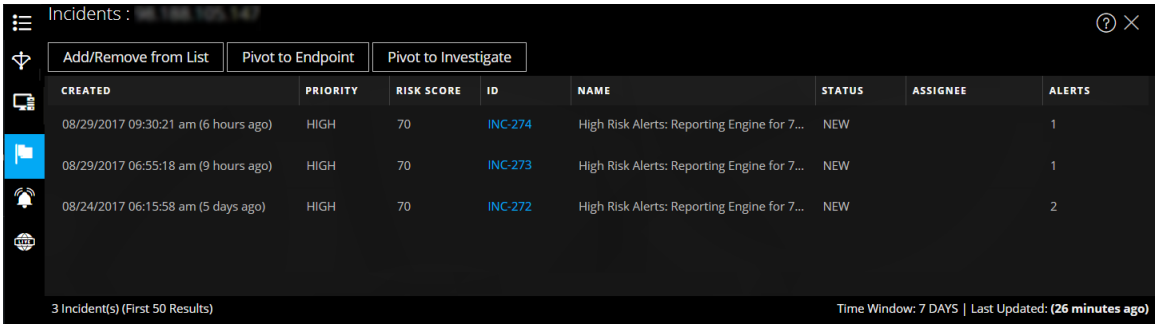
The following information is displayed in the Context Lookup panel for Alerts.

Field	Description
Created	Date and time when the alert was created.
Severity	Severity value of the alerts
Name	Name of the Alert. Click the name to view the details of a specific alert.
Source	Alert source name from where the alert is triggered.
#Events	Number of events associated with the alert.

Field	Description
Incident ID	This is the ID of the incident that the alert is associated with (If any). Click the ID tto view the details of a specific alert.
Count	Displays the number of alerts. By default only the first 100 alerts are displayed. For more information on how configure the settings, see the "Configure Context Hub Data Source Settings" topic in the *Context Hub Configuration Guide*.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	Indicates when contextual data was last fetched from data source.

Incidents

The following figure is an example of the Context Panel for Incidents, which is based on time first (Newest to Oldest) and then priority status.



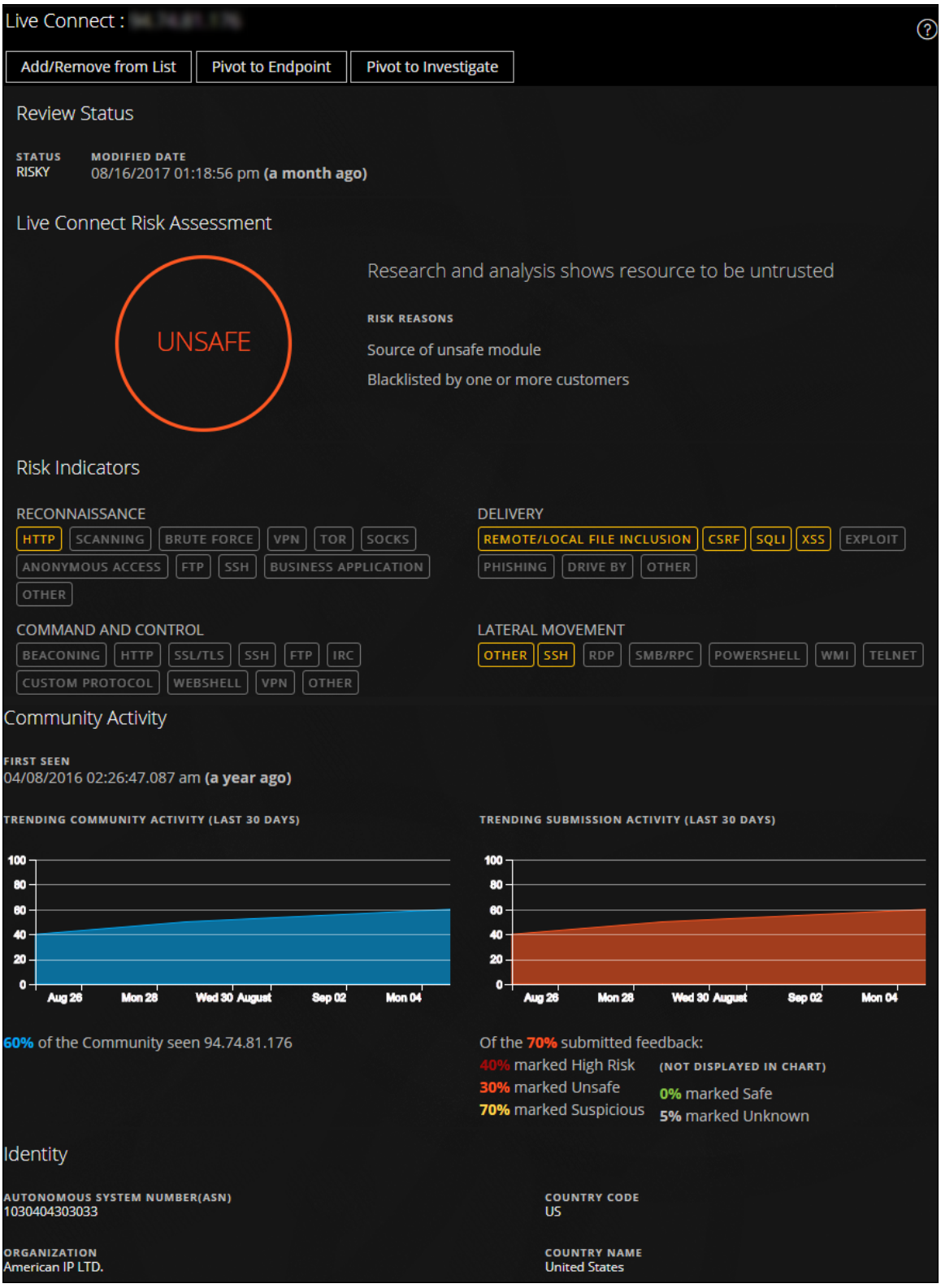
The following information is displayed in the Context Lookup panel for Incidents.

Field	Description
Created	Date when the incident was created
Priority	Priority status of the incidents
Risk Score	Risk score of the incidents
ID	Incident ID of the incident and on clicking displays further details about the incident
Name	Incident Name

Field	Description
Status	Status of the incident
Assignee	Current owner of the incident
Alerts	Number of alerts associated with the incident
Count	Displays the number of incidents. By default only the first 100 alerts are displayed. For more information on how configure the settings, see the "Configure Context Hub Data Source Settings" topic in the *Context Hub Configuration Guide*.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	Indicates when contextual data was last fetched from data source.

Live Connect

The following figure is an example of a Context Panel for Live Connect.


Live Connect :
Add/Remove from List
Pivot to Endpoint
Pivot to Investigate
Review Status
STATUS
RISKY
MODIFIED DATE
08/16/2017 01:18:56 pm (a month ago)
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Source of unsafe module
Blacklisted by one or more customers
Risk Indicators
RECONNAISSANCE
HTTP SCANNING BRUTE FORCE VPN TOR SOCKS ANONYMOUS ACCESS FTP SSH BUSINESS APPLICATION OTHER
DELIVERY
REMOTE/LOCAL FILE INCLUSION CSRF SQLI XSS EXPLOIT PHISHING DRIVE BY OTHER
COMMAND AND CONTROL
BEACONING HTTP SSL/TLS SSH FTP IRC CUSTOM PROTOCOL WEBSHELL VPN OTHER
LATERAL MOVEMENT
OTHER SSH RDP SMB/RPC POWERSHELL WMI TELNET
Community Activity
FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)
TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
60% of the Community seen 94.74.81.176
Of the 70% submitted feedback:
40% marked High Risk
30% marked Unsafe
70% marked Suspicious
(NOT DISPLAYED IN CHART)
0% marked Safe
5% marked Unknown
Identity
AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033
ORGANIZATION
American IP LTD.
COUNTRY CODE
US
COUNTRY NAME
United States

The Live Connect Panel displays the following information:

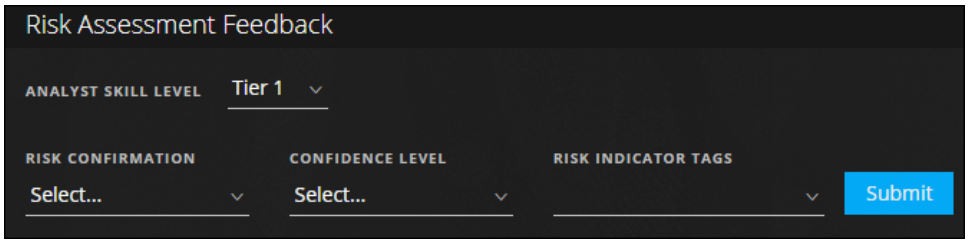
- Review Status
- Live Connect Risk Assessment
- Risk Indicators
- Community Activity
- WHOIS
- Related Files, Domains, and IPs
- Identity
- Certificate Information

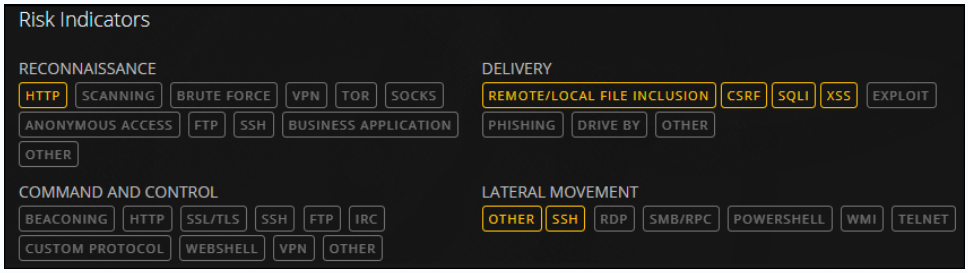
The following information is displayed in the Context Lookup panel for Live Connect.

Field	Description
Review Status	Displays the review status of the selected Live Connect entity (IP, file, or domain) based on the analyst activity. This gives the visibility of the analyst activity within an organization. **Status** Below are the types of status: • **New:** If lookup results for an IP address is viewed for the first time within the organization. • **Viewed:** If any analyst within the organization has already viewed the lookup results for an IP address. • **Marked as Safe:** If any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • **Marked as Risky:** If any analyst within the organization has already viewed the lookup results and marked the IP address as risky.

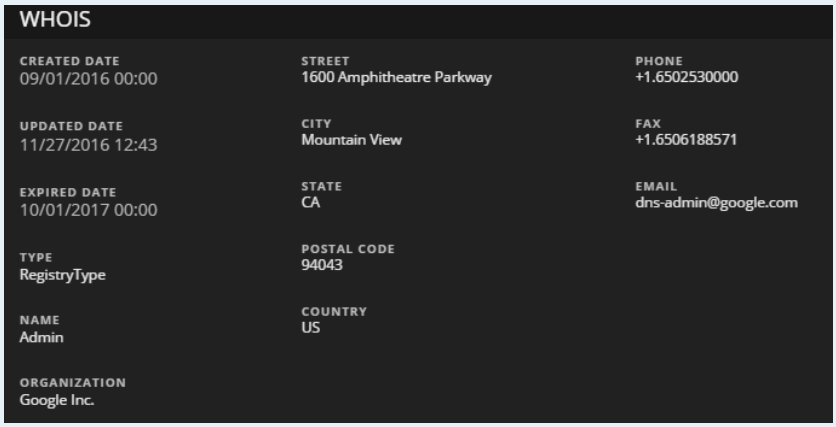
Field	Description
Risk Assessment	Displays the risk assessment for the selected Live Connect entity (IP, file, or domain) based on the Live Connect analysis and analyst feedback. The Risk Assessment categories are: • **Safe:** The Live Connect entity is considered to be safe. • **Unknown:** Live Connect does not have enough information about this entity to calculate the risk. • **High Risk**: Marked as "High Risk" based on the analysis and risk reasons provided by the community. The entities marked as "High Risk" requires immediate attention. • **Suspicious**: Marked as "Suspicious" based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action. • **Unsafe:** Marked as "Suspicious" based on the analysis and risk reasons provided by the community. The entity is rated as High Risk, Suspicious, or Unsafe and displays the associated risk reasons accordingly.

Field	Description
Risk Assessment Feedback	Risk Assessment Feedback allows the analyst to submit threat intelligence feedback about an entity to the Live Connect server. • **Analyst Skill Level** Below are the Analyst skill level options: ◦ **Tier 1** - Analysts at this level generally define procedures for remediation, and decide if an incident should be escalated to other areas in a SOC (Security Operation center). This is the default value. ◦ **Tier 2** - Analysts investigates incidents, and captures intelligence from investigation to feedback into the various work flows in a SOC. ◦ **Tier 3** - Analysts who shares the investigation results to the SOC organization. They generally manage incidents and have a wide breadth and depth in the skills and tools necessary for incident response. **Note:** While creating a new user for NetWitness Suite (Analyst), an administrator should be able to identify the user as Tier 1, Tier 2, or Tier 3 Analyst. • **Risk Confirmation** - The risk confirmation for the selected Live Connect entity (IP, file, or domain). The Risk confirmation categories are: ◦ **Safe**: The Live Connect entity is considered to be safe. ◦ **Unknown**: The analyst does not have enough information to provide a risk confirmation ◦ **High Risk**: Marked as "High Risk" based on the analysis and risk reasons provided by the community. The entities marked as "High Risk" requires immediate attention. ◦ **Suspicious**: Marked as "Suspicious" based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action. ◦ **Unsafe**: Marked as "Unsafe" based on the analysis and risk reasons provided by the community. • **Confidence Level** - The confidence level of an analyst in providing feedback for the Live Connect entity. The confidence level categories are: ◦ High

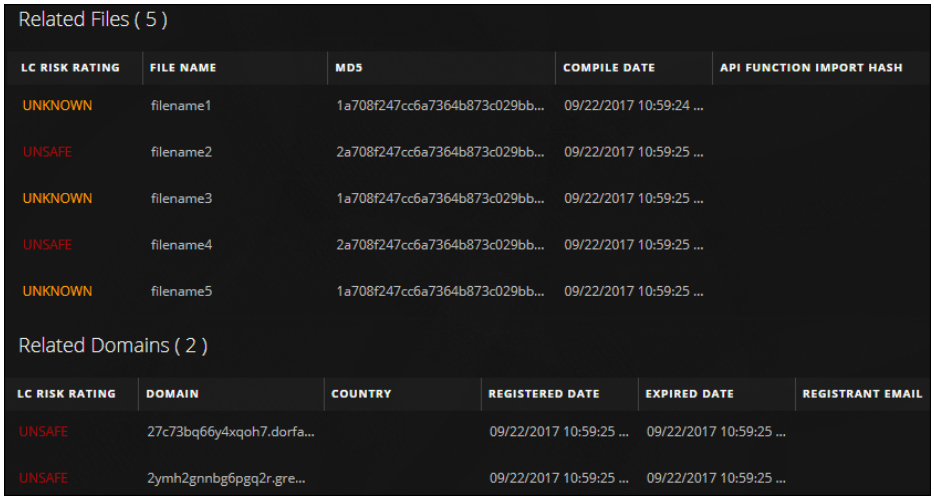
Field	Description
	◦ Medium ◦ Low. • **Risk Indicator Tags** - Allows you to select a tag category based on the analysis. 
Community Activity	Community activities such as: • Date first seen in the community. • Time since the IP/File/Domain was seen for the first time (Current time - First seen time). **Trending Community Activity:** If the IP address is known within the RSA community, a graphical representation of the community activity trend is displayed for the following: • Users (in %) who have viewed the IP address in the Live Connect community over time. • Users (in %) who submitted feedback for the IP address. • Users (in %) who marked the IP address as unsafe over time.

Field	Description
Risk Indicators	Risk Indicators are highlighted based on the tags that are assigned by the community to the entities (IPs, Files, or Domains).  The tags are categorized as given below: • Reconnaisance • Delivery • Command and Control • Lateral Movement • Privilege Escalation • Packaging and Exfiltration These tags are samples and vary based on the inputs received from the community on the Live Connect server. The analyst can choose the appropriate risk indicator tags while providing the review feedback. A highlighted tag indicates that the selected entity is associated with that particular category and tag. Clicking a highlighted tag displays the description of the tag.

Field	Description
Identity	Provides the following identity information for the selected entity or meta value: For IP address: • Autonomous System Number (ASN) • Prefix • Country Code and Country Name • Registrant (Organization) • Date For File Hash: • File Name • File Size • MD5 • SH1 • SH256 • Compile Time • Mime Type For Domain: • Domain Name • Associated IP Address
Certificate Information	Provides the following certificate information for the selected file hash: • Certificate Issuer • Validity of the Certificate • Signature Algorithm • Certificate Serial Number

Field	Description
WHO IS Information	The **WHO IS** information provides the ownership details for a given domain.  The following information of the domain owner is displayed: • Created Date • Updated Date • Expired Date • Type (Registration Type) • Name • Organization • Address with Postal code • Country • Phone • Fax • Email

Field	Description
Related Files	Related Files are displayed for entity types IP and Domain. A list of known associated files are displayed along with the following information: • Live Connect Risk Rating (Safe, Risky, or Unknown) • File Name • MD5 • Compile Time and Date • API Function Import Hash • Mime Type
Related Domains	Related Domains are displayed for entity types IP and Files. A list of known associated domains are displayed along with the following information: • Live Connect Risk Rating (Safe, Risky, or Unknown) • Domain Name • Country Name • Registered Date • Expired Date • Registrant Email address

Field	Description
Related IPs	Related IPs are displayed for entity types Domain and Files. A list of known associated IPs are displayed along with the following information: • Live Connect Risk Rating (Safe, Risky, or Unknown) • IP Address • Domain Name • Country Code and Country Name • Country Name • Registered Date • Expired Date • Registrant Email address 

RSA NETWITNESS® SUITE

Reporting User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Reporting Overview **7**

Reporting Guidelines 13

Access Control for Reporting 22

Configure and Generate a Report **27**

Configure a Rule **28**

Create a Rule Group 28

Create a Rule Using NetWitness Data Source 29

Create a Rule Using Warehouse Data Source 33

Create a Rule Using Respond Data Source 38

Deploy a Rule 41

Test a Rule 58

Create a Lists or List Group 59

Create and Schedule a Report **63**

Create a Report or Report Group 63

Schedule a Report 64

Additional Procedures 70

Generate a List from the Scheduled Report 70

Create a Parameterized Report Using Variable 71

Create a Report Using a Rule 83

View a Report **84**

Investigate a Report **87**

Manage Lists, Rules or Reports **88**

Manage a List 88

Access Control for a List and List Group 88

Edit a List 94

Delete a List or List Group 95

Duplicate a List 96

Export a List or List Group 97

Import a List or List Group 98

Manage a Rule 100
Access Control for a Rule and Rule Group 100
Delete a Rule or Rule Group 110
Duplicate a Rule 111
Edit a Rule 111
View Dependents of a Rule 113
Export a Rule or Rule Group 114
Manage a Report 115
Access Control for a Report or Report Group 115
Delete a Report or Report Group 128
Duplicate a Report 129
Edit a Report 130
Refresh a Report Group or Report List 130
Edit a Scheduled Report 131
Delete a Scheduled Report 135
Export a Report 135
Export a Report Group 136
Import a Report or Report Group 137
Enable or Disable a Scheduled Report 139
Start or Stop a Scheduled Report 139
View an Execution History of a Scheduled Report 140
Manage and Select a Report Logo 141
Search Reporting Details 143

Troubleshooting 150

Meta Values in Investigation Link Issue 151
Internet Explorer 10 Browser Issue 151
Dynamic List Editing Issue 151
Deployment Failure Issue 152
Respond Server Issue 152
Post-Upgrade Issue 152

Appendix 153

Rule Syntax 154
NWDB Rule Syntax 154
Respond Rule Syntax 209
Warehouse DB Simple Rules Syntax 216

Warehouse DB Advanced Rules Syntax 225
Task Scheduler for Warehouse Reporting 248
Query Aggregates 250

Configure and Generate a Chart 275

Configure a Chart 281

Schedule a Chart 284

View a Chart 285

Test a Chart 287

Investigate a Chart 288

Manage a Chart Group and Chart 289

Alerting Overview 298

Configure Reporting Engine 304

Configure an Alert 306

Schedule an Alert 310

View an Alert 311

Investigate an Alert 312

Manage an Alert and Alert Template 313

Reporting Reference 323

Build Chart View 324
Build List View 327
Build Report View 331
Build Rule View 337
Chart Permissions Dialog 345
Chart View 348
Execution History Panel 353
Generate List Panel 360
Import Chart Dialog 363
Import Report Dialog 366

Investigate a Chart View 369
Lists Permissions Dialog 372
List View 376
Reports Permissions Dialog 380
Report View 383
Rule Permissions Dialog 388
Rule View 392
Select a Logo Dialog 397
Schedule a Chart View 400
Schedule Report Panel 404
Scheduled Reports View 414
Test a Chart View 420
View a Chart Panel 424
View All Charts View 429
View a Report Panel 433
View All Reports View 440

Alerting References 444

Alert List View 445
Alert Permissions Dialog 448
Alert Schedules View 451
Create or Modify Alert Panel 454
Investigate an Alert View 464
Import Alert Dialog 467
Alert Template References 470
    Alert Template View 471
    Create or Modify Template View 474
View Alerts Schedule View 476
View Alerts View 479

Reporting Overview

Reporting is a collection of data as a result of monitoring the network traffic, which can be used for further analysis. In NetWitness Suite you can run a report against NetWitness Suite Database core services to identify the network activities. For example, if you want to identify the Top Source Countries and Destination Countries, or top Threat and Risk trends that help monitor any changes to the normal categories or monitor the users and services that may potentially have malicious activities etc.

The reporting typically consist of: Reports and Charts. You can report on the log, packet and endpoint data collected, and customize the reports and charts to enhance the visual appearance. You can create real-time reports for historical data. You can create charts and dashlets, that can be added in the real-time chart dashlets as well.

Reporting Engine

Reporting relies on the Reporting Engine to provide data for the reports, alerts and charts. Hence, you must configure the Reporting Engine as a service to NetWitness Suite before you can generate the reports. You must also specify the data source in the Reporting Engine from which the data is extracted.

The data that you can report or alert depends on the configuration of Reporting Engine and the data sources that you specify as part of the rule definition.

Note: Make sure you have access to the components in the Reporting.

Note: Make sure you have access to the required data sources. Only privileged users with access to sensitive information have the permission to certain data sources. To manage access control to data sources, see the "Add a Role and Assign Permissions for Warehouse Analytics" However, for the existing reports, alerts and charts, if the user role or permissions are modified for the data sources, then it is not applicable unless you manually update the permissions.

Note: Reporting is accessible based on the role based access, defined for the user.

Report

A report is a combination of rules and other formatting objects such as headers and HTML-formatted notes that describe and identify data pertaining to a particular area of interest. Reports are defined and managed in the Build Report page and can be scheduled to run on an adhoc or timely basis. Once a report is run, results are stored centrally and can be automatically sent over email, SFTP, URL, and NFS to users, viewed via the NetWitness Suite web interface, downloaded as PDF and CSV files.

A report consists of the following:

Property	Description	Example
Report Name **Note:** For **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.	Used to identify the report to schedule them at a later time.	Report1
Text	Pre-defined text fields used within a report to make the report more meaningful to the user.	Header1, Comment
Rules	The rules (queries) used to create a report.	select user.dst where ip.src = 10.10.10.1

Note: In the Reporting user interface, the displayed date or time is always according to the user-selected time zone profile.

Rule

A rule is the basic and essential building block in the Reporting. You must create a rule which can be used in a Report, Chart or Alert.

A rule represents a unique query that detects and summarizes the requested information within a collection of network data.

The rule syntax is very similar to that of Standard Query Language (SQL) where you can use the select clause, where clause, sort and group options and limits for the result set. A rule consists of the following:

Property	Description	Example
Name	The name of the rule.	Windows System Account Activity
Select	List of meta types that are returned in the result set. The list of meta types is provided in the Meta Library. Meta Library in the Rule Builder is continually synchronized with the index configuration of the NetWitness Suite host to which NetWitness Suite is connected. The number of meta types that this property can represent depends on how the rule is to be sorted. If the Sort by property is 'None' or Custom, a rule can have more than one select field, for example, for each match, include the ip.src, ip.dst, size, time in the rule result. If a rule is set to be sorted, either by session count, session size, or packet size, then there can only be one field on which to select.	
Where	A clause that is the base query for the rule.	alert='cleartext_ftp_password'

Property	Description	Example
Then (Rule Actions)	A series of functions that manipulate the original result set of a rule in order to make the output in a report more meaningful or add additional functionality other than querying and displaying data.	lookup_and_add ('username','ip.src',10);
Sort By	Determines how the data in the result set is sorted. The various possibilities are: • Total • Value • Column Name	Total
Limit	Designates how large a result set can be for the given rule. Users must note that if a result set is sorted by count or size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.	20

Note: In the User Interface (UI), the date or time displayed depends on the time zone selected by the user.

Rule Types

There are different rule types in the Reporting. Rule types designate the source of data for the report rule. Following are the rule types:

Rule Type	Description
NetWitness Database (**NetWitness DB**)	The NetWitness database extracts the meta from a Reporting Engine configured to use a Concentrator, Broker and Archiver as the data sources and provides the meta for rules.
Warehouse Database (**Warehouse DB**)	The Warehouse database, also referred to as the RSA NetWitness Warehouse, warehouses large volumes of data. The Warehouse is designed so that you can retrieve large volumes of data easily and efficiently. The Warehouse also extracts the meta from the Reporting Engine.
Respond Database (**Respond DB**)	The Respond database contain alerts and incidents generated from different services and you can create a report on those alerts and incidents.

Note: In the User Interface (UI), the date or time displayed depends on the time zone selected by the user.

List

A list is a variable that refers to a series of comma-separated values (CSV). You can insert a list into a rule or use it as an argument to a rule action. Lists can act as placeholders for other values, which you can populate and update as needed.

You can create, manage and view lists that can be used to define rules for Reporting and Alerting.

Lists cannot be empty or have duplicate or blank values.

Note: If you are defining a report with a rule which has lookup_and_add in the **Then** clause and direct the report output to a list, the list is not populated with the result.
For example, if you create a rule with ip.src in the **Select** clause and lookup_and_add ('ip.dst','ip.src', 10) in the **Then** clause, the report displays the result, but if you have redirected the output to a list, the list will be empty

Chart

Chart is a tabular or grid representation of data. It consists of the following:

Property	Description	Example
Chart Name	Identifies the chart.	Chart1
Rule Basis	Identifies the rule path chosen from the folder hierarchy.	

Any NetWitness Suite DB rule in the Reporting Engine system which is not sorted by none can be used to instantly create a chart. In NetWitness Suite, the chart interval can be adjusted from the chart definition panel itself. Each time a chart runs, it stores its result data locally in the Reporting Engine, so that it can be reviewed in either the Dashboard View or Chart View without any performance considerations.

Note: In the Reporting user interface, the output for the field where Date and Time are displayed is always according to the user-selected time zone profile.

Note: The Reporting Engine (RE) will automatically check for the available disk space before you execute a Test Rule, Report, Chart and Alert. If the RE disk space (in percentage) is less than the minimum disk space threshold (default value is 5), the RE will stop the current execution and an error message 'Available disk space of Reporting engine home is <5%, please clean up the space to proceed further' is displayed. Additionally, you may also configure the minimum disk space threshold by using the following path: **RE>Config>General>System Configuration>Mini disk space threshold in %.**

Reporting Guidelines

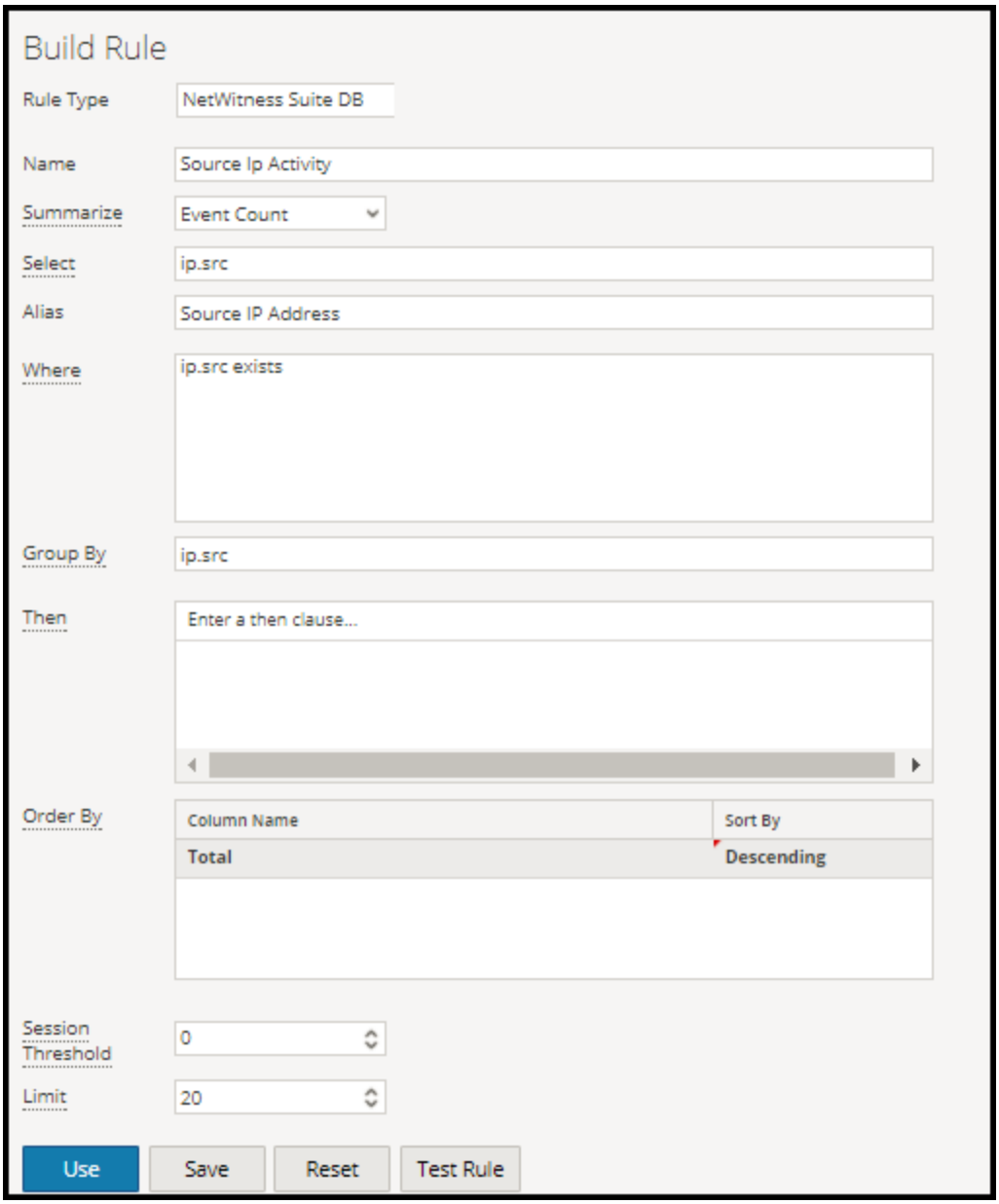
This section lists the RSA recommended guidelines to enhance the execution time of your reporting entities such as rules, reports, alerts, charts, and lists. The guidelines are provided for the following:

- NWDB Rules
- Timeout Configuration for NWDB Rules
- Lookup and Add rule action
- List value Reports

NWDB Rules

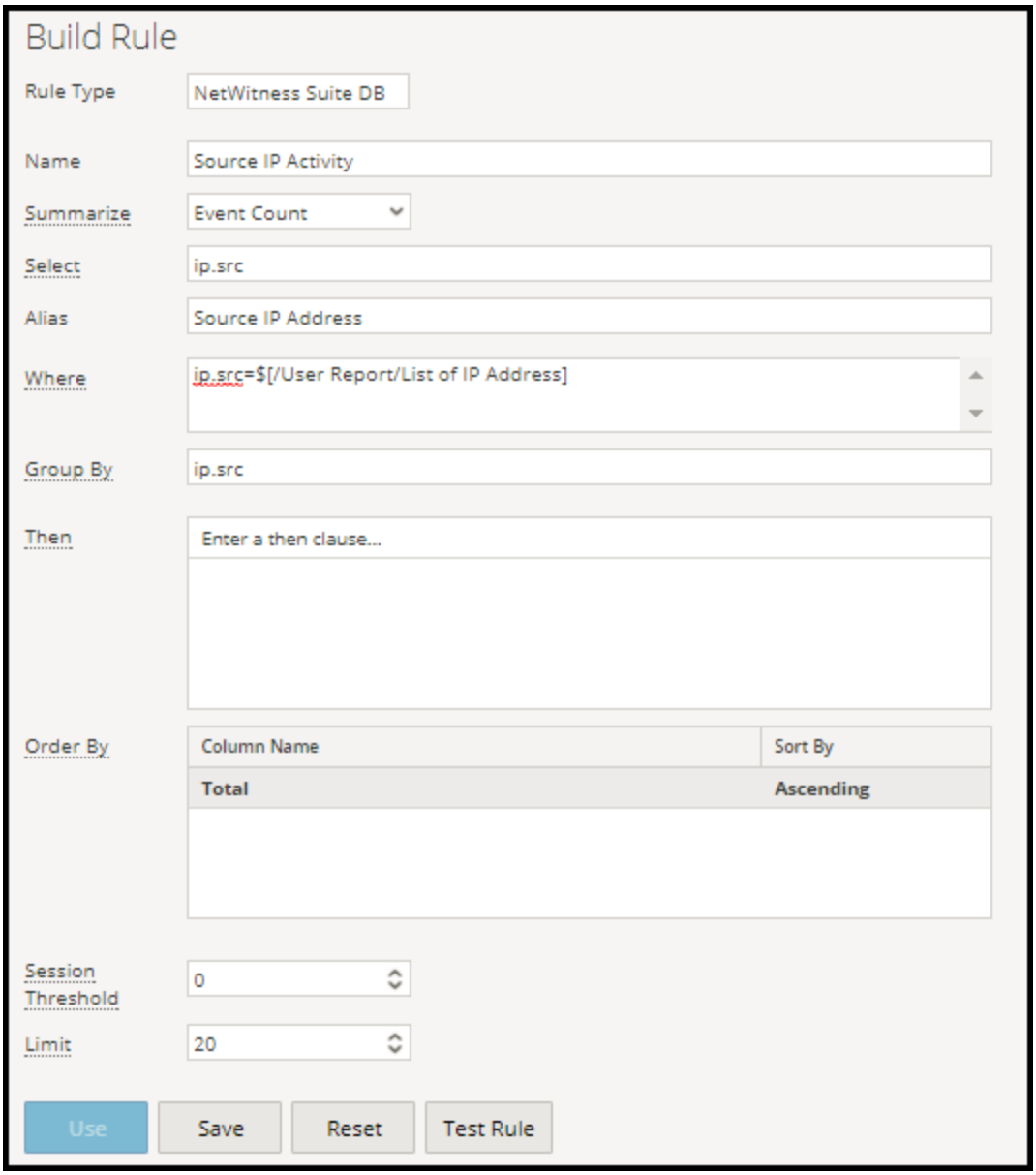
If the reporting entities such as report, alert, or chart contain NWDB rules (in most cases where the query contains Group By) takes a long time to execute, you may do the following:

1. Refine the Where clause:
   You may limit the number of sessions scanned by using or refining the Where clause (especially when you use the Group By option). For example, consider the following rule.

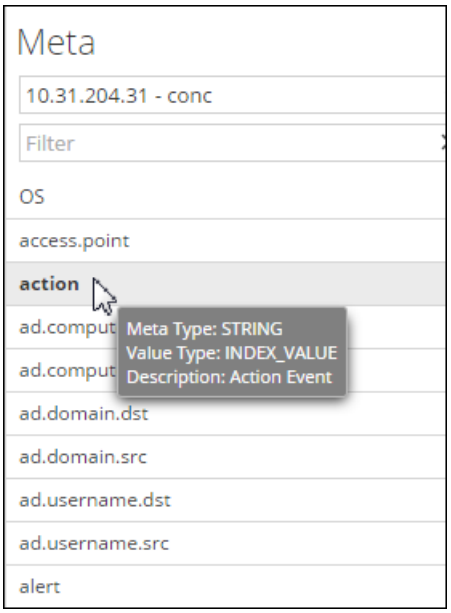


If you use a Where clause as mentioned above, the number of sessions aggregated is huge. To avoid this, you can filter only required sessions by specifying the list of IP addresses or creating a List (list of IP Address) that contains relevant IP addresses.

Note: The NWDB rule where clause is appropriately quoted if the syntax has an invalid quote. For example, in case of an invalid meta, or missing separator, the status and the error message is updated appropriately.



2. Using indexed Meta keys in the Where clause:
   To understand if the Meta is indexed or not, mouse hover the Meta List present on the right panel. If the Value Type is INDEX_VALUE, then the Meta is indexed. The Value Type is INDEX_KEY or INDEX_NONE if the Meta is not indexed.
   Below is a snapshot of a Meta key that is indexed.



3. Configure the Timeout option:
   If the query is taking a long time and fails due to timeout issues, you can configure the timeout for the NWDB rule executions. For more information, see below section "Timeout Configuration for NWDB Rules".
4. Schedule the queries to run at different times:
   If multiple query aggregates are concurrently executed and timeout occurs, you may schedule the queries to run at different times without much overlap.

Timeout Configuration for NWDB Rules

Note: It is a good practice to check the statistics of the Reporting Engine and the NWDB data sources before you make any changes to the configuration. For more information, see the "Monitor Service Details" topic for Reporting Engine and "Monitor System Statistics" topic in the *System Maintenance Guide*.

If NWDB rule execution fails due to timeout, you may get the following errors on the View a Report page:

- Reporting Engine timeout error
  - “Data source ‘`10.31.x.x Concentrator`' did not respond within the configured time `30` minutes for the ‘`/sdk/values`' request.”

- NWDB timeout error
  - "Error occurred while fetching data from source '10.31.x.x Concentrator'. {Timeout message from NWDB}"

  In such cases, you may do the following:

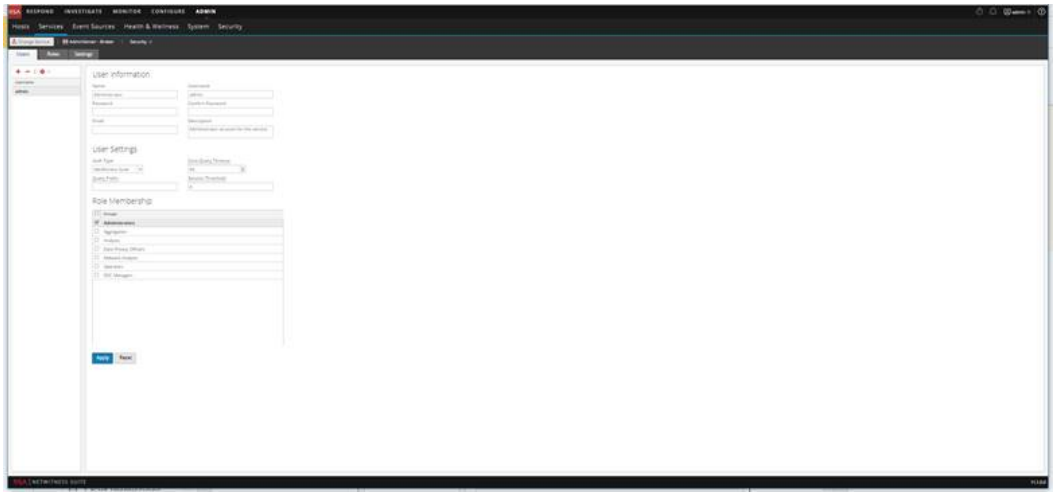
  - Reporting Engine timeout

    In case of Reporting Engine timeout, you may set the timeout to a longer duration so the long running queries can be executed. For more information on setting the NWDB Queries Time Out and NWDB Info Queries Time Out option for the Reporting Engine, see "Step 2. Configure Reporting Engine Settings" topic in the *Reporting Engine Configuration Guide*. RSA recommends you set the NWDB Query Time Out to zero minutes (implies no timeout) and NWDB Info Queries Time Out to 60 minutes.

  - NWDB timeout

    In case of NWDB timeout, you may need to configure the query.level.timeout and max.concurrent.queries parameters for the NWDB data source based on the recommendations in the *Core Database Tuning Guide* to fine tune the queries.

    The following figure is an example of Explorer view where you can set the parameters for NWDB data source.

  - Schedule Reports at different times

    If the NWDB core devices are heavily utilized, you may schedule the reports to run at different times without overlap.

- Split the Report

  If you have many rules in a Report, split the report into multiple reports with each report containing logical set of rules. If you have multiple rules, all rules will begin to execute at the same time based on available threads, therefore you may group the rules logically into separate reports.

LookupAndAdd Rule Action

If a rule that consists of single or multiple `lookup_and_add` rule actions, takes a long time to execute the report, it is because each of the rule action triggers multiple lookup queries on the NWDB data source resulting in longer execution time.

To improve the report execution time, you may do the following:

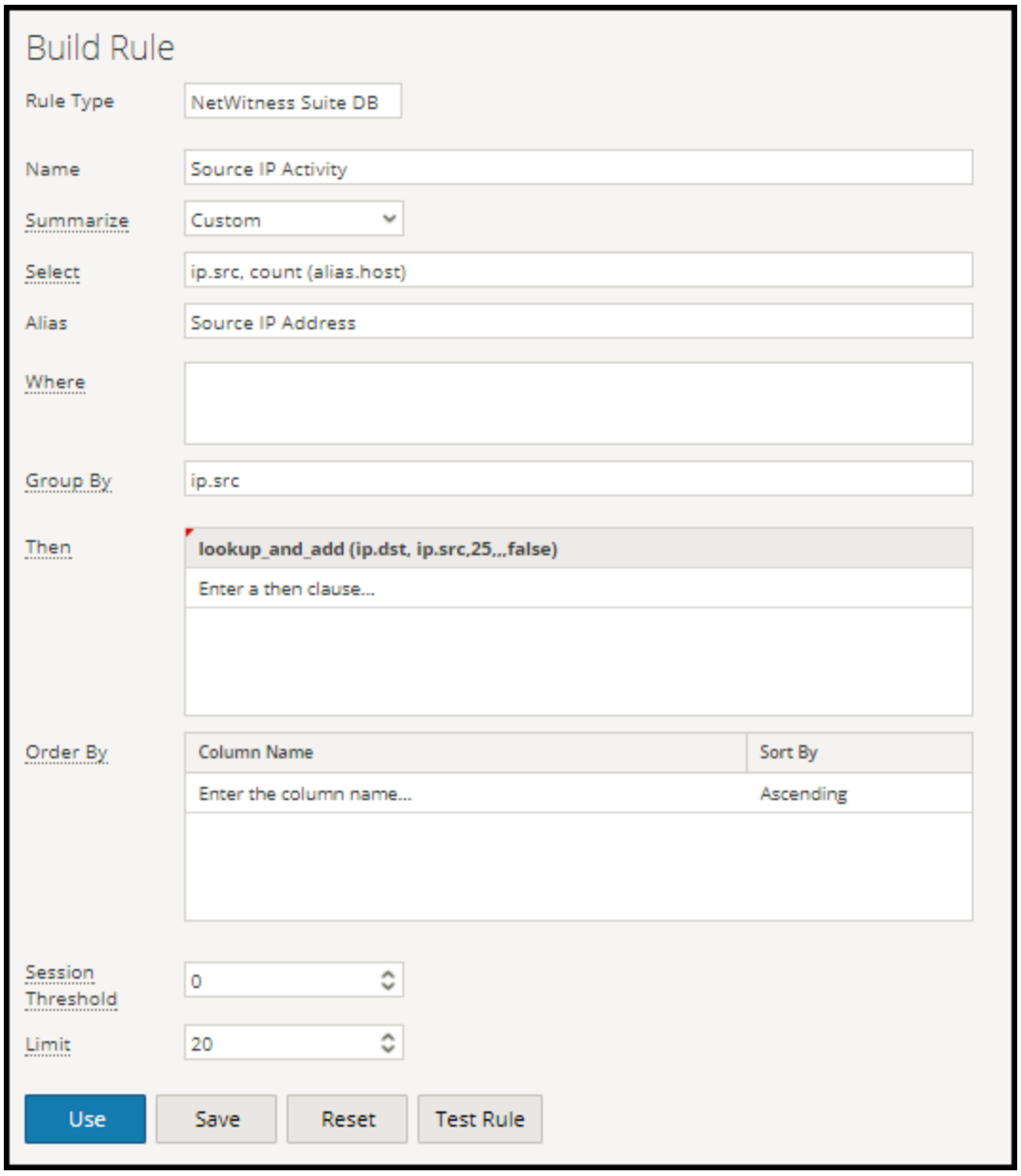
- Refine the Where clause in the following:
  - Rule that contains the `lookup_and_add` rule action
  - `lookup_and_add` rule action
- Set Limits

  You must set appropriate limits for the rule and rule actions. If the limit is high it will result in many queries being triggered and hence the report will take a long time to execute.
- Set the boolean aggregate parameter

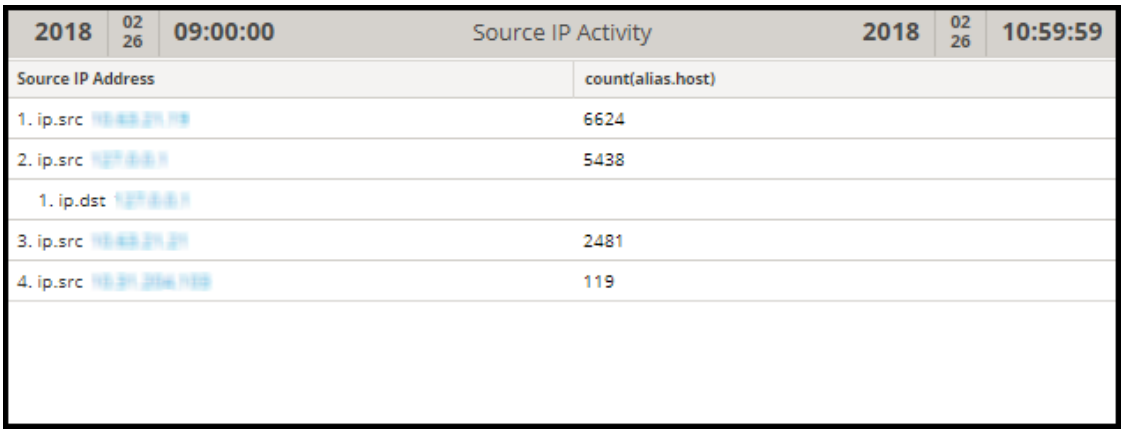
  If you do not want the aggregate value such as `sum(meta), count (meta)` etc. for the lookup values, set the boolean aggregate parameter to false in the `lookup_and_add` rule action. For more information, see the "NWDB Rule Syntax" section in Rule Syntax .

  ```
  lookup_and_add(string select, string field, int limit,
  boolean inherit, string extraWhere, boolean aggregate)
  ```

  Consider the rule with lookup_and_add rule action:

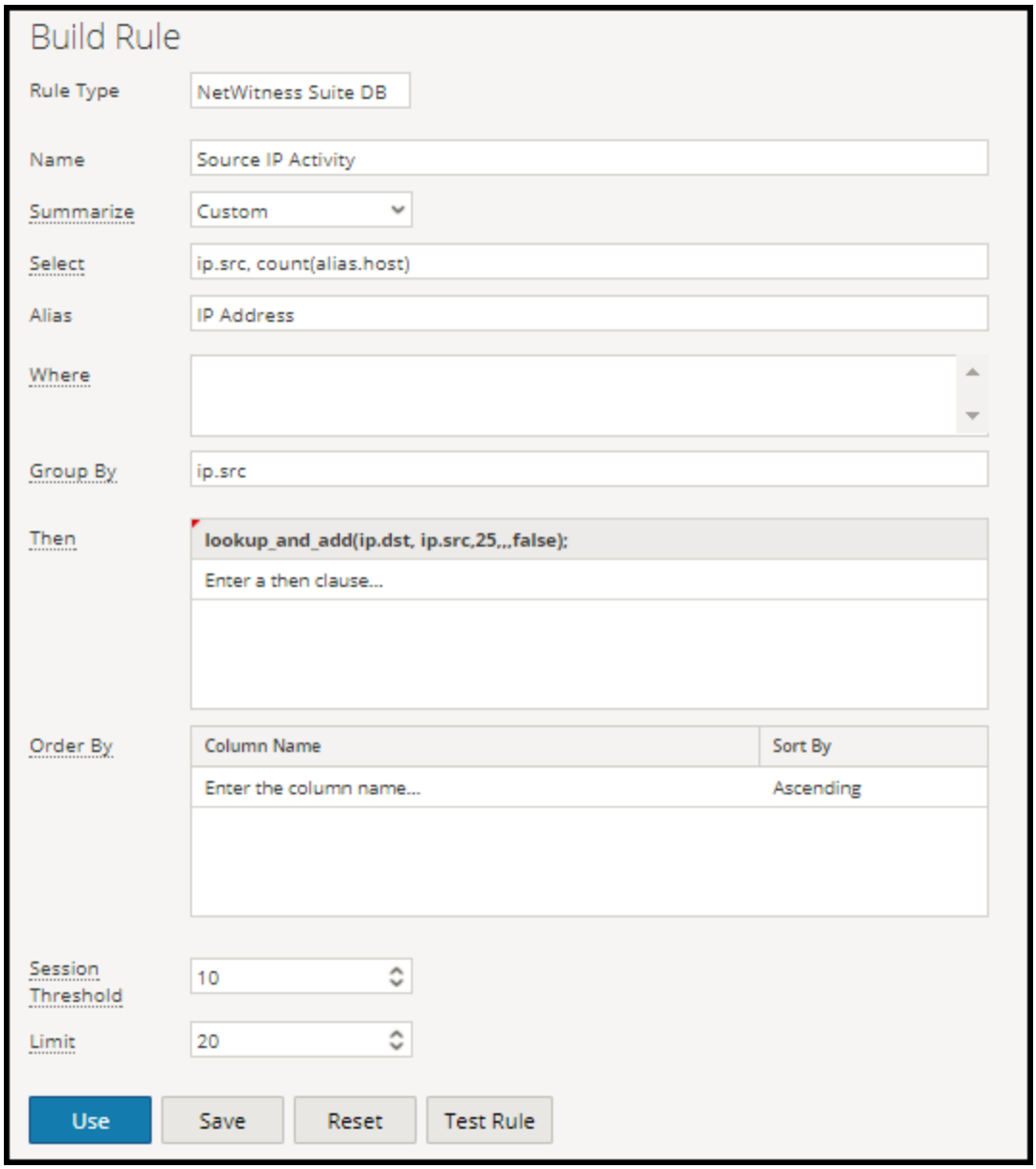


The output is displayed:

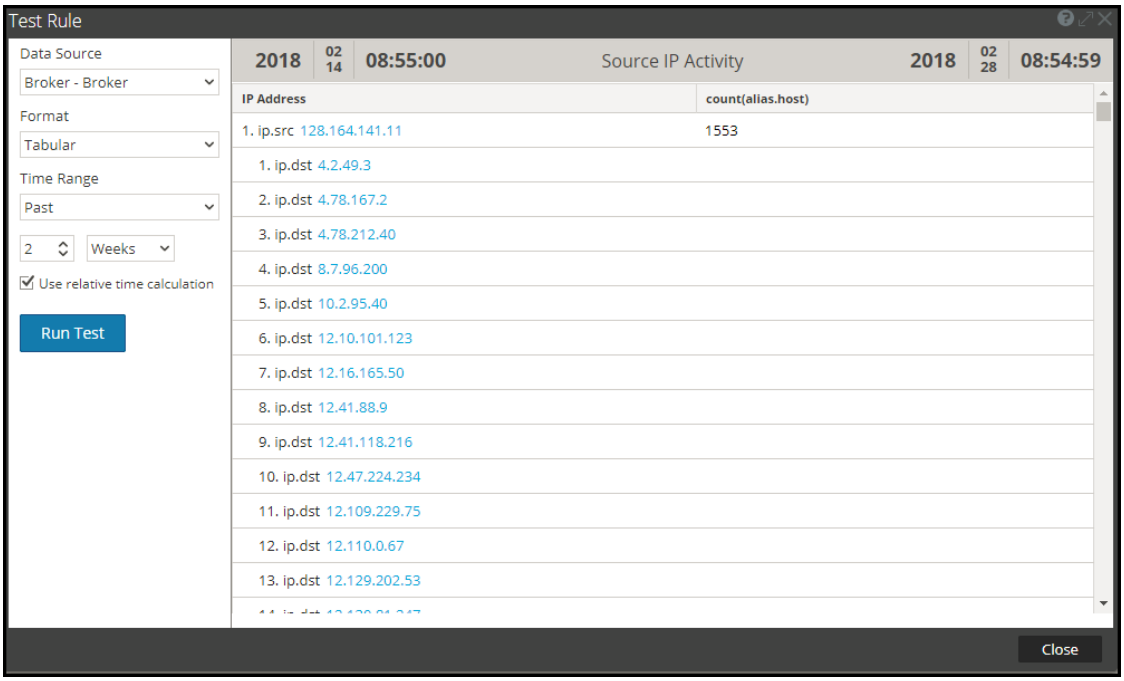


2018 02 26 09:00:00	Source IP Activity	2018 02 26 10:59:59
Source IP Address	count(alias.host)	
1. ip.src	6624	
2. ip.src	5438	
1. ip.dst		
3. ip.src	2481	
4. ip.src	119	

- Each `lookup_and_add` rule action triggers by default two concurrent lookup queries on the data source. RSA recommends that you retain the default setting, however if you want to increase the value you may want to ensure the value of `Max # of Concurrent LookupAndAdd Queries` parameter in Reporting Engine is less than the `Max Concurrent Queries` value in the NWDB data source configuration.
  If the NWDB data source is shared across other services, then you may retain a low value for the `Max # of Concurrent LookupAndAdd Queries` parameter in Reporting Engine as increasing it will impact the queries from other services. For more information, see "Reporting Engine General Tab" topic in *Reporting Engine Configuration Guide*.
- If you are interested only in unique values and not accurate aggregates, then set the `Session Threshold` to a non-zero value for the NWDB rule. For more information, see "Create a Rule Using NetWitness Data Source" section in Configure a Rule. The higher the value, the longer is the rule execution. If the value is set to zero it will take a longer time but will provide accurate aggregates.
  Consider a rule with lookup_and_add rule action and Session Threshold set to 10.



The output is displayed:



List Value Reports

Use a Refined List:

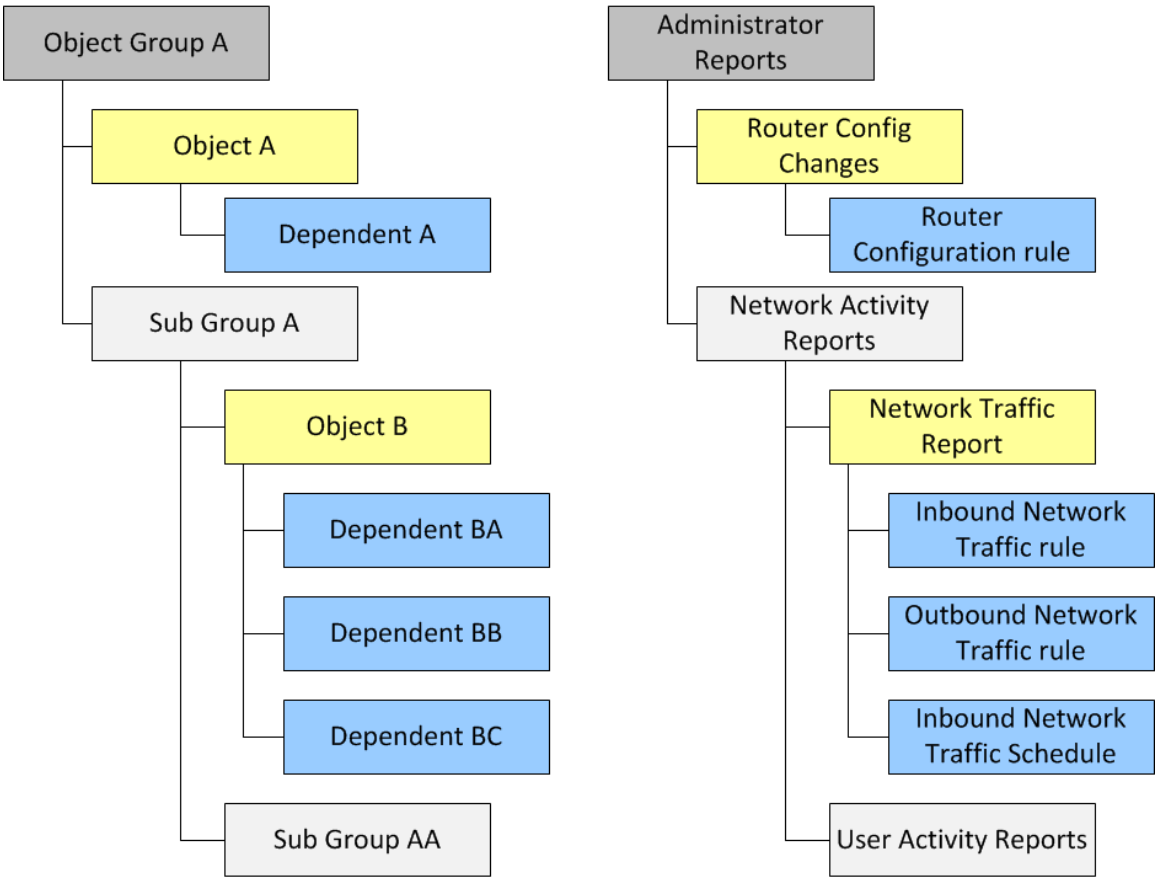
In case of List value reports (for any data source type), individual reports will be generated for each value in the list. Therefore, more the number of values in the list the longer the reports will take to execute. Hence, you must use a refined list to generate such reports.

Access Control for Reporting

Reporting Module provides you the option to set up access control for all the components in the module. In NetWitness Suite, you can define different roles and specify the access control for each of the role from the System Security module. You can define the access control to be provided for the Reporting module for each role. For more information, see "Step 1: Review the Pre-Configured NetWitness Suite Roles" and "Step 2: (Optional) Add a Role and Assign Permission" topics in the *System Security and User Management Guide*.

In the Reports module, you can modify the role permissions or access to the following Reporting objects:

The Following is an example of the hierarchy of the object groups, objects and dependents. This is an illustration of the Report Groups and Reports hierarchy.



Report Groups and Reports Hierarchy

Permission for Object Groups

- You must have the Read & Write permission to set the permissions for the Object Group, Objects, or Dependents. The dependents with “No Access” permission are grayed out and dependents with “Read-Only” permission are indicated with an icon.
- When you set the permission for the Object Group, the Objects and Dependents in the Object Group do not inherit the permission automatically. You must select the "Apply these permissions to sub-groups and <Objects> in this group" option to achieve this. For example, if you do not want Operators roles to access reports in Report Group A, then you must set the permission on Group A to No access for the Operator role and select the "Apply these permissions to sub-groups and Reports in this group" option.
- When you set the permissions for the Object Group and select the "Apply these permissions to sub-groups and <Objects> in this group" option, the

dependents such as rules or schedules in the objects do not inherit the permissions automatically. You must use the "Apply Read-only permission to Rules in the <Object>" option to apply the permission to the rules.

- When you set the permissions for the Objects, you must ensure that the Objects in hierarchy should always have a permission that is less than or equal to the one above in the hierarchy for the permission to be applied. For example, if the reports in a Report Group have Read & Write permission and you apply a Read-Only or No Access permission at the Report Group level and select the "Apply these permissions to sub-groups and Reports in this group" option, then the permission on the rules will remain unchanged.
- The permissions are cascaded from top to down in the hierarchy and not vice-versa. For example, if you apply a permission to a rule, it does not change the permission of the Report that contains the rule.

Permission for Objects or Dependents

- You must have the Read & Write permission to set the permissions for the Objects or Dependents.
- You can specify the permission for multiple objects at once instead of setting the permission for each object.
- When you set the permission for the Object, the dependents in the Object do not inherit the permission automatically. You must select the "Apply Read-only permission to Rules in the <Object>" option to achieve this.

When you apply the permission to dependents the permission is applied based on the existing permission for the role. For example, consider an Analyst and a Operator with the following permissions for the different dependents (Report A object has Rule AA, Rule AB, and Rule AC as dependents).

Object or Dependent	Analyst	Operator
Report A	Read & Write	No Access
Rule AA	Read & Write	No Access
Rule AB	Read and Write	Read and Write
Rule AC	Read-only	No Access

When the Analyst applies a Read & Write permission for the Operator role and selects the option "Apply Read-only permission to Rules in the <Object>", then the permissions will be set for the different dependents as follows:

Modify the Permissions

- **Group Level:** Set the permissions at the Object Group level and for all the object and entities in the Group. For example, if you have 80 reports in the Administrators Reports group and you do not want anyone except the Administrator to add or modify these reports, you can set the permission for all the other roles at the group level to Read-Only and select the option to apply it to all the reports and sub-groups in the report group.
- **Multiple Objects:** Select multiple objects and specify the access for all the selected objects. For example, if you have 10 reports in the Network Traffic sub group with sensitive information that you do not want anyone to access, select the 10 reports and then set the permission for all the roles as "No Access".
- **Single Object:** Select only the object and specify the permission. For example, select the Network Traffic Report and specify the Read-Write permission for the Security Analyst role or select the Login Failure Alert and specify the Read-Write permission for a Security Analyst role.

Object or Dependent	Operator (Before Permission is applied)	Operator (After Permission is applied)
Report A	No Access	Read & Write
Rule AA	No Access	Read-only
Rule AB	Read and Write	Read & Write
Rule AC	No Access	Read-only

Roles and Permissions for Reporting Module

Although NetWitness Suite has five pre-configured roles, you can add custom roles. For example, in addition to the pre-configured Analysts role, you can add custom roles for AnalystsEurope and AnalystsAsia.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to data
Analysts	Access to data but not to configurations
SOC_ Managers	Same access as Analysts and an additional permission to handle incidents
Malware_ Analysts	Access to malware events only

Depending on the user role, you can set the following access permissions to access the Reporting module components (Rules, Reports, Charts, Alerts, Lists):

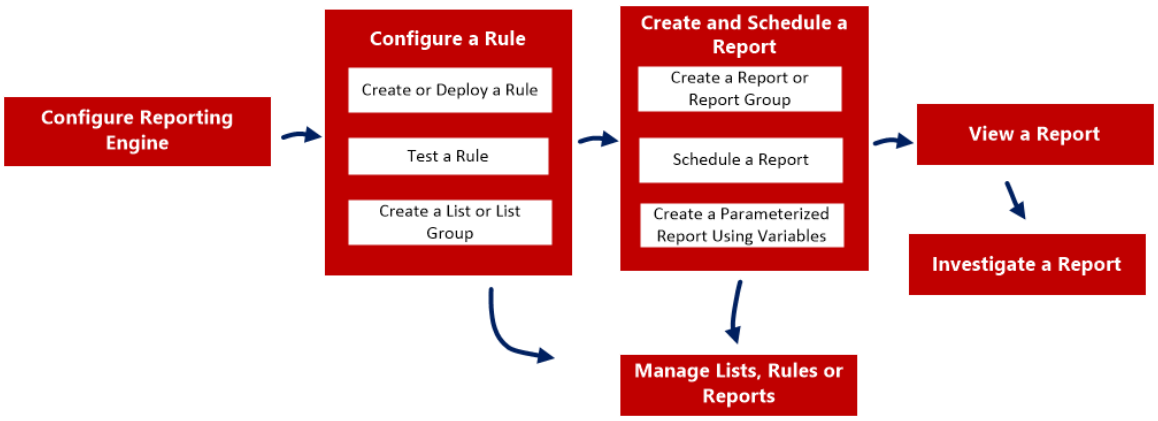
- Create
- Delete
- Export
- Manage
- View

Note: You must enable all these permissions for a user role to be able to define, delete, manage and view each of the Reporting modules. You must also have appropriate permissions for the data source to be listed, while defining the reports, charts, or alerts. For more information, see "Configure Data sources Permissions" topic in the *Reporting Engine Configuration Guide*.

For a detailed list of permissions and how to add a role and assign permissions, see "Role Permissions" and "Step 2. (Optional) Add a Role and Assign Permissions" topics in the *System Security and User Management Guide*.

Configure and Generate a Report

This figure is an overview of the entire process of configuring and generating a report.



To configure and generate a report, perform the following tasks:

1. Configure Reporting Engine - You must configure the Reporting Engine before you can configure and generate a report. You must also specify the data source in the Reporting Engine from which the data is extracted. For more information on how to configure Reporting Engine, see "Configure Reporting Engine" topic in the *Reporting Configuration Guide*.
2. Configure a Rule
3. Create and Schedule a Report
4. View a Report
5. Investigate a Report
6. Manage Lists, Rules or Reports

Configure a Rule

You can create a new rule or deploy an existing rule from the Live Services which can be used in a report. You can use different conditions to refine the data or information in the data sources such as :

- Select clause
- Where clause
- Group By
- Order By and so on

For example, you can write a rule to view the top 20 web addresses that the users visit daily.

You can create different type of rules using different data sources. Based on your requirements you can select any of the following options to create a rule:

- Create a Rule Using NetWitness Data Source
- Create a Rule Using Warehouse Data Source
- Create a Rule Using Respond Data Source

You can also use a list in a rule to refine a search result from the data source. Once a rule is created you can test a rule to see the results returned by the rule.

Create a Rule Group

To create a rule group or rule sub-group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Do one of the following.
   - To define a rule group:
     a. In the Rule Groups Panel, click .
        The new rule group is added to the Rule Groups panel.
     b. Enter the name for the rule group and press ENTER.

- To add a rule sub-group:

  a. In the Rule Groups panel, select the rule group to which you want to add a sub-group.

  b. Click +.

     The new rule sub-group is added to the rule group.

  c. Enter the name for the rule sub-group and press ENTER.

Create a Rule Using NetWitness Data Source

You can create a rule to fetch data or events from a NetWitness data source. The same procedure is used to define a rule to fetch data or events from an Archiver data source.

The Archiver data source can be added in the Services Config View of the Reporting Engine. For more information, see "(Optional) Add Archiver as a Data Source to Reporting Engine" topic in the *Archiver Configuration Guide*.

Prerequisites

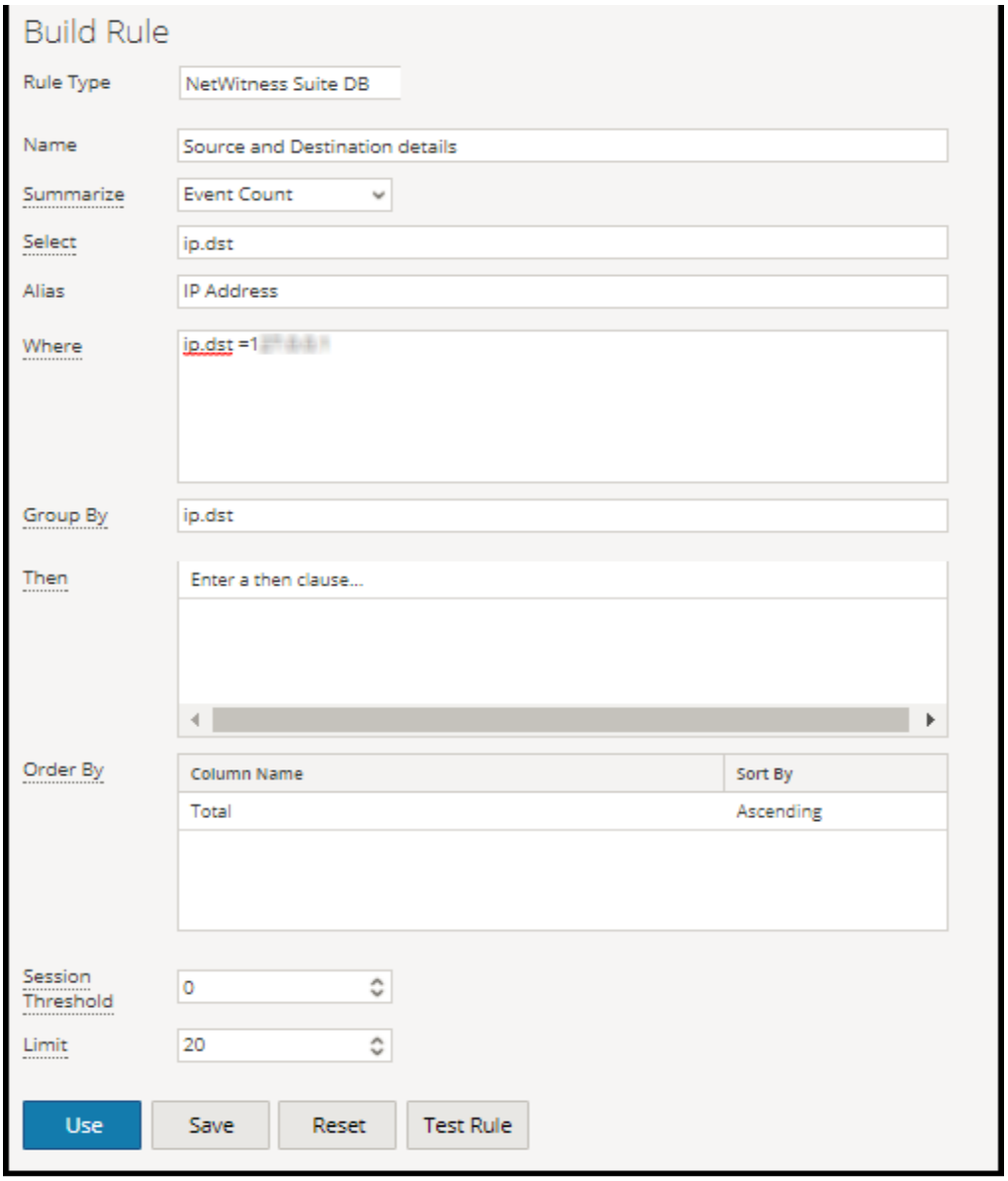
Make sure that you understand how custom meta keys are created using custom feeds. For more information, see "Create Custom Meta Keys using Custom Feed" topic in the *Decoder and Log Decoder Configuration Guide*.

To create a rule to fetch data or events from a NetWitness Data Source, perform the following:

1. Go to **MONITOR> Reports**.

   The Manage tab is displayed.

2. In the Rule toolbar, click + > **NetWitnessDB**.
   The Build Rule view tab is displayed.



3. In the **Rule Type** field, **NetWitness DB** is selected by default.
4. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.
5. The **Summarize** field determines the type of summarization or aggregation for the rule. Based on the type of rule to be defined, you must select one of the following:
   - To define a **Non-Aggregate** rule without any grouping, select: **None**
   - To define an **Aggregate** rule with special aggregation like the collection (sessions/events/packets) related aggregates, select one of the following:

- Event Count
- Packet Count
- Session Size

- To define an **Aggregate** rule with meta values and custom aggregates like sum(), count(), and so on, select: **Custom**

  Choosing 'Custom' in the **Summarize** field enables you to define aggregate function of your choice in the *Select* clause. For example, select ip.src, countdistinct(ip.dst), distinct(ip.dst). The supported aggregate functions are:

  - sum (<meta>)
  - count(<meta>)
  - countdistinct(<meta>)
  - min(<meta>)
  - max(<meta>)
  - avg(<meta>)
  - first(<meta>)
  - last(<meta>)
  - len(<meta>)
  - distinct(<meta>)

  For more detailed information about Aggregate and Non-aggregate rule, see "NWDB Rule Syntax section" in Rule Syntax .

6. In the **Select** field, enter a meta or select a meta from the list of available meta types provided in the Meta Library. For more information, see "Meta Panel" in Build Rule View. The meta name to fetch raw log is raw. raw can only be used in the **Select** field. It cannot be used in the **Where** and **Then** fields. Multiple aggregate functions are supported for Custom aggregate rule in the **Select** field. For example, Select: *ip.src, username, service, distinct(country.src), sum(payload).*
7. In the **Alias** field, enter the alias name for columns used in the Select clause.
8. In the **Where** field, enter a meta or select a meta from the list of available meta types and use the operators to construct the Where clause for the base query criteria.

9. The **Group By** field is a read-only field which gets populated with meta that are defined in the Select clause. For a Non-Aggregate function, this field is not visible. A maximum of six meta are supported in the **Group By** field.

   Note: In earlier versions of NetWitness Suite, only one meta was supported for Custom aggregate rule in the **Group By** clause. From now, a maximum of six meta are supported in the **Group By** clause.

10. In the **Then** field, enter the rule actions that manipulate the original result set of a rule in order to make the output in a report more concrete or add additional functionality other than querying data and displaying it, for example, creating a feed from the results. For a complete list of available rule actions, see "NWDB Rule Syntax" in Rule Syntax .

    Note: When a rule is executed for an Archiver data source, it is recommended not to use query intensive rule actions such as lookup_and_add() and show_whats_new().

11. In the **Order By** field, perform the following:

    a. In the **Column Name** column, enter the name of the columns by which you want to sort the results. By default, the value is empty. The value gets populated based on the value selected in the **Summarize** field.

       - For Summarize 'None', if no **Order By** is selected, then by default it is ordered by session or collection time.
       - For other Summarize values, the default sorting is based on the first 'group by' meta selected when no 'order by' is defined. For Event Count, Packet Count, and Session size, the accepted values are Total and Value.

    b. In the **Sort by** column, select one of the following ways to sort the results:

       - Ascending Order
       - Descending Order

12. In the **Session Threshold** field, enter the optimization setting to stop scanning the matching sessions for each possible unique value for the selected meta. The threshold is an integer between 0 (default) and 2147483647.

Note: This is applicable to only NWDB Aggregate rules. If the default value is specified, all the matching sessions will be scanned and the accurate value will be returned. A higher session threshold allows accurate counts for a value. However, this causes longer rule execution time. For example, consider you set the Session Threshold as 1000 for ip.src. If there are 5000 matching sessions then for a particular ip.src value which is present in more than 1000 sessions, NWDB stops the scan after 1000 sessions and returns the extrapolated aggregate value. This optimizes the query execution time. If the value is present in less than 1000 sessions, then the actual value is returned.

13. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by event count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.
14. Click **Save**.

Note: Unlike parsed meta, raw logs are fetched from decoders. When both raw log and parsed meta are queried in a single rule, due to different retention periods, parsed meta might be available and raw logs missing in the same session. So the result will have parsed meta values and empty raw value for those sessions. For example, for the rule Select **ip.src**, **ip.dst**, **service**, **username**, **raw**, the parsed meta might be populated and the **raw** meta remains empty for a few sessions.

Create a Rule Using Warehouse Data Source

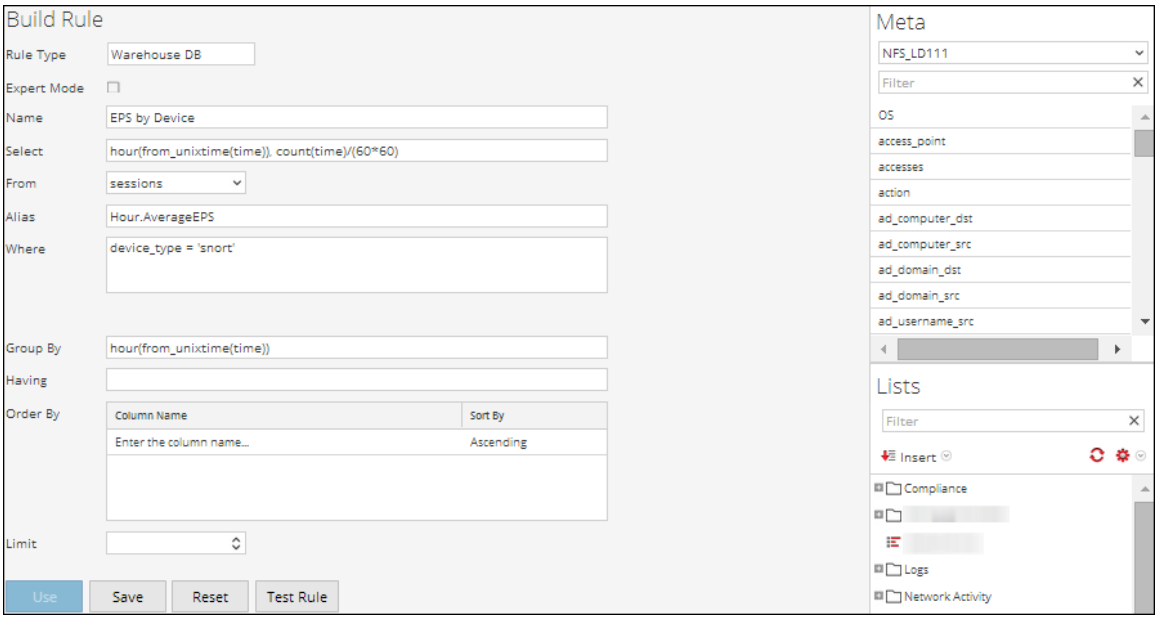
You can create a rule to fetch data or events from a Warehouse event source. You can define the rules in two modes:

- Default Mode
- Expert Mode

Default Mode

In Default Mode, you can create rules containing simple SQL like HIVE queries that contain clauses like Select, Where, Group By, and Having. By default, you can create rules to query sessions or raw logs. For more information on "Simple query syntax and examples", see Warehouse DB Simple Rules Syntax.

The following figure is an example of the **Build Rule view** that displays when you select **Warehouse DB** for **Rule Type** without the Expert Mode selected.

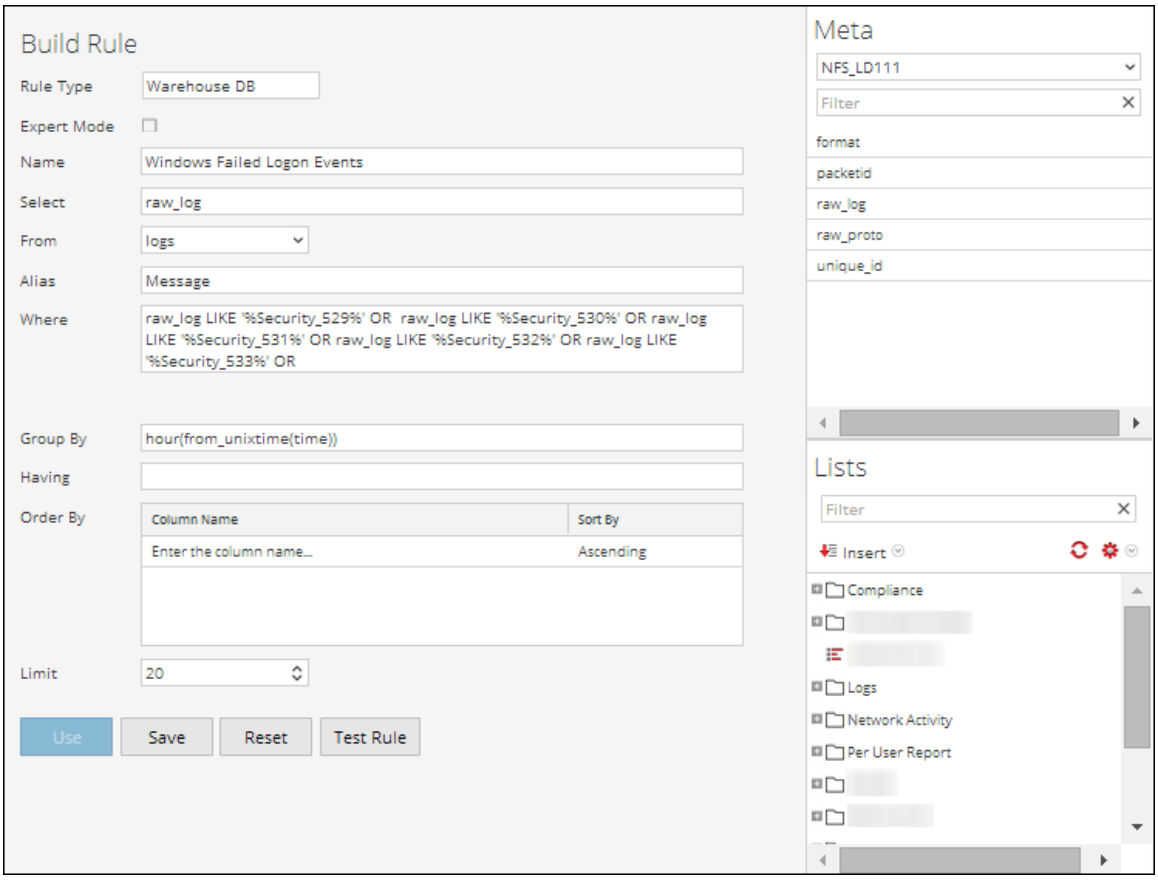


Querying Raw Logs

The raw log format is used in the select or where clause to query for raw logs.

Note: The time range that you can specify in your query is a day (24 hours). If you have specified a time range less than a day in your query, the result set contains data of at least a day (24 hours).

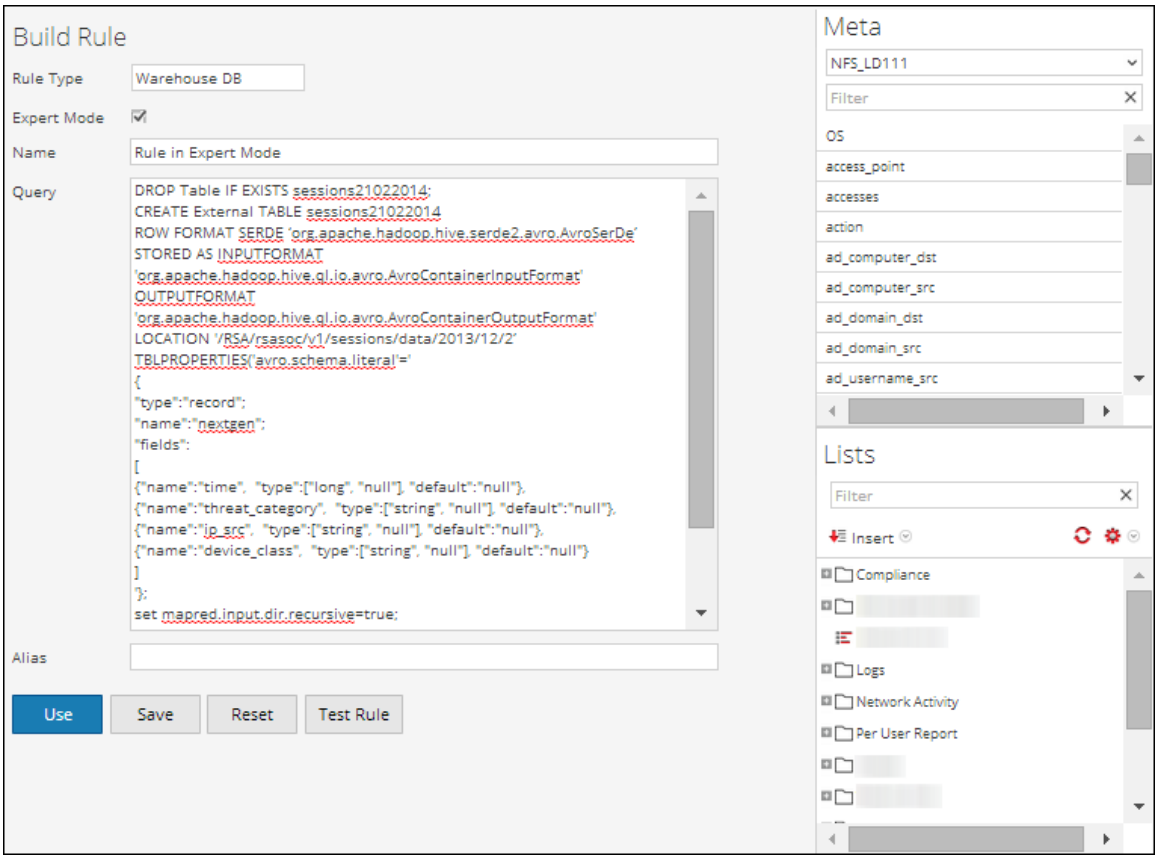
The following figure is an example of the **Build Rule view** that displays when you select **Warehouse DB** for **Rule Type** and create a rule for querying raw logs.



Expert Mode

Advanced rules are defined using complex HIVE queries created using the clauses DROP, CREATE, and so on. Unlike simple rules, we always insert the results into a table. For more information on "Advanced HIVE query language", see *HIVE language manual*.

The following figure is an example of the **Build Rule view** that displays when you select **Warehouse DB** for **Rule Type** with Expert Mode selected.



If you want to generate a report for a specific time range, you need to manually define the time range in the query using the following two variables:

- ${report_starttime} - The starting time of the range in seconds.
- ${report_endtime} - The ending time of the range in seconds.

For example, **SELECT col1, col2 FROM custom_table WHERE timecol >= ${report_starttime} AND timecol <= ${report_endtime};**

Note: By default, Reporting Engine treats `${keyword}` as a variable. If you want to specify HIVE variables, you must mention the complete syntax of a variable. For example, `${hiveconf:hive.exec.scratchdir}`.

Prerequisites

Make sure that you understand how custom meta keys are created using custom feeds. For more information, see "Create Custom Meta Keys using Custom Feed" topic in the *Host and Services Configuration Guide*.

To create a rule to fetch data or events from a Warehouse data source, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. In the Rule toolbar, click + > **Warehouse DB.**

   The Build Rule view is displayed.

3. In the **Rule Type** field, **Warehouse DB** is selected by default.

   If you are defining the rule in Default mode, perform the following:

   a. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.

   b. In the **Select** field, enter a meta or select the meta from the drop-down or select a meta from the list of available meta types provided in the Meta Panel. For more information, see " Meta Panel" in Build Rule View.

   c. In the **From** drop-down menu, select one of the following:

      - Session
      - Logs

   d. In the **Alias** field, enter the alias name for columns used in the Select clause.

   e. In the **Where** field, enter a meta or select a meta from the list of available meta types provided in the Meta Panel. The Where clause provides the base query criteria for the rule.

   f. In the **Group By** field, enter the meta selected in the Select clause, so that the result set is grouped based on the meta.

   g. In the **Having** field, enter the criteria to filter the result set for aggregated queries.

   h. In the **Order By** field, perform the following:

      1. In the **Column Name** column, enter the name of the columns by which you want to group the results.
      2. In the **Sort by** column, select one of the following ways to sort the results:

         - Ascending Order
         - Descending Order

i. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by session count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.

j. Click **Save**.

4. If you are defining the rule in Expert mode, select the **Expert Mode** checkbox and perform the following:

a. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.

b. In the **Query** field, enter the Hive query statement to query the data source.

c. In the **Alias** field, enter the alias name for columns used in the Select clause.

d. Click **Save**.

Create a Rule Using Respond Data Source

You can create a rule to fetch incidents or alerts from a Respond data source.

Prerequisites

Make sure that you:

- Ensure Reporting Engine service is up and running.
- Ensure the Incident Management service is up and running. For more information, see "Configure a Database for the Respond Server Service" topic in the *NetWitness Respond Configuration Guide*.
- (Optional) Ensure the Event Stream Analysis service is up and running. For more information, see "Step 2. Configure Advanced Settings for an ESA Service" topic in the *ESA Configuration Guide*.
- (Optional) Ensure the Malware Analysis service is up and running. For more information, see "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Configuration Guide*.

Note: You need to configure any one of the services (Event Stream Analysis, Reporting Engine, Malware Analysis, or Endpoint) based on your requirement and the type of alerts or incidents you want to generate.

To create a rule to fetch data or events from a Respond Data Source, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. In the Rule toolbar, click + > **RESPOND**.

   The Build Rule view tab is displayed.

3. In the **Rule Type** field, Respond is selected by default.

4. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and incident reports.

5. The **Summarize** field determines the type of summarization or aggregation for the rule. Based on the type of rule to be defined, you must select one of the following:

   - To define a **Non-Aggregate** rule without any grouping, select **None**
   - To define an **Aggregate** rule with meta values and custom aggregates select **Custom**

     Choosing 'Custom' in the **Summarize** field enables you to define aggregate function of your choice in the *Select* clause based on the report type you have selected.

     For more detailed information about Aggregate and Non-aggregate rule, see Rule Syntax .

6. In the **From** field, based on the type of report output to be displayed, you must select one of the following:

   - Alert
   - Incident

7. In the **Select**field, enter a meta or select a meta from the list of available meta types provided in the Meta Library. For more information, see "Meta Panel" in Build Rule View. It cannot be used in the **Where** field. Only one aggregate function is supported at a time in a query.

   For example, the supported metas for alert are:

- alert_host_summary
- alert.name
- alert.numEvents
- alert.severity
- alert.source
- alert.timestamp
- incidentCreated
- incidentId
- receivedTime

For example, the supported metas for incident are:

- categories
- created
- priority
- riskScore
- sealed
- status

For more detailed information, see "Aggregate and Non-aggregate rule" topic in the Rule Syntax .

8. In the **Alias** field, enter the alias name for columns used in the Select clause.
9. In the **Where** field, enter a meta or select a meta from the list of available meta types and use the operators to construct the Where clause for the base query criteria.
10. The **Group By** field is a read-only field which gets populated with meta that are defined in the Select clause. For a Non-Aggregate function, this field is not visible. A maximum of six meta are supported in the **Group By** field.
11. In the **Order By** field, perform the following:
    a. In the **Column Name** column, enter the name of the columns by which you want to sort the results.

Note: by default the first meta in the select clause will be dispalyed.

b. In the **Sort by** column, select one of the following ways to sort the results:

- Ascending Order
- Descending Order

12. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.
13. Click **Save**.

Deploy a Rule

In RSA NetWitness Suite you can deploy the selected rules on the service (for example, Reporting Engine), using the Deployment Wizard.

Prerequisites

Make sure that:

- The services on which you deploy a rule is up and running.
- The Live Services is configured.

To deploy a rule, perform the following:

1. Go to **CONFIGURE > LIVE CONTENT**.
2. In the **Search Criteria** panel, search Live resources (for example, search for the **Application Rule** resource Type).
3. In the **Matching Resources** panel, select **Show Results > Grid**.
4. Select the checkbox to the left or the rules that you want to deploy.
5. In the **Matching Resources** toolbar, click

.
6. Click **Next**.
7. Select the service on which you to deploy a rule (For example, Reporting Engine) and click **Next**.
8. Click **Deploy**.
   The rule is deployed successfully.

Use Meta Aliases for Reporting

When you refer to meta data in Reports and Charts, you can only view aliases for the meta names. These aliases makes them more understandable to a broader audience.

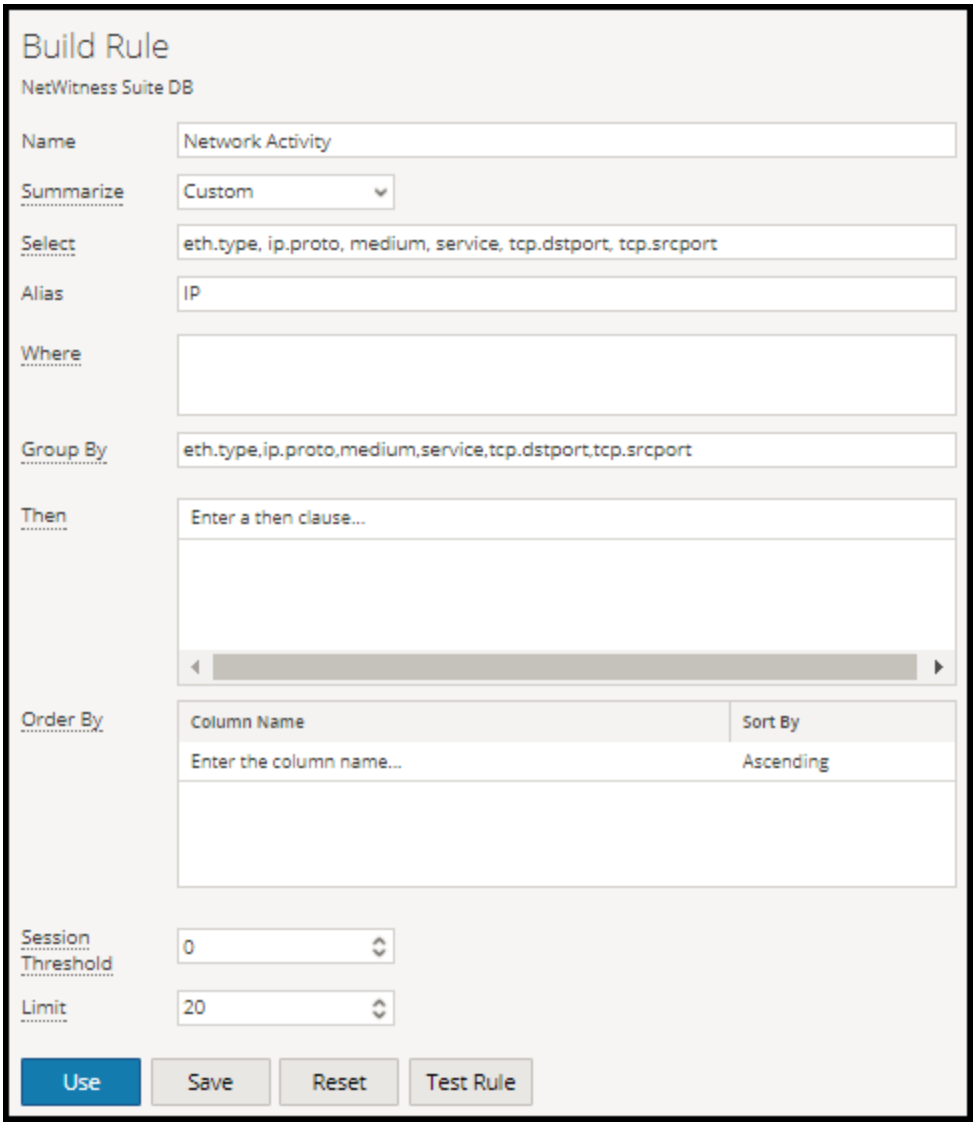
You cannot provide alias values for any meta in the WHERE clause because NetWitness Suite uses the WHERE clause to fetch data from the data source (for example, in the Concentrator) and data sources do not support aliases. In other words, you cannot provide the alias value **HTTP** for the HTTP port # 80.

Note: * You cannot create aliases for meta other than the ones that have existing aliases by Reporting Engine. Also, the format of the aliases cannot be changed.
* Aliases are not supported for Alerts and CSV reports.

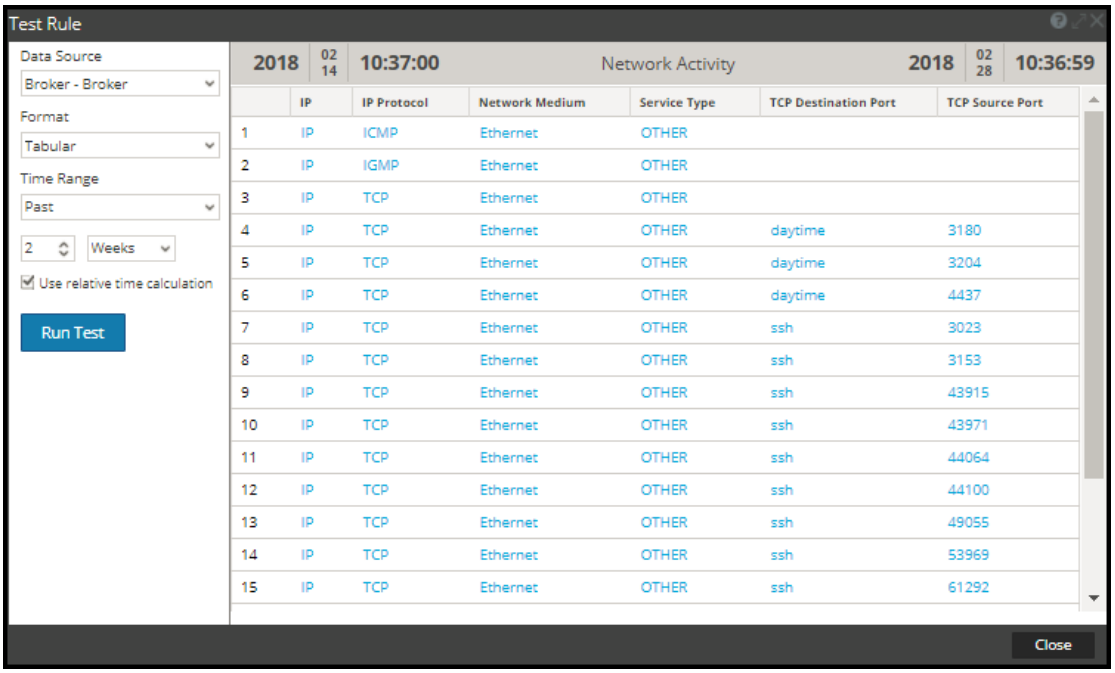
To use alias in a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the Rule List panel, do one of the following:
   - Select a rule and click in the Rules toolbar.
   - Click > **Edit**.
3. Specify the meta with aliases in the **Select** field.

The following example specifies the **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport**, and **tcp.srcport** meta in the Select field.



4. Click **Test Rule**.
   The following example displays the results under the **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport**, and **tcp.srcport** alias columns that were specified in the **Select** field of the rule.



	IP	IP Protocol	Network Medium	Service Type	TCP Destination Port	TCP Source Port
1	IP	ICMP	Ethernet	OTHER		
2	IP	IGMP	Ethernet	OTHER		
3	IP	TCP	Ethernet	OTHER		
4	IP	TCP	Ethernet	OTHER	daytime	3180
5	IP	TCP	Ethernet	OTHER	daytime	3204
6	IP	TCP	Ethernet	OTHER	daytime	4437
7	IP	TCP	Ethernet	OTHER	ssh	3023
8	IP	TCP	Ethernet	OTHER	ssh	3153
9	IP	TCP	Ethernet	OTHER	ssh	43915
10	IP	TCP	Ethernet	OTHER	ssh	43971
11	IP	TCP	Ethernet	OTHER	ssh	44064
12	IP	TCP	Ethernet	OTHER	ssh	44100
13	IP	TCP	Ethernet	OTHER	ssh	49055
14	IP	TCP	Ethernet	OTHER	ssh	53969
15	IP	TCP	Ethernet	OTHER	ssh	61292

RSA-Supplied Alias Definitions

The alias files in this section are examples only and are based on current alias definitions in the Reporting Engine. NetWitness Suite cannot modify these definitions in the Reporting Engine depending on the changes in the concentrator xml file. Since any changes in the Concentrator xml file are not reflected in the Reporting Engine.

The details of different meta are explained in each of the **meta.aliases**.

eth.type

```
ALIAS_FORMAT=$alias
 0=802.3
 257=Experimental
 512=Xerox PUP
 513=Xerox PUP
 1024=Nixdorf
 1536=Xerox NS IDP
 1537=XNS Address Translation (3Mb only)
 2048=IP
 2049=X.75 Internet
 2050=NBS Internet
 2051=ECMA Internet
 2052=CHAOSnet
 2053=X.25 Level 3
 2054=ARP
 2055=XNS Compatibility
 2076=Symbolics Private
```

```
 2184=Xyplex
 2304=Ungermann-Bass network debugger
 2560=Xerox IEEE802.3 PUP
 2561=Xerox IEEE802.3 PUP Address Translation
 2989=Banyan Systems
 2991=Banyon VINES Echo
 4096=Berkeley Trailer negotiation
 4097=Berkeley Trailer encapsulation for IP
 4660=DCA - Multicast
 5632=VALID system protocol
 6537=Artificial Horizons
 6549=Datapoint Corporation (RCL lan protocol)
 15360=3Com NBP virtual circuit datagram (like XNS SPP)
not registered
 15361=3Com NBP System control datagram not registered
 15362=3Com NBP Connect request (virtual cct) not
registered
 15363=3Com NBP Connect repsonse not registered
 15364=3Com NBP Connect complete not registered
 15365=3Com NBP Close request (virtual cct) not
registered
 15366=3Com NBP Close response not registered
 15367=3Com NBP Datagram (like XNS IDP) not registered
 15368=3Com NBP Datagram broadcast not registered
 15369=3Com NBP Claim NetBIOS name not registered
 15370=3Com NBP Delete Netbios name not registered
 15371=3Com NBP Remote adaptor status request not
registered
 15372=3Com NBP Remote adaptor response not registered
 15373=3Com NBP Reset not registered
 16972=Information Modes Little Big LAN diagnostic
 17185=THD - Diddle
 19522=Information Modes Little Big LAN
 21000=BBN Simnet Private
 24576=DEC unassigned
 24577=DEC Maintenance Operation Protocol (MOP) Dump/Load
Assistance
 24578=DEC Maintenance Operation Protocol (MOP) Remote
Console
 24579=DECNET Phase IV
 24580=DEC Local Area Transport (LAT)
 24581=DEC diagnostic protocol (at interface
initialization?)
 24582=DEC customer protocol
 24583=DEC Local Area VAX Cluster (LAVC)
 24584=DEC AMBER
 24585=DEC MUMPS
 24592=3Com Corporation
```

```
 28672=Ungermann-Bass download
 28673=Ungermann-Bass NIUs
 28674=Ungermann-Bass diagnostic/loopback
 28675=Ungermann-Bass ??? (NMC to/from UB Bridge)
 28677=Ungermann-Bass Bridge Spanning Tree
 28679=OS/9 Microware
 28681=OS/9 Net?
 28704=LRT (England) (now Sintrom)
 28720=Racal-Interlan
 28721=Prime NTS (Network Terminal Service)
 28724=Cabletron
 32771=Cronus VLN
 32772=Cronus Direct
 32773=HP Probe protocol
 32774=Nestar
 32776=AT&amp;amp;T/Stanford Univ.
 32784=Excelan
 32787=Silicon Graphics diagnostic
 32788=Silicon Graphics network games
 32789=Silicon Graphics reserved
 32790=Silicon Graphics XNS NameServer
 32793=Apollo DOMAIN
 32814=Tymshare
 32815=Tigan
 32821=Reverse Address Resolution Protocol (RARP)
 32822=Aeonic Systems
 32823=IPX (Novell Netware?)
 32824=DEC LanBridge Management
 32825=DEC DSM/DDP
 32826=DEC Argonaut Console
 32827=DEC VAXELN
 32828=DEC DNS Naming Service
 32829=DEC Ethernet CSMA/CD Encryption Protocol
 32830=DEC Distributed Time Service
 32831=DEC LAN Traffic Monitor Protocol
 32832=DEC PATHWORKS DECnet NETBIOS Emulation
 32833=DEC Local Area System Transport
 32834=DEC unassigned
 32836=Planning Research Corp.
 32838=AT&amp;amp;T
 32839=AT&amp;amp;T
 32840=DEC Availability Manager for Distributed Systems
DECamds
 32841=ExperData
 32859=VMTP
 32860=Stanford V Kernel
 32861=Evans &amp;amp; Sutherland
 32864=Little Machines
```

```
 32866=Counterpoint Computers
 32869=University of Mass. at Amherst
 32870=University of Mass. at Amherst
 32871=Veeco Integrated Automation
 32872=General Dynamics
 32873=AT&amp;amp;T
 32874=Autophon
 32876=ComDesign
 32877=Compugraphic Corporation
 32878=Landmark Graphics Corporation
 32890=Matra
 32891=Dansk Data Elektronik
 32892=Merit Internodal
 32893=Vitalink Communications
 32896=Vitalink TransLAN III Management
 32897=Counterpoint Computers
 32904=Xyplex
 32923=EtherTalk - AppleTalk over Ethernet
 32924=Datability
 32927=Spider Systems Ltd.
 32931=Nixdorf Computers
 32932=Siemens Gammasonics Inc.
 32960=DCA Data Exchange Cluster
 32966=Pacer Software
 32967=Applitek Corporation
 32968=Intergraph Corporation
 32973=Harris Corporation
 32975=Taylor Instrument
 32979=Rosemount Corporation
 32981=IBM SNA Services over Ethernet
 32989=Varian Associates
 32990=TRFS (Integrated Solutions Transparent Remote File
System)
 32992=Allen-Bradley
 32996=Datability
 33010=Retix
 33011=AppleTalk Address Resolution Protocol (AARP)
 33012=Kinetics
 33015=Apollo Computer
 33023=Wellfleet Communications
 33026=Wellfleet BOFL
 33027=Wellfleet Communications
 33031=Symbolics Private
 33067=Talaris
 33072=Waterloo Microsystems Inc.
 33073=VG Laboratory Systems
 33079=IPX
 33080=Novell Inc
```

```
33081=KTI
33087=M/MUMPS data sharing
33093=Vrije Universiteit (NL)
33094=Vrije Universiteit (NL)
33095=Vrije Universiteit (NL)
33100=SNMP
33103=Technically Elite Concepts
33169=PowerLAN
33149=XTP
33238=Artisoft Lantastic
33239=Artisoft Lantastic
33283=QNX Software Systems Ltd.
33680=Accton Technologies (unregistered)
34091=Talaris multicast
34178=Kalpana
34525=IPv6
34617=Control Technology Inc.
34618=Control Technology Inc.
34619=Control Technology Inc.
34620=Control Technology Inc.
34848=Hitachi Cable (Optoelectronic Systems Laboratory)
34902=Axis Communications AB
34952=HP LanProbe test?
36864=Loopback (Configuration Test Protocol)
36865=3Com XNS Systems Management
36866=3Com TCP/IP Systems Management
36867=3Com loopback detection
43690=DECNET
64245=Sonix Arpeggio
65280=BBN VITAL-LanBridge cache wakeups
34915=PPPoe
34916=PPPoe
2056=Frame Relay ARP
16962=IEEE bridge spanning protocol
25944=Bridged Ethernet/802.3 packet
65278=ISO CLNP/ISO ES-IS DSAP/SSAP
```

ip.proto

```
ALIAS_FORMAT=$alias
 0=HOPOPT
 1=ICMP
 2=IGMP
 3=GGP
 4=IP
 5=ST
 6=TCP
 7=CBT
 8=EGP
```

```
9=IGP
10=BBN-RCC-M
11=NVP-II
12=PUP
13=ARGUS
14=EMCON
15=XNET
16=CHAOS
17=UDP
18=MUX
19=DCN-MEAS
20=HMP
21=PRM
22=XNS-IDP
23=TRUNK-1
24=TRUNK-2
25=LEAF-1
26=LEAF-2
27=RDP
28=IRTP
29=ISO-TP4
30=NETBLT
31=MFE-NSP
32=MERIT-INP
33=SEP
34=3PC
35=IDPR
36=XTP
37=DDP
38=IDPR-CMTP
39=TP++
40=IL
41=IPv6
42=SDRP
43=IPv6-Rout
44=IPv6-Frag
45=IDRP
46=RSVP
47=GRE
48=MHRP
49=BNA
50=ESP
51=AH
52=I-NLSP
53=SWIPE
54=NARP
55=MOBILE
56=TLSP
```

```
57=SKIP
58=IPv6-ICMP
59=IPv6-NoNx
60=IPv6-Opts
61=AnyHost
62=CFTP
63=AnyNetwork
64=SAT-EXPAK
65=KRYPTOLAN
66=RVD
67=IPPC
68=AnyFile
69=SAT-MON
70=VISA
71=IPCV
72=CPNX
73=CPHB
74=WSN
75=PVP
76=BR-SAT-MO
77=SUN-ND
78=WB-MON
79=WB-EXPAK
80=ISO-IP
81=VMTP
82=SECURE-VM
83=VINES
84=TTP
85=NSFNET-IG
86=DGP
87=TCF
88=EIGRP
89=OSPFIGP
90=Sprite-RP
91=LARP
92=MTP
93=AX.25
94=IPIP
95=MICP
96=SCC-SP
97=ETHERIP
98=ENCAP
99=AnyPrivate
100=GMTP
101=IFMP
102=PNNI
103=PIM
104=ARIS
```

```
105=SCPS
106=QNX
107=A/N
108=IPComp
109=SNP
110=Compaq-Pe
111=IPX-in-IP
112=VRRP
113=PGM
114=AnyHop
115=L2TP
116=DDX
117=IATP
118=STP
119=SRP
120=UTI
121=SMP
122=SM
123=PTP
124=ISIS
125=FIRE
126=CRTP
127=CRUDP
128=SSCOPMCE
129=IPLT
130=SPS
131=PIPE Pr
132=SCTP St
133=FC Fi
134=RSVP-E2E-
255=Reserved
```

medium

```
ALIAS_FORMAT=$alias
1=Ethernet
2=Tokenring
3=FDDI
4=HDLC
5=NetWitness
6=802.11
7=802.11 Radio
8=802.11 AVS
9=802.11 PPI
10=802.11 PRISM
11=802.11 Management
12=802.11 Control
13=DLT Raw
32=Logs
```

service

```
ALIAS_FORMAT=$alias
 0=OTHER
 20=FTPD
 21=FTP
 22=SSH
 23=TELNET
 25=SMTP
 53=DNS
 67=DHCP
 69=TFTP
 80=HTTP
 110=POP3
 111=SUNRPC
 119=NNTP
 123=NTP
 135=RPC
 137=NETBIOS
 139=SMB
 143=IMAP
 161=SNMP
 179=BGP
 443=SSL
 502=MODBUS
 520=RIP
 1024=EXCHANGE
 1080=SOCKS
 1122=MSN IM
 1344=ICAP
 1352=NOTES
 1433=TDS
 1521=TNS
 1533=SAMETIME
 1719=H.323
 1720=RTP
 2000=SKINNY
 2040=SOULSEEK
 2049=NFS
 3270=TN3270
 3389=RDP
 3700=DB2
 5050=YAHOO IM
 5060=SIP
 5190=AOL IM
 5222=Google Talk
 5900=VNC
 6346=GNUTELLA
 6667=IRC
```

```
 6801=Net2Phone
 6881=BITTORRENT
 8000=QQ
 8002=YCHAT
 8019=WEBMAIL
 8082=FIX
 20000=DNP3
 1000000=KERNEL
 1000001=USER
 1000003=SYSTEM
 1000004=AUTH
 1000005=LOGGER
 1000006=LPD
 1000008=UUCP
 1000009=SCHEDULE
 1000010=SECURITY
 1000013=AUDIT
 1000014=ALERT
 1000015=CLOCK
```

tcp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
```

```
119=nntp
135=epmap
137=netbios-ns
139=netbios-ssn
143=imap
158=pcmail-srv
170=print-srv
179=bgp
194=irc
389=ldap
443=https
445=cifs
464=kpasswd
512=exec
513=login
514=cmd
515=printer
520=efs
526=tempo
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
2049=nfs
3389=rdp
5050=yahoo im
5060=sip
```

```
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

tcp.srcport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
 464=kpasswd
```

```
512=exec
513=login
514=cmd
515=printer
520=efs
526=tempo
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
2049=nfs
3389=rdp
5050=yahoo im
5060=sip
5190=aim
6346=gnuetella
6667=irc
9001=tor
9030=tor
9535=man
```

udp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 37=time
 39=rlp
 42=nameserver
 53=domain
 67=bootps
 68=bootpc
 69=tftp
 88=kerberos
 111=sunrpc
 123=ntp
 135=epmap
 137=netbios-ns
 138=netbios-dgm
 161=snmp
 162=snmptrap
 213=ipx
 443=https
 445=cifs
 464=kpasswd
 500=isakmp
 512=biff
 513=who
 514=syslog
 517=talk
 518=ntalk
 525=timed
 533=netwall
 550=new-rwho
 560=rmonitor
 561=monitor
 749=kerberos-adm
 1167=phone
 1433=ms-sql-s
 1434=ms-sql-m
 1512=wins
 1701=l2tp
 1812=radiusauth
 1813=radacct
 2049=nfsd
 2504=nlbs
```

Test a Rule

You can test a rule based on the time range and the data source selected.

To test a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the Rule List panel, do one of the following:
   - Select a rule and click in the Rules toolbar.
   - Click > **Edit**.
     The Build Rule view tab is displayed.
3. Click **Test Rule**.
   The Test Rule view is displayed.

> **Note:** When you click **Test Rule**, the rule is not saved. You have to click **Save** in the Build Rule view to save the rule.

4. From the **Data Source** drop-down list, select a data source.
   You must select the appropriate data source for the rule defined.
5. From the **Format** drop-down list, select the format in which you want the result displayed.

6. From the **Time Range** drop-down list, select one of the following.
   - **Past** -To specify number of years, days, weeks, months, days or hours.
   - **Range** - To specify a date range and time period.

   Note: In the User Interface (UI), the date or time displayed depends on the time zone profile selected by the user.

7. **X-Axis** and **Y-Axis** are used to specify the meta to be plotted in charts. In **X-Axis**, the Meta for the 'Group by' rule is displayed. In **Y-Axis**, the aggregate functions used in the rule are displayed.

Note: Sum, Count, Countdistinct and Average are the supported aggregate functions for rule. By default, for Custom Rules with multiple 'Group by', you can select only the first meta in **X-Axis**.

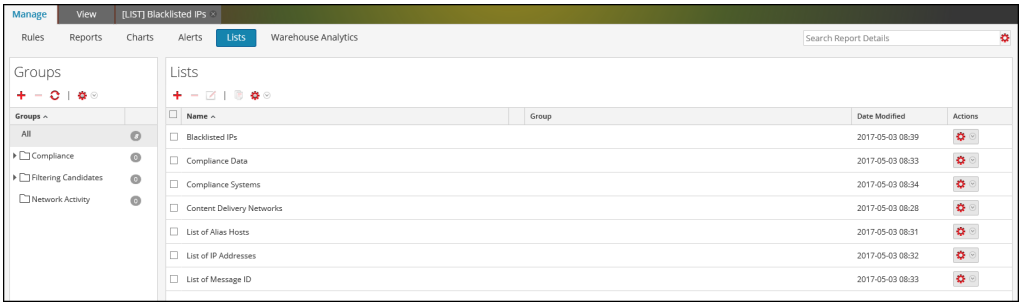
8. Click **Run Test** to execute the rule.
   The rule data (if any) for the selected time range is displayed.

Create a Lists or List Group

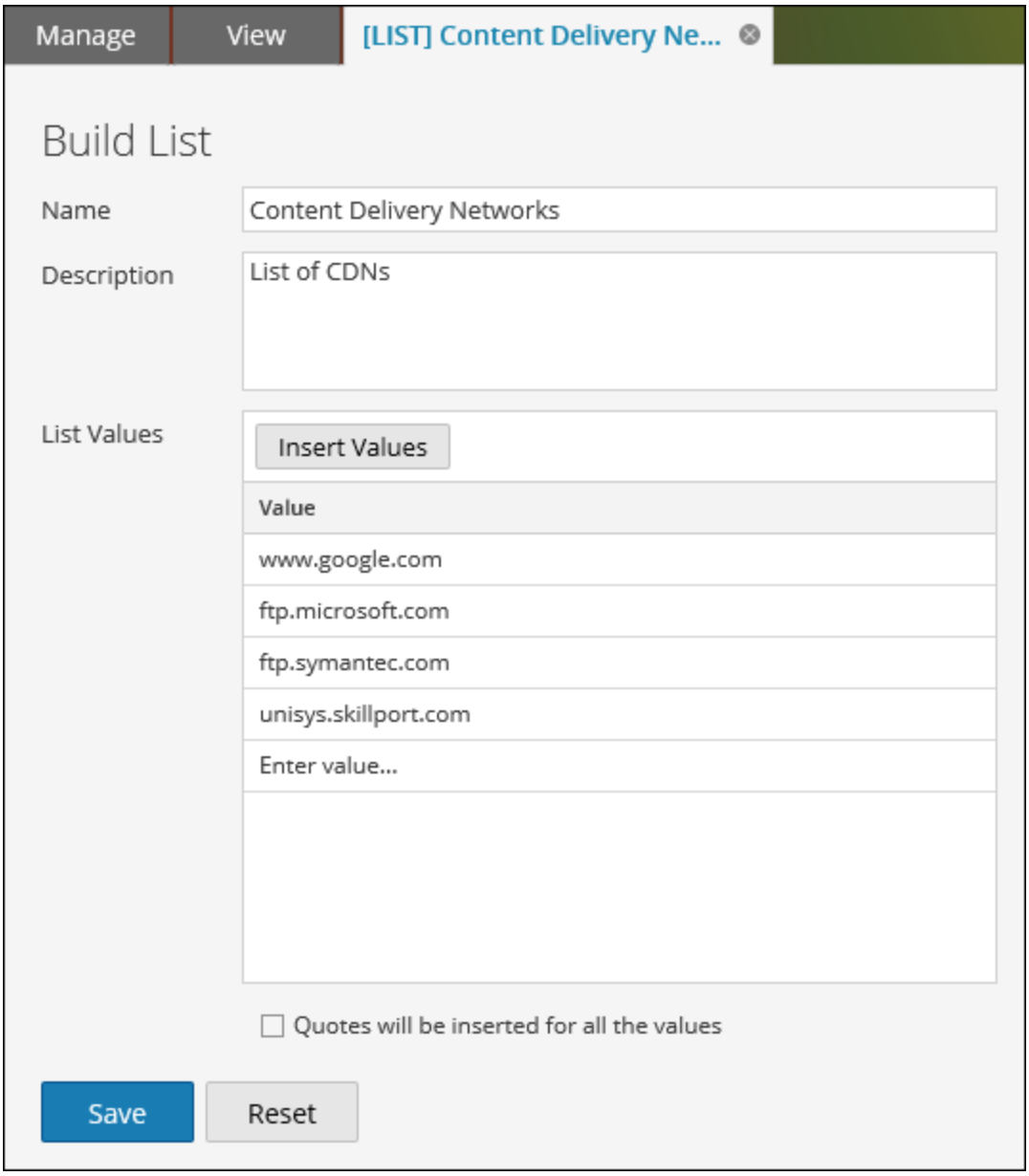
To create a list, perform the following:

Lists can be added within a group or in the root folder.

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. In the **List** toolbar, click +.
   The Build List view tab is displayed.

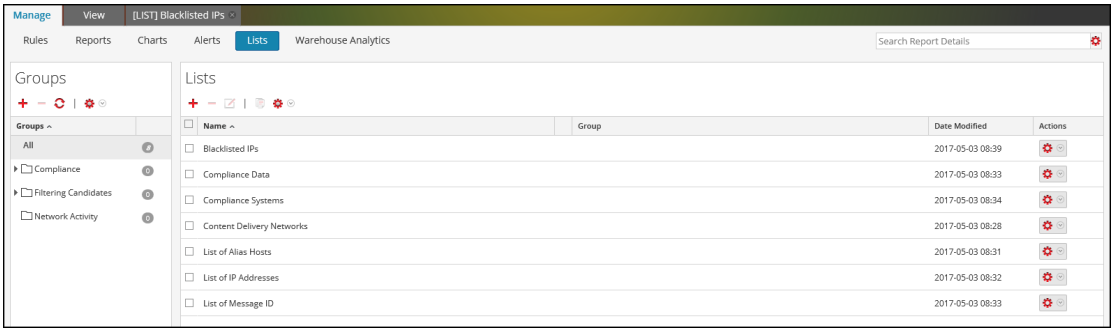


4. In the **Name** field, enter a unique name for the list.
5. In the **Description** field, enter a description for the list.
6. In the **List Values** field, do one of the following:
   - Click **Insert** and enter the values separated by commas. You can paste a list of values from a file or other lists.
   - In the **Value** column, enter the values.
7. If you want quotes to be inserted directly for the values at runtime, select **Quotes will be inserted for all the values**.

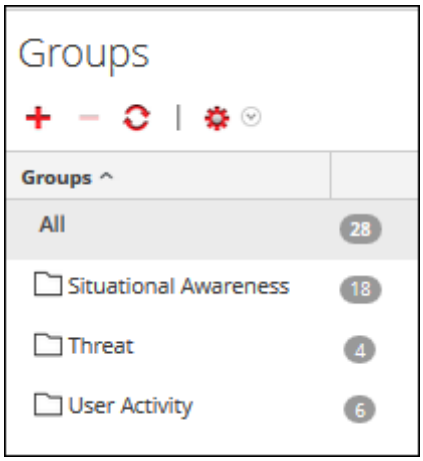
8. Click **Save**.

To create a list group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. Do the following:
   - To create a list group
     1. In the List Groups panel, click + .
        A new list group is added to the List Groups panel.



     2. Enter the name for the list group and press ENTER.
   - To create a list subgroup:
     1. In the List Groups panel, select the list group to which you want to add a subgroup.
     2. Click +.

A new list subgroup is added to the list group.

3. Enter the name for the list subgroup and press ENTER.

Create and Schedule a Report

You can create a simple or complex report and configure its execution properties by scheduling a report. A report can include multiple rules and you can schedule different time range to execute the same report. For example, depending on your requirement, you can schedule a report to run daily, weekly or monthly.

When you run a report, the results are stored in Reporting Engine.

After you generate a report, you can perform the following:

- Send the reports by email to other users by configuring the output actions. You can also configure the output actions before generating a report.
- Download the reports as PDF or Comma-Separated Values (CSV) format files.

Note: The cancel operation is not supported for Respond Reports.

Create a Report or Report Group

To create a report to a group or sub-group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** toolbar, click .
   The Build Report tab is displayed.
4. Enter the name of the report.
5. Drag and drop the text and rules to the report.

   Note: The text entered is optional and you may need this option only when you want to display user-defined headers or content.
6. Click **Save**.
   A confirmation message that the report is saved successfully is displayed.

To create a group to the default folder or add sub-groups under a report group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report Groups** panel, click +.
   A default group is added in the Report Groups panel.
4. Enter the name of the new group.
5. Press **Enter**.
   The group is added to the Report Groups panel.

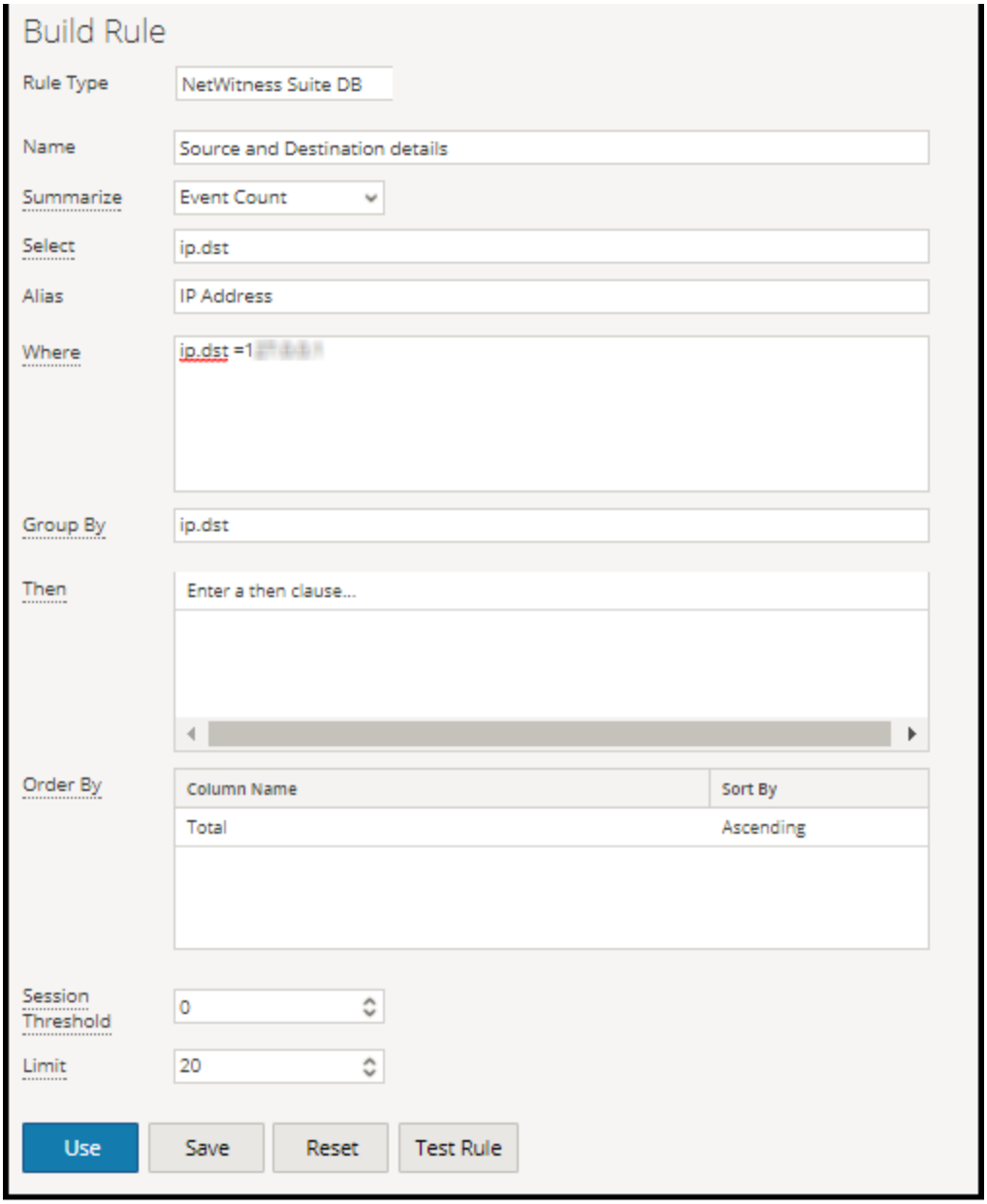
Schedule a Report

Note: When you schedule a Warehouse report, you can use a supported task scheduler to allocate specific resources in a cluster for the scheduled job. For more information on "supported task schedulers", see Task Scheduler for Warehouse Reporting.

To schedule a report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Build Rule** page, click + to create a rule.
4. Click **Save**.

5. Click **Use**.



6. Select the **New report** or **Existing Report**.
7. Select a report group and click **Select**.
8. Enter the Report name and select the rule.
9. Click **Schedule**.
   The Schedule Report view is displayed.

> **Note:** If you provide another user with access permissions to a report, you must also provide permissions for the report group, the rules used in the report, and the rule groups otherwise an error message is displayed.

8. To execute the reports as per the schedule, select the **Enable** checkbox.
9. In the **Schedule Name** field, enter a name for the schedule report configuration.
10. From the Data Source field, select the data source.

> **Note:** If the data source is not listed, then ensure you have **Read**permissions set for the data source. This is applicable for NWDB, Respond and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in *Reporting Engine Configuration Guide*.

11. (Optional) From the **Warehouse Resource Pool** drop-down, select the pools or queues available in the cluster to schedule the report to run on either the pool or queue. This drop-down list is available only if you select a Warehouse DB report.

> **Note:** All the queues or pools you specified in the Explore page for the Reporting Engine are listed. If no pools or queues are configured in the Explorer page, this drop-down is disabled and the jobs are submitted to the clusters without any a queue or pool name.

> **Note:** If the pool or queue configured in the report schedule is removed from the Cluster, then in the Capacity Scheduler, the queue name remains undefined. However, in the Fair Scheduler, the specified pool name will be created using the property mapred.fairscheduler.allow.undeclared.pool.

12. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format. This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
13. From the **Run** field, select the type of run schedule. (For example, Now or Hourly).

    Depending on the type of run schedule, do either of the following:

- If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
- If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
- If you select a **Daily** run schedule, you must enter a value in the **At** field.
- If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

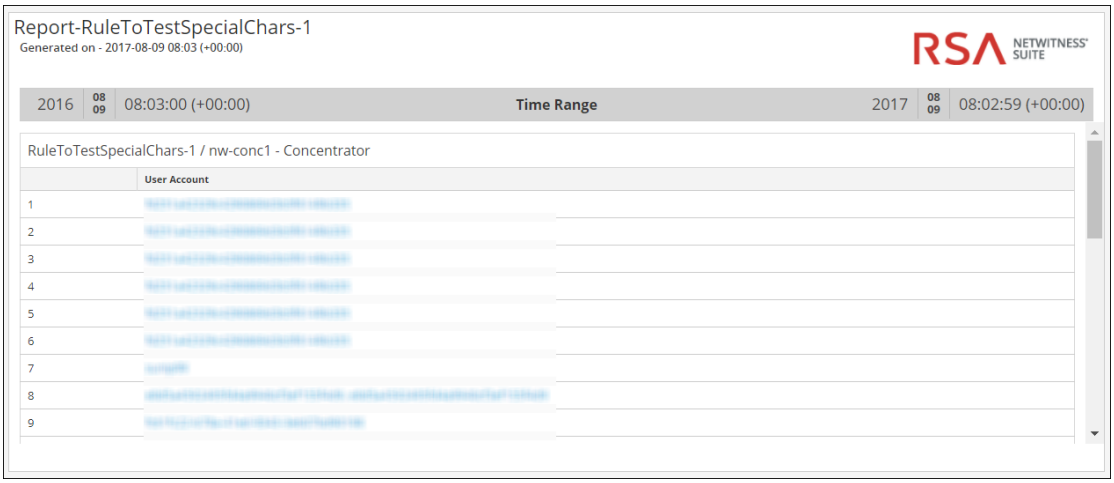
Note: While scheduling a report, if you select **Past** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.

For information on "how to generate a report with variables", see Create a Parameterized Report Using Variable.

14. (Optional) In the **Output Actions** panel, do the following:
    a. Enter the email address and subject.
    b. Edit the body of the message for the report.
    c. Select the format of the attachment.
    d. Enter a value for the CSV and Multi-value delimiters.
    e. (Optional) In the Other Options field, do the following:
        i. Click and select SFTP, URL, or Network Share output action.
        A row gets added with the selected output action.
        ii. Select the appropriate options to send the report in PDF or CSV format, or both to the RE configured SFTP, or URL, or Network Share output action.
15. (Optional) To add a list in the Dynamic List panel, see Generate a List from the Scheduled Report.
16. (Optional) To choose a logo in the Logo panel, see "Manage and Select a Report Logo" section in Manage Lists, Rules or Reports .

Note: If you do not specify a logo, the default RSA logo will be used.

17. Click **Schedule**.
    The scheduled report executes as scheduled and provides the configured outputs.



After you create and Schedule a report, you can perform any of the following tasks:

1. You can notify the email recipient when the report execution completes and send reports in PDF and CSV formats as attachments in the email.
2. You can generate a list based on the scheduled report and view them in the **Lists** module.
3. You can send a scheduled report in PDF or CSV format, or both to the RE configured SFTP location, or URL, or Network Share.
4. You can change the default logo and view them in the scheduled report.
5. You can modify the NetWitness Suite Reporting Engine config details, by navigating to the Reporting Engine General Tab. See the "Reporting Engine General Tab" topic in the *Reporting Engine Guide*.

Examples

When you schedule reports in the Schedule Report view, by default, the results for the **Past** option are presented based on the user specified time zone. The following examples provide a clear picture on what results to expect when you select **Hours**, **Days**, **Weeks**, **Months**, or **Years** for the **Past** option based on the absolute or relative duration.

Note: By default, the relative duration checkbox is de-selected. This implies that the results for the **Past** option are presented based on the absolute duration.

- **Based on Absolute duration** - Absolute Duration allows a report to be scheduled at an absolute time with respect to the current time, excluding the seconds and considering the time interval as a whole. For example, 12.00pm is the absolute time with respect to the current time (12.45 pm).
  - Hours - Suppose that you select Hours and specify one hour. If the current user specified time is 4.20PM, the report is generated for the time range, 3.00PM to 4.00PM.
  - Days - Suppose that you select Days and specify one day. If the current date is August 27, 2014 and the current user specified time is 10.15AM, the report is generated for the range: August 26, 2014, 12.00AM to August 27, 2014, 12.00AM.
  - Weeks - Suppose that you select Weeks and specify one week. If the current date is August 27, 2014 2.30PM and the day is Wednesday, the report is generated for the range: Saturday, August 16, 2014, 12.00AM to Saturday, August 23, 2014, 12.00AM.
  - Months - Suppose that you select Months and specify one month. If the current date is August 27, 2014 2.30PM, the report is generated for the range:
    July 01, 2014, 12.00AM to July 31, 2014, 12.00AM.
  - Years - Suppose that you select Years and specify one year.If the current date is August 27, 2014 2.30PM, the report is generated for the range:
    January 01, 2013, 12.00AM to December 31, 2013, 12.00AM.
- **Based on Relative duration** - Relative Duration allows a report to be scheduled at a time relative to the current time which might vary based on the current time. For example, 12.45 pm is the relative time with respect to the current time (12.45 pm).
  - Hours - Suppose that you select Hours and specify one hour. If the current user specified time is 4.20PM, the report is generated for the time range, 3.20PM to 4.20PM.
  - Days - Suppose that you select Days and specify one day. If the current date is August 27, 2014 and the current user specified time is 10.15AM, the report is generated for the range: August 26, 2014, 10.15AM to August 27, 2014, 10.15AM.

- Weeks - Suppose that you select Weeks and specify one week. If the current date is August 27, 2014 12.30PM and the day is Wednesday, the report is generated for the range: Thursday, August 21, 2014 12.30PM to Wednesday, August 27, 2014 12.30PM.
- Months - Suppose that you select Months and specify one month. If the current date is August 27, 2014, 2.30PM the report is generated for the range:
  July 27, 2014 2.30PM to August 27, 2014 2.30PM.
- Years - Suppose that you select Years and specify one year.If the current date is August 27, 2014 2.30PM, the report is generated for the range: August 27, 2013 2.30PM to August 27, 2014 2.30PM.

Additional Procedures

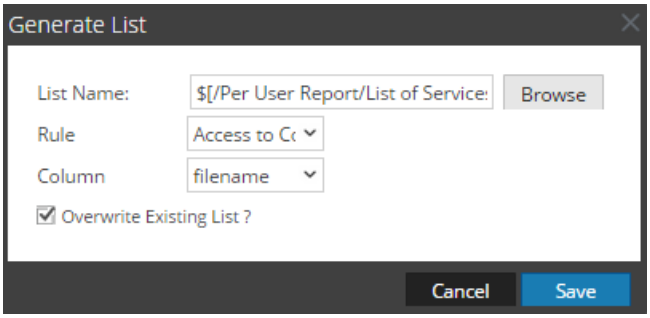
Generate a List from the Scheduled Report

You can generate a list from the output of the scheduled report. Make sure that your lists are created in NetWitness Suite prior to generating a list to schedule a report.

To generate a list from the Build Report view, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report and click > **Schedule Report**.
   The Schedule a Report view tab is displayed.
4. In the **Dynamic List** panel, click .
   The Generate List dialog box opens.
5. Click **Browse**.
   The List Selection panel is displayed.
6. Choose a list item and click **Select**.
   The list name gets populated in the List Name field.

7. Select a valid rule to filter the report results further based on the rule definition.
8. Select a value for the **Column** field.
   The column forms the values for the list that gets created.
9. If you want to overwrite the existing list, select the **Overwrite Existing List?** checkbox.
10. Click **Save**.
    The list name gets populated in the Generate List panel.



11. (Optional) Select a list from the Generate List panel and click − to delete the selected list.
12. (Optional) Select a list from the Generate List panel and click to edit the list details.

Create a Parameterized Report Using Variable

You use variables for reporting in the RSA NetWitness Suite Reporting module. Parameterized reporting allows you to specify values dynamically at runtime without changing the rule definition so you can view the results based on a particular value. You can achieve parameterize reporting by using variables in the query or rule. For information on adding a rule, see Configure a Rule. At runtime, you can enter the value for the variable or select the value from the list based on which the result set is displayed.

The syntax to specify the variable is as follows:

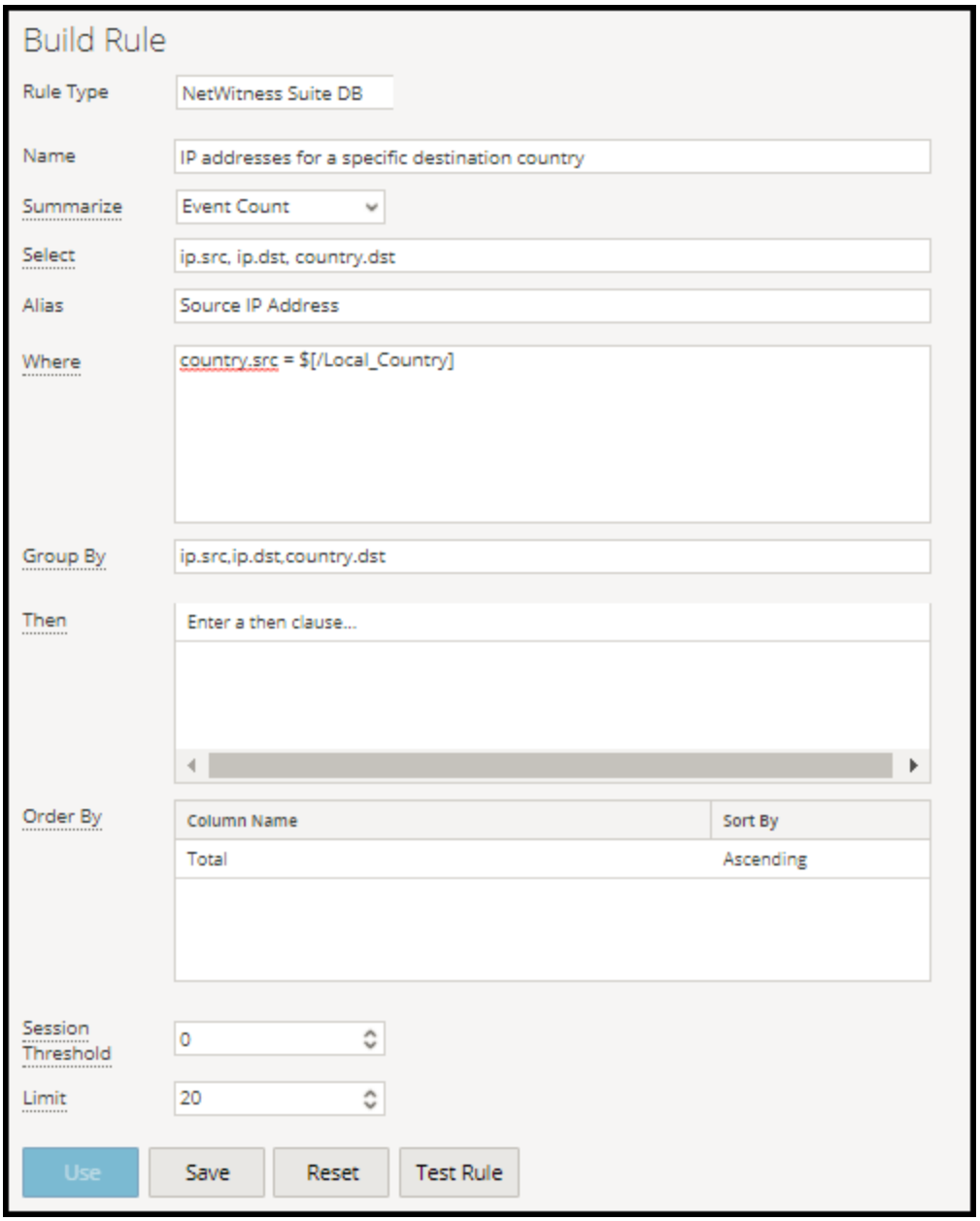
Description	Examples of Supported Syntax
Insert $ before a variable. Enclose a variable within braces.	`columnname=${<variable>}`

The syntax to define the variable is the same for NetWitness DB and Warehouse DB data sources. When you assign the value of the variable in a Run Configuration, you must enclose the value within single quotes: `'<value>'`.

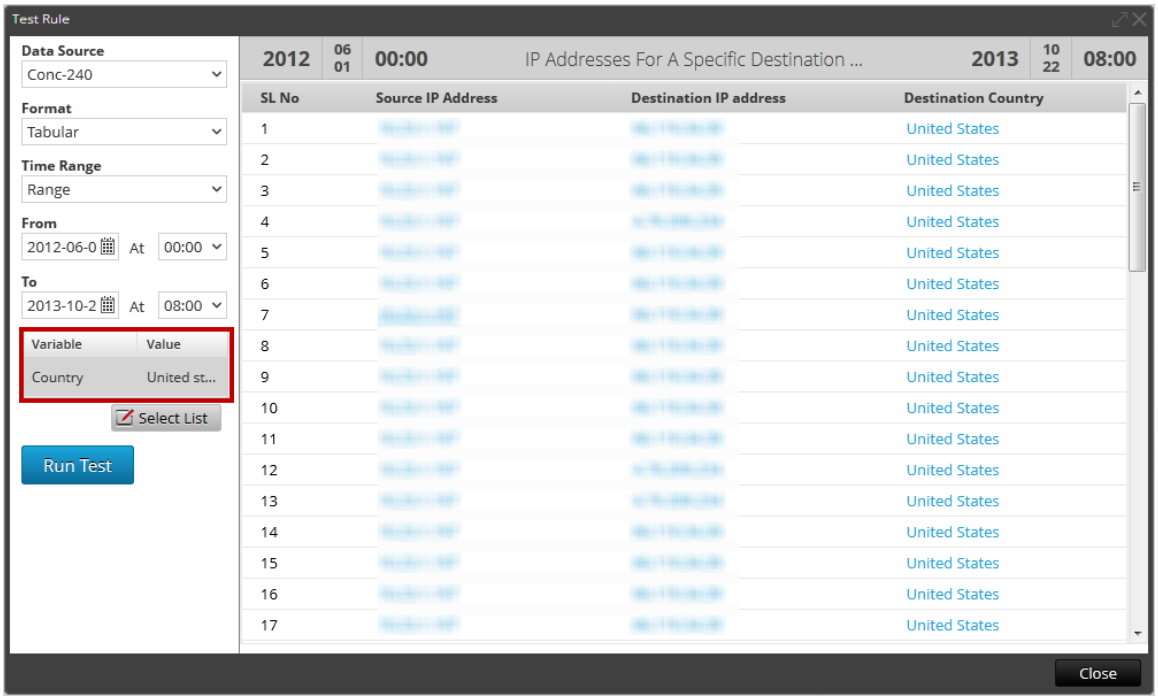
Some examples where a variable can be used are provided in this section.

View Source IP Addresses for a Specific Destination Country

The following is an example of a NetWitness DB rule to view the source and destination ip addresses for a specific destination country. Here the value for source country is defined as a variable `${local_country}`.



At runtime, you are prompted to enter the value for the variable. The figure below shows the `local_Country` variable where you can enter the value. If you enter the value as **United states**, all the source and destination ip addresses with destination country as United states are listed.



You can use the above rule to schedule a report. You can schedule two types of reports:

- Report with Dynamic Variables
- Iterative Report

Report with Dynamic Variables

Dynamic variables allows the user to specify the values for a variable defined in a rule while scheduling a report.

To schedule a report with Dynamic Variable, perform the following:

1. Go to **MONITOR** > Reports.

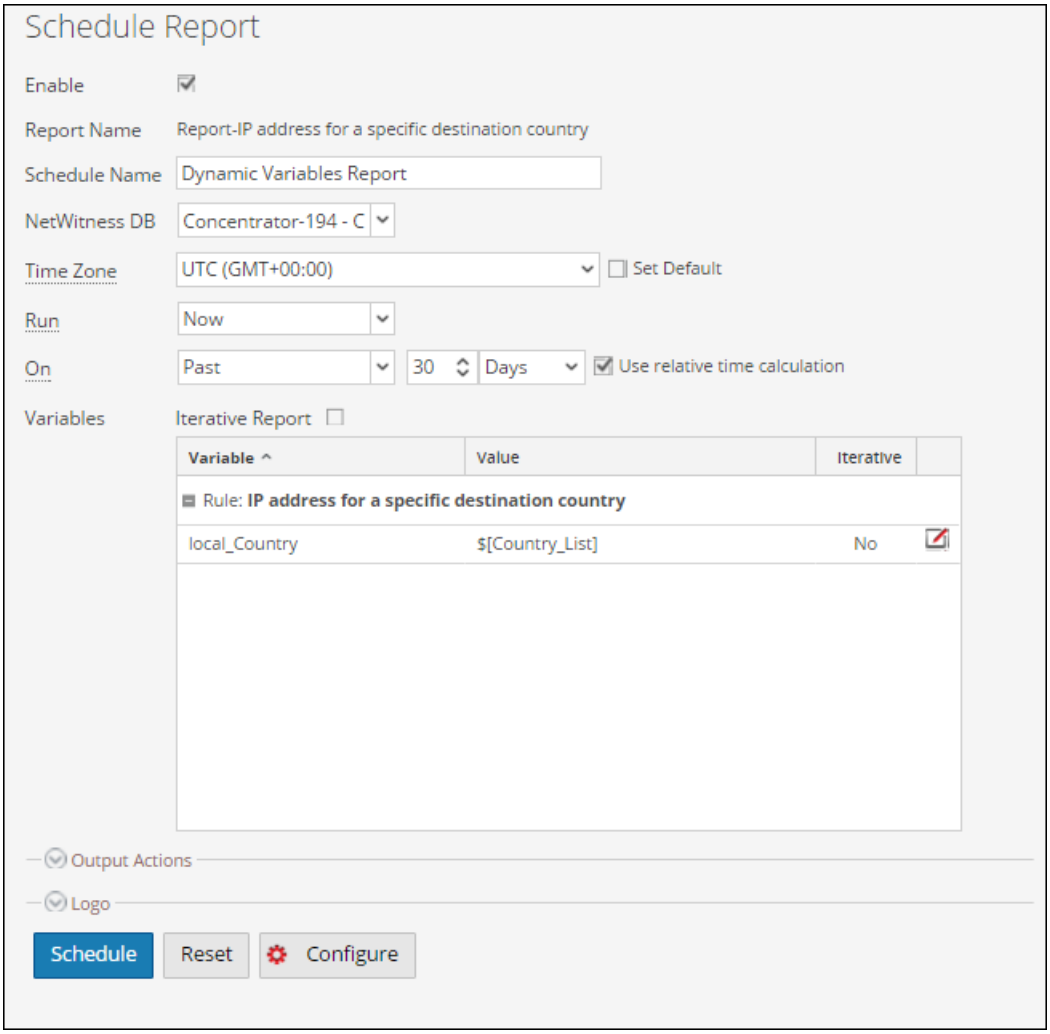
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. On the **Build Report** page, click + to create a report.

4. Add the rule by drag and drop which has the user defined variable from the Rules tab.
5. Click **Schedule**.
   The Schedule Report view tab is displayed.



6. To execute the reports as per the schedule, select the **Enable** checkbox.
7. In the **Schedule Name** field, enter a name for the schedule report configuration.
8. From the **Data Source** field, select the data source.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in the *Reporting Engine Configuration Guide*.

9. (Optional) From the **Warehouse Resource Pool** drop-down, select the

pools or queues available in the cluster to schedule the report to run on either the pool or queue. This drop-down list is available only if you select a Warehouse DB report.

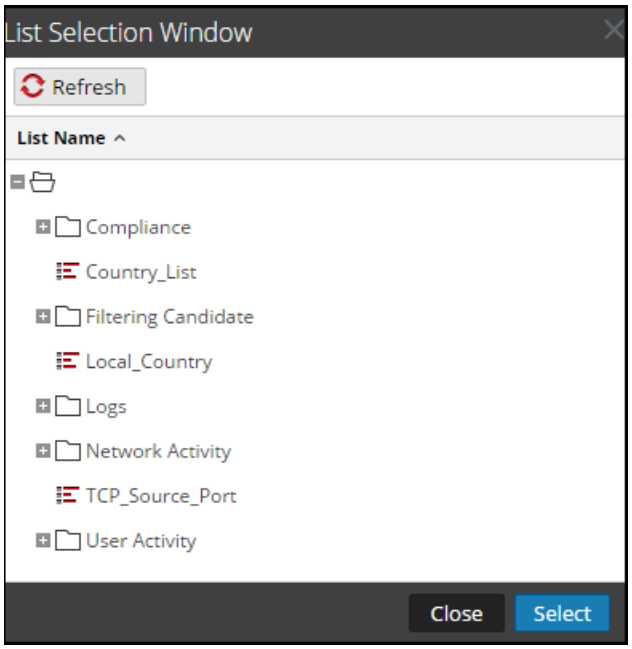
Note: All the queues or pools you specified in the Explore page for the Reporting Engine are listed. If no pools or queues are configured in the Explorer page, this drop-down is disabled and the jobs are submitted to the clusters without any a queue or pool name.

Note: If the pool or queue configured in the report schedule is removed from the Cluster, then in the Capacity Scheduler, the queue name remains undefined. However, in the Fair Scheduler, the specified pool name will be created using the property `mapred.fairscheduler.allow.undeclared.pool`.

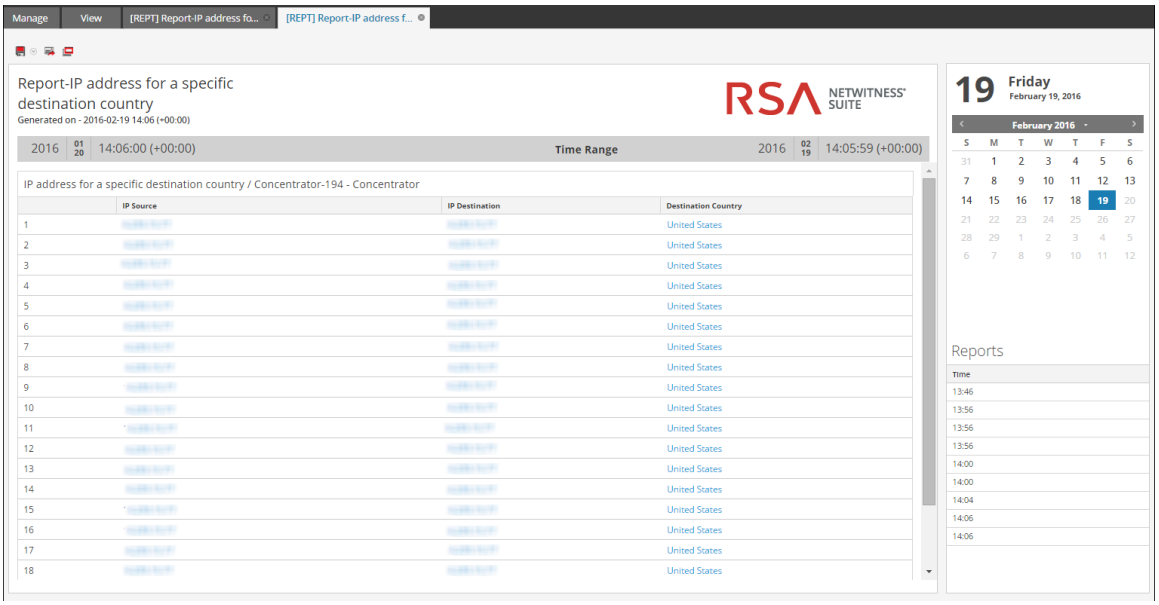
10. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format.This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. From the **Run** field, select the type of run schedule. (For example, Now or Hourly). Depending on the type of run schedule, do either of the following:
    - If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
    - If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
    - If you select a **Daily** run schedule, you must enter a time value in the **At** field.
    - If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

    Note: While scheduling a report, if you select **Paste** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.
12. In the variables field, click .
13. Do one of the following:

- Enter the value for the variable, or
- Choose the list value for the variable.

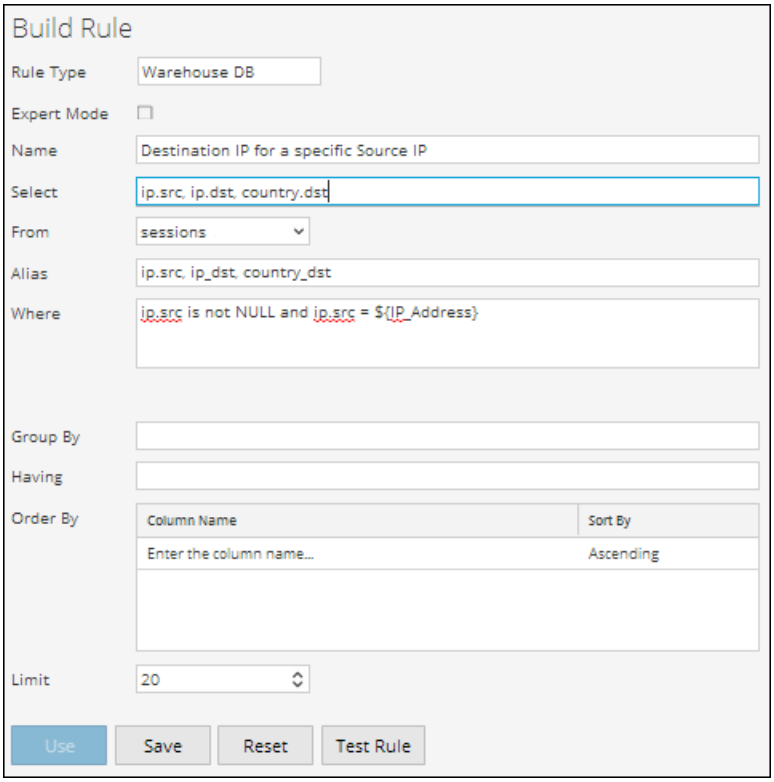


14. Click **Select**.
15. Click **Schedule**.
    The scheduled report executes as scheduled and provides the configured outputs.

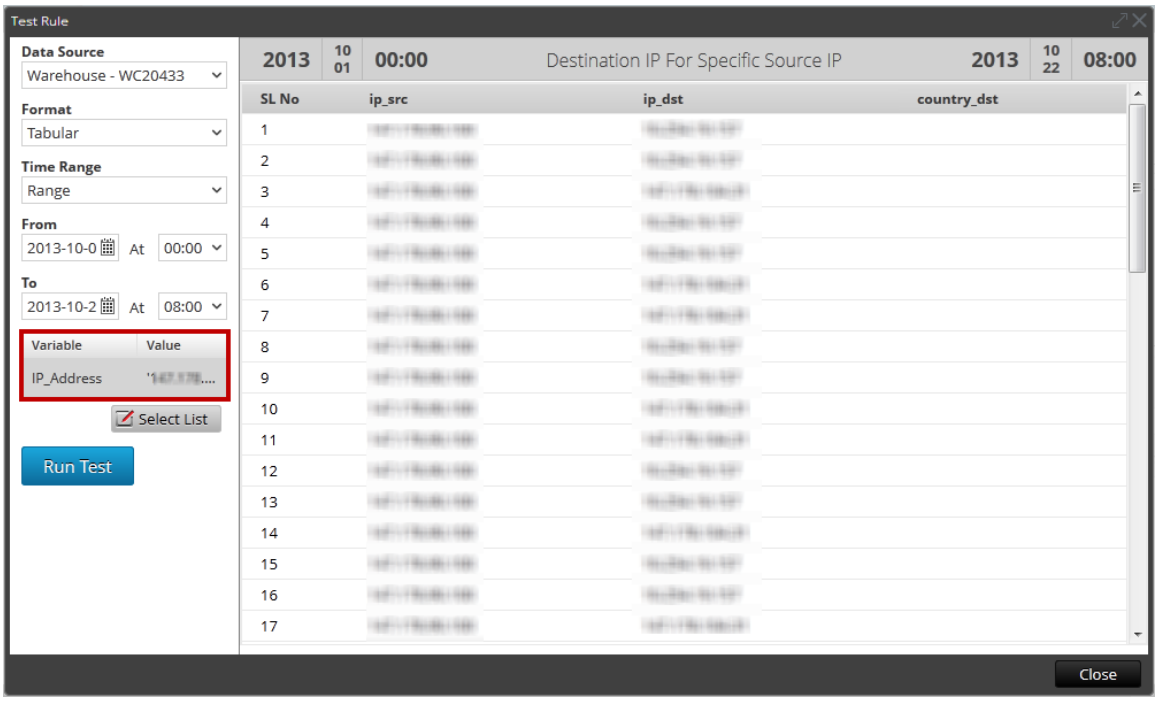


View All Destination IP Addresses for a Source IP Address

The following is an example of a Warehouse rule to view all the destination IP addresses for a specific source IP. The source IP address `ip_src` is defined as a variable `${IP_Address}`.

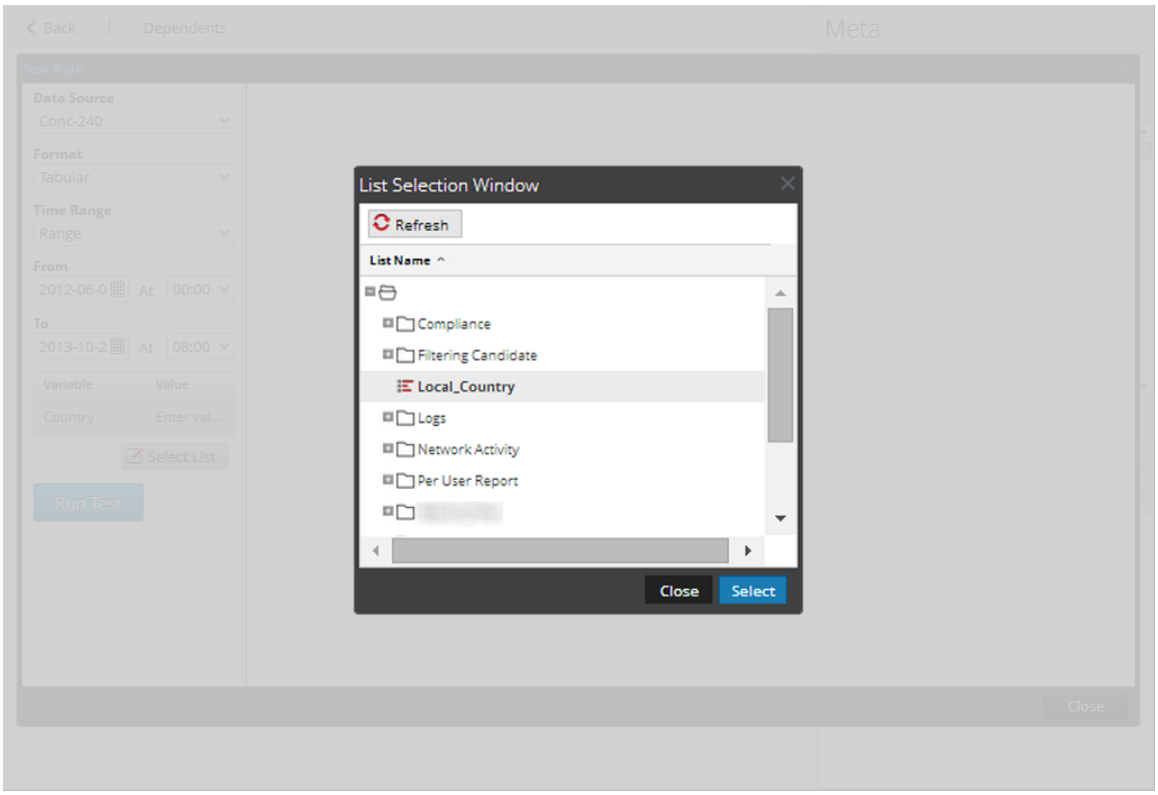


At runtime, you are prompted to enter the source IP address. The figure below shows the `IP_Address` variable, and you can enter a valid source IP address. All the destination IP addresses with the specified source IP are listed.



Associate a Variable to a List of Values

You can associate the variable to a list. For example, you can create a list called `Local_Country` and enter all the country names as values. You can select the list `Local_Country` as the value for the variable `Local_Country`. At Run Configuration, the `Local_Country` list is populated and you can select the country based on which results are displayed.



Iterative Report

An iterative report generates a report for every value in the list.

To schedule an iterative report, perform the following:

1. Go to **MONITOR** > Reports.

   The Manage tab is displayed.

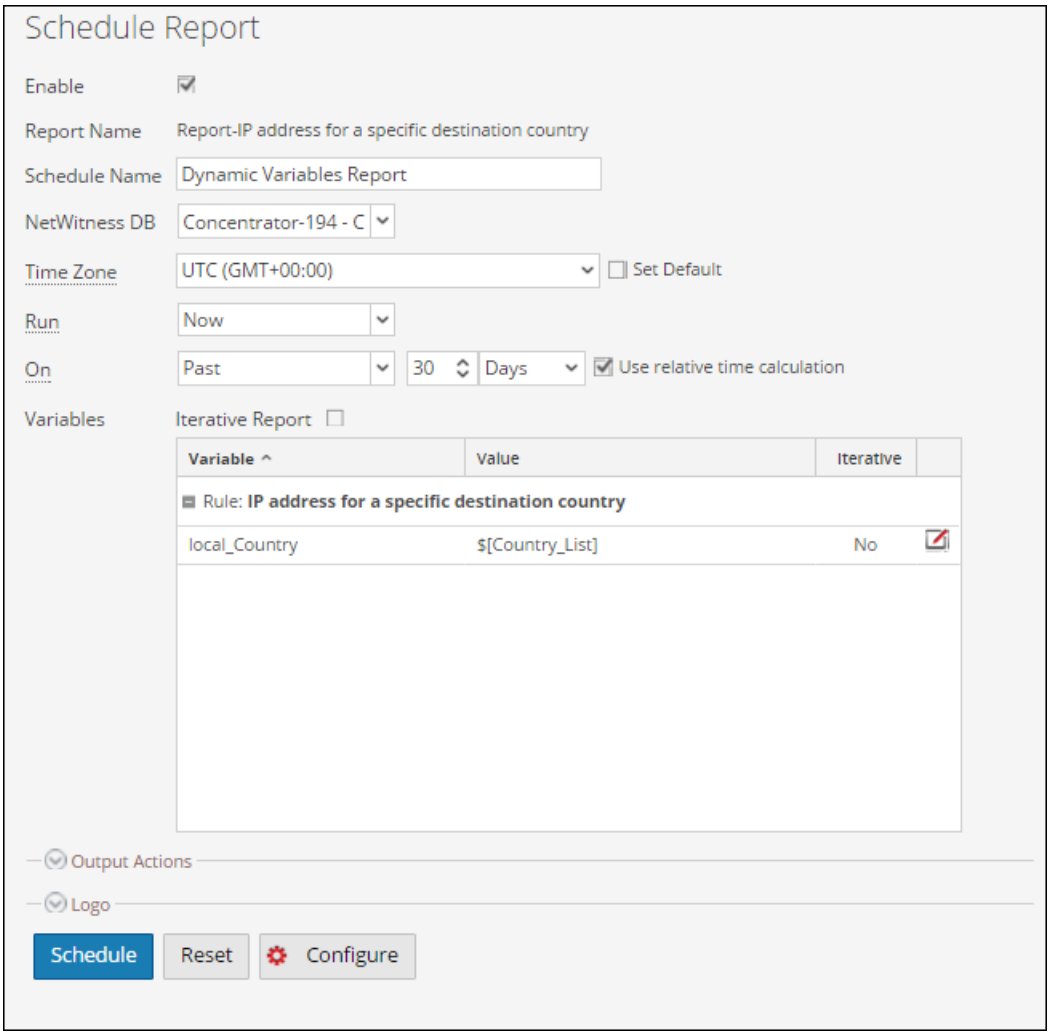
2. Click **Reports**.

   The Report view is displayed.

3. On the **Build Report** page, click + to create a report.

4. Add the rule which has the user defined variable from the Rules tab.

5. Click **Schedule**.
   The Schedule Report view tab is displayed.



6. To execute the reports as per the schedule, select the **Enable** checkbox.
7. In the **Schedule Name** field, enter a name for the schedule report configuration.
8. From the **Data Source** field, select the data source.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in the *Reporting Engine Configuration Guide*.

9. (Optional) From the **Warehouse Resource Pool** drop-down, select the pools or queues available in the cluster to schedule the report to run on either the pool or queue. This drop-down list is available only if you select a Warehouse DB report.

Note: All the queues or pools you specified in the Explore page for the Reporting Engine are listed. If no pools or queues are configured in the Explorer page, this drop-down is disabled and the jobs are submitted to the clusters without any a queue or pool name.

Note: If the pool or queue configured in the report schedule is removed from the Cluster, then in the Capacity Scheduler, the queue name remains undefined. However, in the Fair Scheduler, the specified pool name will be created using the property `mapred.fairscheduler.allow.undeclared.pool`.

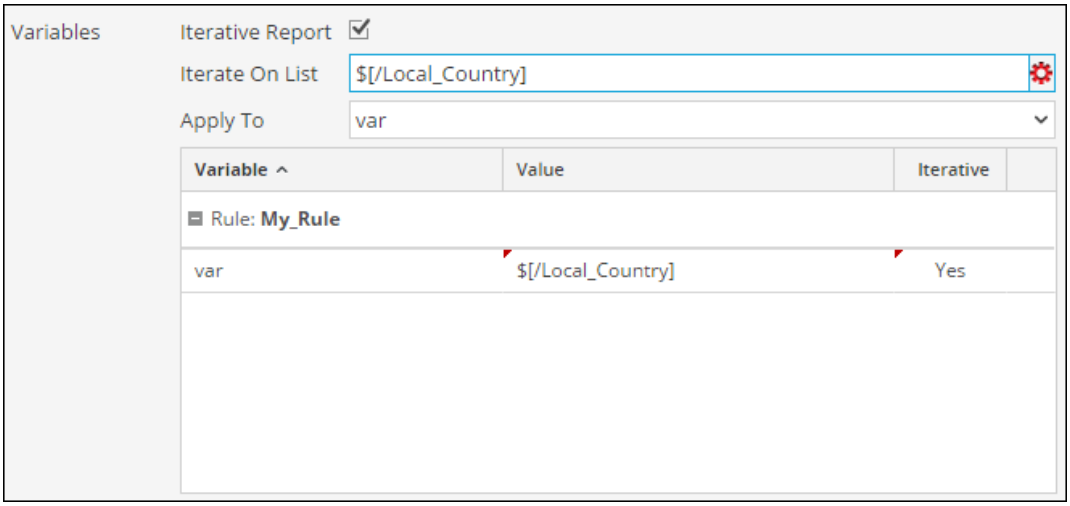
10. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format. This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. From the **Run** field, select the type of run schedule. (For example, Now or Hourly). Depending on the type of run schedule, do either of the following:
    - If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
    - If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
    - If you select a **Daily** run schedule, you must enter a time value in the **At** field.
    - If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

    Note: While scheduling a report, if you select **Paste** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.
12. In the variables field, do the following:
    a. To run iterative reports, select the **Iterative Report** checkbox.
    b. To Iterate on List value, click .

       The List Selection Window opens.
    c. Choose a list and click **Select**.

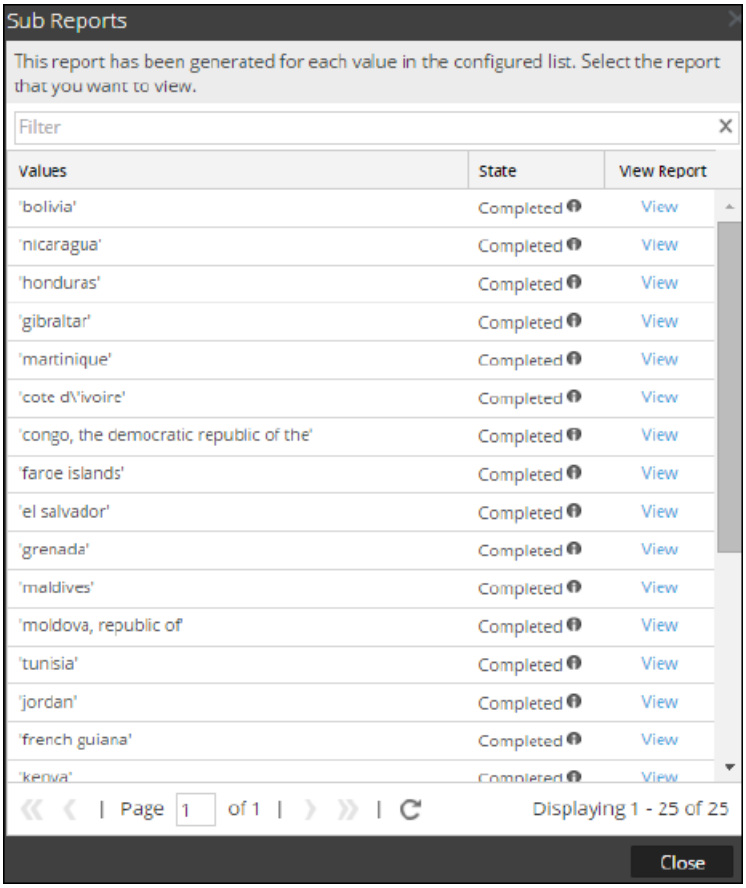
The list item selected gets added to the **Iterate on List** field.

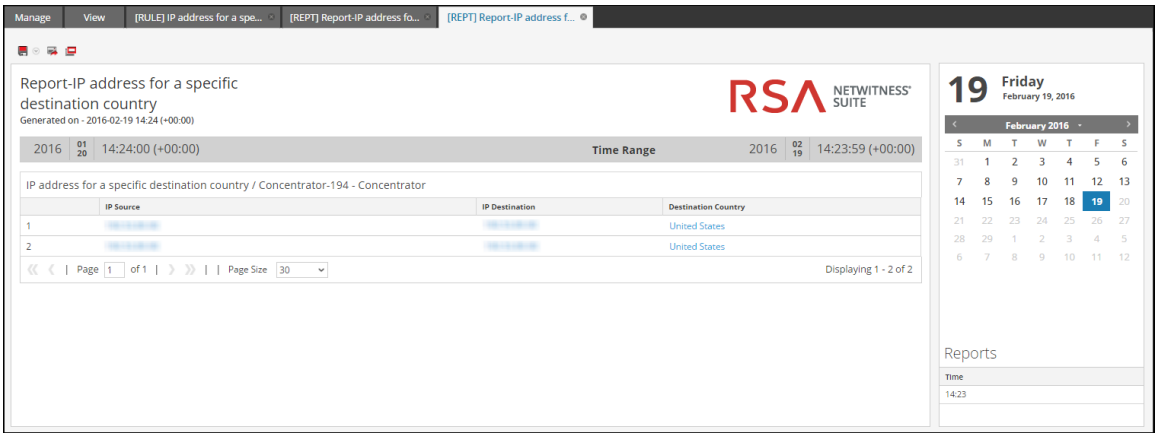
d. Select the variable on which the selected list value has to be applied.



13. Click **Schedule**.
The scheduled report executes as scheduled and provides the configured outputs.

The following figure shows the Iterative Report view.





Create a Report Using a Rule

You can create a report using a rule. When you create a report using a rule, a default report is created with this single rule. You can further edit the report to add more rules.

To create a report using a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Do one of the following:
   - You can create a report using a rule when you create or edit the rule. Perform the following:
     a. In the **Build Rule** view, click **Use**.
        The Use Rule dialog is displayed.
     b. Click **Report**.
     c. Select **New Report** or **Existing Report** based on your requirement.
     d. Click **Select**.
   - Select a rule in the Rule List panel and click in the Rule toolbar. From the drop-down menu, select **Use** > **Report**.
   - In the Rule List panel and click > **Create Report**.

Note: Custom rules can be used to create a Report and If you select the view for the rule as "Area" or "Pie", a window pops up for **X-Axis** and **Y-Axis** inputs. By default, you can select only the first meta in **X-Axis**.

View a Report

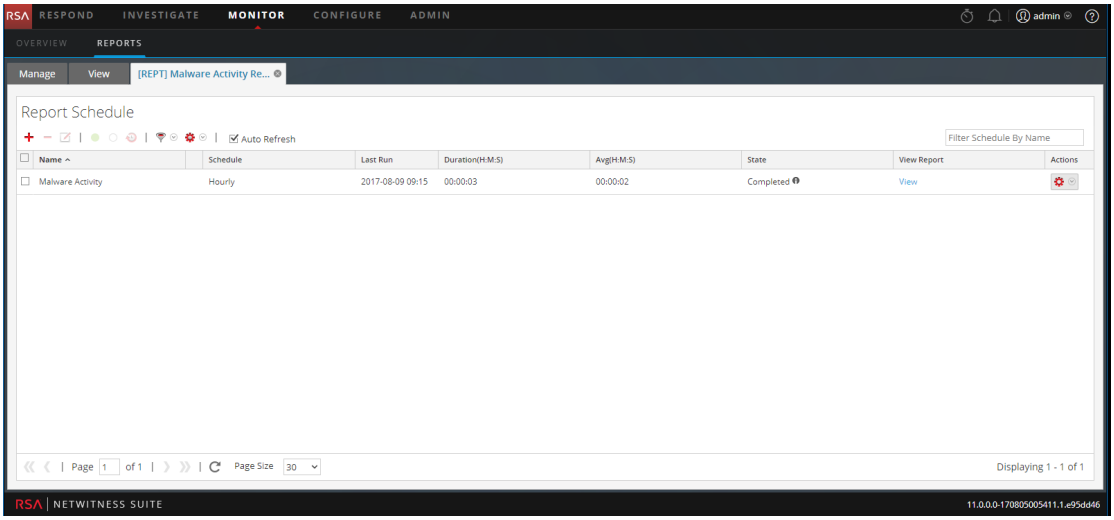
You can view a report or list of all reports. You can also view the scheduled reports to know the state of the scheduled report. If the scheduled report is in a stop or disable state, you can start or enable the scheduled report.

After you view a report, you can perform any of the following tasks:

1. You can print, save, email and view reports on full screen.
2. You can also select a date from the calendar to view a list of successfully run reports for the chosen date.

To view a report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, click > **View Scheduled Reports**.
4. Click the **#Schedules** column.
   The Schedule Reports view tab is displayed with the status of each of the scheduled report.



5. Select a scheduled report and click **View**.
   One of the following is displayed:

- The selected report.
- The Sub reports panel for a scheduled report having 'Iterative' selected.

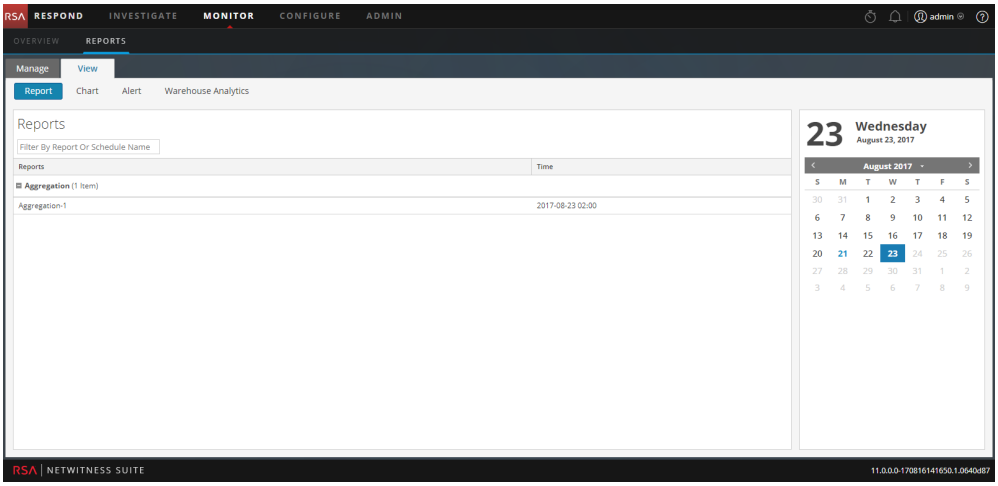
For each value in the configured list a report is displayed.

> **Note:** If the report status is partial or complete, the "last run timestamp" and the "last run (seconds)" are updated. However, the average time taken to run the report is updated only when the report status is complete and not when it is partial.

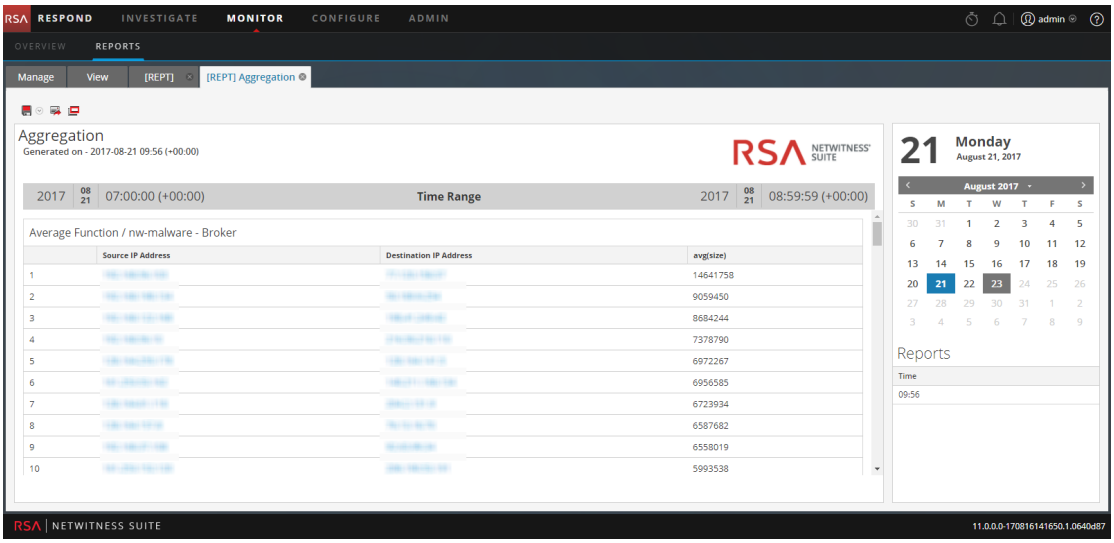
To view a list of all reports, perform the following:

1. Go to **MONITOR** > **Reports**.
   The **Manage** tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report** panel, click **View All Reports**.
   A list of reports along with their schedule name and time are displayed on the View tab.

> **Note:** If no list is displayed, select a date from the calendar to view a list of reports for that date.



4. You can select a scheduled report and print, save as PDF/CSV, send email notifications, or view it on full screen.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
OVERVIEW
REPORTS
Manage
View
[REPT]
[REPT] Aggregation
Aggregation
Generated on - 2017-08-21 09:56 (+00:00)
RSA NETWITNESS SUITE
2017 08 21 07:00:00 (+00:00)
Time Range
2017 08 21 08:59:59 (+00:00)
Average Function / nw-malware - Broker
Source IP Address
Destination IP Address
avg(size)
1 14641758
2 9059450
3 8684244
4 7378790
5 6972267
6 6956585
7 6723934
8 6587682
9 6558019
10 5993538
21
Monday
August 21, 2017
August 2017
S M T W T F S
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Reports
Time
09:56
RSA | NETWITNESS SUITE
11.0.0.0-170816141650.1.0640d87

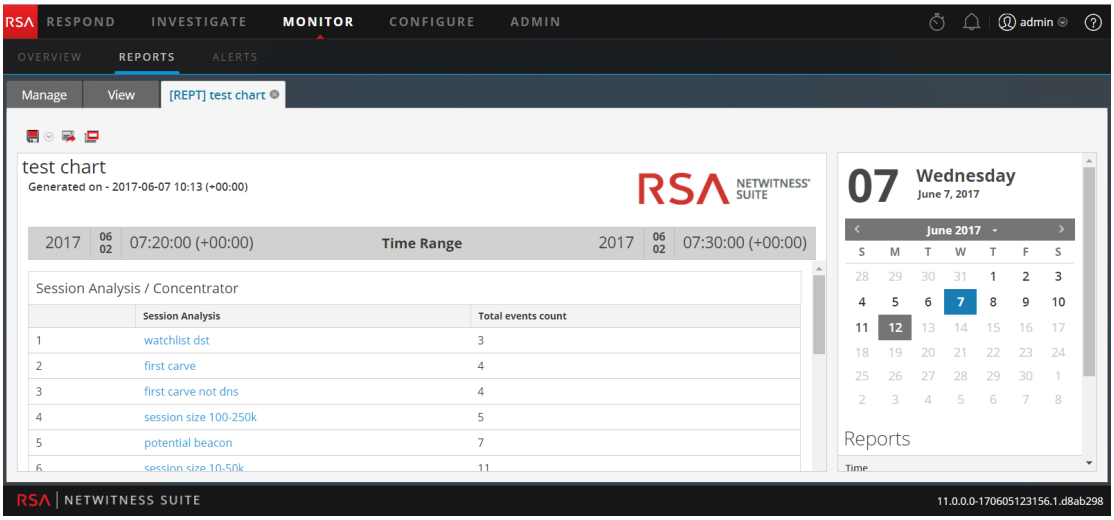
Investigate a Report

You can investigate a report by directly navigating to the Investigation View from the report. With the Investigate a report option, you can investigate each event mentioned in the report.

To investigate a report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report** toolbar, click **View All Reports**.
   The View All Reports tab is displayed.

   Note: If no reports are displayed in the View All Reports, select a date for which you want to display the reports.
4. Double-click the report name to view the report details.
   The Report details screen is displayed.



You can click on the session analysis to investigate on the report.

Note: If you want to manually copy the result data and use it for investigation, make sure that the binary values are prefixed with 'hex:'.

Manage Lists, Rules or Reports

You can set access control, delete, edit, import, or export a list, rule or report.

Manage a List

Access Control for a List and List Group

You can set up the access permissions for the user roles to manage lists or list groups. The Reporting provides access control at the list and list group level. Only a user who has the right set of permissions can perform the tasks in the Reporting. The access control is managed by the administrator from the **ADMIN > Security > Roles** tab.

As an administrator you must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

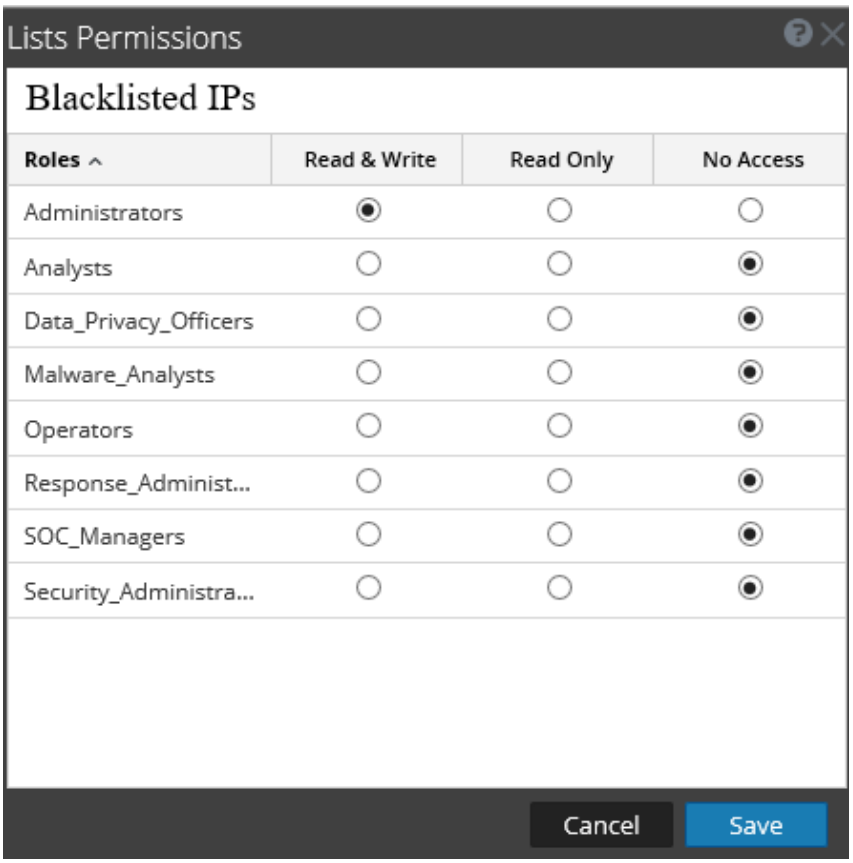
Lists or list groups can be assigned to a specific set of user roles. When users log into NetWitness Suite, they can access only those lists to which they belong. Users who belong to a user role with the **Read & Write** access permission have full access rights on the lists. Further, the access can be strengthened so that lists are accessed only by those who have the **Read Only** access.

Note: You must have **Read Only** permission for a list group to view the lists within that group.

For example, if you want **Security Analysts** to have access to all the lists in a list group, you can set the permission **Read & Write** at the list group level. And, if you do not want the **Operator** role to have access to a specific set of lists in a list group, you can set the permission **No Access** at the list group level.

At the list or list group level, you can set the following access permissions for the user roles in NetWitness Suite. For more information, see List View:

- Read & Write
- Read Only
- No Access



The following table lists the columns in the Lists Permissions panel:

Column	Description
Roles	Describes roles of the users logged into the NetWitness Suite user interface.
Read & Write	Allows users to access, view, edit, delete, import, and export lists on the Lists view. Users can also change the permission on the rule.
Read Only	Allows users to only access and view the list on the lists view.
No Access	Doesn't allow users to access or view the lists.

Access Control for a List

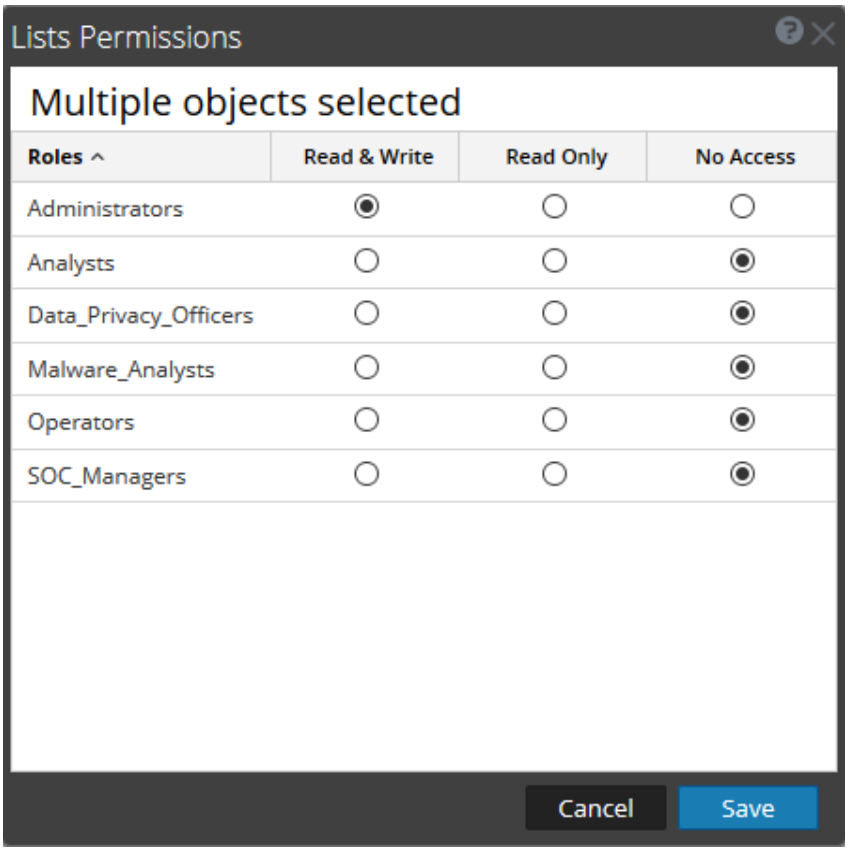
To change the list permissions, you must select a list and set access permissions using the List Permissions panel.

If you want to change the access permission for a specific user role, you must set it at the list level. Except for administrators, the default permission set for all the other user roles is **No Access** before applying job permissions.

Access Control Multiple Lists

You can select multiple lists at once and set access permissions using the Lists Permissions Panel. The access permission that you choose is applied to all the selected lists.

Note: The "*" beside the role name indicates that other permissions are available for the user role. If you want to change the access permission for the required user role, select the user role and change the access permission.



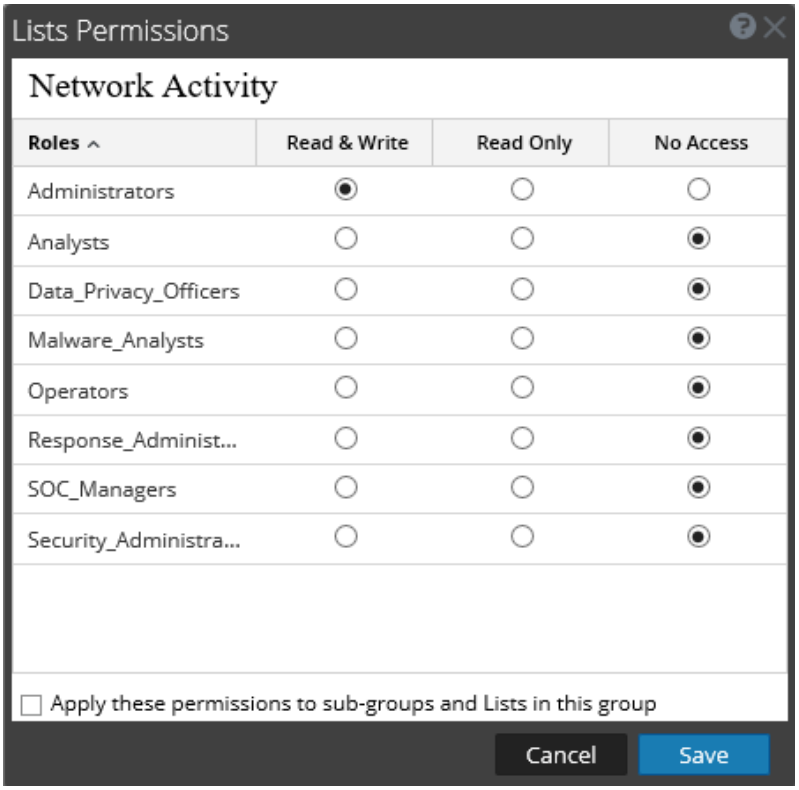
Note: If a user (other than ADMIN) creates a list, ADMIN cannot access that list.

Access Control for a List Group

To change the list group permissions, you must select a list group and set access permissions using the Lists Permissions panel.

If you want to change the access permission for a specific user role, you must set it at the list group level. Except for administrators, the default permission set for all the other user roles is **No Access** before applying job permissions.

You can also apply permissions to subgroups and lists in the group by selecting the checkbox.



The following scenarios describe defining permissions for list groups or subgroups and lists in the groups:

- Scenario 1: Permissions applied to list group or subgroup based on the user role.

  Each of the levels will have a permission set depending on the user role. For example, if a list group is assigned the role of Security Analyst, permissions are set to Read & Write for the list group.

- Scenario 2: Permissions applied to subgroups and lists in the group.

  The access permissions that you set can be applied to subgroups and child objects of this group. Permission at the list group level will be inherited by the subgroups and lists in the group.

Role (Analysts)	Permissions applied to list group or subgroup based on the user role	Permissions applied to subgroup and lists in the group
Group	Read & Write	Read & Write
Subgroup	Read	Read & Write - Inherited
Lists	Read	Read & Write - Inherited

Access permission for a list or list group

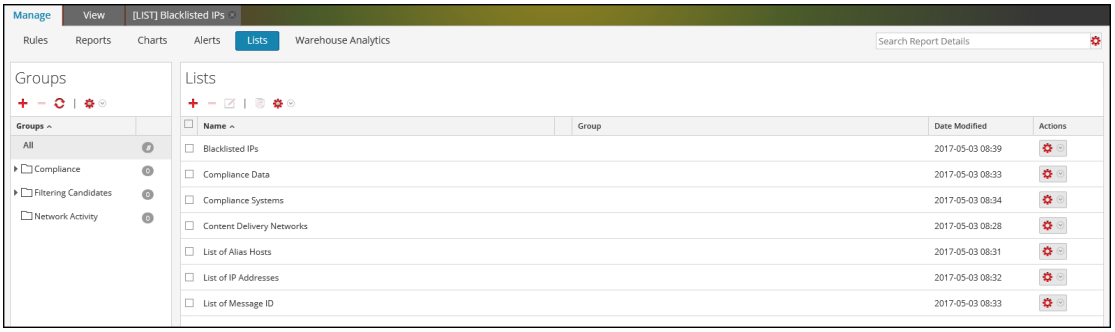
Ensure that you have at least **Read & Write** access permission so that you can set access permissions for lists or list groups.

To set access permission for a list, perform the following:

1. Go to **MONITOR** > **Reports**.

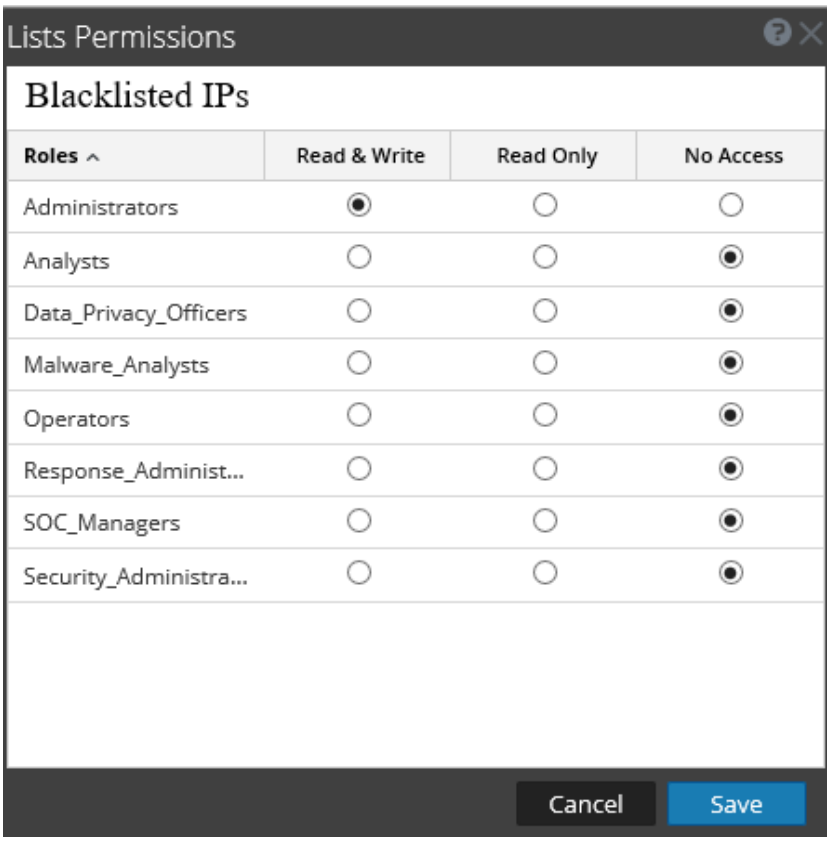
   The Manage tab is displayed.

2. Click **Lists**.
   The List view is displayed.



3. In the **List View** panel, select a list.

4. Click > **Permissions** in the List toolbar.
   The List Permissions dialog is displayed.



5. Select the appropriate access permission for each of the user roles and click **Save**.

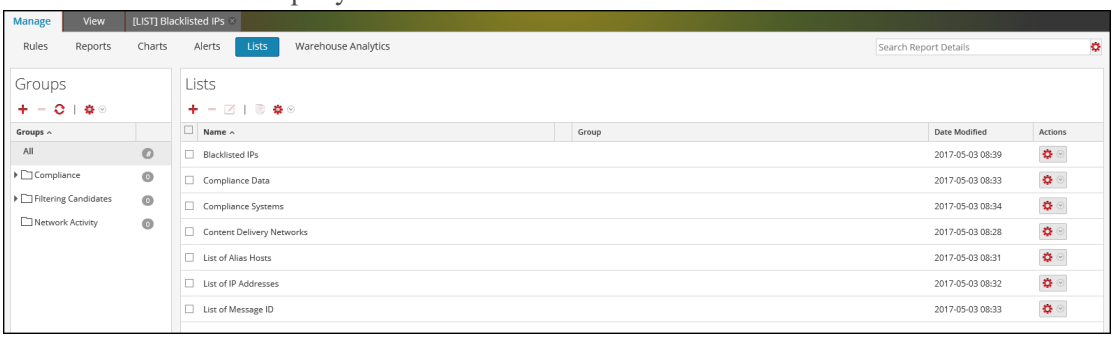
   A confirmation message that the permission is successfully set for the selected list is displayed.

To set access control for a list group, perform the following:

1. Go to **MONITOR** > **Reports**.

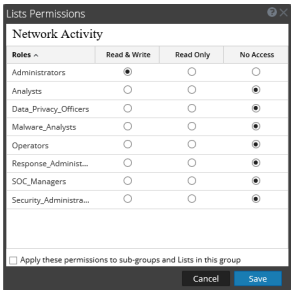
   The Manage tab is displayed.

2. Click **Lists**.
   The List view is displayed.



3. In the **List Groups** panel, select a list group.

4. Click > **Permissions**.
   The List Permissions dialog is displayed.



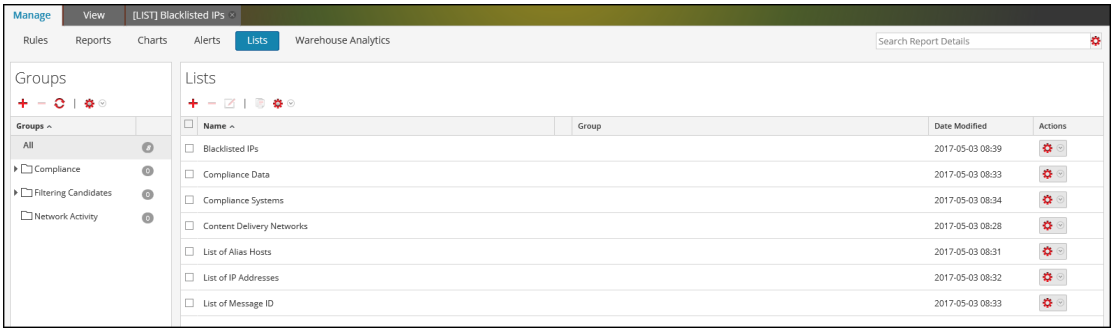
5. (Optional) Select the appropriate checkbox to apply these permissions to subgroups and child objects of this group.
6. Click **Save**.

   A confirmation message that the permission is successfully set for the selected list group is displayed.

Edit a List

To edit a list, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. In the **List View** panel, select a list that you want to edit and do one of the following.
   - Click in the List toolbar.
   - In the List View panel, click > **Edit**.

Note: You can only edit one list at a time.

4. Modify the required fields and add new values to the list.
5. Click **Save**.

   A confirmation message that the list is saved successfully is displayed.

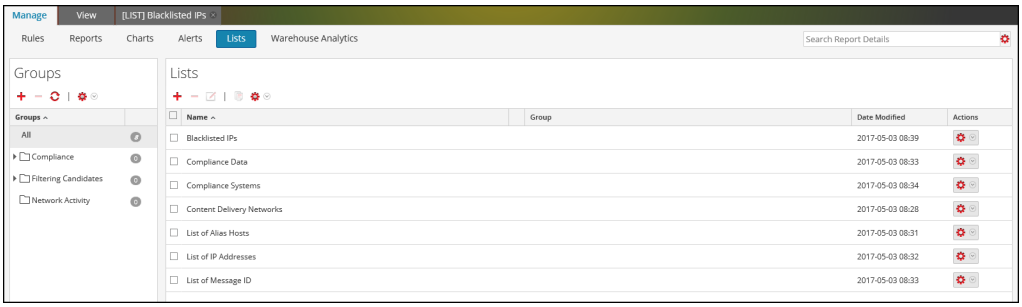
Delete a List or List Group

To delete a list, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.
2. Click **Lists**.

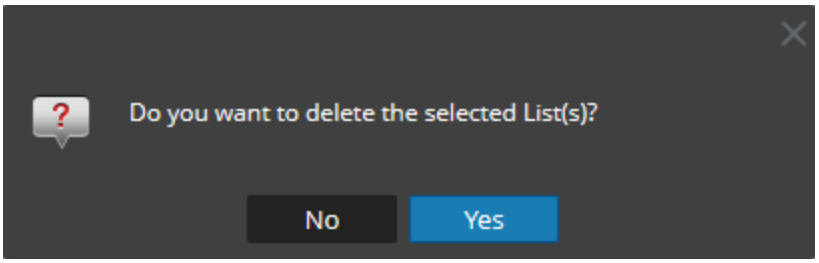
   The List view is displayed.



3. In the **List View** panel, do one of the following:

   - Select a list or multiple lists that you want to delete and click in the **Lists** toolbar.
   - In the **Actions** column, click > **Delete**.

   A confirmation dialog is displayed.



Note: Before you delete a list, make sure that the list is not associated with any rule.

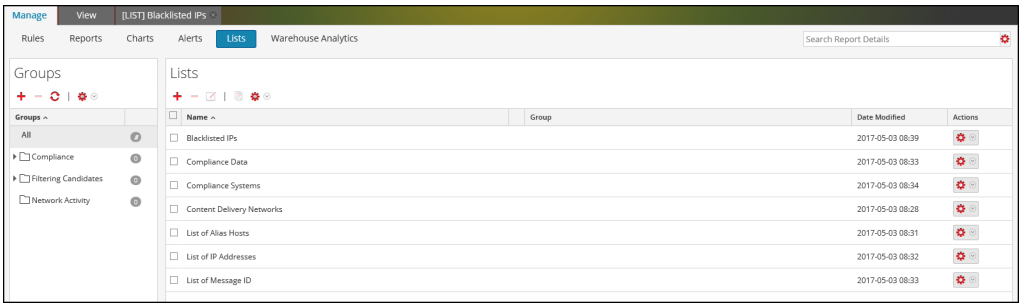
4. Click **Yes** to delete the list.

   A confirmation message that the list is deleted is displayed and the selected

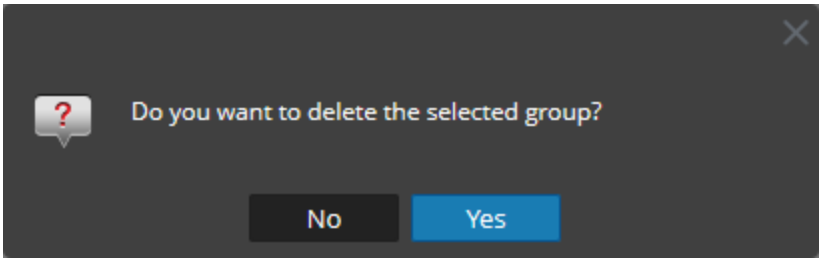
list is deleted from the List View panel.

To delete a list group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. In the **List Groups** panel, select the group and click .
   A confirmation dialog is displayed.



Caution: If you delete a group, all subgroups and lists in that group are deleted.

4. Click **Yes** to delete the selected group.

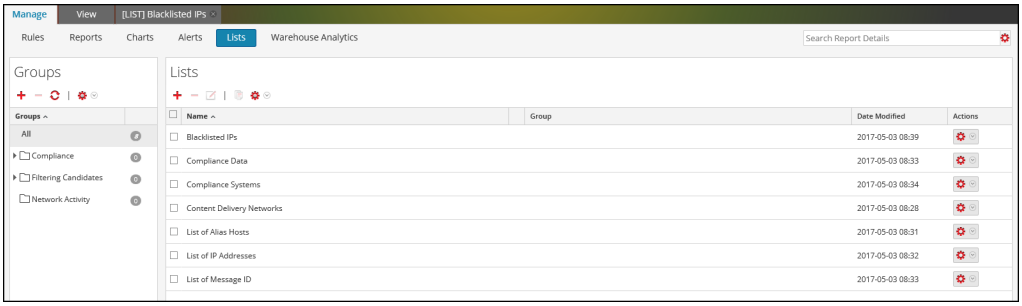
Note: If you try to delete a list group that has lists referenced in a rule or an alert, a warning message that **Lists are referenced in a rule** is displayed.

Duplicate a List

To duplicate a list, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. Click **Lists**.
   The List view is displayed.



3. In the **List View** panel, select a list that you want to duplicate.

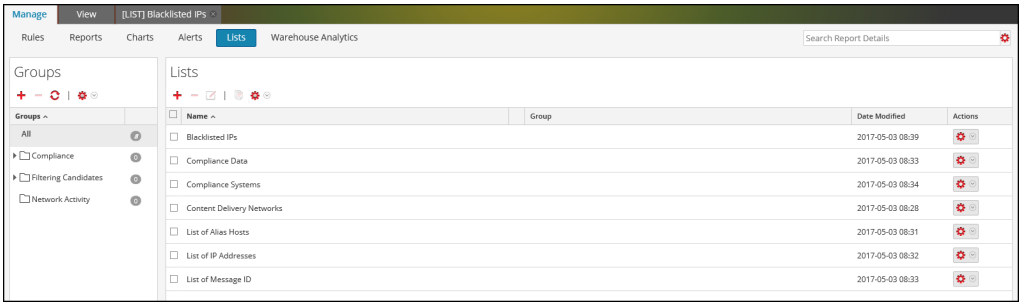
> **Note:** You can only duplicate one list at a time.

4. In the **List** toolbar, click .

Export a List or List Group

To export a list, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. In the **List View** panel, do one of the following:

   - Select a list and click > **Export** in the List toolbar.
   - In **Actions** column, click > **Export**

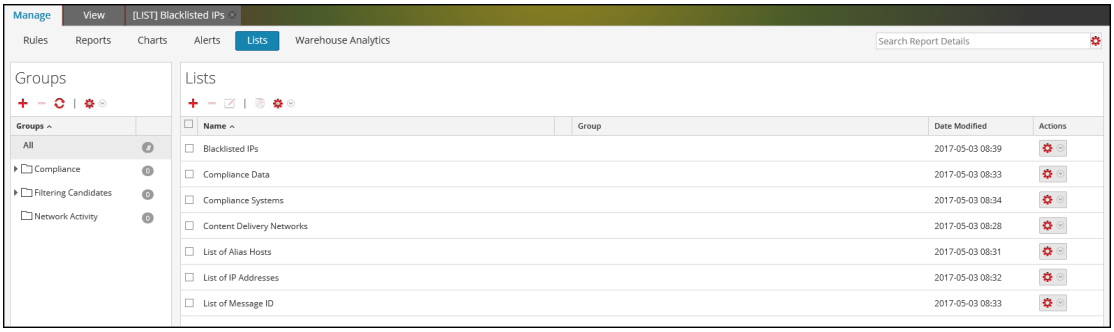
   You can export multiple lists at a time. To select multiple lists, select the checkbox of the lists to be exported. A browser-specific export dialog may

be displayed allowing you to open or save the file.

To export a list group, perform the following:

You can export selected list groups to an external file that can be later imported to NetWitness Suite. If nothing is selected in the List Library panel, the entire list tree is exported. When you export, the result is a single export file in binary format.

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The List view is displayed.



3. In the **List Groups** panel, select the list group containing the lists which you want to export.
4. Click > **Export**.
   You can export multiple list groups at a time. To select multiple list groups, press and hold the CTRL button and select the list groups to be exported. The exported file is saved to the local drive.

Import a List or List Group

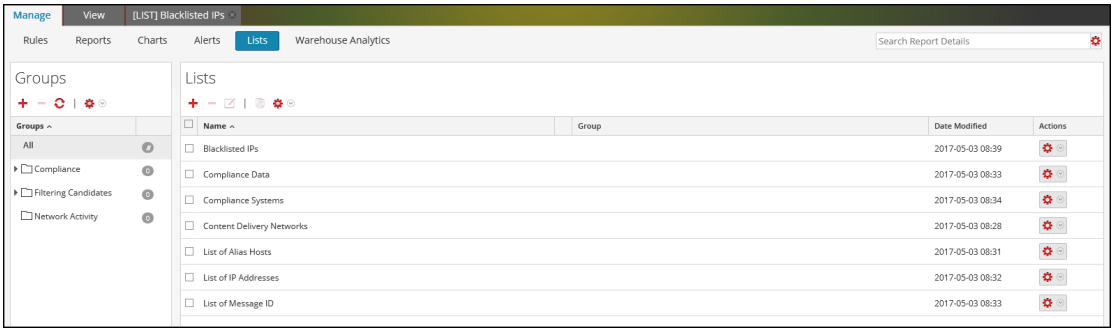
To import a list, perform the following:

You can import lists from instances of NetWitness Suite into the list tree in the List View panel. Lists must be in a valid binary file exported from a NetWitness Suite instance.

1. Go to **MONITOR**> **Reports**.
   The Manage tab is displayed.

2. Click **Lists**.

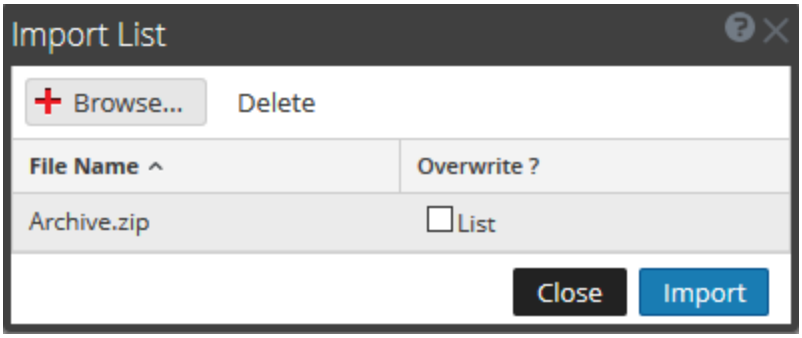
   The List view is displayed.



3. In the **List** toolbar, click > **Import**.

   The Import List dialog box is displayed. You can import multiple lists at a time. To select multiple lists, press and hold the CTRL button and select the lists to be imported.

4. Click **Browse** and select archived file containing the lists.



5. Click **Import**.

Note: During the import process, if a duplicate list exists and you do not select the overwrite option, the list is imported and no message about duplicate lists is displayed.

To import a list group, perform the following:

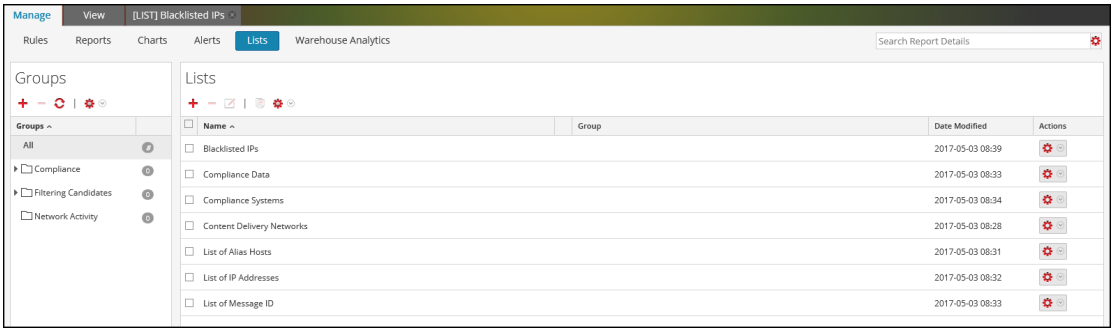
You can import list groups from instances of NetWitness Suite into the list tree in the List Groups panel. Lists must be in a valid binary file exported from a NetWitness Suite instance.

1. Go to **MONITOR> Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

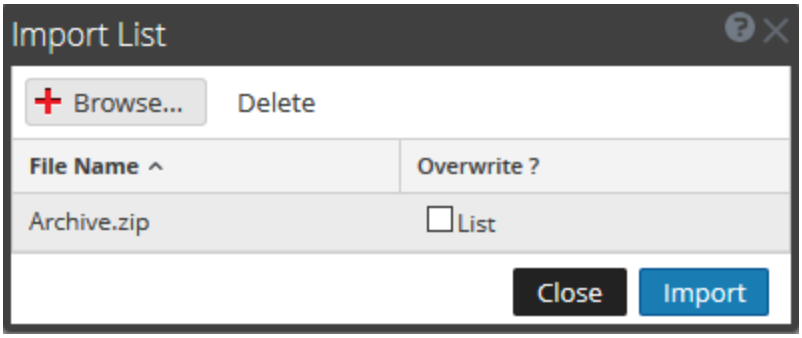
   The List view is displayed.



3. In the **List Groups** panel, click > **Import**.

   The Import List dialog box is displayed.

4. Click **Browse** and select archived file containing the list groups.



   You can import multiple list groups at a time. To select multiple list groups, press and hold the CTRL button and select the list groups to be imported.

5. Click **Import**.

Note: During the import process, if a duplicate list group exists and you do not select the overwrite option, the list group is imported and no message about duplicate list group is displayed.

Manage a Rule

Access Control for a Rule and Rule Group

To set access permissions the user will have depending on the user role to manage a rule or rule group. The Reporting provides access control at the rule and rule group level. Only a user who has the right set of permissions can perform the tasks in the Reporting. The access control is managed by the administrator from the **ADMIN > Security > Roles** tab.

When creating users and user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Rules or Rule Groups can be tied to a specific set of user roles so that when a user logs into NetWitness Suite, the only rules they can access are rules accessible to the group to which the user belongs. Users that belong to a user role with the 'Read & Write' access permission have full access rights on the rule. Further, the access can be tightened so that rules are accessed only by those who have the 'Read Only' access.

Note: You must at least have 'Read Only' permission on a group to view the rules within that group.

At the rule level, you can set the following access permissions for the user roles:

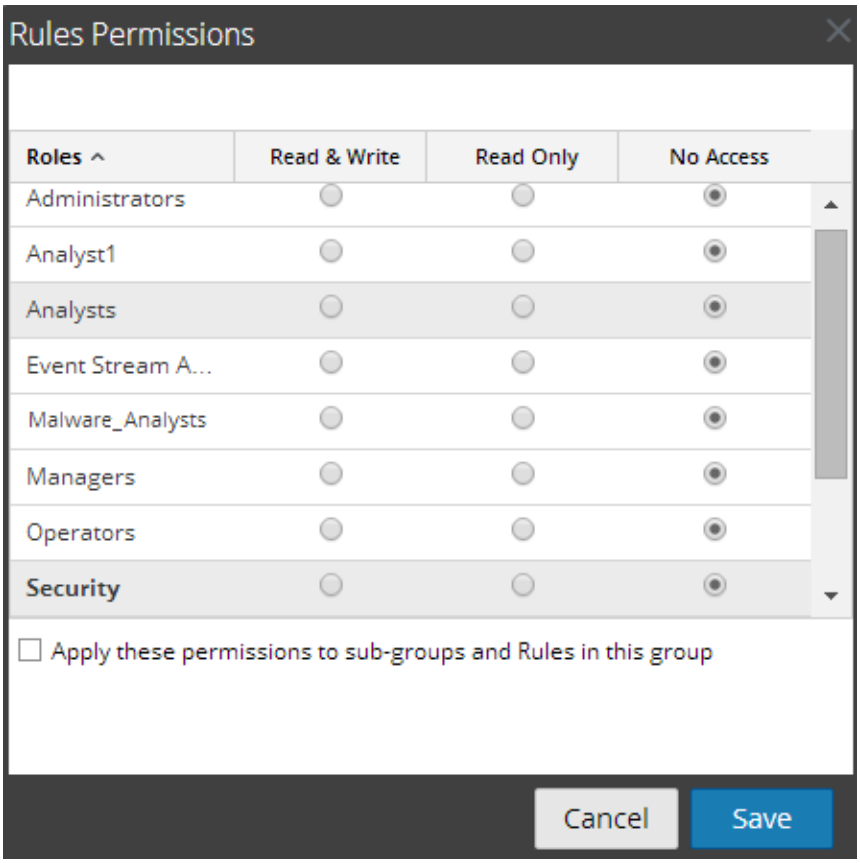
- Read & Write
- Read Only
- No Access

Suppose, you want the **Security Analysts** to have access to all the rules in a Rule Group, you can set the permission '**Read & Write**' at the Rule Group level. And, if you do not want the **Operator** role to have access to a specific set of rules in a rule group, you can set the permission '**No Access**' at the Rule Group level. The permission is set only for the rule group but not the rules or subgroups in the Rule Group.

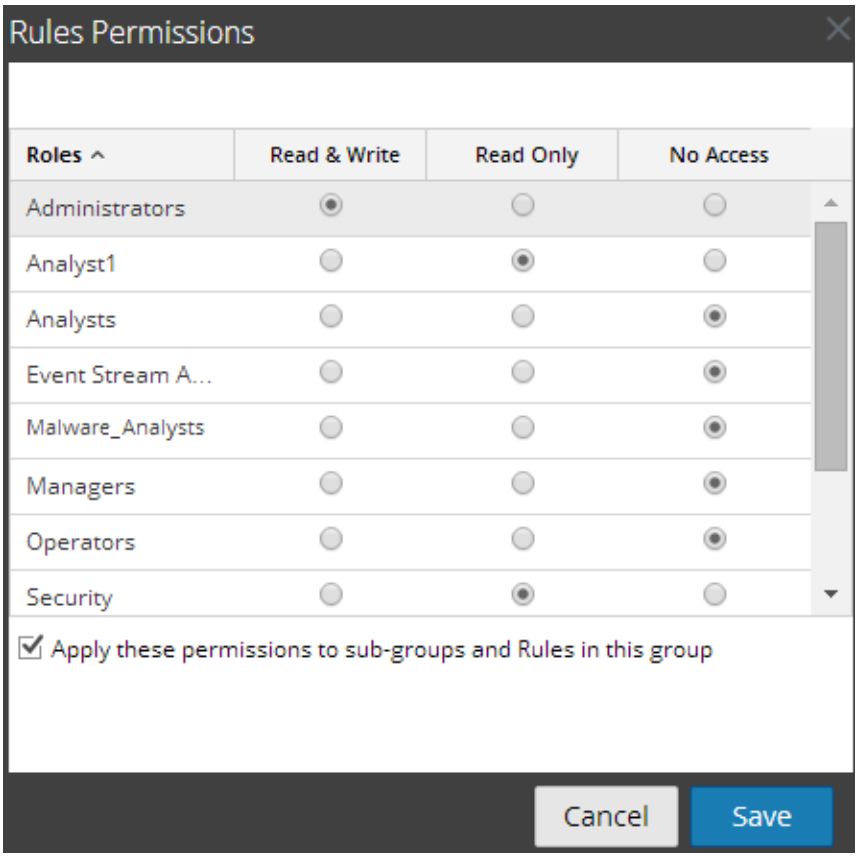
Access Control for a Rule Group

When you want to change the rule group permissions, you must select a rule group and set access permissions using the Rule Permissions panel.

Before applying rule group permissions, the default permission set for all the user roles is 'No Access' permission, and the checkboxes are deselected.



If you want to change the access permission for a specific user role, you must set these at the rule group level, as shown in the figure. Suppose, you want the **Administrators** to have access to all the rules in a Rule Group, you can set the permission '**Read & Write**' in the Rule Group Permissions panel.



You can also apply permissions to subgroups and rules in the group by selecting the checkbox.

The two scenarios are explained in brief:

- Scenario 1: Permissions applied to Rule Group/ Sub Group/ Rules based on the user role.
- Scenario 2: Permissions applied to Sub Group and Rules in the Group.

Role (Analysts)	Permissions applied to Rule Group/ Sub Group/ Rules based on the user role	Permissions applied to Sub group and Rules in the Group
Group	Read & Write	Read & Write
Sub Group	Read	Read & Write - Inherited
Rules	Read	Read & Write - Inherited

The access permissions that you set can be applied to subgroups and child objects of this group.

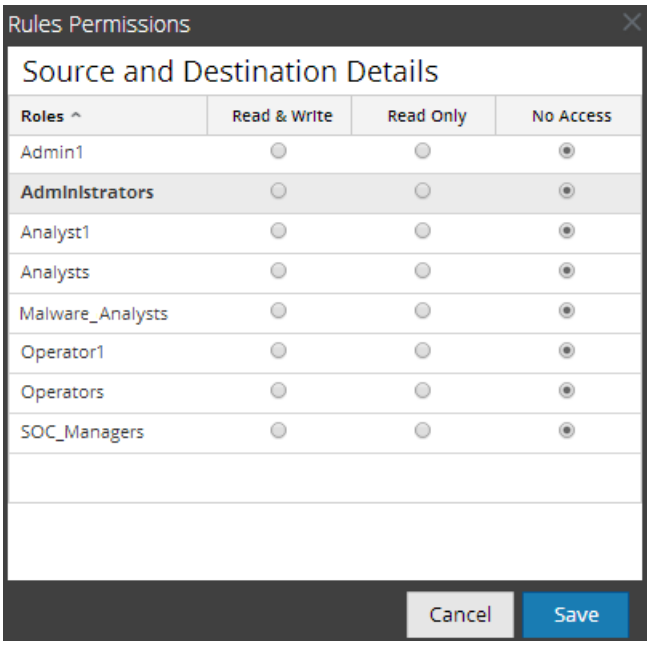
The Rule Group will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** rule group.

For scenario 1, each of the levels will have a permission set depending on the user role. For scenario 2, the permission at the Rule Group level will be inherited by the Sub Group and Rules in the Group.

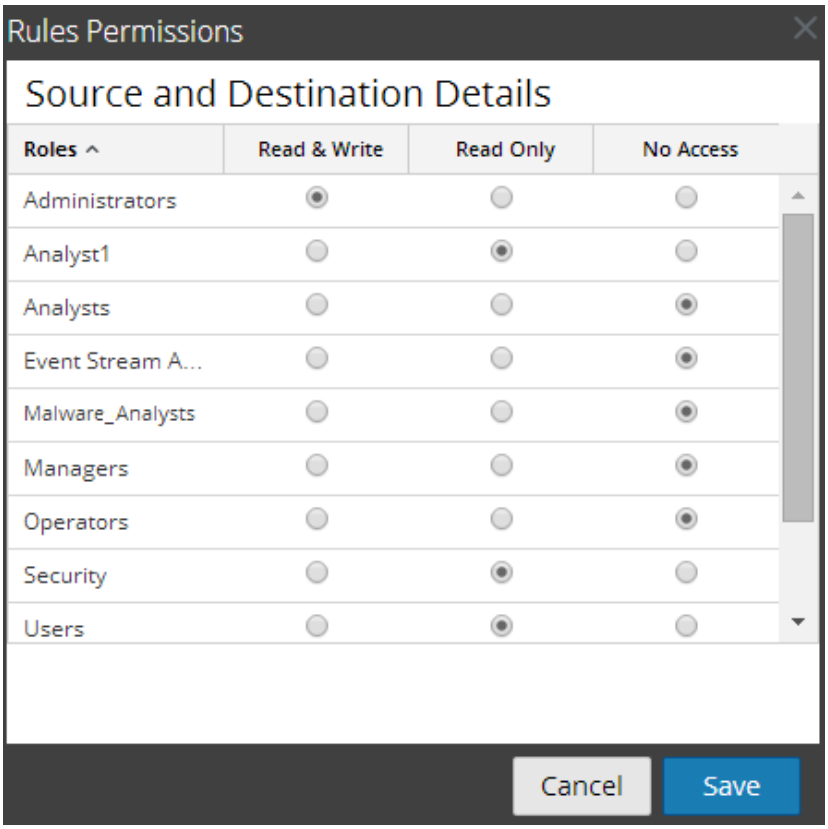
Access Control for a Rule

When you want to change the rule permissions, you must select a rule and set their access permissions using the Rule Permissions panel.

Before applying the Rule permissions, the default permission set for all the user roles is 'No Access' permission and the checkbox is deselected.



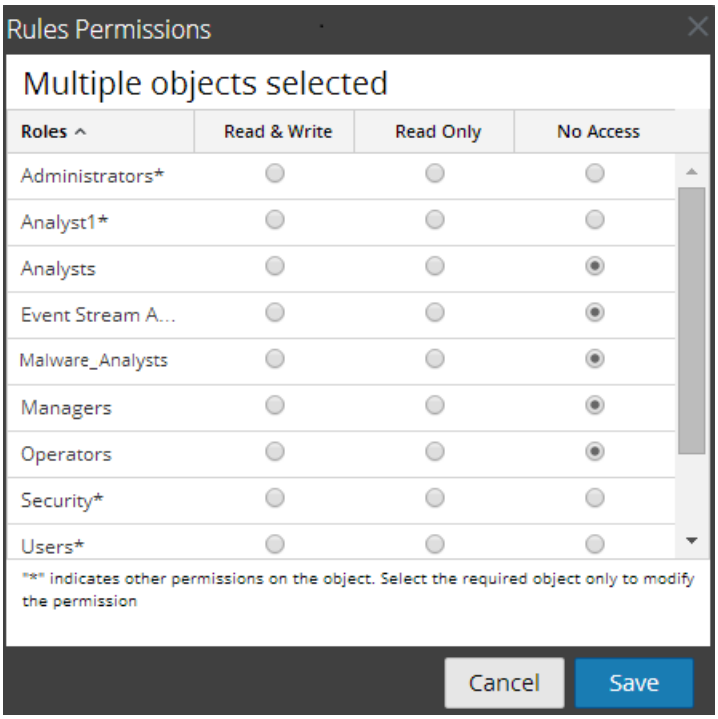
If you want to change the access permission for a specific user role, you must set these at the rule level, as shown in the figure. Suppose, you want the **Administrators** to have access to a specific rule, you can set the permission '**Read & Write**' in the Rule Permissions panel.



Access Control for a Rule When Multiple Rules are Selected

When you want to change permissions of multiple rules, you can select multiple rules at a time and set their access permissions using the Rules Permissions Panel. The access permission that you choose will be applied to all the selected rules.

Note: The '*' besides the role name indicates the other permissions available on the user role. If you want to change the access permission for the required user role, select the user role and change the access permission.



Log in as a specific user and view the access details

When you log in to the NetWitness Suite UI as a user having 'Read access' permission, all the rules will be denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Rules List panel.

When you log in to the NetWitness Suite

UI as a user not having 'Read & Write' access permission on a Rule, all the rules will be denoted with the symbol (👁‍🗨) and the rules appear grayed out on the Rules List panel.

The following figure shows the Rules List panel when logged in with minimal 'Read & Write' access permission.

Name	Type	Group	Date Modified	Actions
*(raw_log)-RULE	Warehouse	Aggregate Function	2014-07-13 09:46	
[redacted]	Warehouse	Regular	2014-07-16 07:34	
Accounts Created	NetWitness DB	Identity Management	2014-07-14 10:56	
Accounts Created SAW	Warehouse	Compliance_old	2014-07-14 09:40	
Accounts Created SAW	Warehouse	Warehouse	2014-07-25 09:48	
Accounts Created SAW(1)	Warehouse	Warehouse	2014-07-25 09:54	
Accounts Deleted	NetWitness DB	Identity Management	2014-06-26 08:35	

Note: If a user (other than administrator) creates a rule, ADMIN cannot access that rule.

Tabular Listing

The following table lists the columns in the Rules Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness Suite user interface.
Read & Write	The user can access, view, edit, delete, import, and export rules on the Rules view. The user can also change the permission on the rule.
Read Only	The user can only access and view the rule on the Rules view
No Access	The user cannot access or view the rule for which this permission is set.

Set Access Control for a Rule

You can set access control for a rule. The Reporting Engine provides access control at the rule level. Only a user who has the right set of permissions can perform tasks on the rule. The administrator when creating users and roles must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

At the rule level, you can set the following access permissions for the user roles in NetWitness Suite:

- Read & Write – View or edit the rules in the rule group.
- Read Only – View the rules in the rule group.
- No Access – Cannot view or edit the rules in the rule group.

Prerequisites

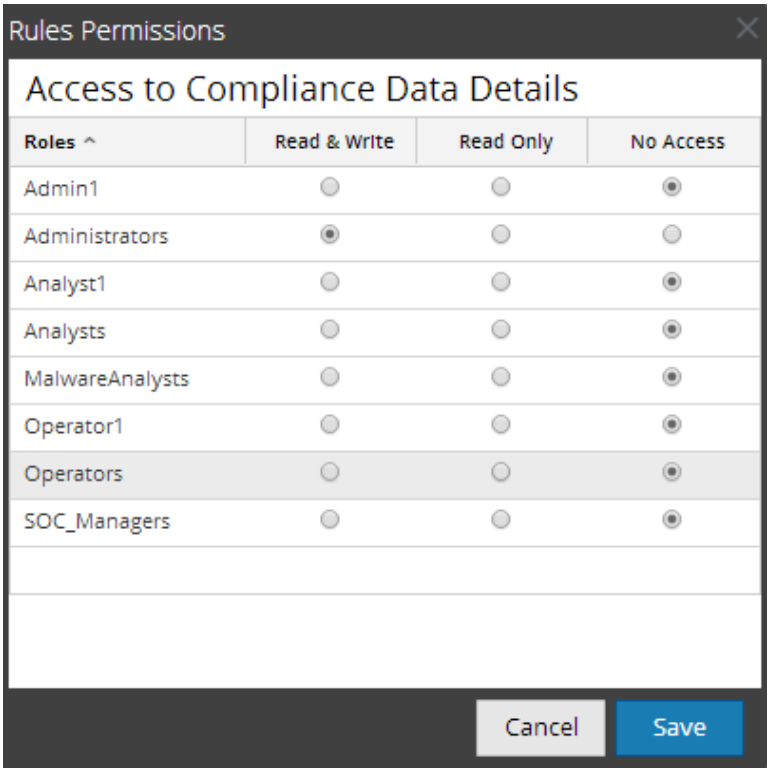
Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a rule.

To set access control for a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rules** list panel, select the rule.

3. Click > **Permissions** in the Rule toolbar.

   The **Rules Permissions** dialog is displayed.



4. Select the following appropriate access permission for the user role and click **Save**.
   - Read & Write
   - Read Only
   - No Access

Set Access Control for a Rule Group

You can set access control at the rule group level. Only a user who has the right set of permissions can perform the tasks on the rule. The administrator when creating users and roles must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

At the rule group level, you can set the following access permissions for the user roles in NetWitness Suite:

- Read & Write – View or edit the rules in the rule group.
- Read Only – View the rules in the rule group.

- No Access – Cannot view or edit the rule in the rule groups.

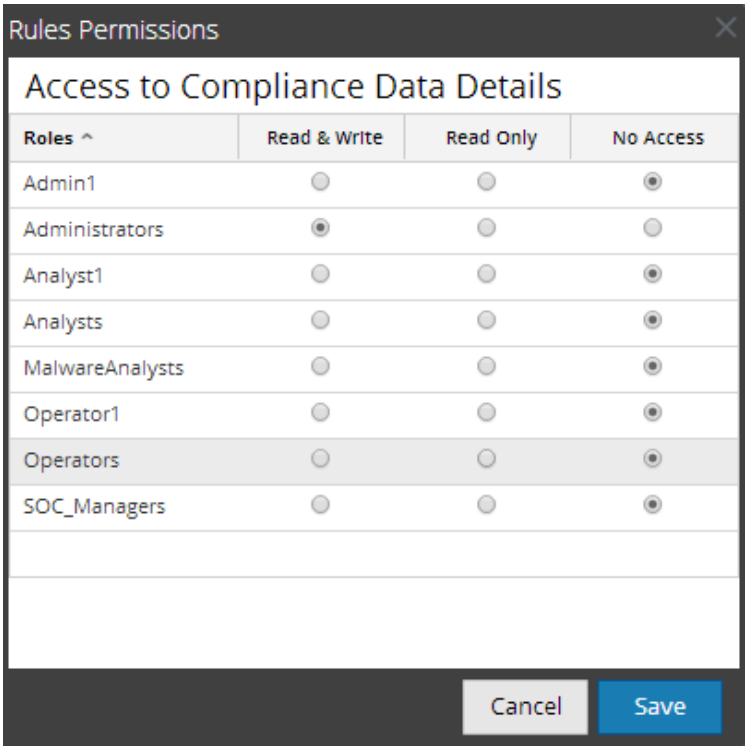
Prerequisites

Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a rule group.

To set access control for a rule group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rule Groups** panel, select the rule group and do one of the following:
   - Click and select **Permissions**.
   - Right-click the selected rule group and select **Permissions**.

   The **Rules Permissions** dialog is displayed.



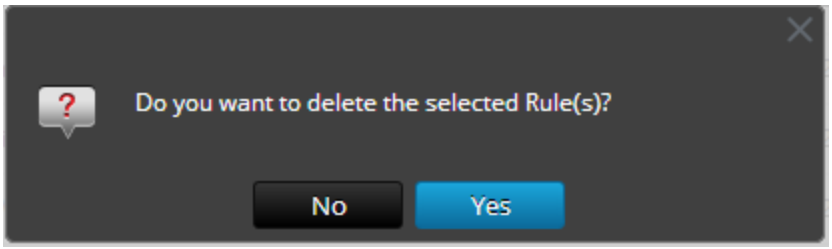
3. (Optional) Select the appropriate checkbox to apply these permissions to subgroups and child objects of this group.
4. Click **Save**.
   A confirmation message that permission is successfully set for the selected rule group is displayed.

Delete a Rule or Rule Group

To delete a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rules** panel, do one of the following.
   - Select a rule and click − in the Rule toolbar.
   - Click > **Delete**.

     A confirmation dialog is displayed.



> **Note:** If a rule is being used in a report, a warning that the rule is in use and cannot be deleted is displayed.

3. Click **Yes** to delete the rule.

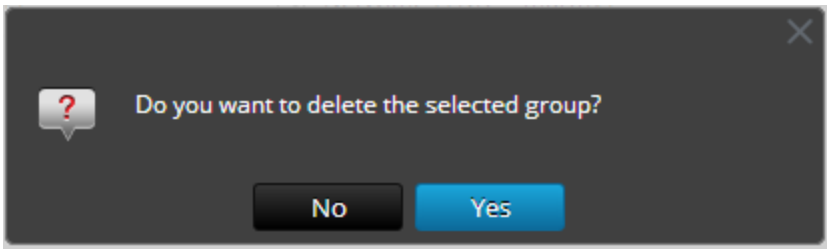
   A confirmation message that the rule is deleted successfully is displayed and the selected rule is deleted from the Rule List panel.

To delete a rule group, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.
2. In the **Rule Groups** panel, select the rule group that you want to delete.
3. Click −.

   A confirmation dialog is displayed.



Note: If any one of the rules in the group is being used in reports, a warning that the rule is in use and cannot be deleted is displayed.

4. Click **Yes** to delete the group.

   A confirmation message that the group is deleted successfully is displayed and the selected group is deleted from the Rule Groups panel.

Duplicate a Rule

To duplicate a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rules** list panel, select a rule that you want to duplicate.
3. In the Rule toolbar, click .

Edit a Rule

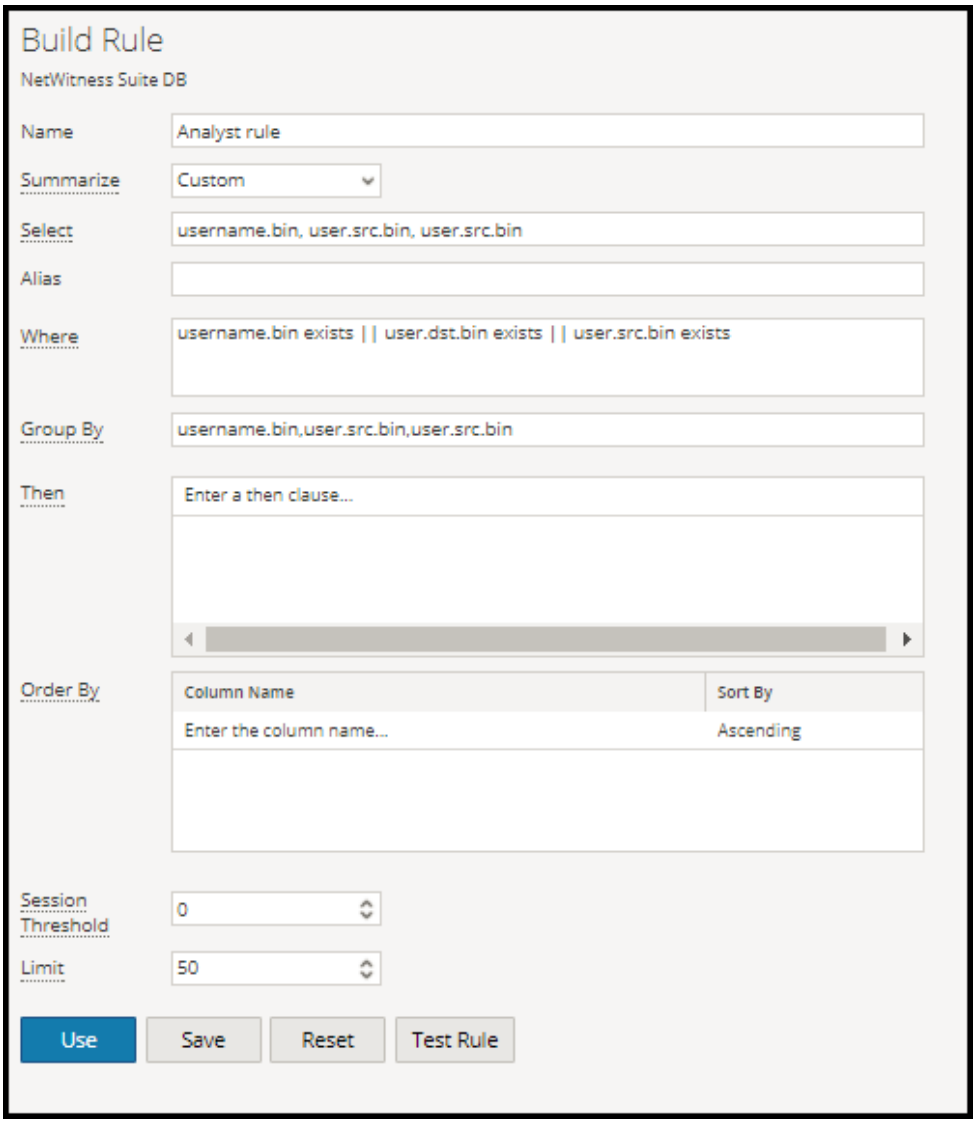
Prerequisites

To edit a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rules** list panel, do one of the following:
   - Select a rule and click in the Rule toolbar.

- Click > **Edit**.

  The Build Rule view tab is displayed.



Note: If a rule is edited, the updated rule definition is applied to the Reports, Charts, and Alerts where the rule is included.

3. Modify the required fields.
4. Click **Save**.

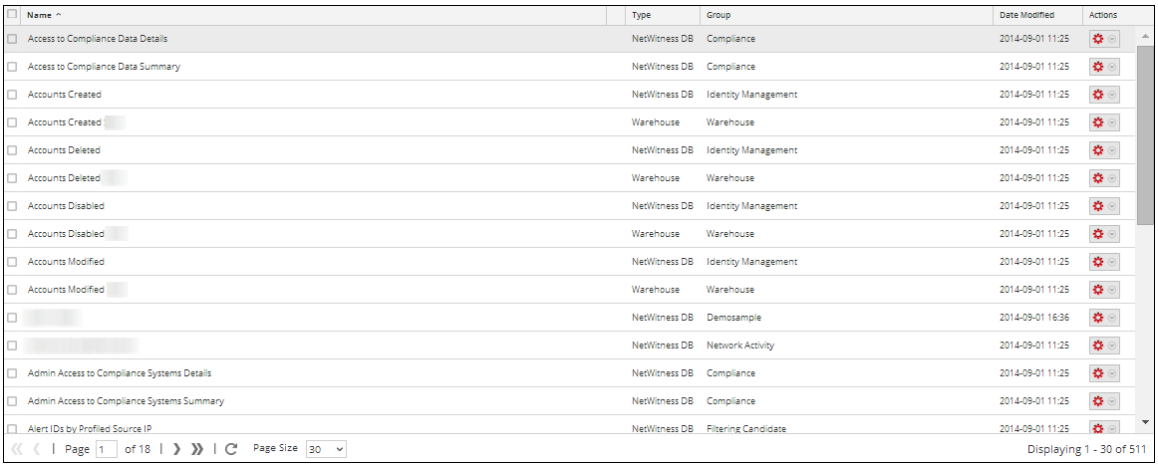
   A confirmation message that the rule is saved successfully is displayed.

When you edit a rule, ensure to re-select the Rule for which you want the Chart to be generated, so that the edited rule is applied. If you do not re-select the Rule and attempt to save or test the rule, the rule is saved and a warning message is displayed.

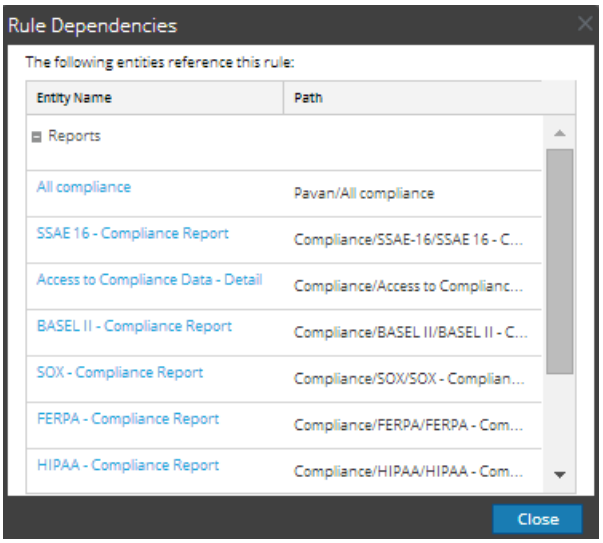
View Dependents of a Rule

You can view dependents of a rule. You must traverse a rule list, select a rule for which you want to identify the dependency over a report, chart, or alert.

The following figure shows the Rule View where you select the rule 'Access to Compliance Data Details'.



The following figure shows the dependency of the rule over alerts and reports.



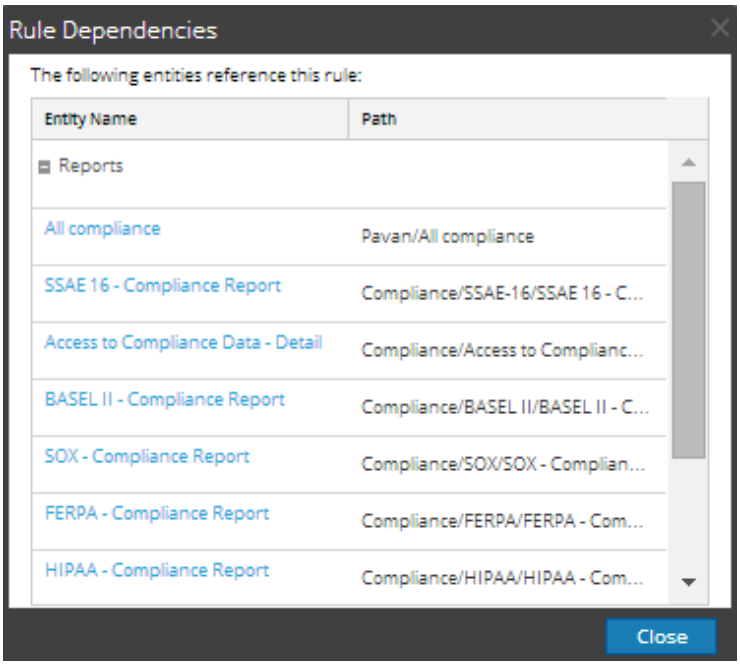
The following table lists the various columns in the Rule Dependencies dialog and their description.

Column	Description
Entity Name	The name of the entity referencing the rule.

Column	Description
Path	The path where the entity is located in the user interface.

To view dependents of a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Rules**.
   The Rule view is displayed.
3. In the **Rule List** panel, click > **Dependents**.
   The Rule Dependencies dialog is displayed.



Export a Rule or Rule Group

Prerequisites

Make sure that you have rules in the rule group.

To export a rule, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. In the **Rules** list panel, do one of the following:
   - Select a rule and click > **Export** in the Rule toolbar.
   - Click > **Export**.

   A browser-specific export dialog may be displayed, allowing you to open or save the file. You can export multiple rules at a time. To select multiple rule, press and hold the CTRL button and select the rules to be exported.

To export a rule group, perform the following :

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rule Groups** panel, select the rule group containing the rules which you want to export.
   You can export multiple rules groups at a time. To select multiple rule groups, press and hold the CTRL button and select the rules groups to be exported.
3. Click > **Export**.
   A browser-specific export dialog may be displayed allowing you to open or save the file.

Manage a Report

Access Control for a Report or Report Group

This section covers the access permissions the user has depending on the user role to manage a report and report group. The Reporting provides access control at the report and report group level. The user who has the right set of permissions can only perform the tasks in reporting module. The access control is managed by the administrator from the **ADMIN > Security > Roles** tab.

When creating users and user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Reports and Report Groups can be tied to a specific set of user roles so that when a user logs into NetWitness Suite, the reports with the access rights for the specific user role can be viewed. Users that belong to a user role with the 'Read & Write' access permission can define reports. Further, the access can be tightened so that reports are accessed only by those who have the 'Read Only' access.

Note: You must have 'Read Only' permission for a group to view the reports within that group.

At the report level, you can set the following access permissions for the user roles in NetWitness Suite:

- Read & Write
- Read Only
- No Access

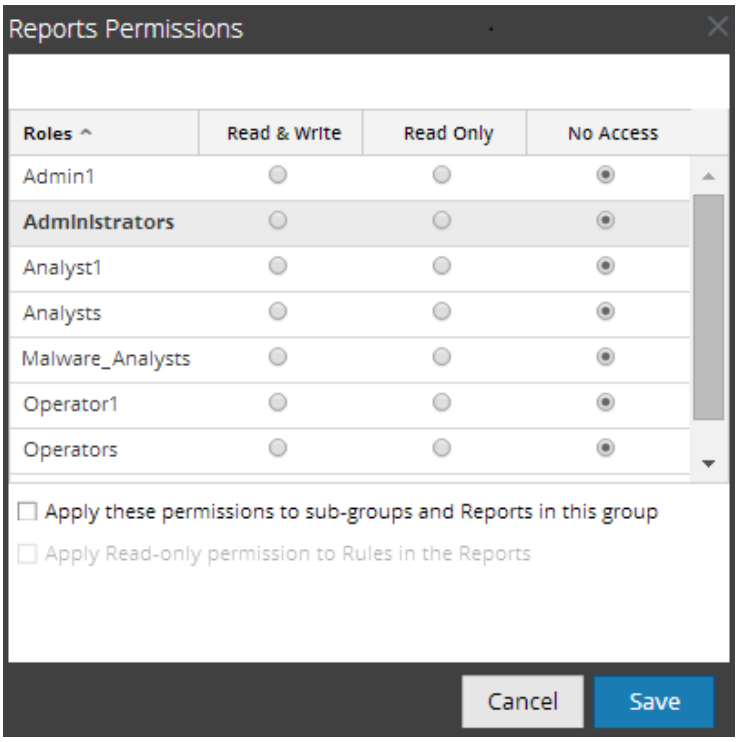
Suppose, you want the NetWitness Suite to have access to all the reports in a Report Group, you can set the permission '**Read & Write**' at the Report Group level. And, if you do not want the **Operator** role to have access to a specific set of reports in a report group, you can set the permission '**No Access**' at the Report Group level.

The permission is set only for the report group but not the reports, rules, or subgroups in the Report Group.

Access Control for a Report Group

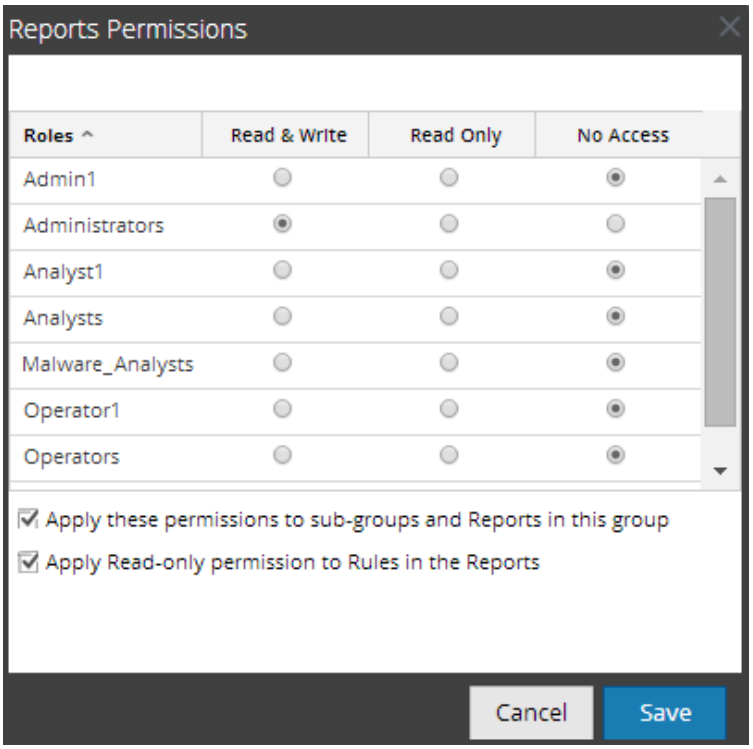
When you want to change the report group permissions, you must select a report group and set access permissions using the Reports Permissions panel.

Before applying report group permissions, the default permission set for all the user roles is 'No Access', except for Administrators, as shown in the figure.



If you want to change the access permission for a specific user role, you must set these at the report group level, as shown in the figure. <suppose,>Administrators to have access to all the reports in a Report Group, you can set the permission '**Read & Write**' in the Report Group Permissions panel.

You can also apply permissions to subgroups and reports in the group, as well as apply read-only permission to rules in the reports by selecting the appropriate checkboxes, as shown in the figure.



The three scenarios are explained in brief:

- Scenario 1: Permissions applied to Report Group/ Sub Group/ Report based on the user role.
- Scenario 2: Permissions applied to Sub Group and Report in the Group.
- Scenario 3: Read-only permission applied to Rules in the Report.

	Role (Analyst)	Permissions applied to Report Group/ Sub Group/ Report based on the user role	Permissions applied to Sub group and Report in the Group	Permission (Read-only) applied to Rules in the Report
Group	Read & Write	Read & Write	Read & Write	Read & Write

	Role (Analyst)	Permissions applied to Report Group/ Sub Group/ Report based on the user role	Permissions applied to Sub group and Report in the Group	Permission (Read-only) applied to Rules in the Report
Sub Group	Read	Read	Read & Write - Inherited	Read & Write
Report	Read	Read	Read & Write - Inherited	Read & Write
Rules	Read	Read	Read	Read

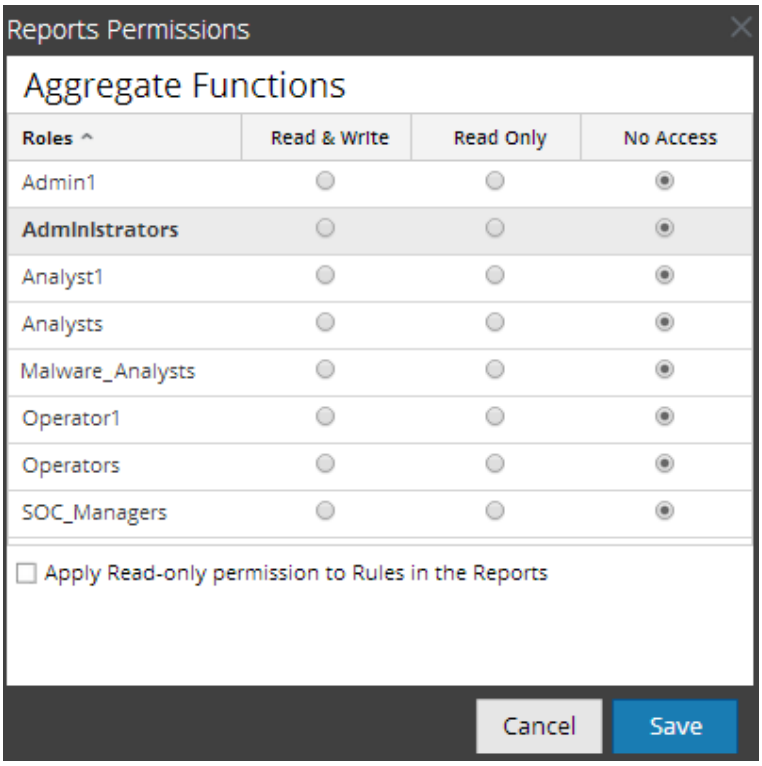
The Report Group will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** report group.

For scenario 1, each of the levels has a permission set depending on the user role. For scenario 2, the permission at the Report Group level (Read & Write) is inherited by the Sub Group and Reports in the Group. For scenario 3, the Read permission is set for the Rules except that the permission set for the rules cannot be higher than the permissions set for the Report Group.

Access Control for a Report

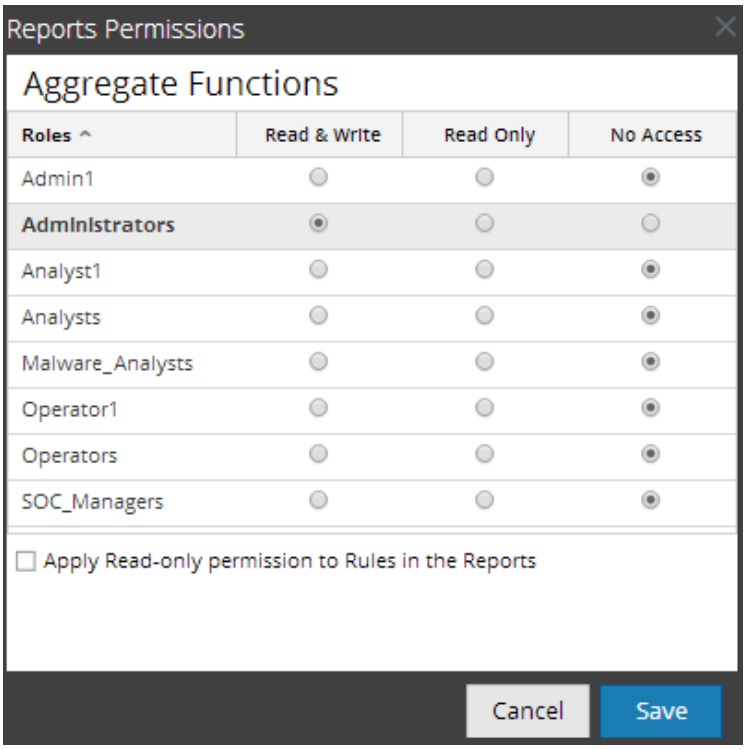
When you want to change the report permissions, you must select a report and set their access permissions using the Report Permissions panel.

Before applying the Report permissions, the default permission set for all the user roles is 'No Access' permission and the checkbox is unchecked, as shown in the figure.



If you want to change the access permission for a specific user role, you must set these at the report level, as shown in the figure. Suppose, you want the **Administrators** to have access to a specific report, you can set the permission '**Read & Write**' in the Report Permissions panel.

You can apply read-only permission to rules in the reports by selecting the checkbox, as shown in the figure.



The two scenarios are explained in brief:

- Scenario 1: Permissions applied to Report Group/ Sub Group/ Report/ Rules.
- Scenario 2: Read-only permission applied to Rules in the Report.

	Role (Analysts)	Permissions applied to Report Group/ Sub Group/ Report/ Rules based on the user role	Permission (Read-only) applied to Rules in the Report
Group	Read & Write	Read & Write	Read & Write
Sub Group	Read	Read	Read & Write
Report	Read	Read	Read & Write

	Role (Analysts)	Permissions applied to Report Group/ Sub Group/ Report/ Rules based on the user role	Permission (Read-only) applied to Rules in the Report
Rules	Read	Read	Read

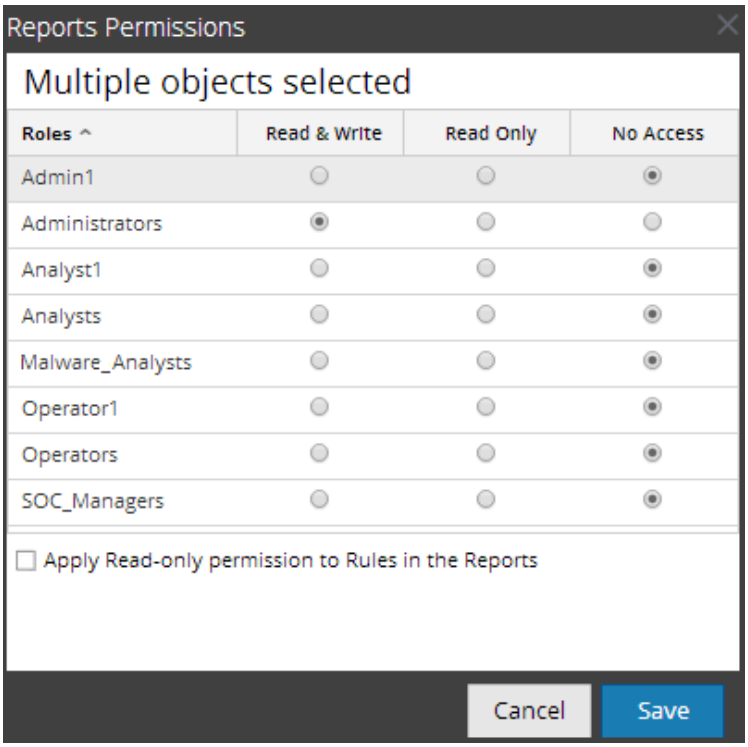
The Report will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** reports.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the Read permission is set for the Rules except that the permission for the rules cannot be higher than the permission for the Reports.

Note: If the permission for the rules is higher than the permission for the Reports then the permission is be applied only to the reports. For example, if you set the permissions for the Report Group as **No Access** and then specify the option *Apply Read-only permission to Rules in the Reports*, then the read-only permission is not set for the rules.

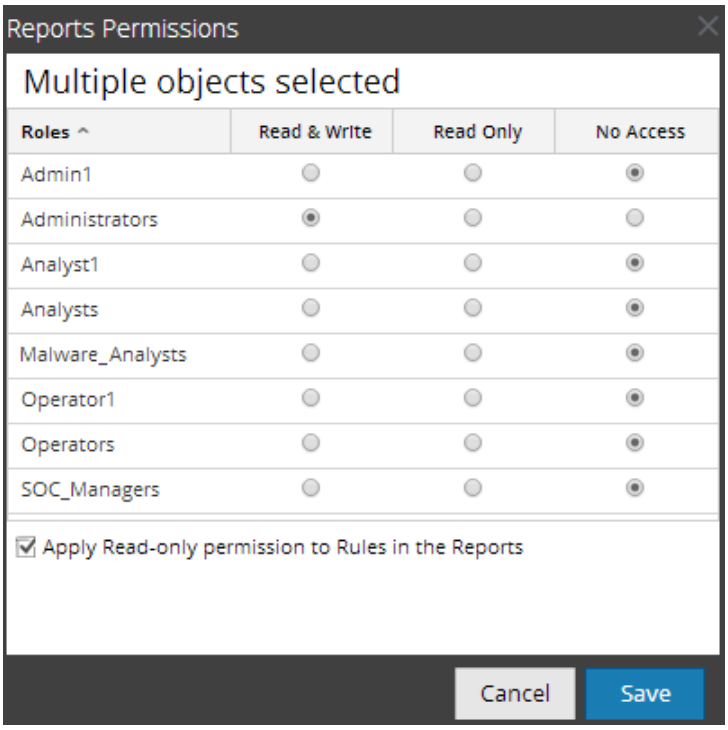
Access Control for a Report When Multiple Reports are Selected

When you want to change permissions of multiple reports, you must select several reports and set their access permissions using the Report Permissions panel. The access permission that you choose is applied to all the selected reports.



Access Control for a Report When Multiple Reports with several rules are Selected

When you want to change permissions when multiple reports with several rules are selected, you must select the checkbox in the Report Permissions panel, as shown in the figure. The read-only access permission is applied to all the rules of the selected reports, provided that the permission of the rules are lower than the permission of the reports.

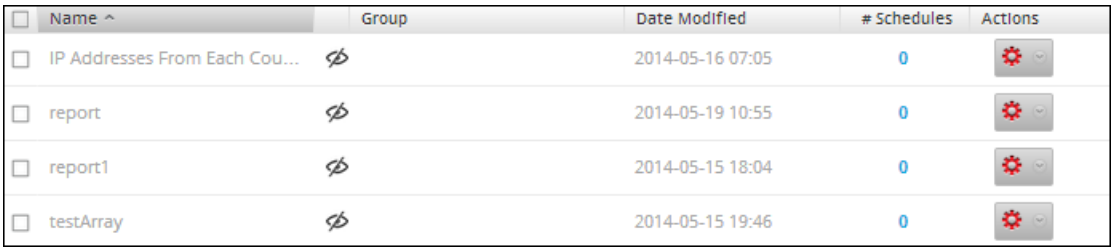


Log in as a specific user and view the access details

When you log in to the NetWitness Suite UI as a user having 'Read access' permission, all the reports is denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Report List panel.

When you log in to the NetWitness Suite UI as a user not having 'Read & Write' access permission on a Report, all the reports are denoted with the symbol (⊘) and the reports appear grayed out on the Report List panel.

The following figure shows the Report List panel when logged in with minimal 'Read & Write' access permission.



Note: If a User (other than the super user) creates a report there will be no access to that report for the super user.

Tabular Listing

The following table lists the various columns in the Reports Permissions Panel:

Column	Description
Roles	The role of the user logged into the NetWitness Suite UI.
Read & Write	The user can access, view, edit, import, export, and delete the report on the Reports view. The user can also change the permission on the report.
Read Only	The user can only access and view the report on the Reports view.
No Access	The user cannot access or view the report for which this permission is set.
Apply these permissions to subgroups and Reports in this group	Select the checkbox to apply the selected permissions to the report group, subgroups in the group and reports in the group. **Note:** This checkbox is populated only when you set access permissions for a Report Group.
Apply Read-only permission to Rules in the Reports	Select the checkbox to automatically apply permissions to the rules in the reports.

Set Access Control for a Report

Prerequisites

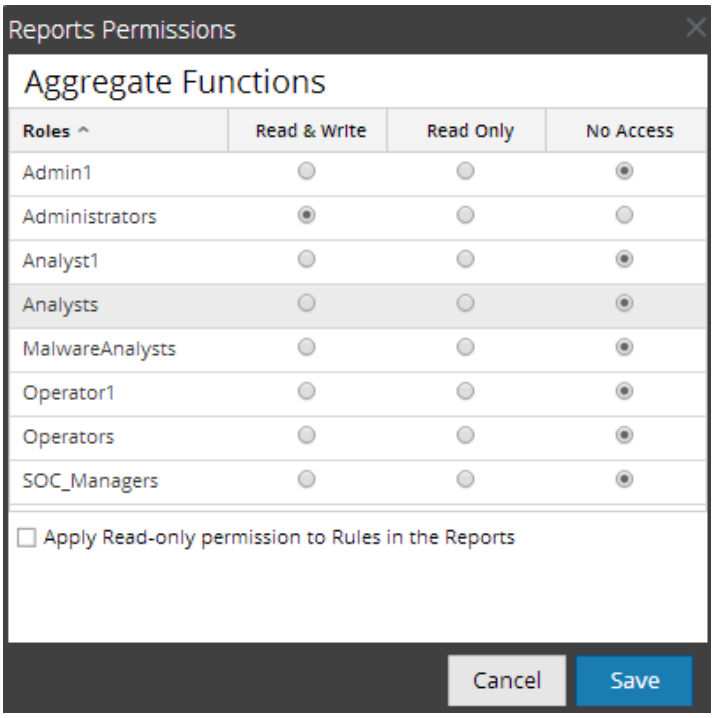
Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a report.

To set access permissions for a report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report.

4. Click > **Permissions**.

   The Reports Permissions dialog is displayed.



5. Based on the user role, select the appropriate buttons.
6. (Optional) Select the checkbox, if you want to provide read access permission to rules in the reports.

Note: On selecting the check box, all dependent rules are given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

6. Click **Save**.

   A confirmation message that the permission is set for the selected report is displayed.

Set Access Control for a Report Group

Prerequisites

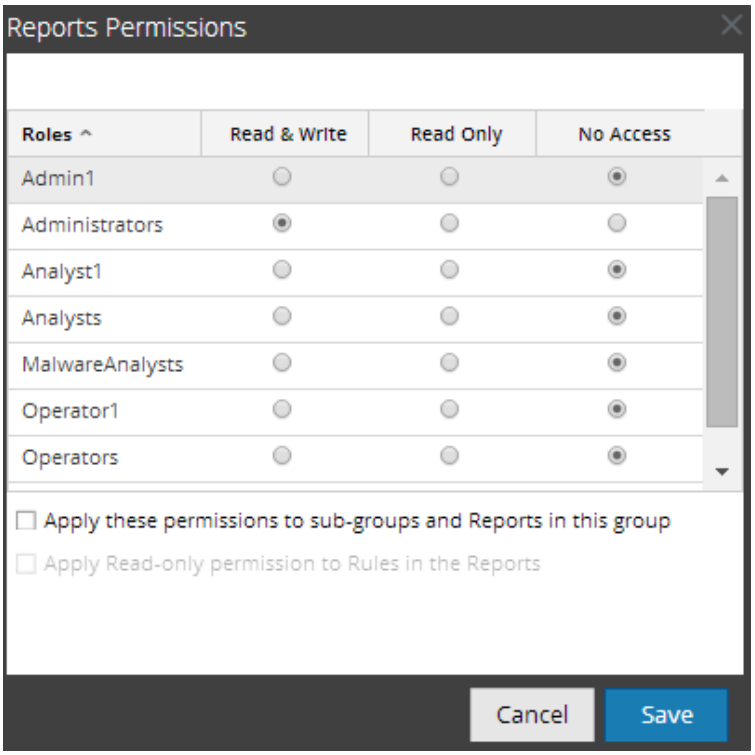
Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a report group.

To set access permissions for a Report Group, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.
   The Report view is displayed.
3. In the **Report Groups** panel, select or right-click on a report group.
4. Click > **Permissions**.
   The Reports Permissions dialog box is displayed.



4. Based on the user role, select the appropriate buttons.
5. (Optional) Select the appropriate checkbox to apply the selected permissions to subgroups and reports in the group.
6. (Optional) Select the appropriate checkbox to provide read access permission to rules in the reports.

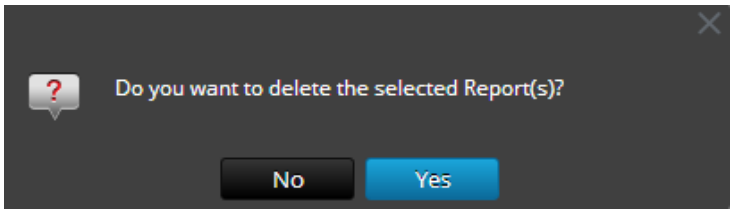
Note: On selecting the check box, all dependent rules is given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

7. Click **Save**.
   A confirmation message that the permission is successfully set for the selected report group is displayed.

Delete a Report or Report Group

To delete reports in a group or subgroup from the Report List panel:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, do one of the following:
   - Select the reports and click −.
   - Click ⚙ > **Delete**.
     A confirmation dialog is displayed.



4. Click **Yes** to delete the report.
   A confirmation message that the report is deleted successfully is displayed and the selected report is deleted from the Report List panel.

Delete a Report Group

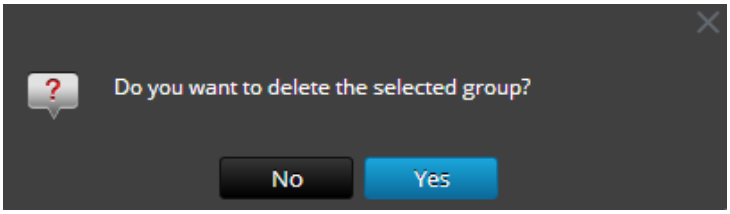
Prerequisites

Make sure that you have no reports associated with the report group.

To delete report groups in the default folder or subgroups under a report group, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.

3. In the **Report Groups** panel, select the report group and click −.
   A confirmation dialog is displayed.



4. Click **Yes** to delete the group.
   A confirmation message that the group is deleted successfully is displayed and the selected group is deleted from the Report Groups panel.

Duplicate a Report

You can duplicate a report to schedule multiple report for the same report. The duplicated report is displayed in the Reports List panel with suffixes. For example, Report (1).

Generally, the duplicate option is used in two scenarios:

- You want to make a copy of the report, to move the same report to another group.
- You want to retain most of the configuration settings for an object but modify few of these settings.
  For example, when you have a complex query in a rule or several rules in a report, it is very much appropriate to use the duplicate option.

To duplicate an existing report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports.**
   The Report view is displayed.
3. In the **Report List** panel, select a report that you want to duplicate and click .
   The report is saved successfully and added to the Report list.

You can move the duplicated report to another group.

Edit a Report

To edit reports in a group or subgroup from the Report List panel, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, do one of the following:
   - Select a report and click .
   - Click > **Edit**.

   The Build Report view tab is displayed.

4. Modify the text and add more rules to the report (if required).
5. Click **Save**.
   A confirmation message that the report is saved successfully is displayed.

Refresh a Report Group or Report List

You can refresh a report group or reports to view the re-arrangement of groups or reports.

To refresh a report group or reports, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.

The Report view is displayed.

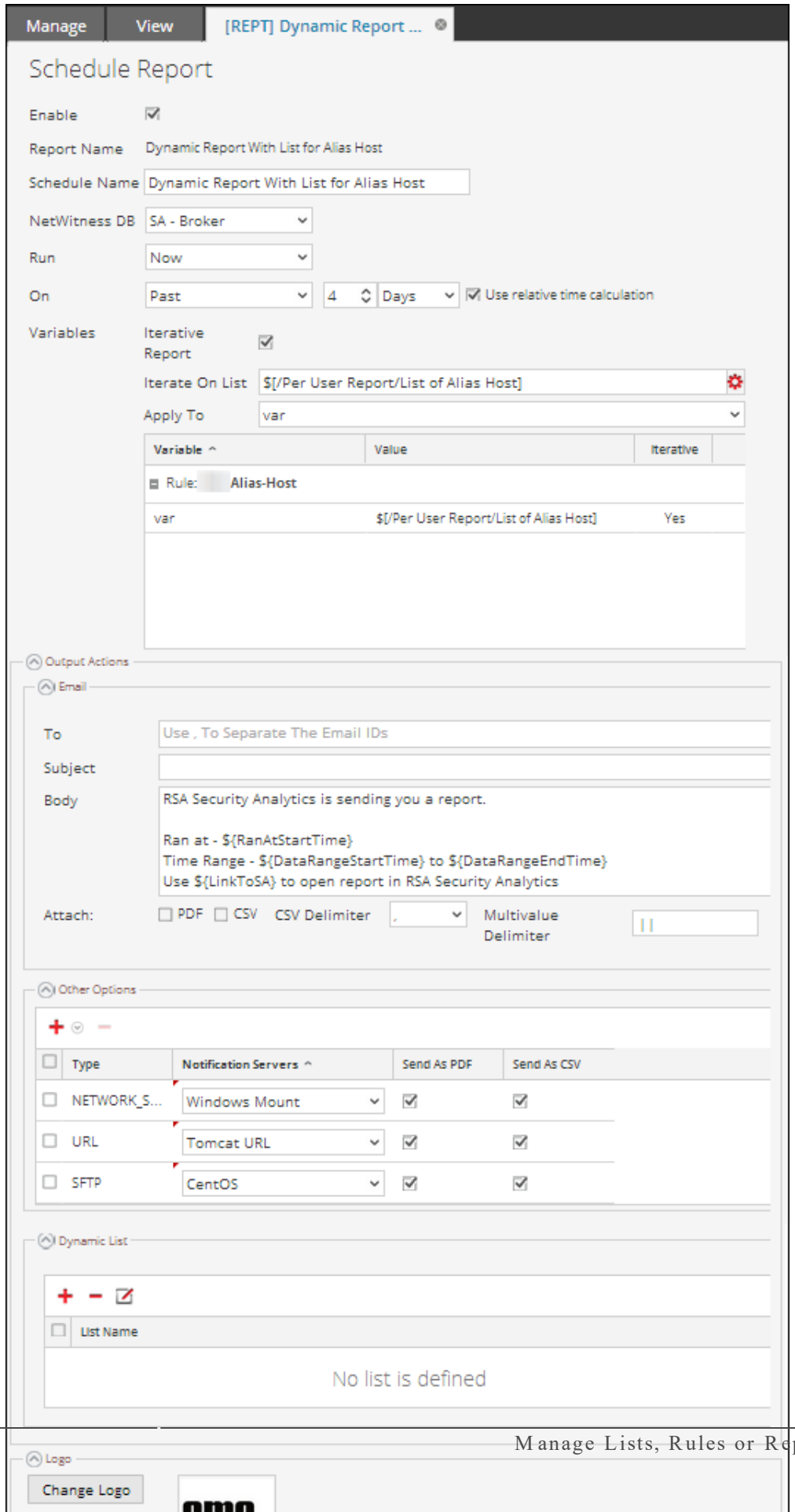
3. Do the following to move the group or reports to a new location:
   - In the **Report Groups** panel, drag and drop the group.
   - In the **Reports List** panel, drag and drop the reports to the desired group in the Report Groups panel.
     The report group or reports are moved to the new location.
4. Do the following to refresh a group or report list:
   - In the **Report Groups** panel, click .
     The report group gets refreshed.
   - In the **Report List** panel, click .
     The Report list gets refreshed.

Edit a Scheduled Report

To edit a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report and click > **View Scheduled Reports**.
   The View Scheduled Reports tab is displayed.
4. In the **Scheduled Reports List** panel, do one of the following:
   - Select a report and click .
   - Select a report and click > **Edit Schedule**.

The Schedule Report tab is displayed.


Manage
View
[REPT] Dynamic Report ...
Schedule Report
Enable
Report Name
Dynamic Report With List for Alias Host
Schedule Name
Dynamic Report With List for Alias Host
NetWitness DB
SA - Broker
Run
Now
On
Past
4
Days
Use relative time calculation
Variables
Iterative Report
Iterate On List
$[/Per User Report/List of Alias Host]
Apply To
var
Variable
Value
Iterative
Rule:
Alias-Host
var
$[/Per User Report/List of Alias Host]
Yes
Output Actions
Email
To
Use , To Separate The Email IDs
Subject
Body
RSA Security Analytics is sending you a report.
Ran at - ${RanAtStartTime}
Time Range - ${DataRangeStartTime} to ${DataRangeEndTime}
Use ${LinkToSA} to open report in RSA Security Analytics
Attach:
PDF
CSV
CSV Delimiter
Multivalue Delimiter
Other Options
Type
Notification Servers
Send As PDF
Send As CSV
NETWORK_S...
Windows Mount
URL
Tomcat URL
SFTP
CentOS
Dynamic List
List Name
No list is defined
Logo
Change Logo

5. In the Schedule Report tab, do the following:
   a. In the **Schedule Name** field, modify the name for the schedule report configuration.
   b. To execute the reports as per the schedule, select the **Enable** checkbox.
   c. From the **Data Source** field, select the datasource.

   Note: If the data source is not listed, ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in the *Reporting Engine Configuration Guide*.

6. (Optional) From the **Warehouse Resource Pool** drop-down, select the pool or queue for the report.

   Note: The **Warehouse Resource Pool** drop- down is displayed only if the Warehouse Rule is selected. If no pools or queues are entered for the Reporting Engine, this field is disabled.

7. From the **Run** field, select the type of run schedule. (For example, Now or Hourly).
8. Select the date range to run the query based on absolute duration or select the **Use relative time duration** checkbox to run the query based on relative duration.
9. (Optional) In the Output Actions panel, do the following:
   i. Type the email address and subject.
   ii. Edit the body of the message for the report.
   iii. Select the format of the attachment.
   iv. Type a value for the CSV and Multivalue delimiters.
10. (Optional) In the Other Options field, do the following:
    i. Click > **SFTP** or **URL** or **Network Share**. Based on the selected option, a row gets added in the Other options field.
    ii. Select the appropriate options to send the report in PDF or CSV format to the configured SFTP, URL or Network Share.
11. (Optional) To add a list in the Dynamic List panel, see Generate a List from the Scheduled Report section in Create and Schedule a Report.

12. (Optional) To choose another logo in the Logo panel, see Manage and Select a Report Logo section.

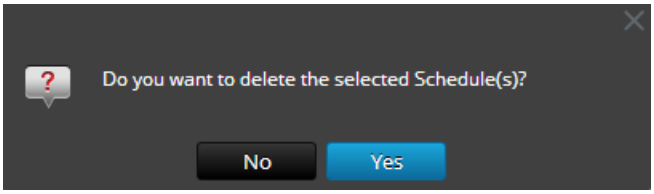
    Note: If you do not specify a logo, the default RSA logo is used.

13. Click **Schedule**.
    The scheduled report executes as scheduled and provides the configured outputs.

Delete a Scheduled Report

To delete a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report** toolbar, click **View All Schedules**.
   View Scheduled Reports is displayed.
4. In the **Scheduled Reports List** panel, select the report.
5. Click >**Delete Schedule**.
   A confirmation dialog is displayed.



6. Click **Yes** to delete the scheduled report.
   A confirmation message that the scheduled report is deleted successfully is displayed and the selected schedule is deleted from the Scheduled Reports List panel.

Export a Report

You can export the selected reports to an external file that can be later imported to another NetWitness Suite environment.

Prerequisites

Make sure that you have reports in the report group.

To export selected reports in the Report Groups panel to an external file, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, do one of the following:
   - Select a report and click > **Export**.
   - Click > **Export**.

   You can export multiple reports at a time. To select multiple reports, check the checkbox of the report to be exported. The exported file is saved to the local drive in an archived format.

Open CSV files with Unicode characters in MS Excel

To open downloaded CSV files containing Unicode characters in MS Excel, follow these steps:

1. Download and save the CSV file.
2. Open Microsoft Excel and navigate to the **Data** tab.
3. Click on **From Text** menu item; find the CSV file that you downloaded and click **Import**.
   The Text Import Wizard is displayed.
4. Select **Delimited** or **Fixed Width** data type from the **Original data type** radio button.
5. Click **File origin** drop down list and select **65001: Unicode (UTF-8)** and click **Next**.
6. Select the delimiter that was used in the file that you imported and click **Next**.
7. Select the data format for each column of data that you want to import and click **Finish**.
   The correct output is displayed in an MS Excel sheet.

Export a Report Group

You can export a selected report groups to an external file that can be later imported to another NetWitness Suite environment.

Prerequisites

Make sure that you have reports in the Report Group.

To export selected report groups in the Report Groups panel to an external file, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report Groups** panel, select a report group and click and select one of the following:
   - **Export** - This selection exports a report in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple report groups at a time. To select multiple report groups, press and hold the CTRL button and select the report groups to be exported. The exported file is saved to the local drive.

Import a Report or Report Group

You can import a group containing subgroups and reports from other instances of NetWitness Suite into Report Groups panel. Reports must be in a valid binary file that was exported from another NetWitness Suite instance. During the import process, you select the binary file and specify whether existing reports with the same name must be overwritten or not by the reports contained in the binary import file.

- If you choose to overwrite, all duplicate rules, lists and reports are overwritten by the contents of the binary import file.
- If you choose not to overwrite, and a duplicate rule, list or report exists in the target folder, the import fails and display a message about duplicate reports.

You cannot import reports to a specific report group. The imported files are stored in the **All**root folder.

Prerequisites

Make sure that you have the reports or report groups exported from other instances of NetWitness Suite.

To import groups containing subgroups and reports from other instances of NetWitness Suite into Report Groups panel, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report Groups** panel, select a folder to import the file.
4. Do one of the following:
   - In the **Report Groups** panel, click > **Import** to import a group.
   - In the **Report** toolbar, click > **Import** to import a report.
     The Import Report dialog is displayed. You can import multiple reports and report groups at a time. To select multiple reports or report groups, press and hold the CTRL button and select the reports or report groups to be imported.
5. Click **Browse** to select the binary file.
   NetWitness Suite provides a file system view of the files.
6. Locate the binary file and click **Open**.
   The file gets added to the Import Report list.
7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, check the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, check the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing report in the library with an identically named report in the binary file when importing, check the **Report** checkbox. If you do not select the Overwrite option, and an identical report is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Enable or Disable a Scheduled Report

To enable or disable a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report and click > **View Scheduled Reports**.
   View Scheduled Reports is displayed.
4. Select a report from the Scheduled Reports List panel.
5. Click > **Enable**.
   The state of the report is changed to 'Running', if the report is scheduled to run immediately.
6. Click > **Disable**.
   The state of the report is changed to 'Inactive'.

Start or Stop a Scheduled Report

To start or stop a scheduled report, perform the following:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report and click > **View Scheduled Reports**.
   The View Scheduled Reports view is displayed.
4. Select a report from the Scheduled Reports List panel.
5. Click > **Start**.
   The state of the report is changed to 'Running', if the report is scheduled to run immediately.

6. Click > **Stop**.

   The state of the report is changed to 'Completed'.

View an Execution History of a Scheduled Report

You can view the execution history of a scheduled report. You can view the history of a scheduled report that is run. You can view the history based on the following criteria:

- Number of past schedules executed
- Start date and end date for the date range

You can view the details such as how many times the scheduled report was executed, the time of execution (seconds), execution state. You can also view the report generated on a full screen.

To view the execution history of a scheduled report, perform the following:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Report List** panel, do one of the following:

   - Click > **View Scheduled Reports**.
   - Click the **#Schedules** column.

     The Schedule Reports view tab is displayed with the status of each of the scheduled report.

4. Do one of the following:

   - Select a scheduled report and click > **Execution History**.
   - Select a scheduled report and click .

     The Execution History view is displayed.

Note: By default, you can view 10 number of execution history of a scheduled report. The execution history shown depends on the Retain Report History Configuration set on the **General**tab of the **ADMIN > Services > Reporting Engine Config**view.
For example, if you set the Retain Report History Configuration to 100 days, the data displayed on the Execution History view. is the past 100 days execution history details considering the current date information.

5. From the **Get history by:** field, select the type of history to be fetched. (For example, Past or Range (Specific))
6. In the **Count** field, enter the number of executions to be displayed.
7. Click **Show History**.
   The execution history of the scheduled report is displayed.

Manage and Select a Report Logo

Prerequisites

Make sure that you have the Reporting Engine service defined prior to managing a logo.

Manage Report Logos

To manage logos, perform the following:

1. Go to **ADMIN** > **Services**.
   The Services view is displayed.
2. In the **Services List** panel, select an Reporting Engine service and click **View** > **Config**.
   The services config view is displayed.
3. Select the **Manage Logos** tab.
   All the available logos are displayed.

Add a Logo

To add a logo, perform the following:

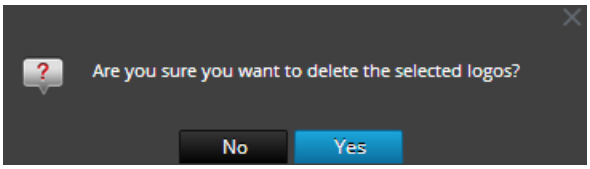
1. In the **Manage Logos** tab, click .
   A file browser opens where you can choose the file from the local drive.
2. Select the logo and click **Select**.
   The selected logo gets added to the Manage Logos section.

Delete a Logo

To delete a logo, perform the following:

1. In the **Manage Logos** tab, do one of the following:
   - Select the logo and click − .
   - Perform (Ctrl+click) to select multiple logos and click −.

   A confirmation dialog is displayed.



2. If you want to delete the logo, click **Yes**.

   The selected logo is deleted from the Manage Logos section.

Set Default Logo

To set a default logo, perform the following:

In the **Manage Logos** tab, select a logo and click Set default.

The chosen logo is set as the default logo for the RE service.

Select a Logo

To select a logo, perform the following:

1. Go to **ADMIN** > **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Report List** panel, select a report.

4. Click > **View Scheduled Reports**.

   The View scheduled reports view tab is displayed.

5. Select a scheduled report and click > **Edit Schedule**.

   The Schedule a Report view tab is displayed.

6. In the Logo panel, click **Change Logo**.

   The Change a Logo dialog box is displayed.

7. Do one of the following:

- Click **Upload new logo** to upload another logo.
- Select a logo from the list.

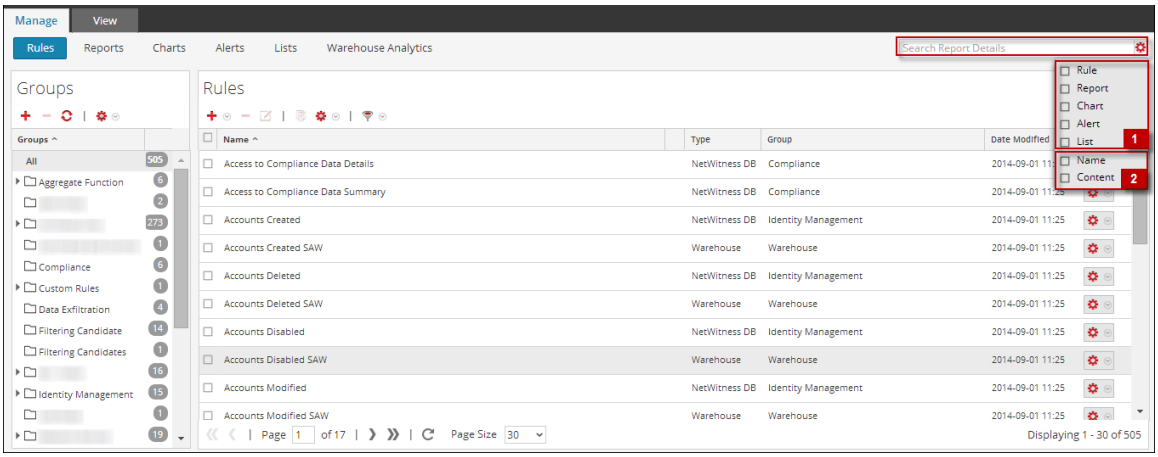
8. Click **Select**.
   The selected logo is available on the Logo panel.

Search Reporting Details

This section provides instructions on how to perform a keyword search on name and content for each of the Reporting components. You can perform a keyword search on name and content for each of the Reporting components (Rule/Report/Chart/Alert/List) on the Reporting UI.

Note: You cannot search based on date and numeric values.

The following figure shows the search parameters available in the Reporting Module:



The following are the search parameters available on the Reporting UI:

1. Search for entities (rule, report, chart, alert, list).
2. Search for the entities based on either the name or content.

Note: Searches are case insensitive. For example, Completed is equivalent to completed.

Prerequisites

In the Reporting Module, you can perform a keyword search based on the name and content (definition). In this context, content implies definition of each of the reporting components. For instance, the value defined in the rule, report, report schedule, chart, and alert panel. You can also prioritize your search by selecting either or all of the components: Rule, Report, Chart, Alert, or List.

Note: You cannot search based on the List values and list path stored in schedule definition panel.

For example, to search for the rule name (ExpertRule), you must select **Rule, Name, and Content** in the **filtering options** drop-down to view all the rule names that matched the search. You can similarly search for a report, chart, alert, or list definition.

To search for reporting details from the Manage tab, perform the following:

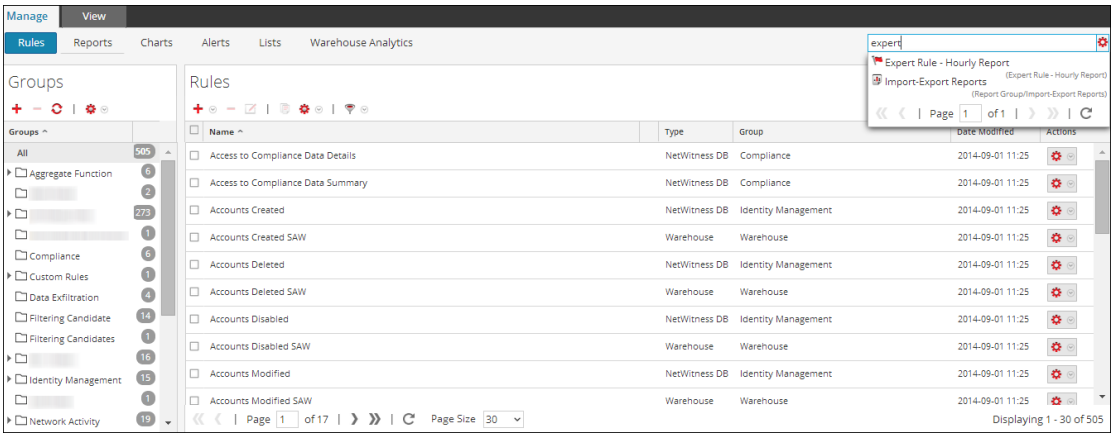
1. Go to **MONITOR** > **Reports**.

   The **Manage** tab is displayed.

2. Click and select the appropriate criteria to search.

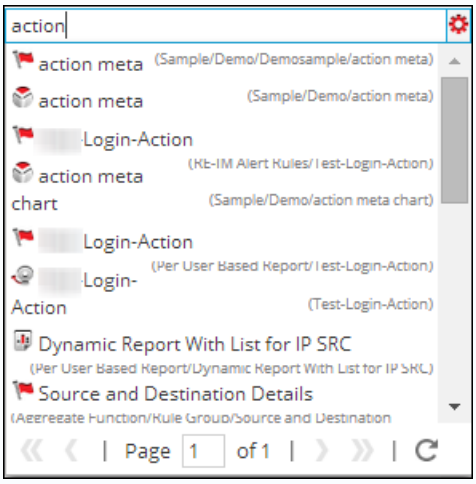
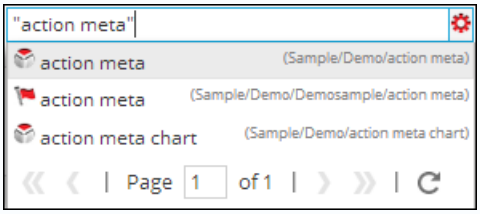
3. In the **Search** field, enter the text to be searched.

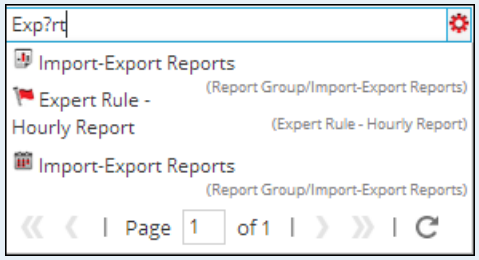
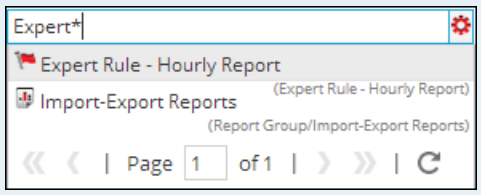
   The search drop-down list is displayed:

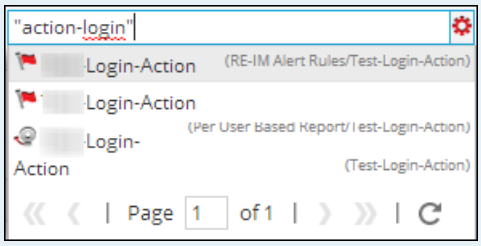


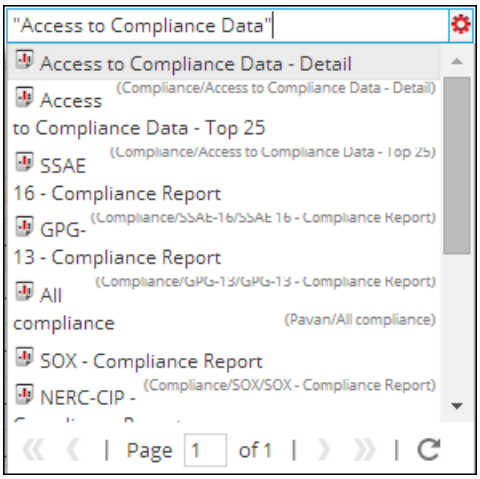
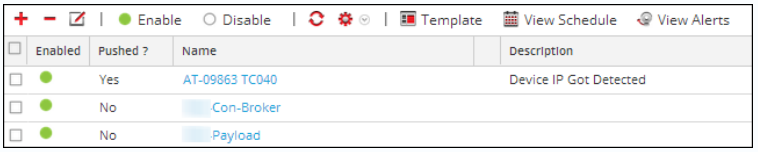
Search Syntax and Different Types of Search

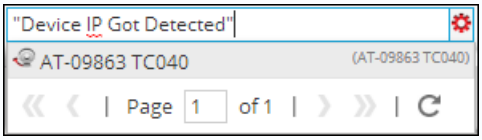
The following table explains the search syntax and the possible searches that can be performed on the Reporting UI.

Search Types	Description
Word or phrase based search	**Word Based Search**: To search for a word such as "action" or "meta", you must enter the word in the search box. The following figure shows the search results for the text **action**.  **Phrase based search:** A Phrase is a group of words surrounded by double quotes such as "action meta". To search for a phrase, you must enclose phrases in double-quotes in the search box. The following figure shows the search results for the phrase "action meta". 

Search Types	Description
Wildcard Search (Single/ Multiple/ Special Character Search) The question mark "?" symbol is used to perform a single character wild card search and asterisk "*" symbol is used to perform multiple character wildcard search.	**Single character search:** The single character wildcard search looks for terms that match with the single character replaced. For example, to search for "Expert" or "Export" you can use the search syntax: Exp?rt The following figure shows the search results for the wildcard character **Exp?rt**.  **Multiple character search:** Multiple character wildcard search looks for 0 or more characters. For example, to search for Expert, or Experts, you can use the search syntax: Expert* The following figure shows the search results for the wildcard multiple character **Expert***. 

Search Types	Description
	Special character search: Certain punctuation and special characters are ignored during search (@#$%^&*(){}"~=+-[]\?|!:,.). For example, a search for action-login will be interpreted during search as "action" "login", that is, if rules exist with name "action-login" and "action@login" and search string is "action-login", the search result will return both the rules. 

Search Types	Description
Search based on name or content	**Search based on name:** When you want to search based on the name of a report, select **Report**and **Name**box from the filtering options drop-down. For example, to search for the report name "Report With Multiple Rules", you can use the search syntax: "Access to Compliance Data" **Note:** When you search for a report, it implies you can search for the report schedules as well. The search result will return the report containing the specific name.  **Search based on content:** When you want to search for the content within an alert, say alert description, select **Alert** and **Content** box from the filtering options drop-down. For example, to search for the alert description "Device IP Got Detected", you can use the search syntax: "Device IP Got Detected"  The search will return the result having the specific content.

Search Types	Description
	

Troubleshooting

This section provides troubleshooting instructions for issues faced when using the Reporting module in NetWitness Suite.

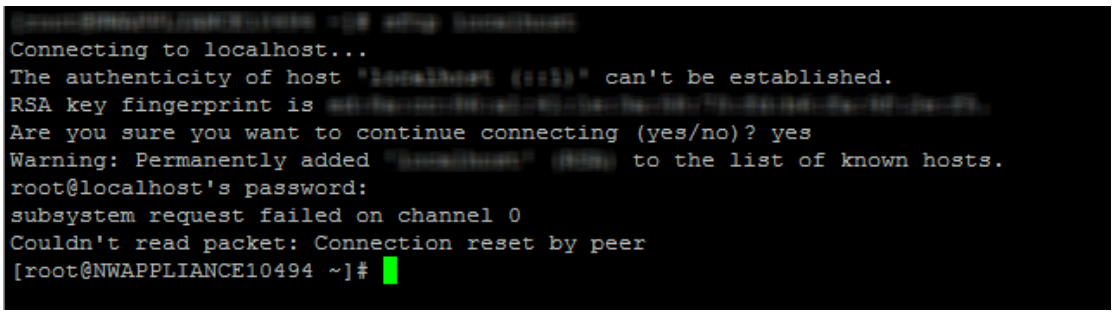
Configuring SFTP Server Issue

Procedure

Try the following steps if you face any issues while configuring the Linux SFTP server:

1. If the Report Output Action for the configured SFTP fails, you must SSH to the SFTP server and try to connect locally to check if SFTP is working fine.

   Connect to SFTP server:

2. If the Local connection fails, open the file **sshd_config> vi /etc/ssh/sshd_config.**
3. Check for the entry in the file:

   ```
   # override default of no subsystems
   Subsystem sftp /usr/libexec/openssh/sftp-server
   ```

4. If this entry does not exist, add the two lines mentioned in Step 3 at the bottom of the file and **Save** it.
5. Restart service from **SSH > service sshd restart**.
6. Retry the SFTP connection now.
7. Make sure SFTP port is not blocked by SA server appliance firewall. Update iptables rules to allow sftp port.

Meta Values in Investigation Link Issue

Issue	When the device information on the datasource is changed, the Investigation link for the meta values of the executed reports is not displayed on the NWDB results page.
Resolution	Remove and re-add the datasource to Reporting Engine. *Note: This workaround is not applicable for reports that are already generated.*

Internet Explorer 10 Browser Issue

Issue	When you click the Test Rule multiple times in quick succession, results with large input data may not displayed in Internet Explorer 10.
Resolution	If this issue occurs, try one of the following steps: • Close the Test Rule window on Internet Explorer 10 and run the test again. • Use other browsers like Chrome or Mozilla Firefox to test the rule execution.

Dynamic List Editing Issue

Issue	A dynamic list cannot be added from the Edit option on the 'View All Schedules' page to an existing schedule.
Resolution	1. Reports > Select the report > 2. Click the #Schedules for the specific report 3. Select the schedule to be modified from the Report Schedule page 4. Edit the schedule

Deployment Failure Issue

Issue	Deployment of reports fail, if the dependencies of certain compliance reports in Live are not deployed prior to the reports.
Resolution	Retry the deployment. If the problem persists, try to deploy the rule or list dependencies first and then deploy the reports.

Respond Server Issue

Issue	When the Forward Alerts to Respond option is enabled and RabbitMQ connections to the Respond Server are blocked, some of the Reporting Engine threads may be blocked.
Resolution	Disable the Forward Alerts to Respond option until the RabbitMQ broker in the NetWitness Suite server at the Respond has begun and accepts the connections.

Post-Upgrade Issue

Issue	Post-upgrade from 10.6.x to 11.1, Categories meta for incident collection is not supported.
Resolution	When using the Categories meta for incident collection, the results rendered are in an incorrect format. Hence this meta is not supported and you cannot use the categories meta in either select clause or where clause. Also, it is not available in the list of metas for selection in the Rule Builder page.

Appendix

This section provides detailed information about the supported aggregate functions, rule syntax, advanced rules query syntax in Reporting and task scheduler for Warehouse Reporting.

Rule Syntax

This section describes the different rule syntax supported in the Reporting Engine.

NWDB Rule Syntax

The NWDB rule is one of the rule syntax supported in the Reporting Engine. To enhance the execution time of your reporting entities, see "Reporting Guidelines" section in Reporting Overview.

A Rule is a function that manipulates the result set of a rule in order to make the output in a report more meaningful or add additional functionality to a rule other than querying data and displaying it. Any combination of these rule actions can be used to create unique and interesting representations of the information collected by NetWitness Suite.

The Reporting Engine supports the following categories of NWDB data source rule syntax:

- **select** clause
  - Non-Aggregate Rule
  - Aggregate Rule
- **alias**
- **where** clause
- **where** clause Operators
- **then** clause
- **Limit** field
- Rule Actions
- Rule Operators

Select Clause

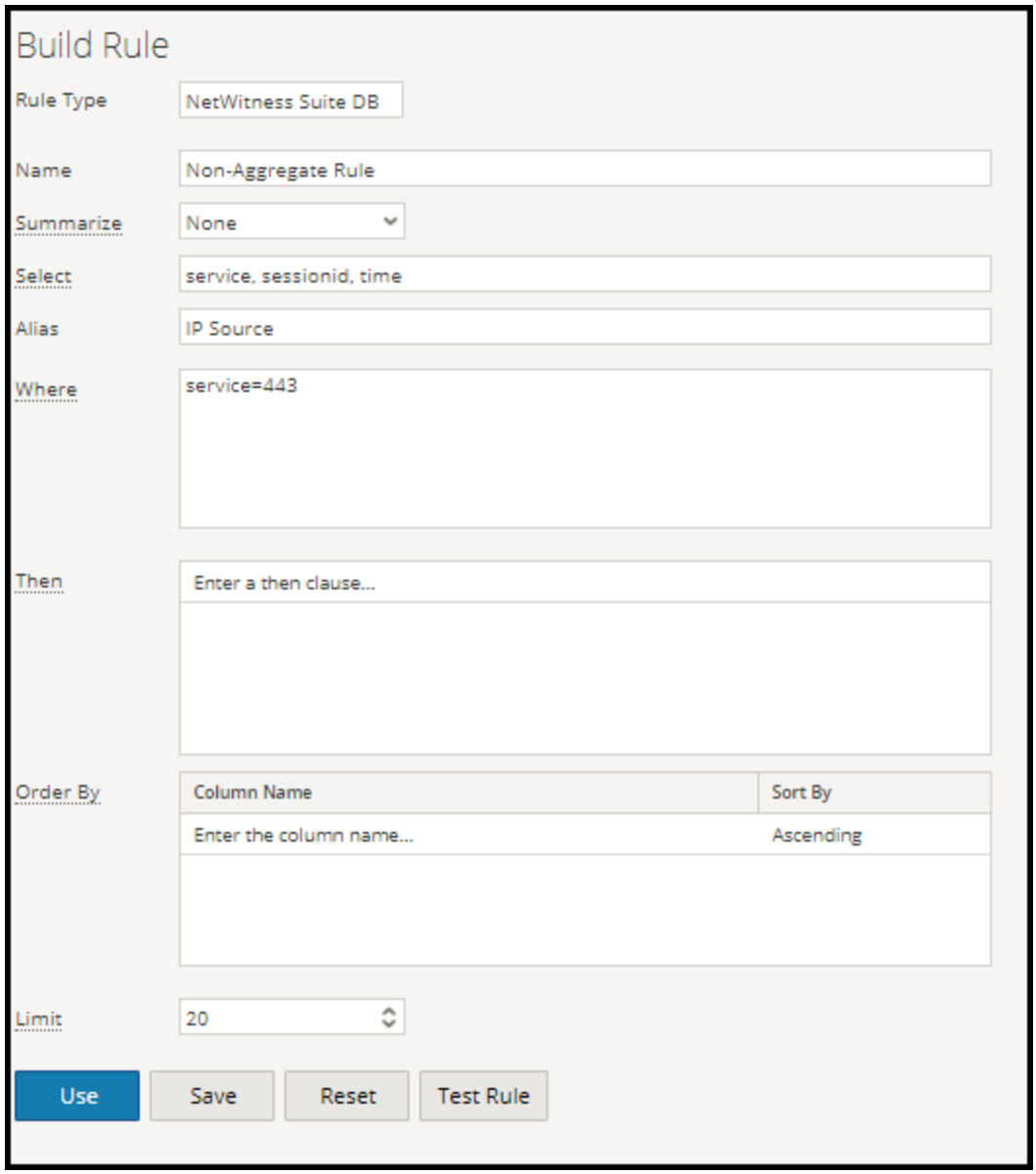
The select clause is a comma separated list of values. For example: select sessionid,time,service.

There are two types of select clause for NWDB Rule:

- Non-aggregate rule
- Aggregate rule

Non-Aggregate Rule

When you want to define a rule without any grouping, choose 'None' in the Summarize field. In a non-aggregate rule, you can select any number of metas in the *Select* clause. For example, select service, sessionid, time.

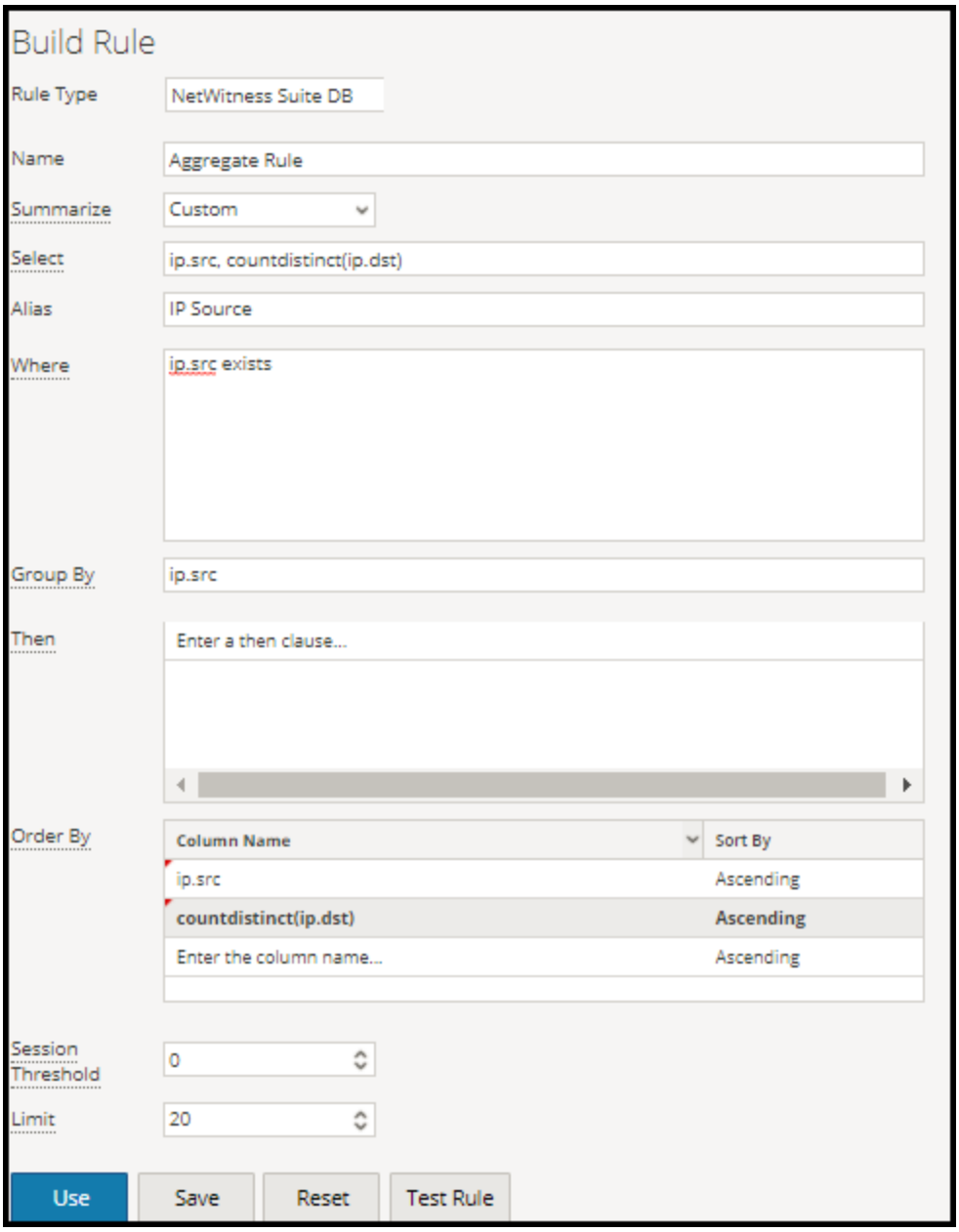


Aggregate Rule

When you want to query for a specific meta and its associated aggregate value then you must use the Aggregate rule. To get an aggregate, you must choose either of the three metas (Event Count, Packet Count, Session Size) or choose 'Custom' in the **Summarize** field to include an aggregate function in the *Select* clause. For example, select ip.src, sum (ip.dst). When Custom aggregate rule is enabled, the following fields are populated in the user interface:

- Group By
- Order By
- Session Threshold

The following figure shows the Build Rule view for Aggregate Rule.



There are two types of aggregate values that can be queried:

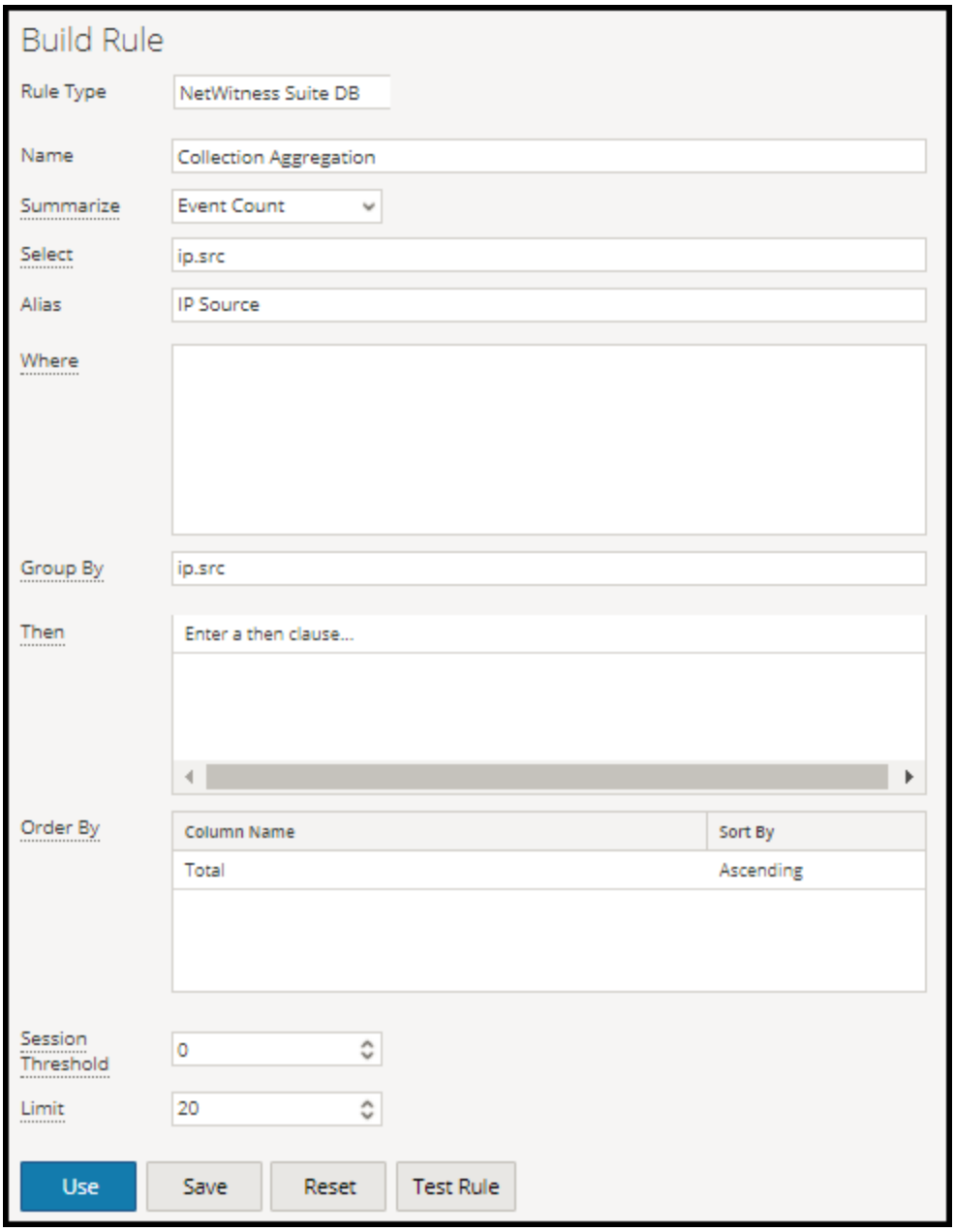
- Collection aggregation
- Meta aggregation

Collection Aggregation

With collection aggregation, you can get aggregates related to Event, Session or Packets. The following values can be queried in a collection aggregation:

- **Event Count**: The total count of events.
- **Packet Count**: The total count of packets.
- **Session Size**: The total session size.

These options are listed in 'Summarize' field and any one of them can be selected in a rule.
For example, choose any of the Collection aggregates (Event Count or Packet Count or Session Size) in the 'Summarize' field and select ip.src.



Meta aggregation

With meta aggregation, you can get aggregates of meta values. The following are the supported meta aggregate functions:

- sum(meta)
- count(meta)
- countdistinct(meta)
- min(meta)
- max(meta)
- avg(meta)
- first(meta)
- last(meta)
- len(meta)
- distinct(meta)

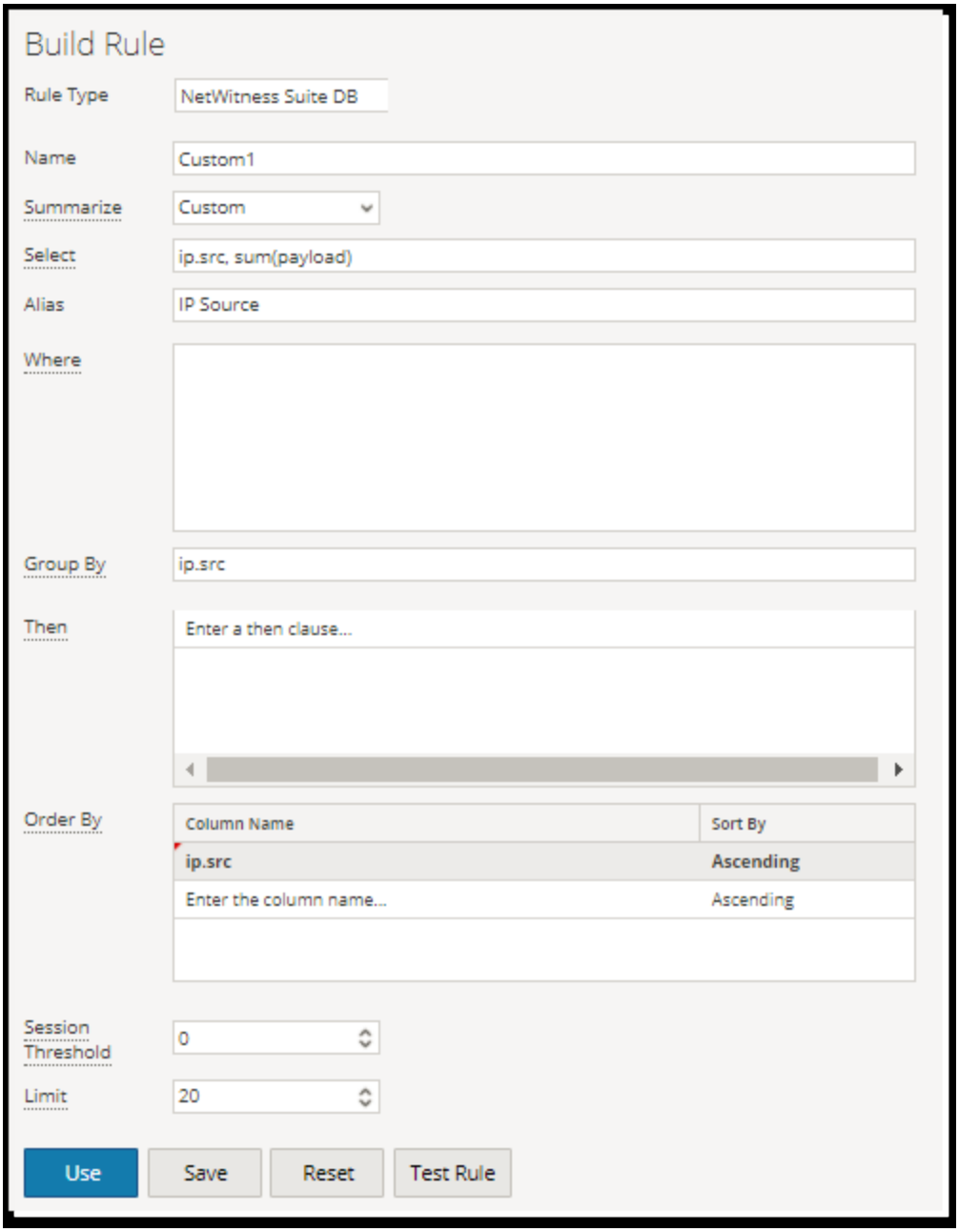
Supported Meta Aggregate Functions

The NWDB service supports the following meta aggregate functions and syntax in this release.

Syntax	Function
sum (<meta>)	The sum of all meta values. For example, if you provide the field sum(payload) in the select clause, the resultset is the sum of payload size. **Note:** The meta field chosen for the sum aggregate function must be of numeric data type.
count (<meta>)	The total number of meta fields that would be returned. For example, if you provide the field count(ip.dst) in the select clause, the resultset is the number of times an ip.dst value is returned.
countdistinct (<meta>)	The total number of distinct meta fields that would be returned. For example, if you provide the field countdistinct (ip.dst) in the select clause, the resultset is the number of times a distinct ip.dst value is returned.

Syntax	Function
min (<meta>)	The minimum of all meta values. For example, if you provide the field min(payload) in the select clause, the resultset is the min of payload size.
max (<meta>)	The maximum of all meta values. For example, if you provide the field max(payload) in the select clause, the resultset is the max of payload size.
avg(<meta>)	The average of all meta values. For example, if you provide the field avg(payload) in the select clause, the resultset is the avg of payload size. **Note:** The meta field chosen for the avg aggregate function must be of numeric data type.
first (<meta>)	The first occurrence of the meta value. For example, if you provide the field first(ip.src) in the select clause, the resultset is the first occurrence of ip.src for that group.
last(<meta>)	The last occurrence of the meta value. For example, if you provide the field last(ip.src) in the select clause, the resultset is the last occurrence of ip.src for that group.
len(<meta>)	Converts all field values to a UInt32 length instead of returning the actual value. This length is the number of bytes to store the actual value, not the length of the structure stored in the meta database. For instance, the meta value "NetWitness" returns a length of 10. All IPv4 fields, like ip.src, returns 4 bytes.
distinct (<meta>)	The distinct values of the meta. For example, if you provide the field distinct(ip.src) in the select clause, the resultset is all the distinct ip.src for that group.

You must select 'Custom' in 'Summarize' field and provide the meta and the meta aggregate functions in the select clause.



Note: Meta aggregate functions cannot be used in a WHERE clause and the rule actions like min_threshold/max_threshold can be used to filter aggregate functions. It is advised to use a more refined WHERE clause to get a better rule performance while using 'group by'.

Aggregate Query for Multiple Meta

To execute aggregate query for multiple Meta, follow these steps:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is highlighted and the **Rules** view is displayed.

2. In the Rule toolbar, click + > **NetWitnessDB**.

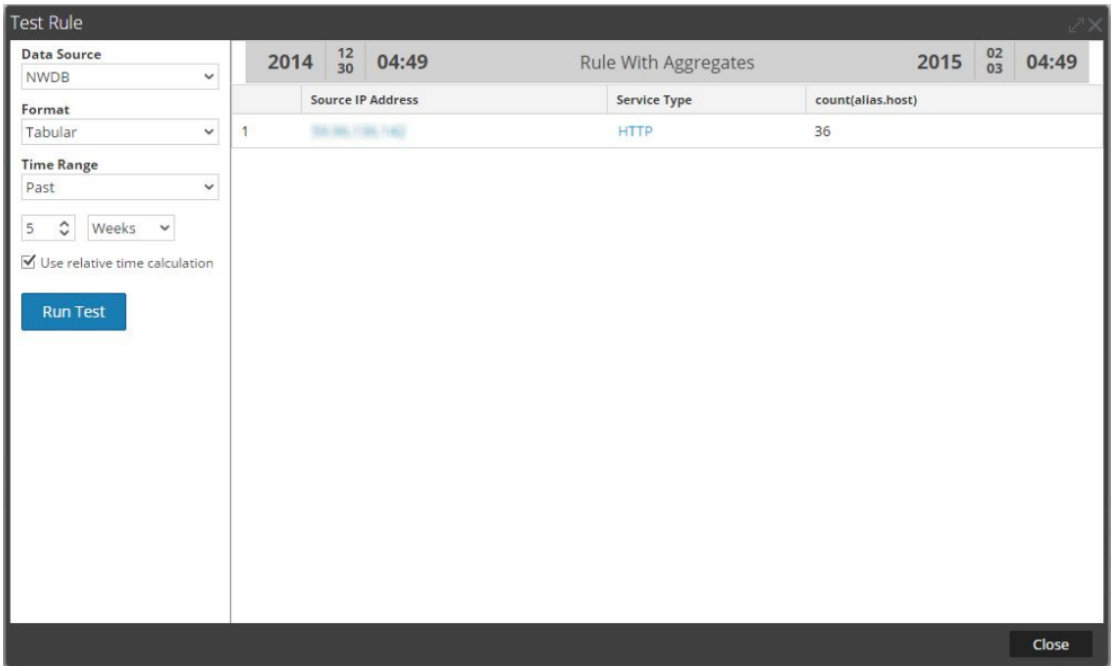
   For example, enter the following meta in the fields highlighted below:

   SELECT: ip.src, service, count(alias.host)
   ALIAS: Source IP Address, Service Type, count(alias.host)
   WHERE: ip.src = 59.96.136.142

   Note: In the alias field you can enter a name for columns used in the select clause. If you do not specify the alias for one of the field in the select clause, then the default description will be used. For example, if the select clause has Field1, Field2, Field3, Field4, and alias has only Field1, Field3, Field4, then for Field2 a default description is used.

3. Click the **Test Rule** button at the bottom of the screen.

   The Test Rule page is displayed.



Summarize

Summarize determines the type of summarization or aggregation for the rule.

Name	Config Value
Summarize	To query metas without any custom grouping, select: • **None**: The data is grouped by session in this case. To get collection (sessions/events/packets) related aggregates, select either of the following: • **EventCount**: The total count of events. • **Packet Count**: The total count of packets. • **Session size**: The total session size. To get meta based aggregates, select: • **Custom**: This indicates that expected meta aggregate function is defined in rule select clause.

Order By

Order By determines how to sort the result set.

Name	Configuration Value
Column Name	The **Column Name** is the name of the columns by which you want to sort the results. By default, the value is empty. When you click on a column, the value gets populated based on the Summarize field. • For 'None' and 'Custom', the value gets populated based on the entries made in the Select field. You can select from this list or add custom name. • For Event Count, Packet Count and Session size, accepted values are Total and Value. • Total - sort by aggregate value • Value - sort by group by meta

Name	Configuration Value
Sort By	**Sort By** determines the order in which you want to sort the results. The following are the values: • Ascending Order • Descending Order

Session Threshold

The session threshold is the optimization setting to stop scanning the matching sessions for each possible
unique value for the selected meta. The threshold is an integer between 0 (default) and 2147483647. The threshold 0 scans for all matching sessions.

Note: If you provide a non-zero value (a value higher than zero), the aggregate results are inaccurate. This can be used only when you are interested in unique values and not aggregate values.

Supported where Clause

Syntax	Description
where <field1> [<field-operator>] < value1>,<value2>,<value3-value4> <logic-operator> <field2>,and so on	The where clause is a comma separated list of language field values and ranges that is used by NwValues function. In the where clause, string values have to be enclosed within single quotes. For example, where username = 'admin' && service = 22.
where <field1> [<field-operator>] <List1>	You can use a list in the where clause if you have multiple values to report on. For example, where ip.src exists && alias.host exists && alias.host contains $[User Reports/List of Alias Host]. When you use the list you must specify in the format $[<path>/<List name>].

In the where clause, make sure the syntax is correct based on the meta type.
For example,
For all text meta type use quotes for example, username = ‘user1’.
For all IP Addresses, Ethernet Addresses, and Numeric meta types do not use quotes for example, service = 80 && ip.src = 192.168.1.1.
For date and time meta types, if the date and time format is 'YYYY-MM-DD HH:MM:SS‘, use quotes.
If the date and time format is 1448034064 (number of seconds since EPOCH (Jan 1, 1970)), do no use quotes.

Note: If list is used in the rule, make sure that the list values are quoted or unquoted based on the type of the meta used. Checking the **Quotes will be inserted for all the values** checkbox in list definition page (for more information see, "Create Lists or List Groups" section in Configure a Rule) would quote all the list values.

Supported where Clause Operators

Syntax	Description
=	Returns results where the field is equal to any provided value. For example, tcp.dstport = 21-25,110 returns session with TCP destination ports of 21, 22, 23, 24, 25, or 110.
!=	Returns results for fields that do not match the values specified. For example, eth.type !=0x0800 returns sessions outside of hex value (decimal value of 2048) that is all non-IP based protocols.
begins	Checks for a value at the beginning of a text or binary field.
contains	Searches a text or binary value for a partial match.
ends	Checks for a value at the end of a text or binary field.
exists	If the field value exists, regardless of value, the operation evaluates to true.
!exists	If the field value does not exist, the operation evaluates to true.
length	Evaluates the length of the field. For example, username length 20-u returns any username that is 20 or more characters long.

Syntax	Description
regex	Performs a regular expression search against text or binary values.
not	Not operator is used to negate a clause or condition. For example, (not(user.dst ends "$")) will not display values for user destination.

Supported then Clause

Syntax	Description
then <rule action>	The then clause contains a rule action that manipulates the original result set of a rule in order to make the output in a report more concrete or add additional functionality other than querying data and displaying it. For example, dedup (filename).

Limit field

This indicates the limit to be put on the query while fetching data from the database. If a result set is sorted by event
count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not
sorted, the first N values are returned.

Rule Actions

The NWDB data source rule syntax supports the following rule actions:

- dedup
- filter_on
- filter_out
- lookup_and_add
- max_threshold
- min_threshold
- regex

- sum_count
- sum_values
- show_whats_new

dedup (string field)

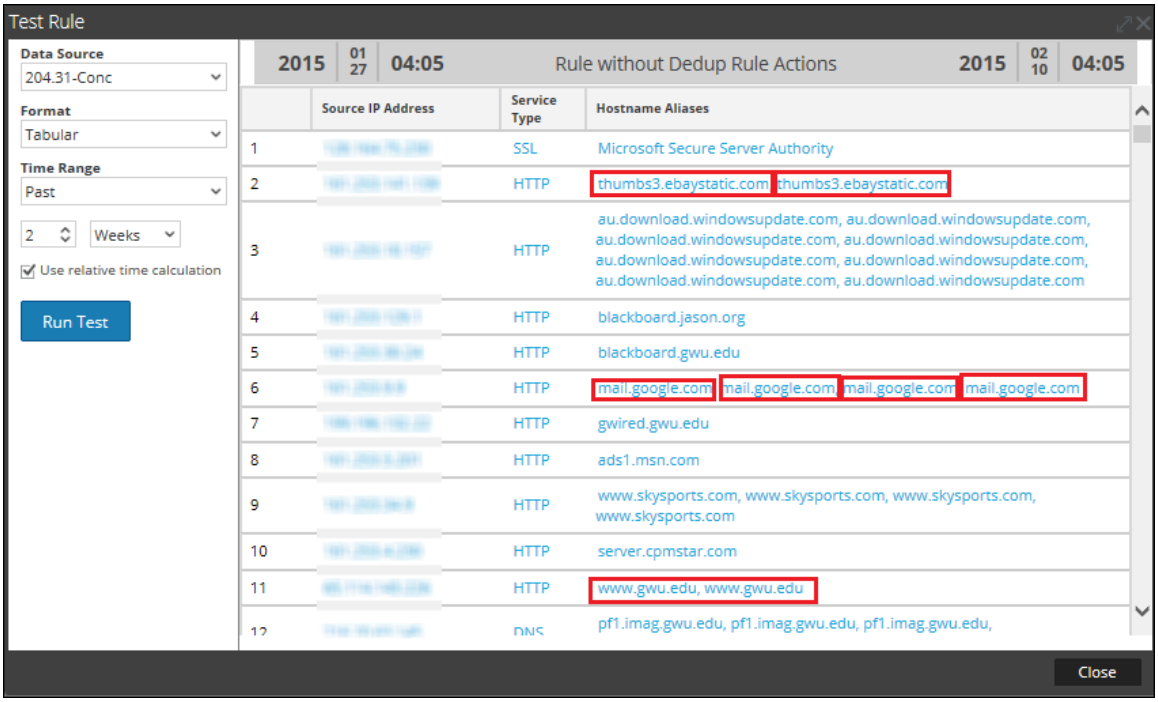
dedup removes the duplicate entries in an unsorted result set and displays only pertinent data. The dedup rule action removes duplicate entries of a specific field in the report, so that only the first occurrence of that value is listed in the report.

Note: The dedup rule action cannot be used with an aggregate rule.

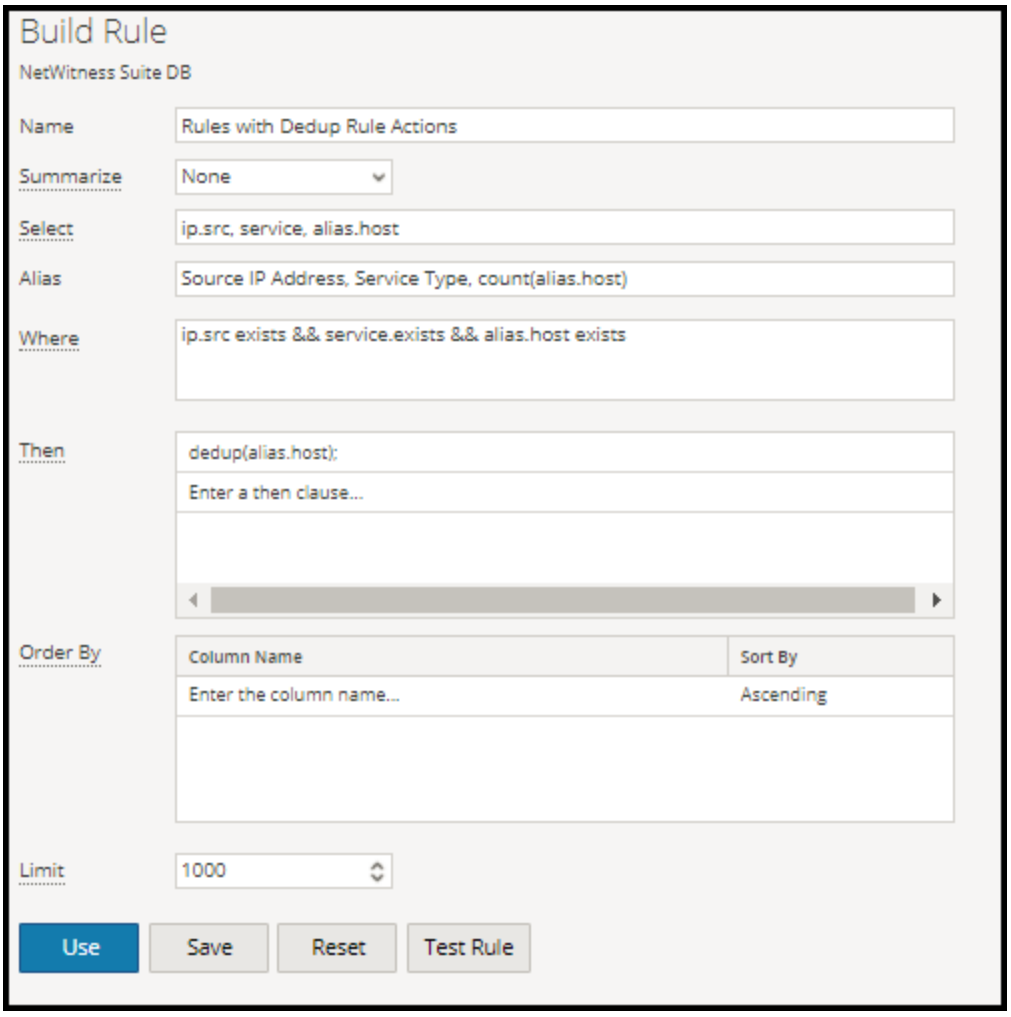
For example, the meta data generated by an individual session is often repetitive, especially when you have sessions with a lot of DNS lookups or web sessions that access the same host multiple times for various resources (such as, javascript, css). To remove the duplicate entries of the host, you can use the dedup rule action.

Example:

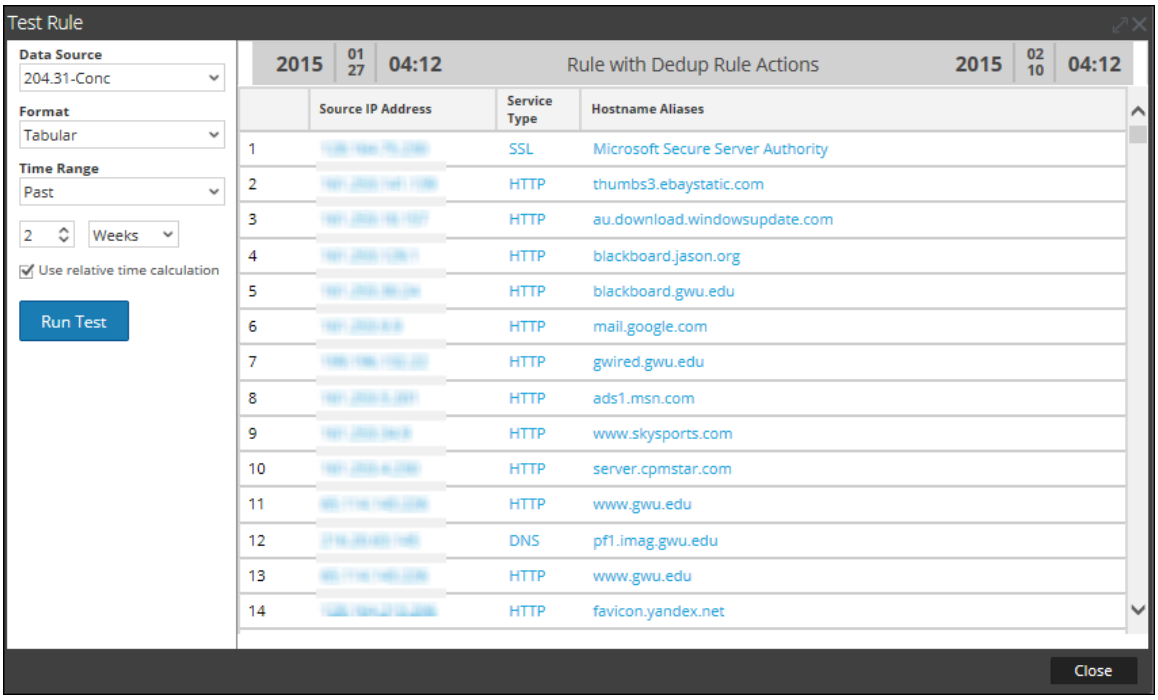
The following example is a lengthy result set that can be trimmed by removing the duplicate values in the same session.



The following figure shows the use of dedup rule action to remove the duplicate entries from the result set.



The duplicate value for each entry in the rule result set is reduced to one value.



filter_on (string filter, string field, bool matchExact)

`filter_on` removes values that do not contain the `filter` criteria from the result set. If the result set contains multiple fields, you must select a specific field to which the filter is applied. To add additional results to a single result set, include function such as lookup_and_add.

The matchExact parameter determines if the match is an exact match or contains a match.

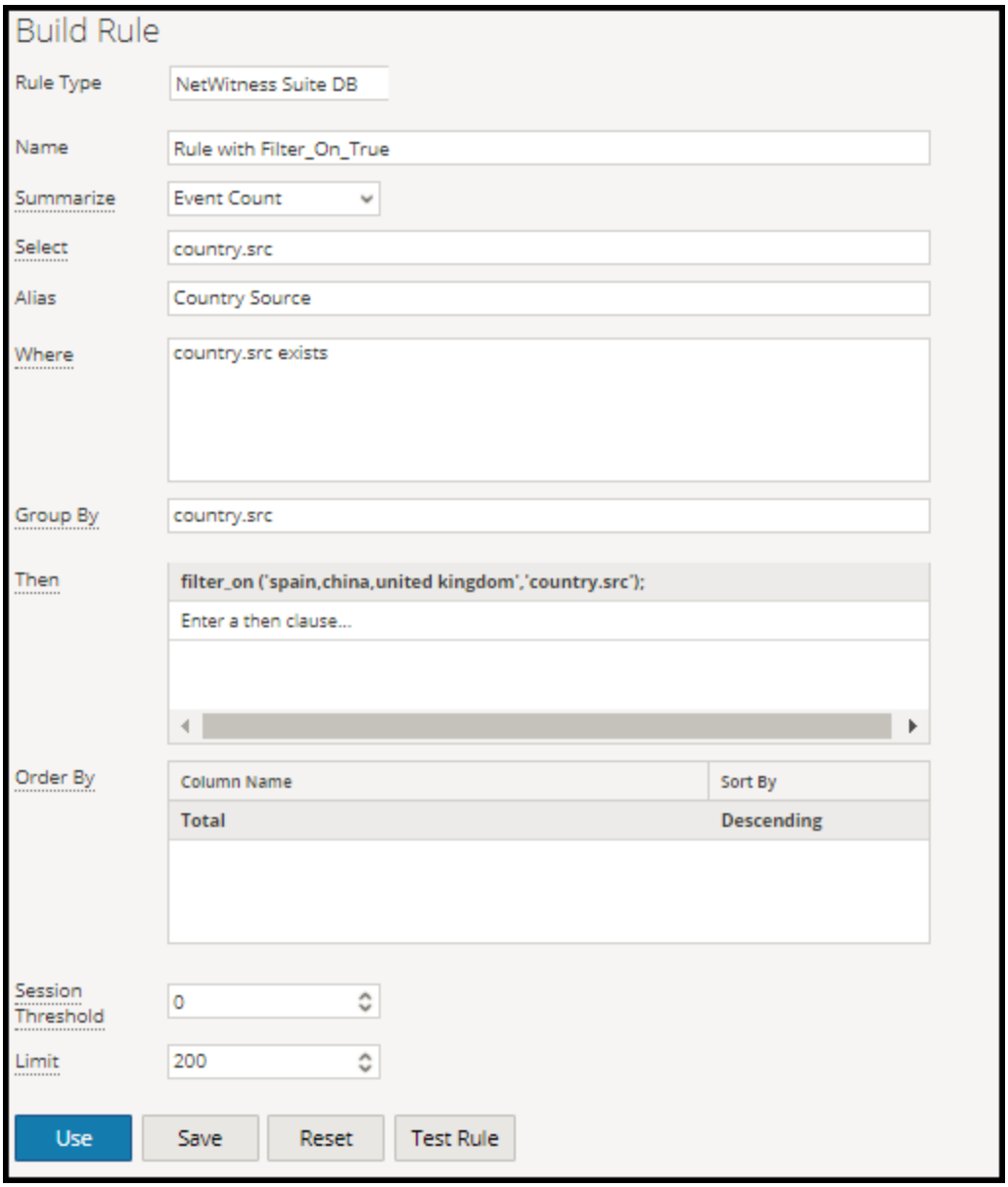
- If matchExact is set to `false`, any value that contains the filter text is considered a match.
- If matchExact is set to `true`, only values that match the provided filter text is included in the result set.

Note: Unless the matchExact parameter is specified, the default behavior of the rule action is to match exactly the text specified in the filter parameter. To specify that results containing the filter text must be kept in the result set, users must set the matchExact parameter to false.

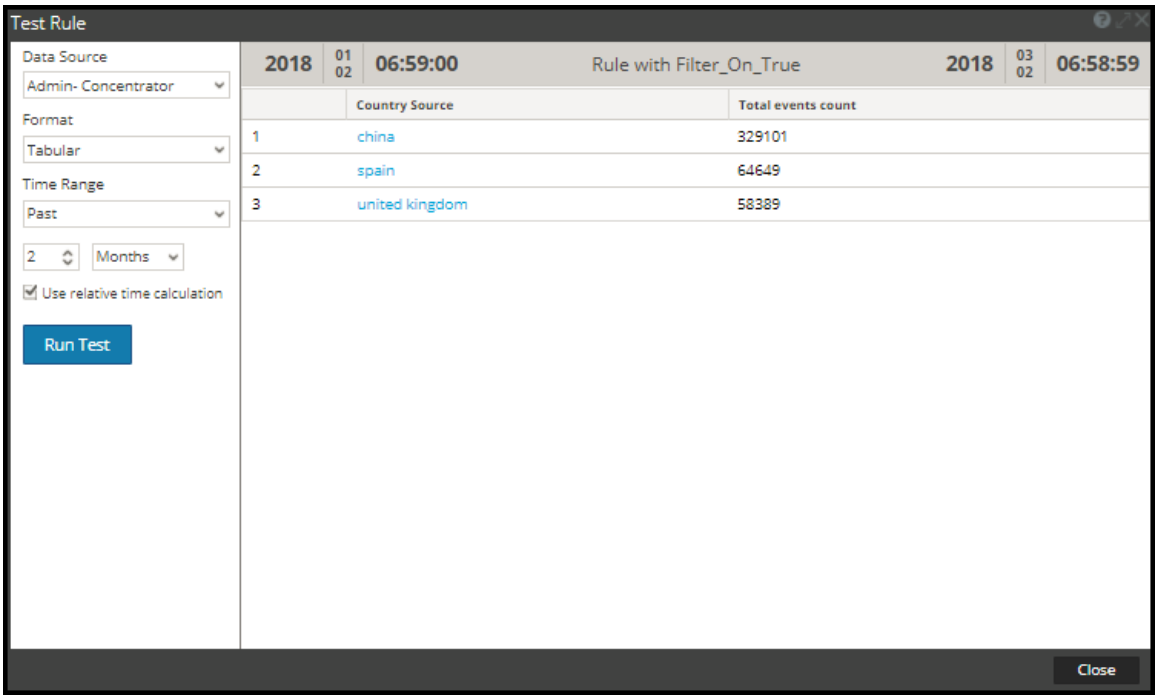
Example:

The following figure displays the list of countries and their event count.

The following figure shows a filter_on rule action to filter out countries except Spain, China, United States and United Kingdom from the result set.



The following figure shows the output with the filter_on rule action.



Another way of filtering out the entries from the result set is to create a list of variables which you want to filter out. For example, you can create a list with United Kingdom, France and Germany as values in the list. You can use this list in the rule action to get the same result set. For example, if you create a list called COUNTRY_LIST, you can use the list as follows:

```
filter_on ('$COUNTRY_LIST', 'country.src', 'false');
```

```
filter_out (string filter, string field)
```

```
filter_out (string filter, string field, bool matchExact)
```

filter_out removes the values that contain the *filter* criteria from the result set. If the result set contains multiple fields, you must select a specific field to which the filter is applied (for example, you can use a lookup_and_add to add results to a single result set).

The matchExact parameter determines if the match is an exact match or contains a match.

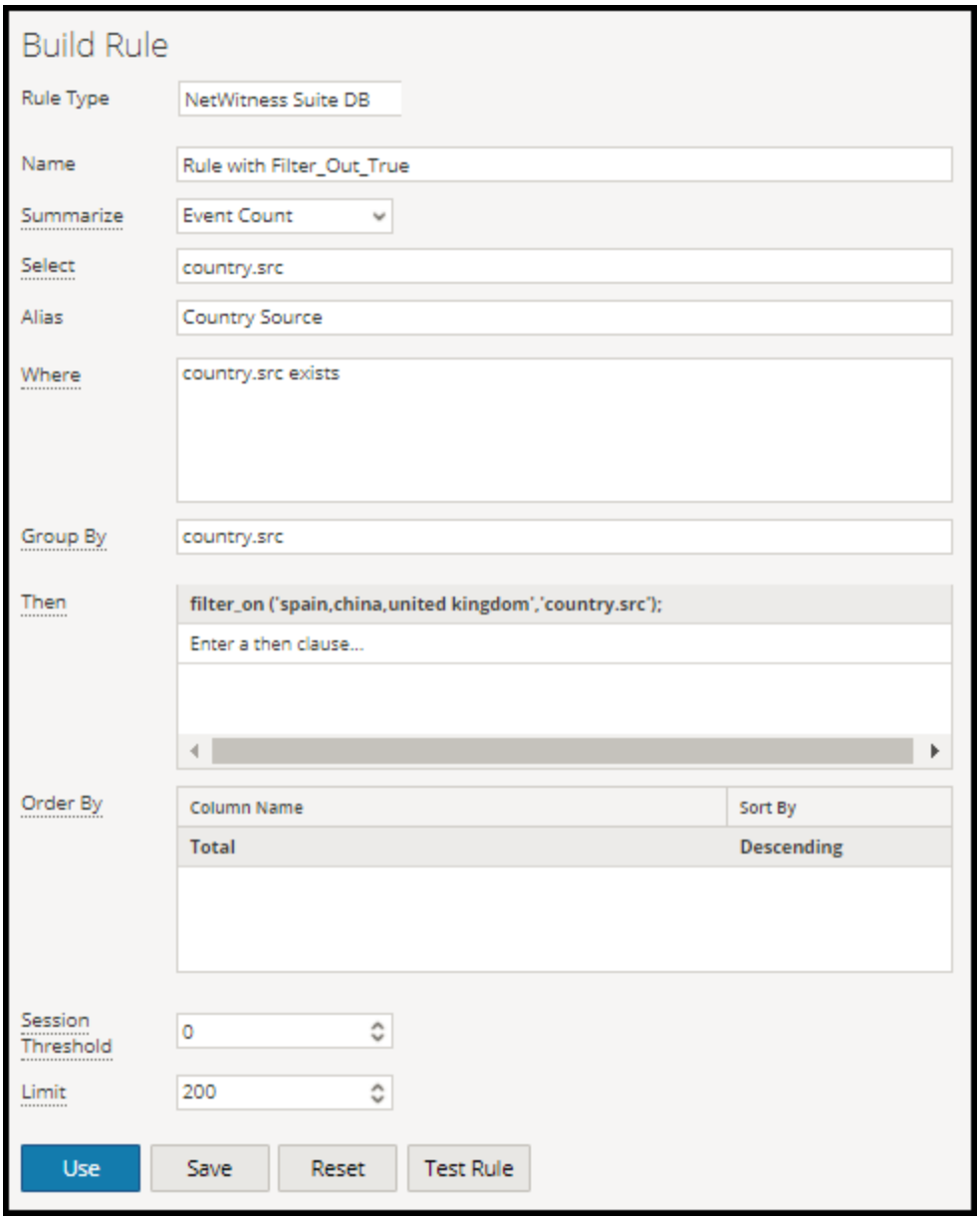
- If matchExact is set to false, any value that contains the filter text is considered a match.
- If matchExact is set to true, only values that match the provided filter text is excluded from the result set.

Note: Unless the `matchExact` parameter is specified, the default behavior of the rule action is to match exactly the text specified in the filter parameter. To specify that results containing the filter text must be removed from the result set, users must set the `matchExact` parameter to false.

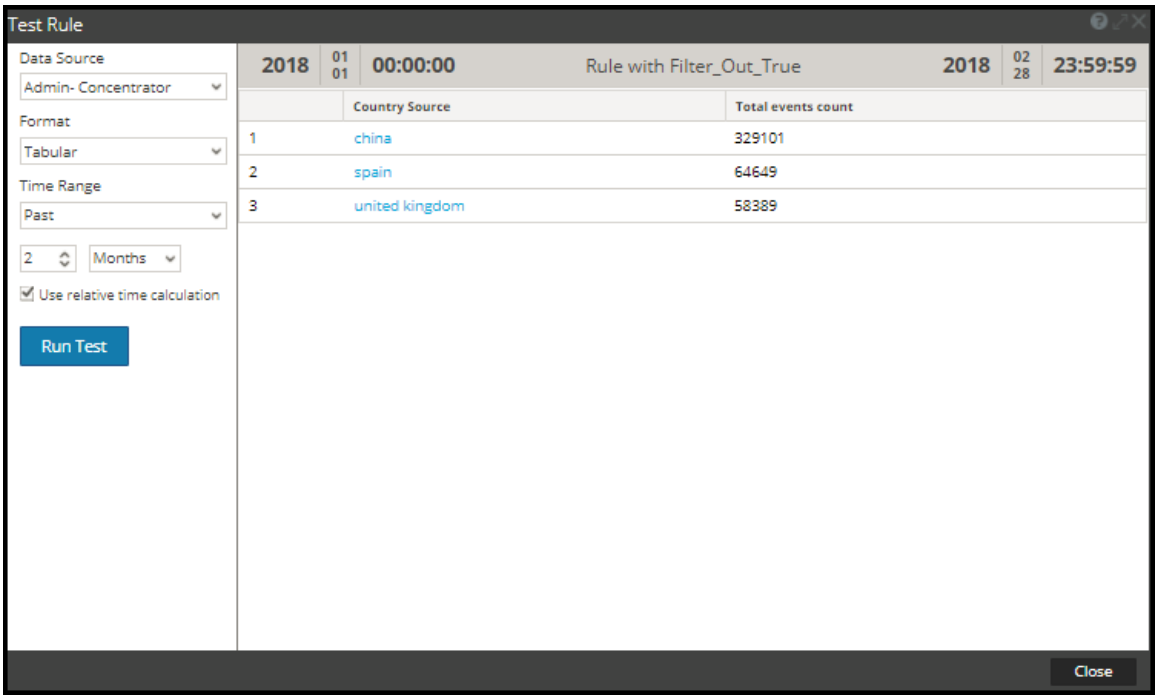
Example:

The following figure displays the list of countries and their event count.

The following figure shows the filter_out rule action to remove the event count for Spain, China, United States and United Kingdom from the result set.



The following figure shows the output with the filter_out rule action.




```
lookup_and_add (string select, string field)

lookup_and_add (string select, string field, int limit)

lookup_and_add (string select, string field, int limit,
boolean inherit)

lookup_and_add (string select, string field, int limit,
boolean inherit, string extraWhere)

lookup_and_add(string select, string field, int limit,
boolean inherit, string extraWhere, boolean aggregate)
```

This rule action iterates through a list of values in a result set and lookup additional meta data to further describe the relationships between various elements in a result set.

Note: The lookup_and_add rule action can be used only with an aggregate rule.

The first parameter, select, designates the type of meta data that must be added to elements of the result set. The second parameter, field, specifies where in the result set the append must apply to. Also, a limit can be applied to avoid crowding the result set with a large result set.

By default, subsequent queries to the SDK will inherit the where clause of the parent rule. To use a unique where clause, you can specify a boolean value in the fourth parameter as false and in the fifth parameter you can specify a different where clause.

Note: If you are using a unique where clause in your query, make sure that you use a single quote (') for enclosing arguments and double quotes (") for string values.

Now, with the addition of **Custom** summarization and **Group By** feature, the result can be achieved even without having lookup_and_add rule action. The new rule syntax with groupby displays the result in a flat structure which is better than the earlier rule syntax without groupby Hence it is recommended to manually edit/update rules with lookup_and_add rule action and use groupby clause wherever it is applicable.

Note: Lookup_And_Add rule action is supported only if the SELECT clause has one meta and aggregate function.

For example, see below scenarios: In Example **2a**, lookup_and_add rule action is used. Instead of using lookup_and_add rule action, the same result can be achieved by using **Custom** summarization and **Group By** feature. See Example **2b** below.

But, lookup_and_add rule action is still supported for NWDB rules on the following conditions:

- All versions of NWDB rules with Summarization as Event Count, Packet Count, or Session Size.
- For Custom summarization, the lookup_and_add rule must have only one group by meta with only one aggregate function where the aggregate function must be either sum() or count().

Note: It is not supported for “Summarize-None”.

For example, lookup_and_add rule action can be used for the following rules:

- select ip.src, sum(size) group by ip.src
- select ip.src, count(filename) group by ip.src

It cannot be used for the following rules:

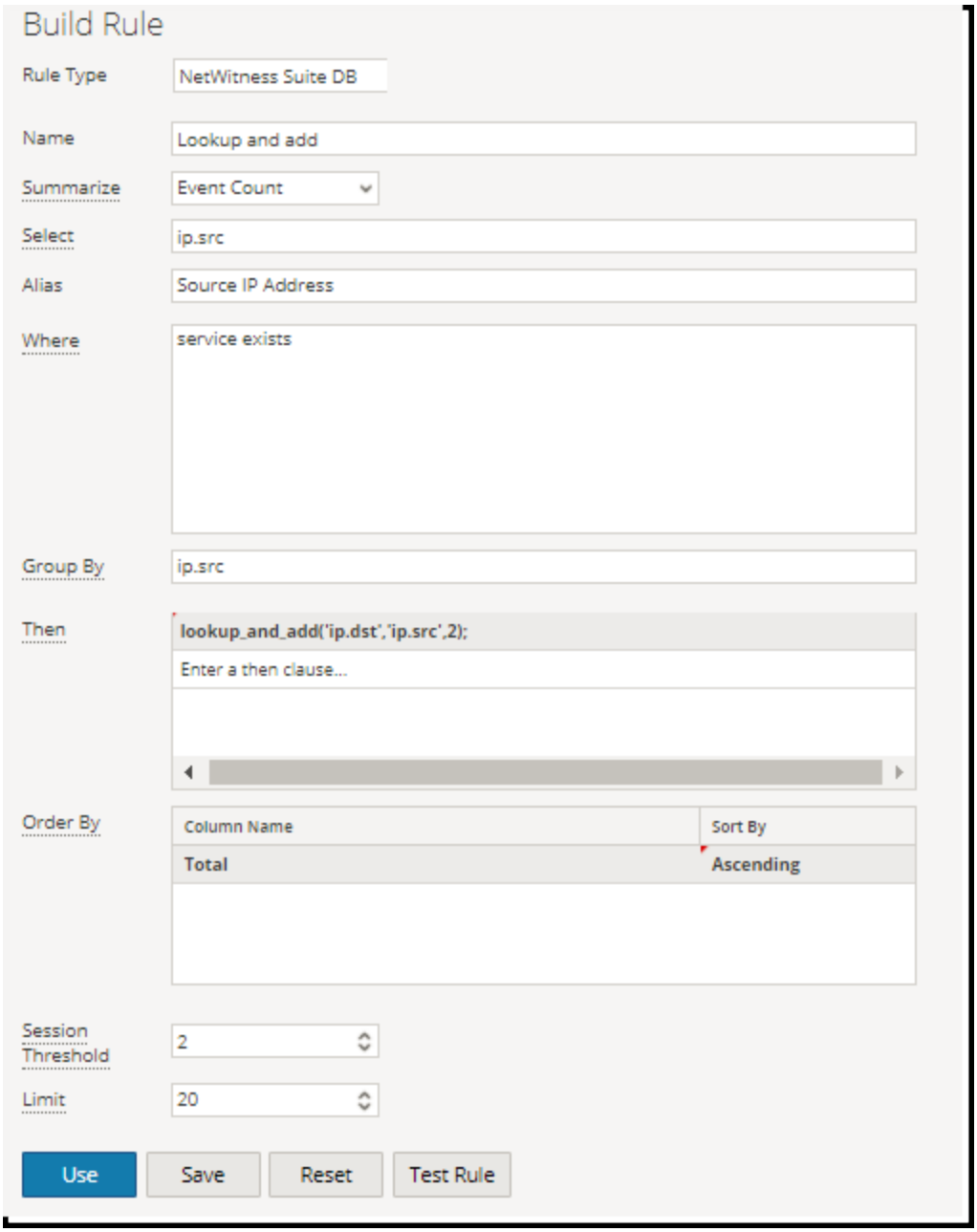
- select ip.src, sum(size),count(filename) group by ip.src
- select ip.src, sum(size),avg(size) group by ip.src
- select ip.src,ip.dst count(filename) group by ip.src,ip.dst

Examples:

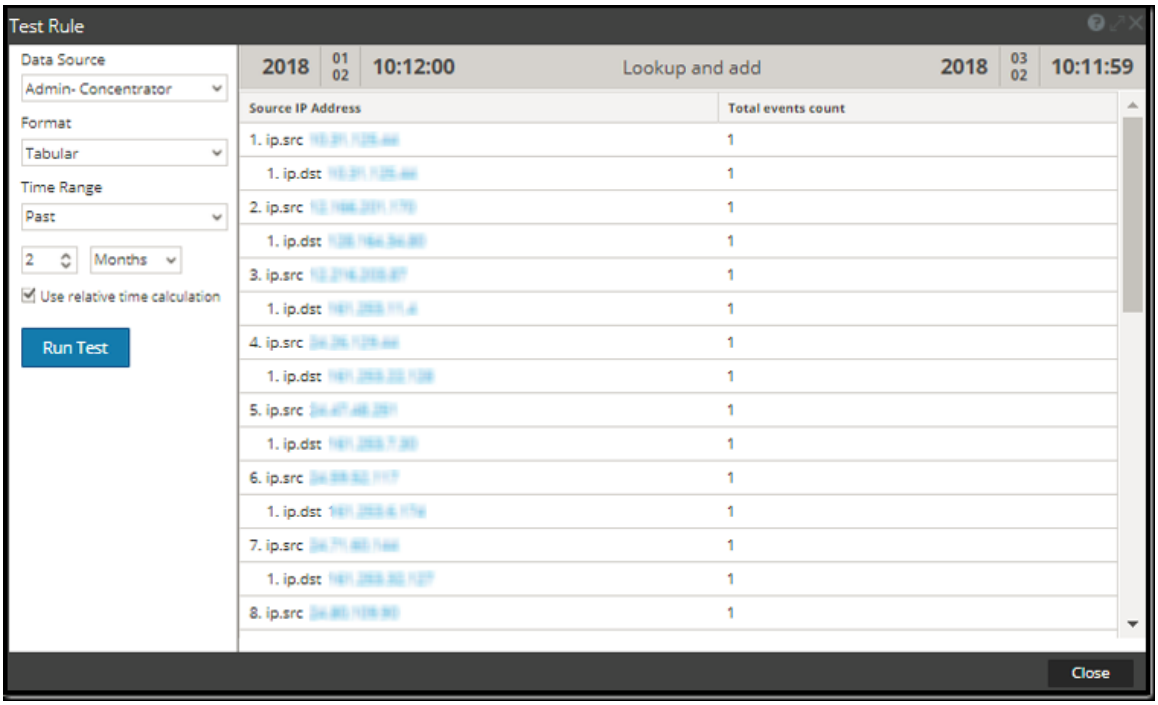
1. lookup_and_add('ip.dst','ip.src', 2);

This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src.

The following figure shows the rule definition.



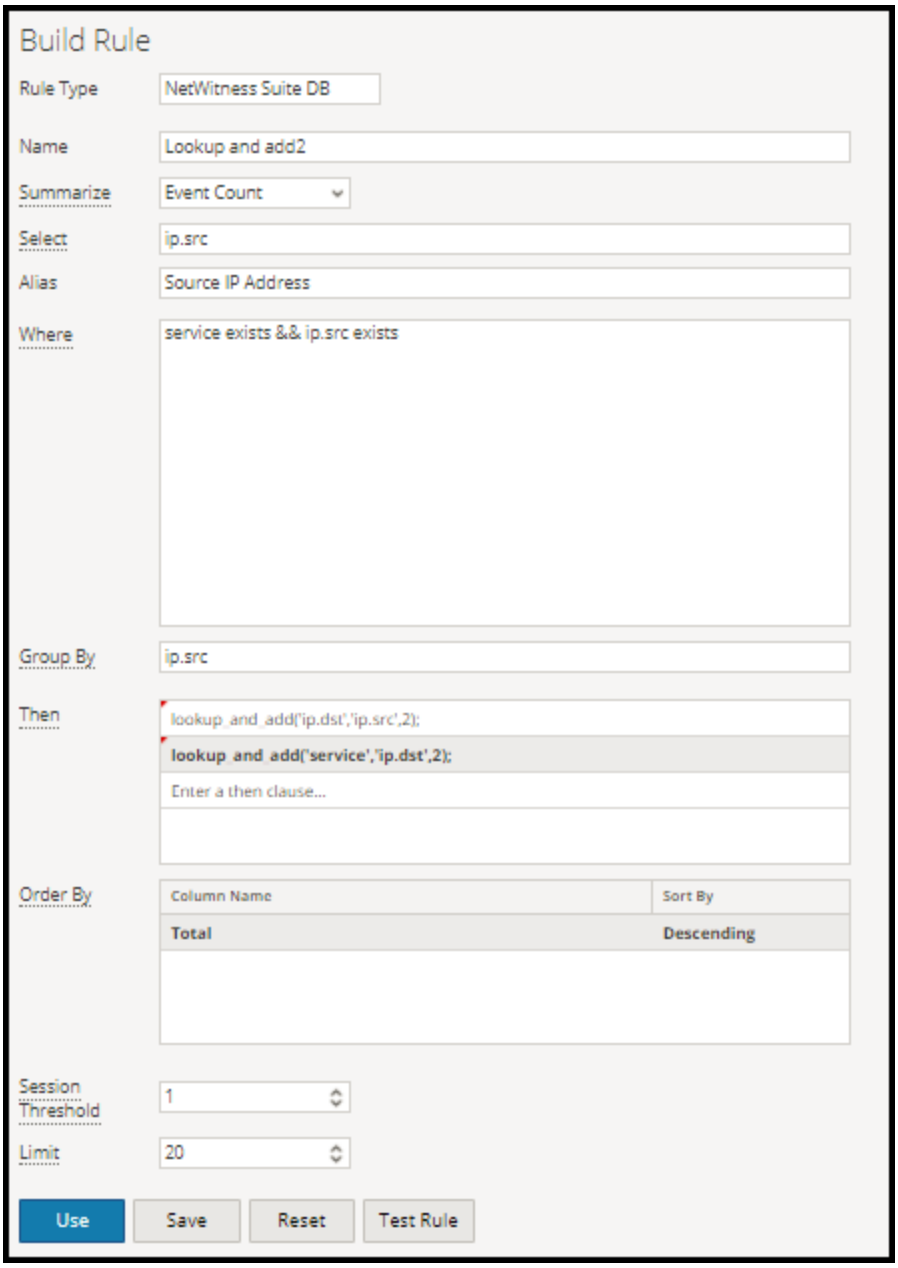
The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src.



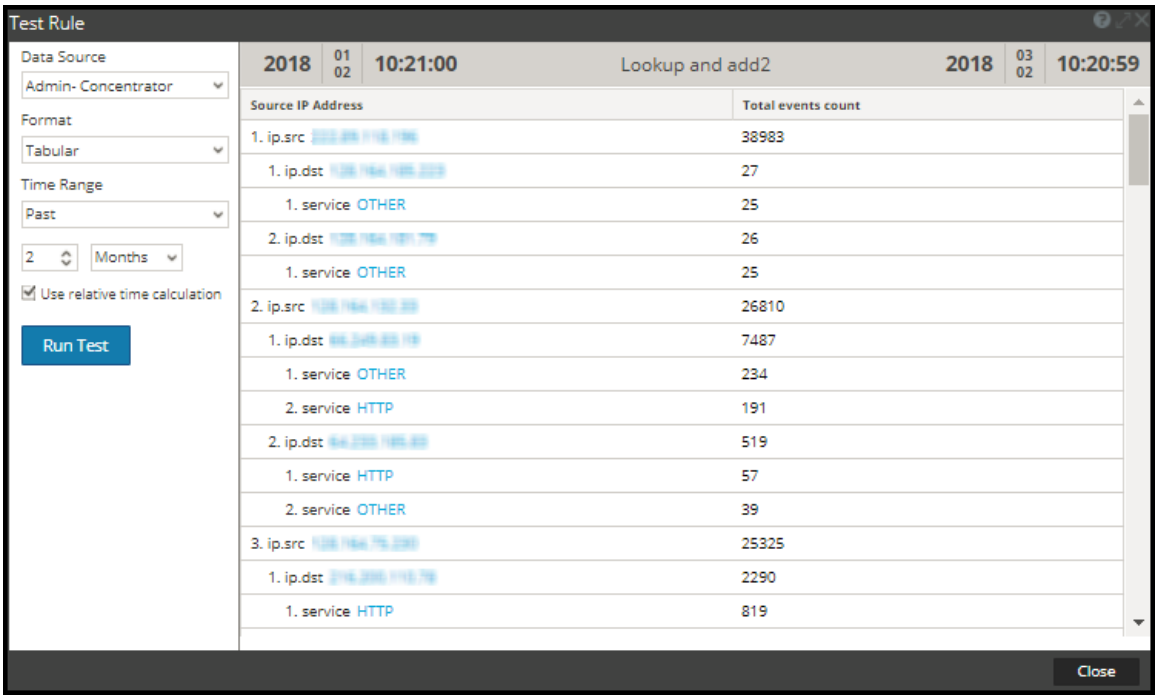
2a. lookup_and_add('ip.dst','ip.src', 2); lookup_and_add('service','ip.src', 3);

This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.

The following figure shows the rule definition.



The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.

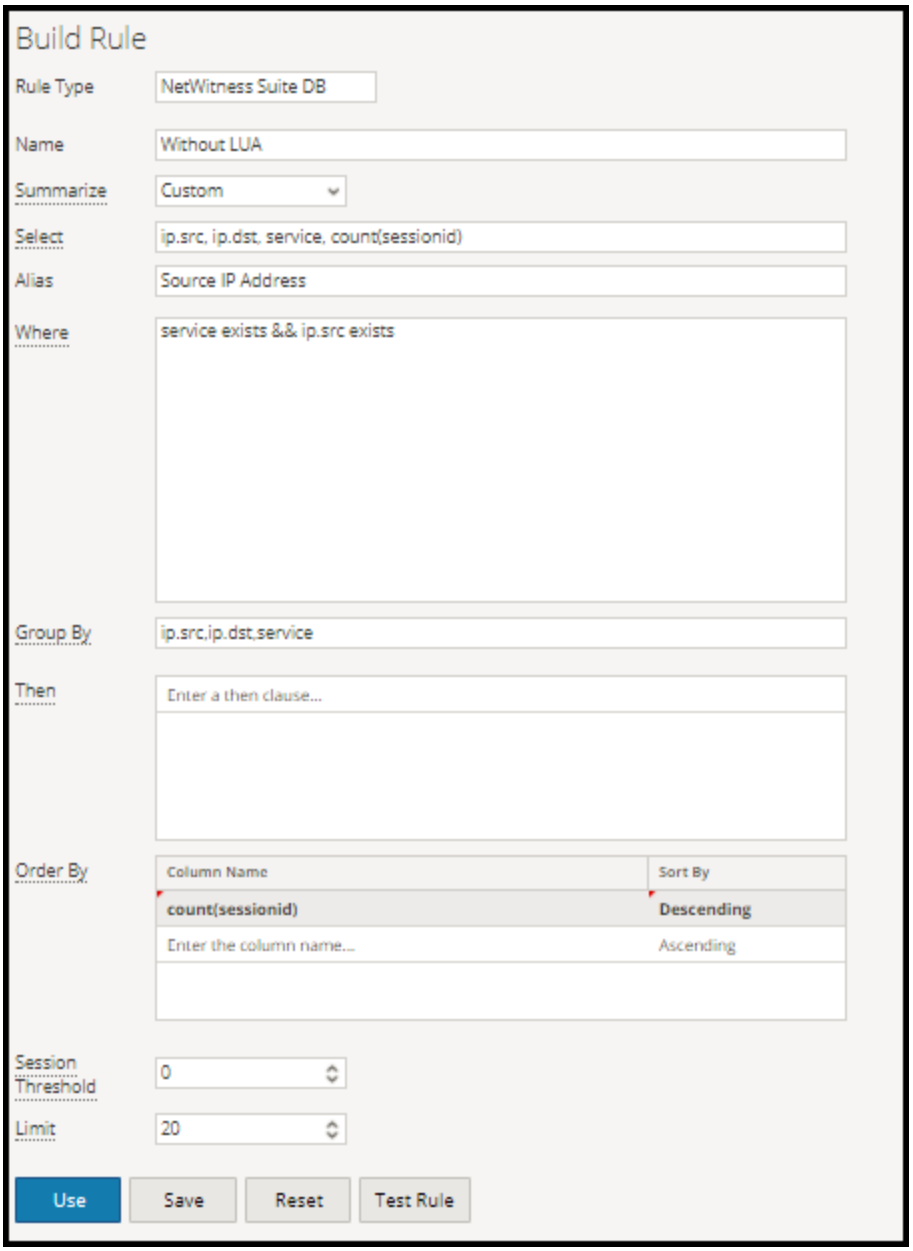


You can make the query as complex as you want by selecting different fields in the result set and by appending to different parts. For example, you may want to know what files each source IP had touched. However, because the parent rule has a WHERE clause of service = 6667 and the default behavior of this rule action is to append to the original WHERE clause, it becomes necessary to override the parent WHERE clause. The easiest way to understand this concept is to look at the previous lookup_and_add call lookup_and_add('ip.dst','ip.src',2). The actual query that is sent to the server is SELECT ip.dst WHERE service = 6667 &&ip.src = 206.42.199.194. In order to force the WHERE clause to override the service = 6667 portion of the WHERE clause (inherited from the parent rule), the user can specify a 4th parameter of false as shown in example 3.

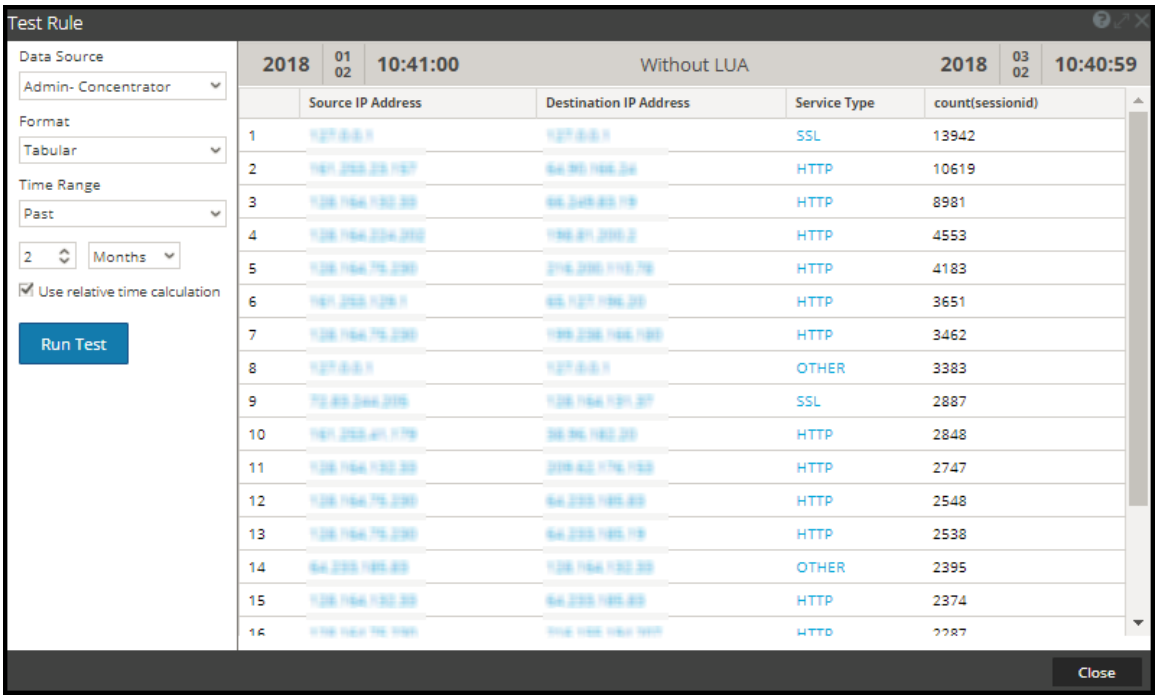
2b. Without Lookup_and_add Rule

This rule uses the Custom summarization and Group By feature to sort the results.

The following figure shows the rule definition.



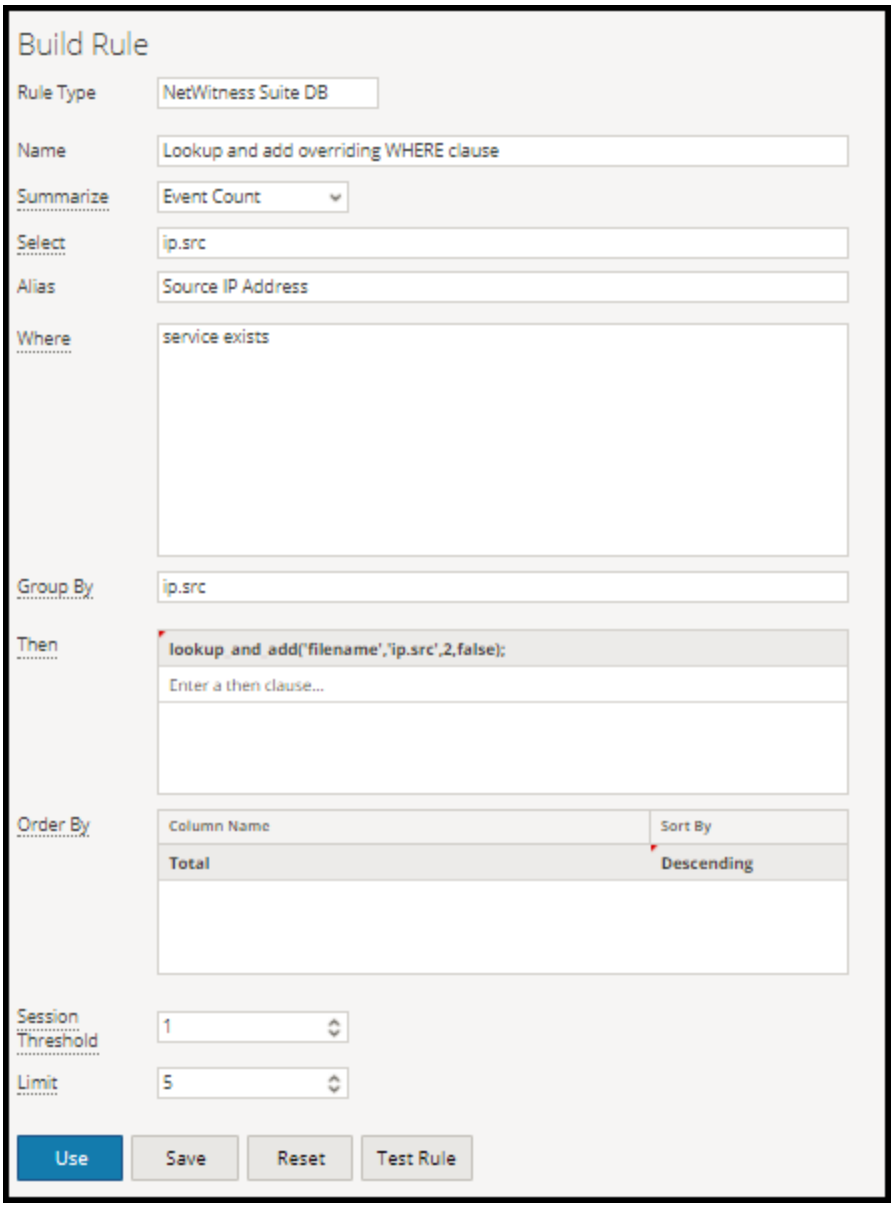
The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.



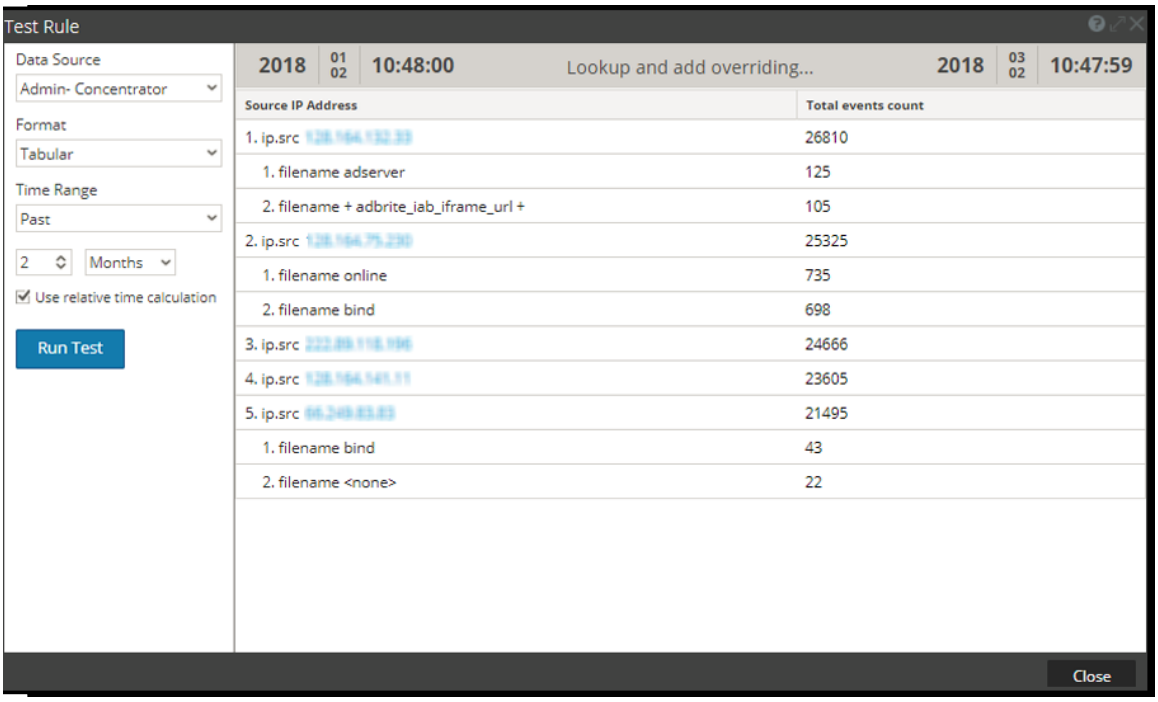
3. lookup_and_add('filename', 'ip.src', 2, false);

This call would issue a query to the server, like `SELECT filename WHERE ip.src = 90.0.0.142` rather than `SELECT filename WHERE service = 6667' && ip.src = 90.0.0.142` because you have specified the rule action to ignore the initial `WHERE` clause of the parent rule.

The following figure shows the rule definition.



The following figure shows the result set.

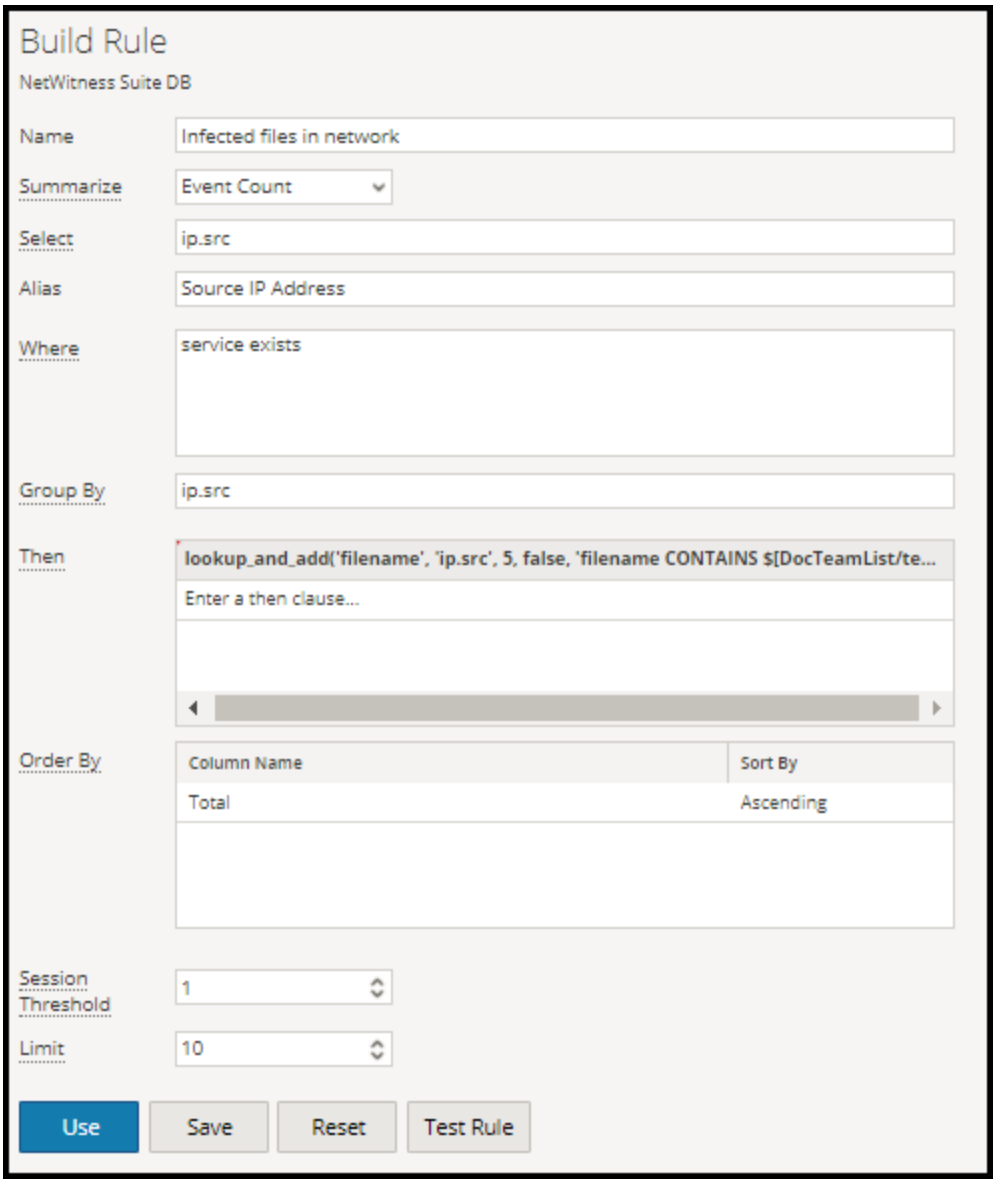


The test list is in a group name netwitness, you can access that list with the following syntax.

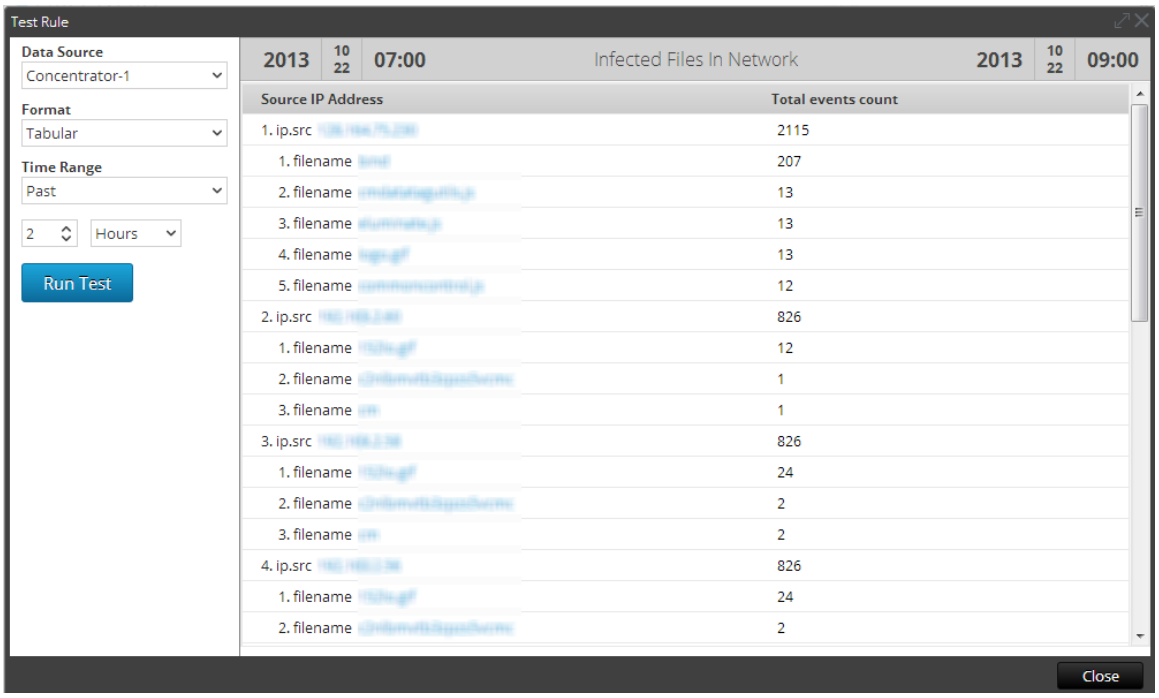
You can even narrow down these appended results even further to only include filenames that have .gif as filename extension by using the fifth parameter in the rule action. The fifth parameter allows you to specify additional WHERE clause criteria. The files with .gif filename extension would be stored in the **test** list within a group named **DocTeamList**. You can access this list with the following syntax: threat.source = $[DocTeamList/test]
This can be referenced in the extra where clause parameter in the following manner:

4. lookup_and_add('filename', 'ip.src', 5, false, 'filename CONTAINS $[DocTeamList/test]');

The following figure shows the rule definition.



The following figure shows the result set.

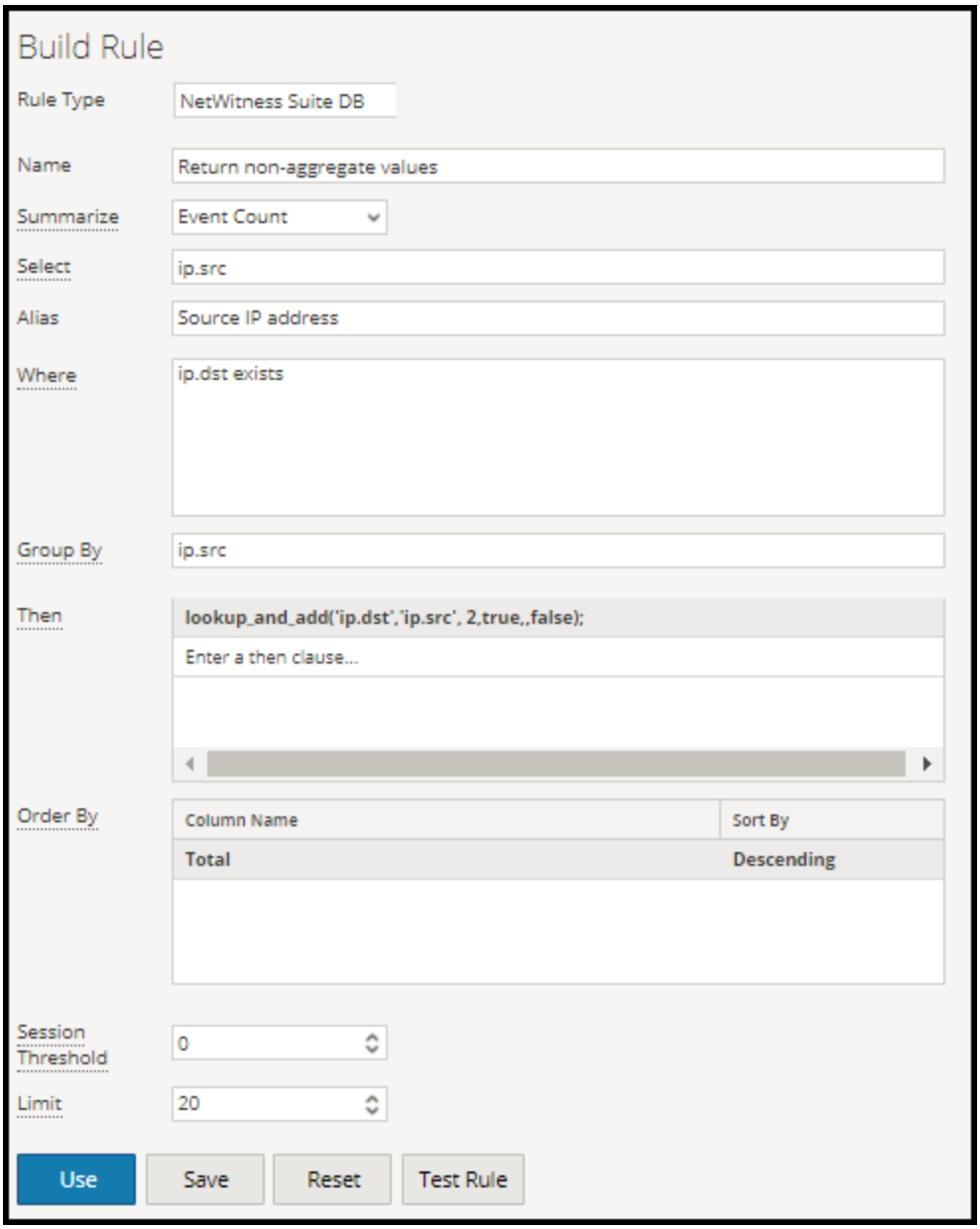


5. lookup_and_add('ip.dst','ip.src', 2,true,,false);

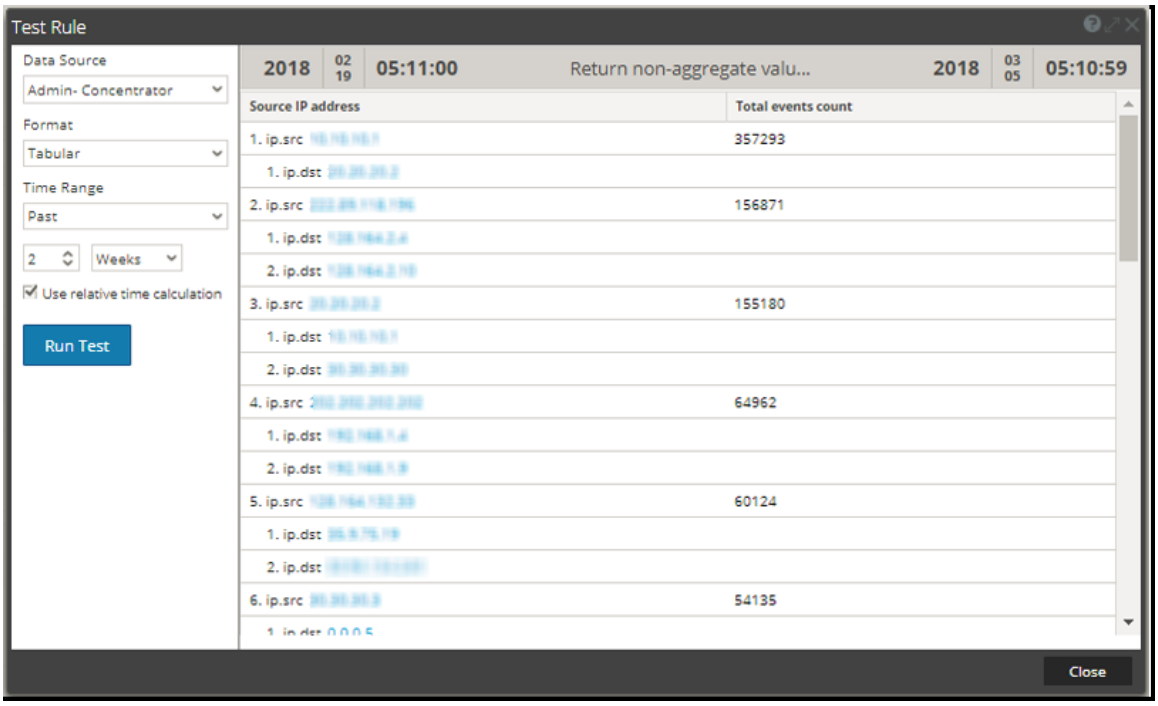
This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src. The 'aggregate' parameter is set to 'false', this implies that aggregates would be skipped for lookup values and hence the lookup query executions will complete faster.

Note:
The default value for 'aggregate' is 'true'. When 'aggregate' is set to 'false', Reporting Engine passes threshold=1, Sort by='value' and Order=Ascending to NWDB to make lookup queries run faster.
. You must set the 'aggregate' to false, when rule contains aggregate functions or when the rule is run against a wide time range. This helps the rule to complete the execution faster.

The following figure shows the rule definition.



The following figure shows the result set.



`max_threshold (string quantity)`

`max_threshold (string quantity, string field)`

max_threshold removes any results with a quantity that is larger than the maximum threshold quantity from a result set. The quantity can either be in terms of count or size and it is relative to the sorting options of the parent rule. This means that if you sort a rule by size, the rule action expects you to specify the parameter in bytes (you can append KB, MB, GB, TB to the parameter to make size conversion easier).

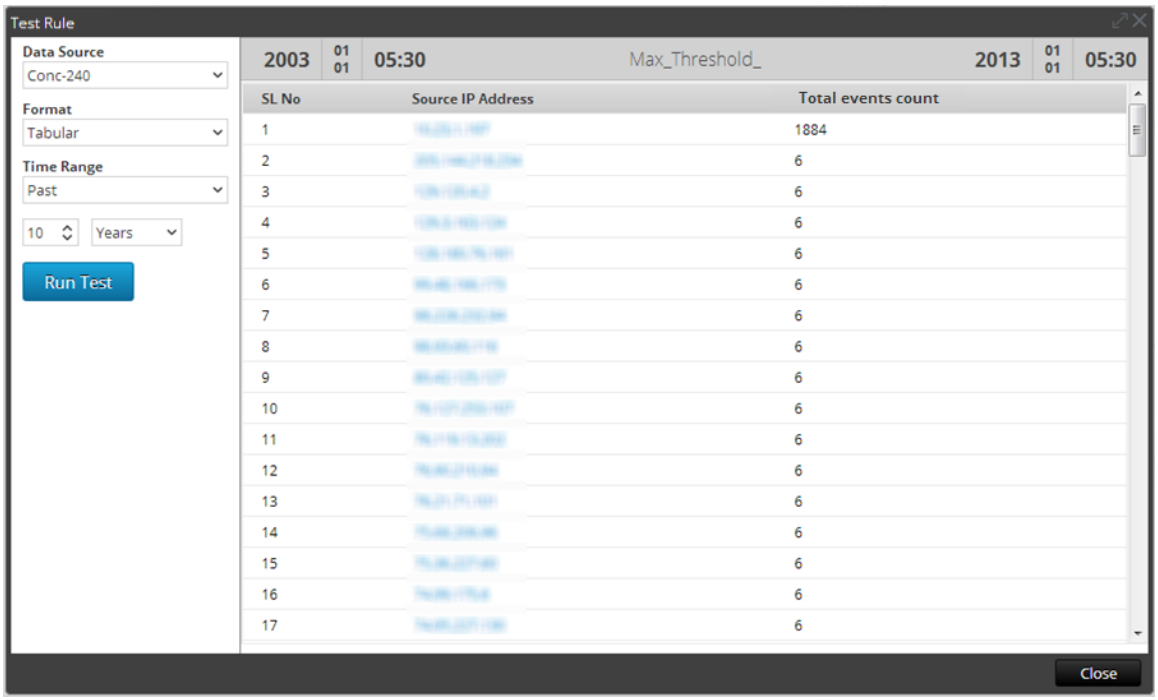
max_threshold rule can also be used to filter values based on the aggregate function values. Use the syntax based on the type of summarization used in the rule as below:

- max_threshold(String quantity): Can be used to filter Event Count, Packet Count, and Session Size.
- max_threshold(String quantity, String field): Can be used to filter values of Custom aggregates or any metas.

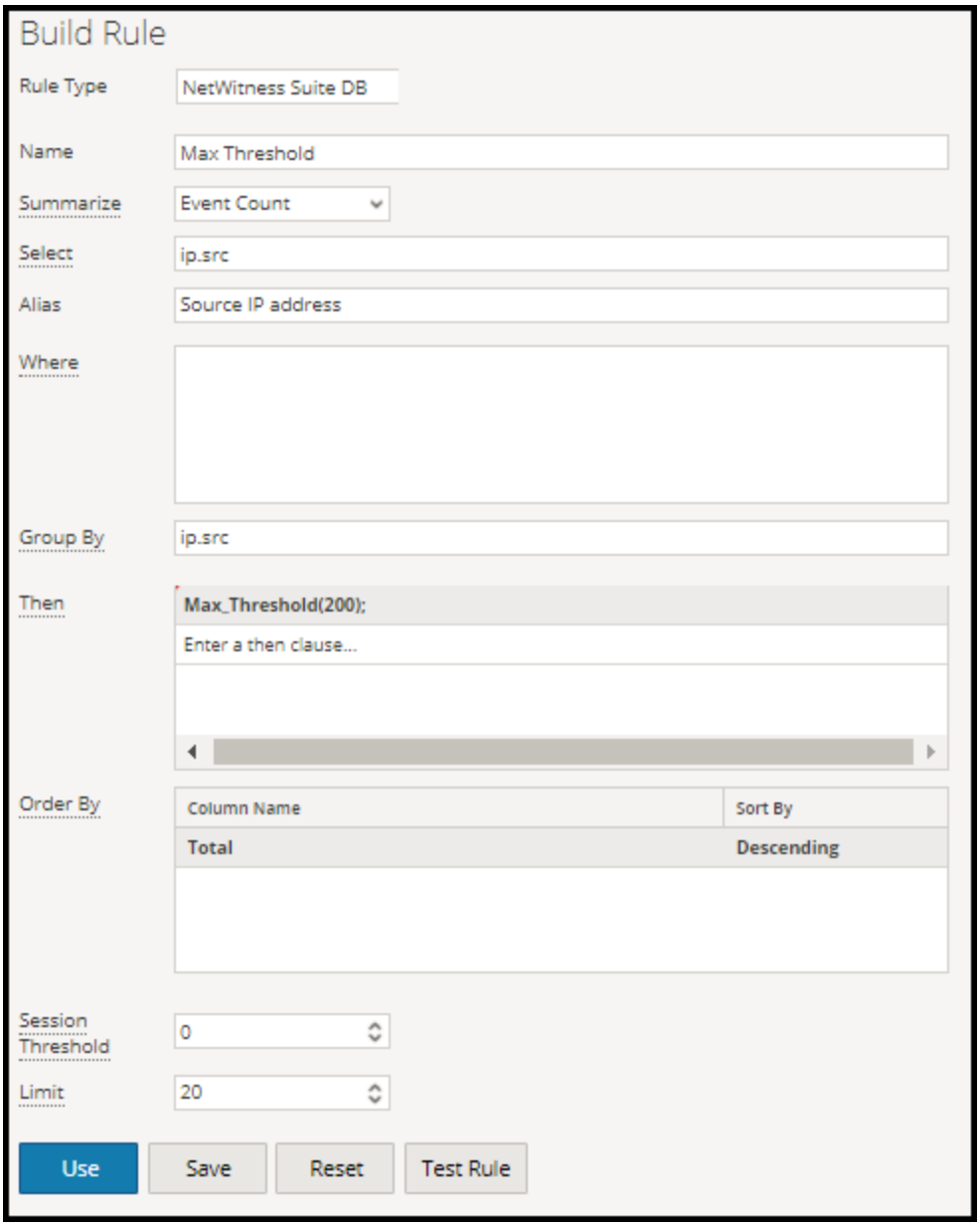
Examples:

1. max_threshold(200);

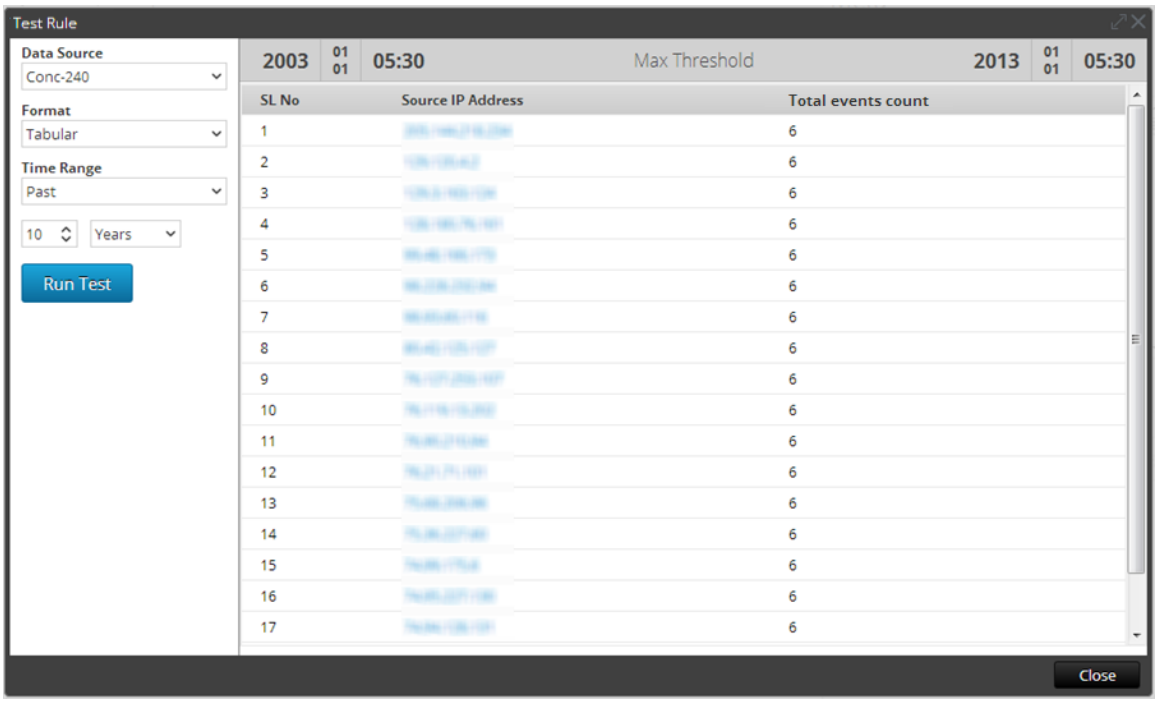
The following figure shows the result without the max_threshold argument. The output results have event counts exceeding 200.



The following figure shows a the max_threshold rule action that puts a limit of 200 bytes on the output. Any output having more than 200 bytes of data are not listed.

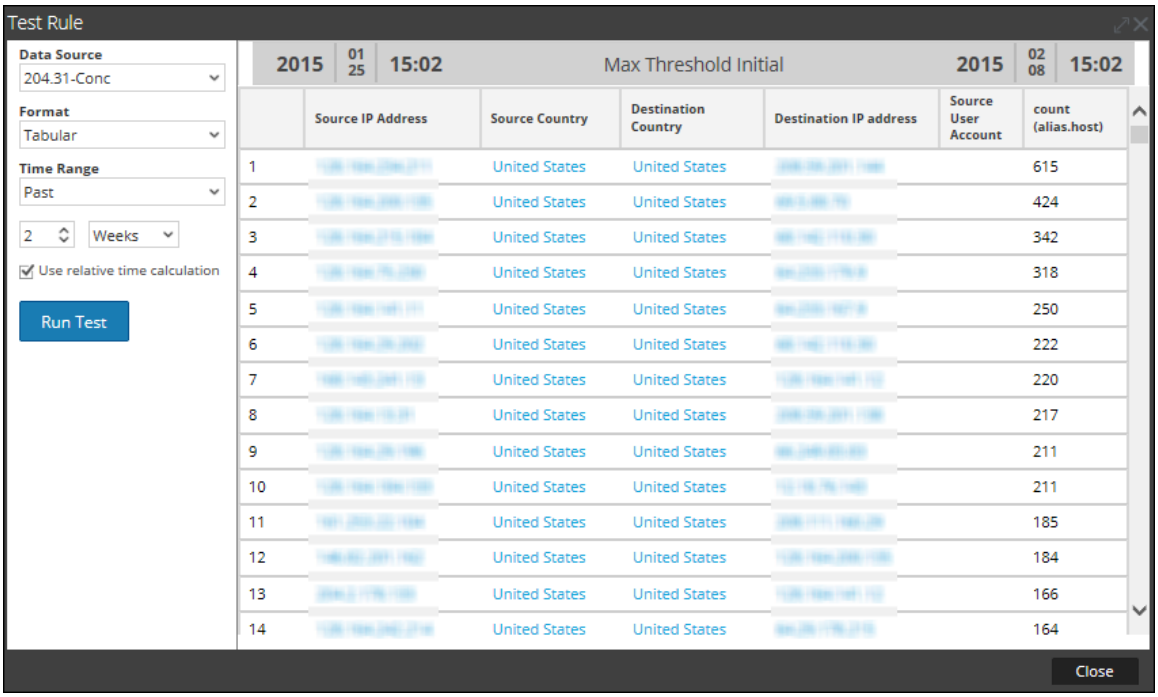


The following figure shows the result when the max_threshold rule action is applied. The result numbered 1 in the above screen capture is removed from the result.

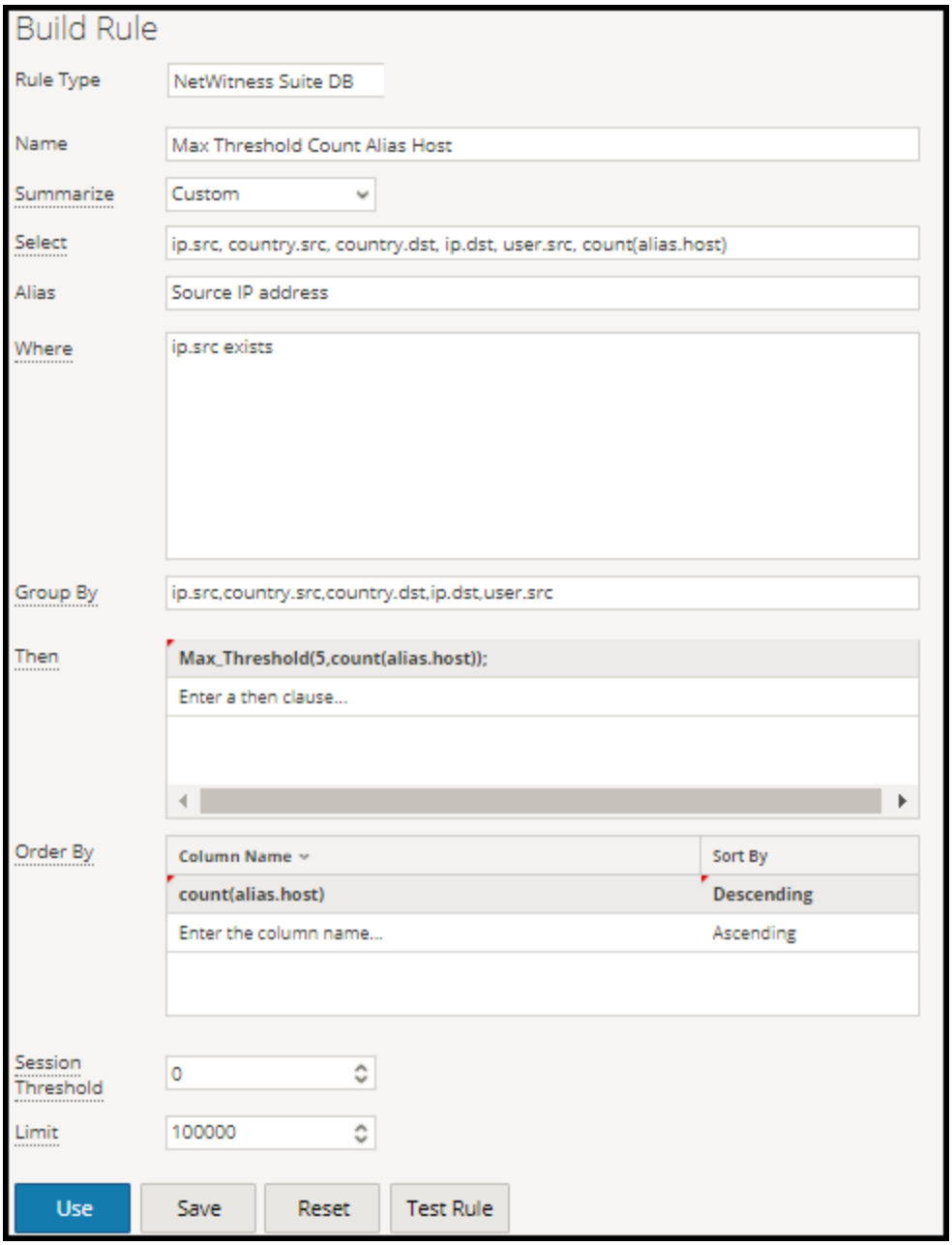


2. max_threshold(5,count(alias.host));

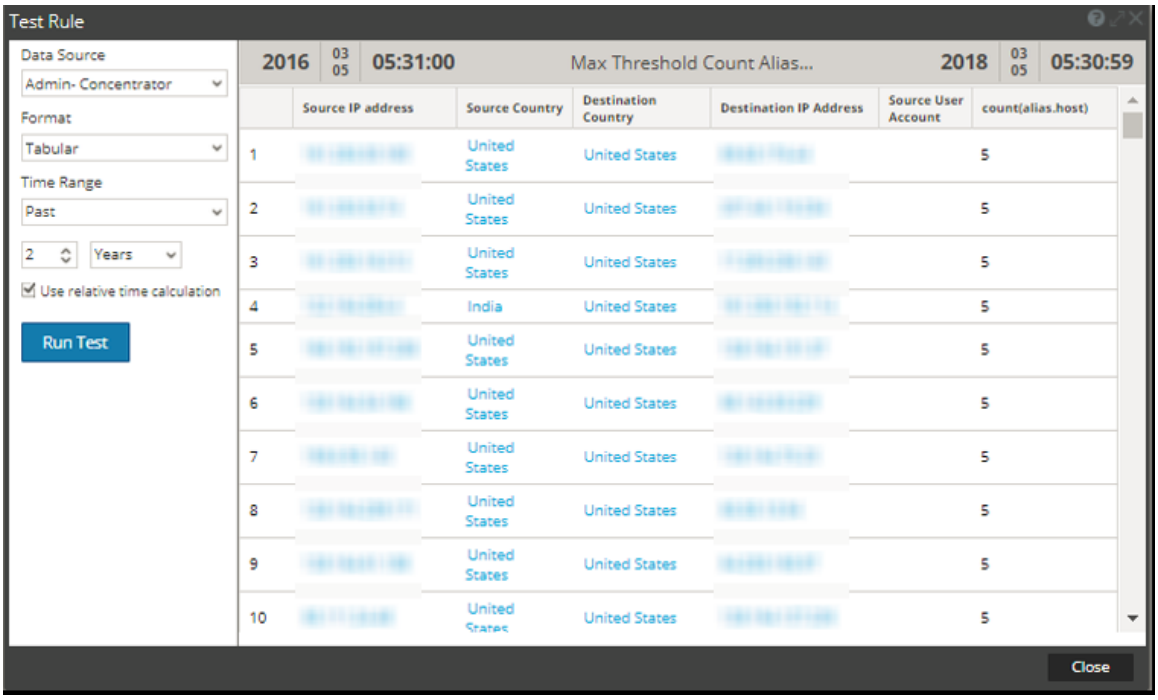
The following figure shows the result without the max_threshold argument. The output results have count of alias.host exceeding 5.



The following figure shows a the max_threshold rule action that puts a limit of 5 on the output. Any output having value more than 5 is not listed.



The following figure shows the result when the max_threshold rule action is applied. Any output having value more than 5 is removed from the result.



min_threshold (string quantity)

min_threshold removes results with a quantity that is smaller than the minimum threshold quantity from a result set. The quantity can either be in terms of count or size and it is relative to the sorting options of the parent rule. This means that if you sort a rule by size, the rule action expects you to specify the parameter in bytes (you can append KB, MB, GB, TB to the parameter to make size conversion easier).

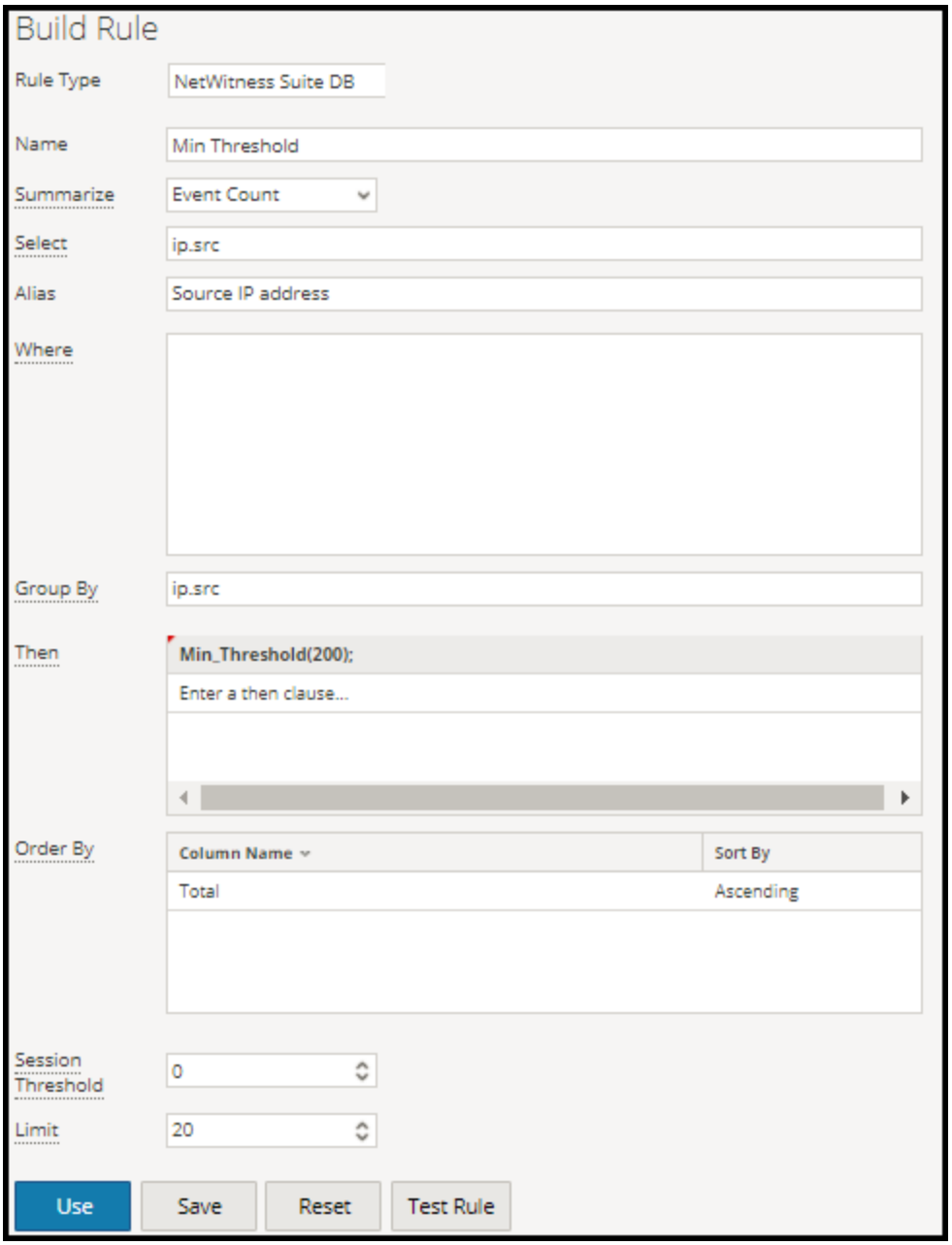
min_threshold rule can also be used to filter values based on the aggregate function values. Use the syntax based on the type of summarization used in the rule as below:

- min_threshold(String quantity): Can be used to filter Event Count, Packet Count, and Session Size.
- min_threshold(String quantity, String field): Can be used to filter values of Custom aggregates or any metas.

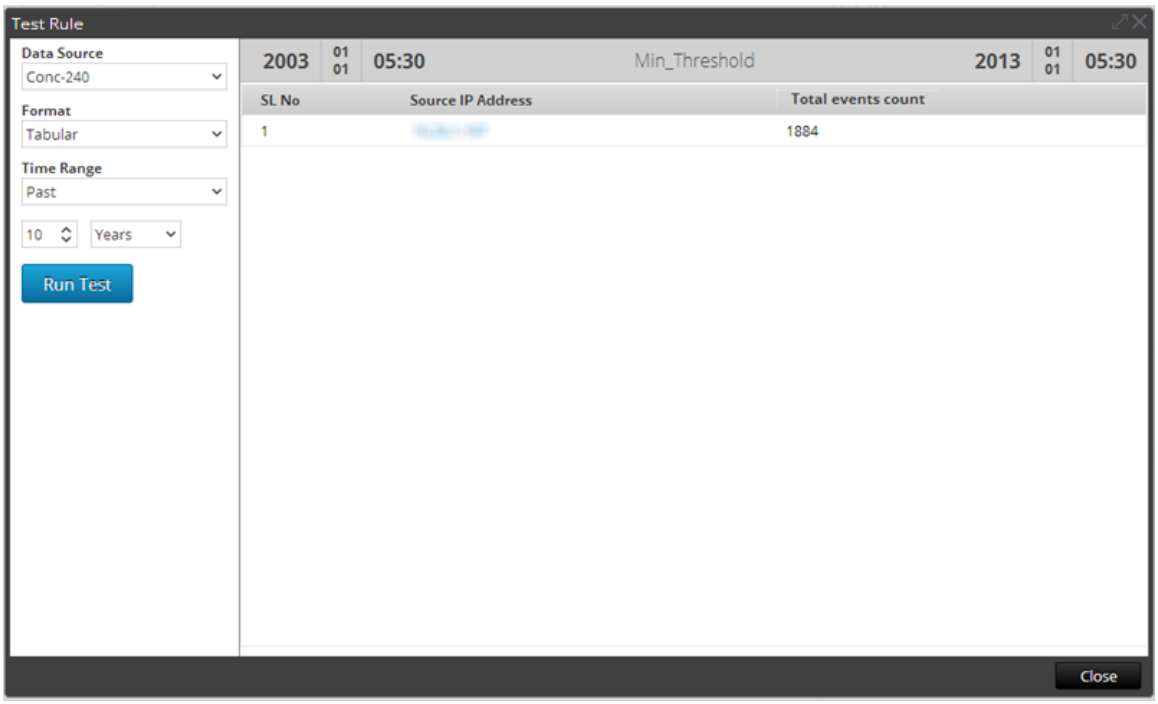
Examples:

1. min_threshold(200);

The following figure shows a sample of the min_threshold query.



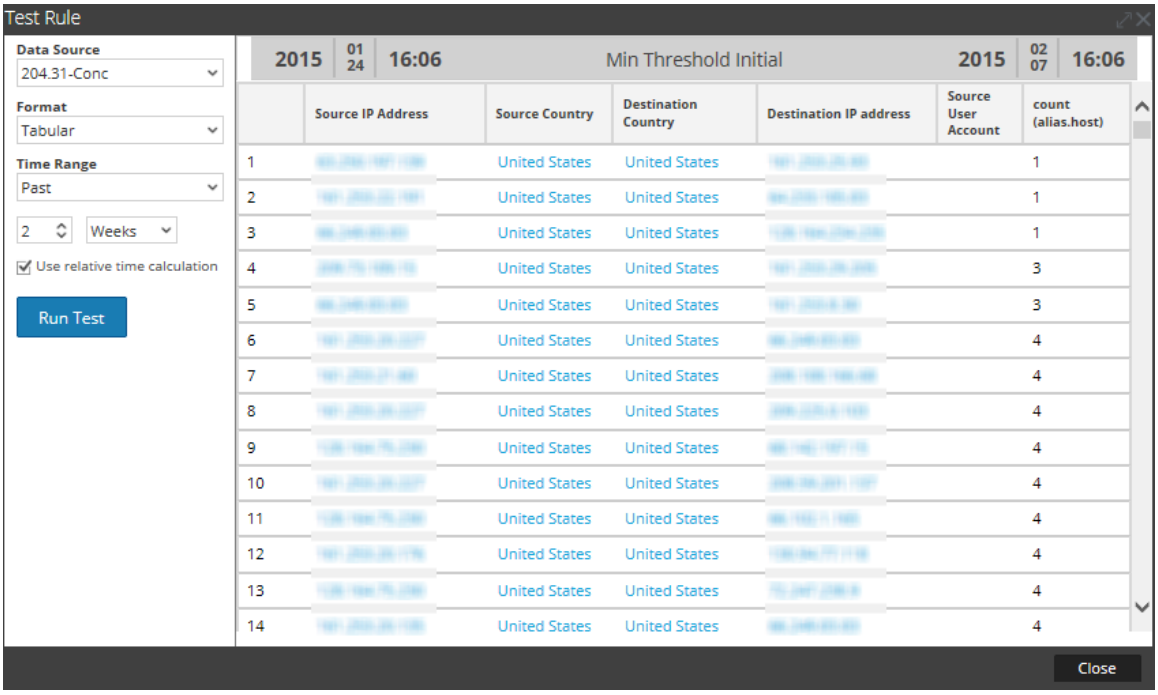
The above figure puts a limit of 200 bytes on the output. Any output having less than 200 bytes of data is not listed. The output with the min_ threshold rule action is applied.



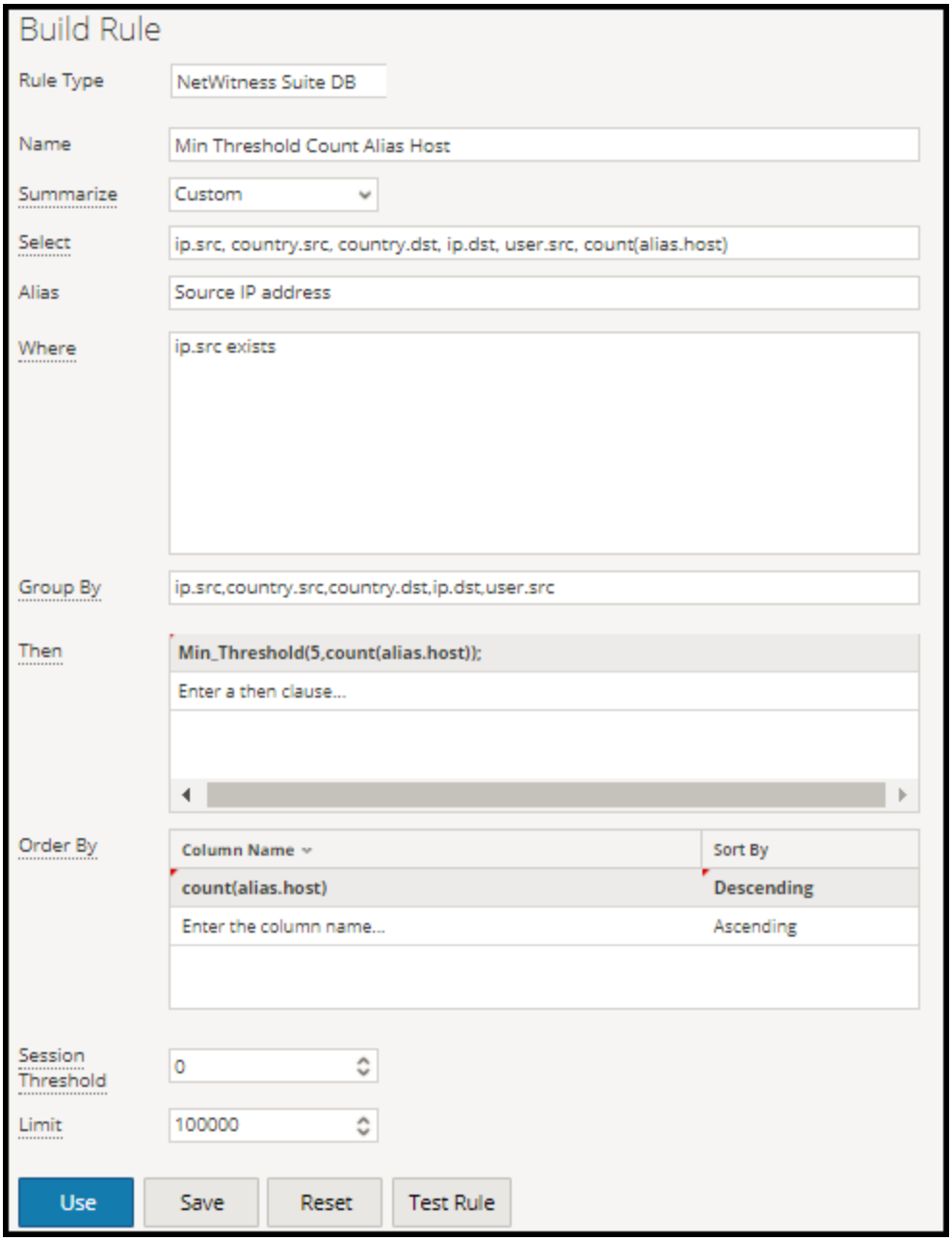
As shown, all the values are greater than 200 bytes.

2. min_threshold(100,count(alias.host));

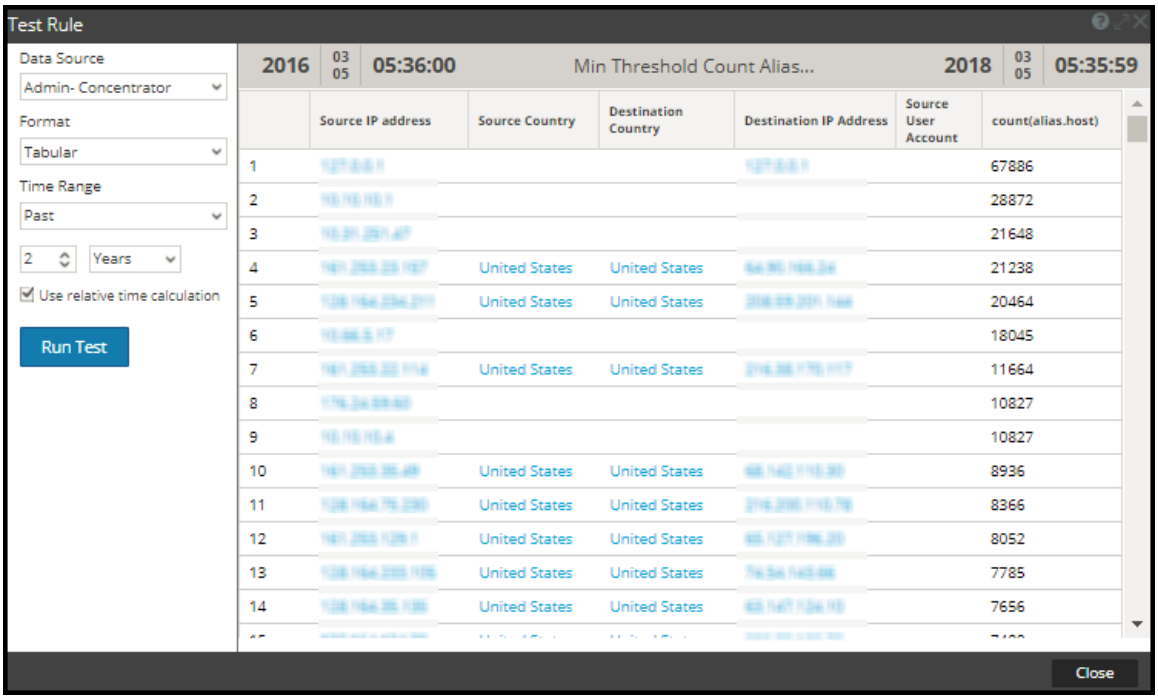
The following figure shows the result without the min_threshold argument. The output results have count of alias.host below 100.



The following figure shows a the min_threshold rule action that sets the minimum limit of 100 on the output. Any output having data less than 100 is not listed.



The following figure shows the result when the min_threshold rule action is applied. Any output having data less than 100 is removed from the result.



regex (string regex, string field)

The regex rule action applies regular expression to the result set. The following is the format of the regex rule action:

regex(regular_expression, meta_name)

Where:

- regular_expression - Regular expression to match the value of the meta.
- meta_name - Meta or field name on which the regex has to be applied.

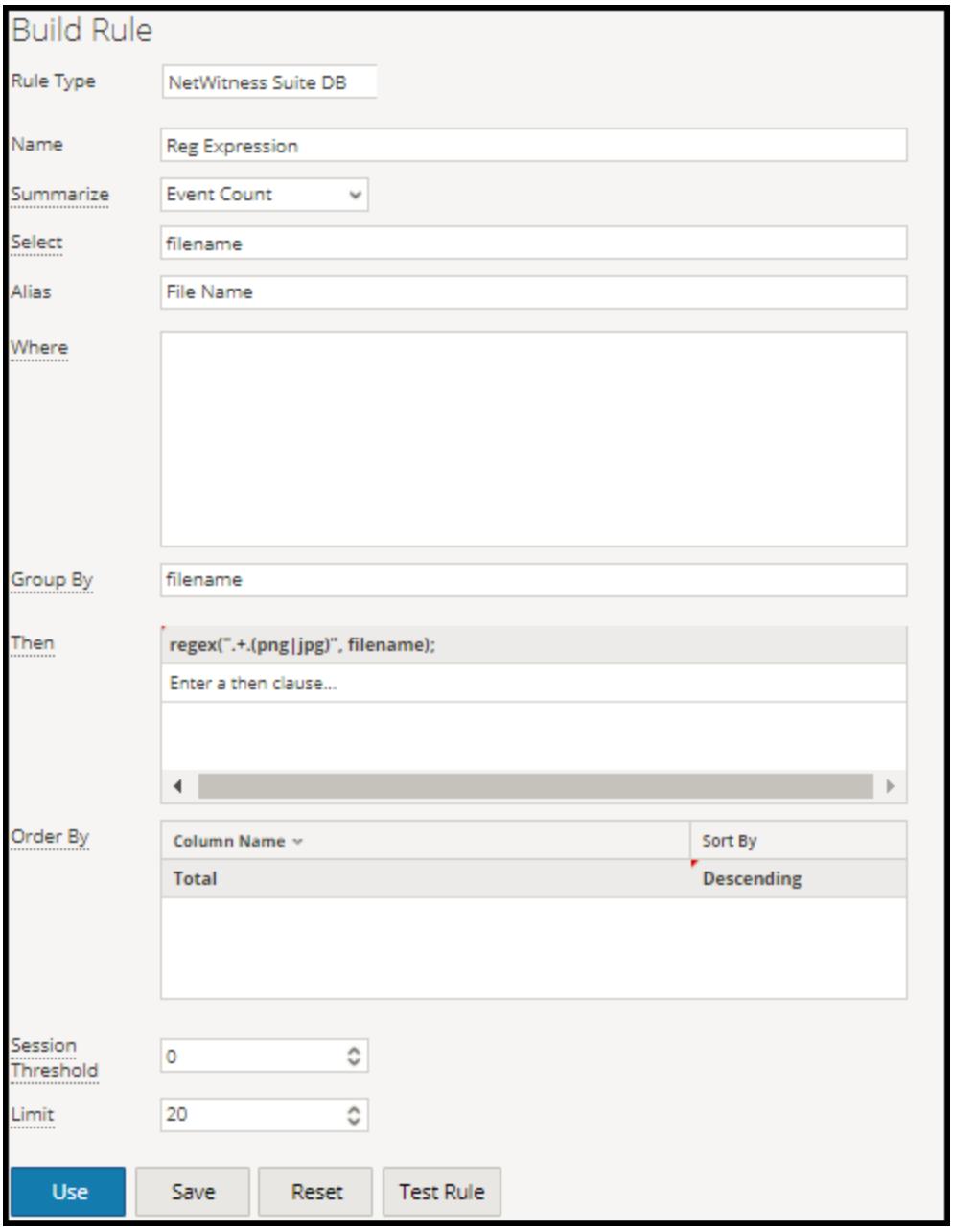
For a comprehensive list of supported regex patterns, refer to http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

Sample regex rule action:

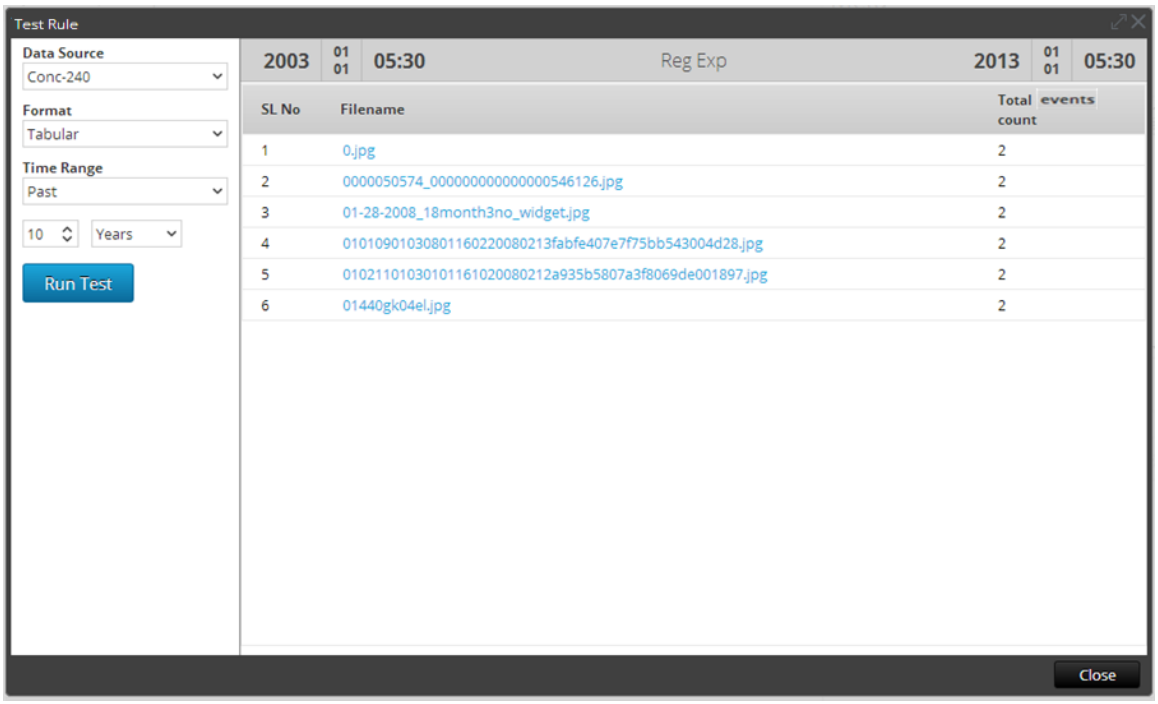
If you want to list filenames of all the PNG and JPEG format files from various sessions, you can write a rule with the following regex rule action:

regex(".+.(png|jpg)", filename);

The following figure shows the rule.



The output with the regex rule action applied is shown in the following figure.

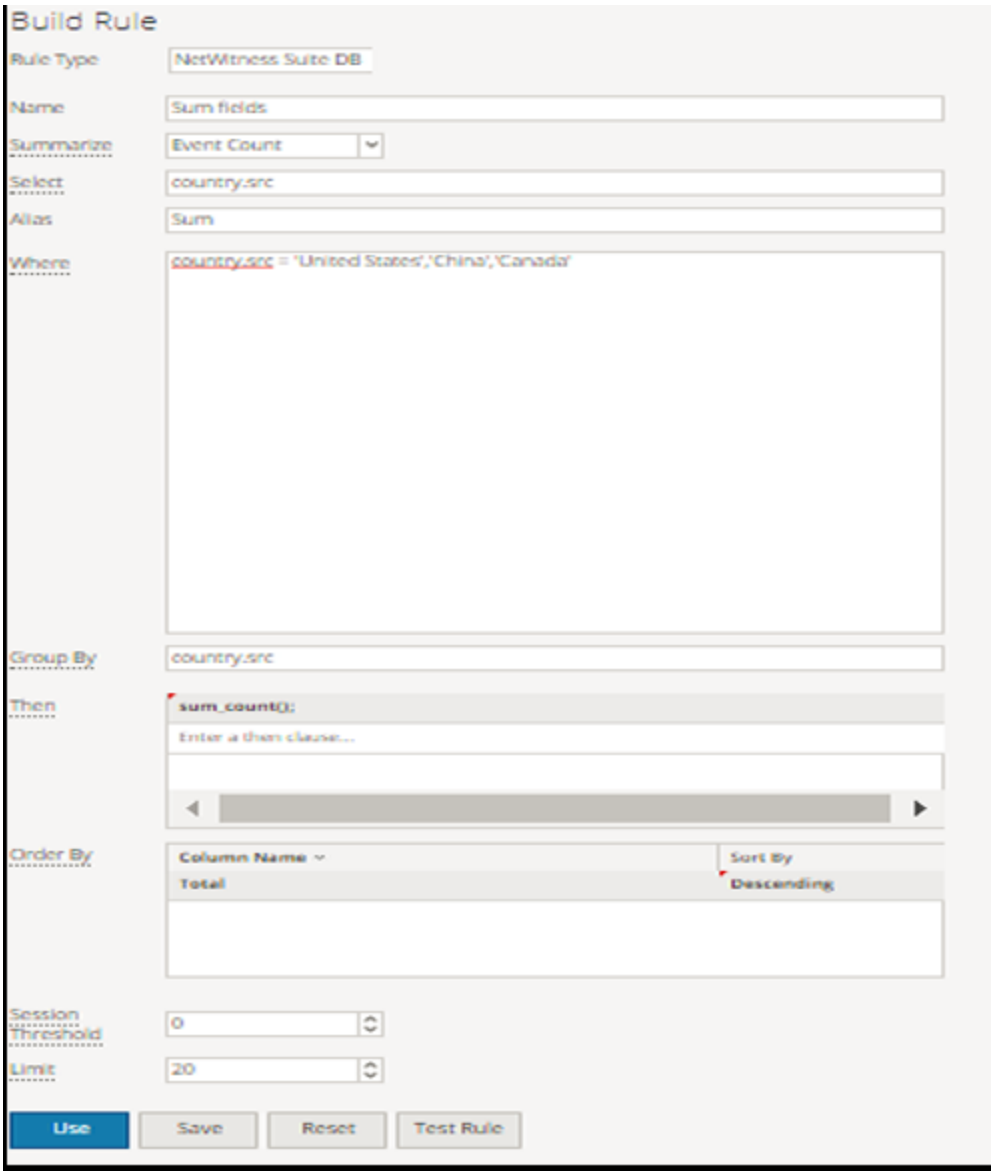


`sum_count()`

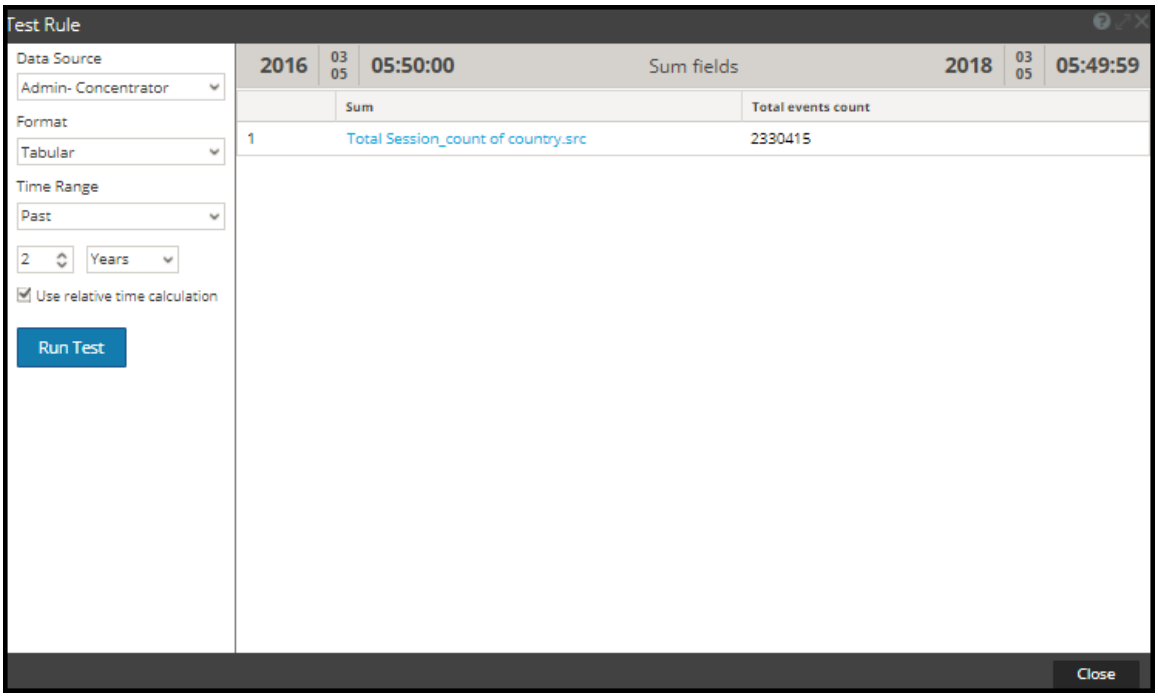
Totals the quantifiers for a given result set. For example, calling a sum_count () for a rule that is sorted by event count totals the size of all values in the result set and displays the total in place of the result set.

Example:

The following figure shows the sum_count() rule action.



With sum_count() rule action, the output shows the total size of all the event counts.

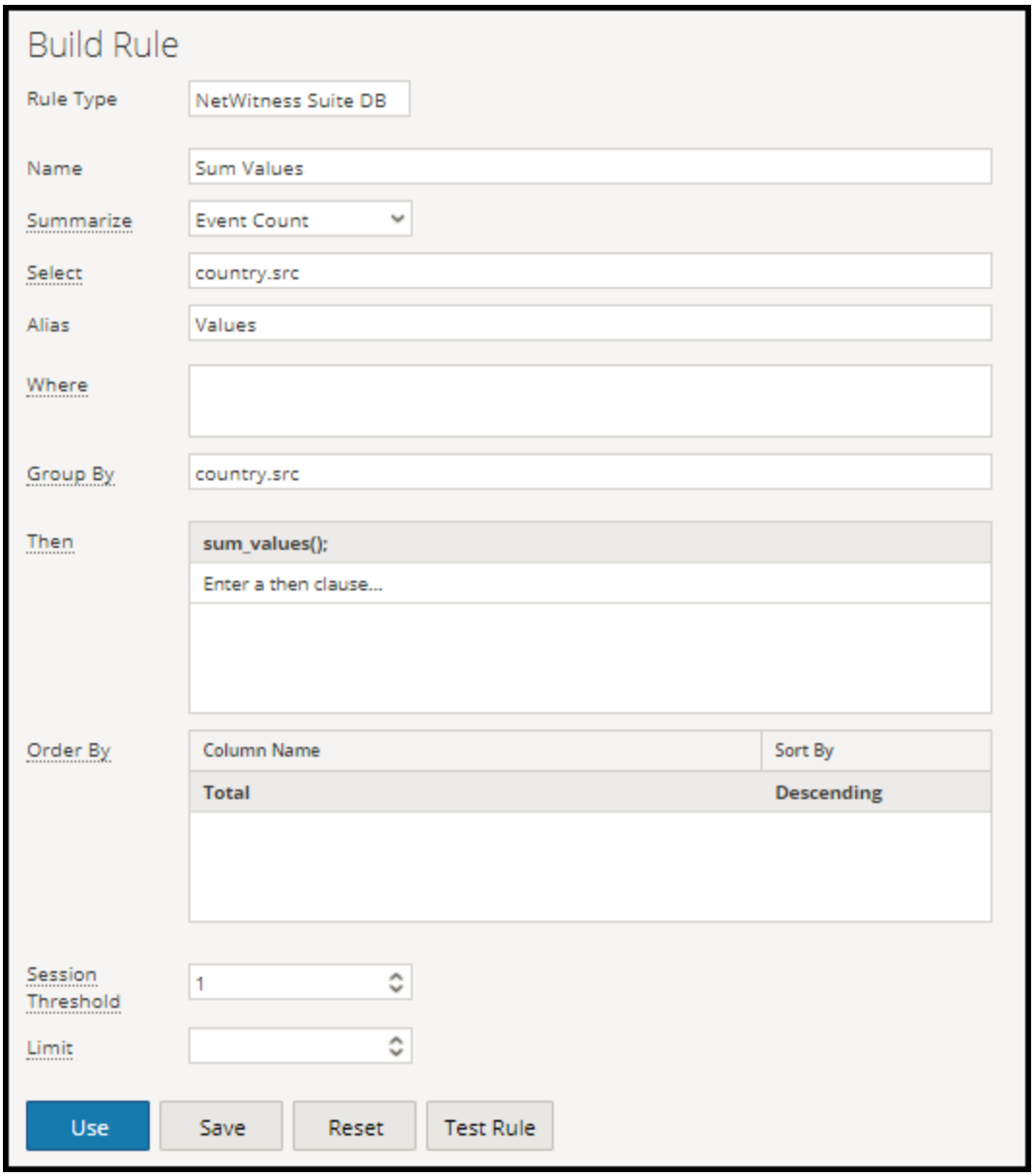


`sum_values()`

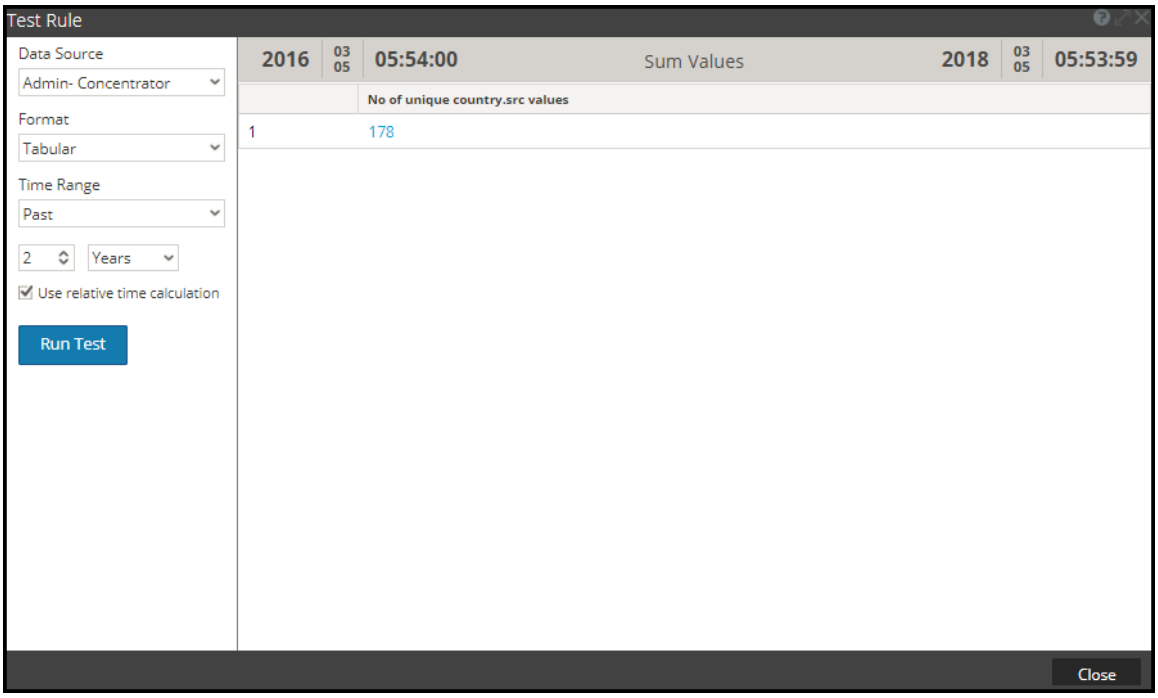
Totals the number of values for a given result set. Use this action to display how many matches exists for a given rule.

Example:

The following figure shows the sum_values() rule action.



The following figure shows the result with sum_values rule action.



show_whats_new()

The show_whats_new() rule action takes any result in a result set and filters out any value that is available in the NetWitness meta database prior to the time frame of the currently running report. When a report runs, NetWitness Suite determines the ID of the first session in the time range of the report. If a value in a result set has a first session id that is greater than the first session id of the report time frame, it did not exist in the NetWitness meta database prior to the report being run and so is new to the NetWitness system relative to the time frame of the report.

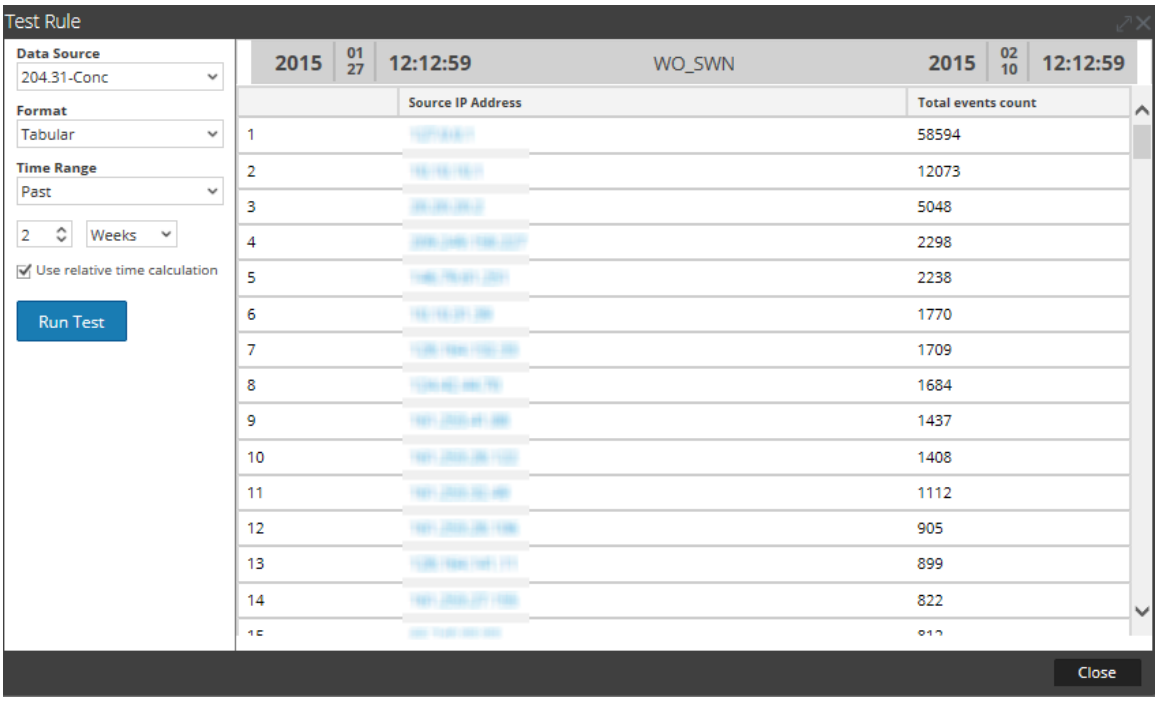
The show_whats_new() rule action is also supported for Custom Aggregate Rule. When multiple meta's are selected in the Custom rule, the first meta is considered for filtering out the old values. See "Example 2" below to understand how this rule action is used for Custom Aggregate Rule.

Note: The show_whats_new() rule action can be used only with an aggregate rule.

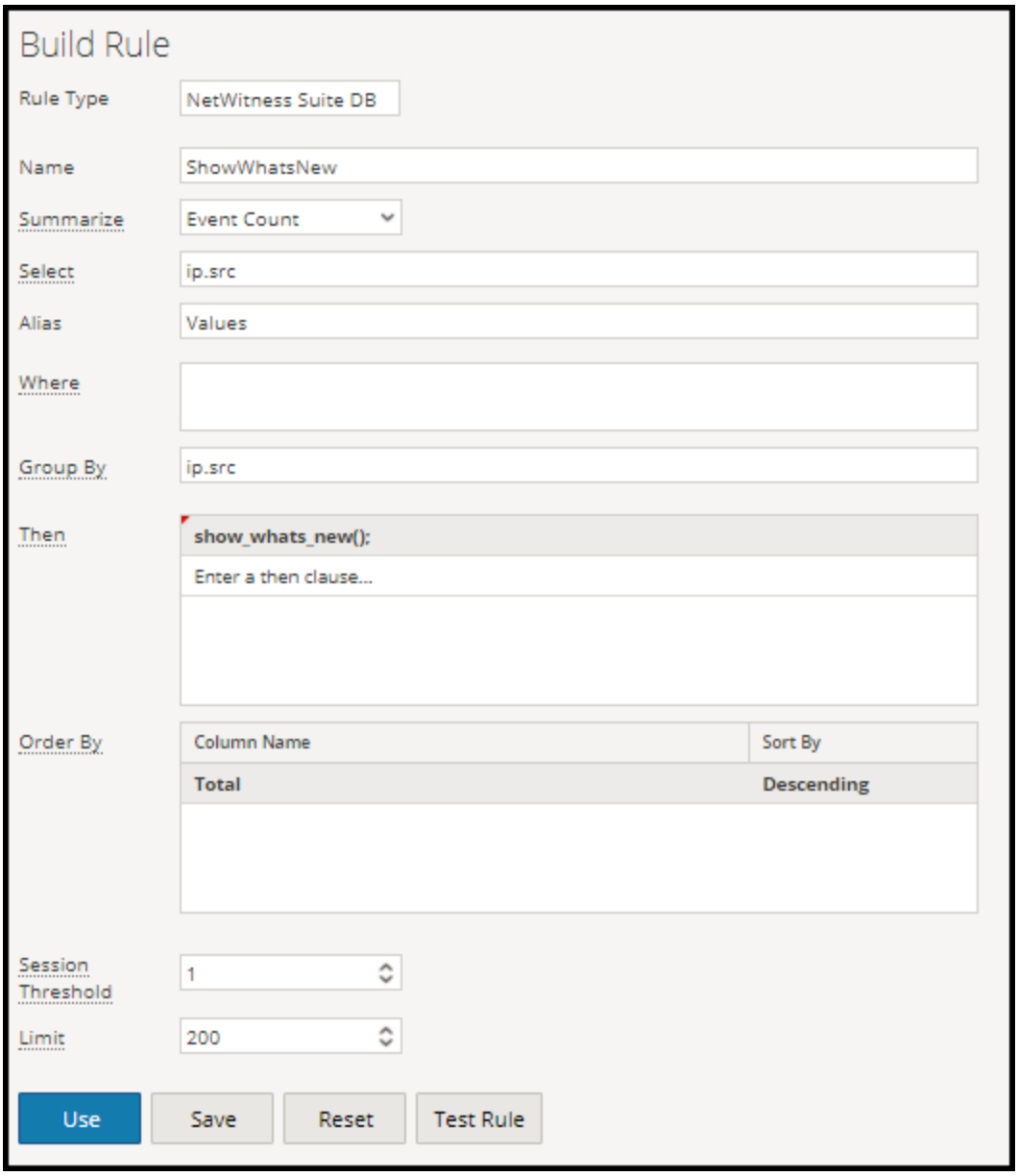
Examples:

1. show_whats_new() for aggregate rule with Event Count

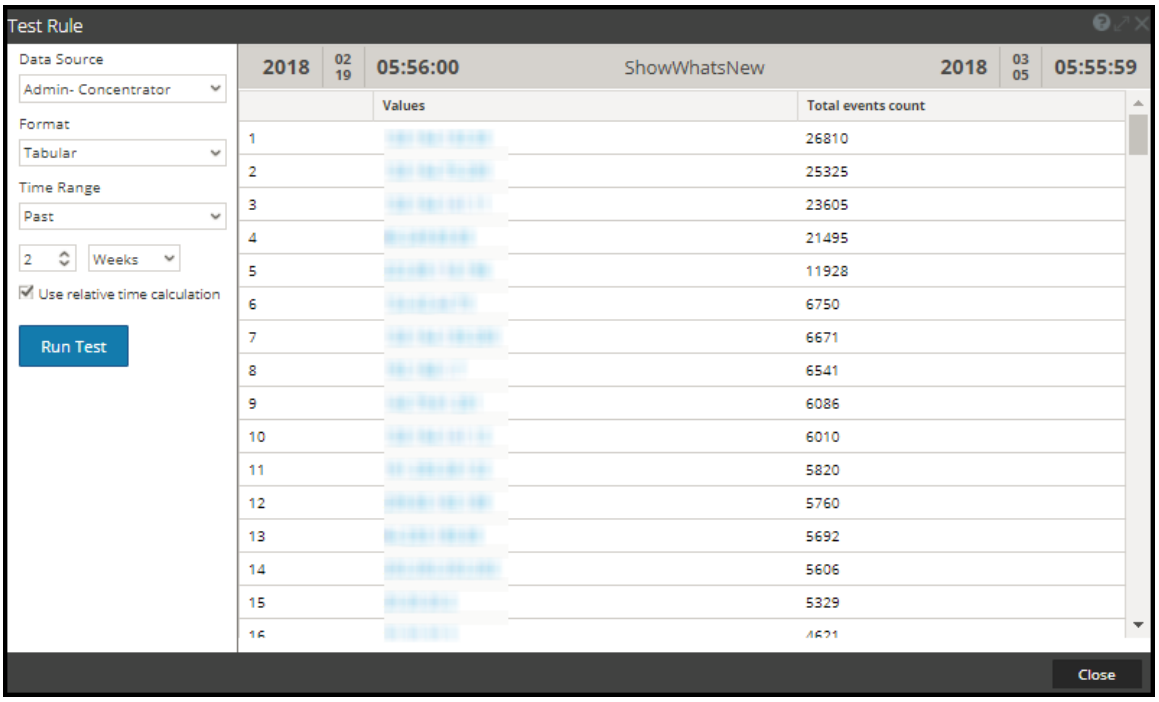
In the following example, all the Source IP Addresses available for the past two weeks are listed.



The following figure shows the use of the show_whats_new rule action to list only the new entries for the past two weeks.

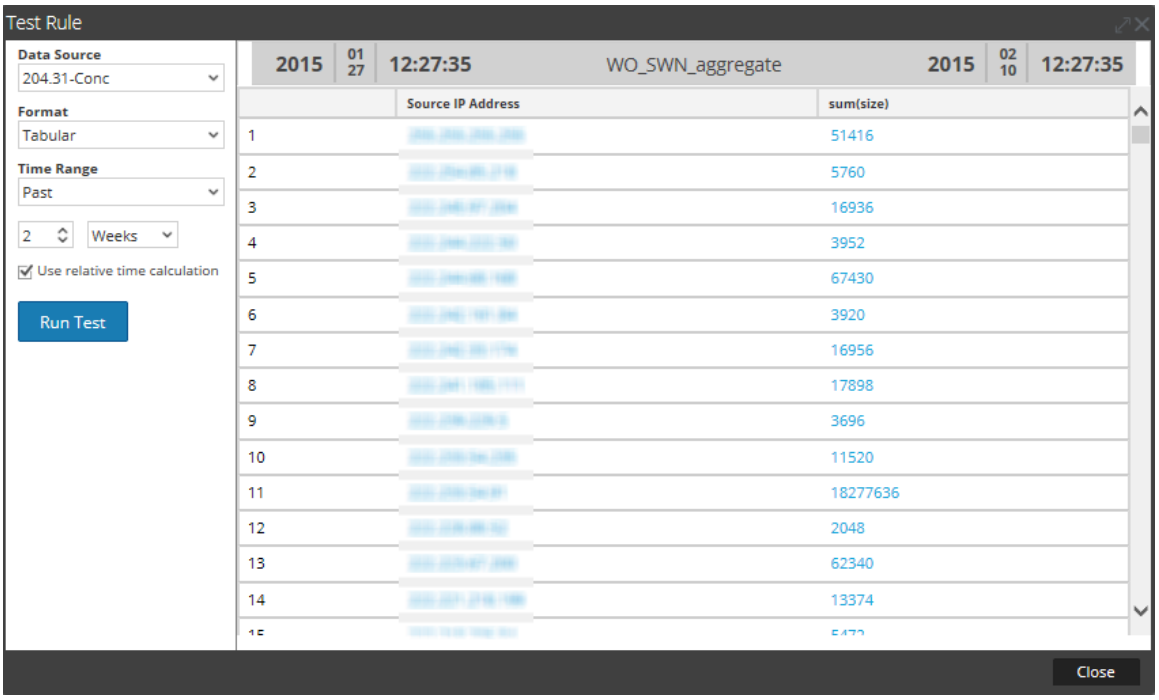


The following figure lists the new entries for the past two weeks.

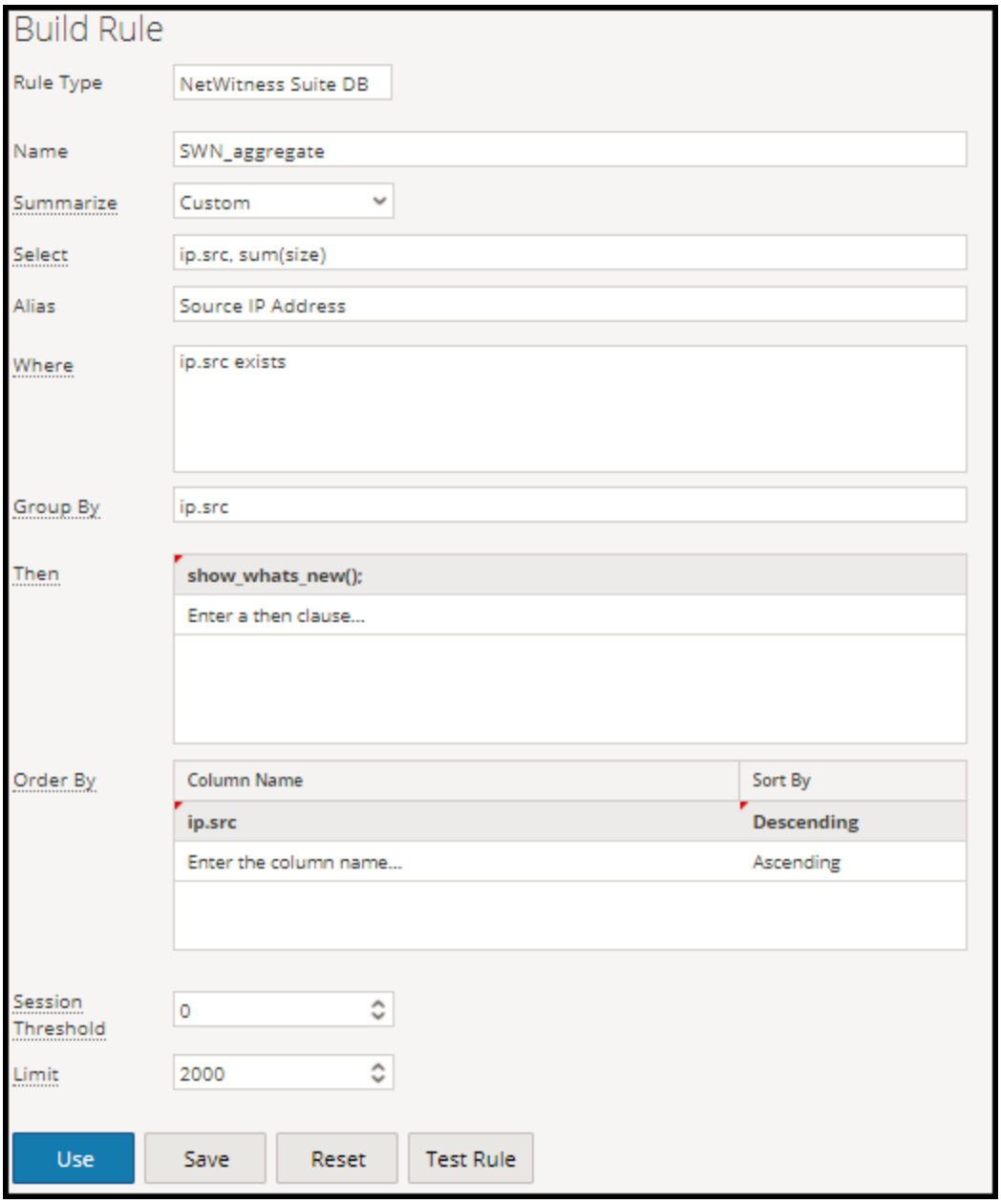


2. show_whats_new() for Custom aggregate rule

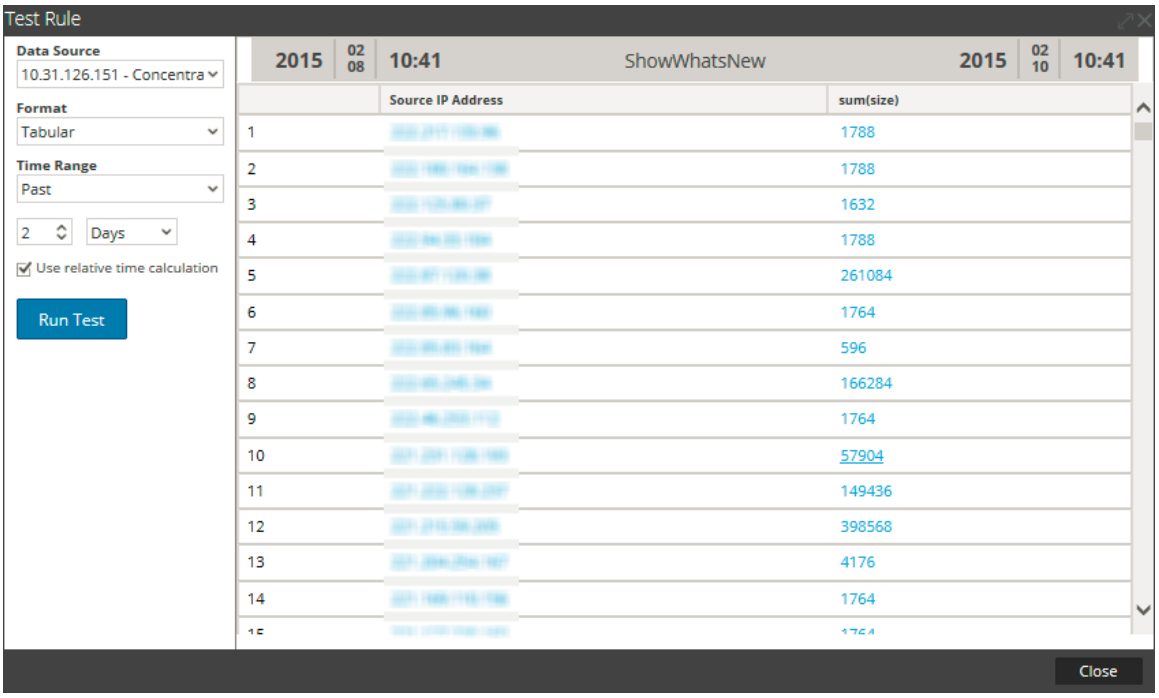
In the following example, all the Source IP Addresses available for the past two weeks are listed.



The following figure shows the use of the show_whats_new rule action to list only the new entries for the past two weeks.



The following figure lists the new entries of Source IP Addresses for the past two weeks.



The power of this feature is that it doesn't matter when the report is run in identifying values that are new to NetWitness. The caveat with this feature is that if a data reset occurs, you will lose your data. However, it is easy to baseline a system and identify changes and new items without a tremendous amount of strain on the system (depending on the size of your result set).

Supported Rule Operators

The NWDB Reporting Engine data source rule syntax supports a subset of rule operators that are supported by NetWitness Suite.

Syntax	Description
*	Use an asterisk (*) as the sole operator in a rule to select all traffic.
=	Equals operator
!=	Does not equal operator
&&	Logical AND operator
||	Logical OR operator

Syntax	Description
-u	Upper boundary. For example, **tcp.port = 40000-u** selects all TCP ports above 40000.
l-	Lower boundary. For example, **tcp.port = l-40000** selects all TCP ports below 40000.
-	The dash (-) operator only applies to numeric values. Separate the lower and upper boundaries of the range with a dash (-). For example, **tcp.port = 25-443** selects all TCP ports between 25 and 443.

Sample Supported Queries

Respond Rule Syntax

The supported rule syntax for the RESPOND service through descriptions and examples of supported and unsupported syntax. There is a finite set of syntax that you can use to construct rules for reports using the RESPOND service in this release.

The Reporting Engine supports the following categories of RESPOND data source rule syntax:

- **select** clause
  - Non-Aggregate Rule
  - Aggregate Rule
- **alias**
- **where** clause
- **where** clause Operators
- Group By
- Order By
- **Limit** field

Note: List is not supported in Respond Data source rules.

Select Clause

The select clause is a comma separated list of values. For example: select alert.severity, alert.name, count(*).

There are two types of select clause for RESPOND Rule:

- Non-aggregate rule
- Aggregate rule

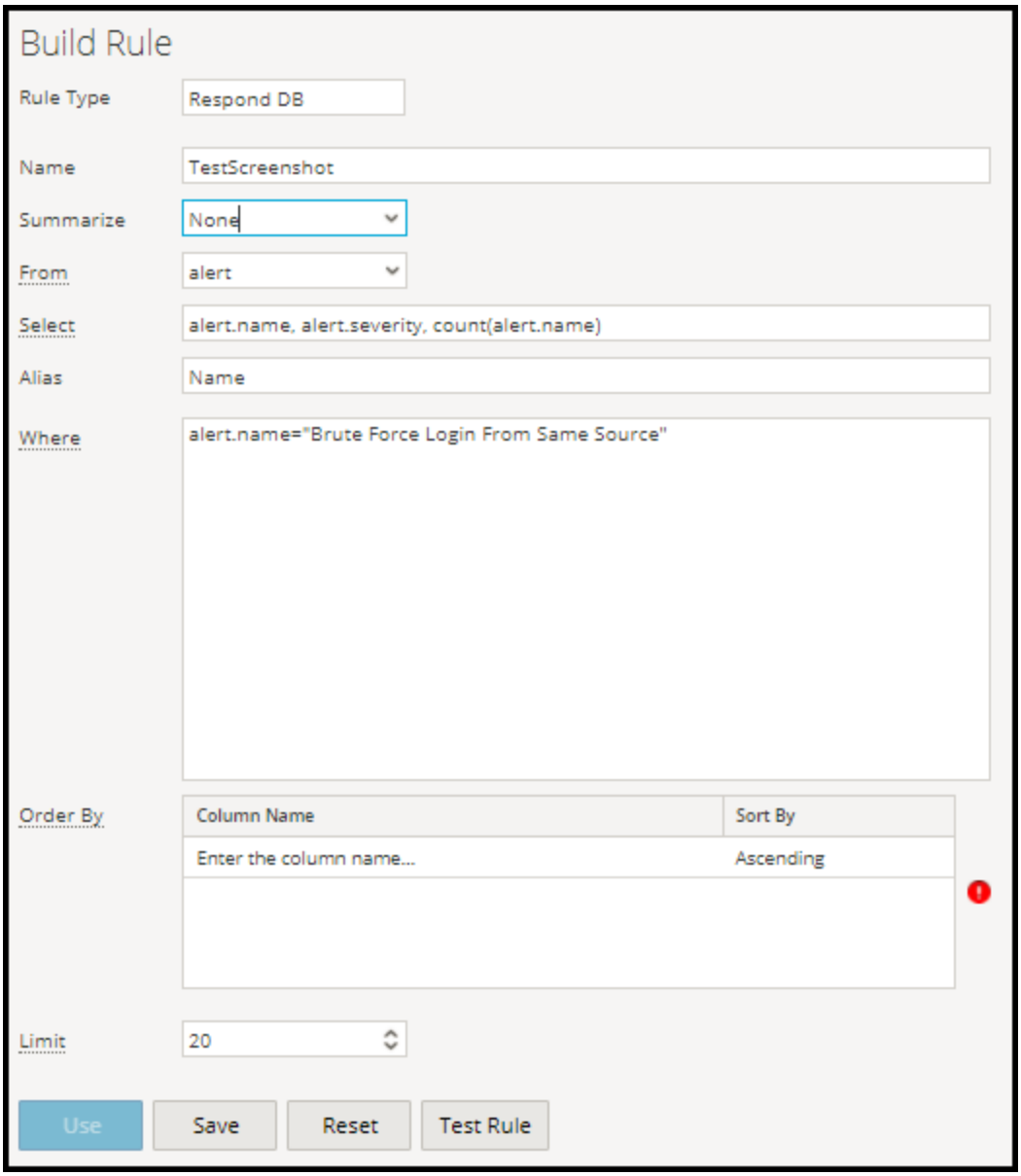
Non-Aggregate Rule

When you want to define a rule without any grouping, choose 'None' in the Summarize field. In a non-aggregate rule, you can select any number of metas in the *Select* clause. For example, select alert.severity, alert.name.

Aggregate Rule

When you want to query for a specific meta and its associated aggregate value then you must use the Aggregate rule. To get an aggregate, you must choose 'Custom' in the **Summarize** field to include an aggregate function in the *Select* clause. For example, select alert.severity, alert.name, count(*).

The following figure shows the Build Rule view for Aggregate Rule.



Supported Aggregate Functions

The rules on RESPOND service supports the following aggregate functions and syntax.

- count
- max
- min
- sum
- avg

Note: The aggregate functions must be added in the end of a select clause for aggregate query. For example, alert.name, alert.severity, sum (alert.numEvents). By default, a maximum of 10,000 rows results are fetched and this can be configured using the **rsa.response.query.QueryProperties**.

Examples of select Clause Syntax

The following table provides examples of the select Clause Syntax.

Examples	Descriptions
select *column1* , *column2* ,*column3*,...,*columnN*	Select specific metas from an RESPOND Data Source (You must separate each column with a comma.).

Examples of Supported Select Queries

select alert.name, alert.numEvents, count(alert.numEvents)

select alert.severity, avg(alert.severity)

select alert.timestamp, incidentCreated where alert.timestamp >= 1475658011

Summarize

Summarize determines the type of summarization or aggregation for the rule.

Name	Config Value
Summarize	To query metas without any custom grouping, select: • **None**: To get meta based aggregates, select: • **Custom**: This indicates that expected meta aggregate function is defined in rule select clause.

Alias

Some meta names may not be descriptive, in this case description can be added in the the alias field to make column names more readable. For example, **SELECT**: alert.severity, alert.name, count(*)
ALIAS: Alert Severity, Alert Name

In the alias field you can enter a name for columns used in the select clause. If you do not specify the alias for one of the field in the select clause, then the default description will be used. For example, if the select clause has Field1,Field2,Field3,Field4, and alias has only Field1, ,Field3,Field4, then for Field2 a default description is used.

Where Clause

The where clause is a language field values and ranges that is used by RESPOND function. In the where clause, string values have to be enclosed within single quotes.

Examples	Descriptions
alert.host summary =' (Primary) Link status "Down" on interface INTNAME.'	For TEXT or string type data, enclose the string or text in single or double quote. If there is any special character such as an apostrophe within the data then you need to add an additional single or double quotes. For example, alert.name = 'top alerts from Cote d"Ivoire'.
alert.timestamp >= 1475658011	For Date and Time (date/timestamp data type columns), use the EPOCH syntax.

Supported Where Clause Operators

Operator	Syntax
= (equals)	*column1* = '*value*'
!= (does not equal)	*column1* != '*value*'
>	*column1* > '*value*'

Operator	Syntax
>=	*column1* >= '*value*'
<	*column1* < '*value*'
<=	*column1* <= '*value*'

Group By

Syntax	Function
group by : alert.severity, alert.timestamp, incidentCreated **Note:** Group by field is enabled for Aggregate queries and are not editable.	RESPOND picks the metas for Group By field from the selected Select clause automatically.

Order By

Order By determines how to sort the result set and is not case sensitive.

Name	Configuration Value
Column Name	The Column Name is the name of the columns by which you want to sort the results. By default, the value is empty. When you click on a column, the value gets populated based on the Summarize field. • order by alert.name asc • order by incidentCreated desc • order by count (numEvents) • order by status
Sort By	Sort By determines the order in which you want to sort the results such as ascending or descending. **Note:** For all queries, it is mandatory for you to select the order by field.

Limit field

This indicates the limit to be put on the query while fetching data from the database. If a result set is sorted by event count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.

Warehouse DB Simple Rules Syntax

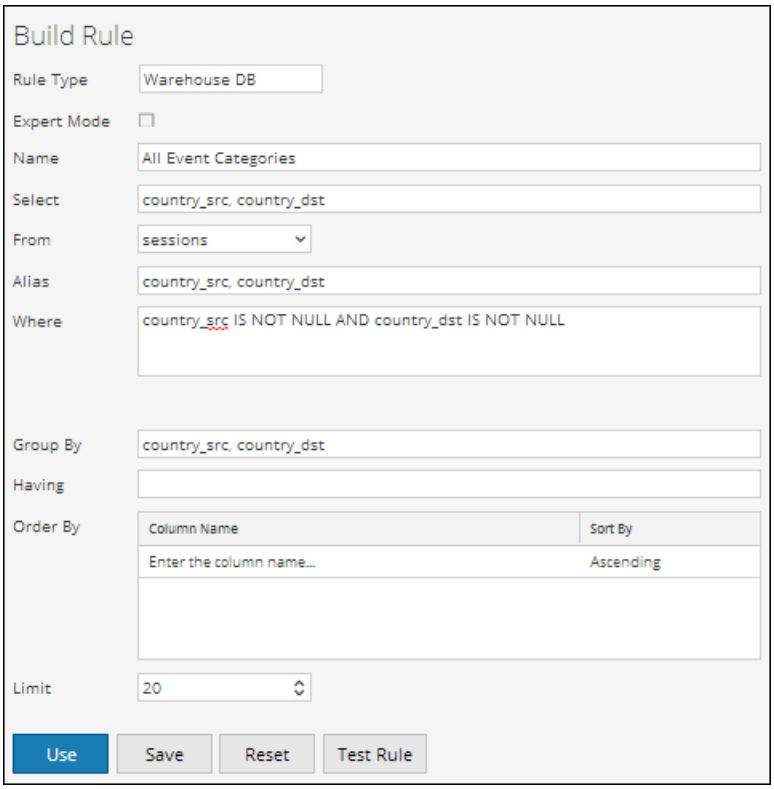
The section explains the simple rules query syntax and examples.

The following examples illustrate simple rules in the default mode:

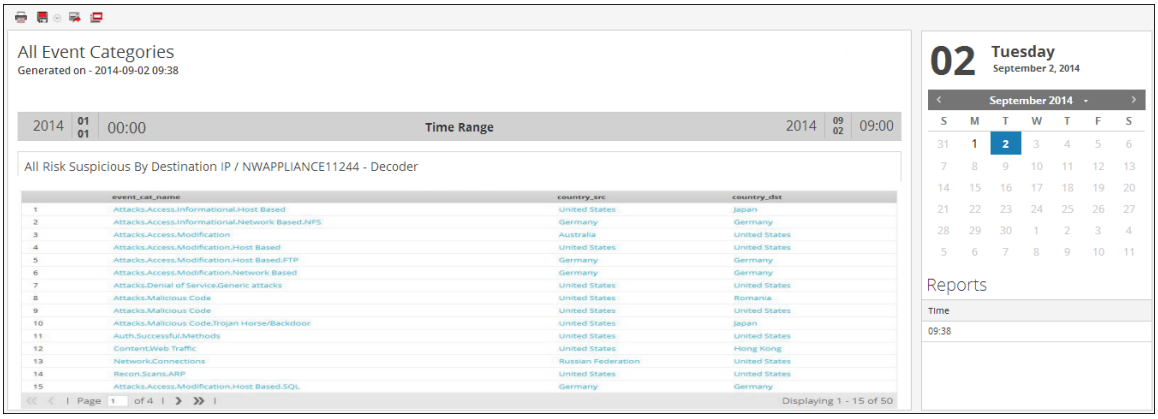
- All Event Categories Report
- Attacks Event Categories Report
- Source: China Event Categories Report
- IP Source and Destination Event Categories Report
- by Time Threat Categories Report
- Array Query Report
- Raw Log Query Report

All Event Categories Report

This rule fetches all event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table, that is, **country_src** for the source country, and **country_dst** for the destination country.

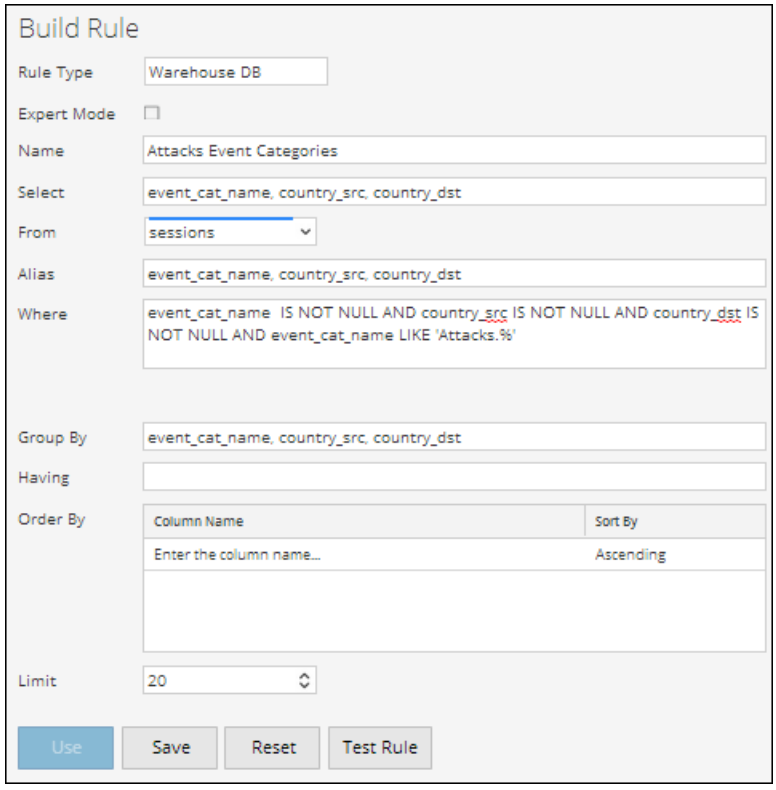


The following figure shows the result set of the All Event Categories rule.

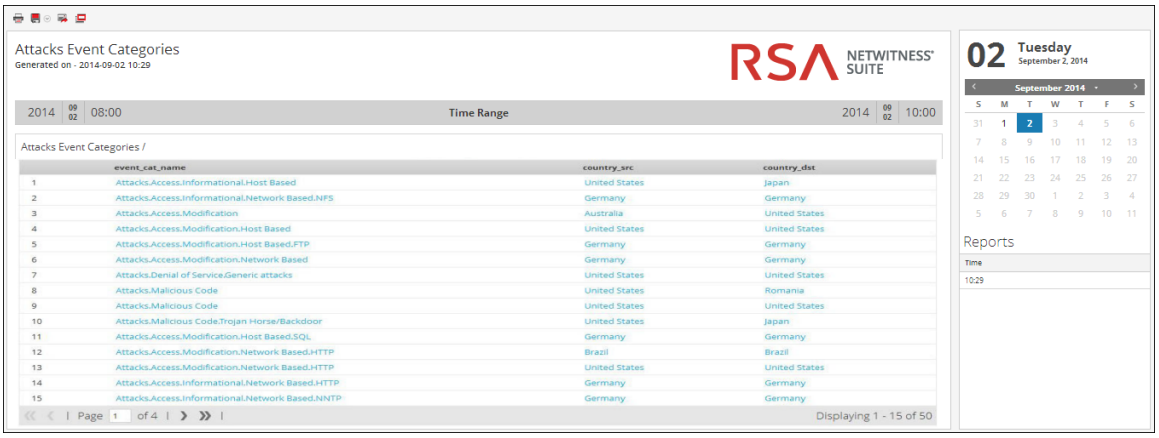


Attacks Event Categories Report

This rule fetches the event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose event category name like 'Attacks.%'.

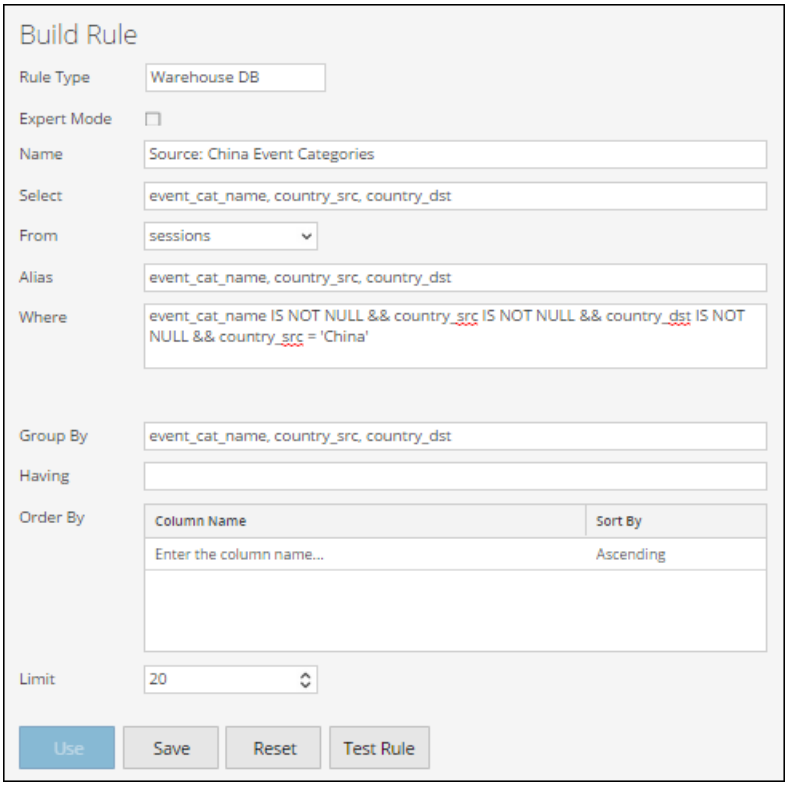


The following figure shows the result set of the Attacks Event Categories rule.

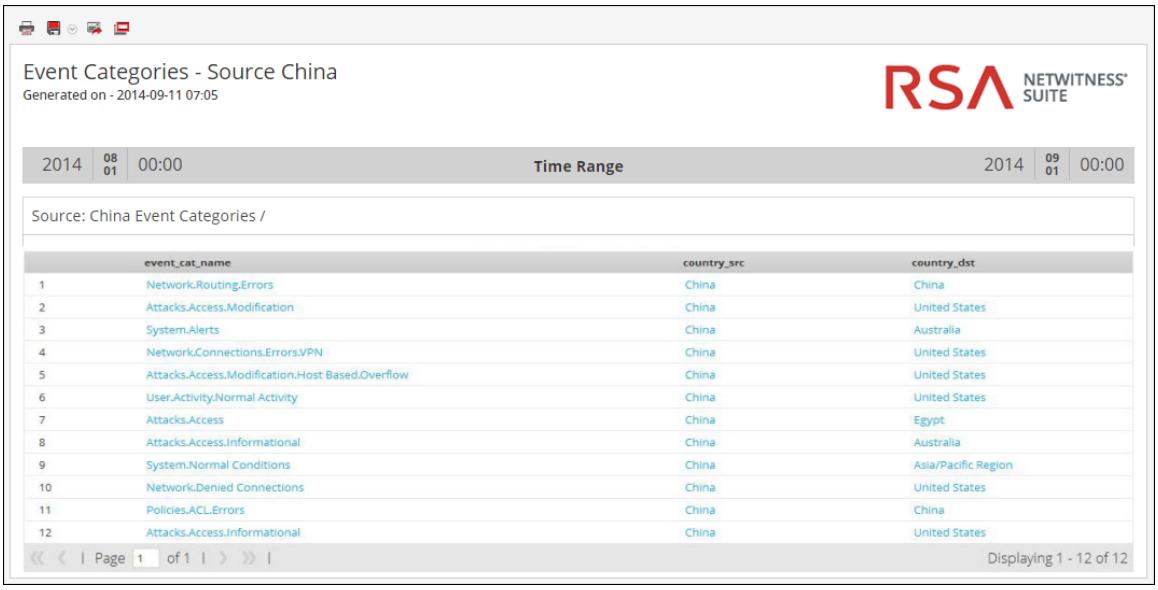


Source: China Event Categories Report

This rule fetches the event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose source country is 'China'.



The following figure shows the result set of the Source: China Event Categories rule.



Event Categories - Source China
Generated on - 2014-09-11 07:05

RSA NETWITNESS SUITE

2014 | 08 01 | 00:00 | Time Range | 2014 | 09 01 | 00:00

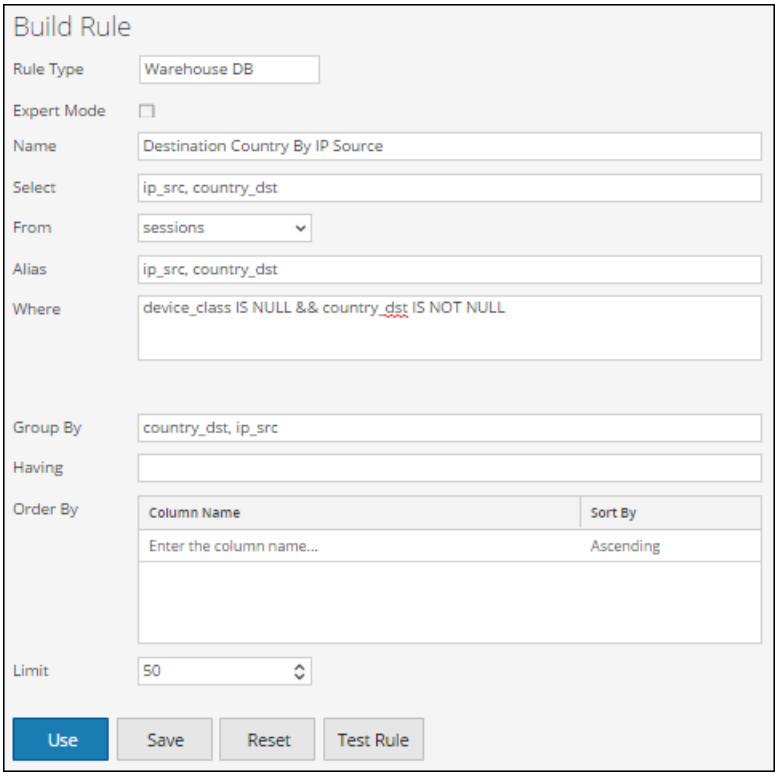
Source: China Event Categories /

	event_cat_name	country_src	country_dst
1	Network.Routing.Errors	China	China
2	Attacks.Access.Modification	China	United States
3	System.Alerts	China	Australia
4	Network.Connections.Errors.VPN	China	United States
5	Attacks.Access.Modification.Host Based.Overflow	China	United States
6	User.Activity.Normal Activity	China	United States
7	Attacks.Access	China	Egypt
8	Attacks.Access.Informational	China	Australia
9	System.Normal Conditions	China	Asia/Pacific Region
10	Network.Denied Connections	China	United States
11	Policies.ACL.Errors	China	China
12	Attacks.Access.Informational	China	United States

Page 1 of 1 | Displaying 1 - 12 of 12

IP Source and Destination Event Categories Report

This rule fetches the IP address of source and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose destination country is NOT NULL.



Build Rule

Rule Type: Warehouse DB

Expert Mode: ☐

Name: Destination Country By IP Source

Select: ip_src, country_dst

From: sessions

Alias: ip_src, country_dst

Where: device_class IS NULL && country_dst IS NOT NULL

Group By: country_dst, ip_src

Having:

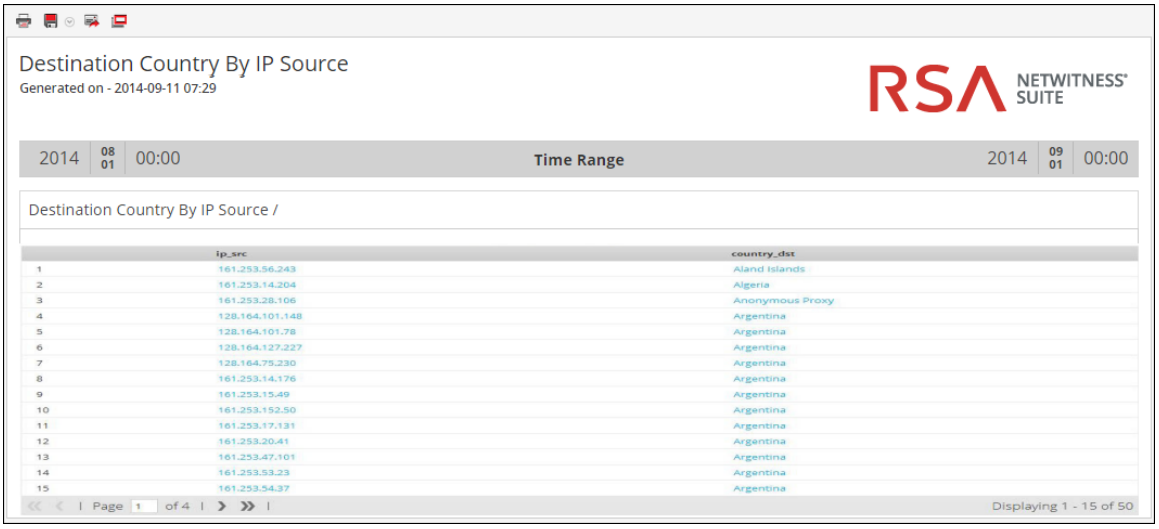
Order By:

Column Name	Sort By
Enter the column name...	Ascending

Limit: 50

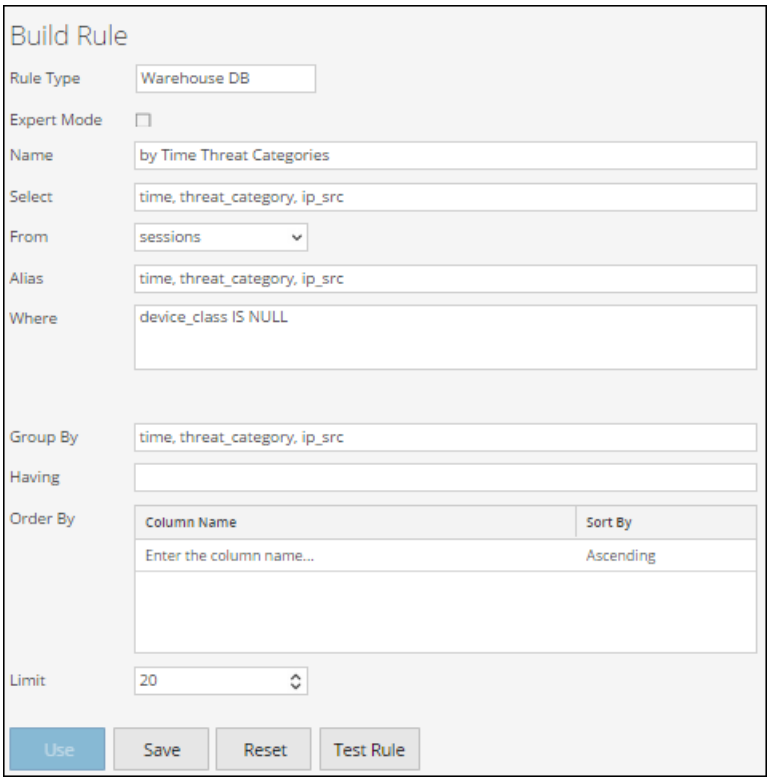
Use | Save | Reset | Test Rule

The following figure shows the result set of the IP Source and Destination Event Categories rule.



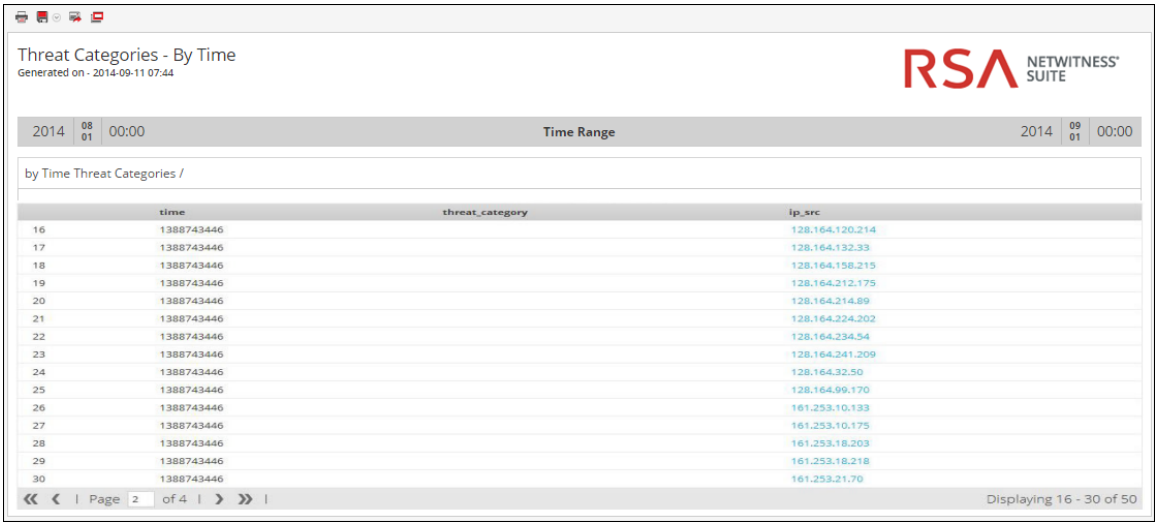
by Time Threat Categories Report

This rule fetches the threat category events, the time the log or event was ingested into Log Decoder/Decoder, and the source IP addresses from the **sessions**table by defining alias names (temporary column names) for each of these fields to be fetched from the table.



The following figure shows the result set of the by Time Threat Categories rule. The time displayed in the time field is the UNIX time (For example, 1388743446).

Note: In the "Select" clause the syntax would be "UNIX time" to convert to UTC time in report. For example, you can use the Epoch time converter tool to convert UNIX time (1388743446) to UTC (Coordinated Universal Time) (1/3/2014 3:34:06 PM).



Threat Categories - By Time
Generated on - 2014-09-11 07:44

RSA NETWITNESS SUITE

2014	08 01	00:00	Time Range	2014	09 01	00:00

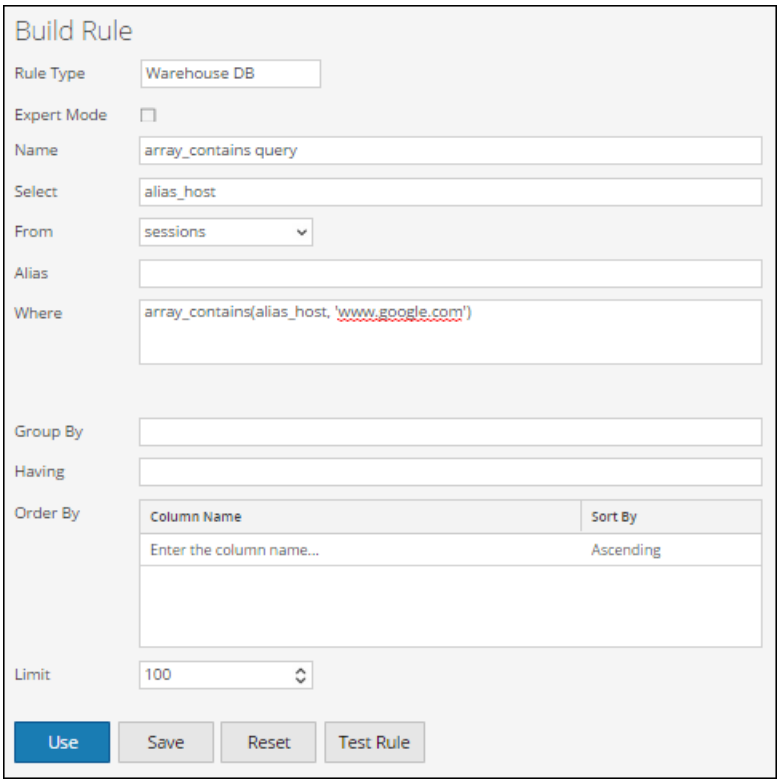
by Time Threat Categories /

	time	threat_category	ip_src
16	1388743446		128.164.120.214
17	1388743446		128.164.132.33
18	1388743446		128.164.158.215
19	1388743446		128.164.212.175
20	1388743446		128.164.214.89
21	1388743446		128.164.224.202
22	1388743446		128.164.234.54
23	1388743446		128.164.241.209
24	1388743446		128.164.32.50
25	1388743446		128.164.99.170
26	1388743446		161.253.10.133
27	1388743446		161.253.10.175
28	1388743446		161.253.18.203
29	1388743446		161.253.18.218
30	1388743446		161.253.21.70

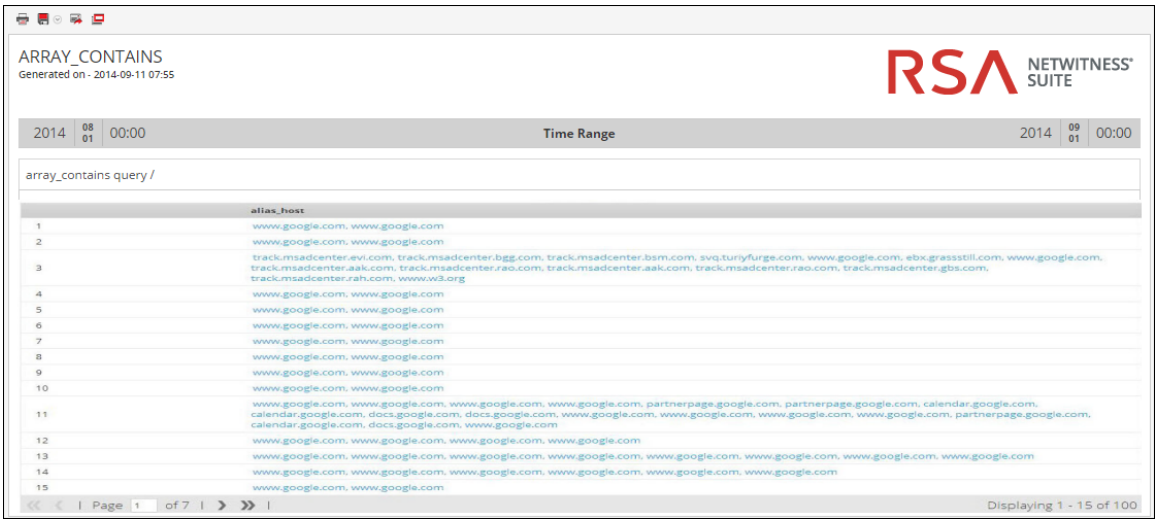
« ‹ | Page 2 of 4 | › » | Displaying 16 - 30 of 50

Array Query Report

This rule fetches an array of alias host names from the **sessions** table which contains the value 'www.google.com'.



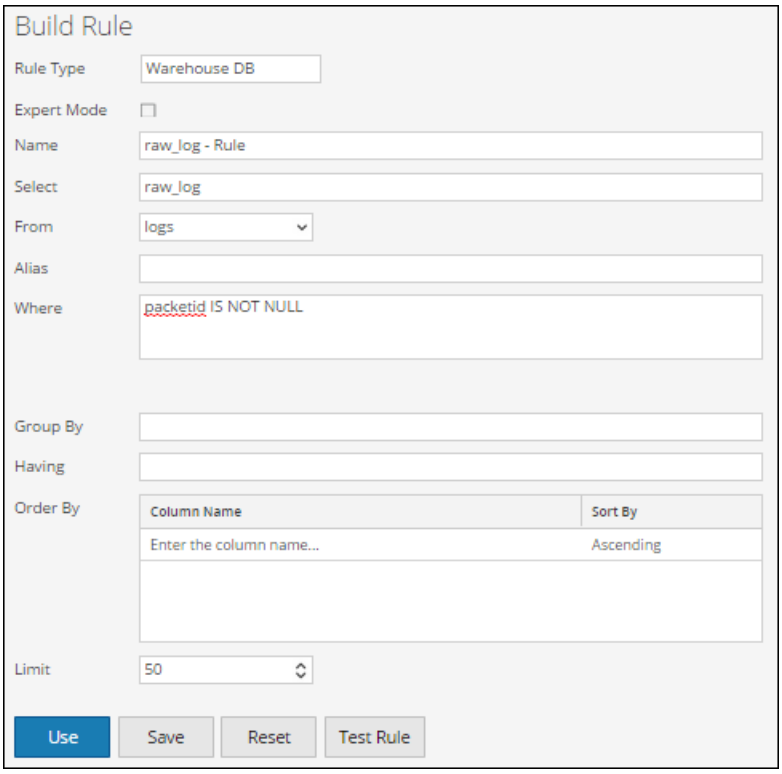
The following figure shows the result set for querying an array from sessions.



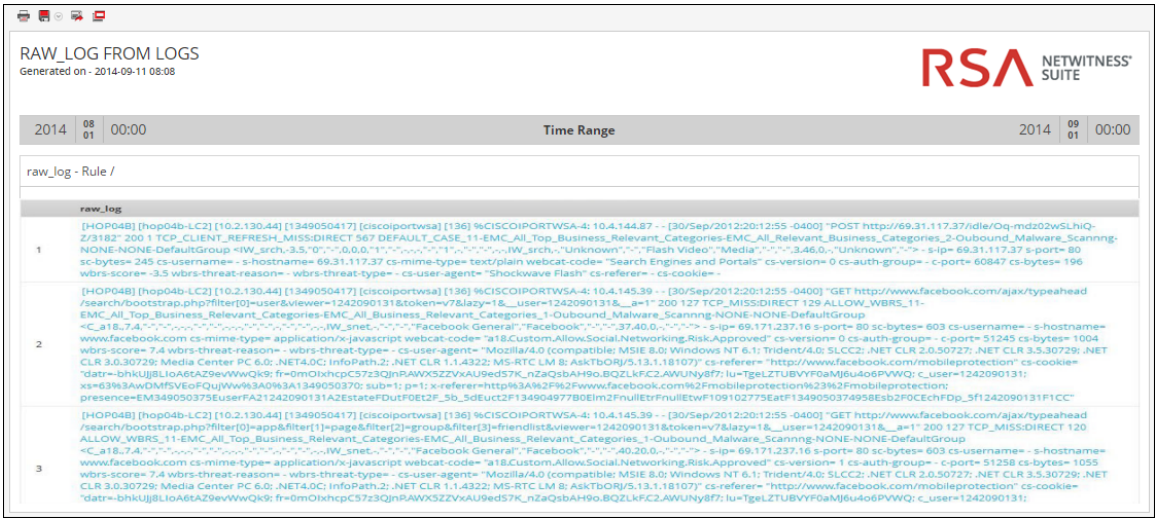
Raw Log Query Report

Raw logs can be queried either from the logs or sessions table.

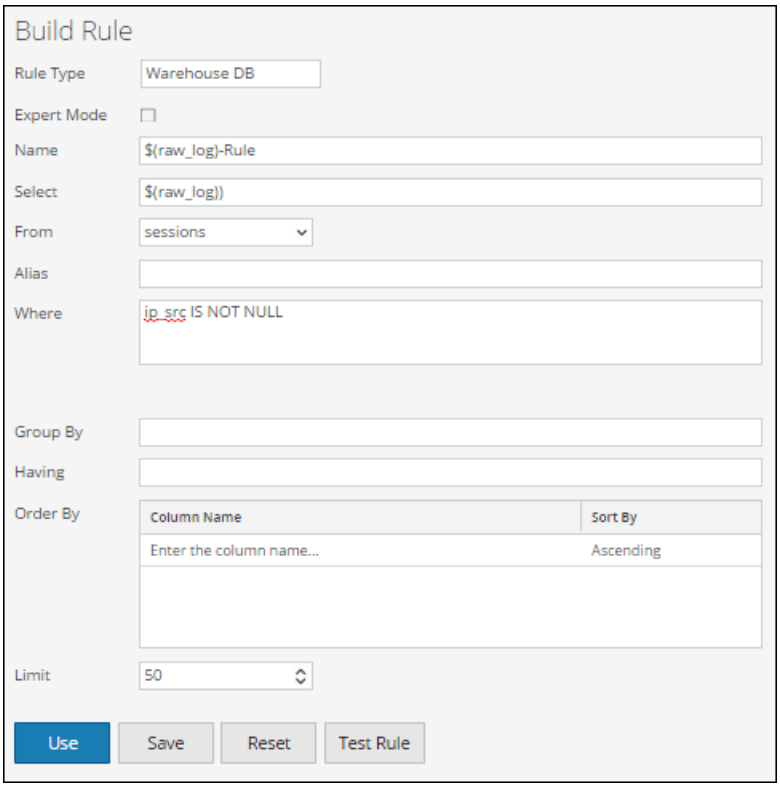
This rule uses **raw_log** as a meta for querying raw log from logs whose packet ID is NOT NULL.



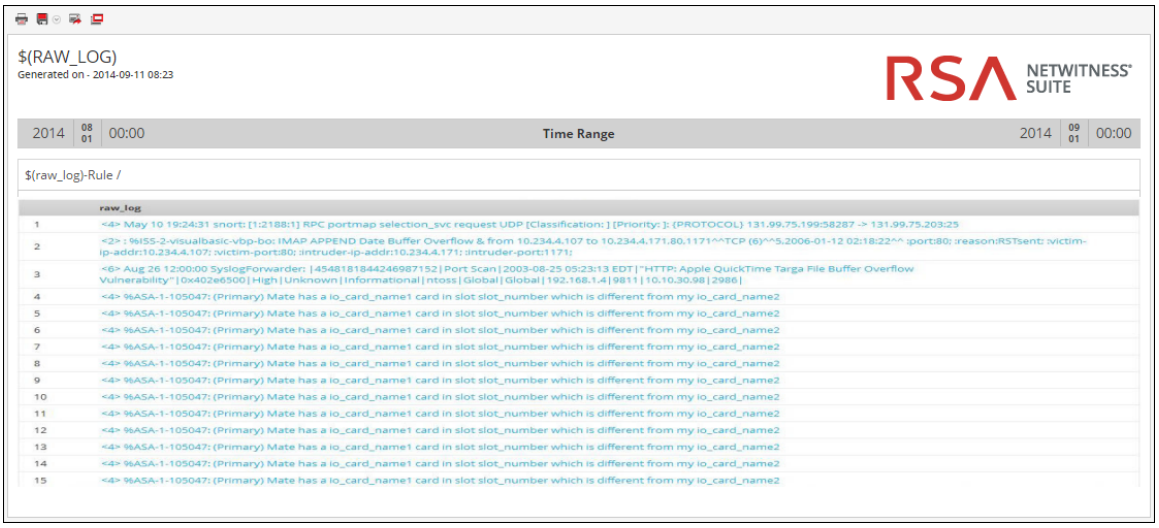
The following figure shows the result set for querying raw logs from logs.



This rule uses **${raw_log}** as a meta for querying raw log from sessions whose source IP address is NOT NULL.



The following figure shows the result set for querying raw logs from sessions.

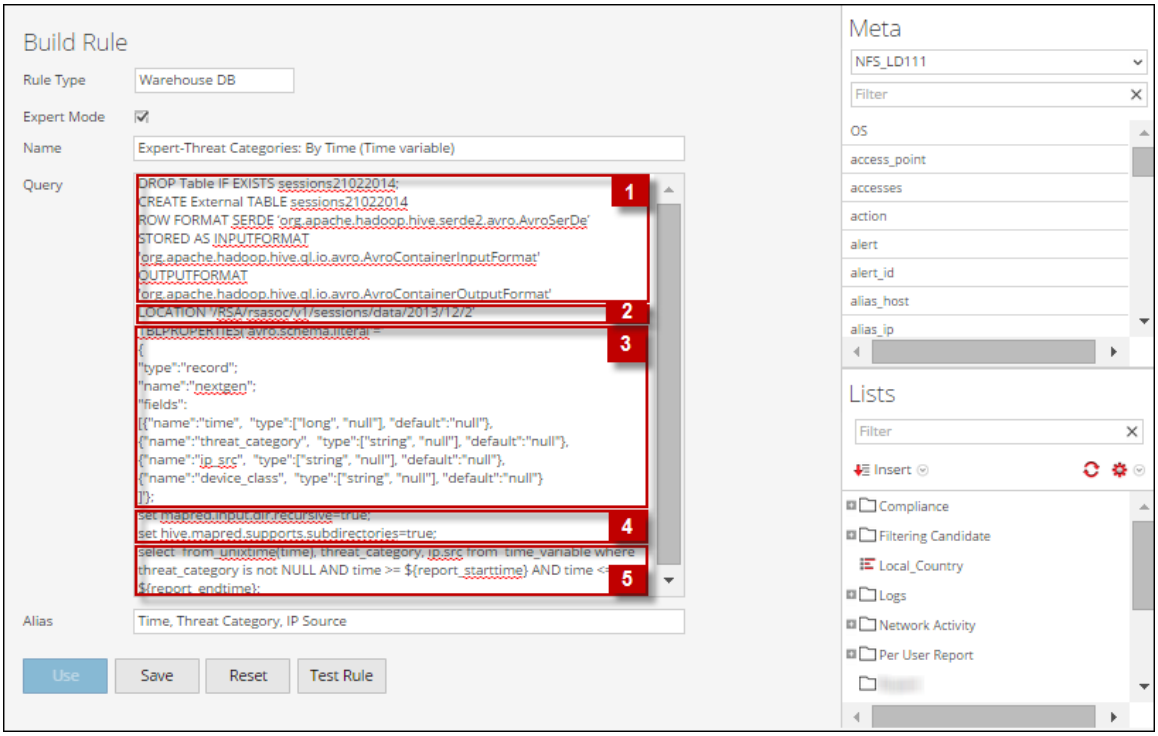


Warehouse DB Advanced Rules Syntax

The section explains the advanced rules query syntax and examples.

General Syntax of an Advanced Rule

The following figure shows how to define an advanced query.



The following syntax is an example of an advanced query:

```
DROP Table IF EXISTS sessions21022014;

CREATE External TABLE sessions21022014

ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.avro.AvroSerDe'

STORED AS INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2'

TBLPROPERTIES('avro.schema.literal'='
 {

"type":"record";
```

```
"name":"nextgen";
"fields":
 [
 {"name":"time",  "type":["long", "null"],
"default":"null"},
{"name":"threat_category",  "type":["string", "null"],
"default":"null"},
{"name":"ip_src",  "type":["string", "null"],
"default":"null"},
{"name":"device_class",  "type":["string", "null"],
"default":"null"}
 ]
 '};
set mapred.input.dir.recursive=true;
set hive.mapred.supports.subdirectories=true;
```

select `from_unixtime(time), threat_category, ip.src` from `time_variable` where `threat_category` is not `NULL` and `time >= ${report_starttime}` and `time <= ${report_endtime};`

Note: Reporting Engine treats a line beginning with <hyphen> <hyphen> as a comment in Expert Warehouse Rule.
For example,

```
set mapred.input.dir.recursive=true;
-- This is an Expert comment
 set hive.mapred.supports.subdirectories=true;
```

The general syntax of an advanced query is as explained below:

1. Drop and create an external table, and then format the row:

   Firstly, we drop the table, if the table already exists and create an external table **sessions21022014**

   ```
   DROP TABLE IF EXISTS sessions21022014
    CREATE EXTERNAL TABLE sessions21022014
   ```

   Note: You must create an external table only if you are using an other table. For example, if you are using an other table apart from **sessions21022014** then you must drop the table and create an external table.

Then, specify the row format as Avro.SerDe interface to instruct HIVE as to how a record is to be processed. Avro.SerDe allows you to read or write Avro data as HIVE tables and store them as input format and output format.

```
ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.avro.Avro.SerDe'
 STORED AS INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFo
rmat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputF
ormat'
```

2. Specify the HDFS location:
   Secondly, you must specify the HDFS location '/RSA/rsasoc/v1/sessions/data/2013/12/2' from where the data is queried before executing the HIVE statements.The location parameter specifies the data to be fetched depending on the date input provided. This is a variable parameter hence you can fetch values depending on the date entered.
3. Define the table schema:
   Thirdly, you define the table schema by defining columns with a specific data type and default value as 'null'.

```
TBLPROPERTIES('avro.schema.literal'='
 {"type":"record";
 "name":"nextgen";
 "fields":
 [
 {"name":"ip_src",  "type":["string", "null"],
"default":"null"}
 ]
 '};
```

4. Import data from directory which contains sub directories:
   Then, you must enable HIVE to recursively scan all sub-directories and fetch all the data from all sub-directories.

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

5. Fetch data from the HIVE table:
   Once you execute all the above statements, you can query the database with the HIVE query **select** clause to fetch the data from the HIVE table.

The following examples illustrate advanced rules in the expert mode:

- Hourly, daily, weekly, and monthly report
- Table partition based on location report
- Join logs and sessions based on unique_id report
- List report
- Parameterized report
- Partition based table with multiple locations
- Automated partition using custom function (10.5.1 onwards)

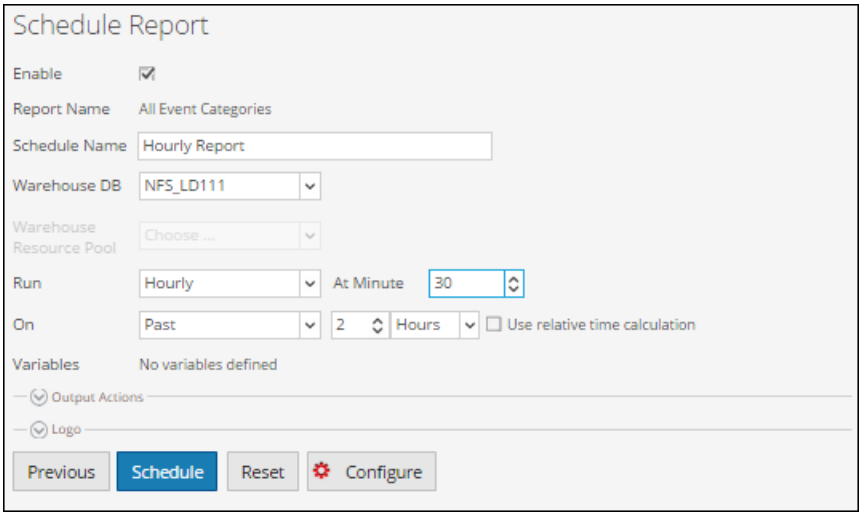
Hourly, Daily, Weekly, and Monthly Report

In these example rules, you can create various reports for December 02, 2013 (as in the below figure). The date variable in the LOCATION statement can be altered, depending on which you can create an hourly, daily, weekly, and monthly report.

Hourly Report

In this example rule, you can create an houly report for December 02, 2013. The LOCATION statement can be altered to generate an hourly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2' - the date input (2013/12/2) indicates year/month/day. The entire data for 02 December, 2013 is retrieved using this location statement.

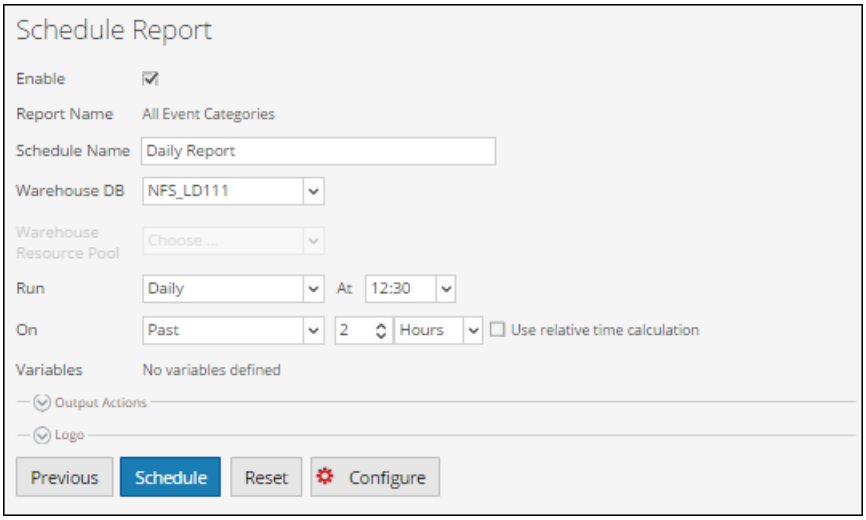


The result set of this query would be an hourly report.

Daily Report

In this example rule, you can create a daily report for December 2013. The LOCATION statement can be altered to generate a daily report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - the date input (2013/12) indicates year/month. The entire data for December, 2013 is retrieved using this location statement.

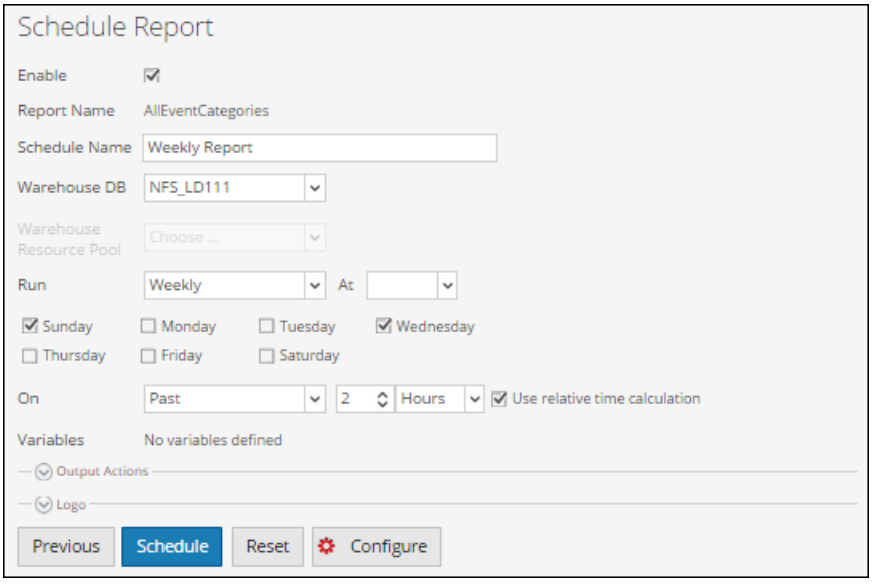


The resultset of this query would be a daily report.

Weekly Report

In this example rule, you can create a weekly report for December 2013. The LOCATION statement can be altered to generate a weekly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - the date input (2013/12) indicates year/month. The entire data for December, 2013 is retrieved using this location statement.

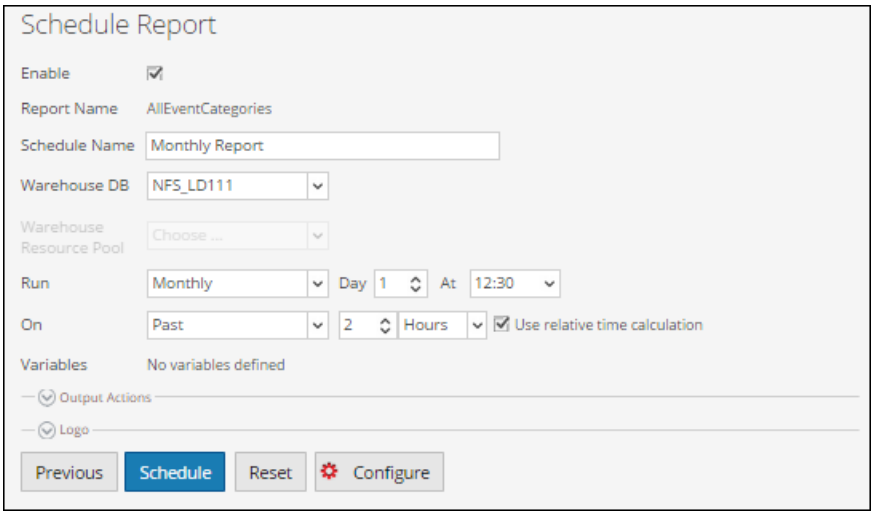


The result set of this query would be a weekly report.

Monthly Report

In this example rule, you can create a monthly report for the year 2013. The LOCATION statement can be altered to generate a monthly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013' - the date input (2013) indicates year. The entire data for the year 2013 is retrieved using this location statement.



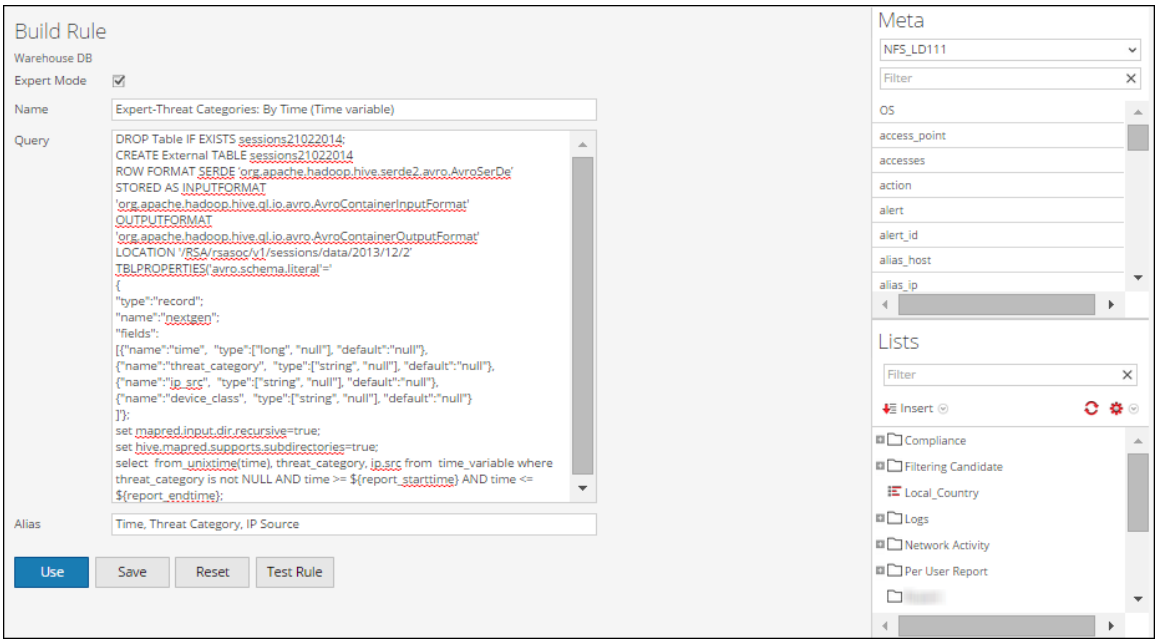
The result set of this query would be a monthly report.

For more information on LOCATION definition, see **Specify the HDFS location** in the **"General Syntax of an Advanced Rule"** section.

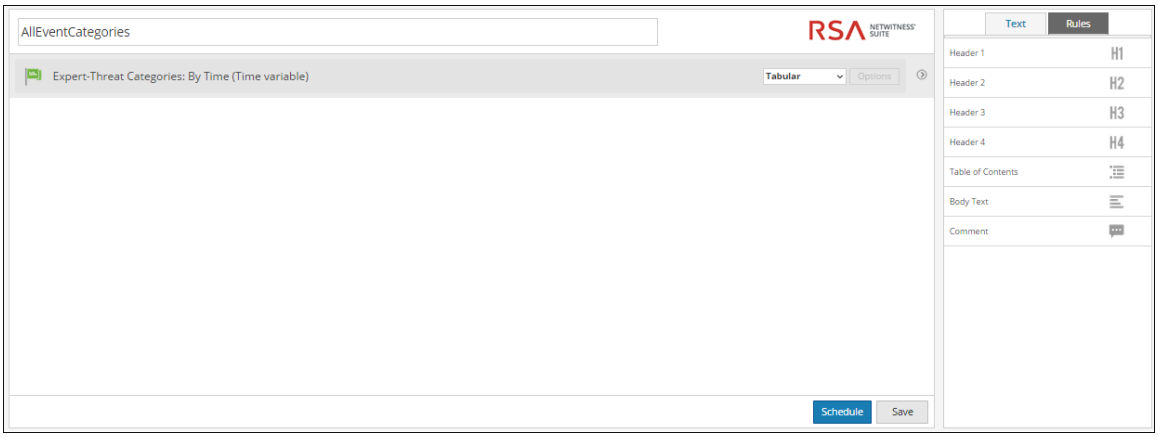
You must perform the following steps in sequence to view the resultset of an advanced rule:

1. Define an Advanced Rule
2. Add an advanced rule to a Report
3. Schedule a Report
4. View a scheduled Report

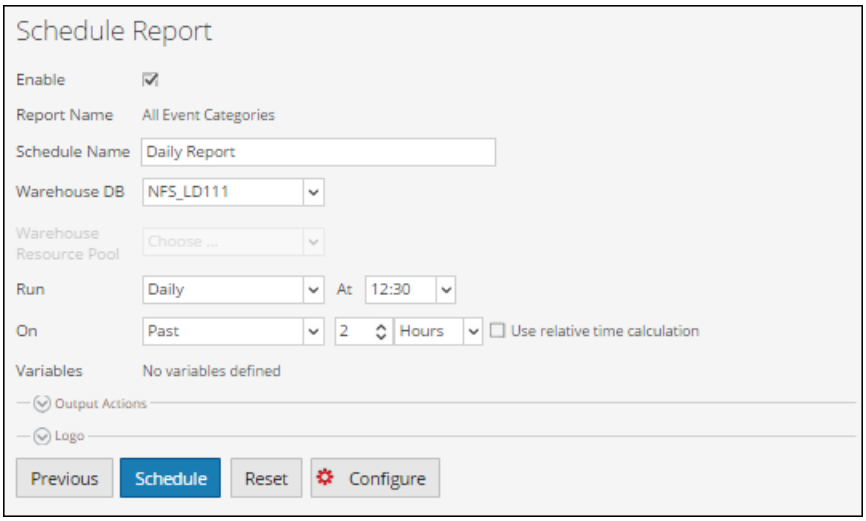
The following figure shows how to define an advanced rule.



The following figure shows how to add an advanced rule to a report (For example, **AllEventCategories**).



The following figure shows how to schedule a daily report.



If you want to generate a report for a specific time range, you need to manually define the time range in the query using the following two variables:

`${report_starttime}` - The starting time of the range in seconds.
`${report_endtime}` - The ending time of the range in seconds.

For example, `SELECT from_unixtime(time), threat_category, ip.src FROM time_variable WHERE threat_category is not NULL AND time >= ${report_starttime} AND time <= ${report_endtime};`

The following figure shows the result set of scheduling a daily report.

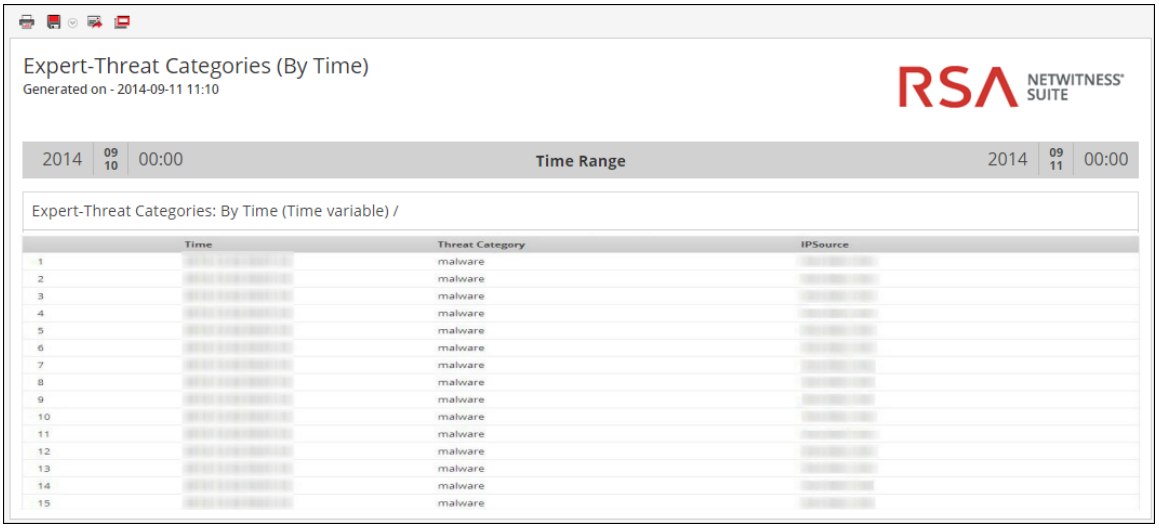
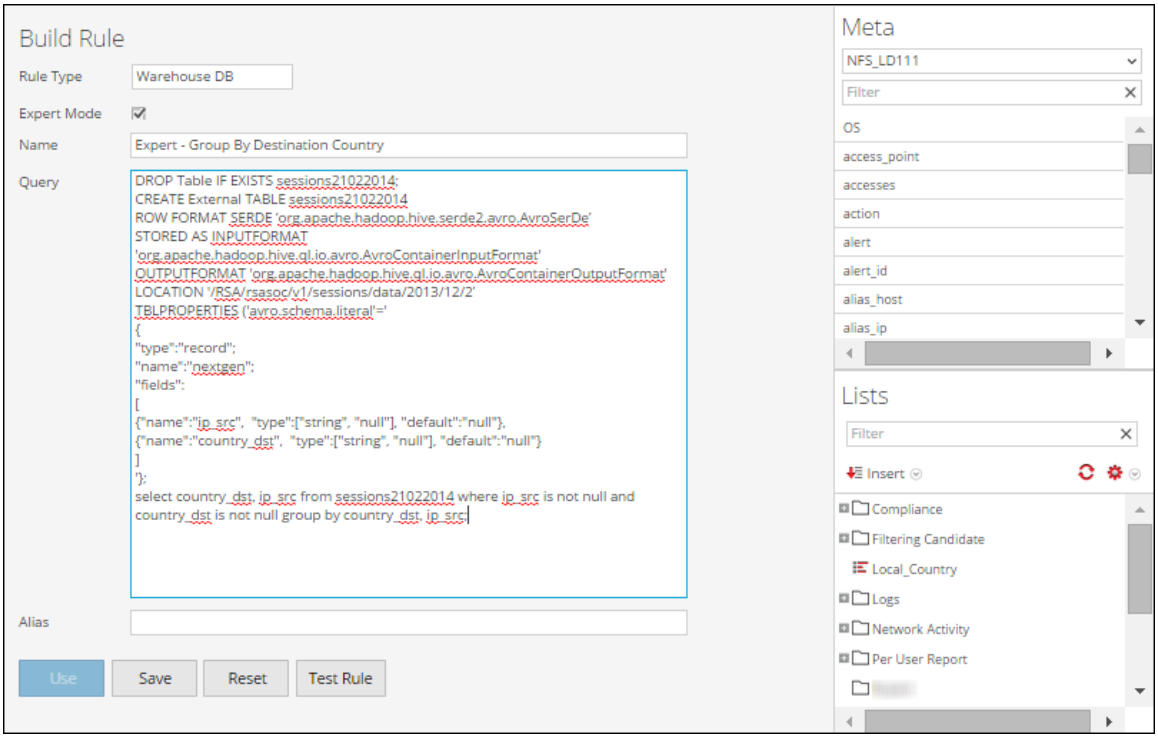


Table Partition Based on Location Report

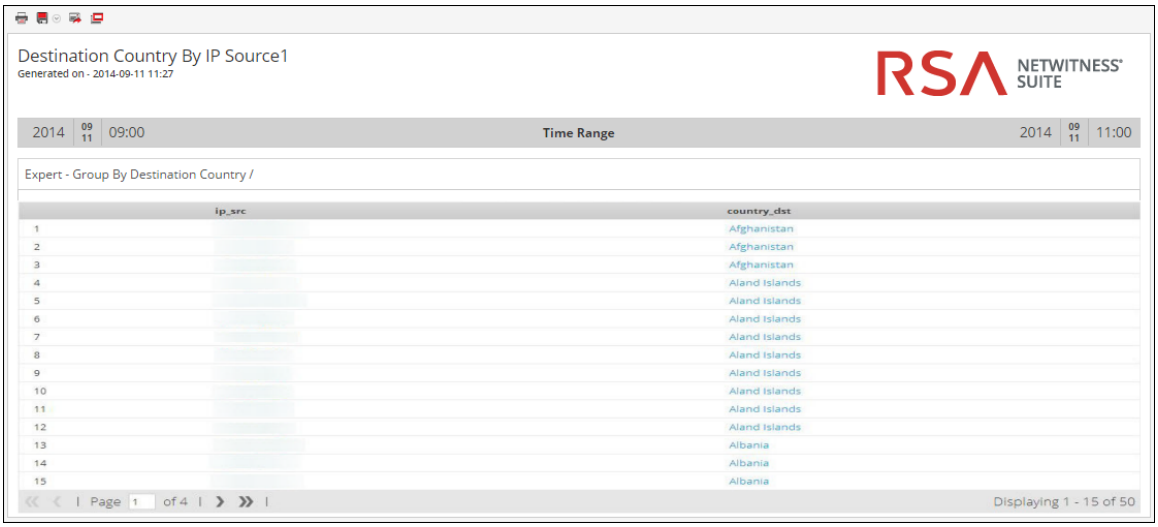
In this example rule, you can create a table partition based on location. Each table can have one or more partition keys which determines how the data is stored. For example, a country_dst of type STRING and an ip_src of type STRING. Each unique value of the partition keys defines a partition of the table.

In the example provided, we execute a HIVE query to fetch destination country and IP address of source from the sessions05032014 table and group the result set by these fields.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see "General Syntax of an Advanced Rule" section.



The following figure shows the result set of creating a table partition based on location report.

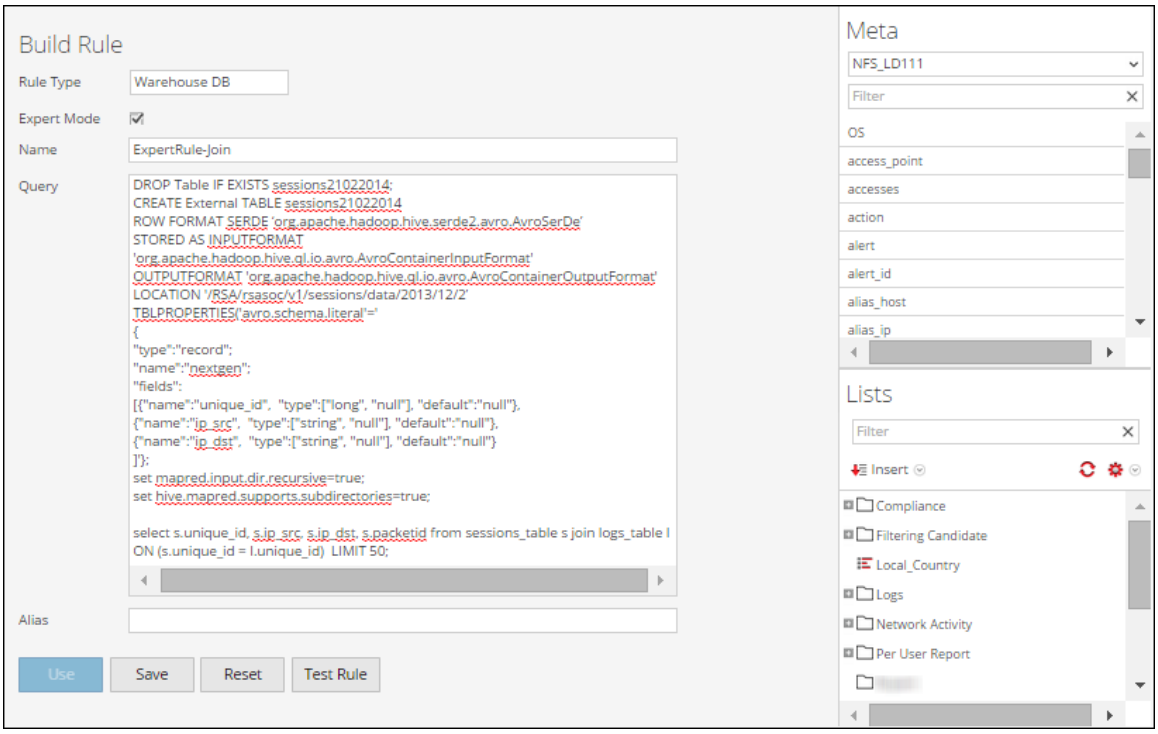


Join Logs and Sessions Based on unique_id Report

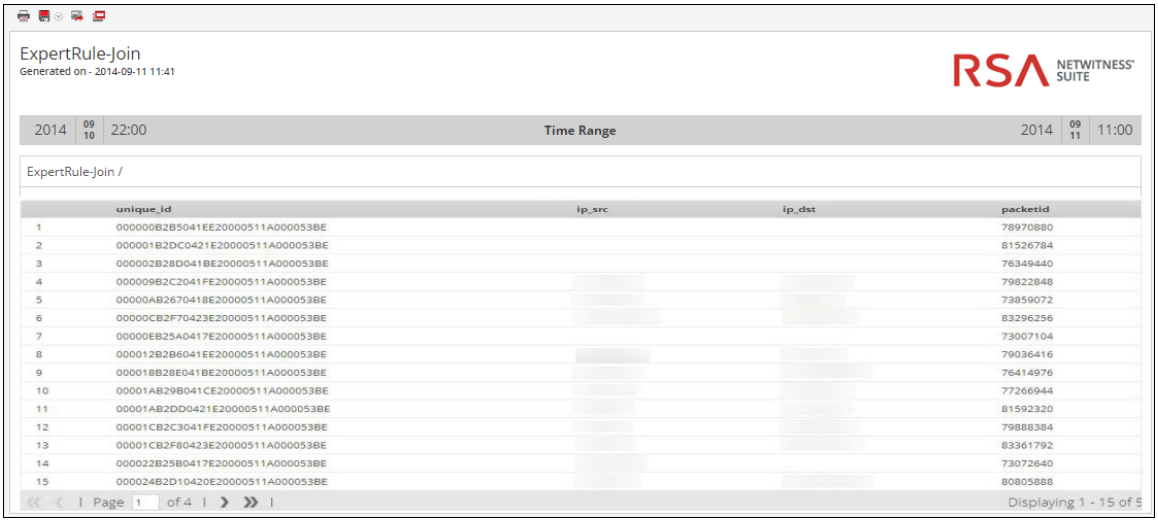
In this example rule, you can create a rule to join logs and sessions table to fetch unique_id, IP address of source and destination, and packet ID based on unique_id.

In the example provided, we execute a HIVE query to fetch certain fields from both the sessions_table and logs_table by performing a join based on the 'unique_id' field.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the **"General Syntax of an Advanced Rule"** section.



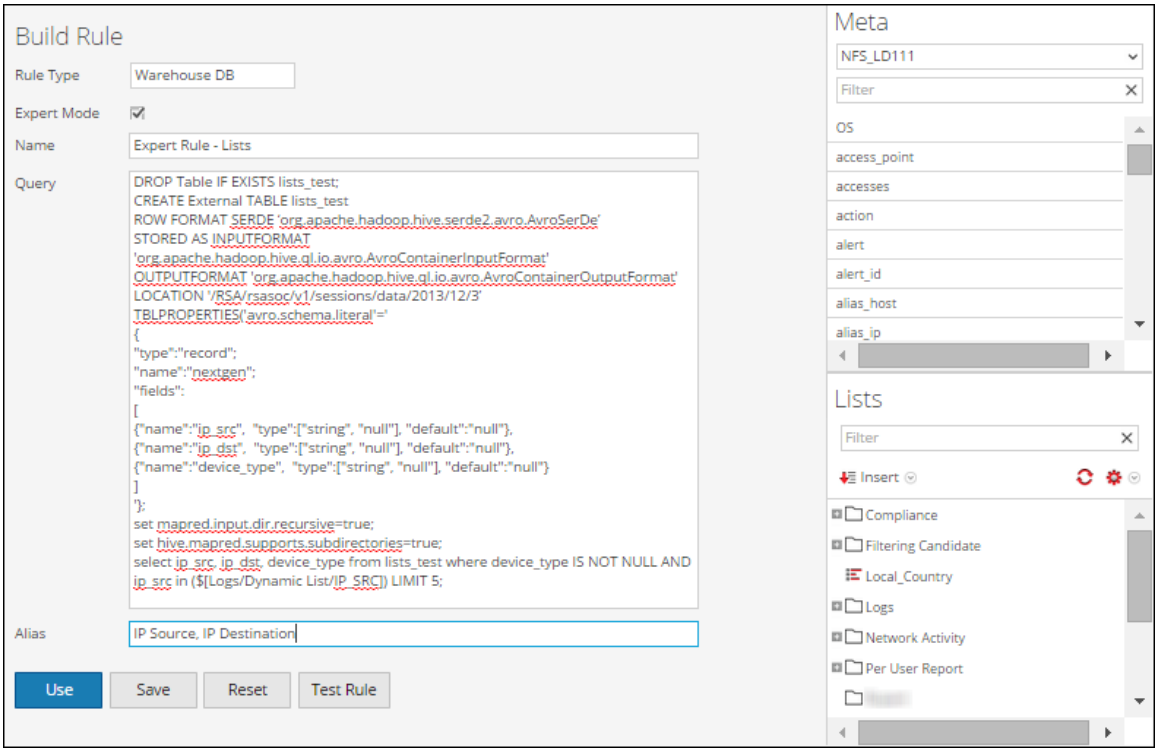
The following figure shows the result set of joining logs and sessions table based on unique_id.



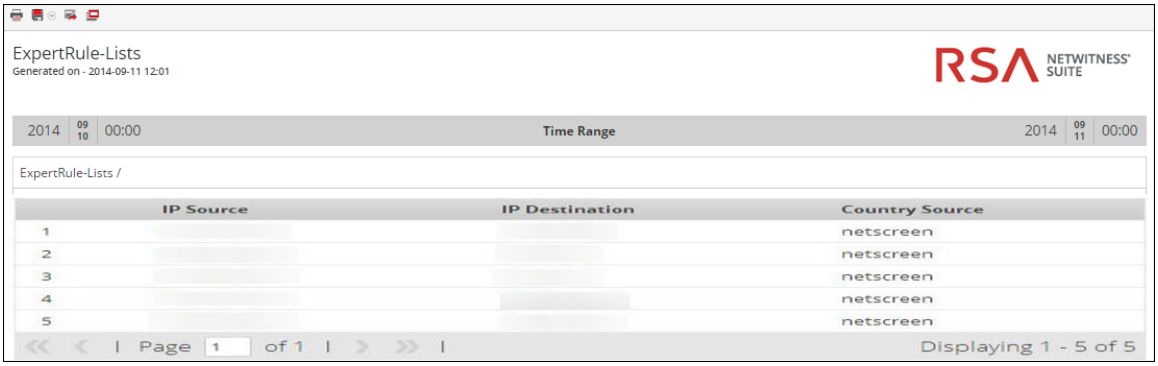
List Report

In this example rule, you can create a List report to fetch IP address of source and destination, and device type from the **lists_test** table where device type is not null and IP address of source is fetched from the appropriate event list.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the "General Syntax of an Advanced Rule" section.



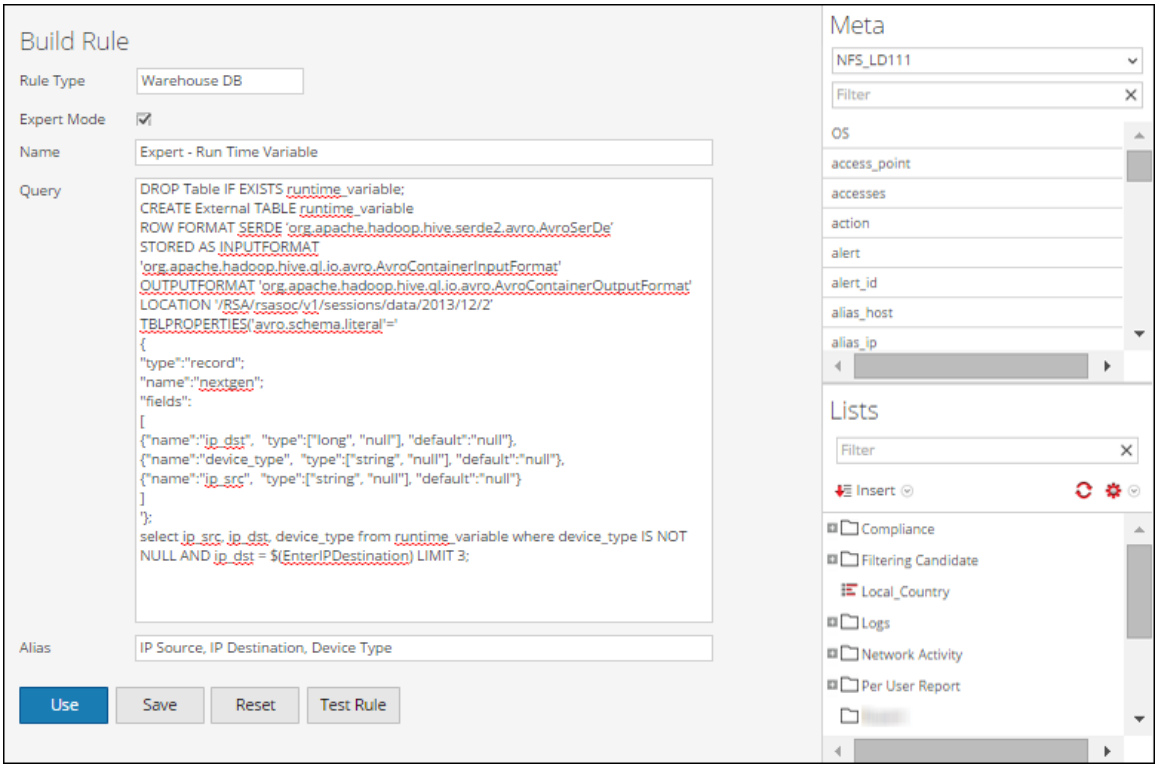
The following figure shows the result set of executing a list report.



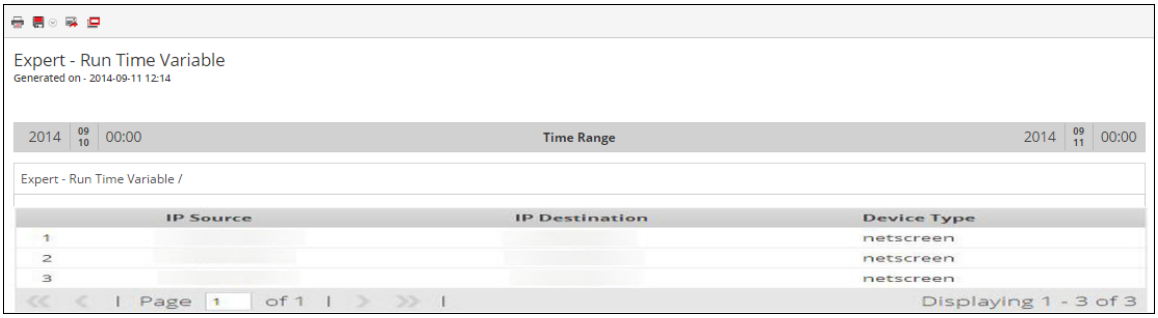
Parameterized Report

In this example rule, you can create a rule to fetch IP addresses of source and destination, and device type from the **runtime_variable** table based on the specified run time variable `${EnterIPDestination}`. At run time, you are prompted to enter a value for the IP address of destination ip_dst. Based on the value entered, the result set is displayed.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the "General Syntax of an Advanced Rule" section.



The following figure shows the result set of executing a parameterized report.



Partition Based Table with Multiple Locations

The following is an example of partition based table with multiple locations:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
 {"name":"sessionid", "type":["null", "long"],
"default" : null},
 {"name":"time", "type":["null", "long"], "default"
: null}
 ]}'
 )
 STORED AS
 INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerInpu
tFormat'
 OUTPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutp
utFormat';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
 SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time
>= ${report_starttime} AND time
 <= ${report_endtime};
```

The partition based table with multiple location is as explained below:

1. Enable HIVE to recursively scan all sub-directories and read all the data from the sub-directories.

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

2. Drop and create an external table, and then format the rows:

```
DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
 {"name":"sessionid", "type":["null", "long"],
"default" : null},
 {"name":"time", "type":["null", "long"],
"default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerIn
putFormat'
 OUTPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerOu
tputFormat';
```

Note: You must create an external table only if you are using any other table. For example, if you are using any other table apart from **AVRO_COUNT** then you must drop the table and create an external table.

Note: Points to remember when you create a table:
- Dropping a 'non-external' table deletes the data.
- The table is partitioned on a single column called partition_id and this is the standard column for Reporting Engine.
- The default value of any column is null as the AVRO file may not contain the specified column.
- The column names should be in the lowercase as HIVE is case insensitive but AVRO is case sensitive.
- You must specify **avro.schema.literal** in the *SERDEPROPERTIES* .

For more information on the "rule syntax", refer to *Apache HIVE*.

3. Add partitions:

Once you define a table, you must specify the HDFS locations from where the data needs to be queried before you execute the HIVE statements.The location parameter specifies the data to be fetched depending on the specified date. The data is spread across multiple locations or directories in HDFS. For each location you need to add a partition with unique values assigned to the partition column. The locations can be any directory in the HDFS

```
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_
id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
```

Note: HIVE reads each file in these locations as AVRO. Incase if there is a non-AVRO file available in one of these locations then the query may fail.

4. Run the query

```
SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE
time >= ${report_starttime} AND time
 <= ${report_endtime};
```

When a table is created, you can execute specific queries to filter the data. For example, after you create the table you can filter the data as shown in the below examples:

Sessions with a specific Source IP Address:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_
starttime} AND time <= ${report_endtime}  AND ip_
src = '127.0.0.1';
```

Group by based on user destination:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_
starttime} AND time <= ${report_endtime}  GROUP BY
usr_dst;
```

Automated Partition using Custom function

In 10.5.1, you can use the custom function to automate the addition of partitions to a user defined table in the expert mode.

General syntax

```
RE WH CUSTOM ADDPARTITIONS(table, namespace, rollup,
[starttime, endtime])
```

The following table describes the custom function syntax:

S.No	Name	Description
1	table	The table name for which the partition has to be added.
2	namespace	The namespace can be sessions or logs.

S.No	Name	Description
3	rollup	This value determines the level of directory path to be included in partitions. The value can be HOUR, DAY, or MINUTE. If Warehouse Connector is configured for Day rollup, setting this value as HOUR produces ZERO results. The number and location of each partition is based on time range used to run the rule and the rollup value.
4	(Optional) starttime, endtime	To generate partitions for a specific time range other than the time range mentioned in the rule, you must specify the starttime and endtime in **Epoch Seconds**. **Note:** Expressions are not supported for the starttime and endtime.

The custom function is invoked when Reporting Engine executes the rule either during test rule or scheduled report. While running a expert rule, whenever Reporting Engine identifies the function declaration, it extracts the required arguments and insert *n* number of ADD PARTITION HiveQL statements and executes them on the Hive Server.

The location and directory structure is determined by the argument passed in the rule and the Hive datasource configuration in Reporting Engine. The number of partitions depends on the rollup specified and the time range used while executing the rule. For example, with the rollup as HOUR and the time range as PAST 2 Days results in 48 partitions for 48 Hours while with the rollup as DAY, Reporting Engine creates 2 partitions, one for each day.

The partition query is generated by the Syntax Template as set in Reporting Engine's Hive Configuration attribute AlterTableTemplate.

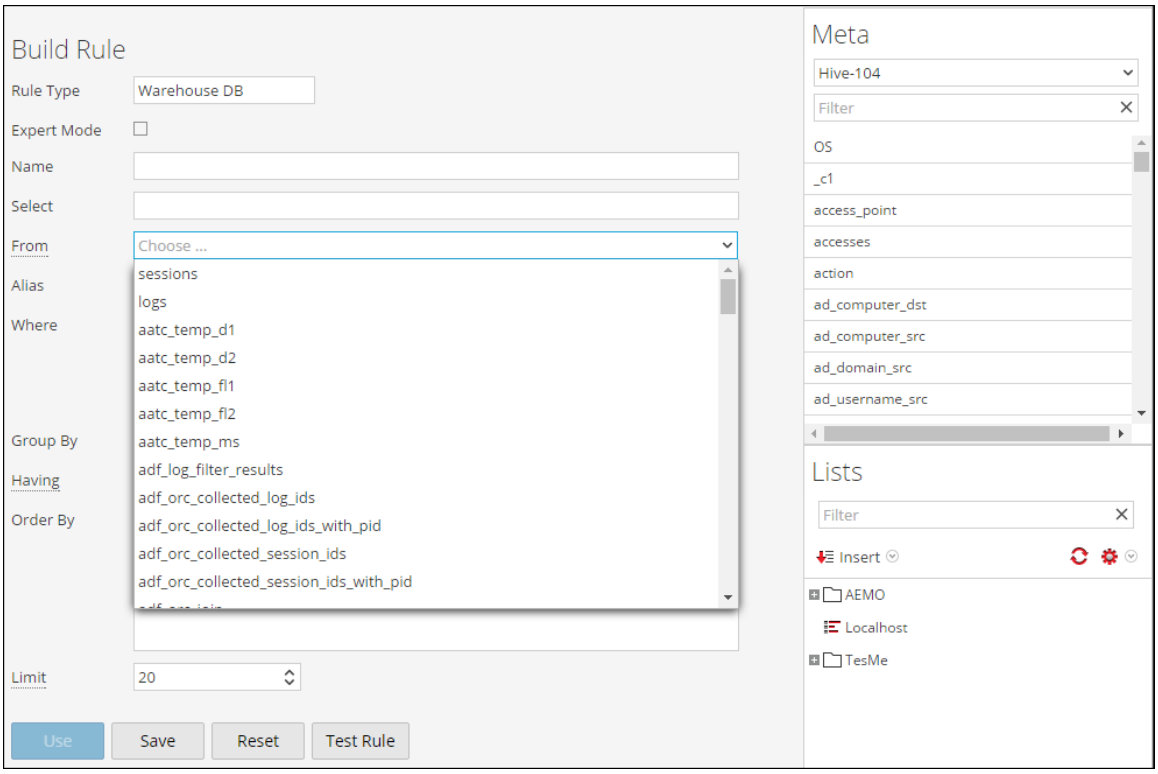
Note: By default, this function starts adding partitions to a table with partition id from 0 to N-1. Hence this requires that the table must be partitioned by single integer column named partition id.

The following is an example of automated partition using custom function:

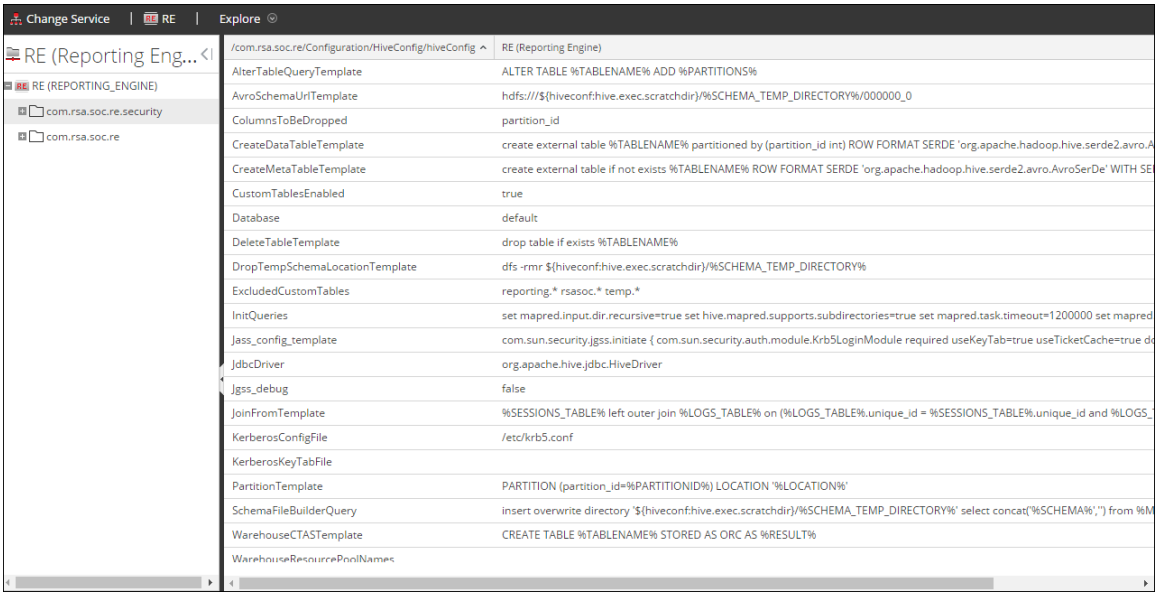
```
 set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;

CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
  "name": "my_record", "type": "record",
  "fields": [
  {"name":"sessionid", "type":["null", "long"],
"default" : null}
  ,{"name":"time", "type":[ "null" , "long"],
"default" : null}
  ,{"name":"unique_id", "type":["null", "string"],
"default" : null}
  ]}'
 )
 STORED AS
 INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerInpu
tFormat'
 OUTPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutp
utFormat';

RE_WH_CUSTOM_ADDPARTITIONS(AVRO_COUNT, 'sessions',
'DAY');
 SELECT COUNT(*) as TotalSessions FROM AVRO_COUNT
 WHERE time >= ${report_starttime} AND time <=
${report_endtime};
```

Creating Custom Tables Report

In 10.6.1, you can use and create Custom Tables on the Hive Server. Reporting Engine supports running queries on user defined tables and the ability to create a new table from a Single Rule output. When this feature is enabled in the Warehouse Rule Builder UI, user can see a list of custom tables available in Hive Server.



To enable this feature set **customTablesEnabled** to **TRUE** by navigating to **Reporting Engine -> Explore ->Hive Config**.



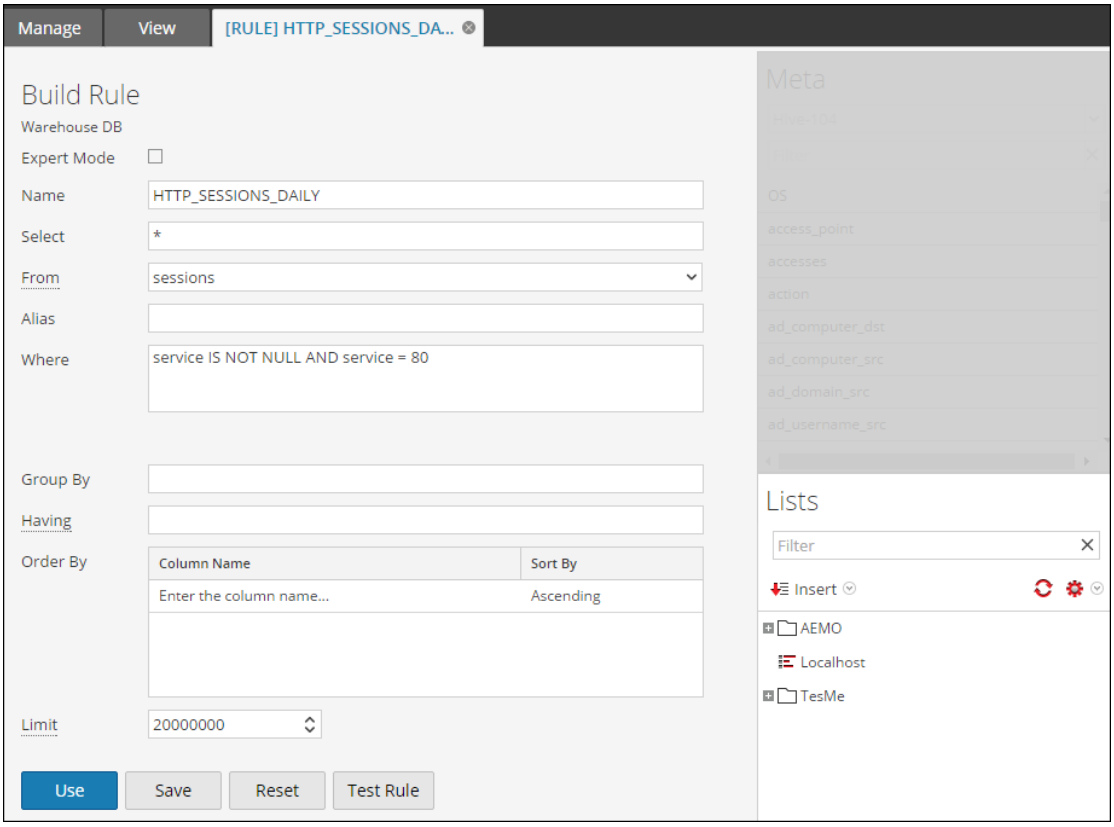
Creating Custom Table from Regular Rules

To schedule a report which contains a single SAW rule, a new text input with a **Warehouse CTAS Name** is added. The user can now specify a Custom Table name that will be created out of the output of the rule in Report.

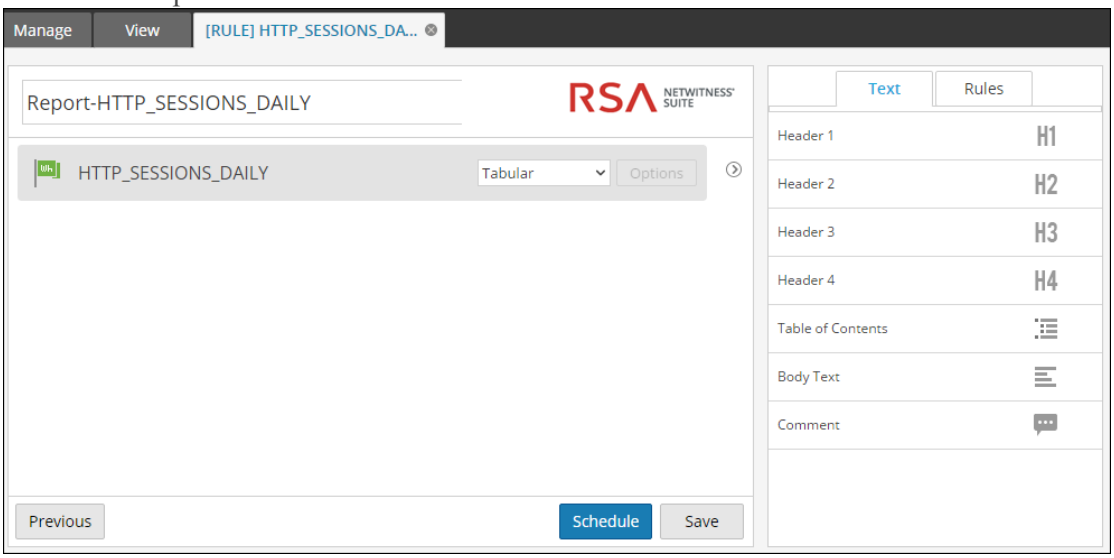
Note: This feature is available only if the Report contains a single SAW rule on the Schedule page. Otherwise, this option is hidden.

The process to use the feature is explained below:

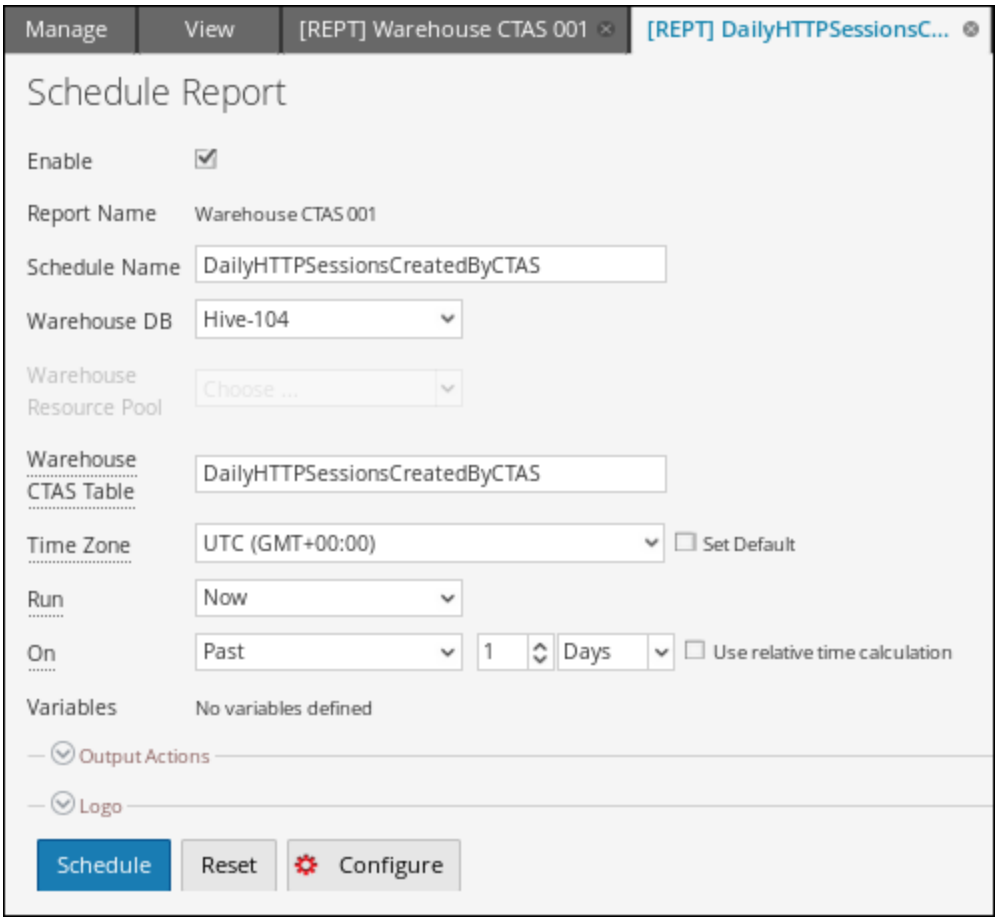
1. Create a rule to filter with data in SAW.



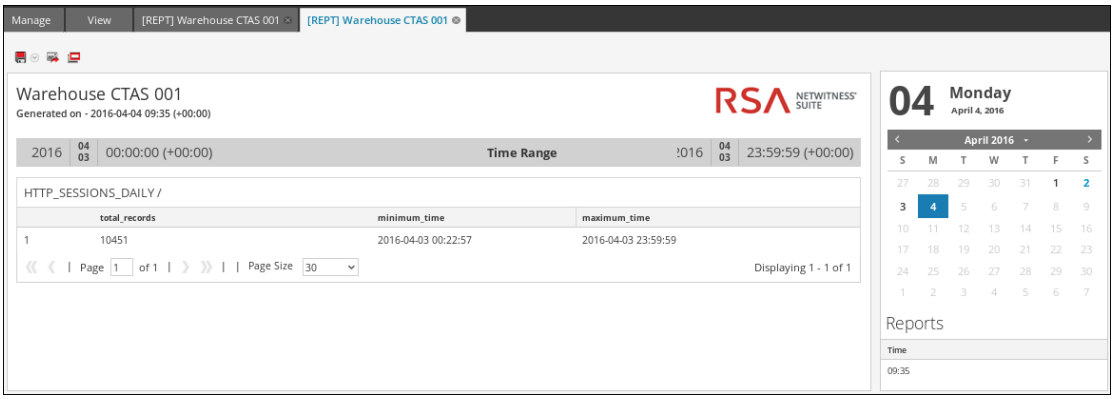
2. Create a Report with the above rule.



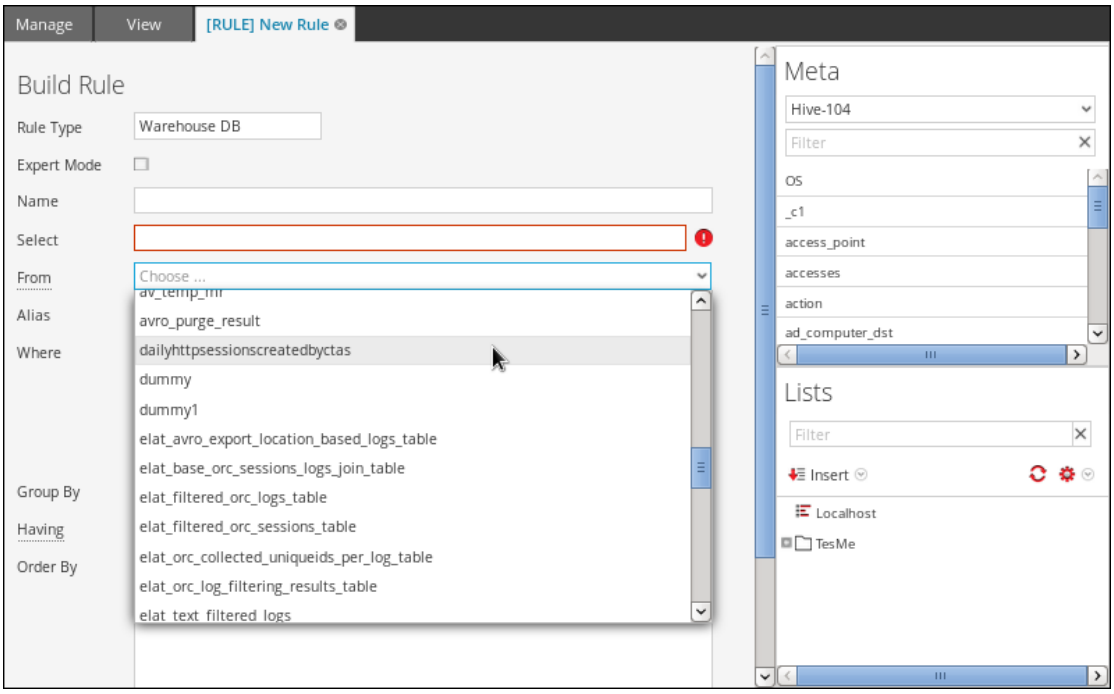
3. Create a Schedule and enter the CTAS Table Name.



4. Run the Report and Reporting Engine will create the Result Summary as below for the Schedule.



5. On the next schema refresh or restart of Reporting Engine, the CTAS Table is listed.


Manage
View
[RULE] New Rule
Build Rule
Rule Type
Warehouse DB
Expert Mode
Name
Select
From
Choose ...
Alias
Where
Group By
Having
Order By
avro_purge_result
dailyhttpsessionscreatedbyctas
dummy
dummy1
elat_avro_export_location_based_logs_table
elat_base_orc_sessions_logs_join_table
elat_filtered_orc_logs_table
elat_filtered_orc_sessions_table
elat_orc_collected_uniqueids_per_log_table
elat_orc_log_filtering_results_table
elat_text_filtered_logs
Meta
Hive-104
Filter
OS
_c1
access_point
accesses
action
ad_computer_dst
Lists
Filter
Insert
Localhost
TesMe

Task Scheduler for Warehouse Reporting

A task scheduler in a Hadoop cluster schedules the jobs consisting of tasks, and allocates specific resources to each job running in a cluster. By default, the task scheduler allocates equal number of resources to all the jobs. For example, if 10 jobs are running they will share resources of the cluster equally. However, you can configure the task scheduler to control the execution of the jobs such that one job runs faster than others by allocating more resources (pools or queues) to the job. This helps you prioritize to run a few reports over others.

Features

NetWitness Suite supports two task schedulers:

- Fair Scheduler (`org.apache.hadoop.mapred.FairScheduler`)
- Capacity Scheduler (`org.apache.hadoop.mapred.CapacityTaskScheduler`)

Fair Scheduler

This scheduler divides the total capacity of the cluster into logical pools. You can submit a job to any one of these pools. All the jobs submitted to a pool share the resources allocated to the pool only. Once a pool has free resources, the freed resources are given to other pools with jobs running. For example, a fair scheduler has 100% resources with two pools namely Pool A and Pool B which share the total resources at 40% and 60% respectively. If Pool A has four jobs running, it allocates 10% resources to each job. When the four jobs are completed, the freed resources are allocated to Pool B.

Note: You can configure a pool to run more than one job in parallel.

Capacity Scheduler

This scheduler divides the total capacity of the cluster into queues. Each queue is allocated a pre-configured share of the total capacity. A job may be submitted to any of these queues. If more than one job is submitted to the same queue, the jobs will be executed sequentially. For example, if a capacity scheduler has 100% resources with three queues namely the Default, Low and High and they share the total resources at 20%, 30% and 50% respectively. If Default has two jobs D1 and D2, Low has three jobs L1, L2 and L3, and High has four jobs H1, H2, H3 and H4, these jobs are executed in their respective queues sequentially. If the jobs in a queue are completed, the freed resources will not be distributed to other queues.

Query Aggregates

This section explains the supported aggregate functions.

Supported Aggregate Functions

The following table lists the supported Aggregate Functions.

Aggregate Function	Description	Input data types	Output data types
count	Returns the count of meta values, which includes duplicate values as well.	Numeric	Numeric
countdistinct	Returns the total number of distinct or unique values.	Numeric	Numeric
distinct	Returns all the unique values.	Any	Any
first	Returns the first occurrence of the meta value.	Any	Same as input
last	Returns the last occurrence of the meta value.	Any	Same as input
sum	Returns a sum of all non-NULL values of metaKey in a group.	Numeric	Numeric
avg (Average)	Returns the average value of all non-NULL values of the metaKey within a group.	Numeric	Numeric
min (Minimum)	Returns the minimum for all values of metaKey in each group. This value is based on order by field.	Any	Any

Aggregate Function	Description	Input data types	Output data types
max (Maximum)	Returns the maximum for all values of metaKey in each group. The maximum value is the value that is returned by order by field.	Any	Any
length	Returns the length of the values of metakey. This is called a "scalar function" in SQL.	Any	Numeric

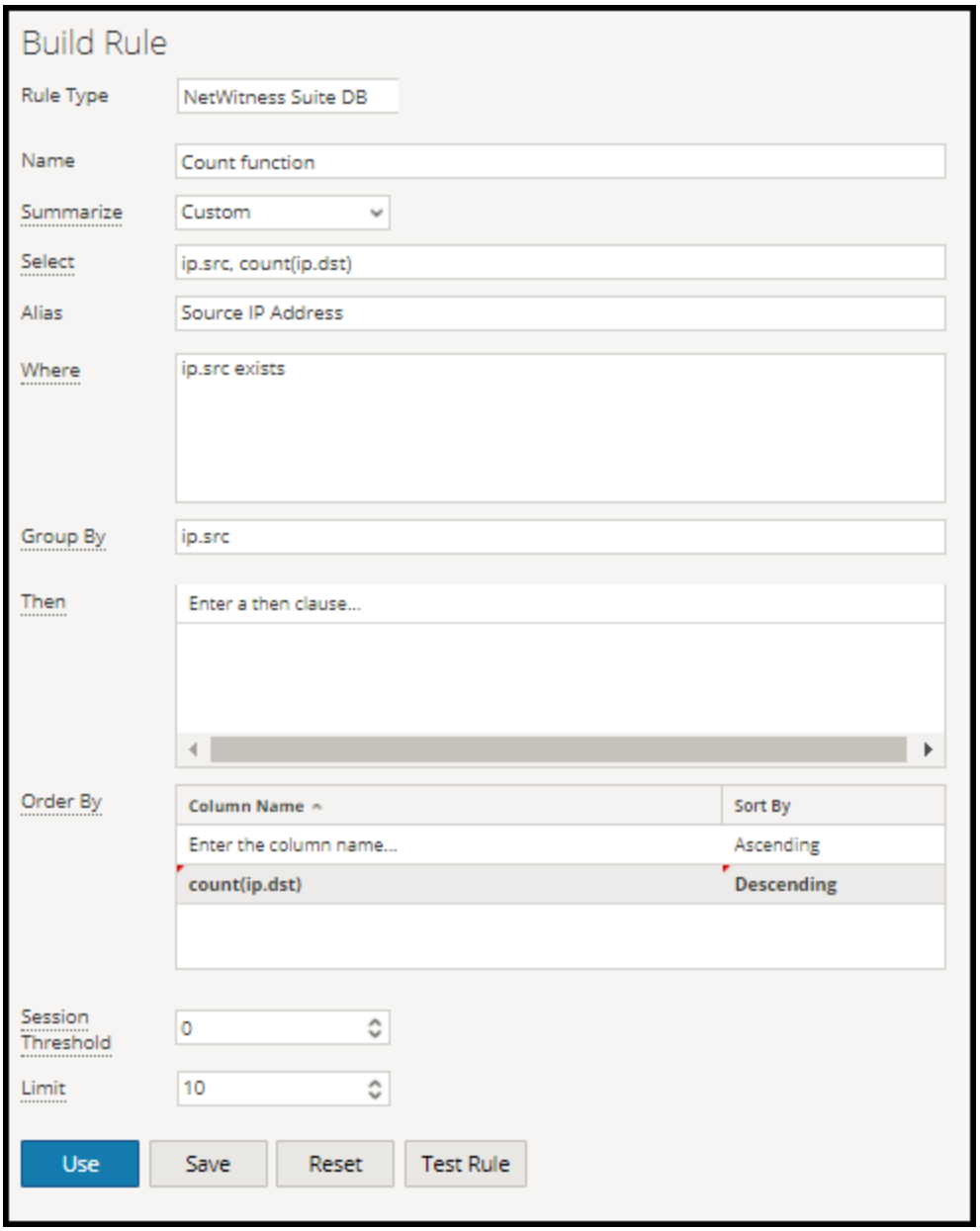
Examples of Queries and Results per Function

Count

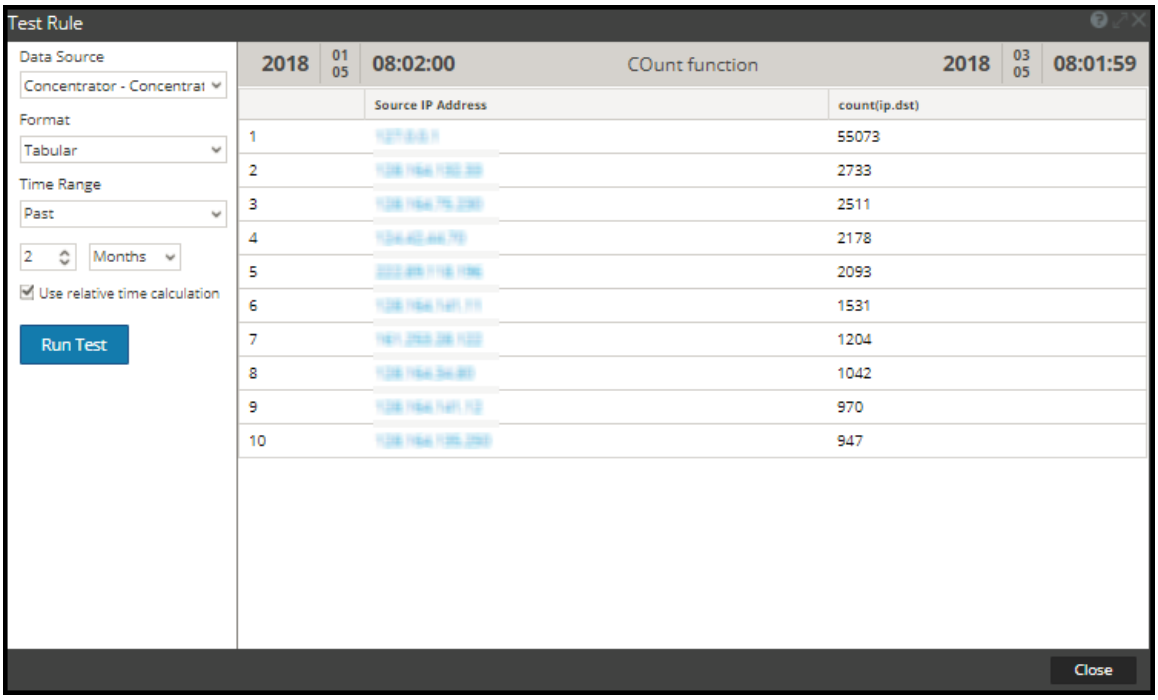
This function returns the number of values for a specified meta key, that exclude null values but include duplicate ones. .

Example

The following figure shows a sample query for count function used for the destination IP and the respective source IP.



The following figure shows the result for the above query.



Here, for each unique ip.src (source IP), the page returns the total number or count of ip.dst (destination IP) values, which include the duplicate values as well.

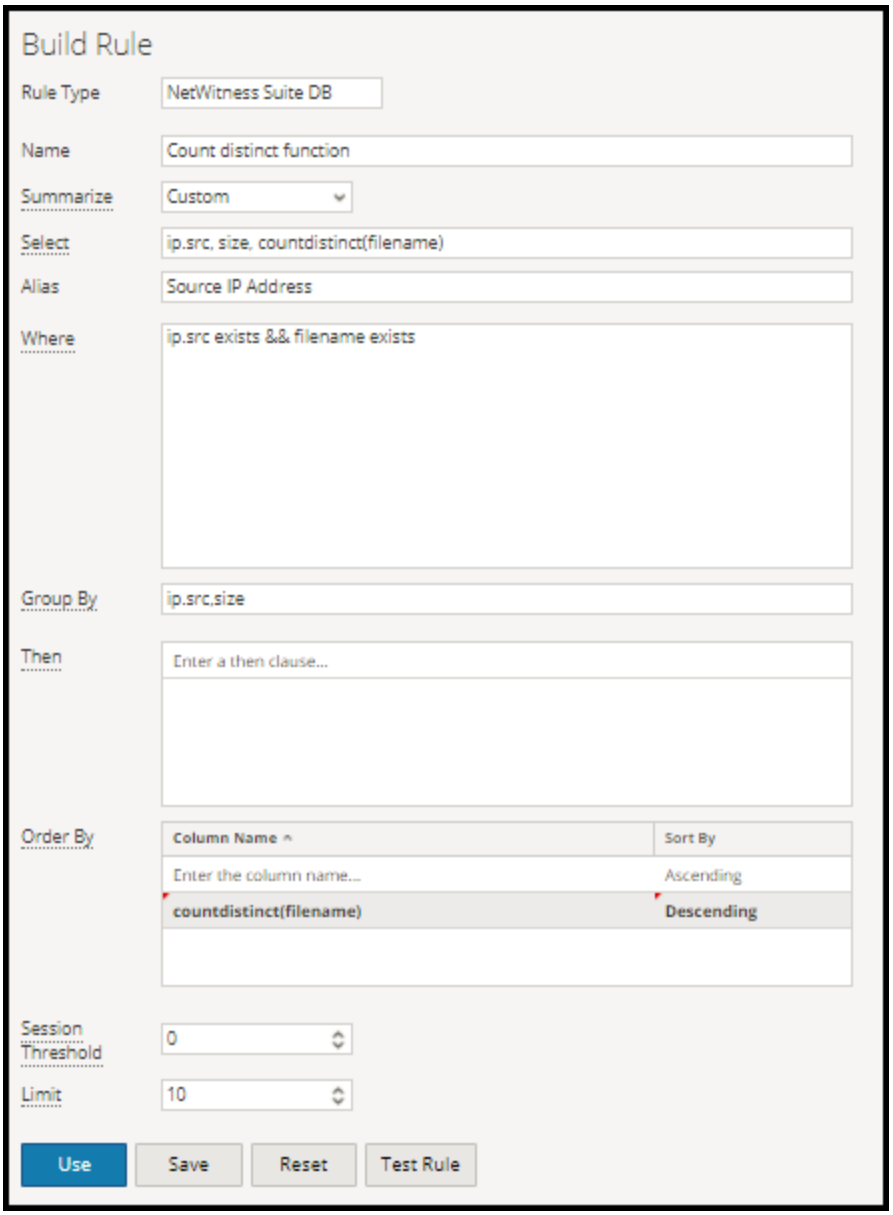
Note: If your RSA NetWitness Suite is currently on 10.5 or newer version and any of the NetWitness Suite Core devices are on 10.3 or 10.4 versions, then some of the aggregate functions may display unexpected errors. However, aggregate functions such as sum() and count() are supported in 10.4 version.

Countdistinct

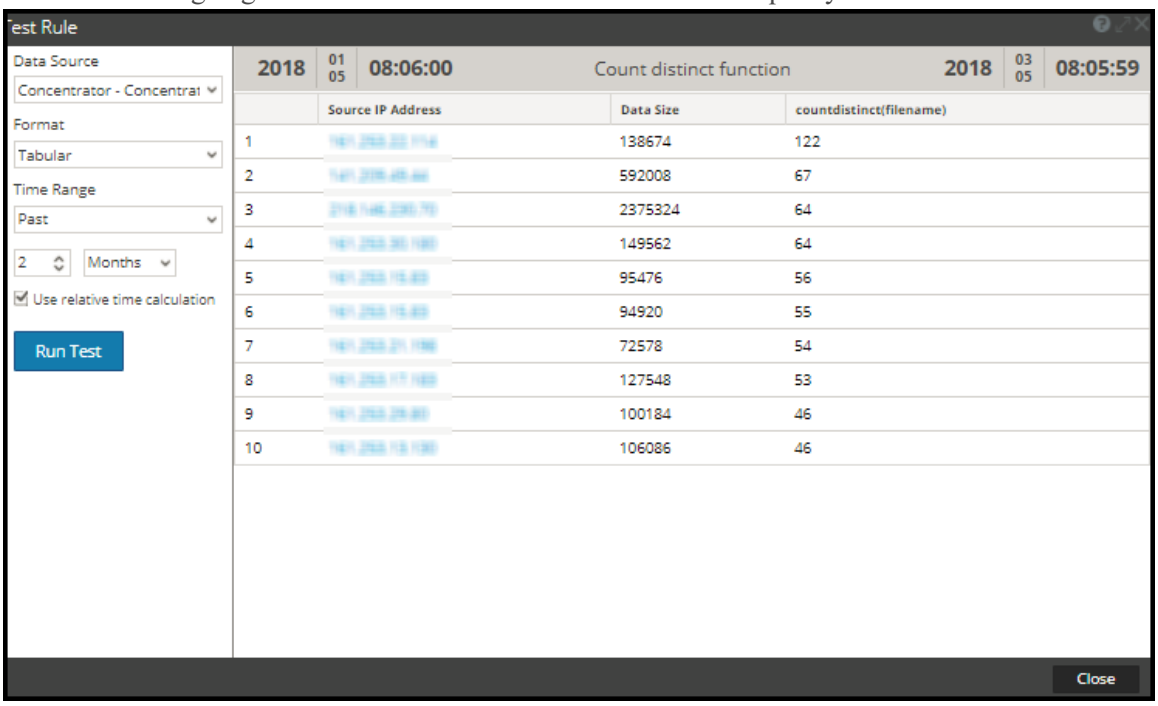
The countdistinct function returns the count of unique or distinct values for the metakey. In other words, countdistinct function can be used to retrieve a number of distinct values for the specified metakey.

The following figure shows a sample query where the countdistinct function is used along with IP source (ip.src) and data size(size).

Example


Build Rule
Rule Type
NetWitness Suite DB
Name
Count distinct function
Summarize
Custom
Select
ip.src, size, countdistinct(filename)
Alias
Source IP Address
Where
ip.src exists && filename exists
Group By
ip.src,size
Then
Enter a then clause...
Order By
Column Name
Sort By
Enter the column name...
Ascending
countdistinct(filename)
Descending
Session Threshold
0
Limit
10
Use
Save
Reset
Test Rule

The following figure shows the result for the above query.



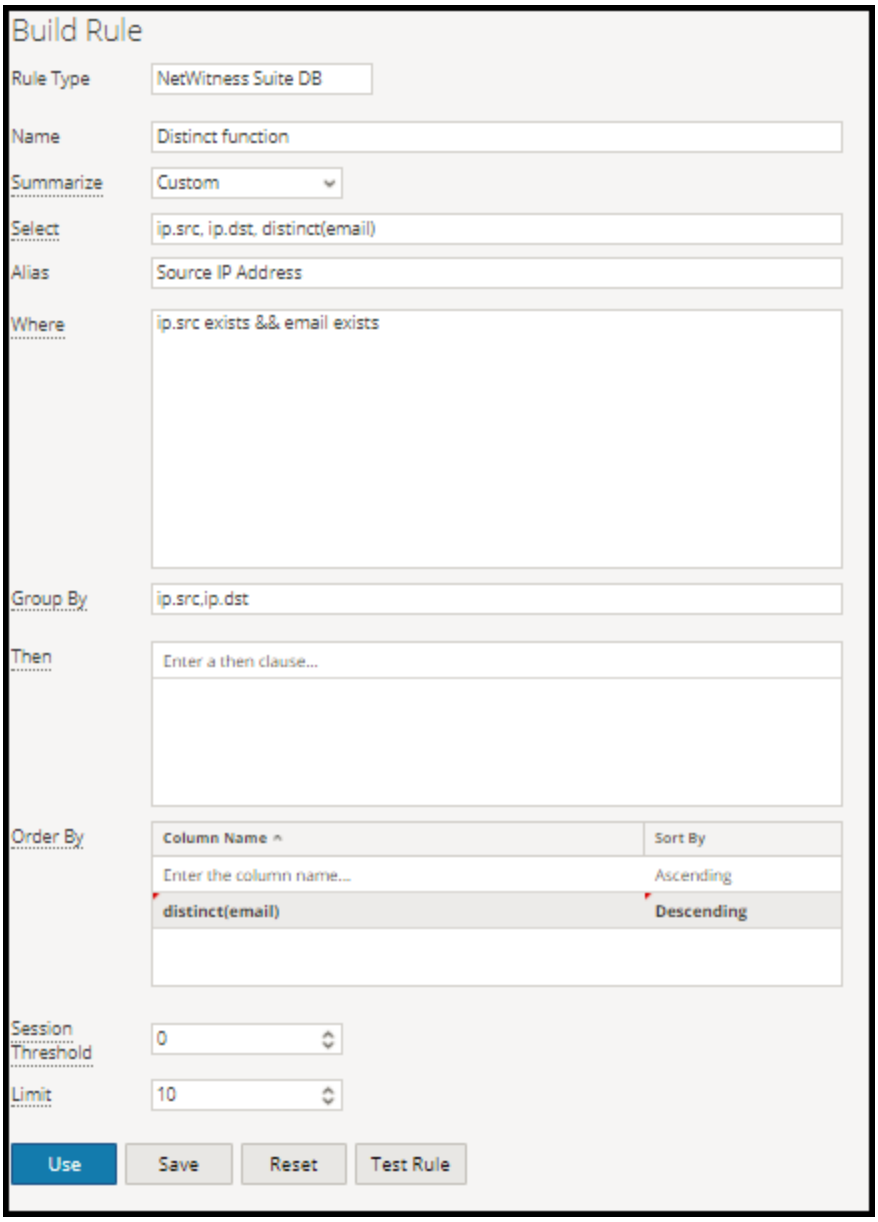
Here, the page displays the data size along with the total number or count of distinct filenames from the respective IP source. Unlike the count function, the countdistinct excludes the duplicate values from the result.

Distinct

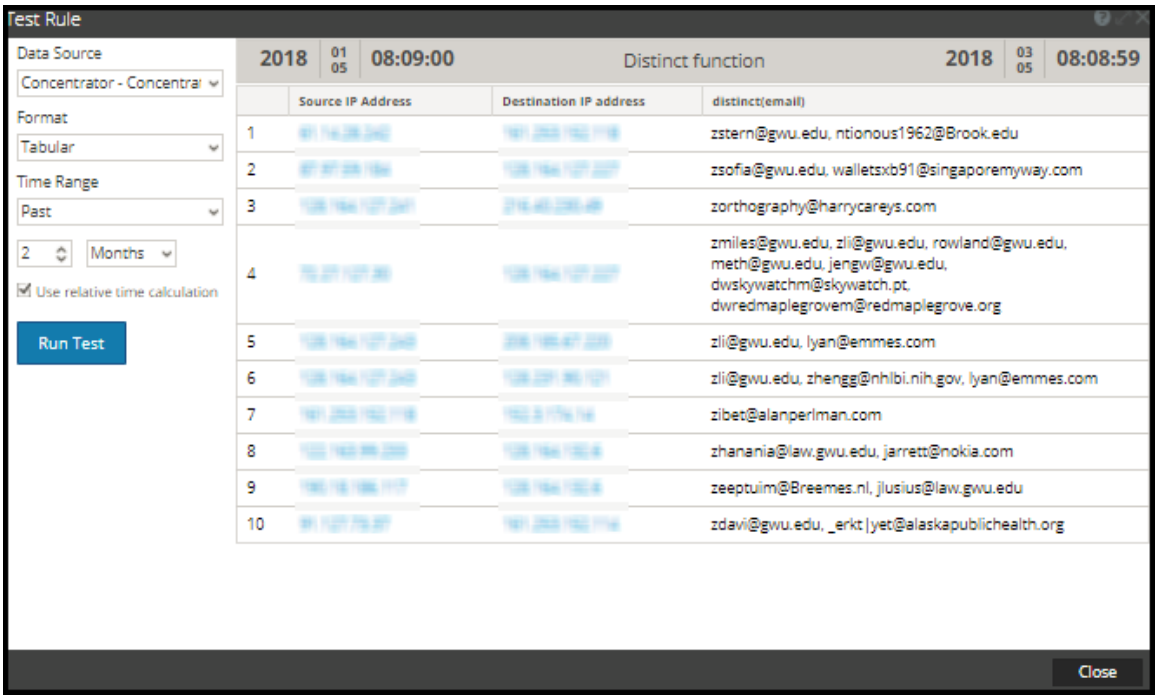
This function returns all the unique or distinct values of the metakey.

Example

The following figure shows a sample query for distinct function used to retrieve e-mails, between various source and destination IP (ip.dst).



The following figure shows the result for the above query.



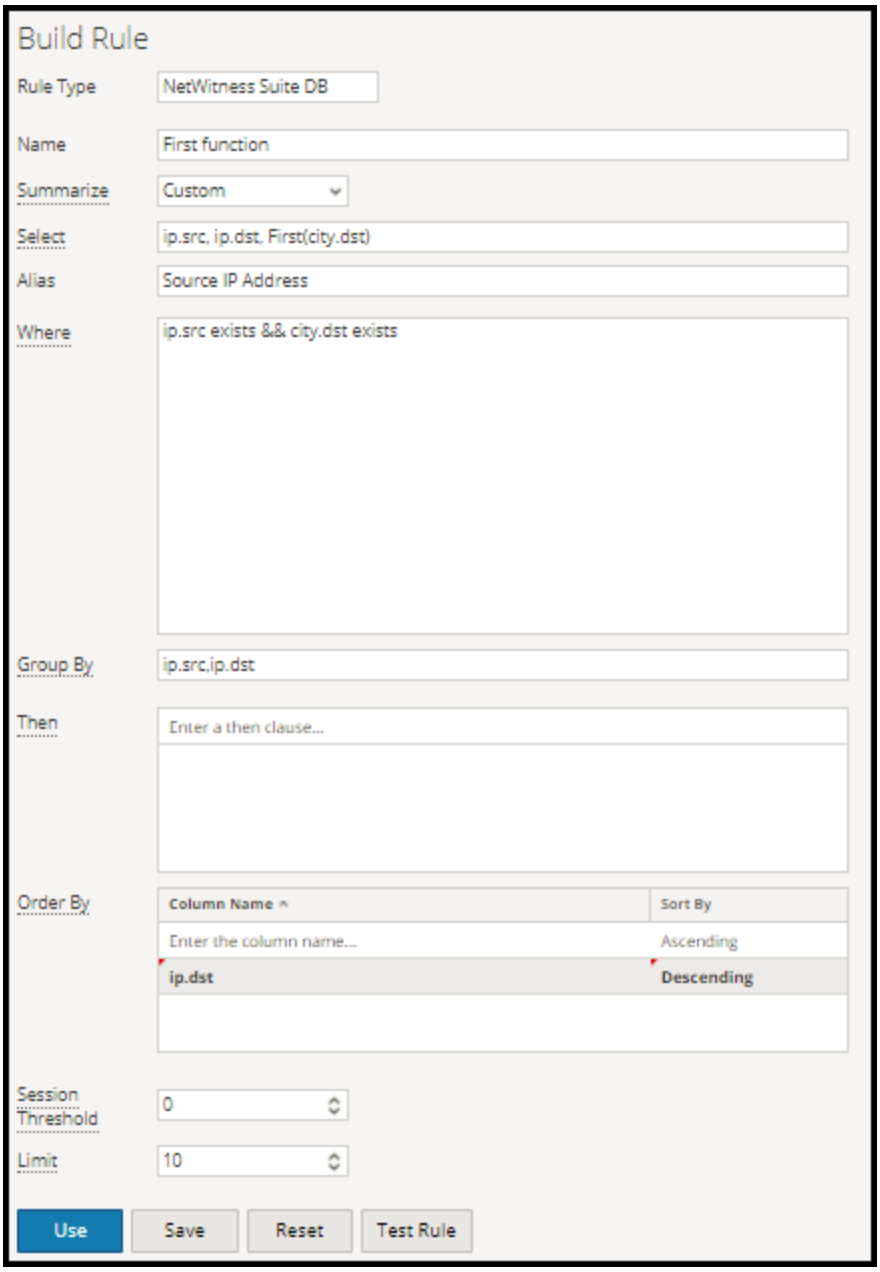
Here, the page displays the list of unique e-mails that were exchanged between the respective IP source and destination.

First

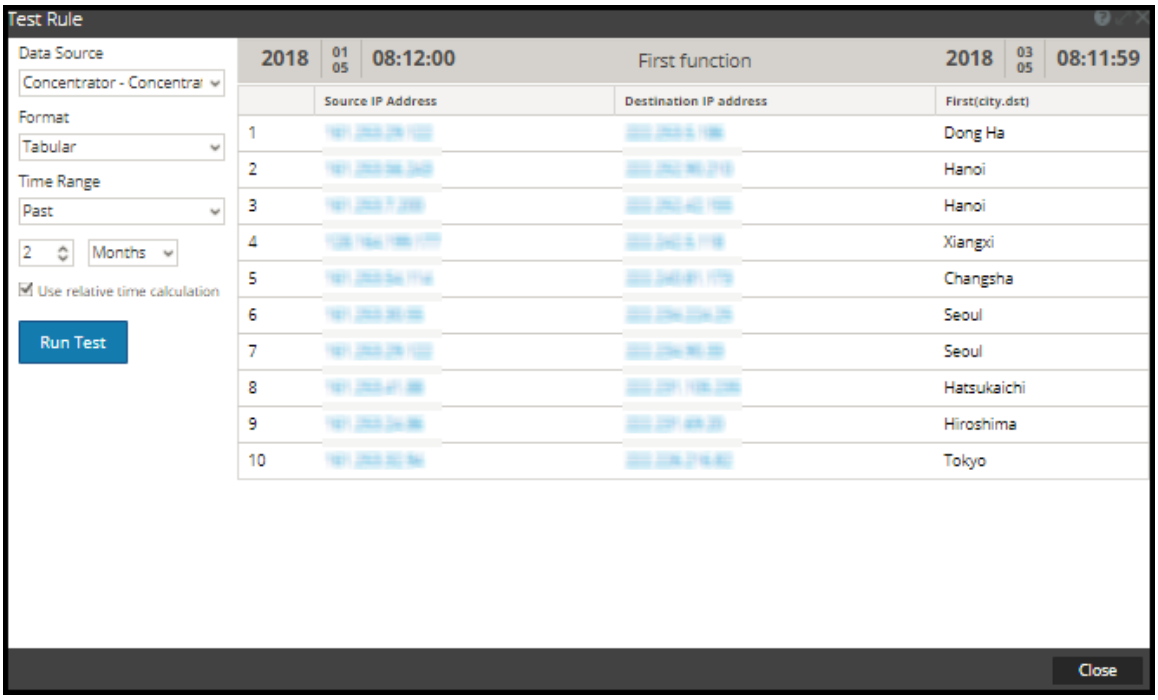
This function is used to retrieve the first value from an ordered sequence of values for a specified metakey.

Example

The following figure shows a sample query for first function used to retrieve the first destination city name.



The following figure shows the result for the above query.



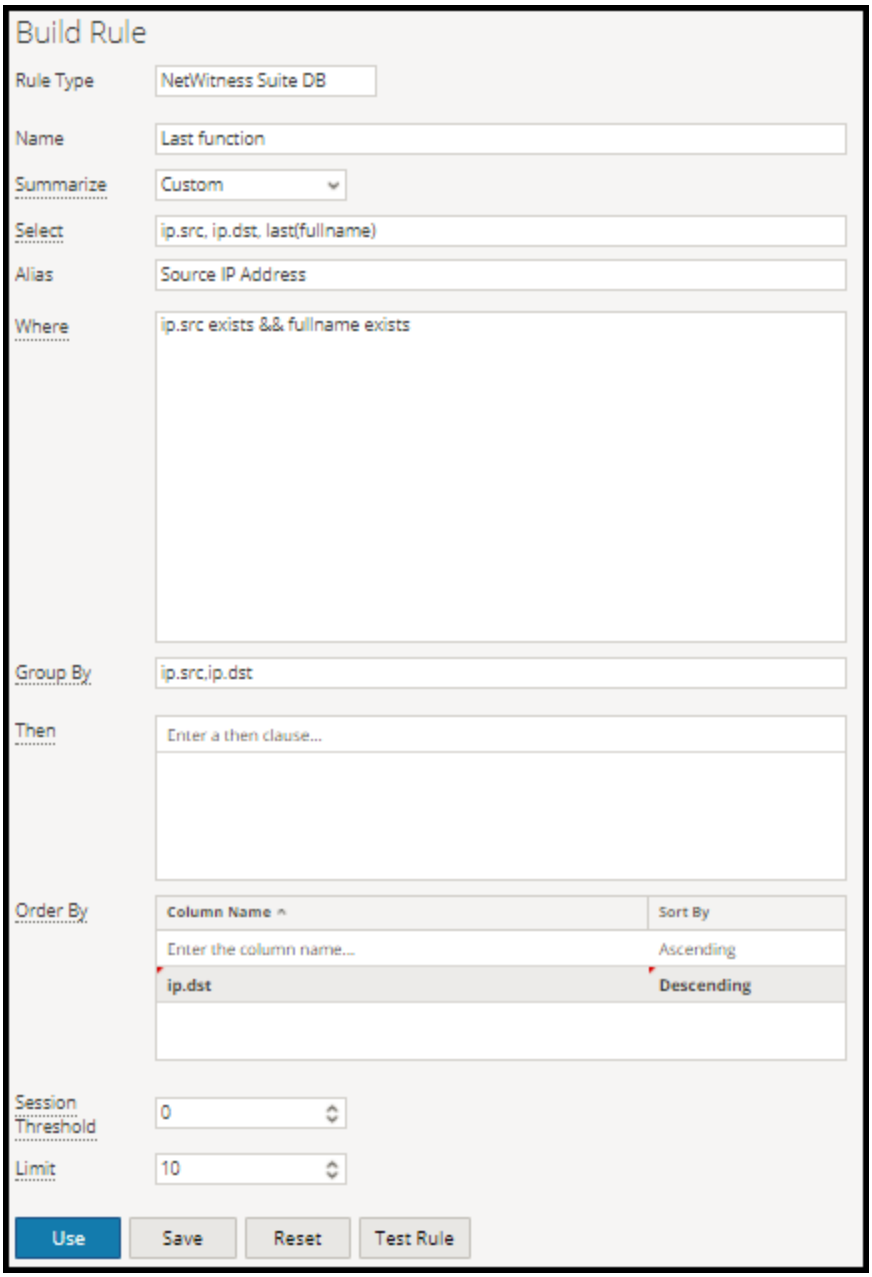
Here, the page displays the the first destination city for the corresponding source and destination IP. You can use the first function to isolate a particular value from a search result.

Last

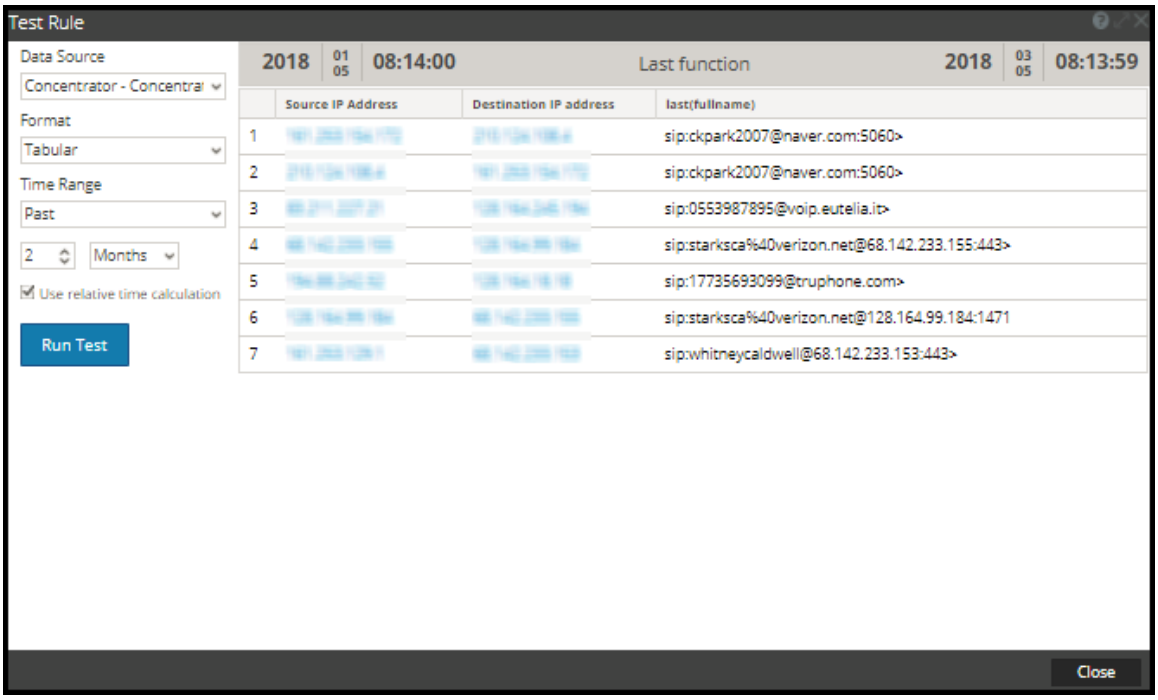
This function is used to retrieve the last value from an ordered sequence of values for a specified metakey.

Example

The following figure shows a sample query for last function used to retrieve the most recent user name.



The following figure shows the result for the above query.



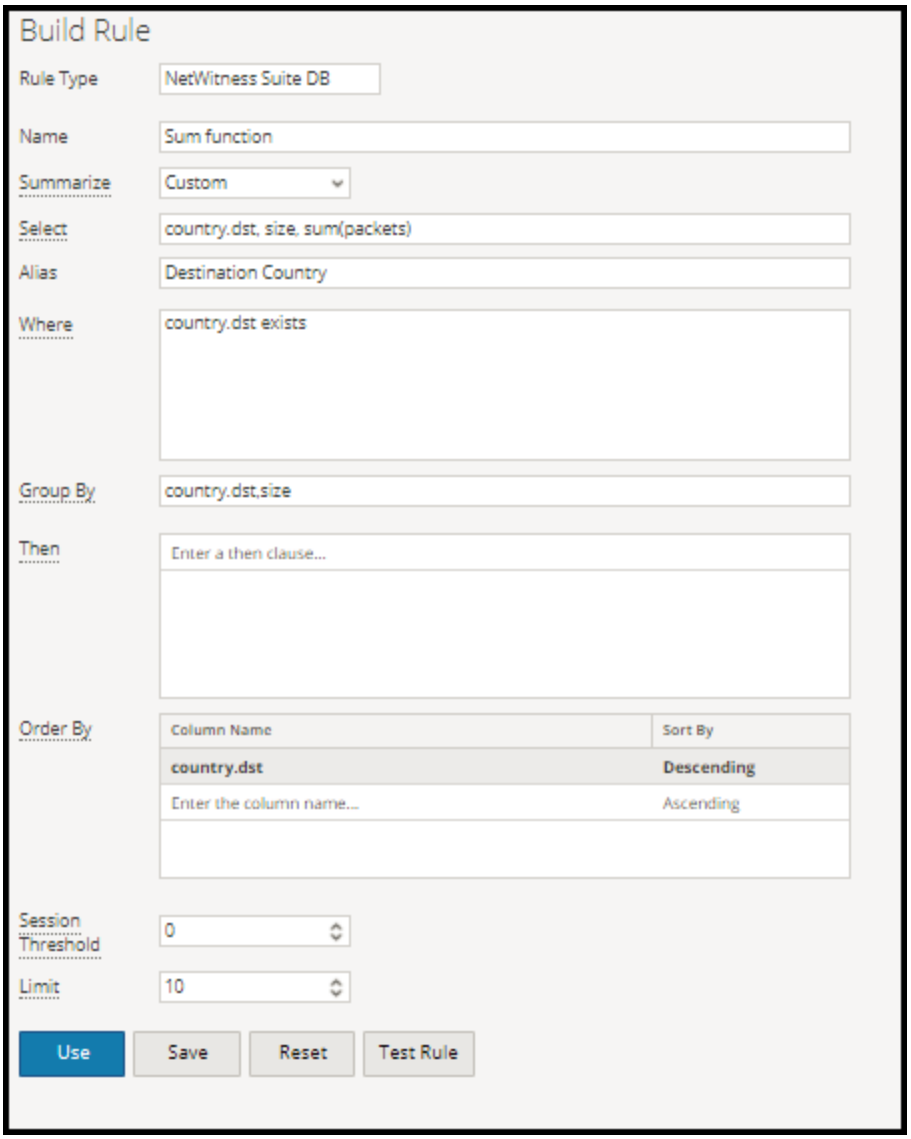
Here, the page displays the list of most recent or last usernames in full, that were exchanged between the source and destination IP.

Sum

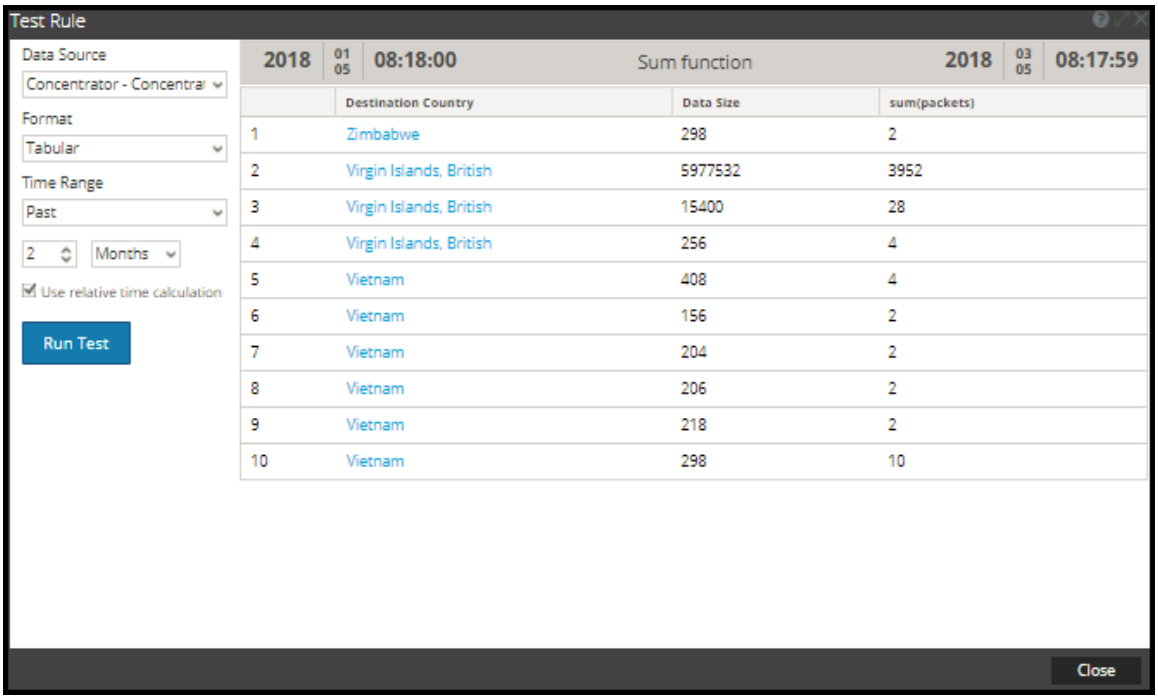
This function returns the total of the non-NULL values of the metaKey within a group.

Example

The following figure shows the query for the Sum function used for packets.



The following figure shows the result of the above query.



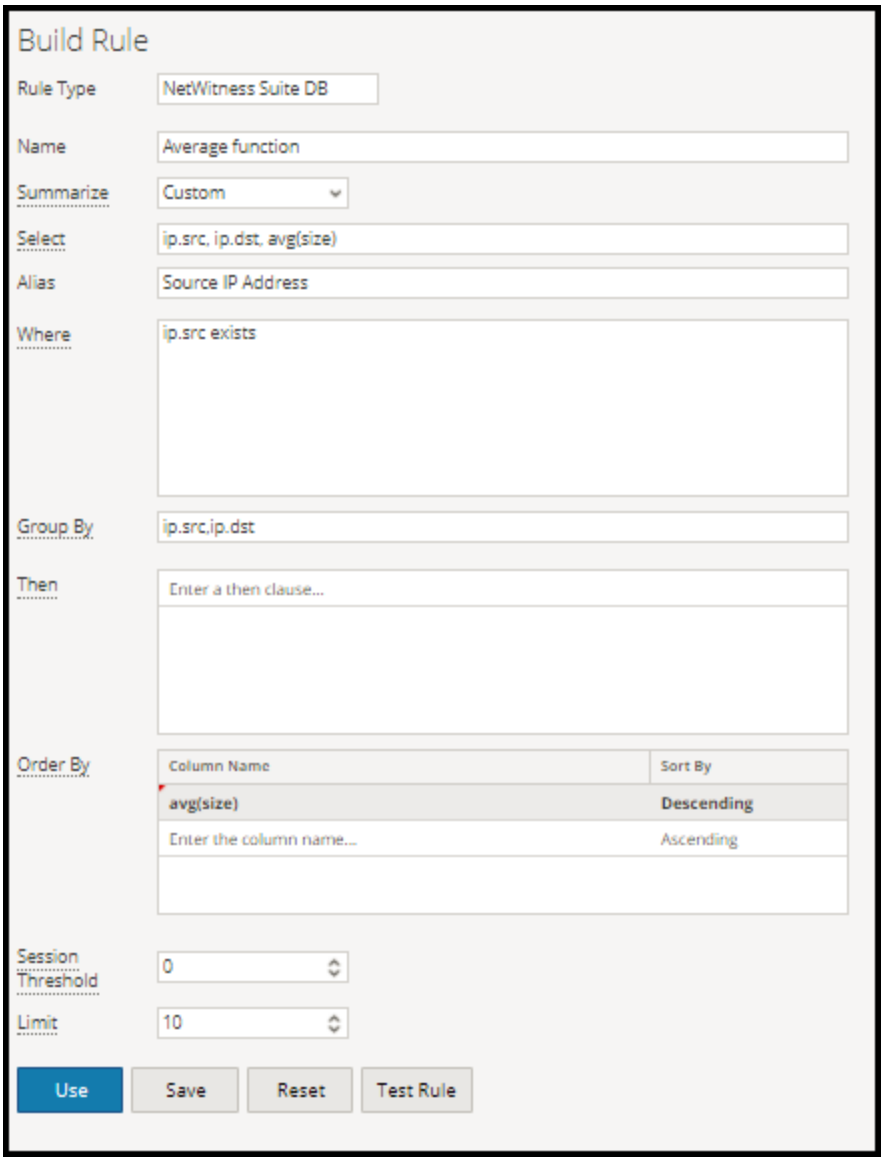
Here the page displays the total or sum of the packets along with the size of the data for the respective destination country.

Avg

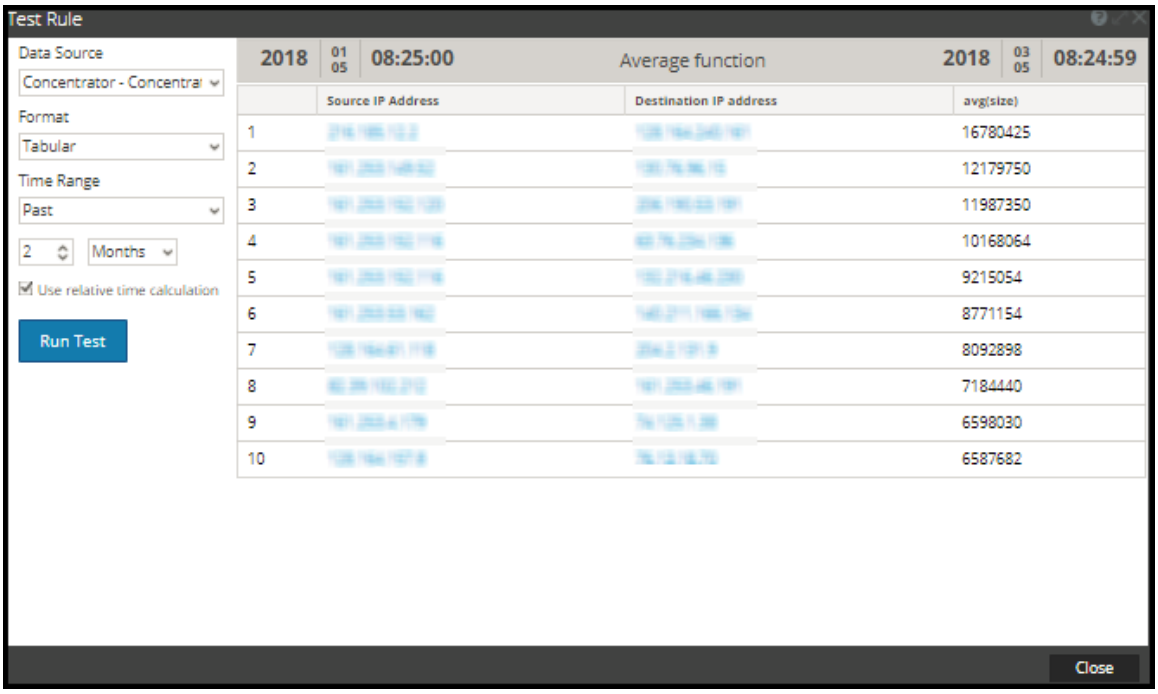
The average function returns the average of non-NULL values of the meta within a group.

Example

The following figure shows a sample query for average data size transmitted between a source and destination IP.



The following figure shows the result for the above query.



Here, the page displays the average size of data exchanged between source and destination IP:

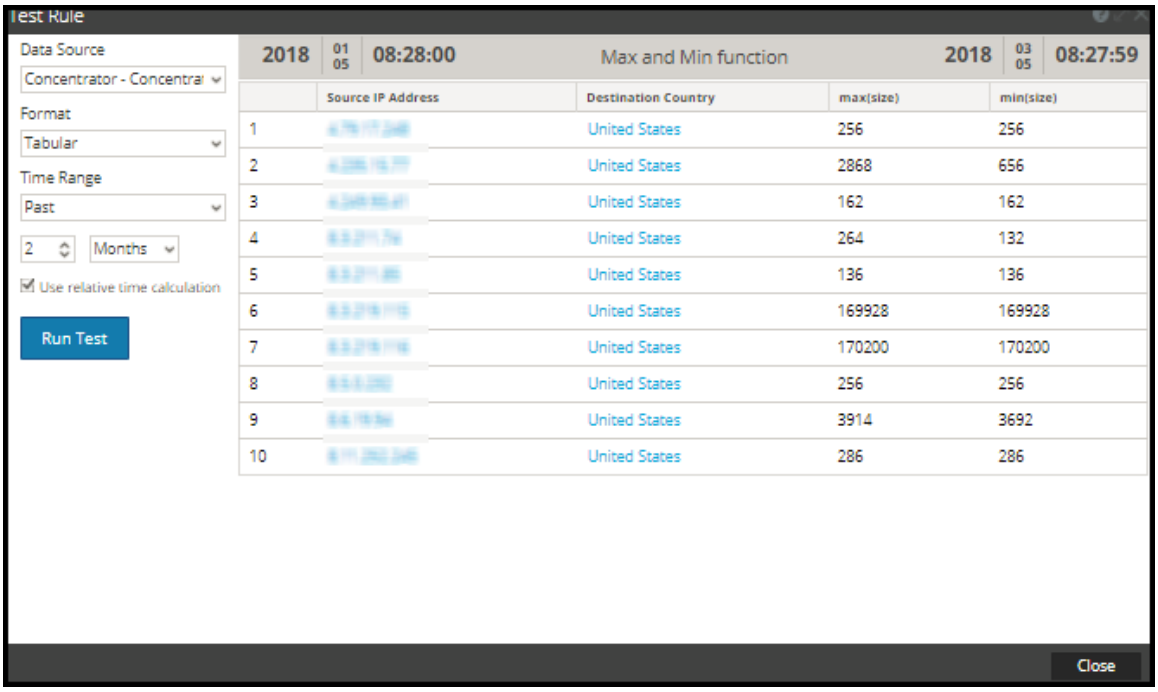
Max and Min

Max and Min functions provide the maximum and minimum for given values of a meta respectively.

The following figure shows a sample query for max and min functions for various data sizes, for source IP and destination country.

Example

The following figure shows the result for the above query.



Here, the page displays the max(size) and min(size) columns, along with the list of source IP and destination country. The max(size) column lists the maximum data sizes exchanged while the min(size) column lists the minimum data sizes that were exchanged.

Filter aggregate meta results with Max_threshold

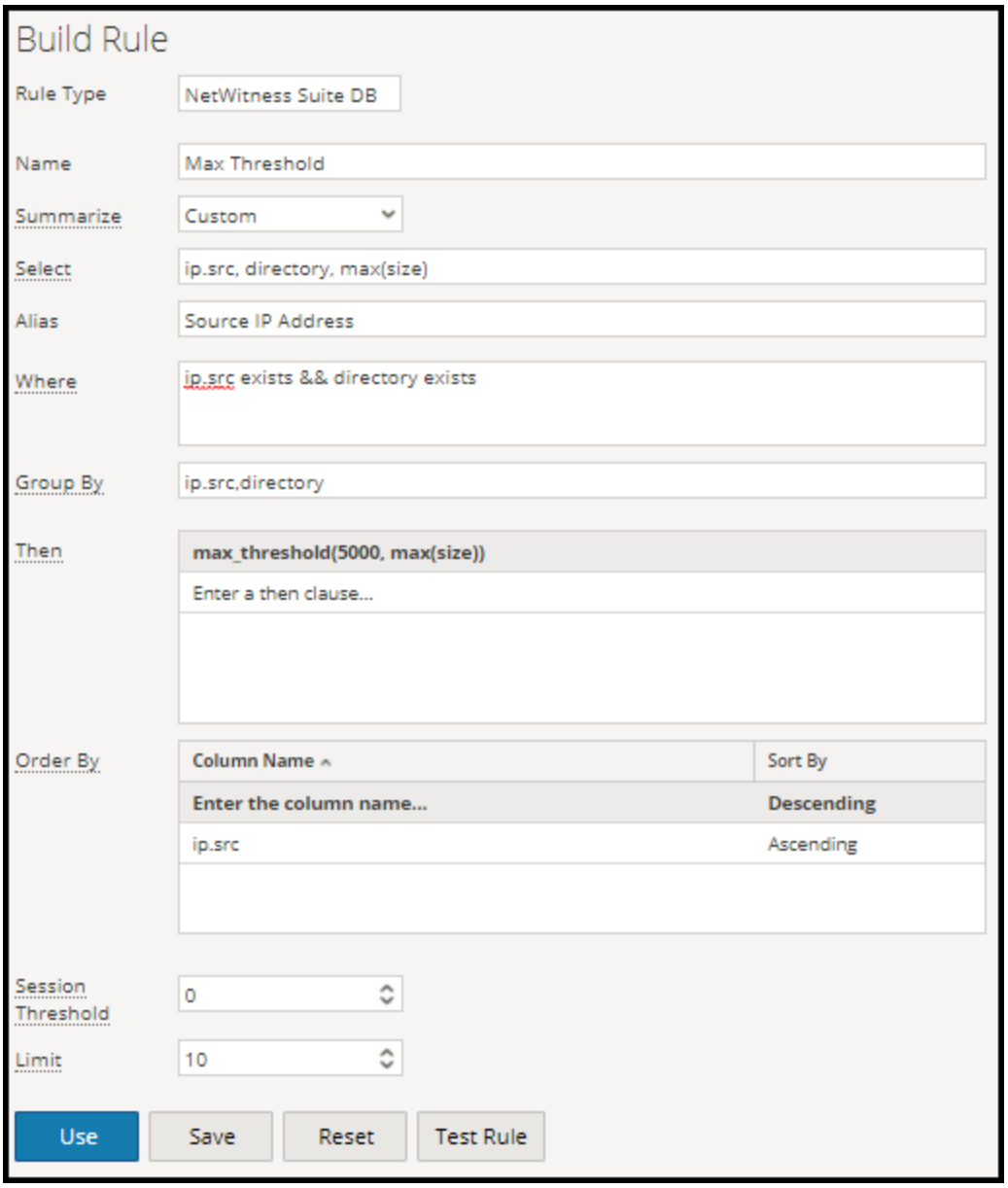
You can further filter the results of any function by using the threshold rule action.

Example

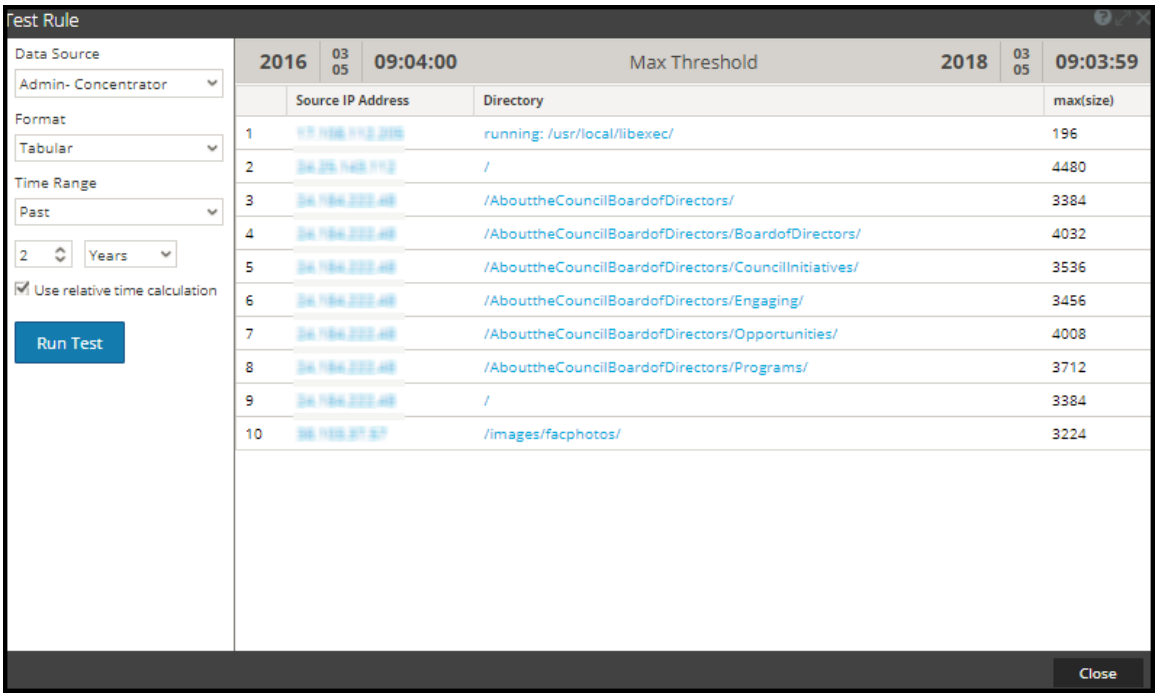
Following is a sample query for max_threshold used along with the Max function in the **Then** field is:

max_threshold(5000,max(size))

The following figure shows the Build Rule screen for the above query.



Here the max_threshold is applied for data size with an upper limit of 5000. The following figure shows the result.



Here, the result page displays the max(size) column, that lists the data sizes lesser than 5000 as this is the maximum threshold in the query, along with the corresponding IP source and the respective directory.

Filter aggregate meta results withMin_threshold

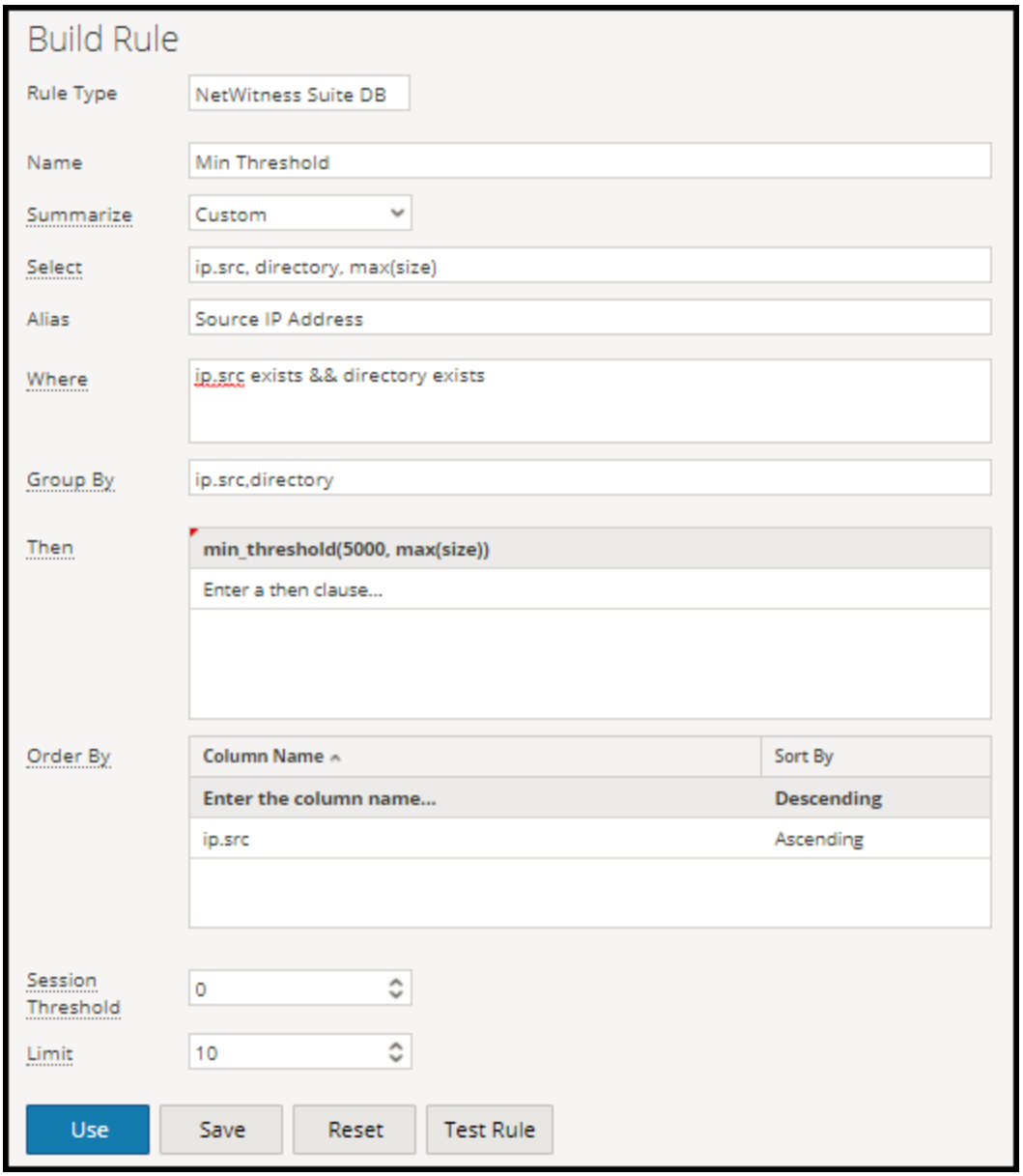
Similarly, min_threshold is used to filter the results for any function. A similar scenario as max_threshold is considered to explain this.

Example

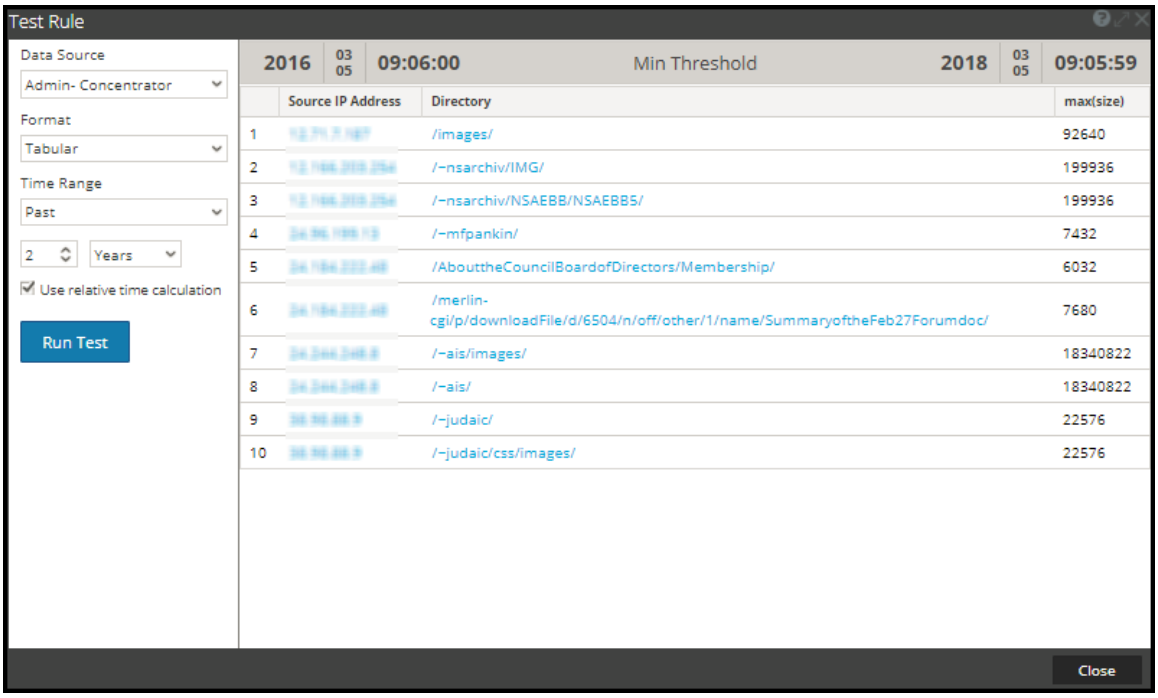
Query for min_threshold used along with the Max function in the **Then** field is:

min_threshold(5000,max(size))

The following figure shows the Build Rule screen for the above query.



Here the min_threshold is applied for data size with a lower limit of 5000. The following figure shows the result.



Here, the result page displays the max(size) column, that lists the data sizes greater than 5000 as this is the minimum threshold in the query, along with the corresponding IP source and the respective directory.

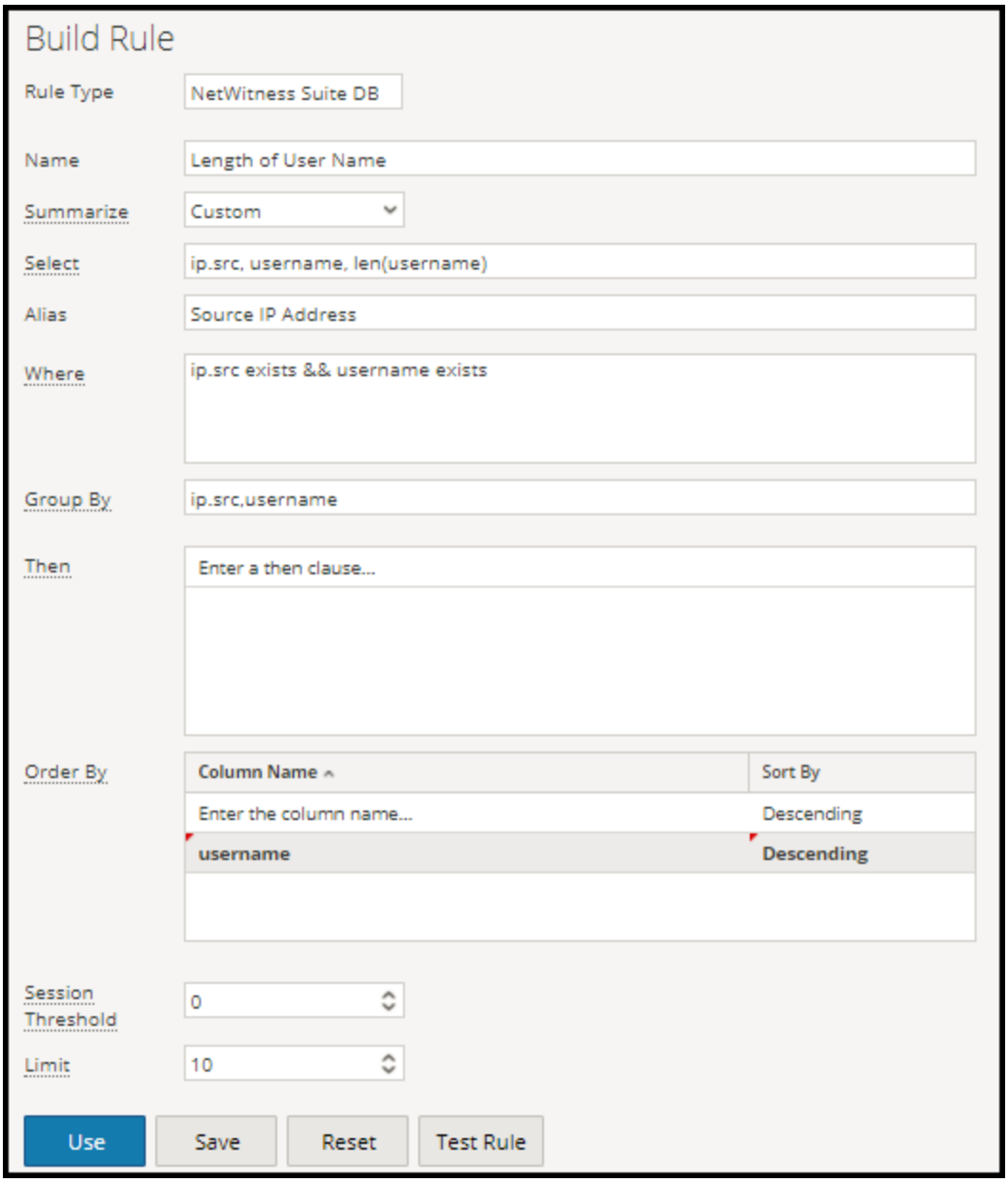
Note: Max_threshold and Min_threshold rule actions are common across all the functions, and can be used along with the other queries in the **Then** field to retrieve the respective output.

Length

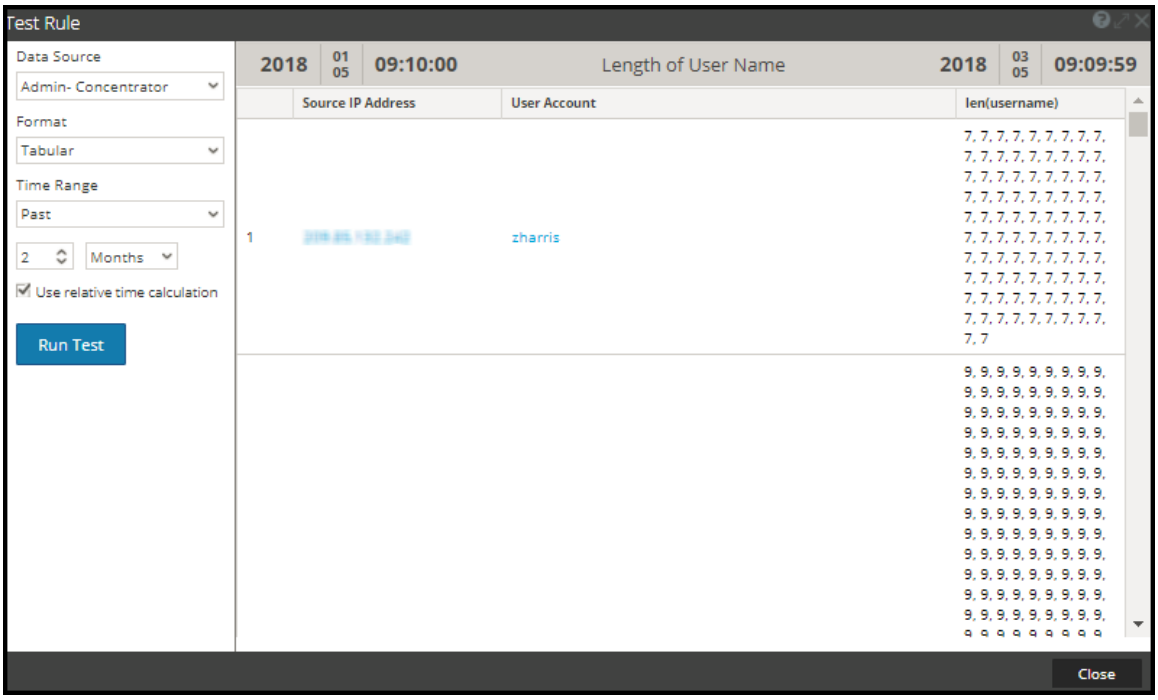
This function returns the length of a meta value. In other words, Length function returns the number of bytes used to store the actual value.
For instance, for the value "Analytics" it returns the length as 9. Similarly, for an IPv4 ip.src, it returns 4 (representing 4 bytes).

Example

The following figure shows a sample query for the length function used for usernames.



The following figure shows the result for the above query.



Here, the page displays the length of the usernames associated with the user account and their respective source IP.

Additional Information

When you query for aggregates (E.g. sum(size)) with **Group By** on a meta which has multiple values in a session, then the session with multiple values is accounted for aggregate calculation for each value of that meta.

Example

When you query for the Count aggregate function with Group By on Alias.host and if the column has multiple values in a session, then the session is counted for each occurrence, including the duplicate values.

Consider the following table.

SessionID	Alias.host	Ip.src	Size
1	host-a, host-b, host-a	a	10
2	host-b, host-c, host-a, host-c	c	20
3	host-b, host-c, host-d	b	30
4	host-c, host-a	a	40

In the above table, alias.host for **host-a** and **host-c** has duplicate values listed for a single session. Let us consider the following query:

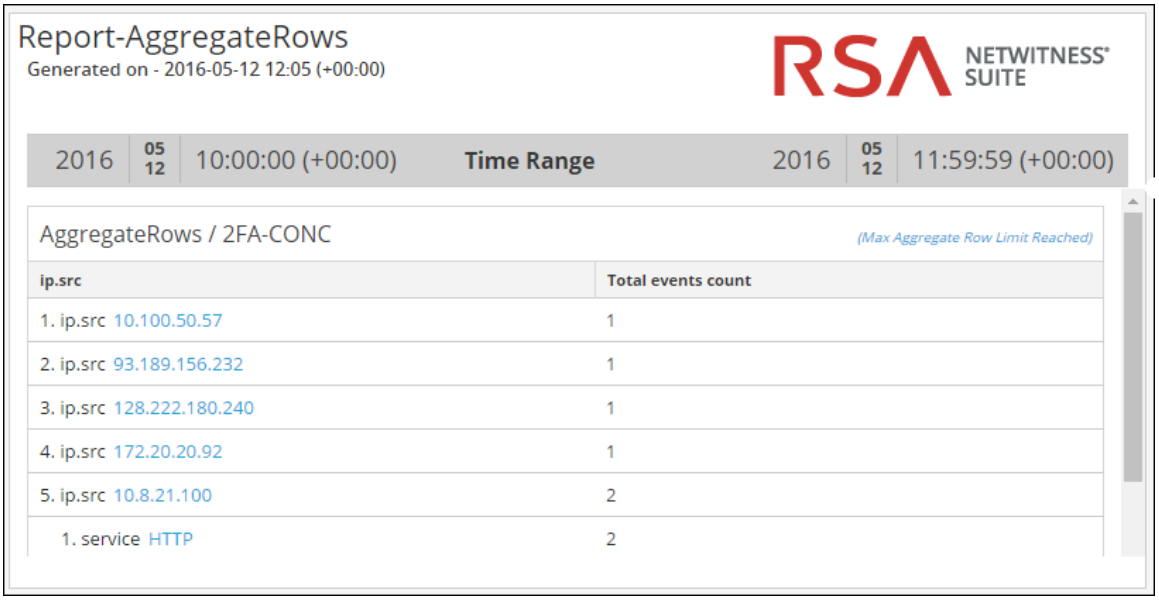
Select : alias.host, count(ip.src), sum(size)
Group By : alias.host

Here, **host-a** and **host-c** are present in 3 sessions and they are duplicated for two different sessions. However, the output is as shown below.

Alias.host	count(Ip.src)	Sum (size)
host-a	4	80
host-b	3	60
host-c	4	110
host-d	1	30

Output table shows that the count for **host-a** and **host-c** is 4. This is because for each alias.host value, the entire session is considered. Similarly to calculate sum (size), the same sessions are considered for each alias.host value.

In the report output if the number of rows has reached **NWDB maximum aggregate rows** defined in RE configuration, then a message **Max Aggregate Row Limit Reached** is displayed to indicate that there is more information to be displayed. The default limit is 1000, and you can change this value as per your requirement, in the Reporting Engine Configuration page .



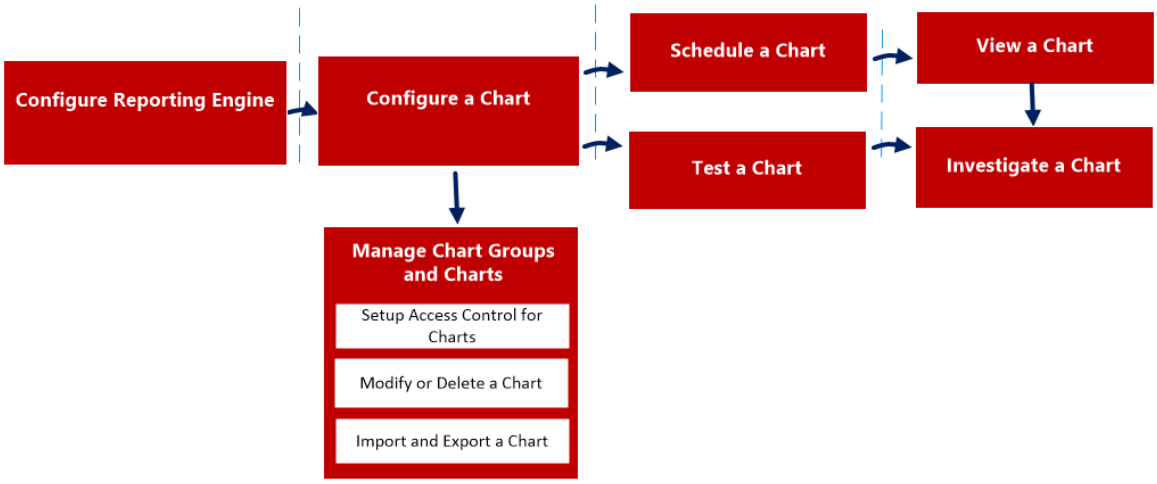
Configure and Generate a Chart

Chart is a graphical visualization of data. You can view different kinds of charts, including multiple types of plot, line, bar, and area charts.

Any NWDB rule in the Reporting Engine system which is not sorted by none can be used to instantly create a chart. For more information on "How to create an NWDB rule", see Configure a Rule.

The chart interval can be adjusted from the chart definition panel itself. Every time a chart is executed, it stores its result data locally in the Reporting Engine, so that it can be reviewed in either the Dashboard View or Chart View without any performance considerations.

The following is an overview of the entire process of configuring and generating a chart.



To configure and generate a chart, perform the following:

1. Configure Reporting Engine
2. Configure an NWDB rule
3. Configure a Chart
4. Schedule a Chart
5. View a Chart
6. Test a Chart
7. Investigate a Chart
8. Manage a Chart Group and Chart

Configure Reporting Engine

You must configure the Reporting Engine before you can configure and generate a chart. You must also specify the data source in the Reporting Engine from which the data is extracted. For more information on how to configure a Reporting Engine, see "Configure Reporting Engine"topic in *Reporting Engine Configuration Guide*.

Configure an NWDB Rule

The NetWitness rule which is not sorted by none is used to create a chart. The NetWitness database extracts the meta from the Reporting Engine and provides the meta for rules. These rules are an essential building block in managing a chart.

Note: If the rule contains the lookup_and_add, sum_count, or sum_values rule actions, the associated chart will not contain data.

Configure a Chart

You can configure a chart using the NWDB rules.

Schedule a Chart

After a chart is defined with the required components, you can configure its execution properties by scheduling a chart. Here, you can quickly view, add, and edit the schedule details for a chart.

View a Chart

You can view the scheduled charts in the Chart View.

Test a Chart

You can run the test on a chart and view all the chart details based on the selected time range.

Access Control for a Chart

The Reporting Module provides access control at the chart level. Only a user who has the right set of permissions can perform the tasks in Reporting module. The access control is managed by the administrator from the **Administration > Security > Roles** tab.

When you create users and user roles, ensure that the roles that you create for specific tasks have access to all the necessary permissions. This could require permissions at several levels of the role hierarchy.

Charts can be tied to a specific set of user roles so that when a user logs in NetWitness, the charts with the access rights for the specific user role can be viewed. Users that belong to a user role with the 'Read & Write' access permission can define charts. Further, the access can be tightened so that charts are accessed only by those who have the 'Read Only' access.

At the chart level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write
- Read Only
- No Access

To change the access permission for a specific user role, you must set the permission at the chart level. For example, for **Administrators** to have access to a specific chart, you could set the permission 'Read & Write' in the Charts Permissions dialog.

You can apply read-only permission to rules in the charts by selecting the checkbox.

Two scenarios that describe how to set access control are explained here:

- Scenario 1: Permissions applied to Chart Group/ Subgroup/ Chart/ Rules based on the user role.
- Scenario 2: Read-only permission applied to Rules in the Chart.

	Role (Analyst)	Permissions applied to chart group, subgroup, chart or rules based on the user role	Permissions (Read-only) applied to rules in the chart
Group	Read & Write	Read & Write	Read & Write
Subgroup	Read	Read	Read & Write
Chart	Read	Read	Read & Write
Rules	Read	Read	Read

The chart is assigned the role of a **Security Analyst** and permissions are set to 'Read & Write' charts.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the Read permission is set for the rules except that the permission for the rules cannot be higher than the permission for the charts.

Note: If the permission for the rules is higher than the permission for the chart, the permission is not applied. For example, if you set the permissions for the Report Group as **No Access** and specify the option *Apply Read-only permission to Rules in the Reports*, the read-only permission is not set for the rules.

Access Control for a Chart When Multiple Charts are Selected

To change permissions for multiple charts, you must select several charts and set their access permissions using the Charts Permissions panel. The access permission that you choose is applied to all the selected charts.

Access Control for a Chart When Multiple Charts with Several Rules are Selected

To change access permissions for a specific user role when multiple charts with several rules are selected, select the checkbox in the Charts Permissions panel.

The read-only access permission is applied to all the rules of the selected charts, provided that the permission of the rules are lower than the permission of the charts.

Note: If a user (other than the super user) creates a chart, the super user cannot access that chart.

Access Control for a Chart Group

To change chart group permissions, select a chart group and set the access permissions using the Charts Permissions panel. Before chart group permissions are applied, the default permission set for all the user roles is 'No Access'.

To change the access permission for a specific user role, set the permission at the chart group level. For example, for administrators to have access to all the charts in a Chart Group, set the permission 'Read & Write' in the Charts Group Permissions panel.

You can also apply permissions to subgroups and charts in the group, and apply read-only permission to rules in the charts by selecting the appropriate checkboxes.

Three scenarios that describe how to set access control are explained here:

- Scenario 1: Permissions applied to chart groups, subgroups, or charts based on user roles.
- Scenario 2: Permissions applied to subgroups and charts in the group.
- Scenario 3: Read-only permission applied to rules in the chart.

	Role (Analyst)	Permissions applied to chart groups, subgroups, or charts based on user roles	Permissions applied to subgroups and charts in the group	Permissions (Read-only) applied to rules in the chart
Group	Read & Write	Read & Write	Read & Write	Read & Write
Subgroup	Read	Read	Read & Write - Inherited	Read & Write
Chart	Read	Read	Read & Write - Inherited	Read & Write
Rules	Read	Read	Read	Read

The chart group is assigned the role of a **Security Analyst** and permissions are set to 'Read & Write'.

For scenario 1, each of the levels will have a permission set depending on the user role.

For scenario 2, the permission at the chart group level will be inherited by the subgroup and by charts in the group.

For scenario 3, the Read permission is set for the rules. However, the permission set for the rules cannot be higher than the permissions set for the chart group.

The following table lists the columns in the Charts Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness UI.
Read & Write	The user can access, view, edit, import, export, and delete the chart in the Charts view. The user can also change the permission for the chart.
Read Only	The user can only access and view charts on the Charts view.
No Access	The user cannot access or view charts for which this permission is set.
☐ Apply these permissions to sub-groups and Charts in this group	Select the checkbox to apply the selected permissions to the chart group, subgroups in the group and charts in the group. **Note:** This checkbox is populated only when you set access permissions for a Chart Group.
☐ Apply Read-only permission to Rules in the Charts	Select the checkbox to automatically apply permissions to the rules in the charts.

Configure a Chart

After a chart is defined with the NetWitness rules with NWDB as the data source, you can configure its execution properties.

Create a Chart Group

To add groups to the default folder or to add subgroups under a chart group:

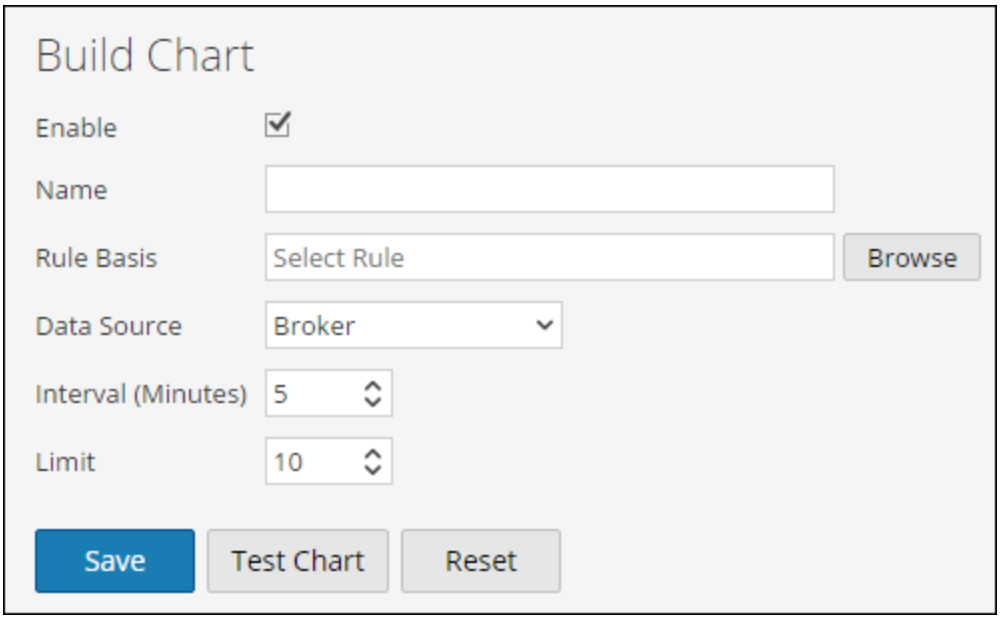
1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart Groups** panel, click +.
   A default group is added in the Chart Groups panel.
4. Enter the name of the new group.
5. Press **Enter**.
   The group is added to the Chart Groups panel.

Create a Chart

To add charts to a group or subgroup:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts** to display the Chart view.

3. In the **Chart** toolbar, click +.
   The Build Chart tab is displayed.



4. Enter the name of the chart.
5. For the Reporting Engine to collect the data and generate chart results, select the **Enable** checkbox.
6. In the Rule Basis field, do the following:
   a. Click **Browse**. The Add Rule dialog box is displayed.
   b. Navigate the Rule tree and select a rule.
   c. Click **Select**.
7. The Rule appears in the Rule Basis field.
8. Select the data source from the **Data Source** drop-down list.

   Note: If the default data source is configured in the Reporting Engine, then the data source is displayed by default on the Build Chart page. If the data source is not displayed, ensure you have Read permissions set for the data source. This is applicable for NWDB and Warehouse data sources. For more information, see the "Configure Data Source Permissions" topic in the *Host and Services Configuration Guide*.

9. (Optional) To modify the Interval value, click the up or down arrow.
   The Interval value is the interval in minutes at which the rule which forms the basis of the chart is run to collect data.

10. Select the **Limit** value to limit the number of records to be displayed.
11. **X-Axis** and **Y-Axis** are used to specify the meta to be plotted in charts.
    In the **X-Axis**, the meta for the 'Group by' rule is displayed. In the **Y-Axis**, the aggregate functions used in the rule are displayed.

    Note: Sum, Count, Countdistinct and Average are the supported aggregate functions for chart. By default, for Custom Rules with multiple 'Group by', you can select only the first meta in **X-Axis**.
12. Click **Save**.
    A confirmation message that the chart is saved successfully is displayed.

Schedule a Chart

You must schedule a chart to further investigate on the chart details.

By enabling a chart, the chart executes as scheduled and provides the configured output with the state of the chart changed to 'Scheduled'.

To schedule a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, select a chart or several charts that display ○ in the **Enabled** column.
4. Click ●.
   A confirmation message indicates that the chart(s) state is changed successfully.

View a Chart

After you view a chart, you can perform the following:

1. You can print, save, email and view charts on full screen.
2. You can also select a date from the calendar to view a list of successfully run charts for the chosen date.

To view a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, do one of the following:
   - Select a chart and click > **View**.
   - Select a chart and click **View** from the View Chart column.
     The View Chart view tab is displayed.
4. In **Chart Options**, do the following:
   a. Select the **Time Range**.

   > **Note:** When you select the Time Range option, you can select a pre-set time range such as last hour, last 3 hours and the Last N Days...or you can customize the selection by choosing Last N Days or Custom. If you select Last N Days option, you can view the historical data for a maximum of 15 days. If you select the Custom option, you can select a start date and end date to view the data for the selected date range.

   b. Select the **Series**, either **Chart Values over Time** or **Chart with Totals**.
   When you select **Chart Values over Time**, the chart displays the change in values for the selected time. When you select **Chart with Totals**, the chart displays a total for each aggregate value for the selected time.
   c. Select **Items to Plot** to define the number of events to view on the chart.
   d. From the **Chart Type** drop-down list, select the chart type.

e. Click **Reload** to reload the selected chart.
   If there is a delay in retrieving the historical data for the selected time range, a message is displayed.

After the chart is generated, a notification is displayed in the notification tray available in the NetWitness toolbar. For more information on the NetWitness toolbar, see the "Browser Window" topic in the *NetWitness Getting Started Guide*.

View all Charts List

To view a list of all the charts:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart** toolbar, click **View All Charts**.
   All the executed charts for the selected date are displayed in a new tab.

   Note:
   * If no list is displayed, you can select a date from the calendar to view a list of charts.
   * If you want to view a specific chart, enter the chart name in the search criteria.
4. Click the chart name to view the chart details for that date.

Test a Chart

You can test a chart in the **Test a Chart** view.

To test a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. Do one of the following:
   - In the **Chart** toolbar, click .
   - In the **Chart** panel, double-click a chart or select a chart and click .
   - In the **Chart List** panel, click > **Edit**.
     The Build Chart view tab is displayed.
4. Click **Test Chart** to view the chart.
   The View Chart view tab is displayed.
5. Select the **From** and **To** date ranges.
6. Select the **Series**, either **Time Series** or **Summary**.
7. From the **Chart Type** drop-down list, select the chart type.
8. Click **Run Test** to run the test.
   The chart data (if any) for the selected time range is displayed.

Investigate a Chart

You can investigate the chart by navigating directly to the Investigation module from the chart.

To investigate a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart** toolbar, click **View All Charts**.
   All the executed charts for the selected date from the **Chart Options** panel are displayed on a new tab.
4. Click the chart name to view the chart details such as the time at which the chart is executed and the default data source used for the chart execution.
5. Do one of the following:
   - Click a data point on the chart to investigate.
   - In the toolbar, click **Investigate** to investigate for the entire time range.

Manage a Chart Group and Chart

You can manage chart groups and charts using the following procedures.

Manage a Chart Group

Depending on the access permissions set for the user role, you can modify or delete, import or export, drag and drop a chart, or refresh a chart group.

Modify a Chart Group

To modify a chart group in the default folder or subgroups under a chart group:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart Groups** panel, select the chart group to modify.
   The selected chart group is modified and can be viewed on the Chart Groups panel.

Delete a Chart Group

To delete a chart group in the default folder or subgroups under a chart group:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart Groups** panel, select the group and click .
   A confirmation dialog asks for confirmation that you want to delete the selected group.
4. Click **Yes** to delete the group.
   The selected group is deleted from the Chart Groups panel.

Import a Chart Group

To import chart groups from other instances of NetWitness Suite:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. Click **Charts**.
   The Chart view is displayed.
3. From the **Chart Groups** panel, select a folder to import the file.
4. Do one of the following:
   - In the Chart Groups panel, click > **Import**.
     The **Import Chart** dialog box is displayed. You can import multiple chart groups at the same time. To select multiple chart groups, press and hold the CTRL button and select the chart groups to be imported.
5. Click **Browse** to select the binary file.
   NetWitness provides a file system view of the files.
6. Locate the binary file and click **Open**.
   The file is added to the Import Chart list.
7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, select the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, select the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing chart in the library with an identically named chart in the binary file when importing, select the **Chart** checkbox. If you do not select the Overwrite option and an identical chart is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Export a Chart Group

To export selected chart groups:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.

3. In the **Chart Groups** panel, select a chart group and click and do one of the following:
   - **Export** - This selection exports a chart in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple chart groups at the same time. To select multiple chart groups, press and hold the CTRL button and select the chart groups to be exported. The exported file is saved to the local drive.

Drag and Drop Chart to a Group

To drag and drop a chart from the Charts List panel to a group in the Charts Groups panel:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. Select a chart from the **Chart List** panel and drag and drop the chart to a group in the **Chart Groups** panel.
   The chart is copied to the group in the Chart Groups panel.

Refresh a Chart Group

To refresh chart groups:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart Groups** panel, drag and drop the group.
   The chart group is moved to the new location.
4. In the **Chart Groups** panel, Click .
   The chart group is refreshed.

Manage a Chart

Depending on the access permissions set for the user role, you can modify or delete, duplicate, import and export, enable or disable charts, search for existing charts, and refresh a chart list.

Access Control for a Chart

To set access permissions for a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, select a chart.
4. Click > **Permissions**.
   The Charts Permissions dialog box is displayed.
5. Based on the user role, select the appropriate buttons.
6. (Optional) Select the checkbox if you want to provide read access permission to dependent rules.

   Note: On selecting the check box, all dependent rules with No access permission are granted a READ access permission.

6. Click **Save**.
   A confirmation message that the permission is successfully set for the selected chart is displayed.

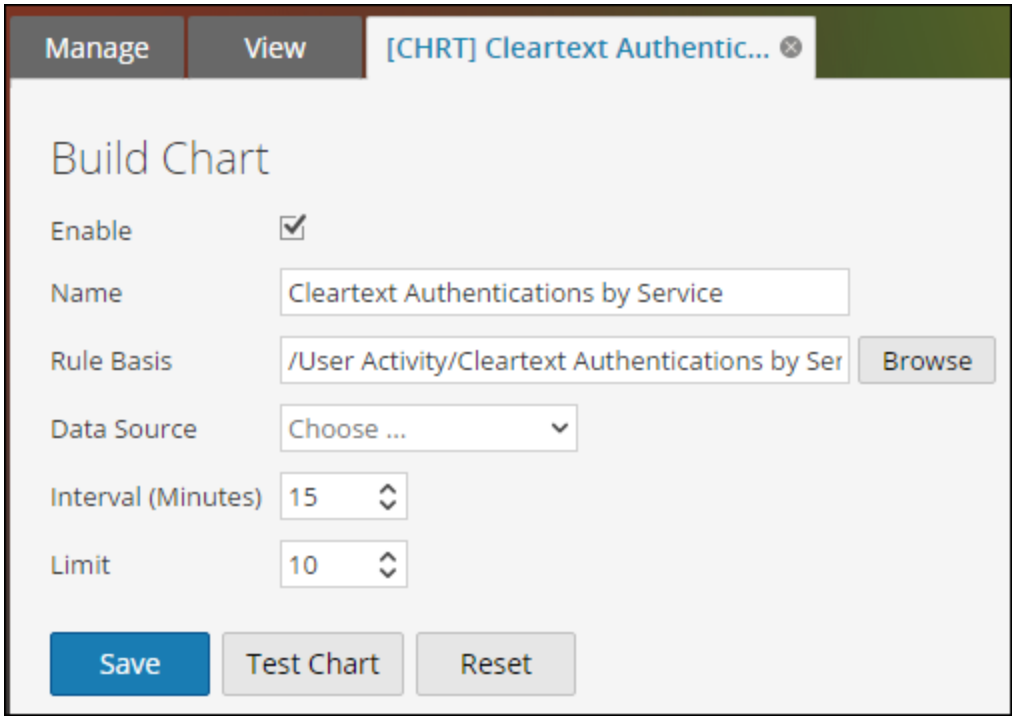
Modify a Chart

To modify a chart in a group or subgroup:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, do one of the following:
   - Double-click a chart or select a chart and click .

- Select a chart and click > **Edit**.

  The Build Chart view tab is displayed.



4. Modify the name of the chart.
5. For the Reporting Engine to collect the data and generate chart results, select the **Enable** checkbox.
6. (Optional) In the **Rule Basis** field, do the following:
   a. Click **Browse**.
      The Add Rule dialog is displayed.
   b. Navigate the Rule tree and select a rule.
   c. Click **Select**.
      The Rule appears in the Rule Basis field.
7. Select the data source from the **Data Source** drop-down list.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data sources. For more information, see the "Configure Data Source Permissions" topic in the *Host and Services Configuration Guide*.

8. (Optional) To modify the Interval value, click the up or down arrows.
9. Select the limit value to limit the number of records to be displayed.
10. Click **Save**.
    A confirmation message that the chart is modified successfully is displayed.

Delete a Chart

To delete a chart in a group or subgroup:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, do one of the following:
   - Select the charts and click .
   - Click > **Delete**.
     A confirmation message asks if you want to delete the selected chart.
4. Click **Yes** to delete the chart.
   A confirmation message that the chart is deleted successfully is displayed and the selected chart is deleted from the Chart List panel.

Duplicate a Chart

To duplicate an existing chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. From the **Chart List** panel, select a chart to be duplicated.
4. In the **Chart** toolbar, click .
   The chart is duplicated and gets added to the Chart List panel.

Import a Chart

To import charts from other instances of NetWitness:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. Click **Charts**.
   The Chart view is displayed.
3. From the **Chart Groups** panel, select a folder from which to import the file.
4. Do one of the following:
   - In the Chart toolbar, click > **Import**.
     The **Import Chart** dialog box is displayed. You can import multiple charts at the same time. To select multiple charts, press and hold the CTRL button and select the charts to be imported.
5. Click **Browse** to select the binary file.
   NetWitness provides a file system view of the files.
6. Locate the binary file and click **Open**.
   The file is added to the Import Chart list.
7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, select the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, select the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing chart in the library with an identically named chart in the binary file when importing, select the **Chart** checkbox. If you do not select the Overwrite option and an identical chart is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Export a Chart

To export selected charts to an external file:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, select a chart and click and do one of the following:
   - **Export** - This selection exports a chart in a .zip file.
   - **Export as Text** - This selection exports a chart from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple charts at the same time. To select multiple charts, select the checkboxes of the charts to be exported. The exported file is saved to the local drive.

Enable a Chart

To enable a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, select a chart or several charts that display ○ in the **Enabled** column.
4. Click ●.
   A confirmation message indicates that the chart(s) state is changed successfully.

Disable a Chart

To disable a chart:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Chart List** panel, select a chart or several charts that display ● in the **Enabled** column.

4. Click ○.

   A confirmation message indicates that the chart(s) status is changed successfully.

Search an Existing Chart

To search for an existing chart:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

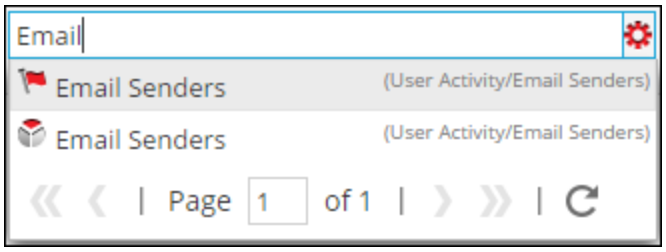
2. Click **Charts**.

   The Chart view is displayed.

3. In the **Chart** toolbar, enter text in the Search text box.

4. Click ⚙ > **Chart**.

   The charts with the substring in their name are displayed in the search drop-down list.



Refresh a Chart

To refresh charts:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Chart List** panel, drag and drop the charts to the desired group in the Chart Groups panel.

   The charts are moved to the new location.

4. Do the following:

   - In the **Chart List** panel, click ↻.
   - In the **Chart Toolbar** panel, select **Auto Refresh**.

     The Chart list is refreshed.

Alerting Overview

Alerts can be used to generate timely insights about current security issues, vulnerabilities, and exploits. For example, when a malicious email is sent from a compromised account, you would need an alert that automatically notifies you when such an event occurs.

The following concepts of alerting will help you understand more about alert rules, conditions, notifications, and templates.

Alert Rules

Alert rules specify the logic for alert generation. Alert rules allow you to set up threshold limits and define how to be notified if these limits are exceeded. For example, you may set up a rule to be alerted if the CPU usage remains abnormally high for 5 minutes or more.

Alert Definitions

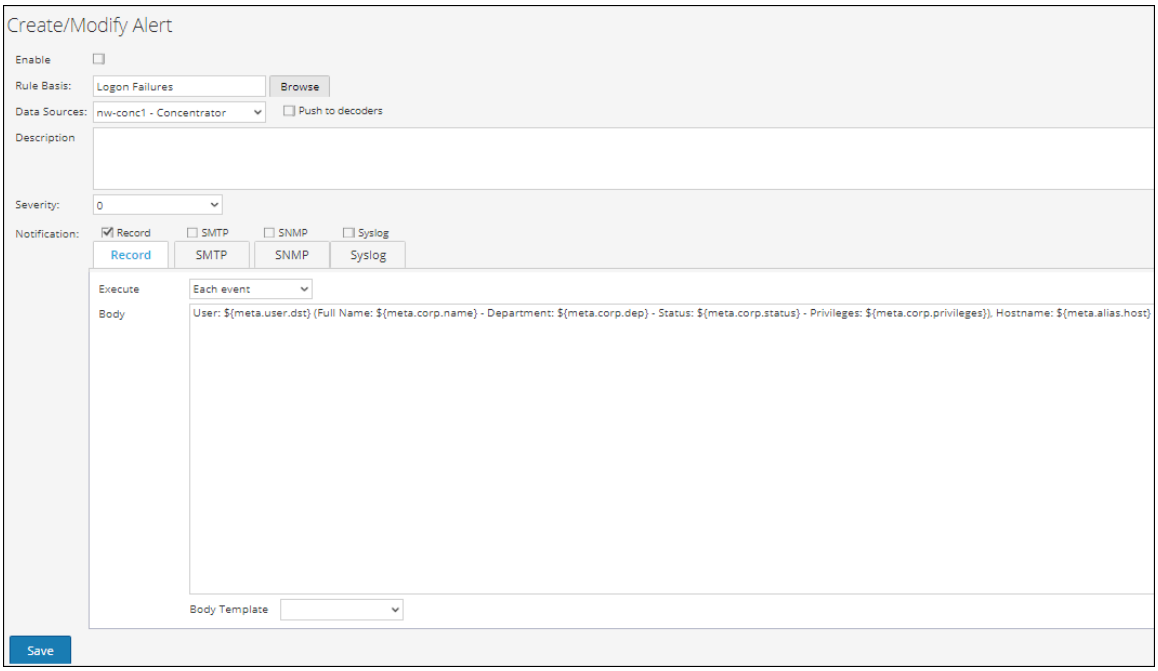
The alert definition is similar to defining rules for reports. These rules must be defined based on your use case. Alert definitions are made by selecting the alert rules you define in the Build Rule view. You select this rule while defining an alert.

Note: You can only alert using rules defined for NetWitness data source.

Once an alert is created, this data is collected from the Reporting Engine and displayed on the user interface.

Once an alert is defined, you can schedule the alert to run every minute (by default), or run at the present time, or run at the near future.

Note: In the NetWitness user interface, wherever Date and Time is displayed, it is always according to the user selected time zone profile.



Alert Notifications

The following are the components required to configure alert notifications:

- Notification server – Notification Server is used to send alert notifications. For example, SMTP mail server. Once you configure a notification server, you can add it to a rule. When the rule triggers an alert, the rule will use that server to send alert notifications.
- Notifications – Alert outputs, which can be email, SMTP, SNMP, and Syslog.
- Templates – The pre-defined format of an alert message.

When ever the rule condition is encountered, alerts get generated based on the severity level and notifies the user depending on the notification method set for that specific alert. The following are the various notification methods:

- Email/ SMTP: Simple Mail Transfer Protocol (SMTP) sends alert emails for system activity. Email alerts can be sent to their intended recipients by selecting SMTP as notification type.
- SNMP: Simple Network Management Protocol (SNMP) sends alerts to multiple computers for SNMP traps. SNMP alerts can be sent to other computers by selecting SNMP as notification type.

- Syslog: Syslog alerts generate notifications from Syslog messages. Syslog alerts can be sent by selecting Syslog as notification type.

Alerts can be configured to notify events that require attention, or as mechanisms to take automated actions based on conditions configured in an alert. An alert is sent when conditions within the entity have met the criteria selected for the alert. The notification criteria determines when and at what frequency the alert is generated.

Alert Templates

Alert templates are pre-defined format for an alert message. You can use these templates to create alerts.

Access Control for Alerting

Depending on the user role, the user is provided with specific set of access permissions in order to manage an alert. The Administrator manages the access rights provided to each user role from the **Administration > Security > Roles** tab. You can set access permissions for the user roles to manage an alert. The Reporting module provides access control at the alert level.

Note: Reporting Engine Alert permissions are prefixed with 'RE' to distinguish them from Event Streaming Analysis (ESA).

When you create users and user roles, ensure that the roles that you create for specific tasks have access to all the necessary permissions. This could require permissions at several levels of the role hierarchy.

Alerts can be combined with a specific set of user roles so that when a user logs into NetWitness, the only alerts they can access are alerts accessible by the role to which the user belongs. Users that belong to a user role with the '**Read & Write**' access permission can define alerts. The access can further be tightened so that the alerts are accessed only by those who have the '**Read Only**' access.

At the alert level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write
- Read Only
- No Access

Note: Before applying the Alert permissions, the default permission set for all the user roles is '**No Access**' permission and the checkbox is unchecked.

If you want to change the access permission for a specific user role, you must set it at the alert level. Except for administrators, the default permission set for all the other user roles is '**No Access**' permission.

The two scenarios are explained in brief:

- Scenario 1: Permissions applied to alert/ rules based on the user role.
- Scenario 2: Read-only permission applied to rules in the Alert.

	Role (Analysts)	Permissions applied to Alert/ Rules based on the user role	Permission (Read-only) applied to Rules in the Alert
Alert	**Read & Write**	**Read & Write**	**Read & Write**
Rules	**Read**	**Read**	**Read**

The Alert is assigned the role of a Security Analyst and permissions are set to **Read & Write** alerts.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the **Read** permission is set for the Rules except that the permission for the rules must not be higher than the permission for the Alerts.

If the permission for the rules is higher than the permission for the Alerts, the permission is not applied. For example, if you set the permissions for the Alert as **No Access** and then specify the option *Apply Read-only permission to Rules in the Alerts*, the read-only permission is not set for the rules.

Access Control for an Alert When Multiple Alerts are Selected

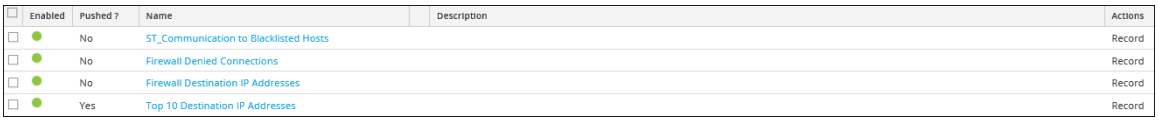
When you want to change permissions of multiple alerts, you must select several alerts and set their access permissions using the Alert Permissions panel. The access permission that you choose is applied to all the selected alerts.

Log in as a specific user and view the access details

When you log in to the NetWitness UI as a user having **Read** access permission, all the alerts will be denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Alert List panel.

When you log in to the NetWitness UI as a user not having **Read & Write** access permission on an Alert, all the alerts will be denoted with the symbol ( ) and the alerts appear grayed out on the Alert List panel.

The following figure shows the Alert List panel when logged in with minimal **Read & Write** access permission.

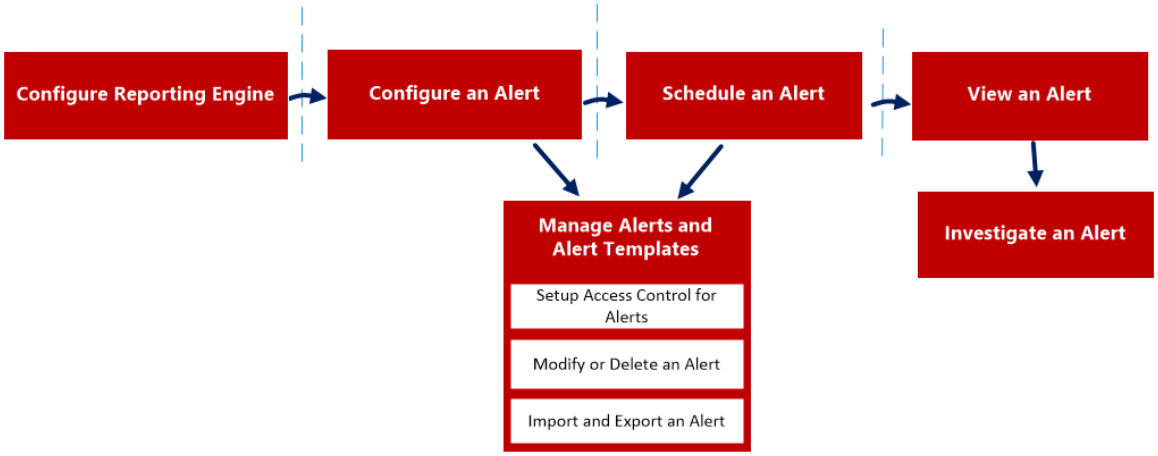


Note: If a user (other than ADMIN) creates an alert, ADMIN cannot access that alert.

The following table lists the various columns in the Alert Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness user interface.
Read & Write	The user can access, view, edit, import, export, and delete the alert on the Alerts page. The user can also change the permission on the alert.
Read Only	The user can only access and view the alert on the Alerts page.
No Access	The user cannot access or view the alert for which this permission is set.
Apply Read-only permission to Rules in the Alerts	The user can automatically apply permissions to the rules in the alerts.

The following is an overview of the entire process of alerting:



To configure and generate an alert on Reporting Engine, perform the following:

1. Configure Reporting Engine
2. Configure an Alert
3. Schedule an Alert
4. View an Alert
5. Investigate an Alert
6. Manage an Alert and Alert Template

Configure Reporting Engine

Ensure that:

- You have Decoders that are connected to the Concentrator added to the Reporting Engine for the selected data source, before creating an alert rule.
- You have installed and configured a Syslog server that supports TCP/TLS in your environment. For example, WinSyslog. You can configure the Reporting Engine to send Syslog messages over TCP with Transport Layer Security (TLS) when an alert is triggered.

To configure the Reporting Engine to send Syslog alerts over TCP with Transport Layer Security (TLS):

1. Obtain the required certificates.
2. Append the CA certificate to the ca.pem file on the NetWitness server.
3. Configure the Syslog server to accept messages from client machines.
4. Configure the delivery of alert messages in the NetWitness UI.

Task 1: Obtain the required certificates

To generate certificates for configuring Reporting Engine to send Syslog messages over TCP with TLS:

1. Generate a Certifying Authority (CA) certificate. For more information, see http://www.rsyslog.com/doc/tls_cert_ca.html.

Note: You can ignore this step if you already have a CA running in your environment.

2. Generate a key pair for the Syslog server. For more information, see http://www.rsyslog.com/doc/tls_cert_machine.html.

Note: You can ignore this step if you have already configured security for the Syslog server using the key and certificates generated by the same CA.

Task 2: Append the CA certificate to the ca.pem file on the NetWitness Server

To append an existing CA certificate to the ca.pem file:

1. Manually append the contents of the CA certificate that you generated to the **/etc/pki/CA/certs/ca.pem** file.

2. Run the following command on the NetWitness server to have the certificate populate to the Truststore:
   `keytool -import -file /etc/pki/CA/certs/ca.pem -keystore cacerts`

Task 3: Configure the Syslog Server to accept messages from client machines

To configure the Syslog server to accept messages from client machines that have the same CA certificates:

1. Copy the following files to your secure TCP server target location:
   - ca_cert.pem
   - server_cert.pem
   - server_key.pem

   Where:

   ca_cert.pem - is the CA certificate

   server_cert.pem - is the server certificate

   server_key.pem - is the server key

   For more information, see the documentation specific to your Syslog server. If you are using rsyslog, refer to http://www.rsyslog.com/doc/tls_cert_server.html.

Task 4: Configure the delivery of alert messages in NetWitness

Configure Reporting Engine to send Syslog messages over TCP with Transport Layer Security (TLS) when an alert is triggered by enabling **SECURE_TCP** in the **Output Actions** tab for the Reporting Engine service in the Reporting Engine Services Config View. For more information, see the **"Reporting Engine Output Actions"** topic in the *Host and Services Configuration Guide*.

Configure an Alert

You can configure an alert by setting up alert notifications and adding a notification method to a rule.

Note: Only Administrators can set up these notifications.

To configure an alert:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click .
   The Create/Modify Alert panel is displayed.
4. Click **Enable** to enable the alert.
5. In the **Rule Basis** field:
   a. Click **Browse**.
      The Lookup Rule Basis dialog box is displayed.
   b. Navigate the Rule tree and select a rule.
   c. Click **OK**.
      The Rule name is displayed in the Rule Basis field.
6. From the **Data Sources** drop-down list, select a data source.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse Connector data sources. For more information, see **"Configure Data Source Permissions"** topic in the *Host and Services Configuration Guide*.
7. Select the **Push to decoders** checkbox for the Reporting Engine to send the rule to the Decoder.
8. (Optional) Enter an alert description in the **Description** field.
9. From the **Severity** drop-down list, select the severity level.
10. In the **Notification** field:
    a. Select the appropriate notification.
       The selected notification tab is displayed in the Create/Modify Alert

dialog box.

b. (Optional) Deselect the notification to disable the notification tab.

c. Define an action in one of the **Notification** tabs:

   i. In the **Record** tab field:

      a. From the **Execute** drop-down list, select the frequency for recording an alert.

      b. Enter the RECORD message. You can create a new message or select a template in the **Body Template** field and modify the template here.

      c. (Optional) If templates have been defined, select a template for the RECORD message that you can use as is or modify.

   ii. In the **SMTP** tab field:

      a. From the **Execute** drop-down list, select a value to identify the number of times to send an email message for the alert.

      b. Enter an email address or comma-separated list of email addresses to send this alert.

      c. Enter the subject of the email message.

      d. Enter the body of the message. You can create a new message or select a template in the **Body Template** field and modify the template here.

   iii. In the **SNMP** tab field:

      a. From the **Execute** drop-down list, select a value to identify the number of times that you want to send an SNMP message for the alert.

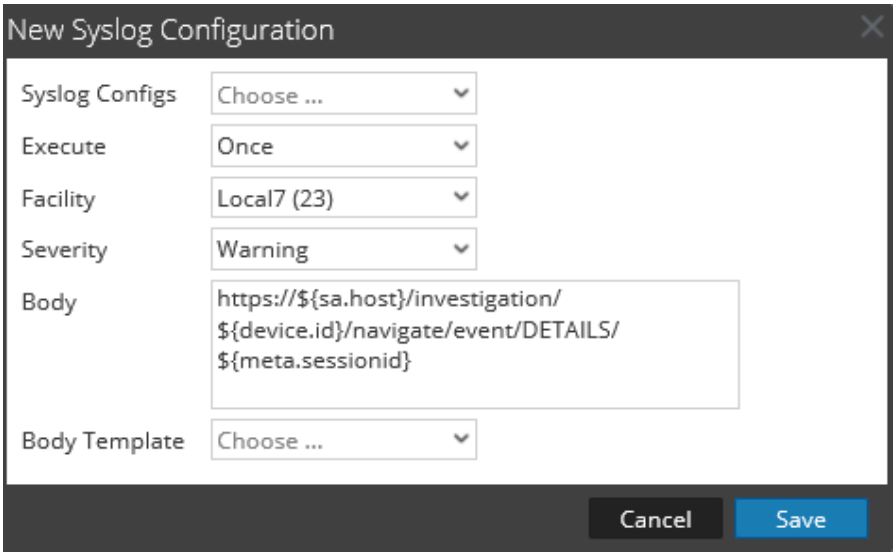
      b. Enter the SNMP message. You can create a new message or select a template in the **Body Template** field and modify the template here.

iv. In the **Syslog** tab field:

> **Note:** You can configure Multiple Syslog servers on the Syslog Configuration panel. For more information, see **"Reporting Engine Output Actions"** topic in the *Host and Services Configuration Guide*.

a. Click +.

The New Syslog Configuration dialog box is displayed.



b. From the **Syslog Configs** drop-down list, select a value for the syslog configuration.

c. From the **Execute** drop-down list, select a value to identify the number of times to send a Syslog message for the alert.

d. From the **Facility** drop-down list, select the facility.

e. From the **Severity** drop-down list, select the severity level.

f. Enter the Syslog message. You can create a new message or select a template in the **Body Template** field and modify the template here.

> **Note:** If you want to add a metakey, specify the same in the format: ${meta.metakey}. For example, ${meta.ip.dst}.

g. Click **Save**.

The Syslog configuration gets added to the alert.

11. Click **Create**.

NetWitness creates an alert with a confirmation message that the alert is

saved successfully. NetWitness generates the alert and executes the output actions every minute.

Schedule an Alert

You must schedule an alert to search for events on a regular schedule.

To schedule an alert:

1. Go to **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Select an alert to schedule.
4. On the **Alert** toolbar, click **Enable**.
   The selected alert is scheduled.

View an Alert

You can view an alert or a list of all alerts.

You can view the alerts triggered and investigate any alert in the Investigation module and customize these views to show alerts for a specific period of time, and set the maximum number of alerts displayed in a single page.

To view an alert:

1. Go to **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. On the **Alert** toolbar, click **View Alerts**.
   The View Alerts view is displayed.

Investigate an Alert

You can investigate every alert that is triggered on the Alert View. For more detailed investigation on a particular alert, you can view the alert on the Investigation module.

To investigate an alert:

1. In the **Alert** section toolbar, click **View Alerts** to navigate to the View Alerts view.
2. Do one of the following:
   - Click the button against the alert you want to investigate.
     The Investigation module displays the details of the first session that registered the match for the given alert for immediate analysis.
   - Click on the alert name of the alert you want to investigate.
     The Investigation module displays all matches for that particular alert for the hour surrounding the registered alert.

Manage an Alert and Alert Template

You can manage alerts, scheduled alerts, and alert templates using the following procedures.

Manage an Alert

Depending on the access permissions set for the user role, you can modify or delete, import and export, enable or disable alerts, view or refresh an alert list.

Access Control for an Alert When a Single Alert is Selected

To set access permissions for an alert:

1. Go to **Monitor> Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the Alert List panel, select an alert.
4. Click > **Permissions**.
   The Alert Permissions dialog box is displayed.
5. Based on the user role, select the appropriate options.
6. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.

Note: When the check box is selected, all dependent rules with the No access permission will be given the READ access permission.

7. Click **Save**.
   A confirmation message that the permission is successfully set for the selected alert is displayed.

Access Control for an Alert When Multiple Alerts are Selected

To change permissions of multiple alerts:

1. In the Alert List panel, select all the alerts whose permissions must be set.
2. Click > **Permissions**.
   The Alert Permissions dialog box is displayed.
3. Select the permission to set for the respective user role.

4. Click **Save**.

   A confirmation message that the permission is successfully set for all the selected alerts is displayed.

Edit an Alert

For example, if you want to be notified about the alert over an email on a different Email ID, you will have to modify the alert notification section with the new Email ID details to be reverted over an email when an alert is generated. Additionally, you can also modify the alert description and alert notification in the Create or Modify Alert panel.

To edit an alert:

1. Go to **Monitor**> **Reports**.

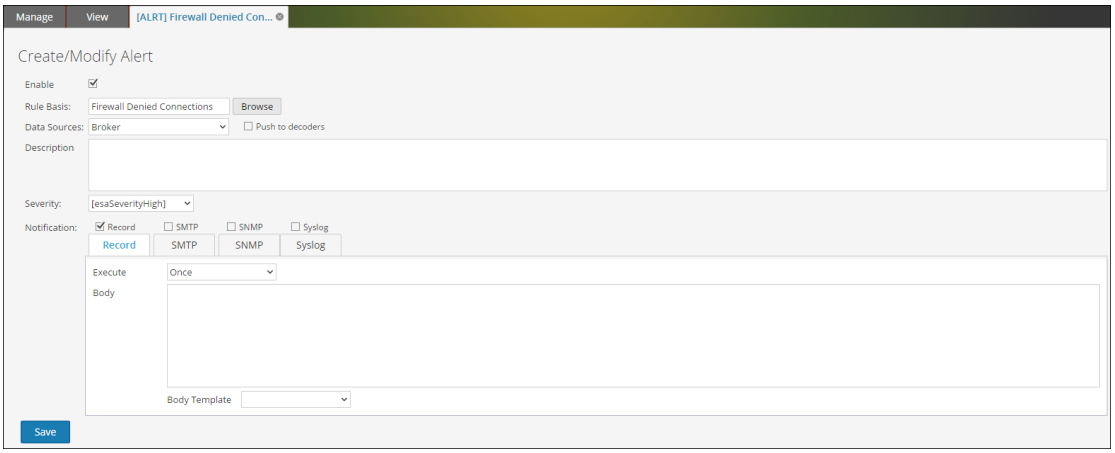
   The Manage tab is displayed.

2. Click **Alerts**.

   The Alert view is displayed.

3. In the **Alert List** panel, select an alert and click .

   The Create or Modify Alert tab is displayed.



4. In the **Rule Basis** field, navigate the rule tree and select another rule. The Rule name is displayed in the Rule Basis field.

5. (Optional) Select a data source from the **Data Sources** drop-down list.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see **"Configure Data Source Permissions"** topic in the *Host and Services Configuration Guide*.

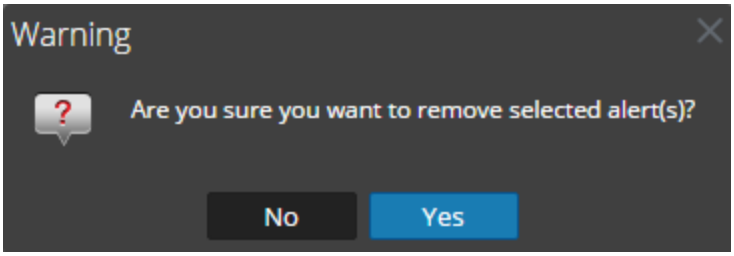
6. (Optional) Modify the alert description in the **Description** field.

7. Modify the appropriate **Notification** tabs – **RECORD**, **SMTP**, **SNMP**, and **Syslog**.
8. Click **Save**.
   A confirmation message that the alert is modified successfully is displayed.

Delete an Alert

To delete an alert:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert List** panel, select the alert and click .
   A warning dialog asks for confirmation that you want to remove the selected alerts.



4. Click **Yes** to delete the alert.
   A confirmation message that the alert is deleted successfully is displayed and the selected alert is deleted from the Alert List panel.

Import an Alert

To import an alert from other instances of NetWitness in the Alerts List panel:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click > **Import**.
   The Import Alert dialog box is displayed.
4. Click **Browse** to select the binary file.
   NetWitness provides a file system view of the files. You can import

multiple alerts at a time. To select multiple alerts, select the checkbox of the alert to be imported.

5. Locate the binary file, and click **Open**.
   The file is added to the Import Alert list.
6. (Optional) To overwrite any existing alert in the library with an identically named alert in the binary file when importing, select the Alert checkbox. If you do not select the Overwrite option, and an identical alert is encountered in the binary file, the binary file is imported and no error message is displayed.
7. Click **Import** to import the binary file.

Export an Alert

To export an alert to an external file that can be later imported to NetWitness:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert List** panel, select an alert and click and do one of the following:
   - **Export** - This selection exports an alert in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format. You can export multiple alerts at a time. To select multiple alerts, check the checkbox of the alert to be exported.
4. Click > **Export**.
   The exported binary file is saved to the local drive.

Enable an Alert

To enable an alert:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.

3. In the **Alert List** panel, select the alert that displays ○ in the **Enabled** column.
4. Click Enable.
   A confirmation message shows that the change to the alert(s) state was successful.

Disable an Alert

To disable an alert:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert List** panel, select the alert that displays ● in the **Enabled** column.
4. Click ○ Disable.
   A confirmation message shows that the alert(s) status is changed successfully.

View an Alert List

To view an alert list:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click **View Alerts**.
   The View Alerts view tab is displayed.
4. Select the last number of days from the drop-down list.
5. Enter a value for the **Max no of alerts**.
   The alerts list is displayed based on the chosen filter value.

Refresh an Alert List

To refresh the list of alerts:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.

2. Click **Alerts**.
   The Alert view is displayed.
3. From the Alert toolbar, click to refresh the alerts list.
   The Alert List panel is refreshed.

Manage a Scheduled Alert

You can enable or disable a scheduled alert, and view all scheduled alerts.

Enable a Scheduled Alert

To enable a scheduled alert:

1. Go to **Monitor> Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click View Schedule.
   The View Alerts Schedule view tab is displayed.
4. In the **Alerts Schedule List** panel, select the scheduled alert (s) to be enabled.
5. Click ●.
   A confirmation message indicates that the alert(s) status is changed successfully and the alert is now available in the Alert List panel.

Disable a Scheduled Alert

To disable a scheduled alert:

1. Go to **Monitor> Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click View Schedule.
   The View Alerts Schedule view tab is displayed.
4. In the **Alerts Schedule List** panel, select the scheduled alert (s) to be disabled.
5. Click ○.
   A confirmation message indicates that the alert(s) status is changed successfully and the alert is now available in the Alert List panel.

View all Alerts Scheduled

To view all the alerts scheduled:

1. Go to **Monitor> Reports**.
   The Manage tab is displayed.

2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click **View Schedule**.
   The View Alerts Schedule view is displayed with a list of all the scheduled alerts.

Manage an Alert Template

You can modify or delete an alert template, and view all alert templates.

Edit an Alert Template

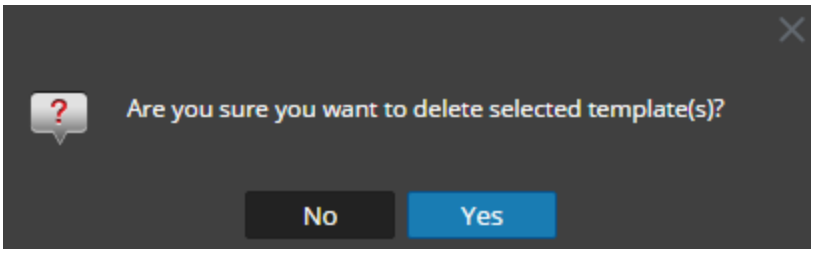
To edit an alert template:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click Template.
   The Template view is displayed.
4. In the **Template List** panel, select a template and click .
   The Create/Modify Template dialog box is displayed.
5. Click **Save**.
   A confirmation message that the template is modified successfully is displayed.

Delete an Alert Template

To delete an alert template:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click Template.
   The Template view tab is displayed.
4. In the **Template List** panel, select a template and click .
   A confirmation dialog is displayed.



5. Click **Yes** to delete the template.
   A confirmation message that the template is deleted successfully is displayed.

View all Alert Templates

To view all alert template messages:

1. Go to **Monitor**> **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click **Template**.
   The Template view tab is displayed with a list of templates.

Reporting Reference

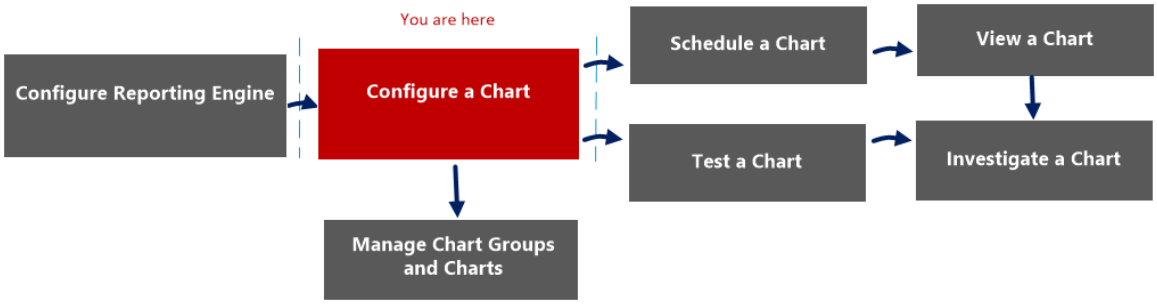
This section provides information about the Reporting user interface. You can look at your place in the workflow for creating and generating a report with theNetWitness Suite, get a quick look at the important features, and follow links to the detailed concepts and procedures.

Build Chart View

In the Build Chart view, you can define and test a chart. You build a chart by assigning a name and then selecting a rule to include.

Note: Only the Netwitness DB rules can be used in charts.

Workflow



What do you want to do?

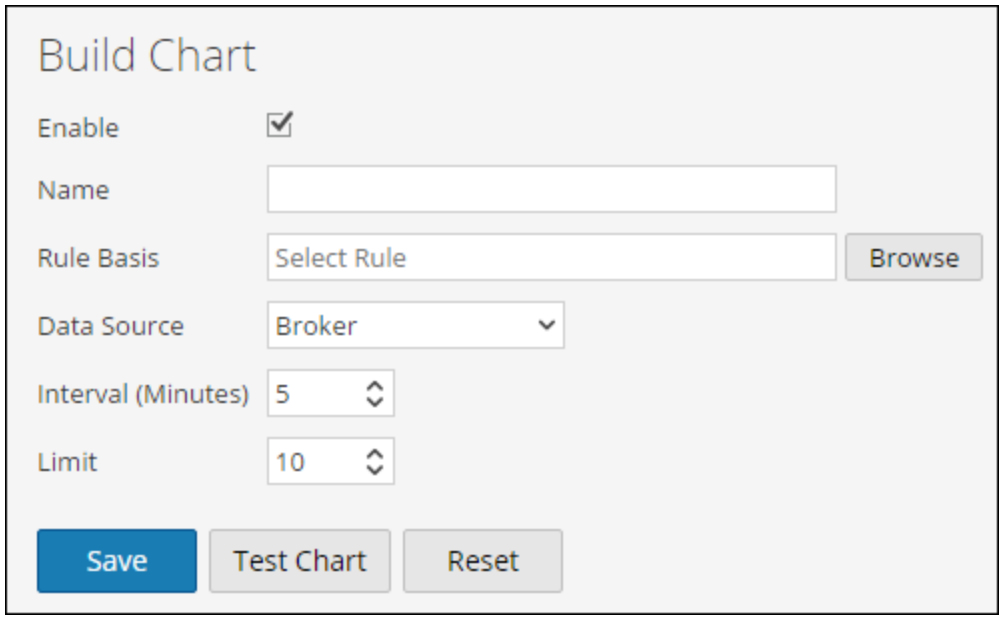
Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart*	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart

Role	I want to ...	Documentation
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

*You can complete these tasks here.

Quick View

The following figure is an example of the Build Chart view.



The following table describes the features in the Build Chart view.

Field	Description
Enable	Specifies if the Reporting Engine must collect the data and generate chart results. If the **Enable** checkbox is not selected, the results are not rendered.
Chart Name	Identifies the name of the chart.

Field	Description
Rule Basis	Displays the Add Rules dialog box from which you select a rule that is the basis of a chart. The rule that you select must be a rule which is not sorted by none.
Data Source	If the default data source is configured in the Reporting Engine, the data source is displayed on the Build Chart page. If a chart is configured to run on any other data source, that data source is displayed on the Build Chart page instead of the default data source. The Reporting module works with the following data sources: • Broker • Concentrator • Decoder • Log Decoder • Log Collector
Interval (Minutes)	The chart data refresh interval in minutes.
Limit	The number of records for which a chart is generated.
Save	Saves a chart to the database.
Test Chart	Plots a test chart based on the chart definition.
Reset	Resets the chart details.

Build List View

In the Build List view, you can enter or import values to create a list and save or reset the values. You can use lists when you are writing reporting rules to simplify the process of specifying values in the rule.

Workflow

This workflow shows the procedure to define lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists.

You must ensure that Reporting Engine is configured on the NetWitness Suite.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report

Role	I want to ...	Show me how
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

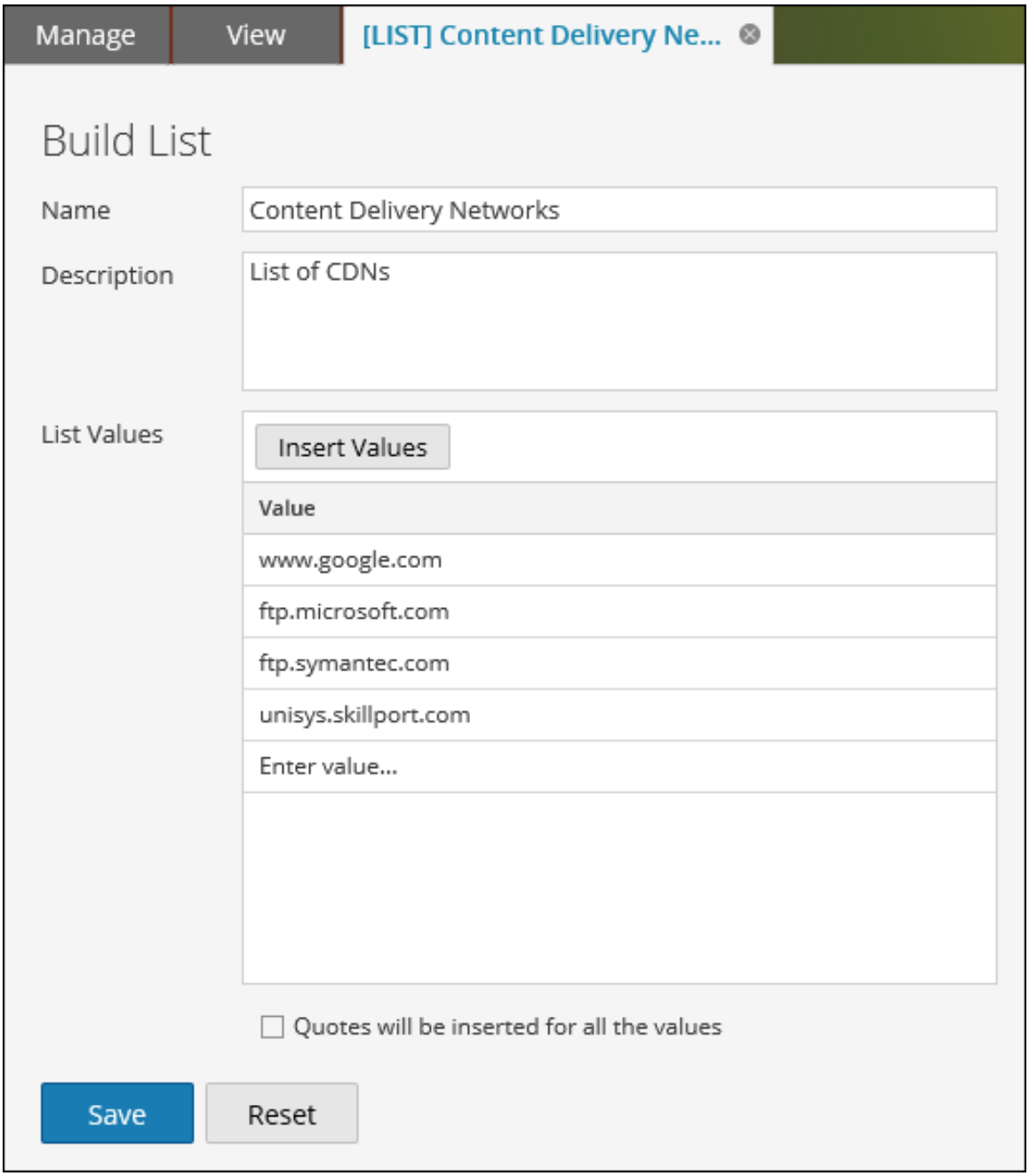
*You can complete these tasks here.

Related Topics

- List View
- Lists Permissions Dialog

Quick View

The following figure shows the Build List View.



To access this view

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The Lists view is displayed.

3. In the **Lists** toolbar, click +.

   The Build List tab is displayed.

The following table describes the features in the Build List view.

Feature	Description
Name	Identifies and labels the list.
Description	Provides a short description for the list.
List Values	Provides the grid of values associated with selected list from the List Library panel. You can import these values from a file or list. You can also enter values manually.
Quotes will be inserted for all the values	Automatically includes quotes for the values at runtime if checkbox is selected. If the checkbox is not selected and if a value in the list contains a comma, then that value has to be enclosed within single quotes. This syntax does not apply to list values for an NWDB rule.
Save	Saves the rule which can be used to create a report, a chart or an alert.
Reset	Deletes all the information from the fields.

Build Report View

In the Build Report view, you can create a report, add text and rules, and schedule a report.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

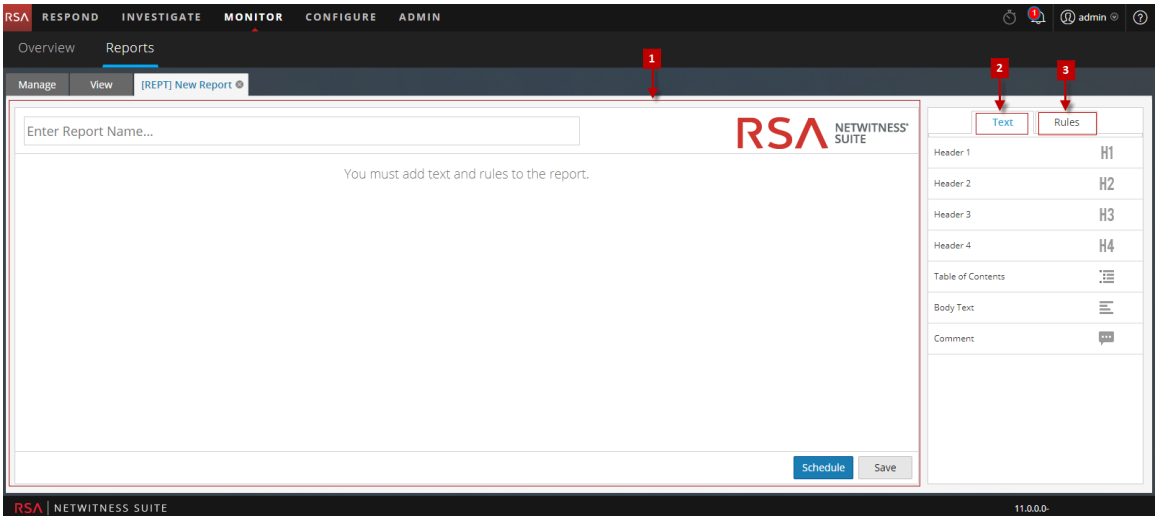
*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Scheduled Reports View
- Reports Permissions Dialog

Quick View

The following figure shows the Build Report View.



To access this view

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Reports view is displayed.

3. In the **Reports** toolbar, click +.

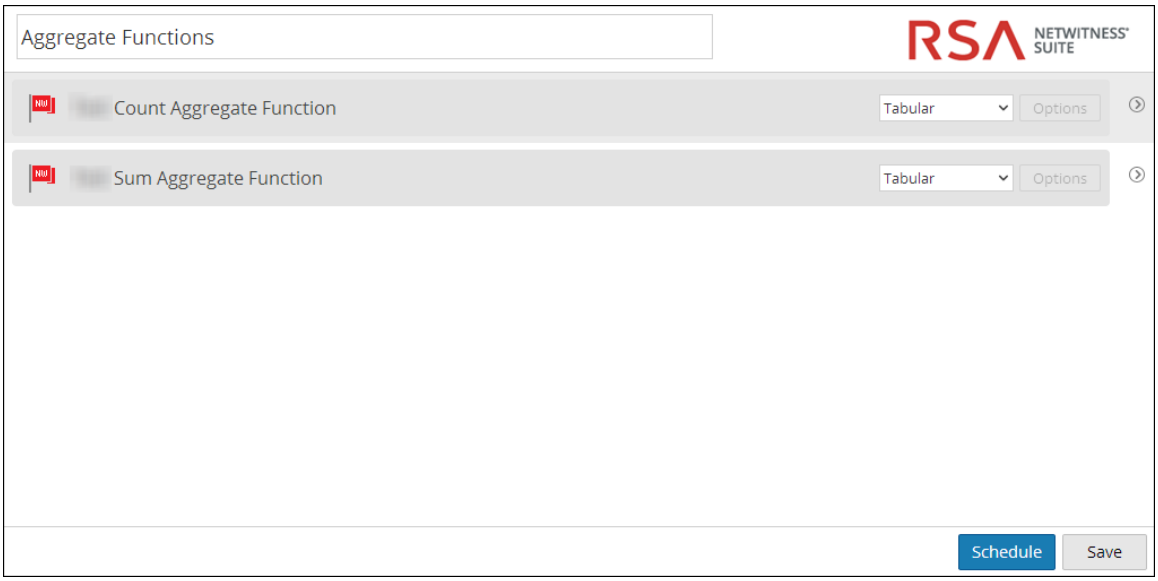
   The Build Report tab is displayed.

The Build Report view consists of the following panels:

1. Report Panel
2. Text Panel
3. Rules Panel

Report Panel

The Report panel allows you to create a report by assigning a name to the report. The content in a report depends on the items selected from the Text and Rules panels.



When you add rules to a report, you can change the output format of these rules either to tabular, area, line or pie by clicking the ˅ button.

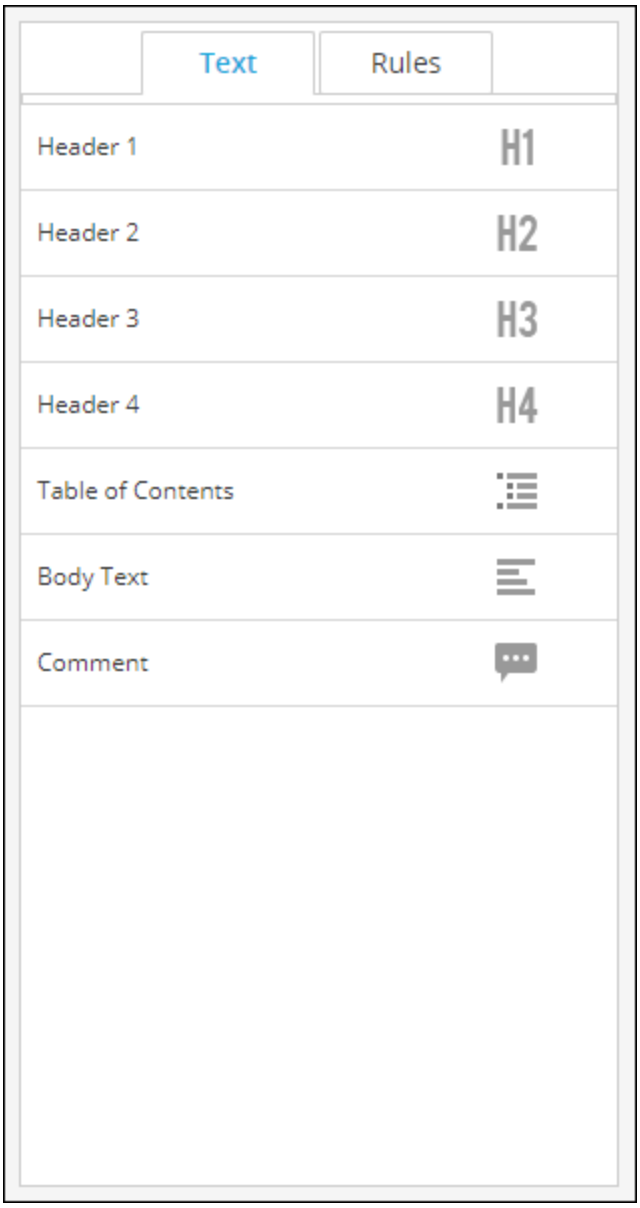
The following table lists the features of the Report Panel and the description.

Feature	Description
Name	This field allows you enter the name of the report.
Options	This field allows you to select the output format of the report such as Tabular, Area, Bar, Bubble, Column, Line, Pie, Step Line, Step Area, Spline Area and Spline.
Schedule	Clicking this option generates the report.
Save	Clicking this option saves the report.

Text Panel

The Text panel consists of a list of text elements that add to the look and feel of the report. You can use these text elements to format the report.

- To add more structure to reports, you can use these headers defined in the Text panel to indent up to four levels. This allows you to identify specific sections in a report that can be included in the Table of Contents for easy navigation in the report result.
- To add headers to the Report panel, drag and drop H1, H2, H3, or H4 onto the Report pane based on the desired level of indentation.



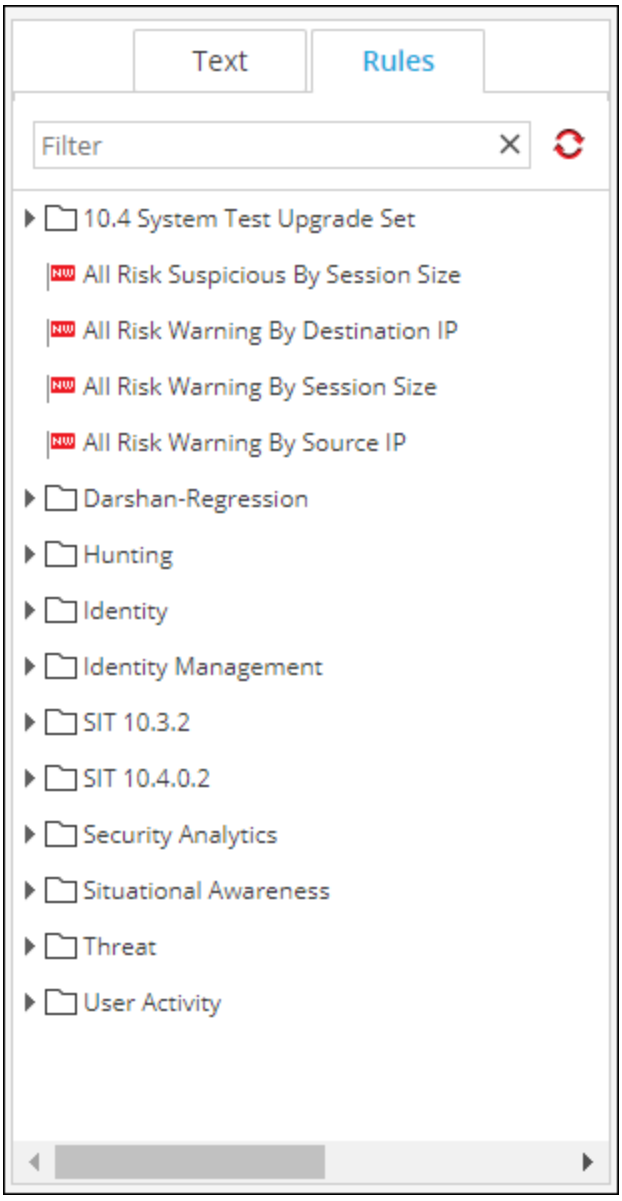
The following table lists the text elements used to format a report:

Text Elements	Description
Header 1	The Header 1 element adds a first-level heading to the report definition.
Header 2	The Header 2 element adds a second-level heading to the report definition.
Header 3	The Header 3 element adds a third-level heading to the report definition.
Header 4	The Header 4 element adds a fourth-level heading to the report definition.
Table of Contents	The Table of Contents adds table of contents to the report definition.
Body Text	The Body Text element adds body text to the report definition.
Comment	The Comment element adds comments to the report definition. **Note:** The Comment element is not displayed when you view all the reports.

Rules Panel

The Rules panel consists of a list of rules that are defined in the Rules. From the rules list, you can drag and drop rules onto the Report panel to associate those rules with the report.

You can search for a specific rule using search text box provided in the Rules panel.


Text
Rules
Filter
10.4 System Test Upgrade Set
All Risk Suspicious By Session Size
All Risk Warning By Destination IP
All Risk Warning By Session Size
All Risk Warning By Source IP
Darshan-Regression
Hunting
Identity
Identity Management
SIT 10.3.2
SIT 10.4.0.2
Security Analytics
Situational Awareness
Threat
User Activity

Build Rule View

The Build Rule view explains the actions and associated procedures that you can perform under Rules.

Workflow

This workflow shows the procedure to create or deploy a rule.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

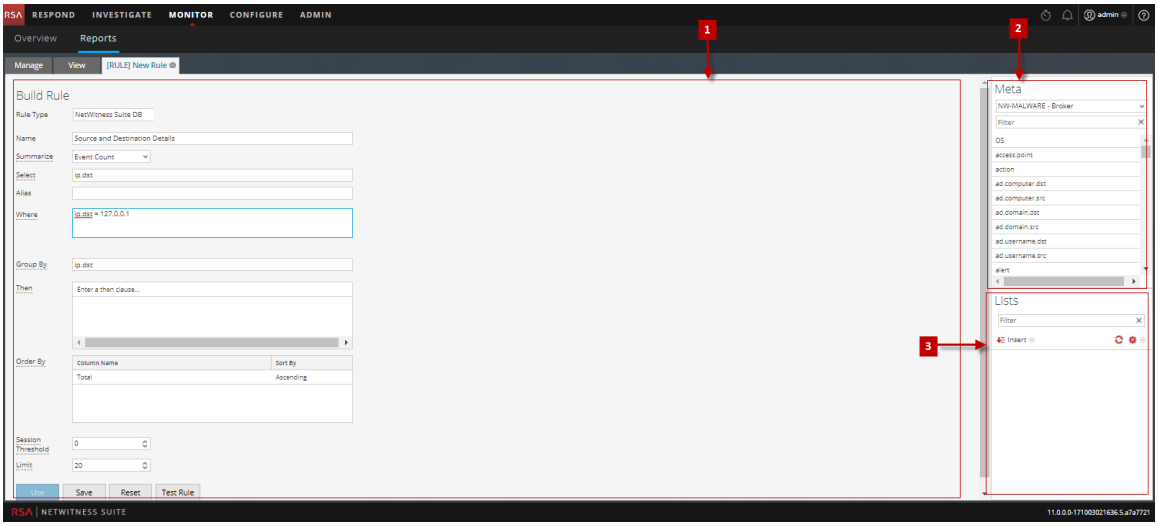
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Rule Permissions Dialog
- Rule View

Quick View



To access the Build Rule view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the Rule toolbar, click + > **NetWitnessDB**.
   The Build Rule view tab is displayed

Features

The Build Rule view includes the following panels.

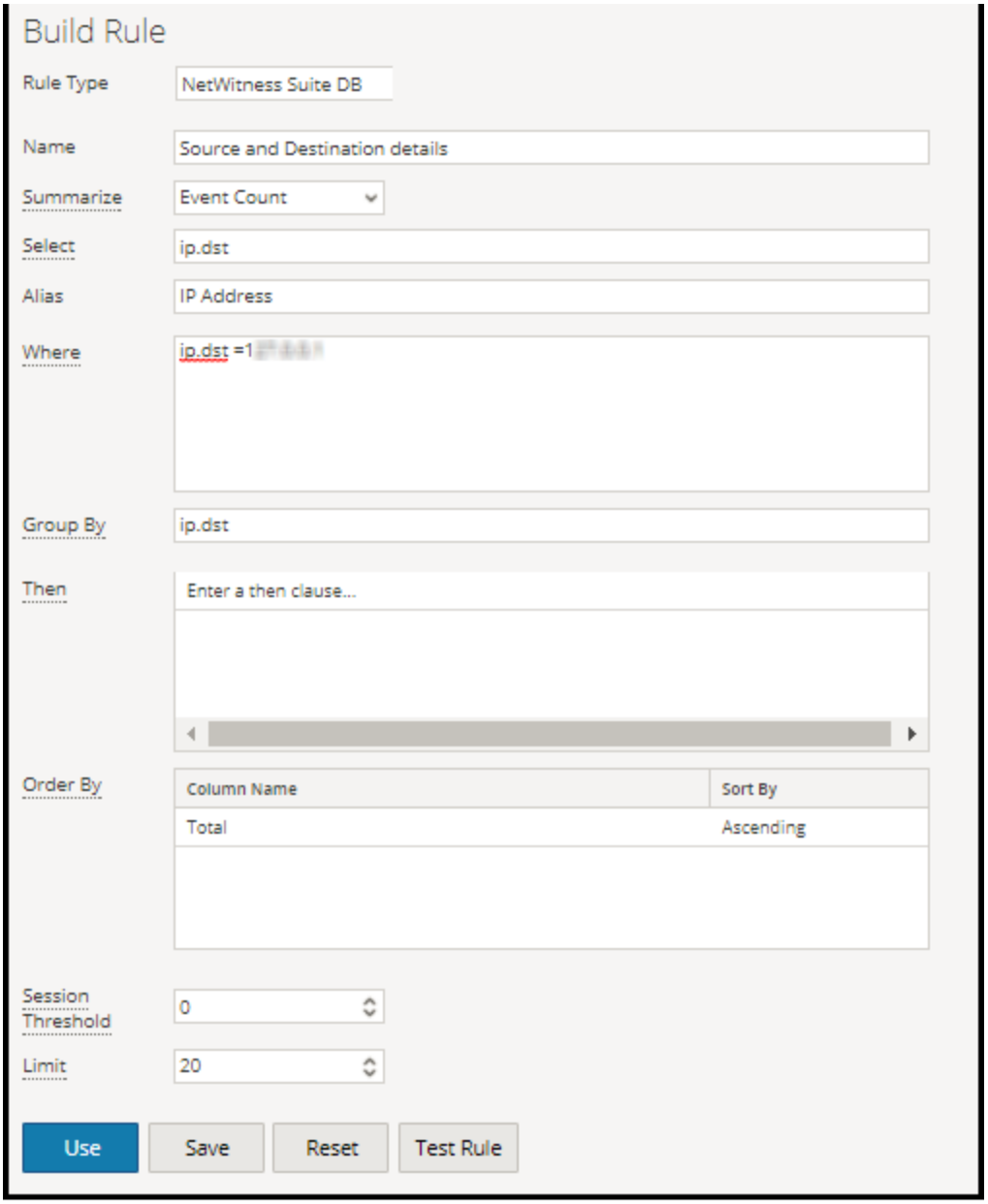
1	Rule panel
2	Meta panel

3 Lists panel

Rule Panel

The Rule panel allows you to create a rule for the selected database type.

The following figure shows the Rule panel.



The following table describes the features in the Rule panel.

Feature	Description
Rule Type	A drop-down list of supported database types for which you can create rules. The options are: Netwitness DB and Warehouse DB.
Name	The name of the rule that you are creating or editing.
Summarize	A drop-down list of summarize options. The options are: None, Event Count, Packet Count, Session Count and Custom.
Select	The meta key for which you need the aggregate values; for example, ip.dest.
Where	A Where clause that defines the conditions that trigger the rule execution; for example, ip.dest = 127.0.0.1.
Group By	The grouping method for the results. For example, specifying ip.dest produces a report in which like ip.dest values are grouped.
Then	A Then clause that defines the rule actions for additional processing on the output.
Order By	The sequencing method used to show results. For example, specifying Order By the value in the Total column, Ascending, produces a report in which the results are sorted in ascending order based on the value in the Total column.
Session Threshold	A selection list for the session threshold, which specifies maximum number of sessions that should be processed for aggregate functions.
Limit	A selection list for the maximum number of result rows to be fetched.
Use	Clicking Use enables you to use the Rule to generate a Report, Alert of Chart.

Feature	Description
Save	Clicking Save saves the rule that you are editing and the Build Rule panel remains open. Before testing a rule, you must save it if you want to keep your changes.
Reset	Clicking Reset clears all the field information .
Test Rule	Clicking test rule opens the Test Rule dialog.

Test Rule Dialog

To access the Test Rule view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the Rule List panel, do one of the following:
   - Select a rule and click in the Rules toolbar.
   - Click > **Edit**.
     The Build Rule view tab is displayed.
3. Click **Test Rule**.
   The Test Rule view is displayed.

The following table describes the features in the Test Rule Dialog.

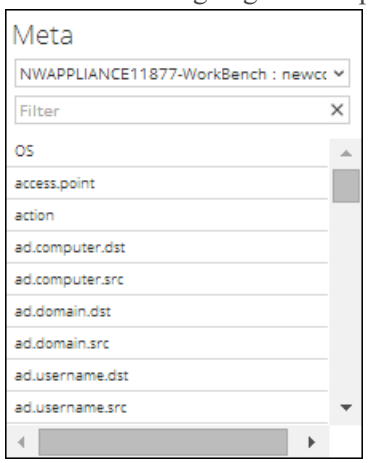
Feature	Description
Data Source	A drop-down list of data sources for the type of rule you are testing. Possible data sources are: Concentrator, Broker, Decoder or Log Decoder.
Format	A drop-down list of the formats for displaying results for the rule. Possible formats are: Tabular, Area, Bar, Bubble, Column, Line, Pie, Step Line, Step Area, Spline Area, and Spline.
Time Range	A drop-down list of time range specification methods. • Selecting Past allows you to specify a number of years, months, days, weeks, or hours. For example, Hours, Days, Weeks, Months, or Years. • Selecting Range allows you to specify a date range and time period. For example, start date to end date. In the user interface, the date or time displayed depends on the time zone profile selected by the user.
Use relative time calculation	Selecting this option calculates the time range relative to the current time.
X Axis	X-Axis and Y-Axis specify the metadata to be plotted in charts. In the X-Axis drop-down list, the meta types for the `Group by` setting in the rule are listed. You can select multiple meta types when the rule has a single `Group by` setting. For Custom Rules with multiple `Group by` values, you can select only the first meta type for the X-Axis.

Feature	Description
Y Axis	In the Y-Axis drop-down list, the aggregate functions used in the rule are listed. Sum, Count, Countdistinct and Average are the supported aggregate functions for rules. You can select one or more aggregate functions.
Run Test	Clicking Run Test executes a test of the rule last saved in the Rule Builder dialog. When the test is complete, the rule data (if any) for the selected time range is displayed.

Meta Panel

The Meta panel provides a list of available meta types that you can use to build the rule. You can use the meta types in the Select, Where, and Then clauses. The Reporting Engine maintains an active list of the available meta names by continuously synchronizing with the data source to which it is connected.

The following figure displays the Meta panel.



The following table describes the features in the Meta panel.

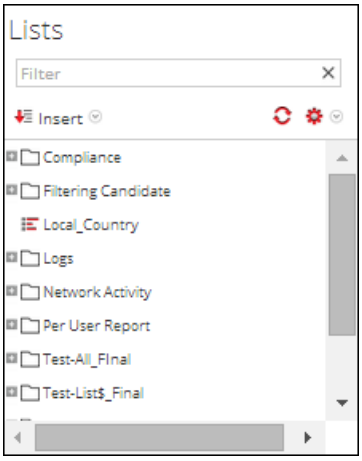
Operation	Description
Choose	Based on the rule type that you have selected, the available data sources are displayed in the drop-down list of the Meta panel. Select the required data source. The available meta types for the data source are displayed. Select a meta.
Filter	Filter the meta for a specific meta value.

Lists Panel

A List is a placeholder for a set of values that you can use in a meta or a variable. For example, you can define a list with all the whitelisted event source IP addresses. Once the List is defined then you can use the List name in the rule. This provides the flexibility of adding, modifying, and deleting the list values.

The Lists panel is a collection of Lists. The Reporting Engine maintains an active list of the available list names by continuously synchronizing with the collection to which it is connected.

The following figure displays the Lists panel.



The following table describes the features in the Lists panel.

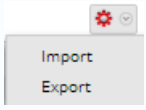
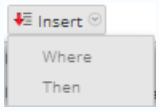
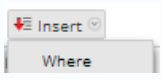
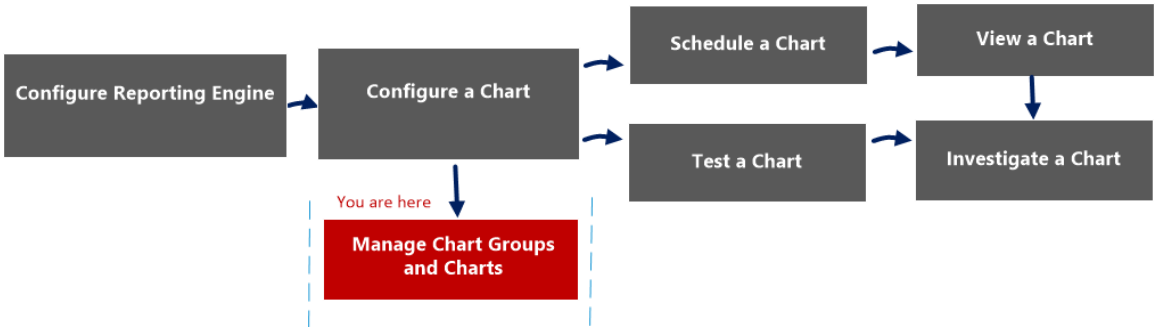
Operation	Description
	Import or Export a list.
	Refresh the Lists.
	If you select the **NetWitness DB** rule type, the options Where and Then are displayed. Insert the list in the Where or Then clause in the rule.
	If you select the **Warehouse DB** rule type, the option Where is displayed. Insert the list in the Where clause in the rule.

Chart Permissions Dialog

In the Chart Permissions dialog, you can manage access permissions for user roles at the chart and chart group level. Only a user with the 'Read & Write' permission can configure the chart in the Reporting module.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart*	Manage a Chart Group and Chart

*You can complete these tasks here.

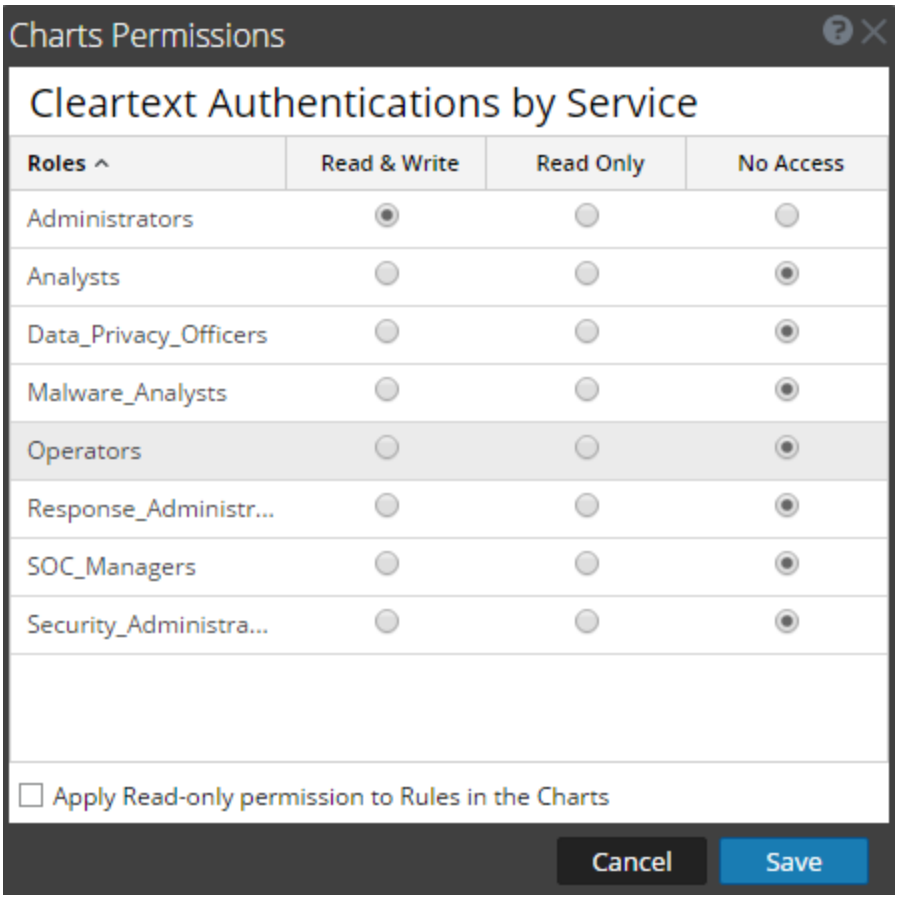
Related Topics

- Configure and Generate a Chart

Quick View

The Chart permissions dialog allows you to set chart permissions depending on the user role.

The following figure is an example with the important features labeled.



1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Charts** to open the Chart view.
3. In the **Chart List** panel, select a report and click > **Permissions**. The Chart Permissions dialog box is displayed.
4. Based on the user role, select the appropriate options.
5. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.

6 Click **Save**.

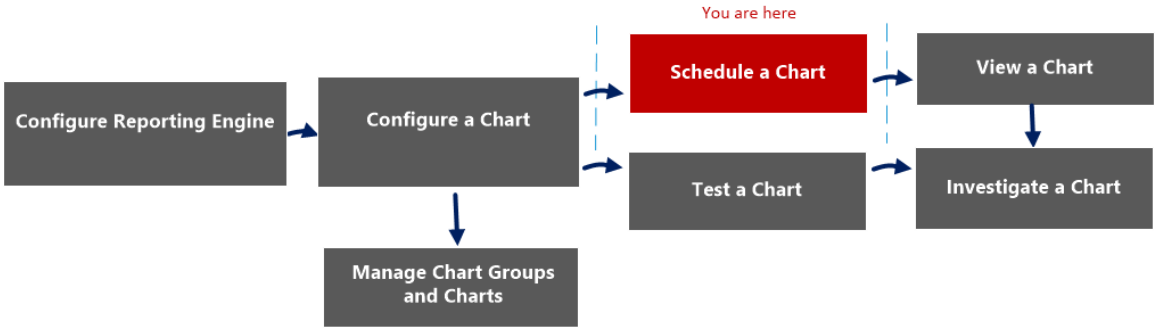
The following table lists the columns in the Charts Permission dialog.

Column	Description
Roles	Displays all the user roles in the NetWitness user interface.
Read & Write	Allows you to apply 'Read&Write' access to the chart.
Read Only	Allows you to apply only 'Read' access to the chart.
No Access	By selecting this permission, you cannot access or view the chart.
☐ Apply these permissions to sub-groups and Charts in this group	Allows you to apply permissions to the chart group, subgroups in the group and charts in the group. **Note:** This checkbox is populated only when you set access permissions for a Chart Group.
☐ Apply Read-only permission to Rules in the Charts	Allows you to automatically apply permissions to the rules in the charts.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selection and provides access to the role based on the selection.

Chart View

In the Chart View, you can see the available charts and groups in a grid format and also schedule them by enabling the charts.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart*	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

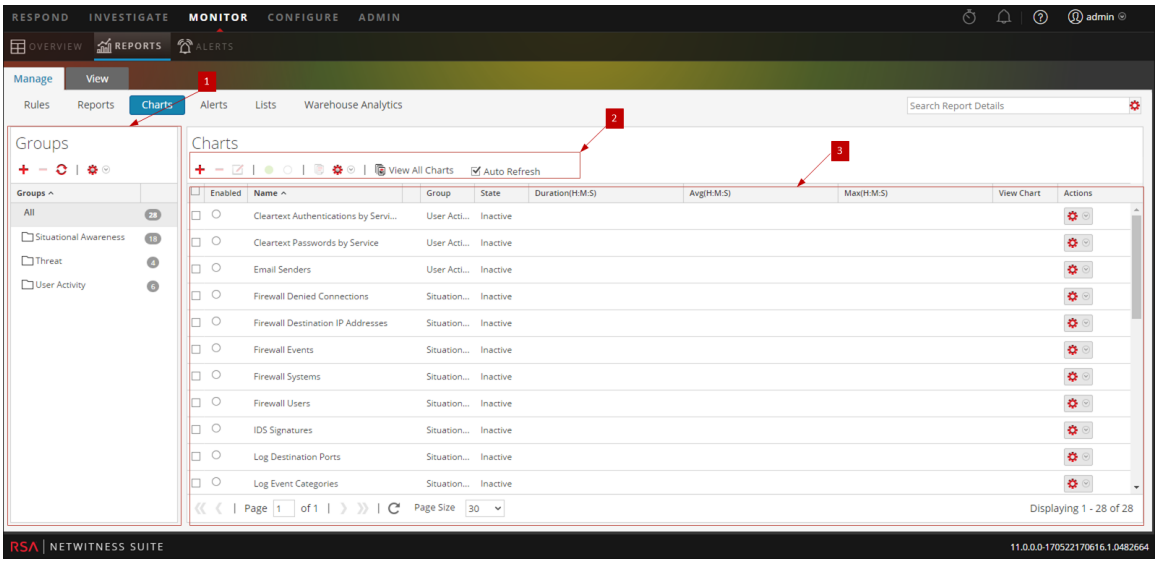
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.

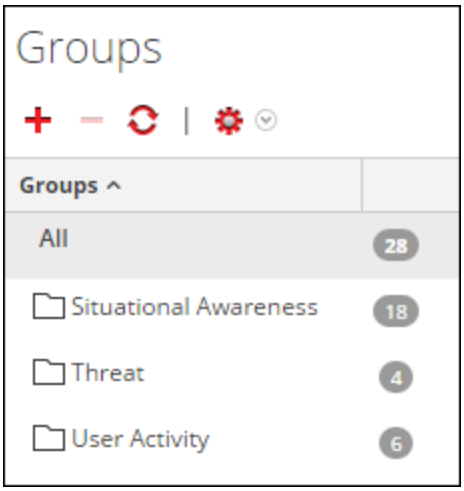


The Chart view includes the following panels:

1	Chart Groups panel
2	Chart toolbar
3	Chart View panel

Chart Groups Panel

The Chart Groups panel allows you to organize charts in a group. You can create a group, add charts to the group and move charts among groups. The following figure shows the Chart Groups panel.



The Charts Groups Panel includes the following options:

Feature	Description
+	Adds a new chart to the Reporting module.
−	Deletes one or more selected charts.
	Edits a chart.
	Refreshes the view.
	Provides the following options: Import, Export and Permissions.

Chart Toolbar

The Charts toolbar allows you to add, modify, delete, duplicate, activate, deactivate, import and export a chart. You can also set access permissions for charts in a group.

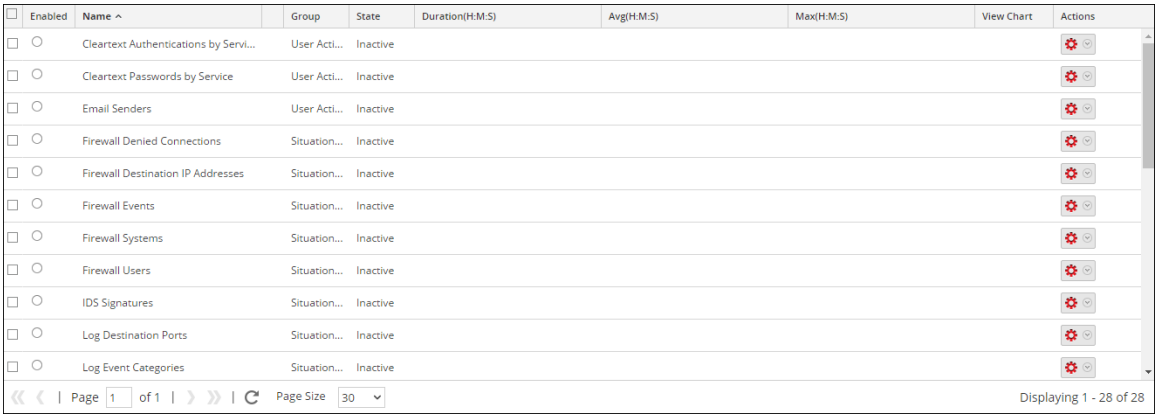
The Chart toolbar includes the following options:

Feature	Description
+	Adds a new chart to the Reporting module.
−	Deletes one or more selected charts.

Feature	Description
	Edit charts.
	Enables the selected charts.
	Disables the selected charts.
	Creates a duplicate copy of the selected chart.
	Provides the following options: Import, Export, Export as Text and Permissions.
View All Charts	Displays all the executed charts.
Auto Refresh	Automatically refreshes the charts list.

Chart View Panel

The Chart View Panel presents all the charts in a tabular or grid format.



The following table lists the columns in the Chart View panel and their description.

Feature	Description
Enabled	- The chart is enabled. - The chart is disabled.
Name	The name of the chart.

Feature	Description
Group	The Chart Group to which the chart belongs.
State	The state of the chart: • Queued • Completed • Failed
Duration (H:M:S)	The time taken to execute the latest chart.
Avg (H:M:S)	The average time taken to run the chart.
Max (H:M:S)	The maximum time taken to run the chart.
View Chart	A hyperlink that redirects to the View a Chart panel.
	The actions menu has the following options: Enable, Disable, View, Delete, Edit, and Export.

Execution History Panel

The Execution History panel allows you to fetch and display history details.

Workflow

This workflow shows the procedure to view report or report groups.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access control for lists, rules or Reports	Manage Lists, Rules or Reports

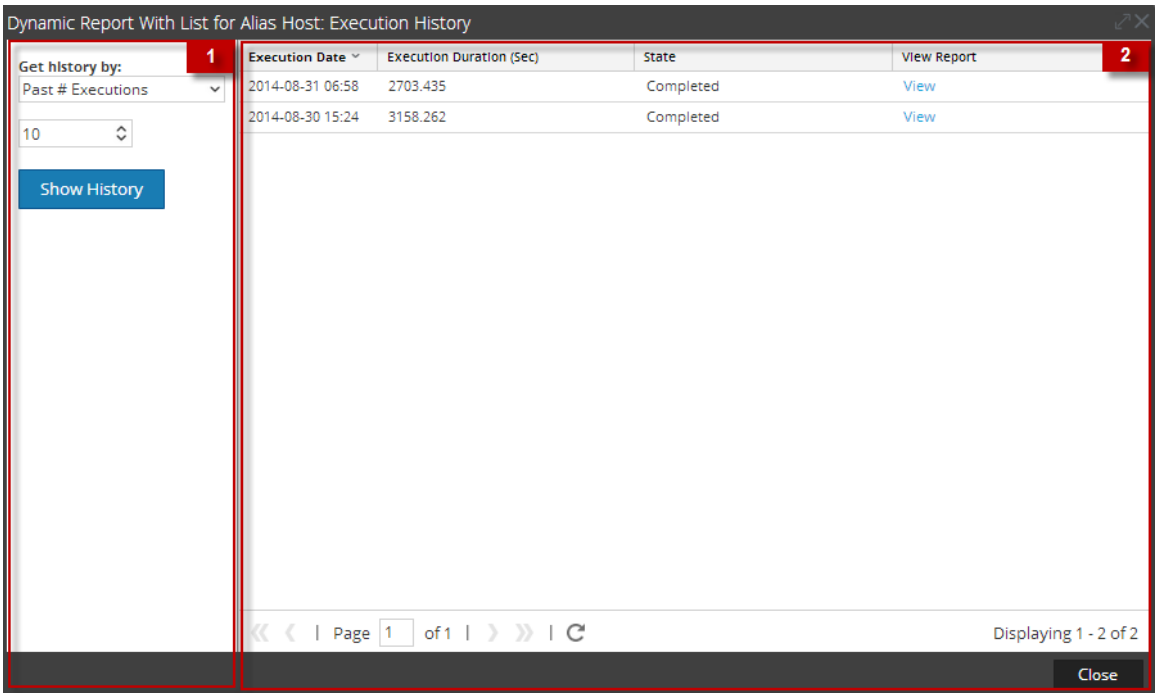
*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Generate List Panel
- Scheduled Reports View

Quick View

The following figure is an example of the Execution History view.



Features

The View Execution History has the following panels:

1 Execution History Options panel

2 Execution History Output panel

To access this view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.

2. In the Rule List panel, do one of the following:
   - Hover the mouse over a report and click > **View Scheduled Reports**.
   - Click **#Schedules** column.
     The Schedule Reports view is displayed with the status of each of the scheduled report.
3. Select a scheduled report and do one of the following:
   - Click > **Execution History**.
   - Click from the Scheduled Reports Toolbar Panel.

Execution History Options Panel

The Execution History Options panel allows you to fetch the history details based on either past n number of scheduled reports or a specific date range.

The following table lists the operations in the Execution History Options panel:

Operation	Description
Get history by:	This is the criteria to view the execution history: • **Past # Executions**: The past n number of scheduled reports. By default this option is displayed. • **Range (specific)**: The start date and end date for the date range. **Note:** The **From** and **To** field is populated in the NetWitness Suite UI only when you select 'Range (Specific)' from the **Get history by** list.
From	The start date for the date range.
To	The end date for the date range.
Count	The number of execution history of the scheduled report to be displayed.
Show History	Shows the history details based on the selected criteria.

Execution History Output Panel

The Execution History Output panel displays the history details with the execution date, execution duration (seconds), state of the scheduled report, and a link to view the report.

The following table lists the various columns in the Execution History Output panel:

Column	Description
Execution Date	The date on which the scheduled report was executed. By default, the execution date is in descending order.
Execution Duration (Sec)	The time duration taken to execute the scheduled report.

Column	Description
State	The state of the scheduled report: • Scheduled: If a report is scheduled to run on an hourly, daily, weekly, monthly, or later time, the state of the report is displayed as scheduled, for the first run. • Queued: If a report is still waiting to get executed, the state of the report is displayed as queued. • Running: If the report schedule is in progress, the state of the report is displayed as running. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule schedule executions failed, the state of the report is displayed as failed. • Completed: If a report schedule is successfully executed, the state of the report is displayed as completed. • Canceled: When cancel request is completed, the state of the report is displayed as canceled. • Inactive: If a report schedule is disabled, the state of the report is displayed as Inactive. • Not available: If the report schedule executed information is not available, the state of the report is displayed as not available.
View Report	The hyperlink to View a Report on full screen.

Column	Description
Close	Closes the execution history view.

Generate List Panel

The Generate List dialog allows you to generate and customize a list.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

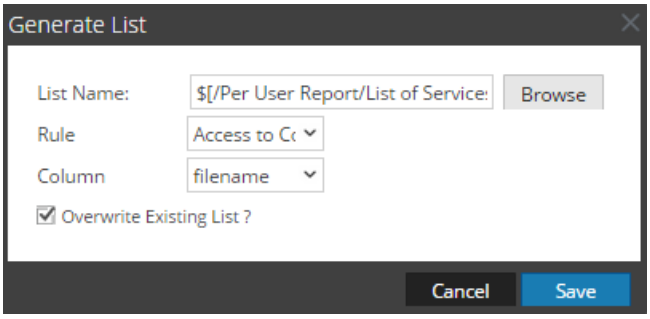
*You can complete these tasks here.

Related Topics

- List View
- Build List View
- Lists Permissions Dialog

Quick View

The following figure is an example of the Generate List dialog.



To access this view:

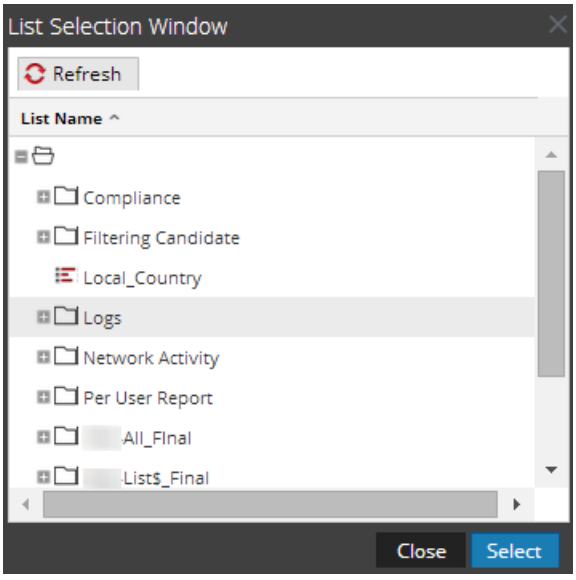
1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report and click > **Schedule Report**.
   The Schedule a Report view tab is displayed.
4. In the **Dynamic List** panel, click .
   The Generate List dialog is displayed.

Features

The following table lists the features in the Generate List dialog.

Field	Description
List Name	The name of the list chosen from the List Selection panel.
Browse	Click this button to select a list from the List Selection Window dialog.
Rule	Select a rule to be used to create the list.
Column	Select a value for the column.
Overwrite Existing List?	Overwrites the existing list.
Save	Adds the desired list to the Generate List panel of the Schedule Report view.

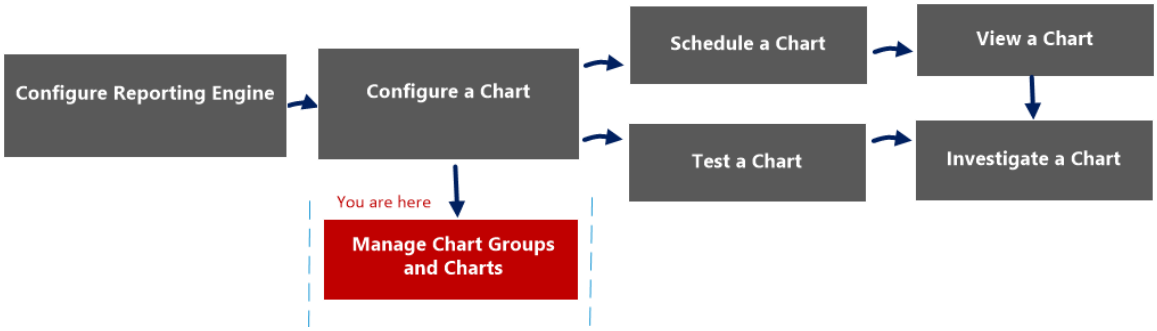
The List Selection Window dialog consists of lists that are defined in the Lists panel. Here, you can select a list to associate it with the report. The following figure shows the dialog.



Import Chart Dialog

In the Import Chart dialog, you can import charts containing subgroups and charts from other instances of NetWitness into the Chart Groups panel. Charts must be in a valid binary file that was exported from another NetWitness instance.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart

Role	I want to ...	Documentation
Administrator/ Analyst	Manage a chart group and chart*	Manage a Chart Group and Chart

*You can complete these tasks here.

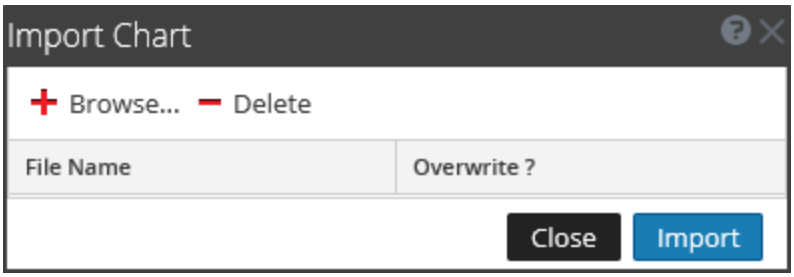
Related Topics

- Configure and Generate a Chart

Quick View

This dialog displays differently when you use it to import groups containing subgroups and charts from other instances of NetWitness into the Chart Groups panel.

The following figure is an example of the Import Chart dialog.



1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Charts** to open the Chart view.
3. In the **Chart Groups** panel, select a folder to import the file.
4. In the Chart Groups panel or Chart toolbar, click > **Import** to import the file.

The following table describes the features in the Import Chart dialog.

Feature	Description
Browse	Displays a view of the local file system so that you can select the chart to be imported.
Delete	Deletes an imported report from the list of imported charts.

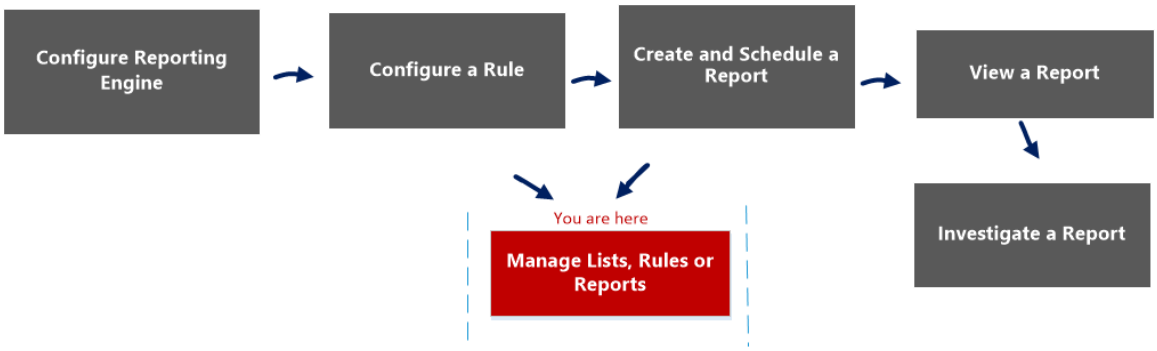
Feature	Description
File Name	Displays a list of chart files that will be imported to your Charts module when you click Import.
Overwrite?	Allows you to select the option to overwrite an existing version of the chart you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	Closes the dialog. If you have charts to select for import, but have not clicked Import. The charts are not imported, and are not saved in this dialog.
Import	Imports the selected charts to your Charts module.

Import Report Dialog

In Import Report dialog, you can import groups containing subgroups and reports from other instances of NetWitness Suite into Report Groups panel. Reports must be in a valid binary file that was exported from another NetWitness Suite instance.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

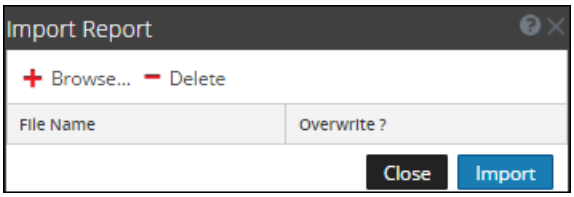
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Reports Permissions Dialog

Quick View



To access the Import Report dialog:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report Groups** panel, select a folder to import the file.
4. Do one of the following:
   - In the **Report Groups** panel, click > **Import** to import a group.
   - In the **Report** toolbar, click > **Import** to import a report.

The following table lists the features of the Import Report dialog.

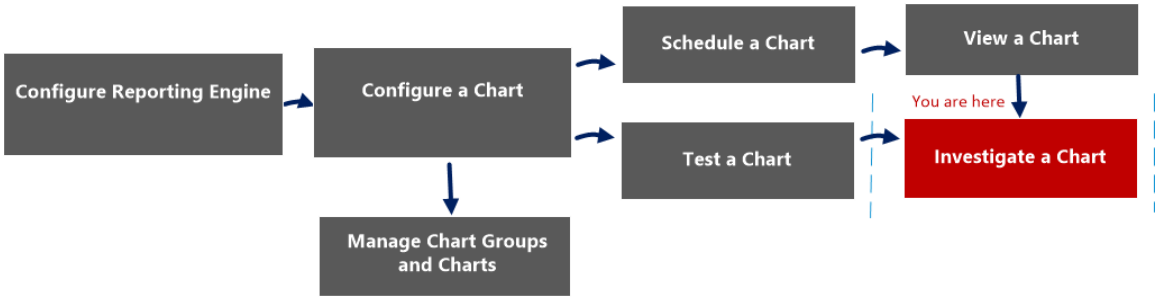
Feature	Description
Browse	This option displays a view of the local file system so that you can select the report to be imported.

Feature	Description
Delete	This option deletes an imported report from the list of imported reports.
File Name	Displays a list of report files that will be imported to your Reports module when you click Import.
Overwrite?	Allows you to select the option to overwrite an existing version of the report you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	This option closes the dialog. If you select a report and not clicked Import. The reports are not imported, and are not saved in this dialog.
Import	This option imports the selected reports to your Reports module.

Investigate a Chart View

In the Investigate a Chart view, you can view and investigate chart details. There are options for filtering and sorting the information in the chart, as well as options for the type of chart, the number of items to chart, and charting values or totals. When viewing a chart, you can open the charted sessions in the Investigation module and save the chart as a PDF.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engin" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart*	Investigate a Chart

Role	I want to ...	Documentation
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

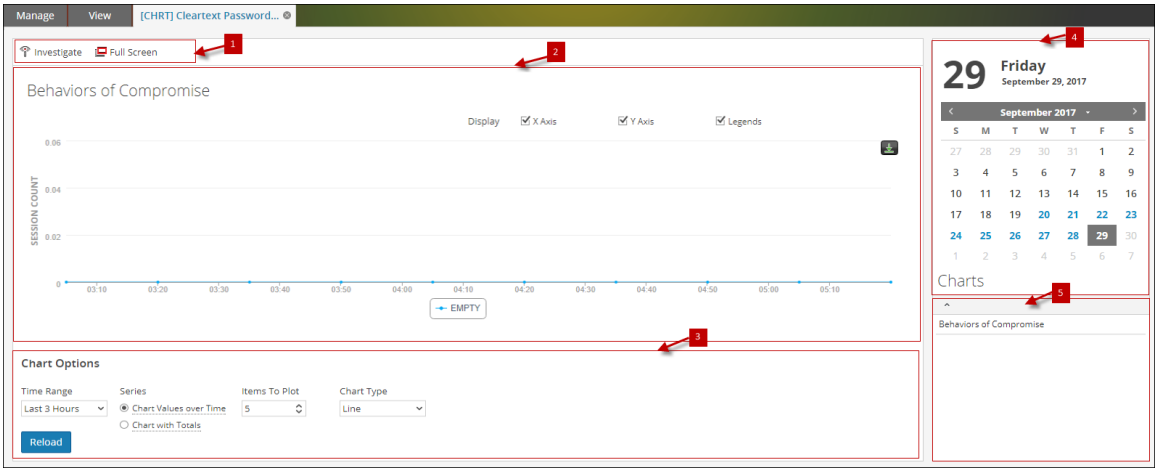
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The View a Chart panel includes the following panels:

1. Chart toolbar
2. Chart Output panel
3. Chart Calendar panel
4. Chart Options panel
5. Chart Executed list

Chart Toolbar

The Chart toolbar has options that allow you to investigate, and view the chart on another screen.

The following table lists the options in the Chart toolbar.

Operation	Description
Investigate	Investigates the chart details.
Full Screen	Displays the chart on a full screen.

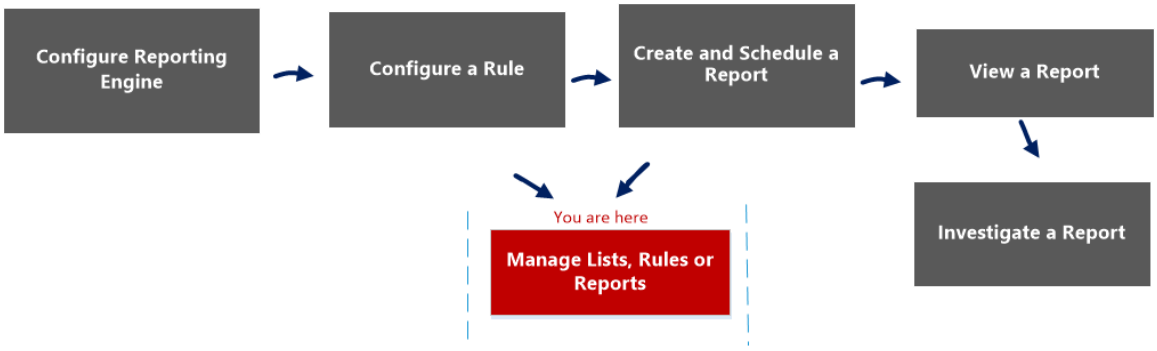
Lists Permissions Dialog

In the Lists Permissions dialog, you can manage access permissions for a user role at the list or list group level. Only a user with **Read and Write** permission can configure the list in the Reporting Module.

Workflow

This workflow shows the procedure to manage lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists. You can use lists to define rules for generating reports, charts and alerts.

You must ensure that Reporting Engine is configured on NetWitness Suite.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report

Role	I want to ...	Show me how
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

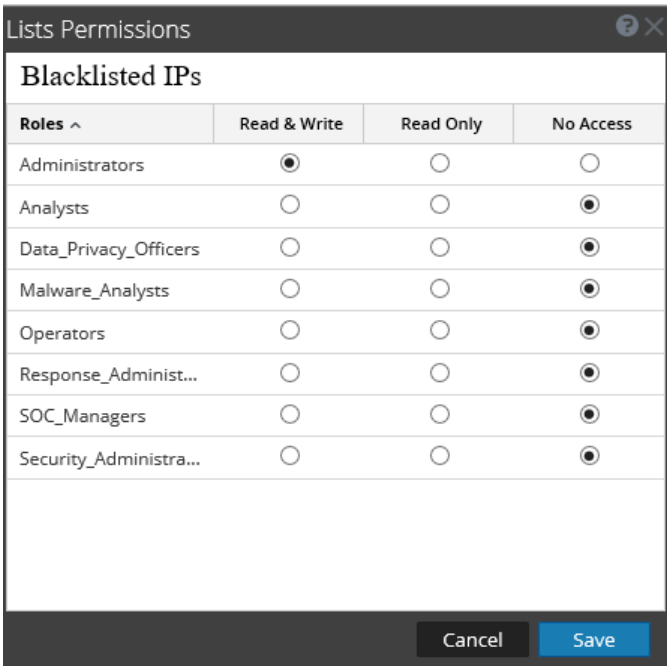
*You can complete these tasks here.

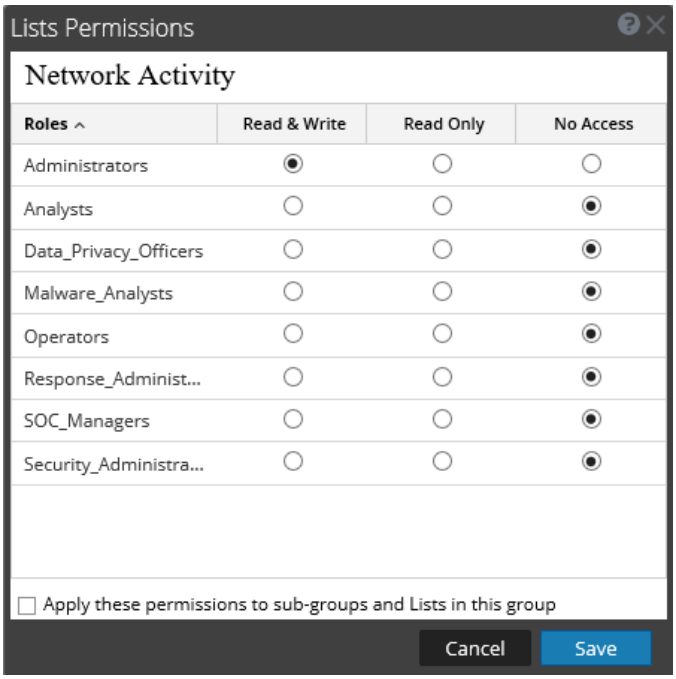
Related Topics

- List View
- List section in the "Role Permissions" topic in the *System Security and User Management Guide*.

Quick View

The following figures are examples of the Lists Permissions dialog and List Group Permission dialog:





To access this view

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The Lists view is displayed.
3. In the **Lists** view, select a report.
4. In the **Lists** toolbar, click > **Permissions**.
   The Reports Permissions dialog is displayed.

The following table describes the features in the Lists Permissions dialog:

Feature	Description
Roles	Describes roles of the users logged into the NetWitness Suite user interface.
Read & Write	Allows users to access, view, edit, delete, import, and export lists on the Lists view. Users can also change the permission on the rule.

Feature	Description
Read Only	Allows users to only access and view the list on the lists view.
No Access	Doesn't allow users to access or view the lists.
Apply these permissions to subgroups and lists in this groups	Automatically applies permissions to the subgroups and lists in the groups, if checkbox is selected.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selections and provides access to the roles based on the selections.

List View

In the List view you can see available lists and groups in a grid.

Workflow

This workflow shows the procedure to define lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists. You can use lists to define rules for generating reports, charts and alerts.

You must ensure that Reporting Engine is configured on NetWitness Suite.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report

Role	I want to ...	Show me how
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

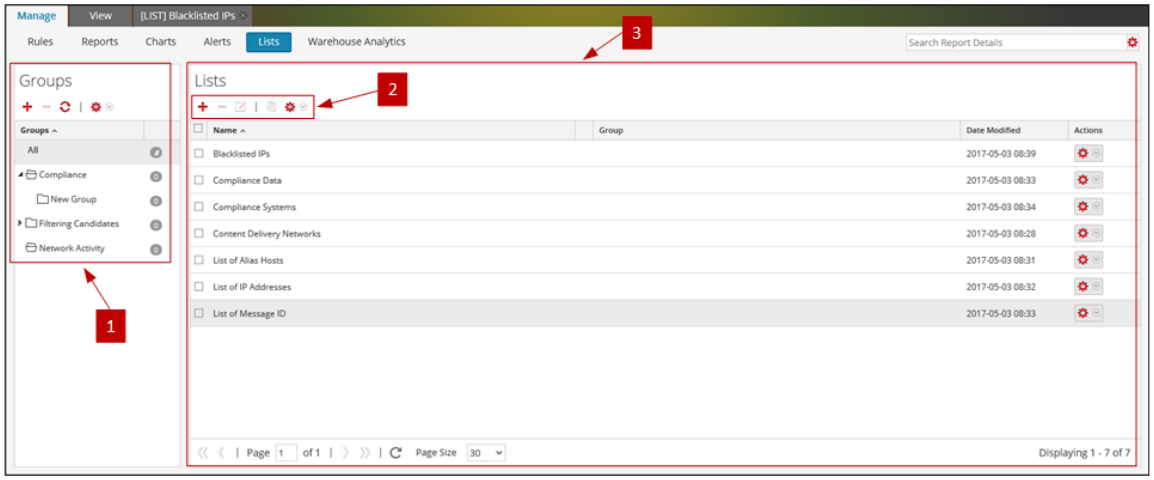
*You can complete these tasks here.

Related Topics

- Lists Permissions Dialog
- Build List View

Quick View

The following figure shows the List view.



To access this view

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The Lists view is displayed.

The List view includes the following panels:

1 List Groups panel

2 List toolbar

3 List View panel

List Groups Panel

The List Groups panel provides a list of groups used to organize lists and has a toolbar that allows you to create and manage the groups.

Feature	Description
	Allows users to add a new group to the Reporting module.
	Allows users to delete groups.
	Refreshes the view.
	Allows users to access following options: Import, Export and Permissions.

You can perform the following actions using the List Groups panel.

- Refresh lists in a group.
- Move lists between different groups. You can move a list from one group to another by dragging and dropping the list in the required group.
- Create list groups.
- Delete list groups.
- Import list groups.
- Export list groups.
- Set access control for list groups.

List Toolbar

Feature	Description
	Allows user to add a new list to the Reporting module.
	Allows user to delete one or more selected lists.

Feature	Description
	Allows user to edit lists.
	Creates a duplicate copy of the selected list.
	Allows user to access the following options: Import, Export and Permissions.

List View Panel

The List View panel displays all the lists defined in a tabular format.

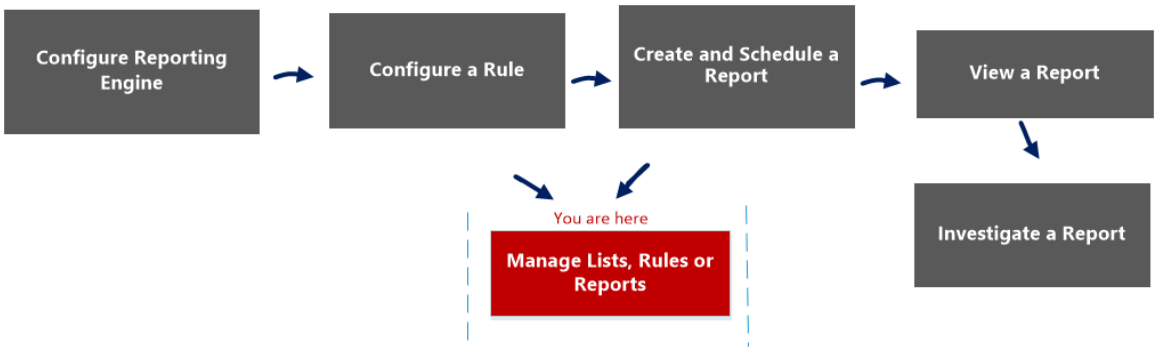
Column	Description
Name	Displays the name of the list. **Note:** For **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.
Group	Displays the list group to which the list belongs.
Date Modified	Displays the date and time when the list was modified.

Reports Permissions Dialog

In the Reports Permissions dialog, the users with 'Read & Write' access permission can configure permissions.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

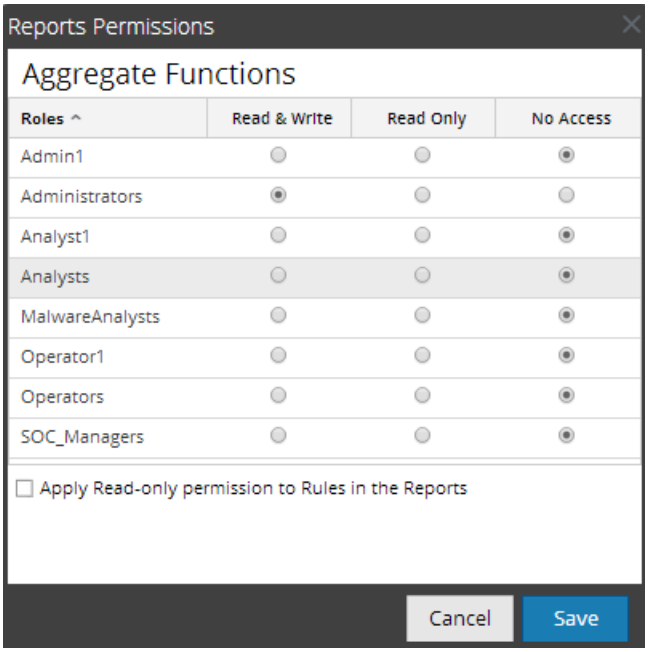
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Import Report Dialog

Quick View



To display the Reports Permissions dialog:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Report List** panel, select a report.

4. Click > **Permissions**.

   The Reports Permissions dialog is displayed.

Note: When you select the check box, all dependent rules are given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

The following table describes the features in the Reports Permissions dialog.

Feature	Description
Roles	Displays all the roles who can get access to the permissions.
Read&Write	Allows you to get Read&Write access to the Rules in the Reports.
Read Only	Allows you to get Read Only permissions to the Rules in the Reports.
No Access	If you select this option, you will not get permission to the Rules in the Reports.
Apply Read-only permissions to Rules in the Reports	Allows to set Read Only permissions to the Rules in the Reports for all the roles .
Cancel	This option cancels all the changes made to the permissions.
Save	This option saves the selections and provides access to the roles based on the selections.

Report View

In the Report view, you can create and manage the report or report groups.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

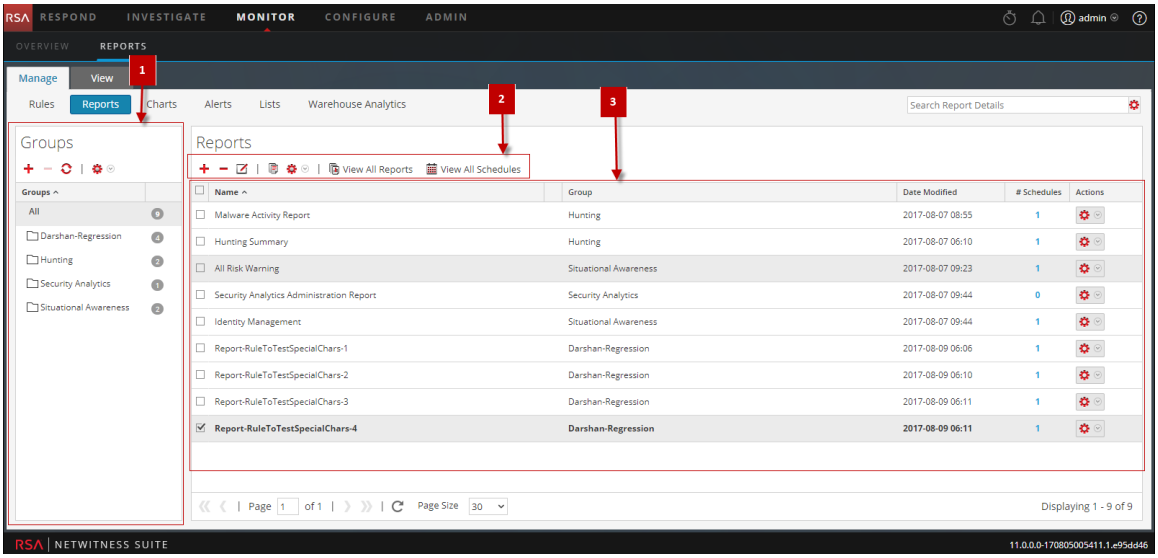
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Build Report View
- Import Report Dialog
- Scheduled Reports View
- Reports Permissions Dialog

Quick View



To access this view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Reports view is displayed.

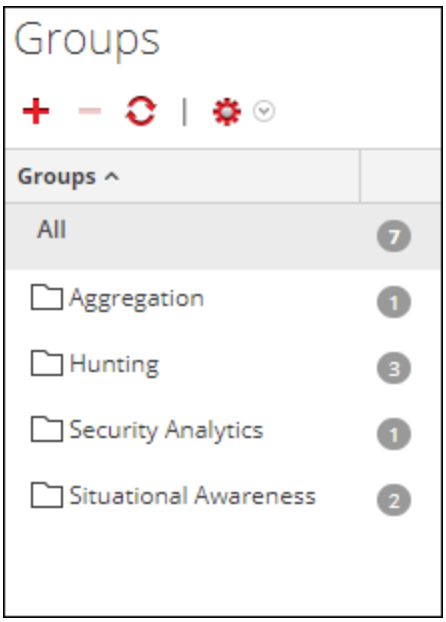
Features

The Report view includes the following sections:

1. Report Groups panel
2. Report toolbar
3. Report List panel

Report Groups Panel

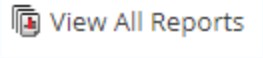
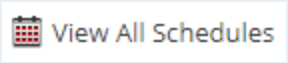
The Report Groups panel allows you to organize reports in a group. You can create a report group, add reports to the group, and move reports among groups. You can view all reports by selecting All option under the Groups column.



Feature	Description
+	This option allows you to add a new report to the Reporting module.
−	This option allows you to delete one or more selected report.
↻	This option refreshes the view.
⚙	The actions menu has the following options: Import, Export and Permissions.

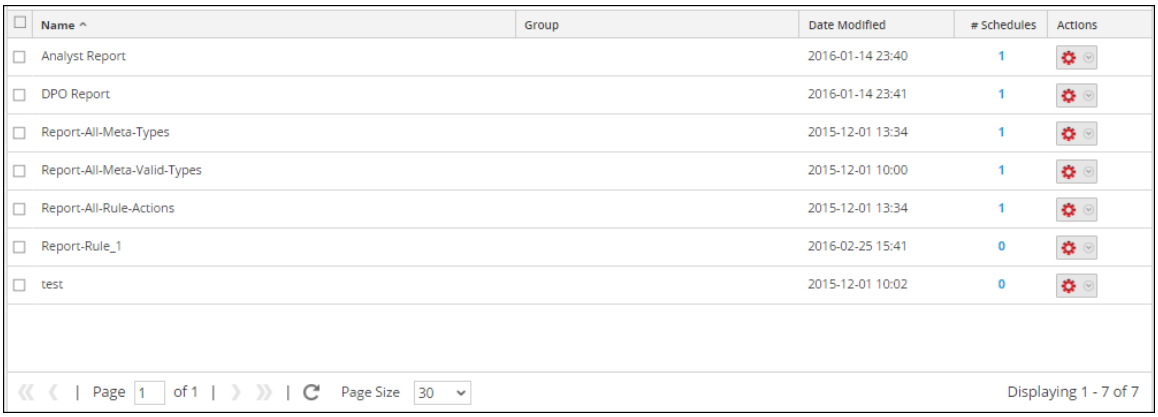
Reports Toolbar

The Reports toolbar allows you to add, modify, delete, duplicate, import and export reports. You can also set access permissions for a report in a group.

Feature	Description
	This option allows you to add a new report to the Reporting module.
	This option allows you to delete one or more selected reports.
	This option allows you to edit a chart.
	This option creates a duplicate copy of the selected report.
	The actions menu has the following options: Import, Export , Export as Text and Permissions.
	This option allows you to view a list of reports along with their schedule name and time.
	This option allows you to view all the scheduled reports.

Report List Panel

The Report List panel lists all the reports in a tabular format.



The following table describes the columns in the Report List panel.

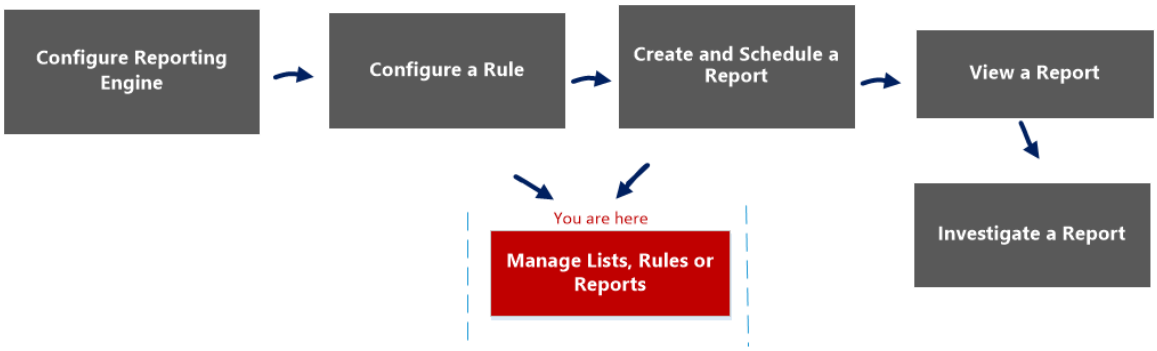
Column	Description
Name	The name of the report.
Group	The Report Group to which the report belongs.
Date Modified	The date and time when the report was modified.
#Schedules	The count indicates the number of schedules created for a report.
Actions	The actions menu has the following options: Schedule Report, View Scheduled Reports, Delete, Edit, and Export.

Rule Permissions Dialog

The Reporting module provides access control at the rule level. Only a user who has the right set of permissions can perform tasks on the rule. When creating user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Workflow

This workflow shows the procedure to manage rule or rule groups.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report

Role	I want to ...	Show me how
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

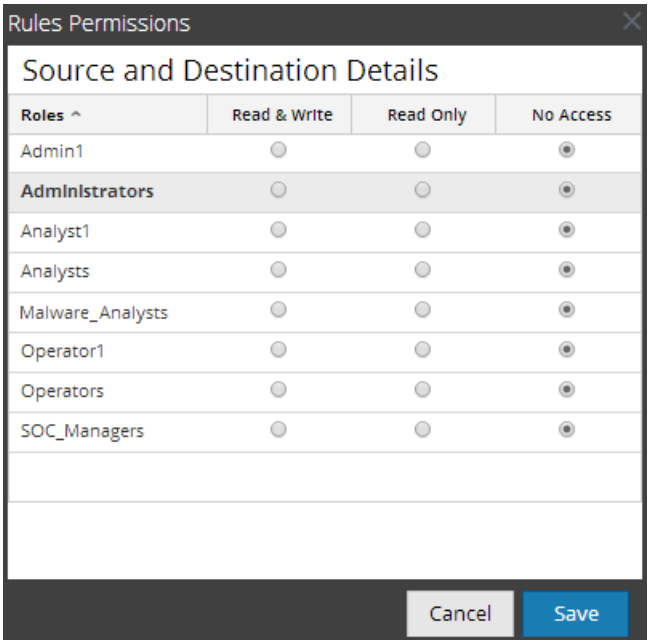
*You can complete these tasks here.

Related Topics

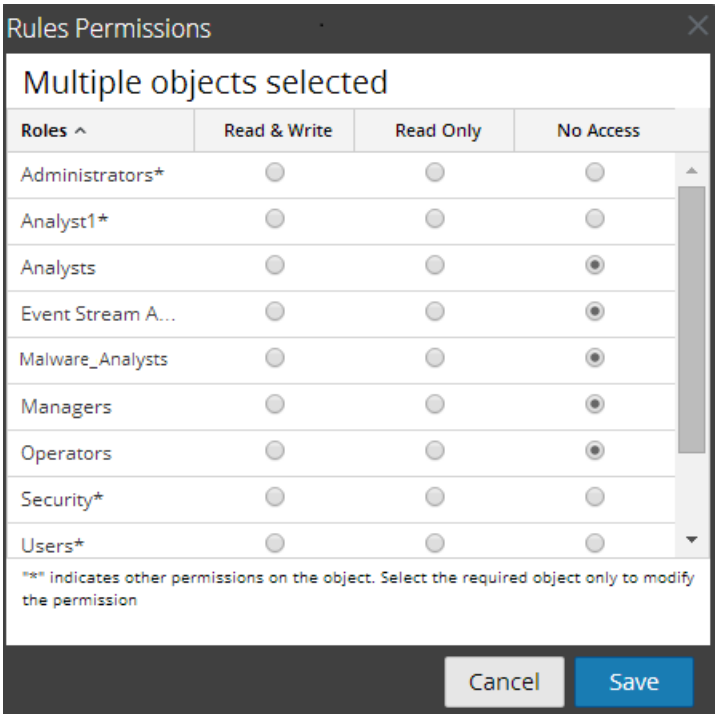
- Rule View

Quick View

This figure shows the Rules Permissions dialog for a single rule.



This figure shows the Rules Permissions dialog when multiple rules are selected.



The dialog has a different appearance for rule groups versus rules. To access the dialog:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. In the **Rules** list panel, select one or more rules or a rule group.
3. Click > **Permissions** in the toolbar.
   The Rules Permissions dialog is displayed.

Feature	Description
Roles column	Lists the NetWitness Suite user roles, both built-in and custom roles. Each user who is logged in to NetWitness Suite has user roles assigned. When multiple rules are selected, the asterisk beside the role name, for example, `Security*`, indicates there are other permissions available on that user role. To change the other permissions, you must select the user role and change the access permission.

Feature	Description
Read & Write column	When the checkbox in this column is selected, the corresponding user role has permission to view, edit, delete, import, and export rules in the Rules view. The user can also change the permission on the rule.
Read Only column	When the checkbox in this column is selected, the corresponding user role has permission to view the rules in the rule group.
No Access column	When the checkbox in this column is selected, the corresponding user role cannot view or edit the rules in the rule group. Before applying rule permissions, this is the default permission set for all the user roles though the checkbox is unchecked.
Apply these permissions to sub-groups and Rules in this group checkbox	When checked, NetWitness Suite applies permissions to sub-groups and rules in the group.
Cancel option	Clicking Cancel closes the dialog without saving any changes made.
Save option	Clicking Save closes the dialog and updates the rule group permissions for user roles. If specified, the access permissions are applied to subgroups and child objects of this group. When multiple rules are selected, the access permission is applied to all the selected rules.

Rule View

The Rule view is the user interface for managing rules.

Workflow

This workflow shows the procedure to define rule or rule groups.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

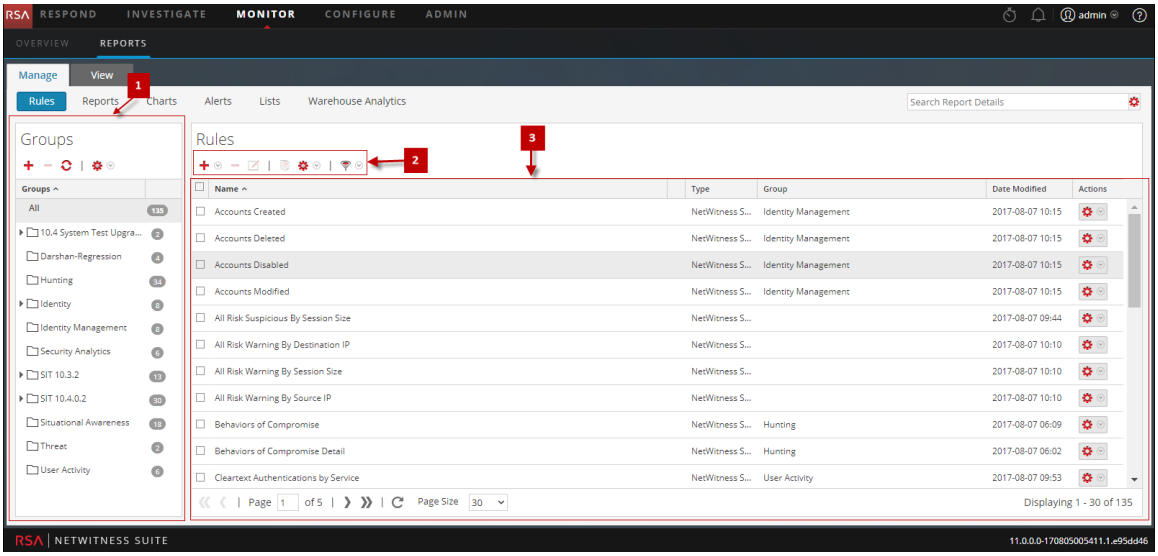
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Rule Permissions Dialog
- Build Rule View

Quick View



To access the Rules view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Rules**.

   The Rules view is displayed.

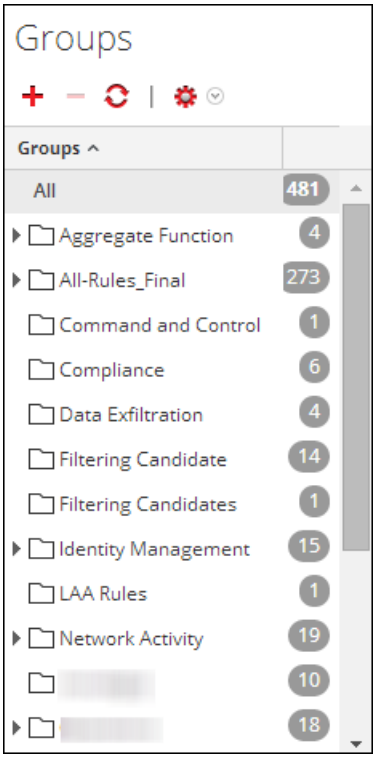
The Rule view includes the following panels.

1	Rule Groups
2	Rules List
3	Rule Toolbar

Rule Groups Panel

The Rule Groups panel allows you to organize rules into groups using the options in the toolbar. You can create groups and sub-groups and add rules to them. You can also group and move rules between different groups.

The following figure shows the groups in the Rule Groups panel:



The following table describes the features in the Rule Groups Panel.

Feature	Description
+	This option allows you to add a new rule group to the Reporting module.
−	This option allows you to delete one or more rule groups.
↻	This option refreshes the rule group list.
⚙	The actions menu has the following options: Import, Export and Permissions.
All	Displays a list of all the rule groups.

Rule Toolbar

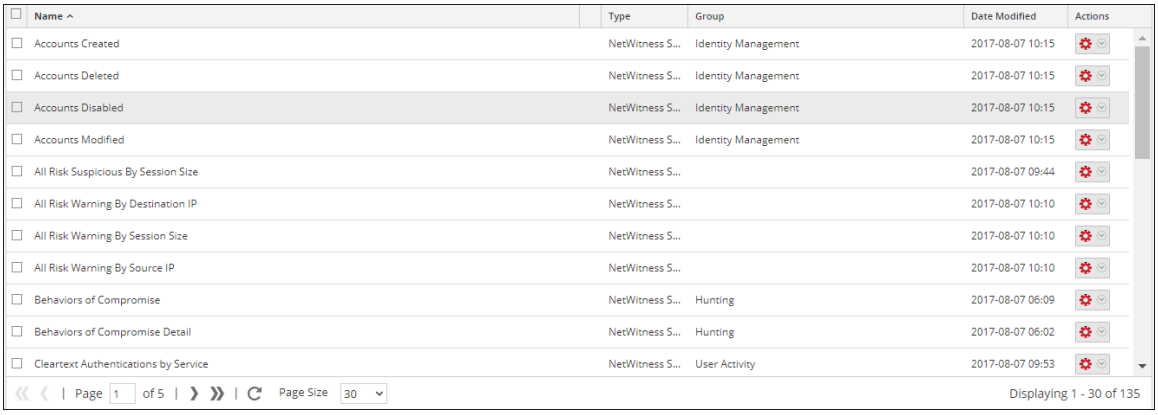
The Rule toolbar allows you to add, delete, edit, and duplicate a rule. The following figure shows the toolbar.

The following table describes the features in the Rule Toolbar

Feature	Description
	This option allows you to add a new rule to the Reporting module.
	This option allows you to delete one or more selected rules.
	This option allows you to edit a rule.
	This option allows you to duplicate a rule.
	The actions menu has the following options: Use, Import, Export and Permissions.
	This option allows you to select the rule type.

Rule List Panel

The following figure shows the list of rules in the Rule List panel.



The following table describes the features in the Rule List Panel.

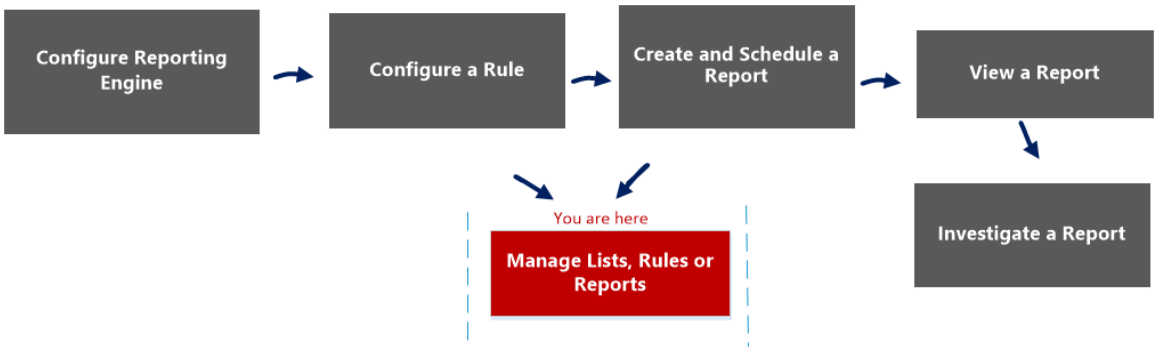
Feature	Description
Name	Displays the name of the rule that you are created or edited. **Note:** For the **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.
Type	Displays the supported database type for the rule you created.
Group	Displays the values which are grouped.
Date Modified	Displays the date when the rule was last modified.
Actions	Displays the actions menu has the following options: Create Alert, Create Chart, Create Report, Delete, Edit, Export, and Dependents.

Select a Logo Dialog

In the Select a Logo dialog, you can upload a new logo that is not available in Reporting Engine Services Config view or choose an existing logo from the Reporting Engine Services Config view.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

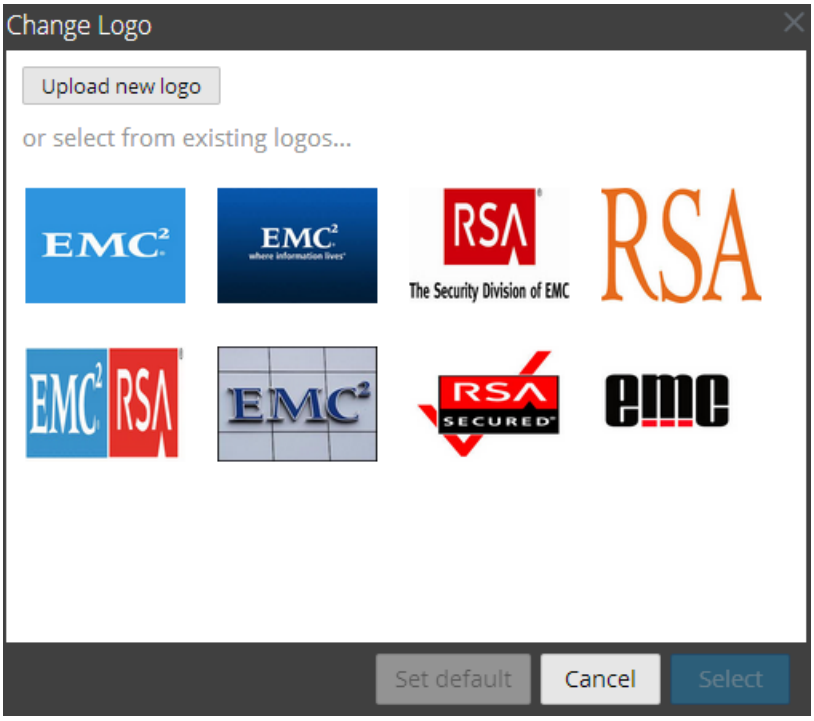
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Scheduled Reports View
- Report View

Quick View



To access this dialog:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Reports view is displayed.
3. In the **Report List** panel, select a report.

4. Click > **View Scheduled Reports**.
   The View scheduled reports view tab is displayed.
5. Select a scheduled report and click > **Edit Schedule**.
   The Schedule a Report view tab is displayed.
6. Click the **Logo** panel.
   The Change a Logo dialog box is displayed.

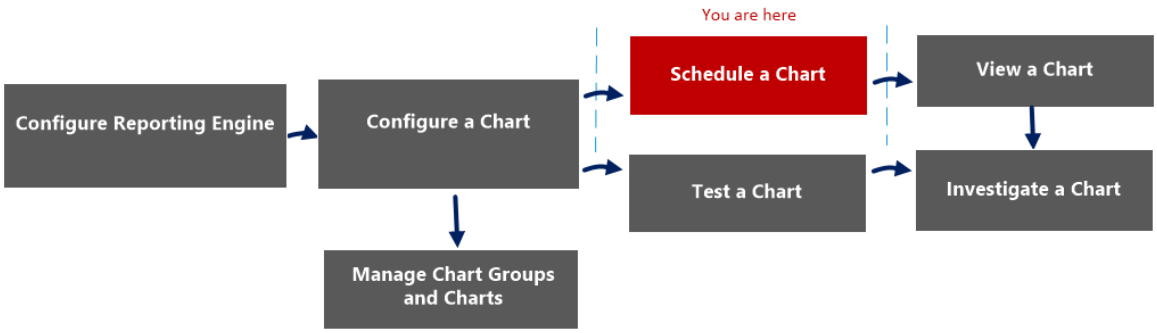
The following table lists the fields in the Select a Logo dialog.

Field	Description
Upload new logo	Click the icon to upload a new logo from the local directory.
Select	Select a logo from the existing list to be used as a logo in the scheduled report.
Cancel	Cancels the logo selection and returns to the Schedule a Report panel.
Set Default	Select a logo to set it as the default logo.

Schedule a Chart View

In the Schedule a Chart View, you can enable or disable a chart.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart*	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

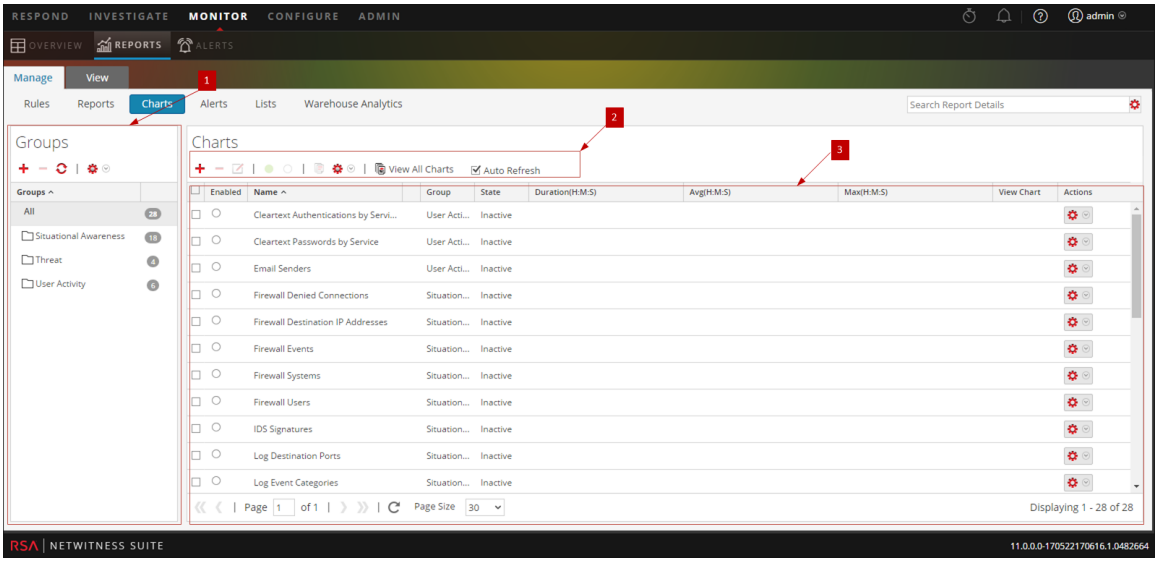
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure shows the Schedule a Chart view.



The Schedule a Chart view includes the following panels:

1. Chart Groups panel
2. Chart toolbar
3. Chart View panel

Chart Toolbar

The Charts toolbar allows you to add, modify, delete, duplicate, enable, disable, import and export a chart. You can also set access permissions for charts in a group.

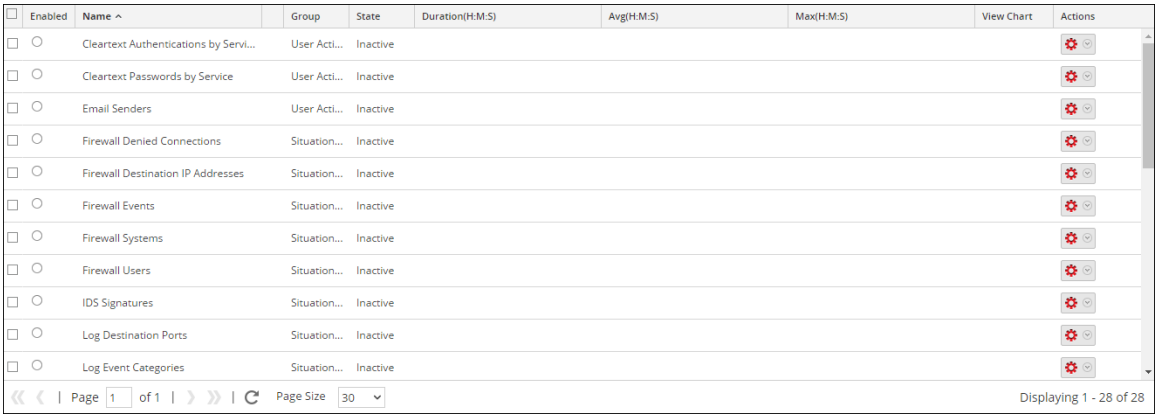
The Chart toolbar includes the following options:

Feature	Description
+	Adds a new chart to the Reporting module.
−	Deletes one or more selected charts.

Feature	Description
	Edit charts.
	Enables the selected charts.
	Disables the selected charts.
	Creates a duplicate copy of the selected chart.
	Provides the following options: Import, Export, Export as Text and Permissions.
View All Charts	Displays all the executed charts.
Auto Refresh	Automatically refreshes the charts list.

Chart View Panel

The Chart View Panel presents all the charts in a tabular or grid format.



The following table lists the columns in the Chart View panel and their description.

Feature	Description
Enabled	- The chart is enabled. - The chart is disabled.
Name	The name of the chart.

Feature	Description
Group	The Chart Group to which the chart belongs.
State	The state of the chart: • Queued • Completed • Failed
Duration (H:M:S)	The time taken to execute the latest chart.
Avg(H:M:S)	The average time taken to run the chart.
Max(H:M:S)	The maximum time taken to run the chart.
View Chart	A hyperlink that redirects to the View a Chart panel.
	The actions menu has the following options: Enable, Disable, View, Delete, Edit, and Export.

Schedule Report Panel

The Schedule Report panel allows you to schedule a customized report. Prior to scheduling a report, you can create a dynamic list (with the overwrite option selected) with services added. For more information, see "Generate a List from the Scheduled Report" section in Create and Schedule a Report. Then use the list to generate a report with details in the report like services and host names.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report

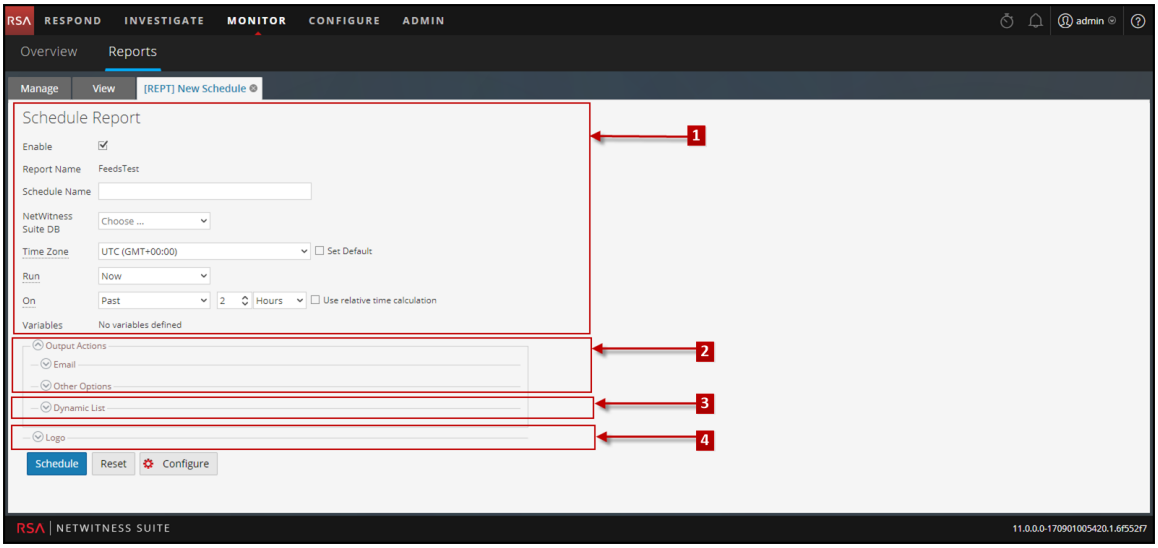
Role	I want to ...	Show me how
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Scheduled Reports View

Quick View



To access this view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.

The Reports view is displayed.

3. In the **Report List** panel, click > **Schedule Report**.

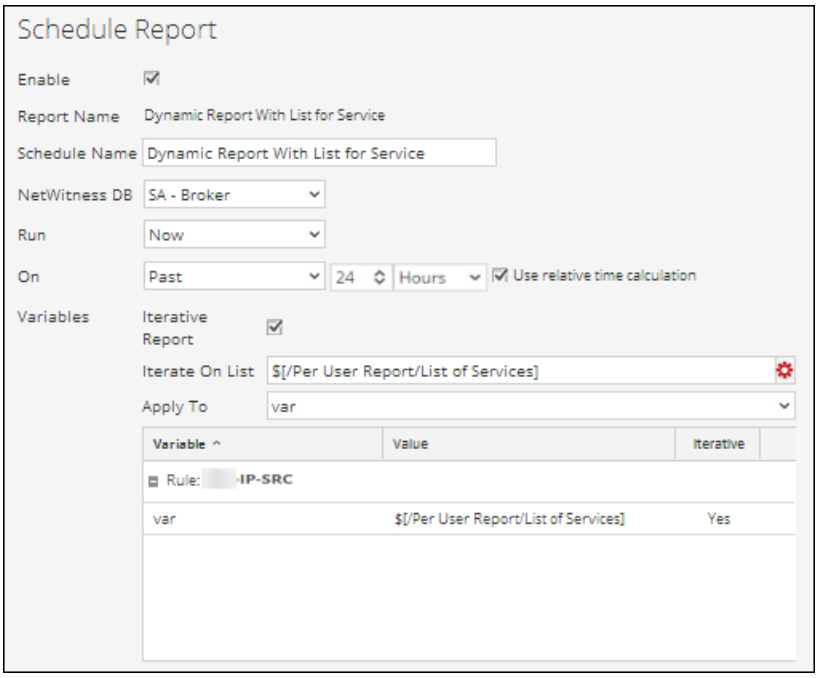
Features

The Schedule Report view consists of the following panels:

1. Schedule Report View
2. Output Actions Panel
3. Dynamic List Panel
4. Logo Panel

Schedule Report View

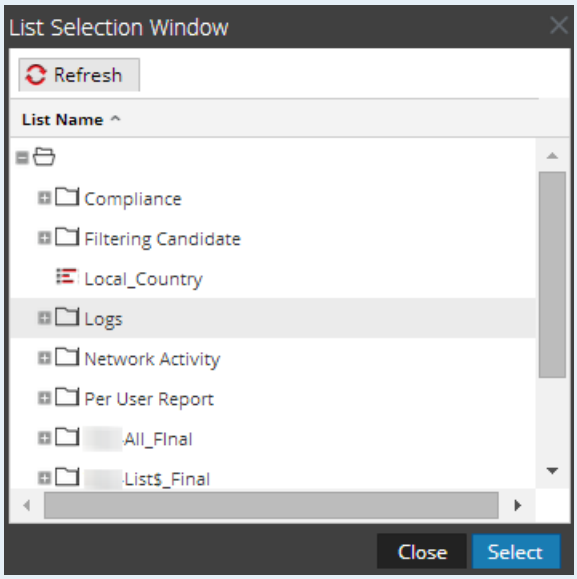
The Schedule Report view allows you to schedule reports.



The following table lists the fields in the Schedule Report panel.

Field	Description
Enable	Enables the report schedules and runs the report.
Report Name	The name of the report.
Schedule Name	The name of the scheduled report configuration.

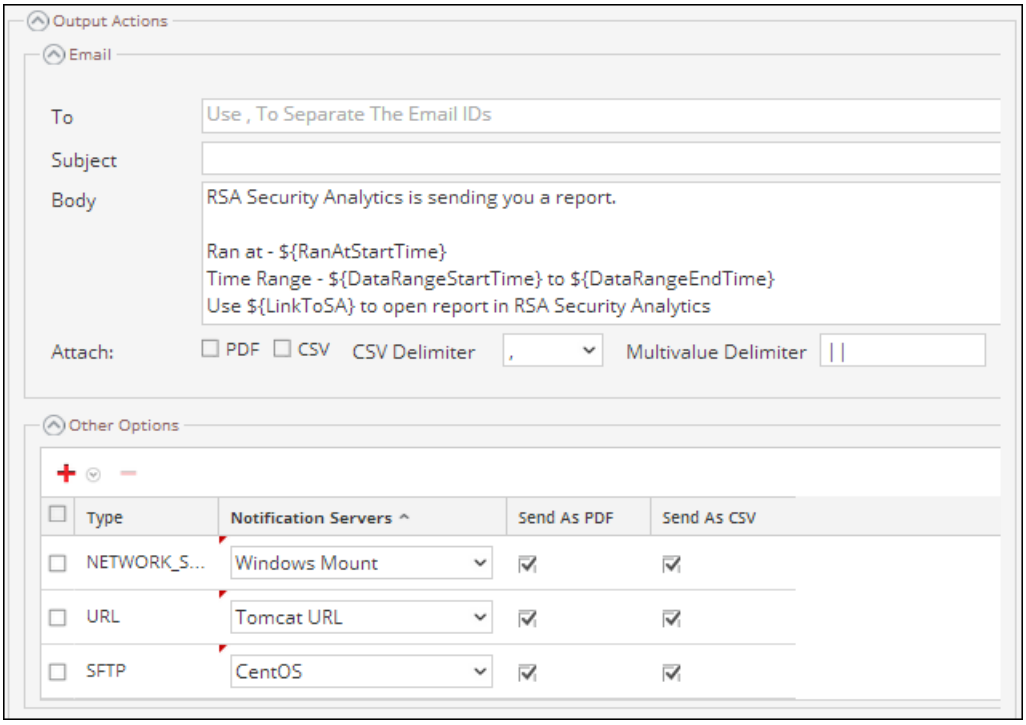
Field	Description
NetWitness DB	The database can be NWDB and Warehouse DB depending on the type of database that you selected in the rule definition. If the report has rules of NWDB and Warehouse DB types, all the database types or rule types are displayed.
Warehouse Resource Pool	If the report has rules of Warehouse DB, the Warehouse Resource Pool drop-down is displayed to select the pools or queues available in the cluster. If no pools or queues are entered for the Reporting engine, this field is disabled. For more information, see "Step 5: Configure Task Scheduler for a Reporting Engine" topic in the *Host and Services Configuration Guide*.
Run	Provides the type of schedule for the run configuration: • Ad-hoc execution • Hourly execution • Daily execution • Weekly execution • Monthly execution
On	The data range on which the query is run.
Use relative time calculation	Uses the relative time duration to schedule a report.
Iterative Report	Select the checkbox to schedule a report for the selected list value.

Field	Description
Iterate on List	Click this button to navigate to the List Selection panel and select a list. The following figure displays this panel:  The List Selection panel is a collection of Lists. The Reporting Engine maintains an active list of the available list names by continuously synchronizing with the collection to which it is connected.
Apply To	Apply list values on the selected variable.
Variables	Displays the rule variables along with their associated values and the iterative properties included in the report. **Note:** Depending on the rule chosen while creating a report, you can view dynamic variables defined for the rule in the **Variables**field of the Schedule Report panel. For example, Test-Country is the rule having the dynamic variable var.
Schedule	Schedules the report.
Reset	Resets the scheduled report.

Field	Description
Configure	Allows you to alter the Reporting Engine configuration details on the "Reporting Engine General Tab" topic in the *Host and Services Configuration Guide*. **Note:** This button is visible on the Schedule Report panel only when you have the 'Manage Device' access permissions on the Reporting module.

Output Actions Panel

The Output Actions panel specifies output actions to notify the email recipient when the report execution completes and also sends reports in PDF and CSV formats as attachments in the email, based on your selection.

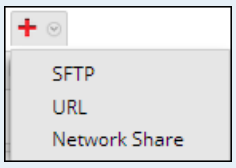


The following table lists the fields in the Output Actions panel.

Field	Description
To	A comma-separated list of email addresses to receive the output.
Subject	The subject entered in the mail.

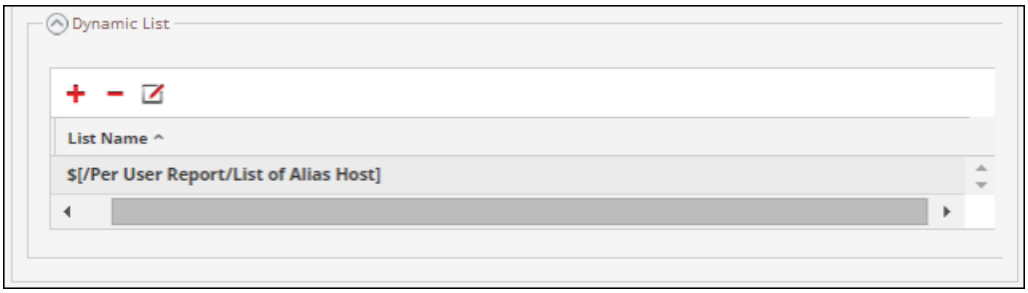
Field	Description
Body	The body of the email. By default, the body field is populated with pre-defined text that has certain variables that will add meta appropriate to the generated report. In the Reporting Engine, these variables are replaced with actual values. • `${RanAtStartTime}` : The Start time of the report. • `${DataRangeStartTime}` : The Start time of the data time range. • `${DataRangeEndTime}` : The End time of the data time range. • `${LinkToSA}` : The link to the NetWitness SuiteHost from the email which in turn opens the report in NetWitness Suite interface. • `${ReportName}` : The name of the report. • `${DataSource}` : The name of the data source.
Attach:	The output format in which the report is attached to the email, such as PDF or CSV as configured in the Schedule Report dialog.

Field	Description
CSV Delimiter	The default CSV delimiter is comma (,). If the CSV content contains a comma, you must identify a unique separator so the content is stored in its original form. For example, if msg is a column in the report to be saved as CSV and the msg content is as follows: `ASA-SSM-CSC-20 Module in slot 1," application reloading ""CSC SSM""," version ""6.2.1599.0"" CSC SSM scan services are reloading because of a pattern file or configuration update` The above content will be included in three columns due to the commas (,). To avoid this, you must specify a different delimiter such as a pipe line character "|". **Note:** To import the CSV file into Microsoft Excel, use the Data > From Text option in the Excel application. When you import the CSV file you must specify the file type of the file being imported as Delimited and use the same delimiter that you specify to generate the CSV file.
Multivalue Delimiter	The data in multivalued fields are separated by the multivalue delimiter. The default Multivalue delimiter is two pipe line characters (||).
Other Options	You can select an SFTP, URL, or Network Share location configured in ((RE}} and then send the report either in PDF or CSV format based on the requirement.

Field	Description
	Select this option to send the report to the SFTP, URL or Network Share location configured in the Reporting Engine Services Config view.
Type	The type of output action chosen. For example, SFTP, URL or Network Share.
Output Actions	Select the SFTP, URL or Network Share name configured in the Reporting Engine Services Config view.
Send as PDF / Send as CSV	Select these options to send the report either in PDF or CSV format, or both to the configured Notification Server (SFTP, URL or Network Share).

Dynamic List Panel

The Dynamic List panel populates the lists created and you can add, edit or delete the list. The list is generated based on the scheduled report which can be viewed in the Lists view.



The following table lists the operations in the Generate List panel.

Operation	Description
+	Adds a new list to the report.
−	Deletes all the lists added to the report.
	Displays the Generate List dialog.

Operation	Description
List Name	The name of the list chosen from the List Selection panel. For more information on the "List Selection panel" topic, see Generate List Panel.

Logo Panel

The Logo panel populates the default logo from the Select a Logo panel. For more information on choosing a logo from this panel, see "Manage and Select a Report Logo" section in the Manage Lists, Rules or Reports.

You can set the default logo for a Reporting Engine. This is the logo that is used in the generated reports. For more information on choosing a logo, see Select a Logo Dialog.

Note: If you have not selected any logo then the default RSA logo is used on the report. The option **Save as PDF** for the previously executed reports does not support a new customer logo. It displays the default RSA Logo, if the customer logo must be displayed in the Schedule a Report view.

Scheduled Reports View

The Scheduled Reports view allows you to create, view and manage scheduled reports.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

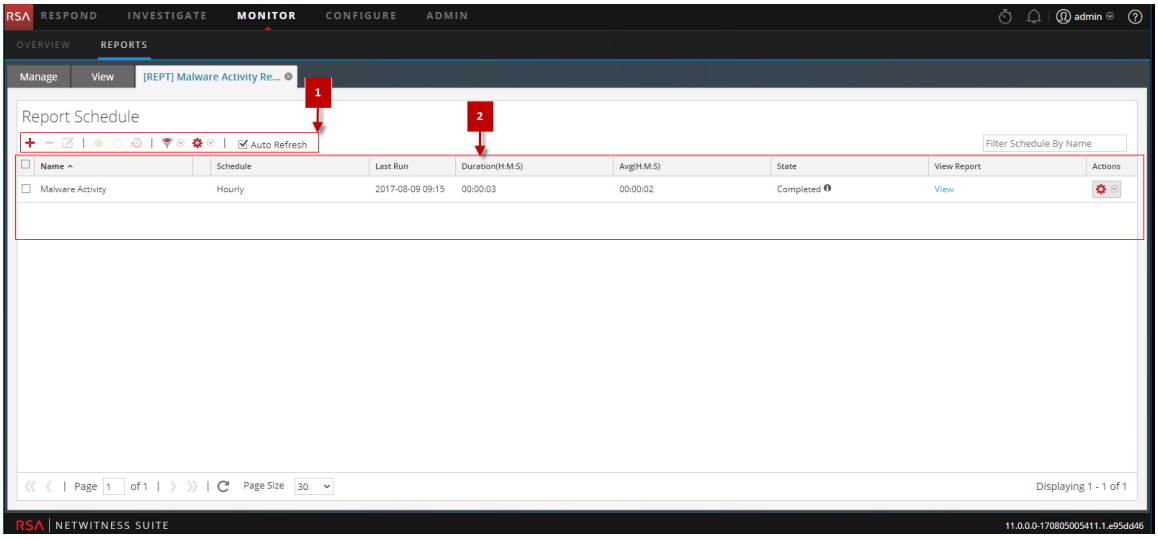
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Build Report View
- Report View
- Schedule Report Panel
- Reports Permissions Dialog

Quick View



To access this view:

1. Go to **MONITOR** > **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Report List** panel, do one of the following:

- Click > **View Scheduled Reports**.
- Click the **#Schedules** column.

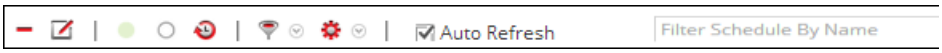
Features

The View Scheduled Reports has the following features:

1. Report ScheduleToolbar
2. Report Schedule List panel

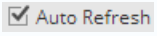
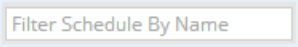
Report ScheduleToolbar

The Scheduled Reports has options to add, modify and delete the scheduled report as well as options to enable or disable the selected run configuration.



The following table lists the operations in the Scheduled Reports toolbar.

Operation	Description
	Create a new report schedule.
	Delete the selected report schedule.
	Edit the selected report schedule. **Note:** Double-click on a desired report schedule to edit it.
	Enables the selected report schedule.
	Disables the selected report schedule.
	View the history of the scheduled report.

Operation	Description
	Filter schedules based on the type of schedule. (For example, AdHoc)
	Allows you to set permissions for the selected scheduled report.
	Automatically refreshes the scheduled reports list.
	Searches schedules based on the schedule name.

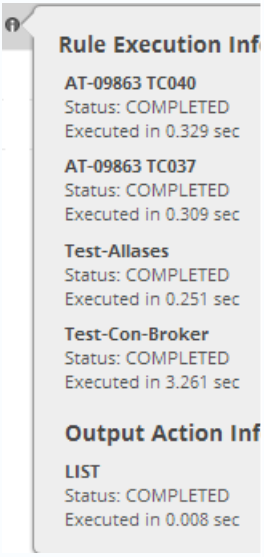
Report Schedule List Panel

The Scheduled Reports List panel lists the scheduled reports in a tabular format.

The following table lists the columns in the Scheduled Reports List panel:

Column	Description
Name	The name of the scheduled report.
Schedule	The type of schedule for the run configuration: • Ad-hoc execution • Hourly execution • Daily execution • Weekly execution • Monthly execution
Last Run	Displays the last time the report was run.
Duration (H:M:S)	Displays the time taken for last execution of the report
Avg(H:M:S)	Displays the average time taken to run the report.

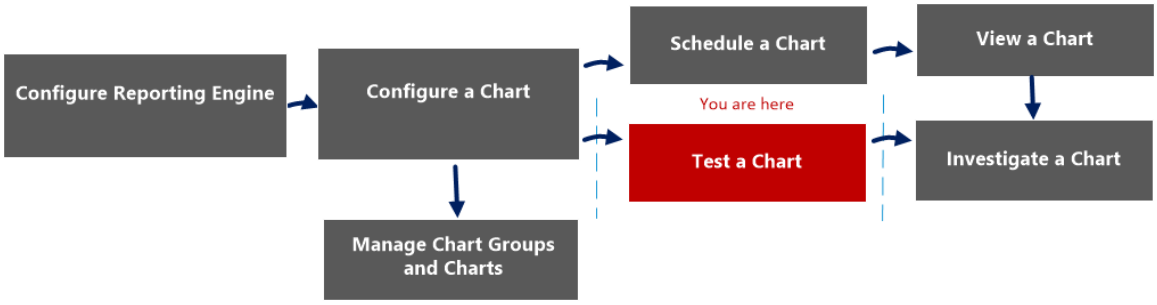
Column	Description
State	Indicates the state of the scheduled report. • Scheduled: If a report is scheduled to run on an hourly, daily, weekly, monthly, or later time, the state of the report is displayed as scheduled, for the first run. • Queued: If a report is still waiting to get executed, the state of the report is displayed as queued. • Running: If the report schedule is in progress, the state of the report is displayed as running. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule schedule executions failed, the state of the report is displayed as failed. • Completed: If a report schedule is successfully executed, the state of the report is displayed as completed. • Canceled: When cancel request is completed, the state of the report is displayed as canceled. **Note:** Cancel option may not work for Warehouse Analytics jobs. You must kill the job manually. Following are the steps to kill the job: **For MapR**: 1. Get the Jobid from job logs. 2. Login to jobtracker UI and search for Jobid to kill under "Running Jobs". Sample URL: http://<job-tracker-host>:50030/jobtracker.jsp 3. Kill the Jobid: • Select Jobid under "Running Jobs" and click Kill Selected Jobs.

Column	Description
	(or) • Click on Jobid link, scroll down and click Kill this job link. • Inactive: If a report schedule is disabled, the state of the report is displayed as Inactive. • Not available: If the report schedule executed information is not available, the state of the report is displayed as not available.
	Click to view the rule execution information and output action information. This pop-up notifies the status of multiple rules in a report and the time taken for its execution. **Note:** You can view the rule execution and output action information for a scheduled report having the state **Completed**, **Running**, **Partial** or **Failed**. By default, the Output Actions for Completed Report on Reporting Engine Config page is set to enable, to receive an email when the report status is completed. To receive an email for **Failed** or **Partial** reports, you must disable this option.
View Report	Click to view the rule execution information on the View a Report Panel. You can view the rule execution information for a scheduled report having the state 'running' as well.

Test a Chart View

In the Test a Chart view, you can view and test the charts.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart*	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

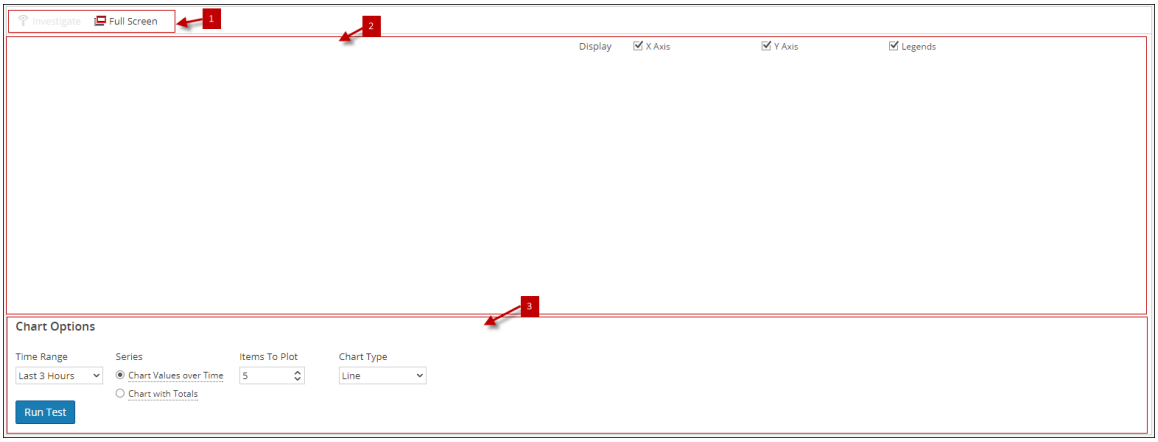
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The Test a Chart view consists of the following panels:

1. Chart toolbar
2. Chart Output panel
3. Chart Options panel

Chart Toolbar

The Charts toolbar allows you to investigate on a particular chart and change the screen to full screen.

Feature	Description
Investigate	Investigates further on the selected chart.
Full Screen	Displays the chart in full screen.

Chart Output Panel

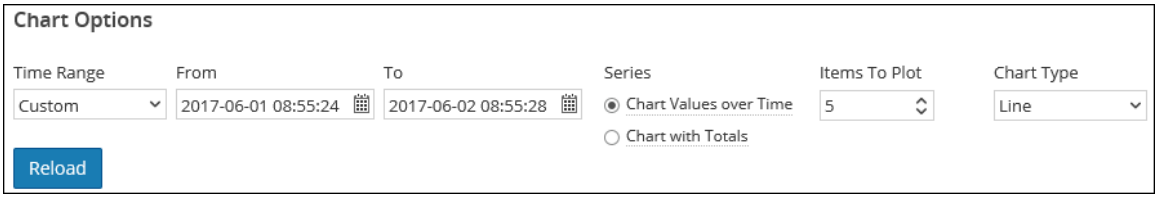
The Chart Output panel displays the information in a chart format for the selected time chart options.

The following table lists the features in the Test a Chart View and their descriptions.

Feature	Description
Display	Allows you select the values that needs to be displayed and have the following options: X Axis, Y Axis and Legends.
X Axis	Displays the session count.
Y Axis	Displays the actual output.
Legends	Displays the list of variables appearing in the chart.

Chart Options Panel

The following figure shows the Chart Options panel, which displays the time range, series, and chart type fields to configure the chart display.



The following table lists the fields in the Charts Options panel and the descriptions.

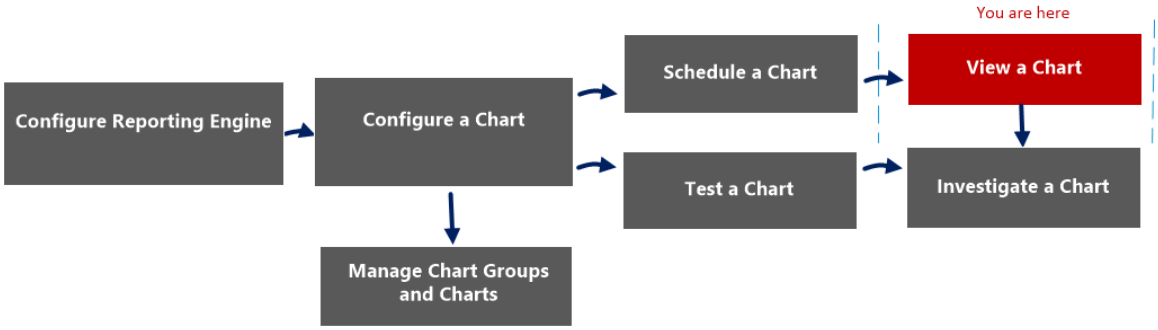
Feature	Description
Time Range	The default time range is Last 3 Hours. However, you can select a different value from the drop-down list, for example, Last Hour, or Last 6 Hours which are the preset values. Or you can customize by selecting Last N Days or the Custom option.
From	The start date and time. (only for custom options).
To	The end date and time. (only for custom options).

Feature	Description
Series	The series field provides you with two options: • Chart Values over Time: Renders the chart for the entire time range selected. • Chart with Totals: Renders the summary of data for the selected date range.
Items to Plot	The maximum number of events the user wants to view on the chart.
Chart Type	The type of chart to be rendered either area, bar, column, line, step line, step area, spline area or spline.

View a Chart Panel

In the View a Chart panel, you can view and manage charts. There are options for filtering and sorting the information in the chart, as well as options for the type of chart, the number of items to chart, and charting values or totals. When viewing a chart, you can open the charted sessions in the Investigation module and save the chart as a PDF.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart*	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart

Role	I want to ...	Documentation
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

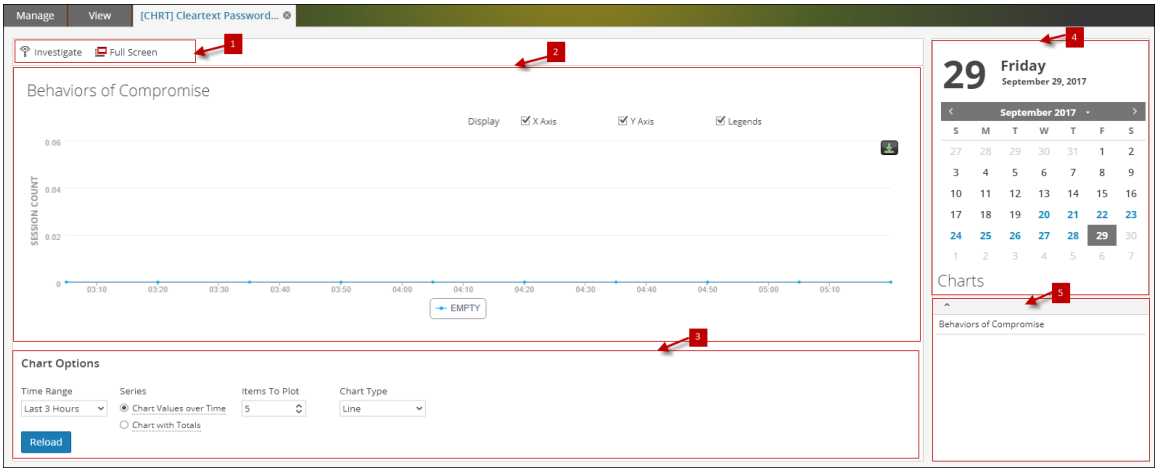
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The View a Chart panel includes the following panels:

1	Chart toolbar
2	Chart Output panel
3	Chart Calendar panel
4	Chart Options panel
5	Chart Executed list

Chart Toolbar

The Chart toolbar has options that allow you to investigate, and view the chart on another screen.

The following table lists the options in the Chart toolbar.

Operation	Description
Investigate	Investigates the chart details.
Full Screen	Displays the chart on a full screen.

Chart Output Panel

The Chart Output panel displays the chart with sortBy on the Y-axis, time on the X-axis and legends.

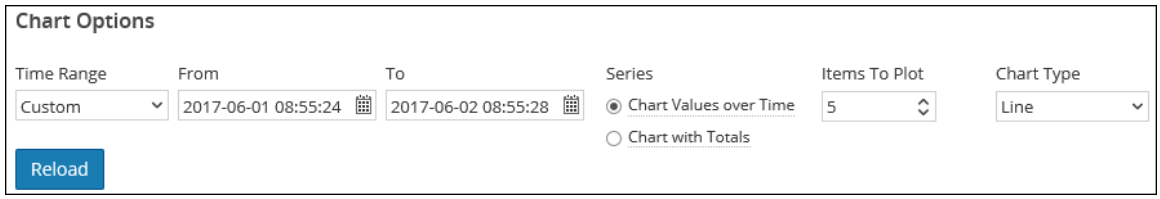
Note: You can save the chart as PDF using the icon on the Chart Output panel.

Chart Calendar Panel

The Chart Calendar panel is the default calendar with which you can filter the list of charts depending on the date you select from the Calendar, as shown in the following figure.

Chart Options Panel

The Chart Options panel displays the time range, series, and chart type fields to configure the chart is displayed.



The following table lists the fields in the Chart Options panel.

Field	Description
Time Range	The default time range is Last 3 Hours. However, you can select a different value from the drop-down list, for example, Last Hour, or Last 6 Hours which are the preset values. Or you can customize by selecting Last N Days or the Custom option. **Note:** The time range selected by you for a chart will be saved. When you open the same chart the next time, the time range that is saved will be displayed. This behavior is not applicable for the custom option.
From	The start date and time. (only for custom options)
To	The end date and time. (only for custom options)
Series	The series field provides the user with two options: • Chart Values over Time: Renders the chart for the entire time range selected. • Chart with Totals: Renders the summary of data for the selected date range.
Items to Plot	The maximum number of events the user wants to view on the chart.
Chart Type	The type of chart to be rendered. Either area, bar, column, line, step line, step area, spline area or spline.

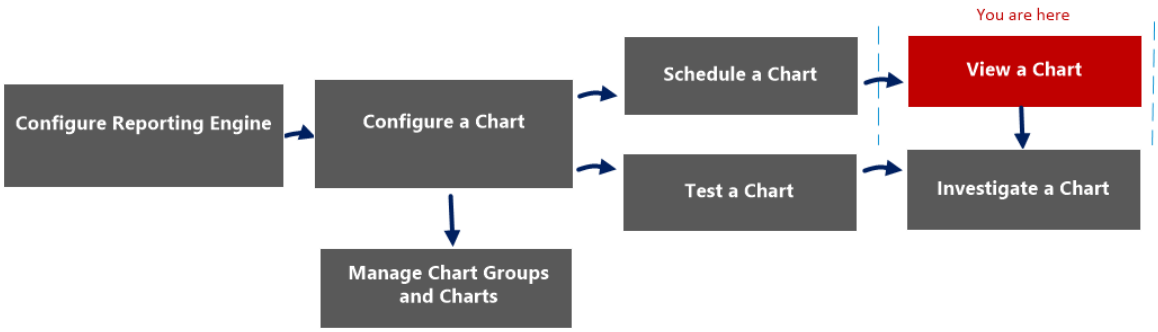
Chart Executed List Panel

The Chart Executed List panel displays all the executions for a particular chart for the selected date. Double-clicking on any chart execution loads the chart on the Chart Output panel. By default, the last executed chart is displayed in the Chart Output panel.

View All Charts View

In the View All Charts view, you can display, print, save and email charts.

Workflow



What do you want to do?

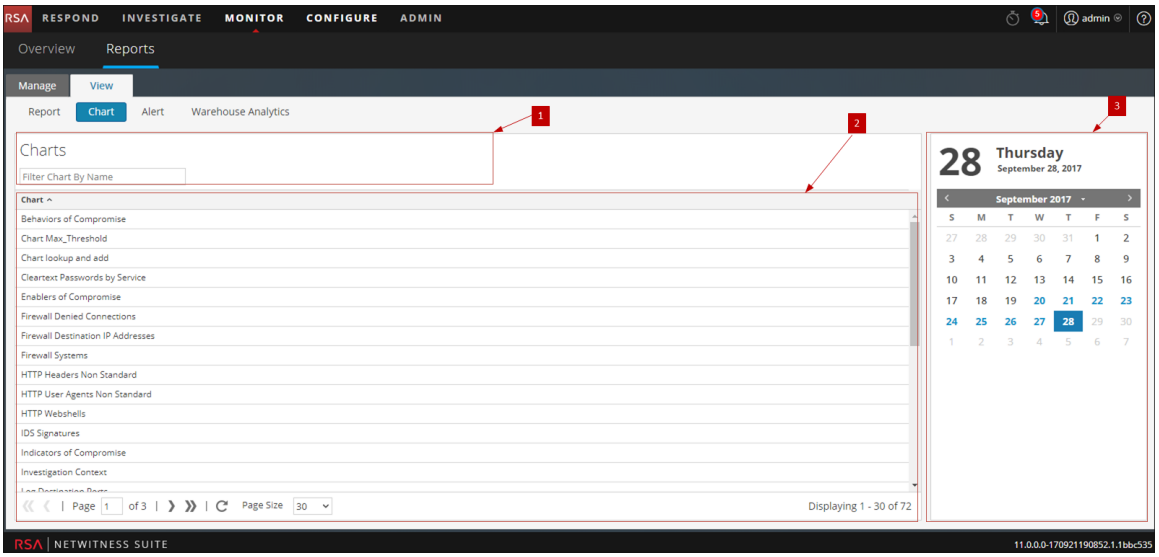
Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart*	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View



The View All Charts panel includes the following panels.

1	Charts Toolbar
2	Charts Output panel
3	Charts Calendar panel

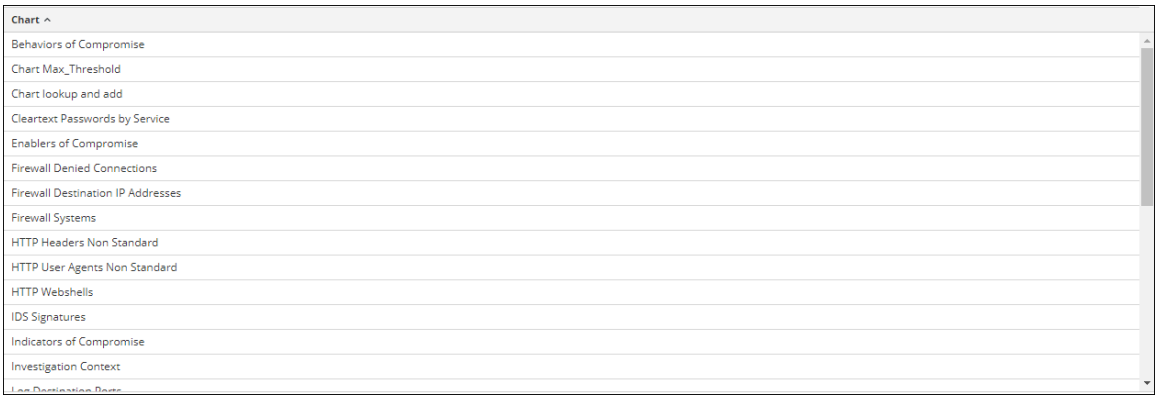
Charts Toolbar

The following table lists the options in the View All Charts toolbar:

Operation	Description
Filter Chart By Name	Searches schedules based on the chart name for a selected calendar day.

Charts Output Panel

The Charts Output panel displays the chart with the chart schedule name.



Feature	Description
Chart	This field displays all the successfully executed charts.

Charts Calendar Panel

The Charts Calendar panel is used to select a date from the Calendar. Based on the date you select, the list of successfully run charts for the date is displayed.

28
Thursday
September 28, 2017
September 2017
S M T W T F S
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7

View a Report Panel

The View a Report panel is used to review the reports.

Workflow

This workflow shows the procedure view a report or list of all reports.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

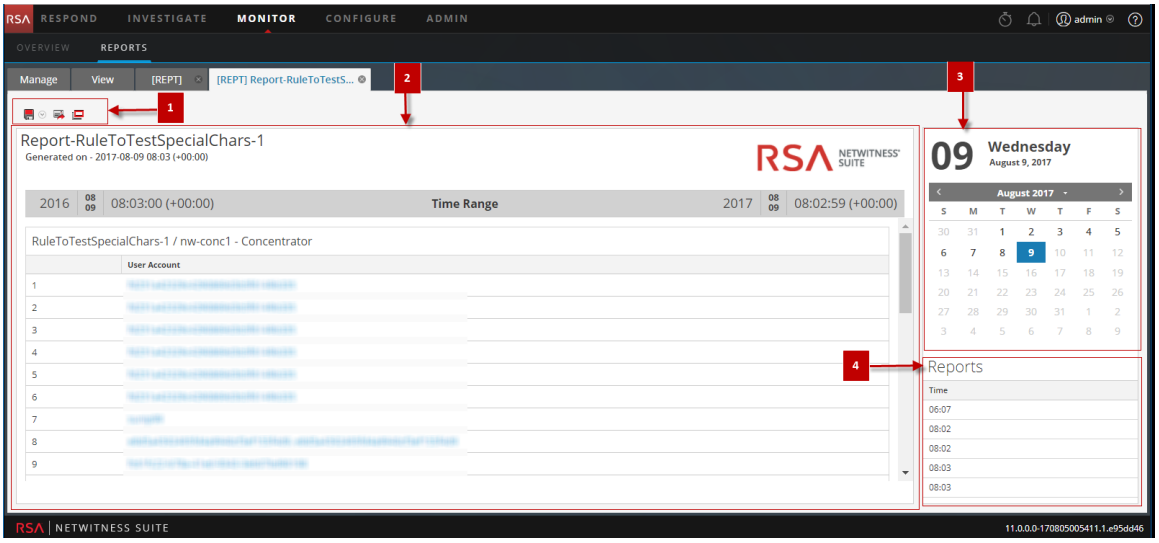
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Build Report View
- Import Report Dialog
- Scheduled Reports View
- Reports Permissions Dialog
- View All Reports View
- Report View

Quick View



To access this view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.

3. In the **Report List** panel, do one of the following:
   - Click >**View Scheduled Reports**.
   - Click the **#Schedules** column.
     The Report Schedule view is displayed.
4. Click **View** .

Features

The View a Report panel has the following sections.

1	Reports Toolbar
2	Reports Output panel
3	Reports Calendar panel
4	Reports Time panel

Reports Toolbar

The Reports toolbar allows you to print, save, email, and view reports on full screen.

Note: The Reporting Engine is responsible for generating PDF and CSV output of the reports based on the report definition. The size of the PDF files for a report must not exceed 50,000 cells.

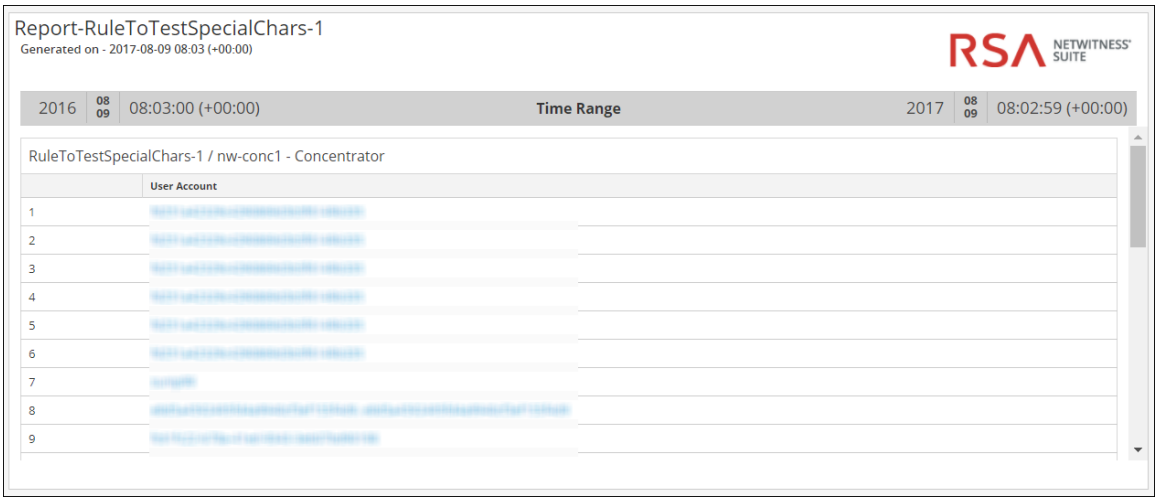
The following table lists the options in the Reports toolbar.

Operation	Description
	Prints the generated report.

Operation	Description
	Saves the report as a PDF and a CSV file. **Note:** The **Save As PDF** option is not available for a large report. If you are generating a PDF for a report and it takes a longer time than expected, you get a warning message stating **PDF generation is in progress, please try after some time**. When you click download as a CSV file, the Select Rule to download dialog is displayed. You must select a rule from this dialog to download the rule result in a CSV file. If the file generation takes a while, you can click on the **Notify me** option to be notified once the PDF or CSV is generated. Once the PDF or CSV is generated, you can view the Notifications for the status.
	Emails the report with the PDF or CSV attachment.
	Opens the generated report on a new window.

Reports Output View

The Reports Output panel view the report with the report schedule name, report generated time and the actual report with the selected rule variables.



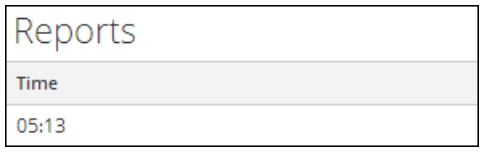
Feature	Description
Name	This field displays the name of the scheduled report.
Time	This field displays the time when the report is generated.
Report	This field displays the details report with the selected rule variables.

Reports Calendar View

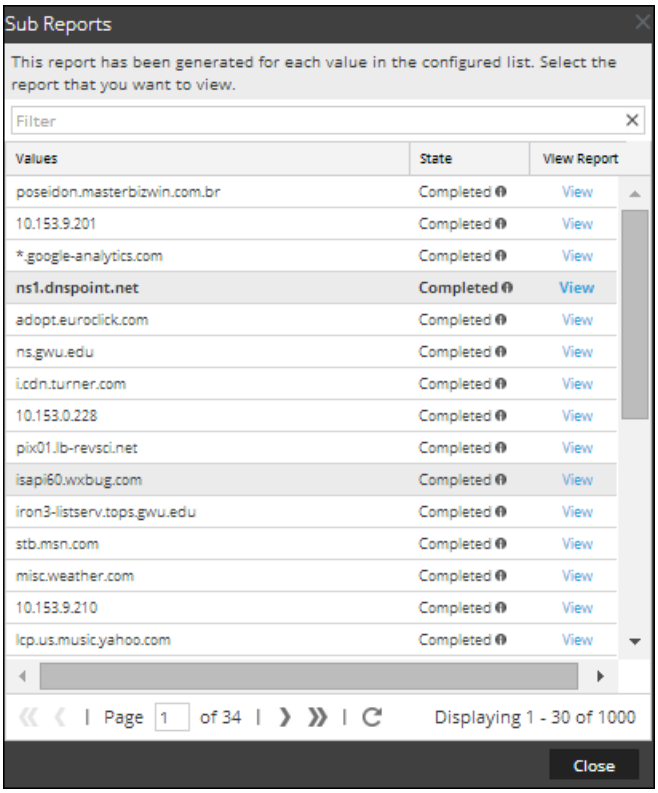
The Reports Calendar view is used to select a date from the Calendar. Based on the date you select, the list of successfully run reports for the date is displayed.

Reports Time View

The Reports Time view displays the time when the report was actually run.



When you click **View** on the scheduled report having **Iterative** selected, the **Sub Reports** panel is displayed. For each value in the configured list a report is generated.



The following table lists the columns in the Sub Reports panel.

Column	Description
Values	The List values chosen for a dynamic variable from the List Selection panel.

Column	Description
State	Indicates the state of the scheduled report for each of the list values. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule executions failed, the state of the report is displayed as failed. • Completed: If a report is successfully executed, the state of the report is displayed as completed.
View	Clicking on any of the report schedules or sub reports listed and then **View** displays the desired report. **Note:** You can view the completed rules on the **View a Report** page even when the report is 'running'.

View All Reports View

In the View All Reports view, you can display, print, save and email reports.

Workflow

This workflow shows the procedure view a report or list of all reports.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report

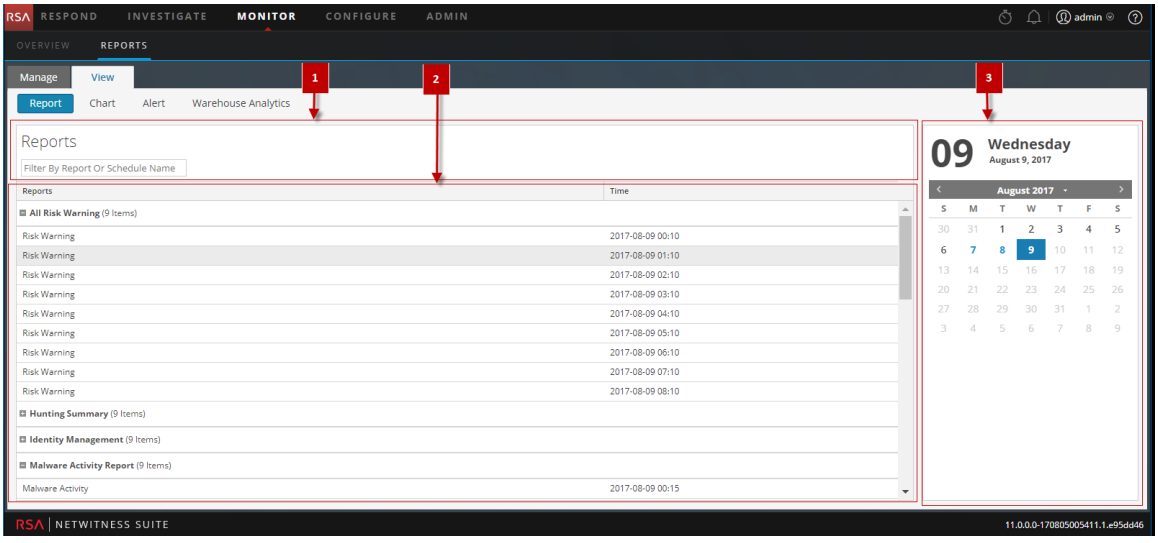
Role	I want to ...	Show me how
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Build Report View
- Import Report Dialog
- Scheduled Reports View
- Reports Permissions Dialog
- View a Report Panel
- Report View

Quick View



To access this view:

1. Go to **MONITOR** > **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.

3. In the **Report** panel, click **View All Reports**.
   The Reports panel is displayed, clicking on any of the reports listed allows you to view the report.

Features

The View All Reports panel has the following features.

1. Reports Toolbar
2. Reports Output panel
3. Reports Calendar panel

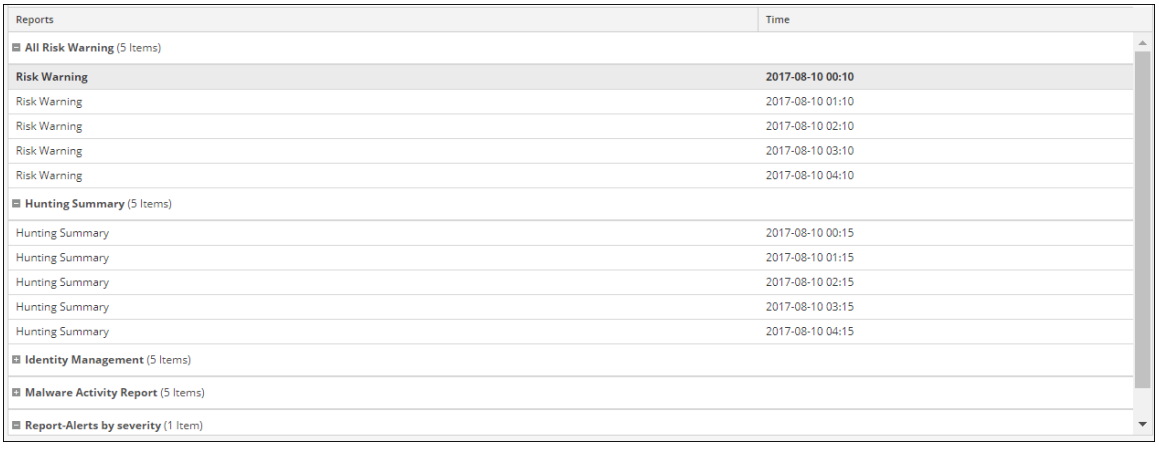
Reports Toolbar

The following table lists the options in the View All Reports toolbar:

Operation	Description
Filter By Report Or Schedule Name	Searches schedules based on the report name or schedule name for a selected calendar day.

Reports Output Panel

The Reports Output panel displays the report with the report schedule name and report generated time.



Feature	Description

Reports	This field displays the detailed report with the selected rule variables.
Time	This field displays the time when the report is generated.

Reports Calendar View

The Reports Calendar view is used to select a date from the Calendar. Based on the date you select, the list of successfully run reports for the date is displayed.

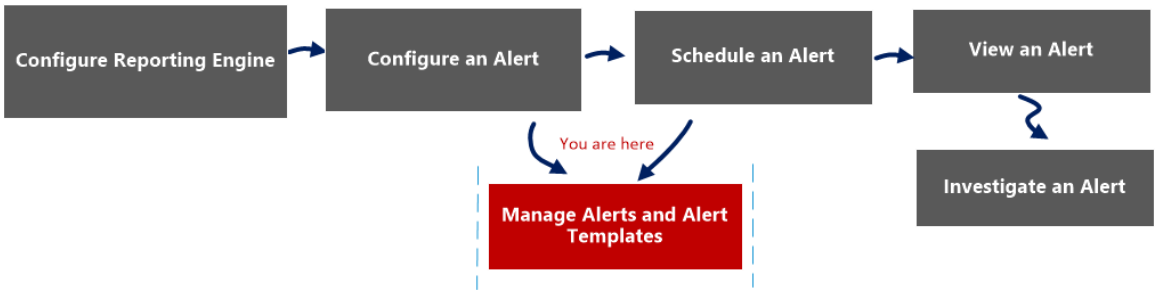
Alerting References

The Reporting module user interface provides access to NetWitness alerts. This topic contains descriptions of the user interface as well as other reference information to help users manage Alerts.

Alert List View

The Alert List view allows you to import, export, manage, and add alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

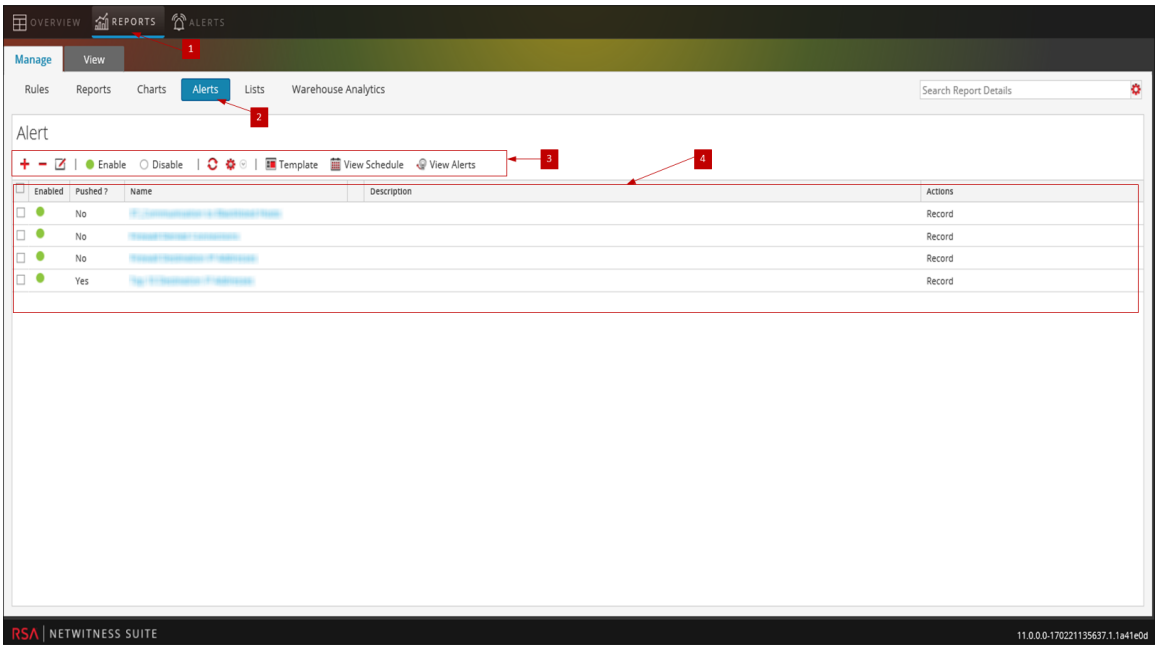
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



1	Click **Monitor**> **Reports** to view the Manage tab.
2	Click **Alerts** to open the Alert view.
3	The Alert toolbar allows you to add, modify, delete, enable, disable, refresh, import, and export an alert. Using this toolbar, you can also set access permissions for the selected alert.
4	The Alert List panel lists all the alerts in a tabular format.

The Alerts List view has the following panels:

- Alert Toolbar
- Alert List

Alert Toolbar

The Alert toolbar panel has the following features:

Feature	Description
	Adds a new alert to the Reporting module.
	Deletes one or more selected alerts.
	Edits an alert.

Feature	Description
Enable	Enables the selected alerts.
Disable	Disables the selected alerts.
	Refreshes the view.
	Enables the following options: Import, Export and Permissions.

Alert List

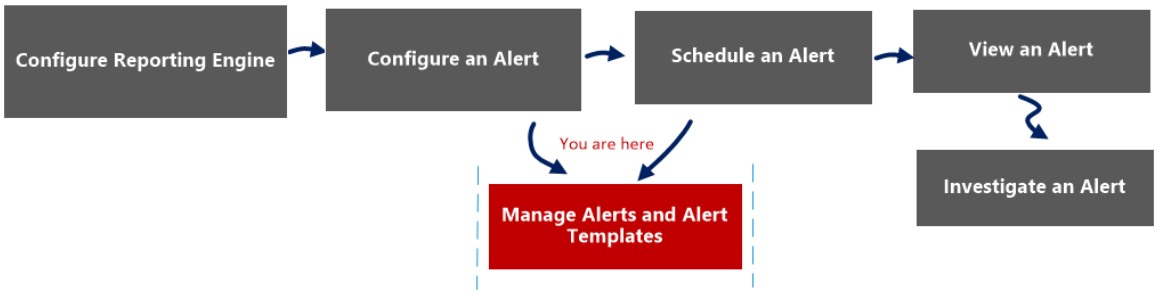
The Alert List panel lists all the alerts in a tabular format. The following table lists the columns in the Alert List panel and their descriptions.

Feature	Description
Enabled	Displays the state of the alert: • Enabled - the alert is active and fires based on the rule assigned to it. • Disabled - the alert is not active.
Pushed?	Indicates whether the alert is sent to Decoders or Log Decoders: • Yes - Alert is pushed to Decoders or Log Decoders. • No - Alert is not pushed to Decoders or Log Decoders.
Name	Identifies the name of the alert. Clicking the alert name displays the rule on which this alert is based in the Define Rules panel.
Description	Indicates the alert description.
Actions	Indicates the action the system takes when the alert fires. The different available action types are: • Record • SMTP • SNMP • Syslog

Alert Permissions Dialog

In the Alert Permissions dialog, the users with 'Read & Write' access permission can set access permissions for an alert to configure permissions in the Alert Permissions dialog.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

*You can complete these tasks here.

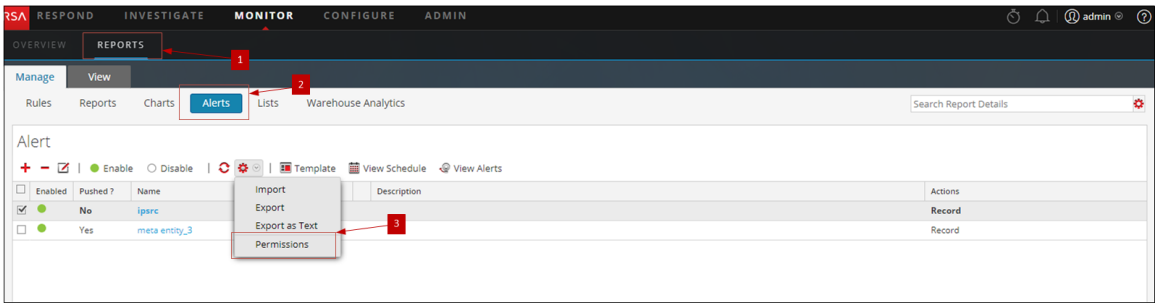
Related Topics

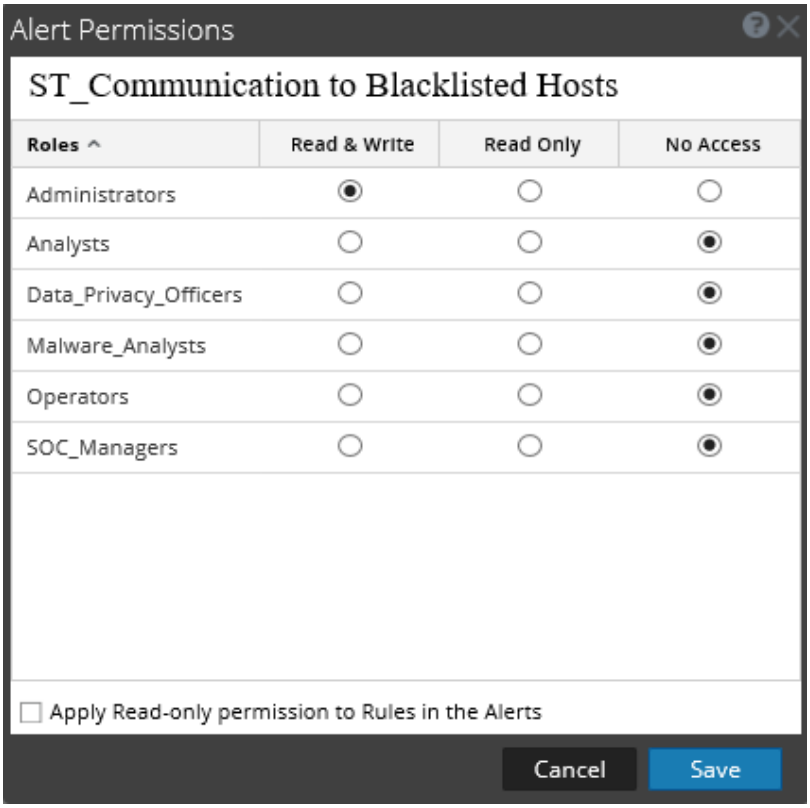
Alerting Overview

Quick View

The Alert permissions dialog allows you to set alert permissions depending on the user role.

The following figure is an example with the important features labeled.





1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Click > **Permissions**. The Alert Permissions dialog box is displayed.
4. Based on the user role, select the appropriate options.
5. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.

6 Click **Save**.

Note: If a User (other than a super user) creates an alert, super users will not be able to access the alert.

The following table lists the columns in the Alert Permissions dialog.

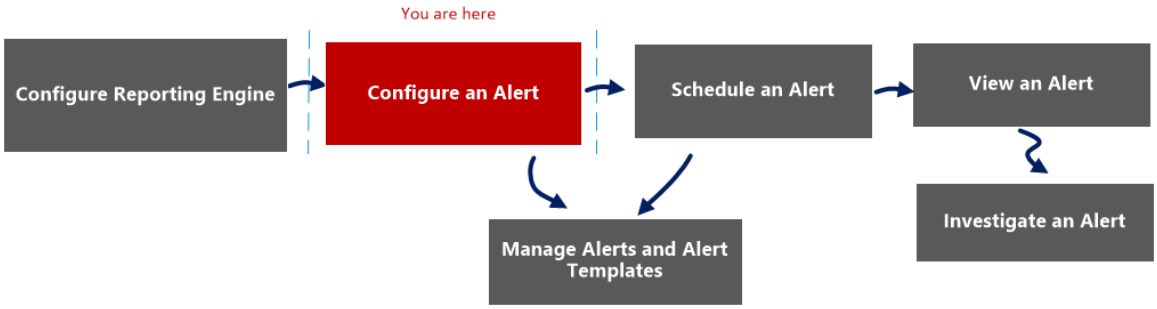
Column	Description
Roles	Displays all the user roles in the NetWitness user interface.
Read & Write	Allows you to apply 'Read&Write' access to the alert.
Read Only	Allows you to apply only 'Read' access to the alert.
No Access	By selecting this permission, you cannot access or view the alert.
Apply Read-only permission to Rules in the Alerts	Allows you to automatically apply permissions to the rules in the alerts.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selection and provides access to the role based on the selection.

Alert Schedules View

In the Alert Schedules view, you can view all the alerts scheduled. Alternately, you can also disable the scheduled alerts.

Workflow

The following workflow shows the tasks involved in creating or modifying an alert.



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert*	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

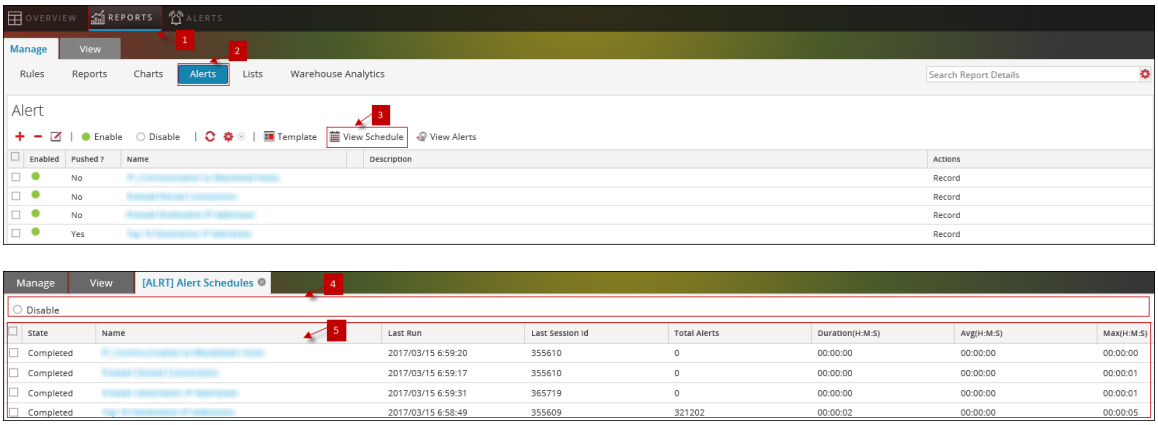
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following example shows you how to access the Alert Schedules view dialog.



1	Click **Monitor> Reports** to view the Manage tab.
2	Click **Alerts** to open the Alert view.
3	Click **View Schedule** to open the View Alerts Schedule view.
4	The Alerts Schedule toolbar allows you to modify the state of the scheduled alert.
5	The Alerts Schedule List panel lists only the Enabled alerts in a tabular format.

Features

The different panels on the Alert Schedules View dialog are:

- Alerts schedule toolbar panel
- Alerts schedule list panel

Alerts Schedule Toolbar Panel

In the Alerts Schedule Toolbar panel, the Disable icon disables the selected alert. When schedule alerts are no longer needed or are determined to be ineffective, you can disable them so that they are no longer executed. You can select one of more alerts to disable. When an alert is disabled, it is removed from the scheduled alerts list so that you cannot view it here, and it will not execute again unless you manually execute the alert or set up a new schedule for it.

Alerts Schedule List Panel

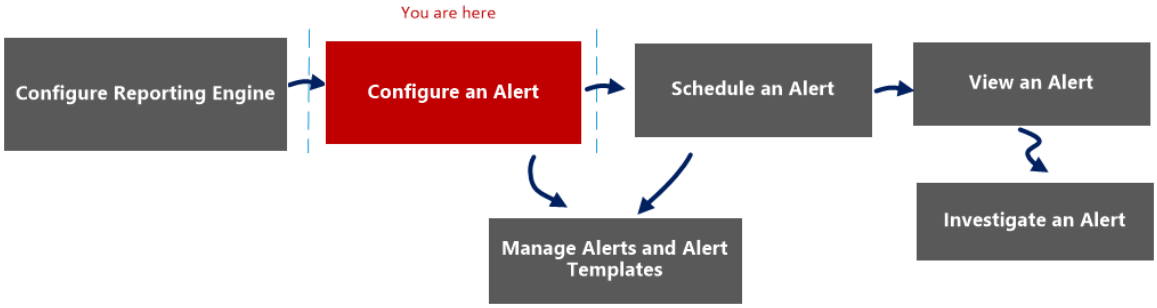
The following table lists the columns in the Alerts Schedule List panel and their description.

Column	Description
State	The state of the scheduled alert: • Completed • Failed
Name	The name of the scheduled alert.
Last Run {#time}	The last time the scheduled alert was run.
Last Session Id	The Session Id of the last scheduled alert.
Total Alerts	The total number of event occurrences.
Duration	The time taken to run the scheduled alert.
Avg (s)	The average time taken to run the scheduled alert.
Max (s)	The maximum time taken to run the scheduled alert.

Create or Modify Alert Panel

The Create or Modify alert panel is a panel in the Alert List view. This panel allows you to create or modify an alert as per the requirement.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert*	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

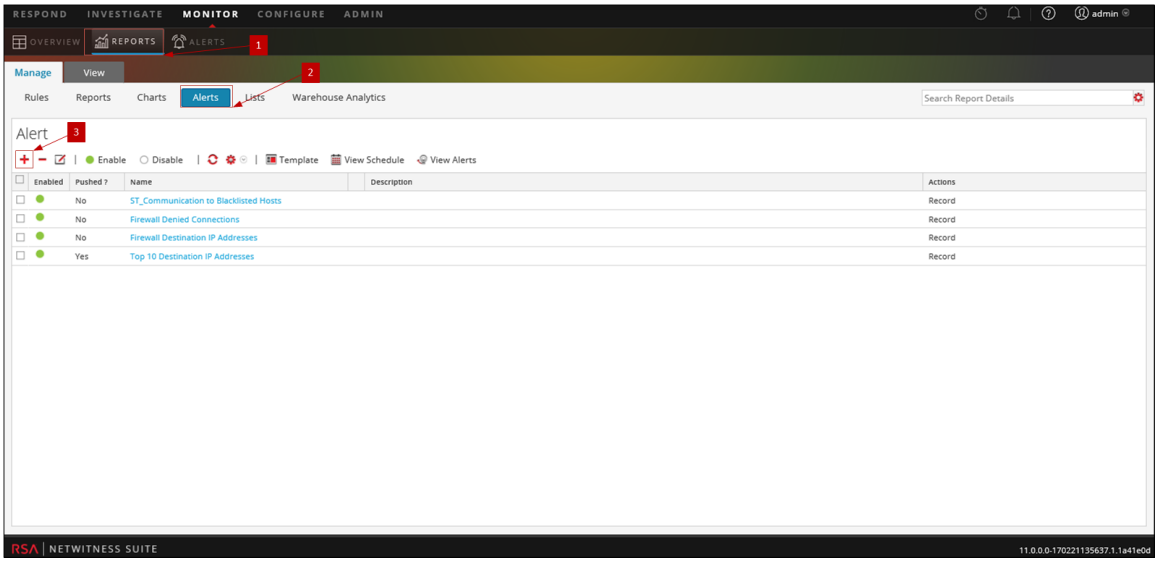
*You can complete these tasks here.

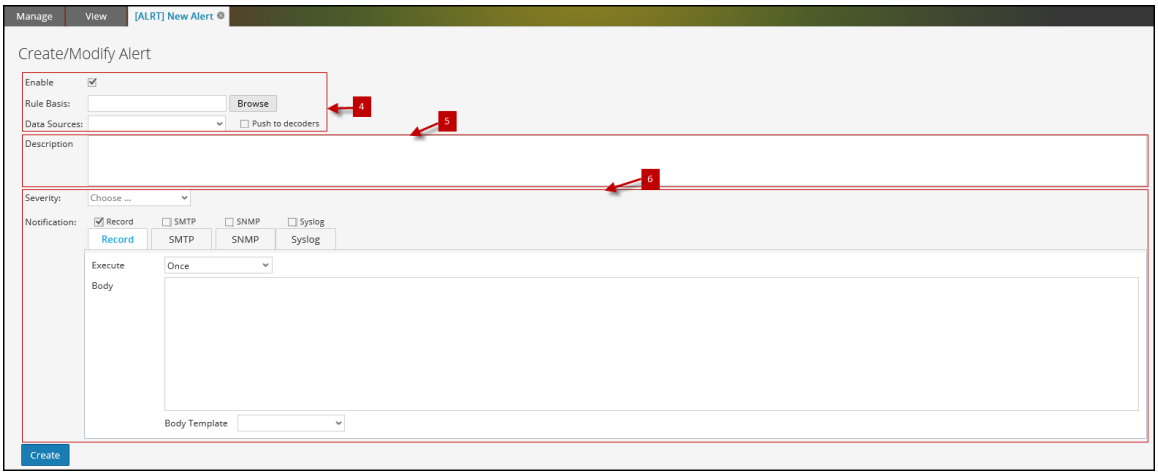
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1	Click **Monitor**> **Reports** to view the Manage tab.
2	Click **Alerts** to open the Alert view.
3	Click + to navigate to the Create or Modify Alert panel.
4	Enable the alert, navigate the rule, and select a data source to alert.
5	Enter a brief description of an alert.
6	Define the alert notification methods(RECORD, SMTP, SNMP, Syslog) to alert, when an alert condition is matched.

The Create or Modify Alert panel has the following sections:

- Alert Definition
- Alert Description
- Alert Notification

Alert Definition

The following table describes the fields in the Alert Definition:

Field	Description
Enable	• **Enable** activates the alert. The alert executes and sends output actions every minute (by default) when the alert conditions are met. • **Disable** deactivates the alert. The alert does not execute and does not send any output actions.
Rule Basis	Click **Browse** to display the Rules Library panel from which you select the rule that is the basis of this alert. You must select a rule that has a unique 'where' clause for an alert.
Data Sources	Specifies the data source for the alert.
Push to decoders	Pushes the ‘where’ clause of the alert rule to Decoders connected to the selected NWDB data source. This is the recommended option used to create RE alerts, as the alert conditions are checked on the Decoder itself and the alert queries will be comparatively faster in NWDB. If you deselect this option, the alert rule ‘where’ clause will be queried against the selected NWDB data source. Based on the complexity and metas in the ‘where’ clause of the rule, the alert queries might take more time to process in NWDB. **Note:** NetWitness does not send rules to the Decoder automatically.

Alert Description

The following table describes the fields in the Alert Description:

Field	Description
Description	Describes the alert.
Create	Creates the alert. (This option is displayed when you create an alert.)
Save	Saves the changes made to the alert. (This option is displayed when you modify an alert.)

Alert Notification

The Alert Notification allows you to define the notification action NetWitness takes when an alert is generated, for example, recording or sending the alert using one of the defined output actions. The output actions are Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), or Syslog message.

The Notification contains the default Record tab, which you use to create an alert. The icon beside the Record tab allows you to select the notification type from the drop-down list for the output to specify for the alert: SMTP, SNMP, or Syslog.

Depending on the selected notification type, the Notification section is populated with predefined text that contains variables that add Meta that is appropriate for the alert. In the Reporting Engine, these variables are replaced with actual values. The following table lists the variables and their descriptions.

Variable	Description
${meta.<metakey>}	The meta key value. **Note:** If the <metakey> did not fetch any value, an empty string("") is printed. By default, Reporting Engine displays all the repeated values for a meta key. If you do not want the meta values to repeat in the Alert output, enable the "removeRepeatedMetaValue" option by navigating to **Configuration > Alert Configuration** available for the Reporting Engine in the **Services - Configuration > Explore** view. For example, in an HTTP Session the value for the action is displayed as get, get, put, put, post, get. When this option is enabled, the value is displayed as get, put, post.
${meta.time} / ${meta.time:<time_format>}	${meta.time} - The session time is printed in "yyyy-MMM-dd HH:mm:ss" format. ${meta.time:<time_format>} - The session time is printed in the user-defined custom time format. For example, ${meta.time:dd-MM-yyyy HH:mm:ss}. For more information on the supported time formats, see http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html **Note:** If the time format provided by the user is invalid, the default time format will be used. The default time format is "yyyy-MMM-dd HH:mm:ss".
${name}	The alert name defined in Reporting Engine.
${count}	The number of times an alert is detected in a given time frame. (By default, it is one minute)
${nw.host}	The NetWitness host name as configured in Reporting Engine.
${device.id}	The NetWitness device ID of the data source.

The Alert Notification has four tabs:

- **Record Tab**
- **SMTP Tab**
- **SNMP Tab**
- **Syslog Tab**

Record Tab

Use the Record tab to define the frequency for recording an alert and the message to generate when an alert is generated.

The following table lists the fields in the Record tab and their description.

Field	Description
Execute	The frequency for recording an alert. • **Once** - Record the alert only once based on the alert interval no matter how often the alert is generated. NetWitness records the number of times the alert has actually generated during that interval in the log file so that analysts know how many times the alert registered a match over a given day. • **Each Event** - Record the alert each time as it generates. If an alert generates unlimited number of times during a day, that alert is often treated as noise and can be ignored, except in case of alerts that require continuous monitoring such as network configuration changes and DDOS attacks. **Note:** Select **Each Event** setting from the **Execute** drop-down list for SNMP and Syslog output actions.
Body	The body of the message.

Field	Description
Body Template	(Optional) If templates have been defined, select a template for the alert message.

SMTP Tab

The SMTP tab allows you to define the SMTP (email) output for this alert.

The following table lists the fields in the SMTP tab and their description.

Field	Description
Execute	The frequency to send an email message for the alert. • **Once** - Sends only one email for an interval, if an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Send an email with the alert for every event in which the rule criteria are met.
To	The email addresses to which to send this alert.
Subject	The subject of the email message.
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the SMTP message that you can use as is or modify.

SNMP Tab

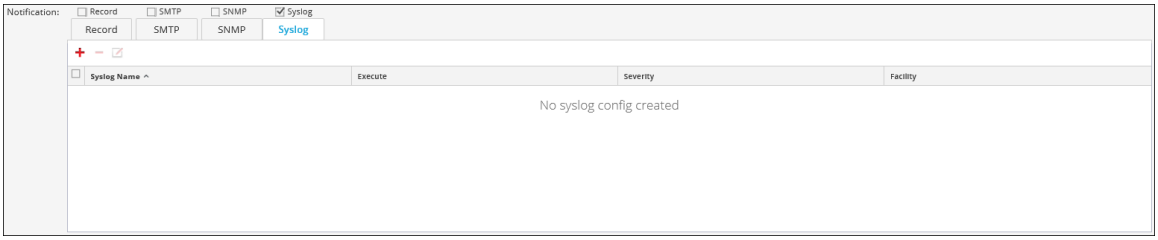
The SNMP tab allows you to define the SNMP output for the alert.

The following table lists the various fields in the SNMP tab and their description.

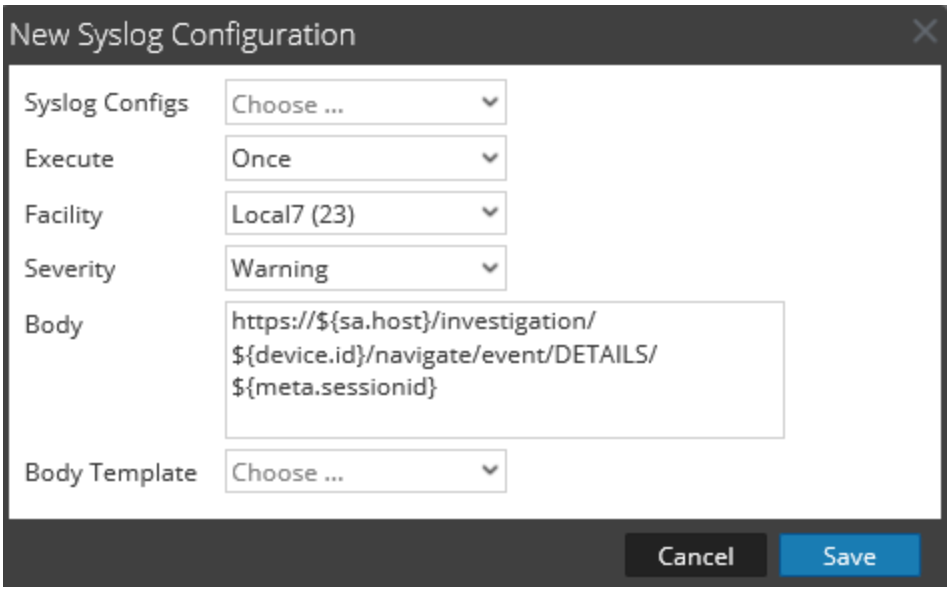
Field	Description
Execute	The frequency to send an SNMP output for an alert. • **Once** - Sends an SNMP message along with an email for an interval, if an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Sends an SNMP message with the alert for every event in which the rule criteria are met.
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the SNMP message to use as is or modify.

Syslog Tab

The Syslog tab allows you to define the Syslog message output for this alert.



Click + to add Syslog configuration to an alert. The New Syslog Configuration dialog box is displayed:



The following table describes the fields in the New Syslog Configuration dialog:

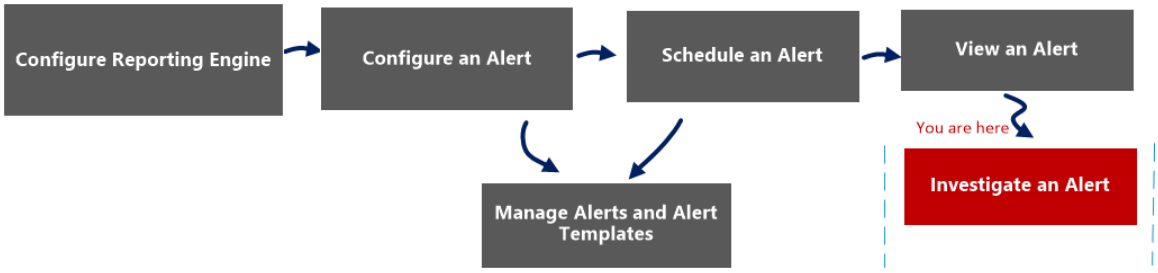
Field	Description
Syslog Configs	The Syslog configuration of the Device Config view located at the Syslog Configuration panel .
Execute	The number of times that you want to send a Syslog output for the alert. • **Once** - Sends a Syslog output along with an email for an interval, an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Sends a Syslog output with the alert for every event in which the rule criteria are met.
Facility	The type of program logging the message. Examples for the type of programs are Syslog, Daemon, Mail, and Kernel.

Field	Description
Severity	The severity level of the alert that generated. • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the Syslog message to use as is or modify.

Investigate an Alert View

In the Investigate an Alert view, you can view and investigate alert details. When investigating an alert, you can open the sessions in the Investigation module for further investigation.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert*	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

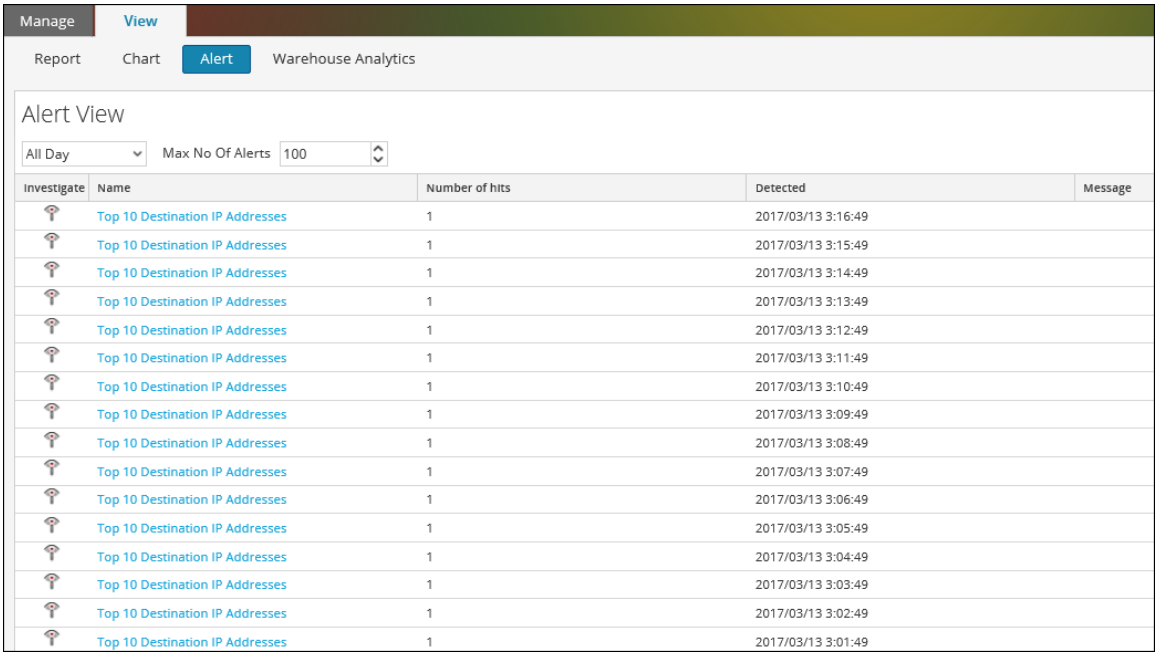
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



The View an Alert view has the following panels:

- View Alerts Toolbar
- View Alerts List

View Alerts List

The following table lists the columns in the View Alerts List panel.

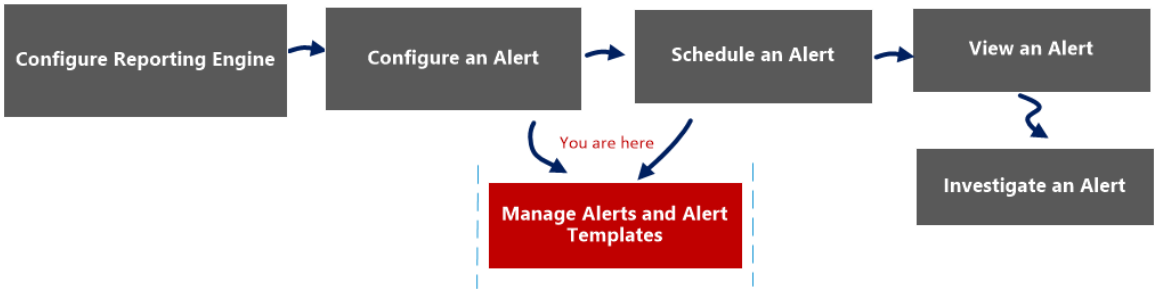
Column	Description
	The icon that opens the Investigation module, where the details of the first session that registered the match for the given alert is displayed for immediate analysis. **Note:** You are not redirected to the Investigation module when: -You reconfigure a data source for an existing alert and run an alert on the new data source. -You enter a host name instead of an IP address in the data source field.
Name	The name of the alert that registered the match. The hyperlink on the name opens the Investigation module to view all matches for that particular alert for the hour surrounding the registered alert.

Column	Description
Number of hits	The number of times the alert is generated.
Detected	The date and time at which the alert generates.
Message	The alert message.

Import Alert Dialog

The Import Alert dialog allows you to import an alerts archive and specify whether to overwrite existing rules, lists, and alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

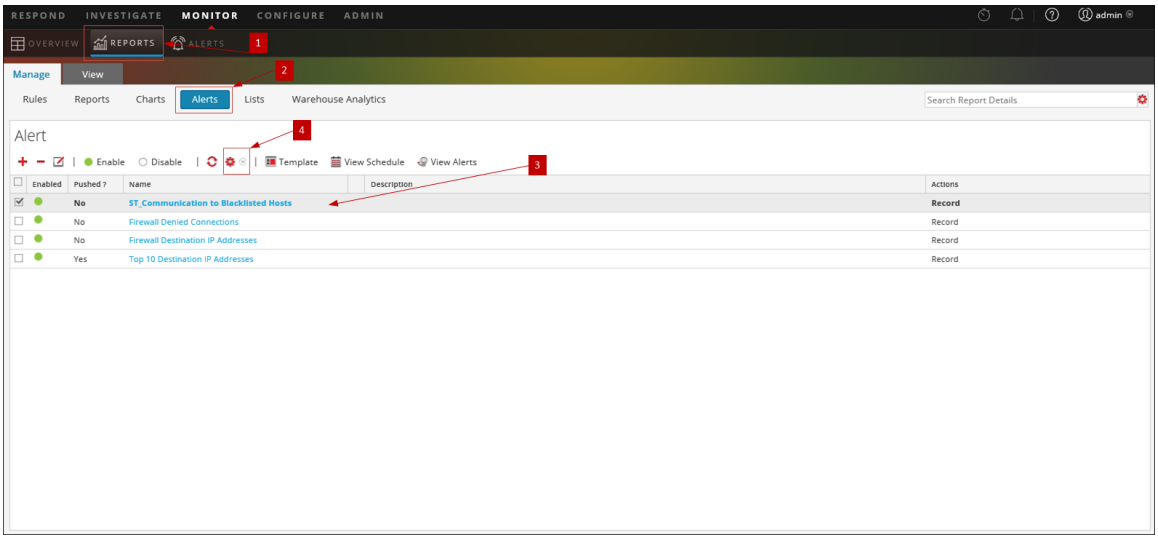
*You can complete these tasks here.

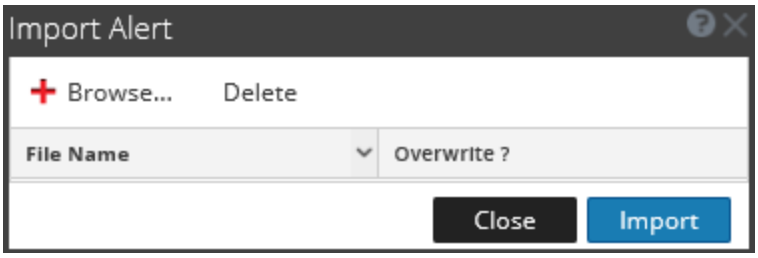
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. In the **Alert** panel, select a folder to import the file.
4. In the **Alert** toolbar, click > **Import** to import an alert.

The following table lists the actions in the Import Alert dialog and their description.

Actions	Description
Browse...	Displays a view of the local zip file system so that you can select the alert to be imported.
−	Deletes the selected alert from the Import Alert dialog.
File Name	Name of the imported binary file.

Actions	Description
Overwrite?	Selects the option to overwrite an existing version of the alert you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	Closes the Import Alert dialog.
Import	Imports the alert with a confirmation message.

Alert Template References

The Reporting module user interface provides access to NetWitness alerts and alert templates as well. This topic contains descriptions of the user interface as well as other reference information to help users manage alert templates.

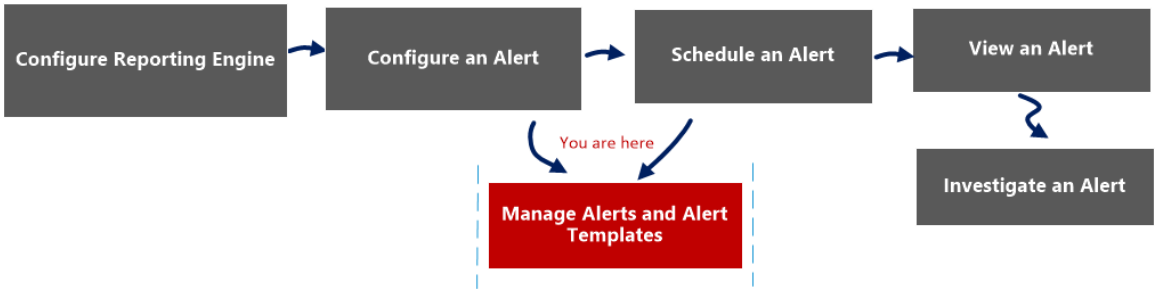
Topics:

- Create or Modify Template View
- Template View

Alert Template View

In the Template view, you can add, modify, view, and delete alert templates.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

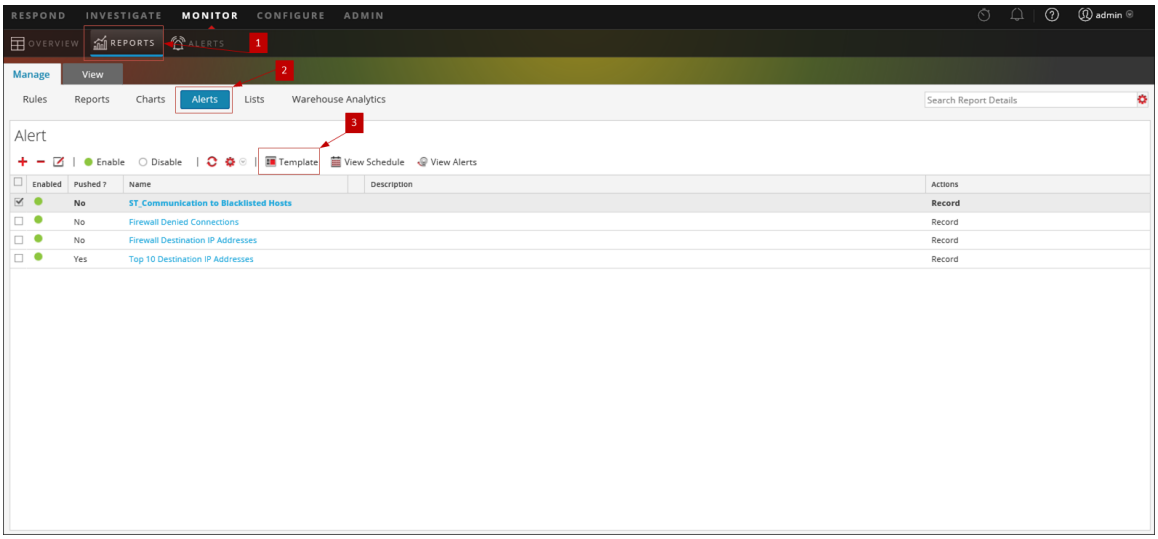
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Click Template to open the Template view.
4. The Template toolbar allows you to add, modify, and delete alert templates.
5. The Template List panel allows you to view a list of all the templates in a tabular format.

The Alert Template view has the following panels:

- Template Toolbar
- Template List

Template Toolbar

Once the templates are defined, you can select a template to simplify defining and modifying alert messages.

The following table lists the various actions in the Template view and their description.

Actions	Description
	Creates a new alert template.
	Deletes the selected alert template.
	Edits an existing alert template.

Template List

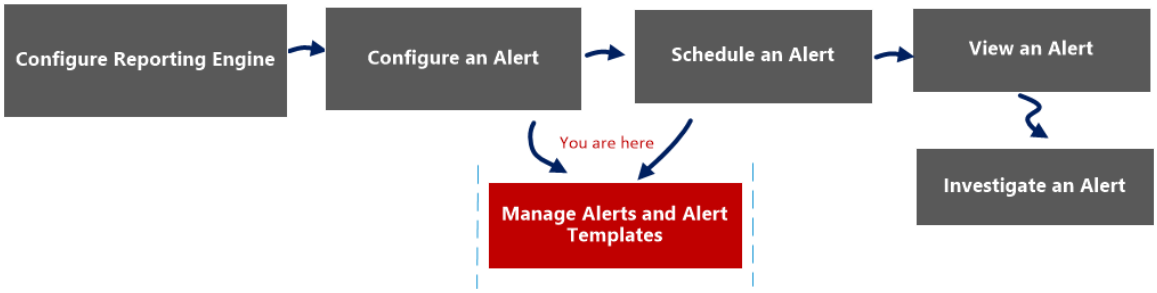
The following table describes the columns in the Templates List panel.

Column	Description
Name	Name of the template.
Message	Alert message defined for the template.

Create or Modify Template View

In the Create/Modify Template view, you can customize alert templates to use when creating alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

*You can complete these tasks here.

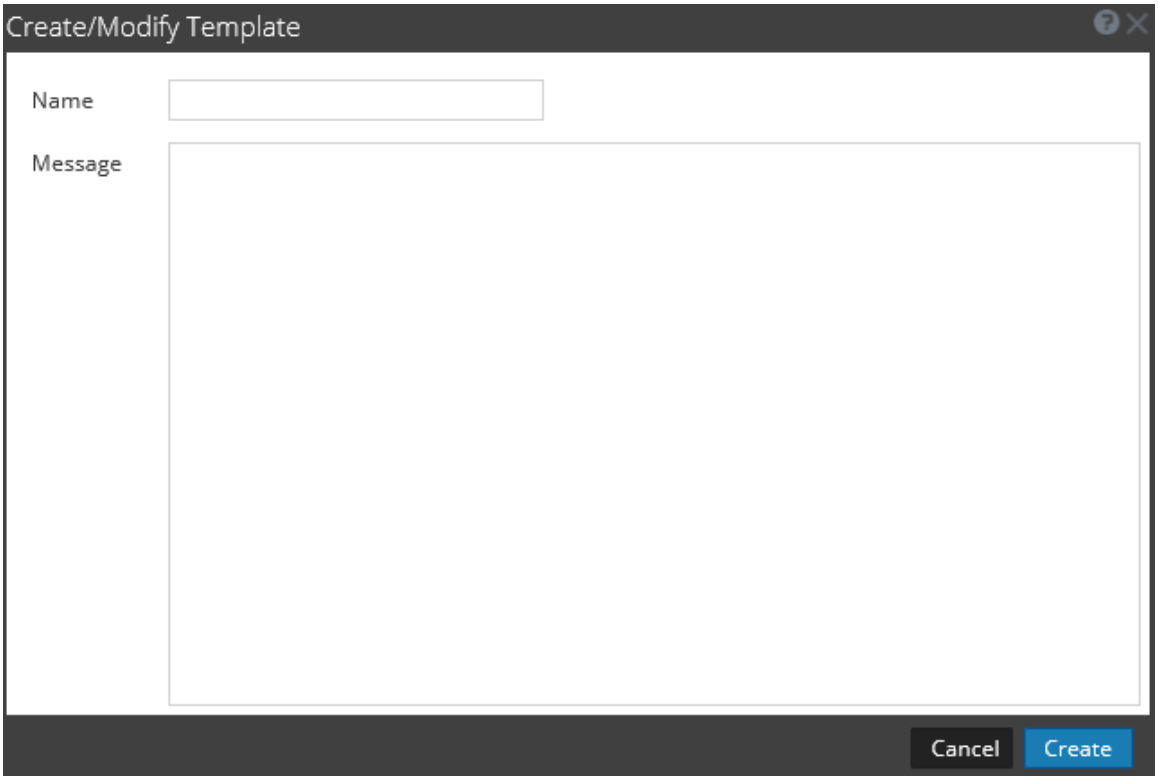
Related Topics

Alerting Overview

Quick View

You can create or modify an alert template name and message on this view.

The following figure is an example of the Create or Modify alert template.



The following table describes the fields in the Create/Modify template.

Feature	Description
Name	Indicates the name of the template for Reporting alerts. For example, source IP.
Message	Specifies the message that will be sent when an alert is triggered.
Create	Creates the template with a confirmation message and becomes available for use in Reporting immediately.
Save	Saves the template with the edited details or when a new template is created. This button is visible only in the edit mode.
Cancel	Closes the dialog without saving the template or any changes made to the template.

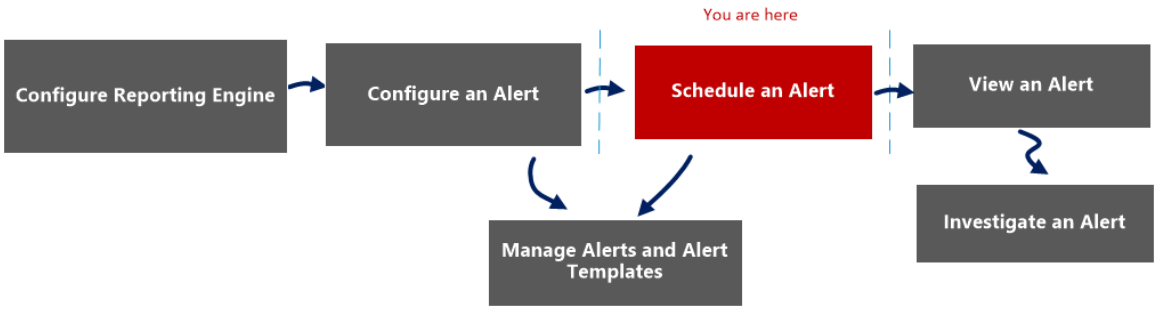
View Alerts Schedule View

In the View Alerts Schedule view, you can view the following information about each of your scheduled alerts.

- Completion status, name, last run time, last session ID, total alerts triggered.
- Statistics about the time taken to run the scheduled alert: duration, average duration, maximum duration.

Note: You can also disable the scheduled alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert*	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

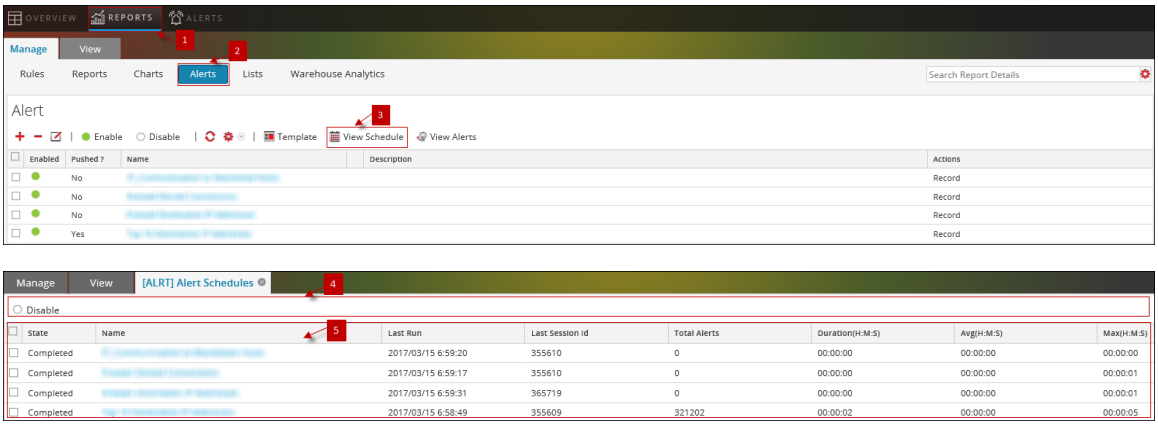
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Click **View Schedule**to view all the alerts scheduled.
4. The Alerts schedule toolbar allows you to disable the scheduled alert.
5. The Alerts schedule list allows you to view the scheduled alert details.

The View Alerts Schedule view includes the following panels:

1. Alerts Schedule toolbar
2. Alerts Schedule list

Alert Schedule Toolbar

The Alerts Schedule Toolbar panel allows you to modify the state of the scheduled alert.

Feature	Description
Disable	Clicking **Disable** disables the selected alert. When schedule alerts are no longer needed or are determined to be ineffective, you can disable them so that they are no longer executed. You can select one of more alerts to disable. When an alert is disabled, it is removed from the scheduled alerts list so that you can't view it here, and it will not execute again unless you manually execute the alert or set up a new schedule for it.

Alert Schedule List Panel

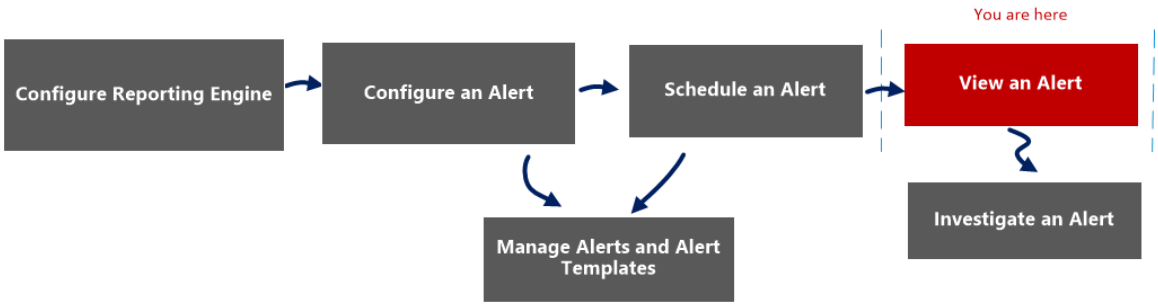
The Alerts Schedule List panel lists only the Enabled alerts in a tabular format. The following table lists the columns in the Alerts Schedule List panel and their description.

Feature	Description
State	The state of the scheduled alert: • Completed • Failed
Name	The name of the scheduled alert.
Last Run {#time}	The last time the scheduled alert was run.
Last Session Id	The Session Id of the last scheduled alert.
Total Alerts	The total number of event occurrences.
Duration	The time taken to run the scheduled alert.
Avg (s)	The average time taken to run the scheduled alert.
Max (s)	The maximum time taken to run the scheduled alert.

View Alerts View

In the View Alerts view, you can view all the alerts. Also, you can also customize the view to show alerts for a specific period of time, and set the maximum number of alerts displayed in a single page.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert*	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

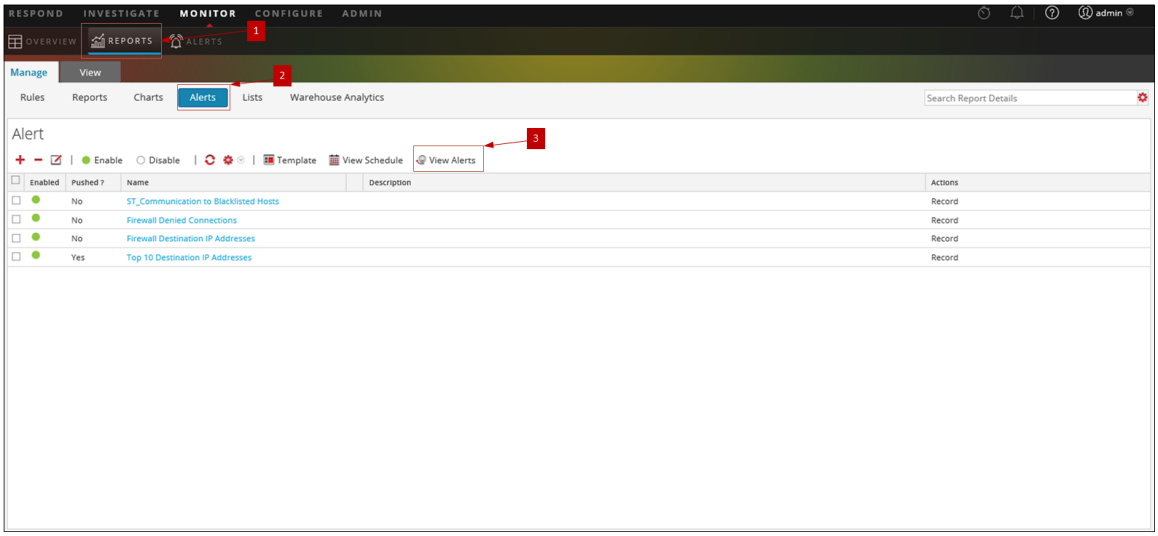
*You can complete these tasks here.

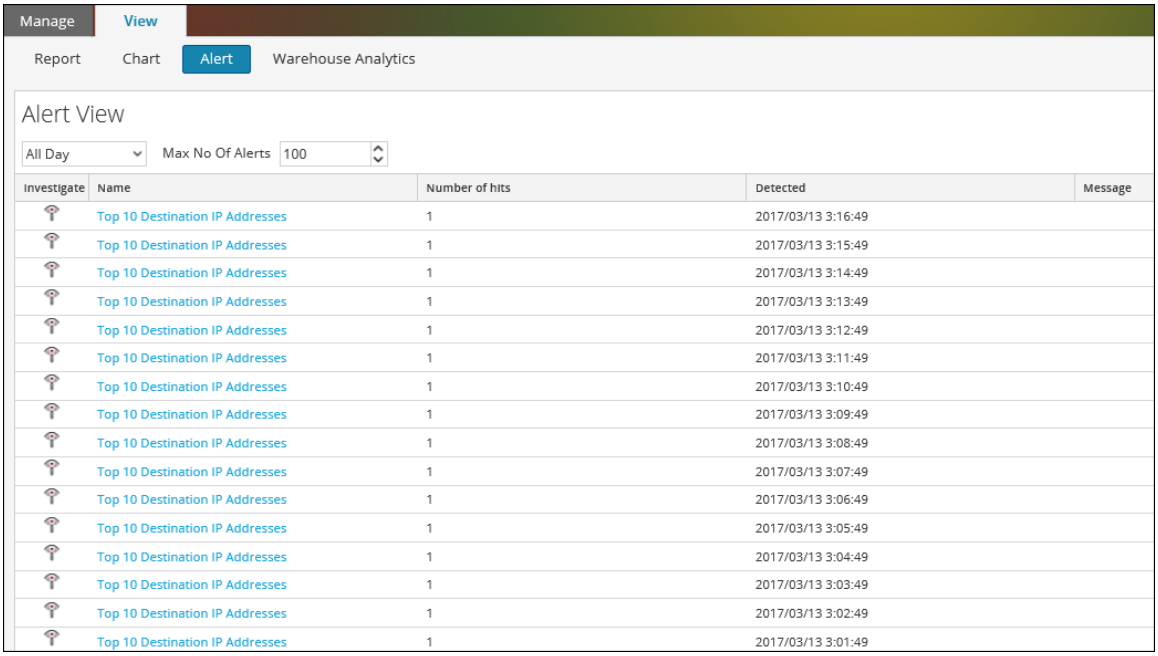
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1. Click **Monitor**> **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Click **View Alerts** to view the different panels on View Alerts.
4. The View Alerts toolbar allows you to filter alerts based on a count, or the start and end date of the alerts.
5. The View Alerts List lists all the filtered alerts in a tabular format.

The View Alerts view has the following panels:

- View Alerts Toolbar
- View Alerts List

View Alerts Toolbar

The following table lists the operations in View Alerts toolbar panel.

Option	Description
Last Hour(s) data	The data fetched from the previous execution.
Max No Of Alerts	The maximum number of alerts that you want to fetch from the Reporting Engine service for a specific time-range.

View Alerts List

The following table lists the columns in the View Alerts List panel.

Column	Description
	The icon that opens the Investigation module, where the details of the first session that registered the match for the given alert is displayed for immediate analysis. **Note:** You are not redirected to the Investigation module when: -You reconfigure a data source for an existing alert and run an alert on the new data source. -You enter a host name instead of an IP address in the data source field.
Name	The name of the alert that registered the match. The hyperlink on the name opens the Investigation module to view all matches for that particular alert for the hour surrounding the registered alert.
Number of hits	The number of times the alert is generated.
Detected	The date and time at which the alert generates.
Message	The alert message.

RSA NETWITNESS® SUITE

Hosts and Services Configuration Guides

for Version 11.1

RSA NETWITNESS® SUITE

Archiver Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

February 2018

Contents

Archiver Overview **5**

Configuring an Archiver **7**

Prerequisites 7

Workflow 7

Add the Archiver Service 9

Add Log Decoder as a Data Source to Archiver 11

Add Log Decoder as a Data Source to Archiver 11

Archiver Meta Settings Considerations 12

(Optional) Configure Meta Filters for Aggregation 13

(Optional) Add Index Entries for Archiver Reporting 15

Configure Archiver Storage and Log Retention 17

Configure Hot, Warm, and Cold Storage 20

Configure Log Storage Collections 34

Define Retention Rules 38

Add Archiver as a Data Source to Reporting Engine 41

Configure Archiver Monitoring 44

Additional Archiver Configuration **45**

Configuring Data Backup and Restore 46

Add Archiver Service 46

Create Collection 48

Add Archiver Service as a Data Source to Reporting Engine 50

Mount Archiver Directories 52

Create a Collection 53

Delete a Collection 55

Example Procedure: How to Restore a Collection for Reporting and Investigation 55

Investigate a Collection 57

View Archiver Collection Statistics 57

View Archiver Logs 58

Add Archiver Service as a Data Source to Broker 58

Retrieve Hash Information 61

References **67**

Archiver Collection Dialog 68

Archiver Services Config View - General Tab 71

Aggregate Services Section 73

Aggregation Configuration Section 76

Archiver Service Configuration 78

Data Retention Tab - Archiver 80

Total Hot, Warm, and Cold Storage 82

Services Config View - Archiver 84

General 87

Aggregation Settings 89

Service Heartbeat 89

Files 89

Archiver Overview

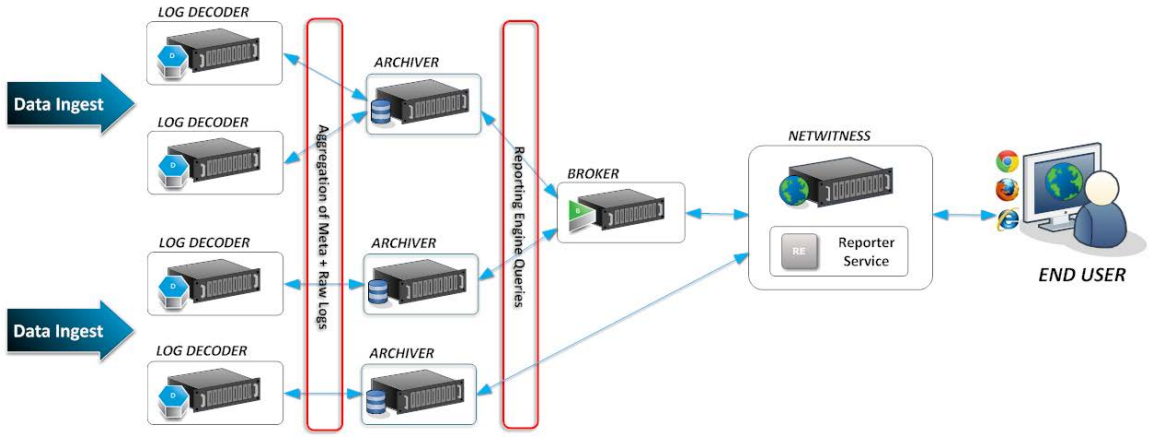
This guide provides detailed instructions on how to configure Archiver in your network, additional procedures that are used at other times, and reference materials that describe the user interface for configuring Archiver in your network.

The NetWitness Suite Archiver is an appliance that enables long-term log archiving by indexing and compressing log data and sending it to Archiving storage. The Archiving storage is then optimized for long-term data retention and compliance reporting.

Archiver stores raw logs and log meta from Log Decoders for long-term retention and it uses Direct-Attached Capacity (DAC) for storage.

Note: Raw packets and packet meta are not stored in the Archiver.

The following figure depicts the architecture of a NetWitness Suite network that implements the Archiver.



Configuring an Archiver

The NetWitness Suite Archiver is an appliance that enables long-term log archiving by indexing and compressing log data and sending it to Archiving storage. The Archiving storage is then optimized for long-term data retention and compliance reporting.

Archiver stores raw logs and log meta from Log Decoders for long-term retention and it uses Direct-Attached Capacity (DAC) for storage.

Note: Raw packets and packet meta are not stored in the Archiver.

Prerequisites

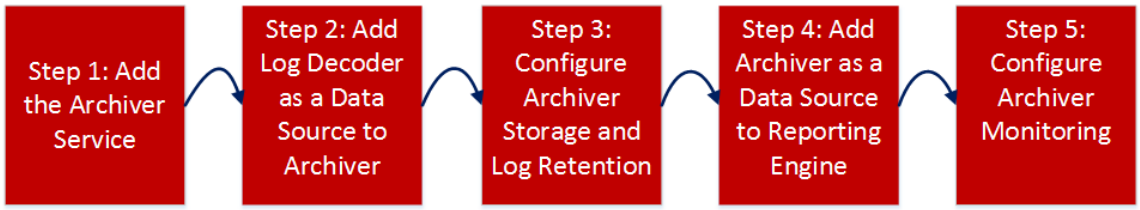
Ensure that you have:

- Installed the Archiver host in your network environment.
- Installed and configured Log Decoder version 11.1 in your network environment.

If you want to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them, refer to **Group Aggregation** in the *Deployment Guide*.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.



The following table describes the basic steps for configuring an Archiver.The tasks must be completed in the sequence they are given.

Configuration Step	Description
Add the Archiver Service	Provides information on how to add an Archiver service to the Archiver host and apply a license to it.
Add Log Decoder as a Data Source to Archiver	Provides instructions on how to add a Log Decoder to an Archiver.

Configuration Step	Description
Configure Archiver Storage and Log Retention	Provides instructions on how to configure storage and log retention on an Archiver.
Add Archiver as a Data Source to Reporting Engine	Provides instructions on how to add an Archiver as a data source to Reporting Engine to generate reports for the data collected by an Archiver.
Configure Archiver Monitoring	Provides instructions on how to configure the alert mechanism related to Archiver storage.

Add the Archiver Service

In order to add an Archiver service, ensure that you have installed an Archiver host on which you want to run the Archiver service. See "Step 1: Add or Update Host" topic in the *Host and Services Getting Started Guide* for the procedure that explains how to add a host.

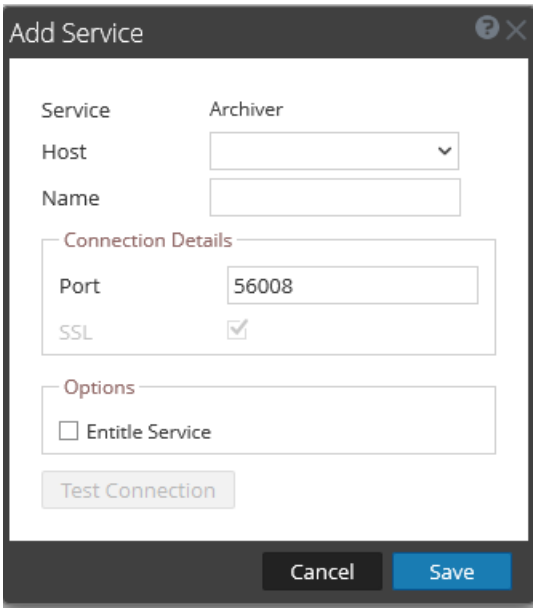
After you install an Archiver host, you need to add an Archiver service an apply a license to it, as explained in the following procedure.

Note: This procedure is only required if you do not have the Archiver service installed.

Perform the following steps to add the Archiver service:

1. Go to **ADMIN > Services**.
2. In the **Services** panel toolbar, select + **> Archiver**.

   The Add Service dialog is displayed.



3. Provide the following details.

Field	Description
Host	Select a host from the drop-down menu.
Name	Type a name for the service.
Port	Default port is 50008.

Field	Description
SSL	Select **SSL** if you want NetWitness Suite to communicate with the service using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. **Note:** If you select SSL, ensure SSL is enabled in the System Configuration panel.
Username	(Optional) Type the username for the service.
Password	(Optional) Type the password for the service.
Entitle Service	Select if you want to apply the entitlements currently configured to this service. For more information, see "Entitlement Capability Implementation" topic in the *Licensing Guide*.

4. Click **Test Connection** to determine if NetWitness Suite connects to the service.
5. When the result is successful, click **Save**.

   The added service is now displayed in the services panel.

   Note: If the test is unsuccessful, edit the service information and retry.

6. Apply license to the Archiver service.

   Refer to the "Synchronize NetWitness Server" topic in the *Licensing Guide* for details on the procedure to activate (apply a license to) the Archiver service.

Add Log Decoder as a Data Source to Archiver

In order to add a Log Decoder as a data source to Archiver, you need to have installed the Archiver host in your network environment, installed and configured a Log Decoder in your network environment, and added the Archiver host to NetWitness Suite and make sure the Archiver service shows as active and licensed.

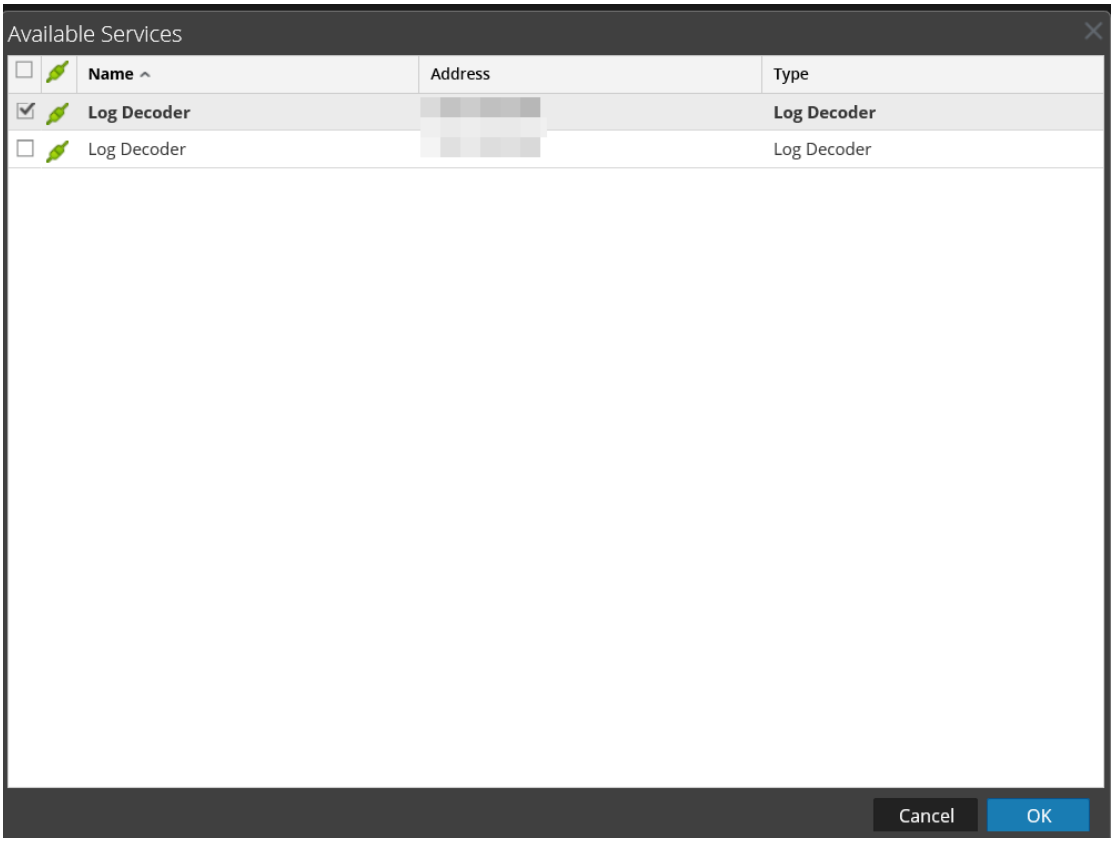
Add Log Decoder as a Data Source to Archiver

To add a Log Decoder as a data source to an Archiver:

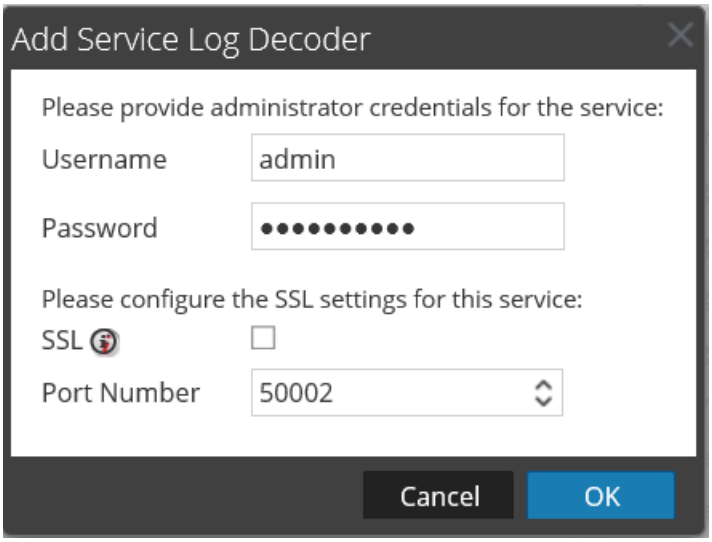
1. Go to **ADMIN > Services**.
2. Select the Archiver service.
3. In the **Actions** column, select **View > Config**.

   The Services Config view of Archiver is displayed.
4. On the **General** tab, in the **Aggregate Services** panel, click .

   The Available Services dialog is displayed.



5. Select the Log Decoder service to add as a data source to the Archiver and click **OK**.
6. If the Log Decoder is using the trust model, an Add Service dialog is displayed.



7. Type the username and password for the Log Decoder, and configure the SSL settings.
8. Click **OK**.
   The selected Log Decoder service is listed in the **Aggregate Services** panel.

Archiver Meta Settings Considerations

To maximize retention time, the meta items and index of the Archiver have been reduced (when compared to the Concentrator) to support common reporting needs. This means that, by default, you may not be able to run all of the reports you run on the Concentrator on the Archiver. You can view a list of the current meta and index items used by the Archiver in the following locations:

- **Explorer view**: The **/archiver/devices/<logdecoder>/config/options** path in the **metaInclude** field shows the current list of meta items.
- **Config view > Files tab**: The **index-archiver.xml** shows the default index configuration. The **index-archiver-custom.xml** shows any modifications.

The meta items and index of the Archiver can be customized to support customer specific reporting needs, however this will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

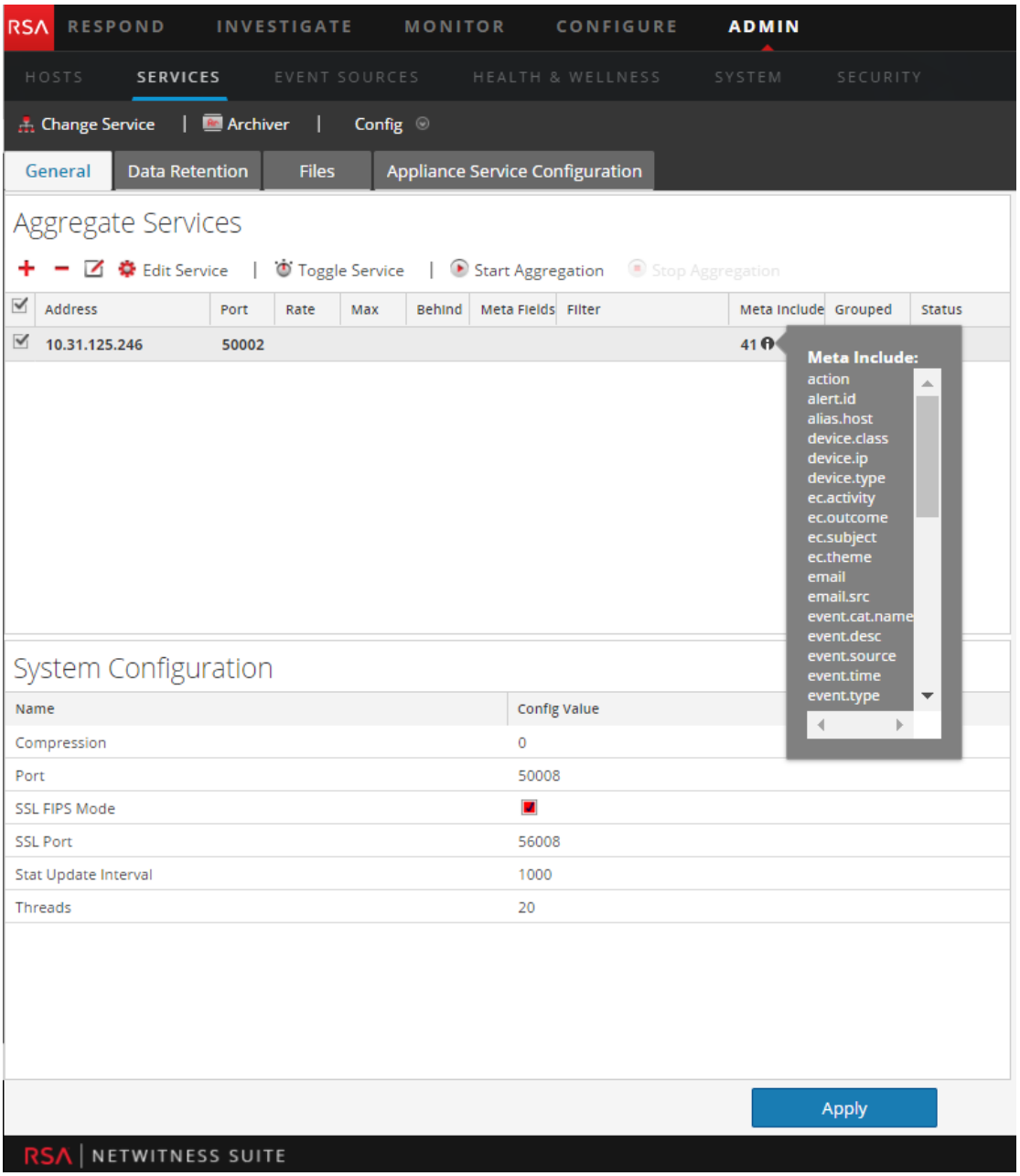
See (Optional) Configure Meta Filters for Aggregation and (Optional) Add Index Entries for Archiver Reporting for additional details.

(Optional) Configure Meta Filters for Aggregation

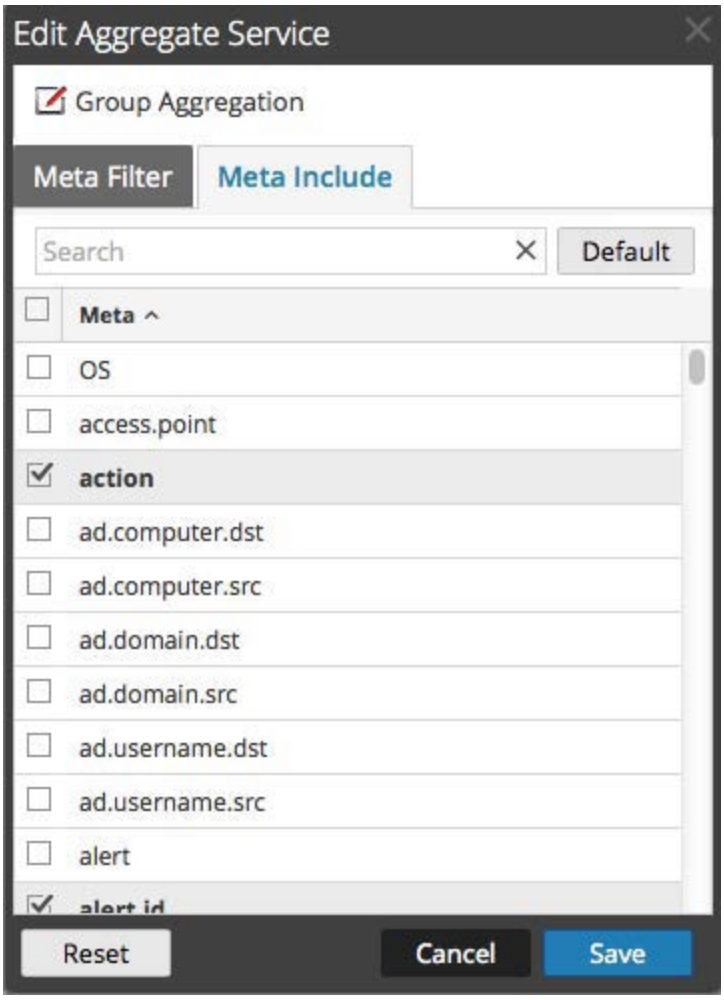
Follow this procedure to view and add additional meta items to the Archiver.

Caution: Adding meta or indexes will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

1. To view the current meta items, in the **Aggregate Services** panel, select the Log Decoder service and click in the **Meta Include** field.



2. To add additional meta items, select the Log Decoder service and click .



3. In the Edit Aggregate Service dialog, select the meta items to include in the Meta Include list. For example, you may want to consider including ip.srcport, tcp.srcport, udp.srcport, msg, url, query, bytes, alias.host, ip.dst, ip.dstport, ip.src, tcp.dstport, megabytes, time, event.desc, and word.
4. Click **Save** and then click **Apply**.
5. See (Optional) Add Index Entries for Archiver Reporting below for information on how to index the additional meta keys.

(Optional) Add Index Entries for Archiver Reporting

Caution: Adding meta or indexes will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

The Archiver's default index configuration only includes value indexes for these keys:

- time
- decoder source (did)
- destination user account (user.dst),
- alert ID (alert.id)
- device IP (device.ip)
- source IP address (ip.src)
- destination IP address (ip.dst)
- event description (event.desc)
- device class (device.class)
- medium
- object name (obj.name)
- word

For information on customizing this list, see "Index Customization" in the *Core Database Tuning Guide*.

Configure Archiver Storage and Log Retention

This topic provides instructions for Administrators to configure storage and log retention on an Archiver.

For compliance reasons, it is often necessary to retain some logs longer than other logs. Some logs are legally sensitive and cannot be retained for a long period of time. Other logs have a requirement to be retained for years. In addition to compliance, some logs are useful for historic forensics and other logs have little to no security or operationally relevant value and can be deleted after a short time.

Because business requirements vary, NetWitness Suite enables you to configure Collections, which are log retention sets for storing log data. For each collection, you can specify how much of the total storage space to use and how many days to retain the logs in the collection. To specify the type of logs to put in the collection, you define retention rules to associate with the collections. Retention rules for all of your collections execute sequentially in an order that you define.

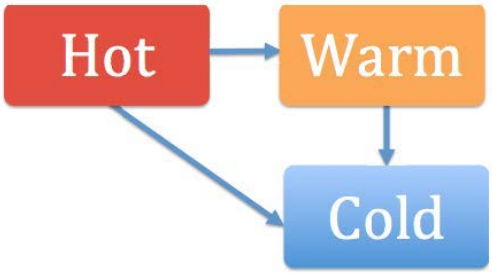
To do this, you must first define the total physical storage space for your collections. NetWitness Suite enables you to define three types of storage:

- **Hot Tier Storage**: This storage contains log data that is in active use as part of the business process. Users can access these logs faster than other types of storage and they can use these logs for reporting and other tasks. Hot storage is usually Direct-Access Capacity (DAC) or SAN storage.
- **Warm Tier Storage**: (Optional) This storage contains older log data aggregated by Archiver. Log data access is slower than hot storage. Users can also use these logs for reporting and other tasks. Warm storage is usually Network Attached Storage (NAS).
- **Cold Tier Storage**: (Optional) This storage contains the oldest log data that is either required for the operation of the business or mandated by regulatory requirements. The logs are offline and Archiver cannot access these logs for reporting or other tasks. However, if you want to access this log data, you can restore it to the collections created on the Archiver service and then use it for reporting. Cold storage is usually offline storage, such as NAS, or temporary storage before archiving to tape. Once data moves to the Cold Tier, that data is no longer managed by Archiver. Once moved, it is incumbent on external processes to back it up or manage that Cold Tier space such that it does not reach 100% capacity. If capacity is reached, this will cause the Archiver to stop aggregation until the problem is fixed.

Archivers are preconfigured to use available hot storage and a default log collection, so you do not have to configure Archiver storage and log retention if you do not have complex log retention requirements.

Logs can move from one type of storage to another in the following ways:

- Hot Storage > Cold Storage
- Hot Storage > Warm Storage > Cold Storage



When a collection reaches its retention limits for hot and warm storage, NetWitness Suite deletes the log data from hot or warm storage. With cold storage configured, a copy goes into cold storage before the logs are deleted from hot or warm storage. For example, if you have a collection with Hot Storage of 1 TB, Warm Storage of 1 TB, and Cold Storage enabled, when the log data reaches 1 TB of hot storage, the oldest log data moves to warm storage. When the log data in warm storage reaches 1 TB, the oldest log data from warm storage is copied to cold storage before it is removed from warm storage.

For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first. For example, if you have a collection with Hot Storage of 1 TB, no Warm or Cold Storage, and a Retention period of 20 days, if the Log data exceeds 1 TB after 11 days, the oldest logs over 1 TB are deleted even though the collection has a 20 day retention period.

After you create hot, warm, and cold storage, you configure your log retention storage collections. You can specify the maximum size of the Hot and Warm Storage for the collection, whether to use Cold Storage, the number of days to retain the logs in the collection, the data compression, and whether to use a hash algorithm to be able to verify the data integrity of the files being saved.

After configuring your collections, you define retention rules for your collection. These rules specify the type of logs to be stored in the collection. Each collection must have at least one retention rule associated with it in order to store log data.

Procedure

Perform the following tasks in the order shown to configure storage and log retention.

Task	Reference
1. Configure total hot, warm, and cold storage.	Refer to Configure Hot, Warm, and Cold Storage.

Task	Reference
2. Configure log retention storage collections.	Refer to Configure Log Storage Collections.
3. Define retention rules for the collections and determine the order of execution of the overall list of retention rules.	Refer to Define Retention Rules.

Configure Hot, Warm, and Cold Storage

This topic provides instructions for Administrators on how to configure total hot, warm, and cold storage on an Archiver.

An Archiver host has hot storage pre-configured to the defaults. Administrators can configure total hot, warm, and cold storage to meet their specific business requirements. An Archiver must have total hot storage configured, but warm and cold storage configurations are optional. NetWitness Suite does not manage cold storage.

Prerequisites

Ensure that you have:

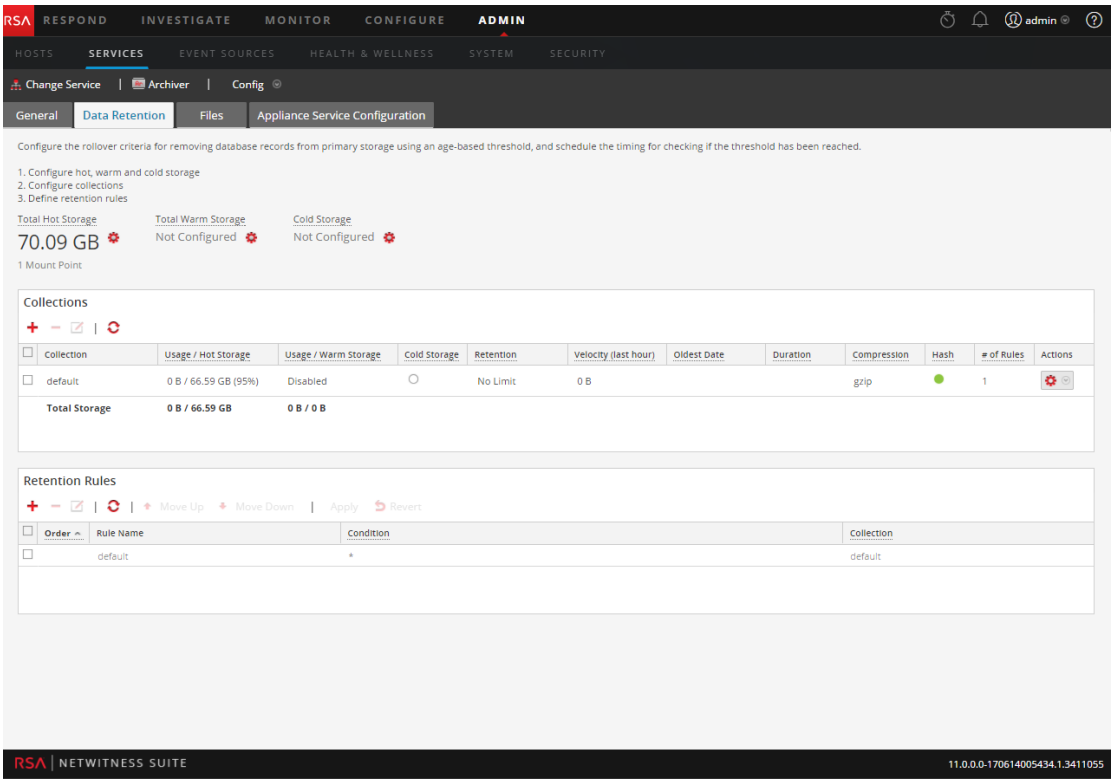
1. Installed the Archiver host in your network environment.
2. Installed and configured Log Decoder in your network environment.
3. Added Archiver as a Core service to your NetWitness Suite deployment.
4. Added Log Decoder services as a data source for Archiver.
5. Installed and configured a DAC or other physical storage in your network environment.
6. Determined your log retention and storage requirements.

Procedures

Configure Total Hot Storage for an Archiver

1. Go to **ADMIN > Services**.
2. Select the Archiver service and **> View > Config**.

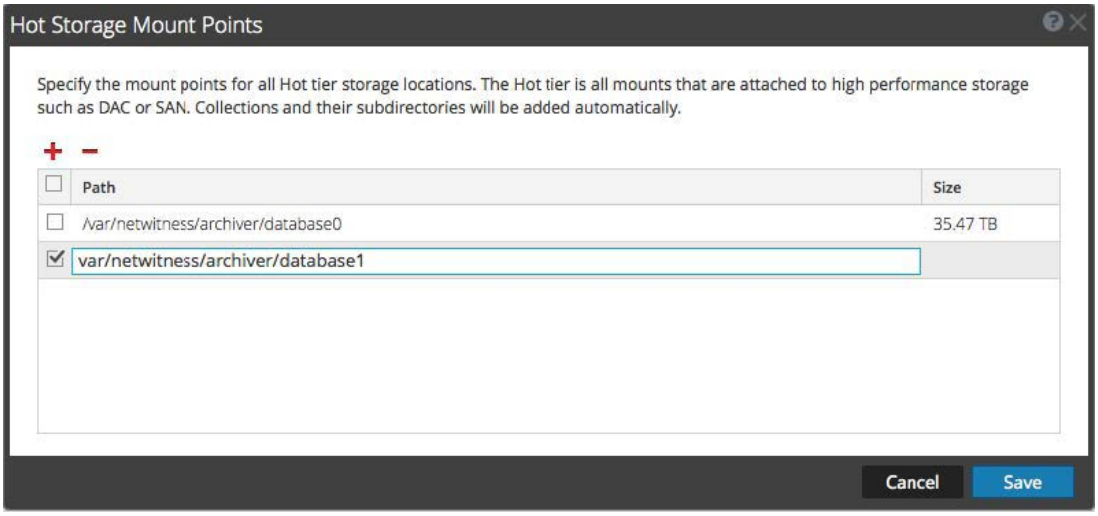
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Total Hot Storage** section, click to configure total hot storage.



4. In the **Hot Storage Mount Points** dialog, add the mount points attached to the Archiver host that you want to include in Total Hot Storage.

   These are the paths to high performance storage, such as DAC storage and SAN. Do not add collections or subdirectories to the mount points.

   To add a mount point, click + and type the path to the mount point.



5. Verify that your mount point paths are correct and click **Save**.

   NetWitness Suite will automatically create metadb, packetdb, sessiondb, and index

directories for each collection defined on the Archiver:
<storageLocation>/<CollectionName>/metadb
<storageLocation>/<CollectionName>/packetdb
<storageLocation>/<CollectionName>/sessiondb
<storageLocation>/<CollectionName>/index

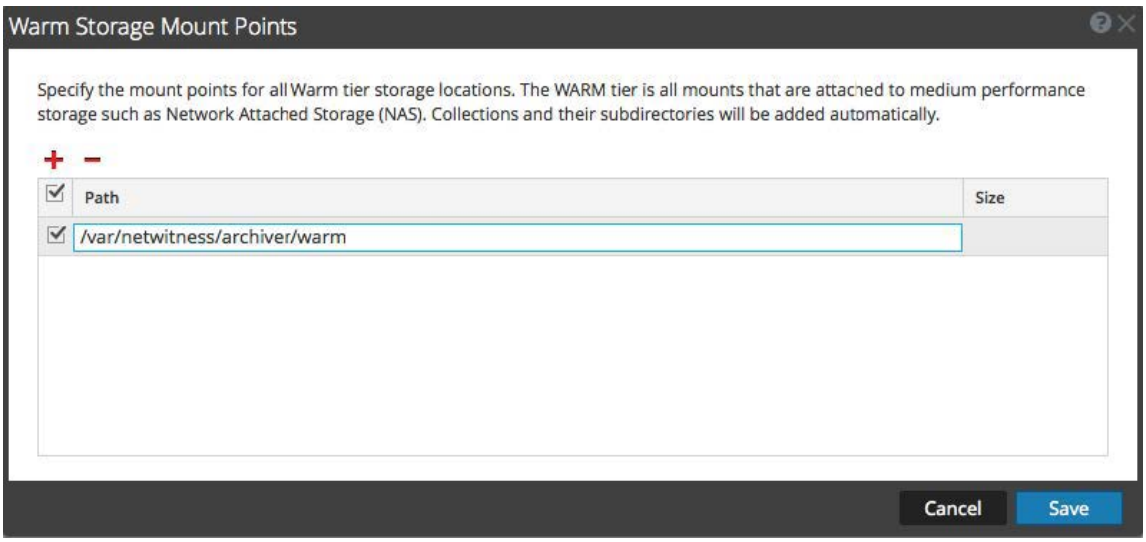
For example, if your mount point is /var/netwitness/archiver, then the following directories will be created for each of your collections:
/var/netwitness/archiver/<CollectionName>/metadb
/var/netwitness/archiver/<CollectionName>/packetdb
/var/netwitness/archiver/<CollectionName>/sessiondb
/var/netwitness/archiver/<CollectionName>/index

After the Archiver service is restarted, data will start being saved to your defined collections. Ensure that your log retention collections are correct before restarting the Archiver service.

Caution: After data has been saved to a mount point, it cannot be removed from the user interface.

Configure Total Warm Storage for an Archiver

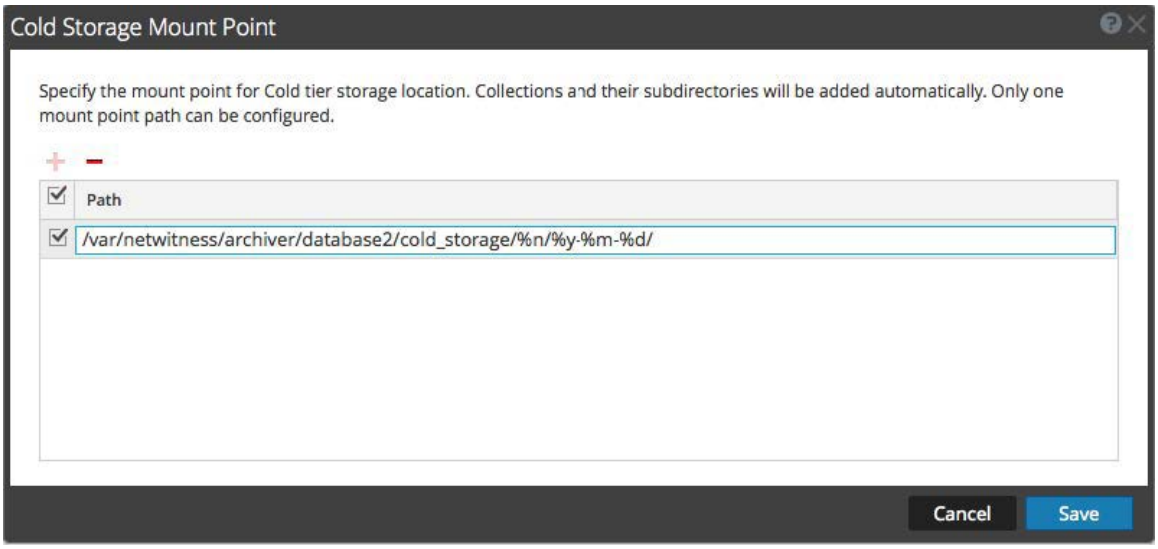
(Optional) The procedure to configure Total Warm Storage for an Archiver is the same as for Total Hot Storage, except that you click in the Total Warm Storage section and add the mount points that you want to use for warm storage, which are the physical paths to warm storage, such as Network Attached Storage (NAS).



Configure Total Cold Storage for an Archiver

(Optional) The procedure to configure Total Cold Storage for an Archiver is the same as for Total Hot Storage, except that you click in the Total Cold Storage section and you add only one mount point for cold storage. NetWitness Suite does not manage cold storage.

You must include the collection name format specifier `%n` somewhere in the cold storage mount point path name to avoid filename collisions between collections.



The following format specifiers are allowed in the path:

Format Specifier	Description
%n	collection name (required)
%y	year the data moved to cold storage
%m	month
%d	day
%h	hour
%##r	block of hours for the current day. For example, if you want three 8 hour blocks, you can set it to %8r. The first 8 hours of the day returns 0, the second 8 hours returns 1, and last 8 hours of the day returns 2.

Changes take effect immediately.

For example, if you have a collection named **compliance** and you create the following cold storage path:

```
/sa-cold-storage/%n/%y-%m-%d/
```

NetWitness Suite creates a directory each day with the following format:

/sa-cold-storage/compliance/2015-11-20/

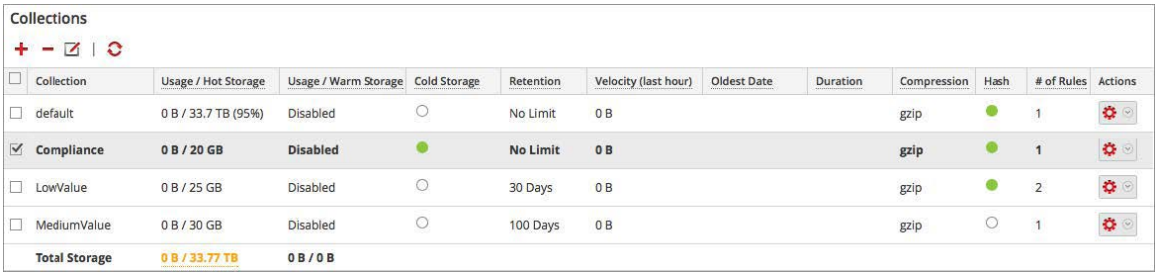
Hot, Warm, and Cold Tier Storage Features

The following table describes features of the Hot, Warm, and Cold Tier Storage dialogs.

Feature	Description
	Adds a mount point.
	Removes a mount point. You cannot delete a mount point that is in use unless you delete the associated collections.
	Select the mount points that you want to include for the Total Hot, Warm, and Cold Storage. You can only select one mount point for Total Cold Storage.
Mount Point	Shows the path to the attached physical storage. For example: **/var/netwitness/archiver/database0**, which is the location of the hot storage DAC. Do not add collections or subdirectories to the mount points. NetWitness Suite will automatically create metadb, packetdb, sessiondb, and index directories for each collection defined on the Archiver: <storageLocation>/<CollectionName>/metadb <storageLocation>/<CollectionName>/packetdb <storageLocation>/<CollectionName>/sessiondb <storageLocation>/<CollectionName>/index For example, if your hot storage mount point is /var/netwitness/archiver, then the following directories will be created for each of your collections: /var/netwitness/archiver/<CollectionName>/metadb /var/netwitness/archiver/<CollectionName>/packetdb /var/netwitness/archiver/<CollectionName>/sessiondb /var/netwitness/archiver/<CollectionName>/index For Cold Storage, you must include the collection name format specifier `%n` somewhere in the cold storage mount point path name to avoid filename collisions between collections.
Storage Size	Shows the size of the attached storage. The Data Retention tab shows the total amount of storage for your reference.

Collections

The Collections section lists all of your storage collections along with Total Storage for Hot and Warm Storage.



Collections Features

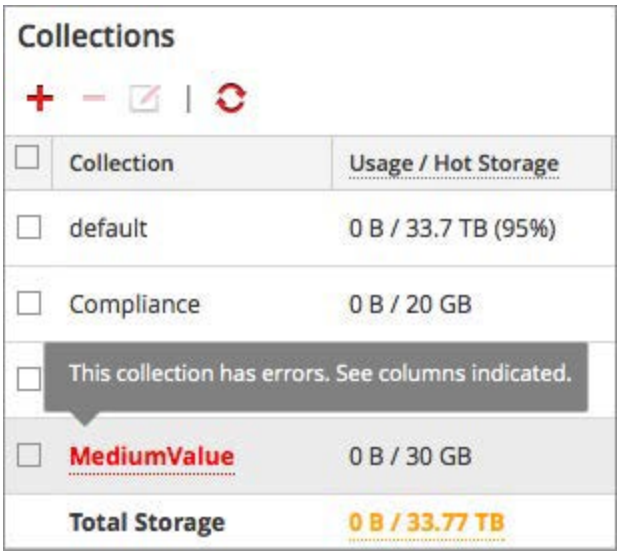
The following table describes the icons and columns of the Collections section. You can hide some of the columns based on your requirements.

Feature	Description
	Opens the Collections dialog, in which you can add a storage collection.
	Removes the selected collection. Deleting the collection permanently removes all stored data from the collection, but the empty data directories remain.
	Opens the Collections dialog, in which you can edit the selected collection.
	Refreshes collection information.
	Selects a collection. For example, you can select a collection for editing or removal.
Collection	Shows the name of your collection, such as Default, Compliance, MediumValue, and LowValue. You can create multiple collections with different criteria for retaining logs. If you do not create any collections, the Default collection is used. If a collection has errors, the collection name and the columns with errors appear in red text.

Feature	Description
Usage / Hot Storage	Shows the current hot storage usage and the maximum hot storage for the collection. When the size of the logs reach the maximum hot storage amount, the logs are removed or they roll to the next available storage tier (warm or cold).
Usage / Warm Storage	Shows the current warm storage usage and the maximum warm storage for the collection. When the size of the logs reach the maximum warm storage amount, the logs are removed or they roll to available cold storage.
Cold Storage	Indicates whether cold storage is enabled or disabled. A solid colored green circle indicates that cold storage is enabled ( ). An blank white circle indicates that cold storage is disabled.
Retention	Shows the number of days that logs are retained before being removed or optionally moved to cold storage. No Limit indicates that log retention is not restricted by a specified number of days. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Velocity (last hour)	Shows the number of logs captured over the last hour.
Oldest Date	Shows the date and time of the last log capture.
Duration	Shows how may days ago that the last log was captured. For example: 20 days.
Compression	Shows the compression type used for the meta and raw data in the collection.
Hash	Shows whether hash is enabled or disabled. When enabled, the hash algorithm is used to ensure the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as data.

Feature	Description
# of Rules	Shows the number of rules applied to the collection. Define at least one rule for each collection. A collection without any associated rules shows a zero in red text as a warning: The collection name also appears in red text, which indicates an error in the collection. **Caution:** If a collection does not have a rule, no logs will ever go into that collection.
Actions	Enables you to see the rules associated with a collection in the Retention Rule section when you select <actions button> **> Select Rules**. In the Retention Rule section, you can change the overall priority of the collection rules.
Total Storage	Shows the current total hot storage usage and the maximum total hot storage at the bottom of the **Usage / Hot Storage** column. It also shows the current total warm storage usage and the maximum total warm storage at the bottom of the **Usage / Warm Storage** column.

Any errors in the collection appear in red text. A dotted underline indicates that a tooltip is available with information about the error.



Collections that have editing disabled (grayed out) also have tooltips that provide information on the problem.

Retention Rules

The Retention Rules section lists all of the retention rules used for your storage collections listed in the order of rule execution.

The following table describes the features of the Retention Rule section.

Feature	Description
	Opens the Rule Definition dialog, in which you can add a retention rule to use in a storage collection.
	Removes the selected retention rule. In order for your log collections to gather and store log data, you must associate them with at least one retention rule.
	Opens the Rule Definition dialog, in which you can edit the selected retention rule.
	Refreshes retention rule information.
Move Up	Moves the selected retention rule up in the Retention Rule priority list. Retention Rule order is very important. NetWitness Suite evaluates the the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section. You can also use drag and drop to reorder retention rules.
Move Down	Moves the selected retention rule down in the Retention Rule priority list. Retention Rule order is very important. NetWitness Suite executes the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section.
Apply	Saves the rule order change.
Revert	Reverts the rule order change.
	Selects or shows a selected retention rule.
Order	Shows the order of a rule in the overall list of retention rules.

Feature	Description
Rule Name	Shows the name of rule, such as ComplianceDevices and GeneralWindowsLogs.
Condition	Shows the conditions for the rule. These conditions specify the type of logs to include in the collection. Define Retention Rules presents the guidelines for all queries and rule conditions in Core services.
Collection	Shows Collection name and how many days that the collection is retained. For example: MediumValue (30 Days)

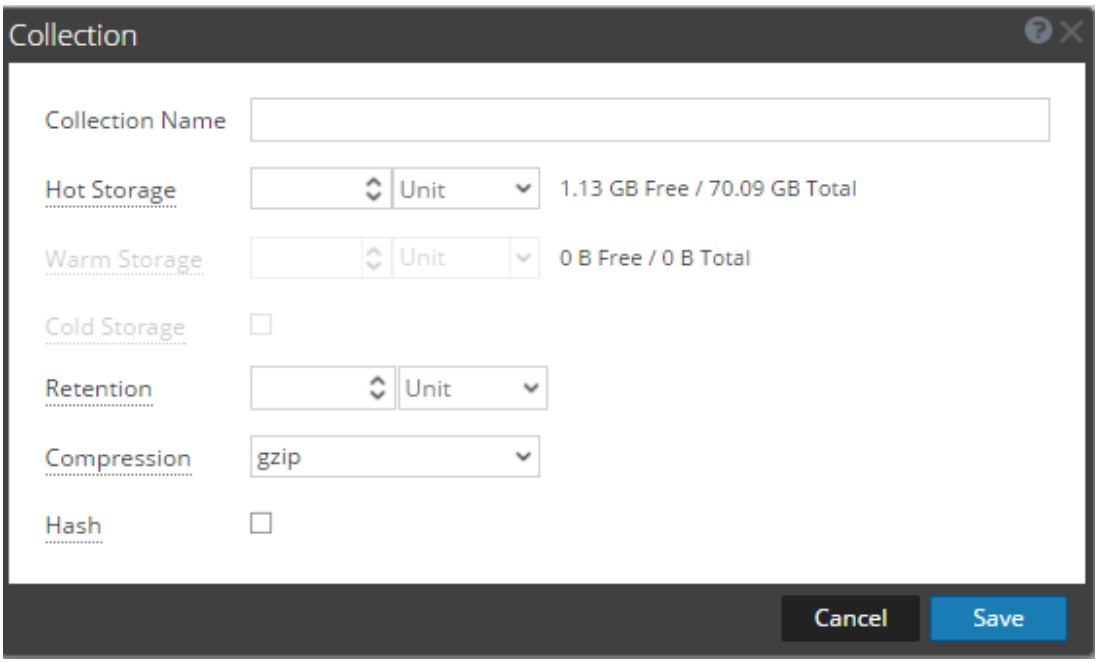
Collection Dialog

On the ADMIN > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Collection dialog, which is accessible from the Collections section, you can define individual storage collections to use for different log types. For example, you may want to create collections for compliance reasons or to selectively retain critical logs.

Procedures related to this dialog box are described in Configure Archiver Storage and Log Retention and Configure Log Storage Collections.

To access the Collection dialog:

1. Select **ADMIN > Services**.
2. Select an Archiver service and **>View > Config**.
3. In the Services Config view for the service, click the **Data Retention** tab.
4. In the **Collections** section, click to add or edit the rule.
   The Collection dialog is displayed.



The following table describes the fields in the Collection dialog.

Field	Description
Collection Name	Specify a name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage are shown next to this field. When the size of the logs reach the maximum hot storage size, the logs are removed or they roll to the next available storage tier (warm or cold).
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage are shown next to this field. When the size of the logs reach the maximum warm storage size, the logs are removed or they roll to available cold storage.

Field	Description
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside of the specified size and retention limits roll over to cold storage. If you do not use cold storage, logs outside of the specified size and retention limits are removed.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as

Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

Rule Definition Dialog

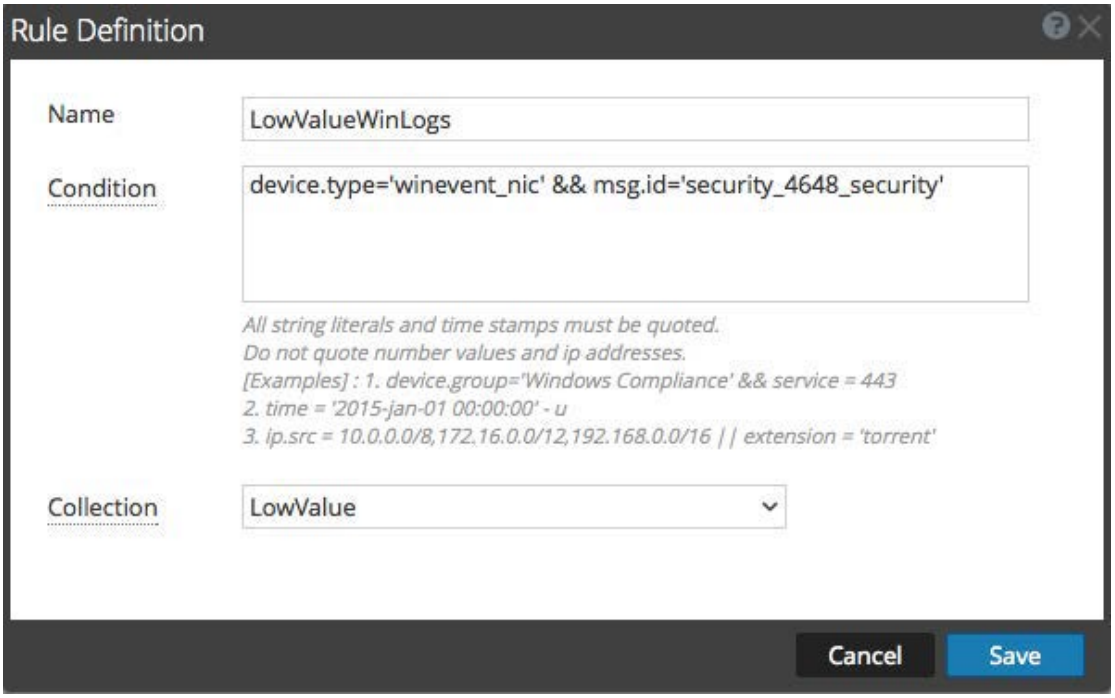
In the ADMIN > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Rule Definition dialog, which is accessible from the Retention Rules section, you can define retention rules to use for your storage collections.

Procedures related to this dialog box are described in Configure Archiver Storage and Log Retention and .Define Retention Rules

To access the Rule Definition dialog:

1. Select **ADMIN > Services**.
2. Select an Archiver service and **>View > Config**.
3. In the Services Config view for the service, click the **Data Retention** tab.
4. In the **Retention Rule** section, click + or ✎.

   The Rule Definition dialog is displayed.



The following table describes fields in the Rule Definition dialog.

Field	Description
Name	Specify a unique name for your retention rule. For example: ComplianceDevices
Condition	Specify the conditions for the type of logs that you want to include in the collection. All sting literals and time stamps must be quoted. Do not quote number values and IP addresses. For example: device.group='PCI Devices' || device.group='HIPPA Devices'
Collection	Select the collection on which you want to apply this rule. For example: Compliance

Next Step

Configure log storage collections.

Configure Log Storage Collections

This topic provides instructions for Administrators on how to configure log storage collections on an Archiver.

NetWitness Suite enables you to define individual storage collections for different log types. You can specify the maximum size of the Hot and Warm Storage space used by the collection, whether to use offline storage (Cold Storage), the number of days to retain the logs in the collection, the data compression, and whether to use a hash algorithm to be able to verify the data integrity of the files being saved. You should create collections based on your log retention storage requirements. Each collection that you create must be associated with at least one retention rule.

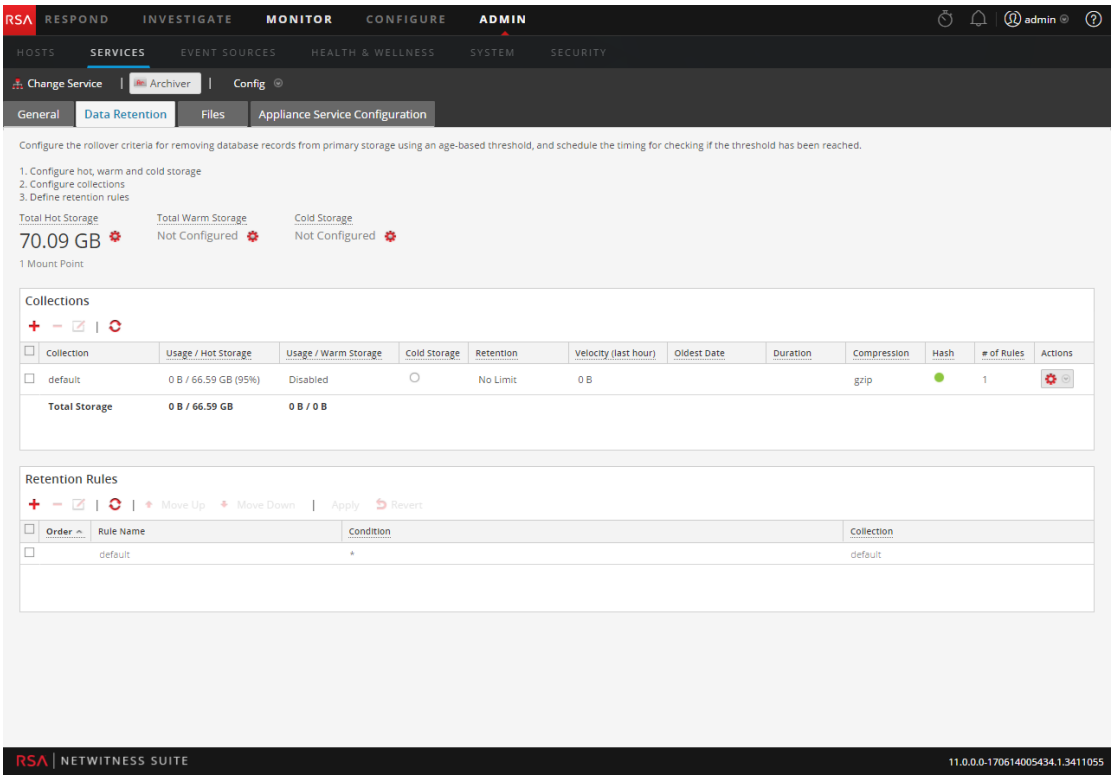
Prerequisites

Before you configure your log retention storage collections, configure total hot, warm, and cold storage.

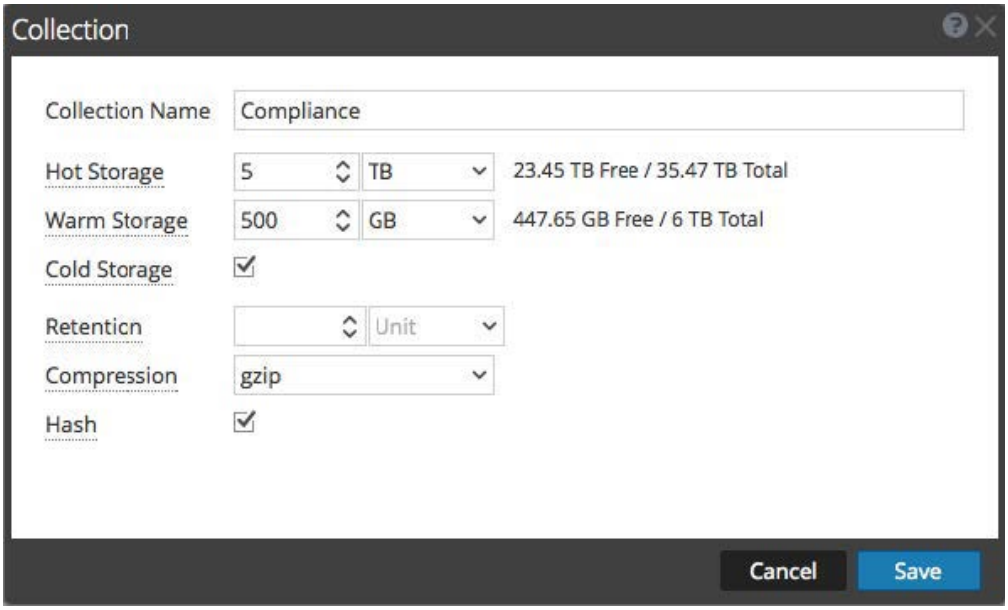
Configure a Log Storage Collection

To configure a log retention storage collection on an Archiver:

1. Go to **ADMIN > Services**.
2. Select the Archiver service and **> View > Config**.
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Collections** section, click to add a collection.
   (If you decide to make changes to an existing collection, you can select the collection and click to change the settings.)



The **Collection** dialog is displayed.



4. Configure the collection as described in the following table.

Field	Description
Collection Name	Specify a unique name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage is shown next to this field.
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage is shown next to this field.
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside the storage limits are copied to cold storage before they are deleted from hot or warm storage.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as data.

5. Click **Save**.
   Any errors in the collection appear in red text. A dotted underline indicates that a tooltip is available with information about the error. Your collection name appears in red text until at least one retention rule is defined for your collection.

If you have a collection with editing disabled (grayed out), look at the associated tooltip for more information.

Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

Next Step

Define retention rules for your collections.

Define Retention Rules

Administrators can define and order retention rules for log storage collections on an Archiver. Retention rules specify the type of logs to be stored in the collection. For your log collections to gather and store log data, you must associate them with at least one retention rule. When you configure a retention rule, you specify a condition and a collection for that rule. The condition (rule definition) determines the type of logs stored in that collection.

For the condition, you can use anything that works in a regular query `where` clause.

For example, to get logs from compliance services, you can use the following condition:

```
device.group='PCI Devices' || device.group='HIPPA Devices'
```

After you define the retention rules for your collections, it is important that you specify the order of your retention rules. NetWitness Suite evaluates the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section of the Data Retention tab of the Archiver (**ADMIN > Services Config view**).

Caution: Rule order is very important. It determines the priority for evaluating the log data for storage retention.

Prerequisites

Before you configure your retention rules:

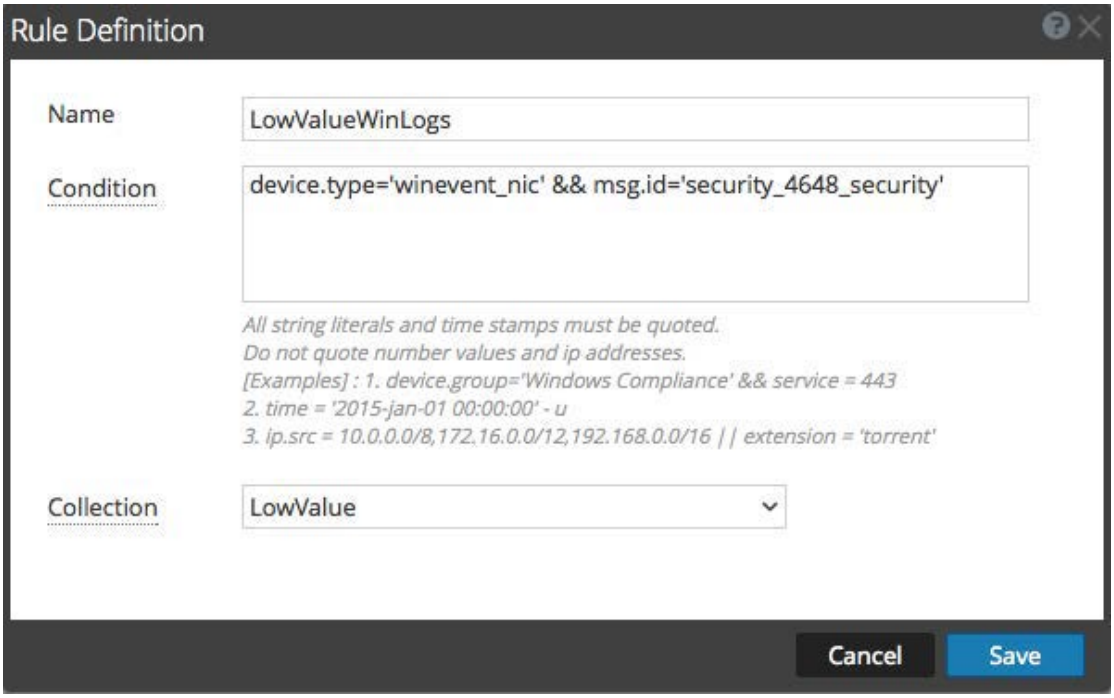
- Configure total hot, warm, and cold storage
- Configure log storage collections

Procedures

Define a Retention Rule for a Collection

1. Go to **ADMIN > Services**.
2. Select the Archiver service and **> View > Config**.
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Retention Rule** section, click .

The **Rule Definition** dialog is displayed.



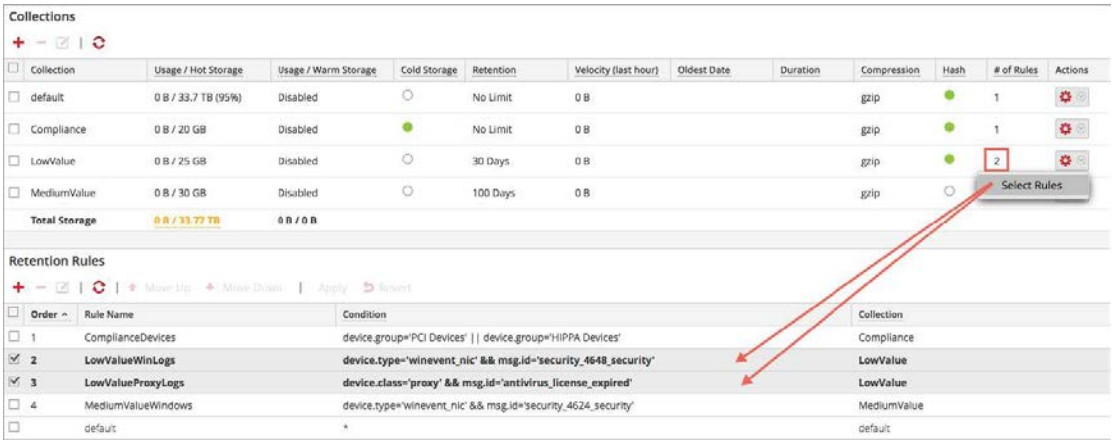
4. Configure the fields in the Rule Definition dialog as described in the following table:

Field	Description
Rule Name	Specify a unique name for your retention rule. It cannot include spaces. For example: LowValueWinLogs
Condition	Specify the conditions for the type of logs that you want to include in the collection. All string literals and time stamps must be quoted. Do not quote number values and IP addresses. For example: `device.type='winevent_nic' && msg.id='security_4648_security'`
Collection	Select the collection on which you want to apply this rule. For example: LowValue.

5. Click **Save**.

The retention rule that you define becomes associated with the collection you selected. On the **Data Retention** tab, in the **Collections** section, you can click > **Select Rules** in

the **Actions** column for the selected collection to view the retention rules associated with the collection in the **Retention Rule** section.



Specify the Order of your Retention Rules

To prioritize the complete list of all of your retention rules:

1. In the **Retention Rule** section of the **Data Retention** tab, select a retention rule and use drag and drop (or select **Move Up** and **Move Down**) to change its order in the priority list.

2. Click **Apply** to save the order of the retention rules.

Caution: Rule order is very important. It determines the priority for evaluating the log data for storage retention.

Next Step

Add Archiver as a Data Source to Reporting Engine.

Add Archiver as a Data Source to Reporting Engine

This topic provides instructions on how to add Archiver Archiver as a data source to Reporting Engine to generate reports for the data collected by Archiver.

Prerequisites

Ensure that you have:

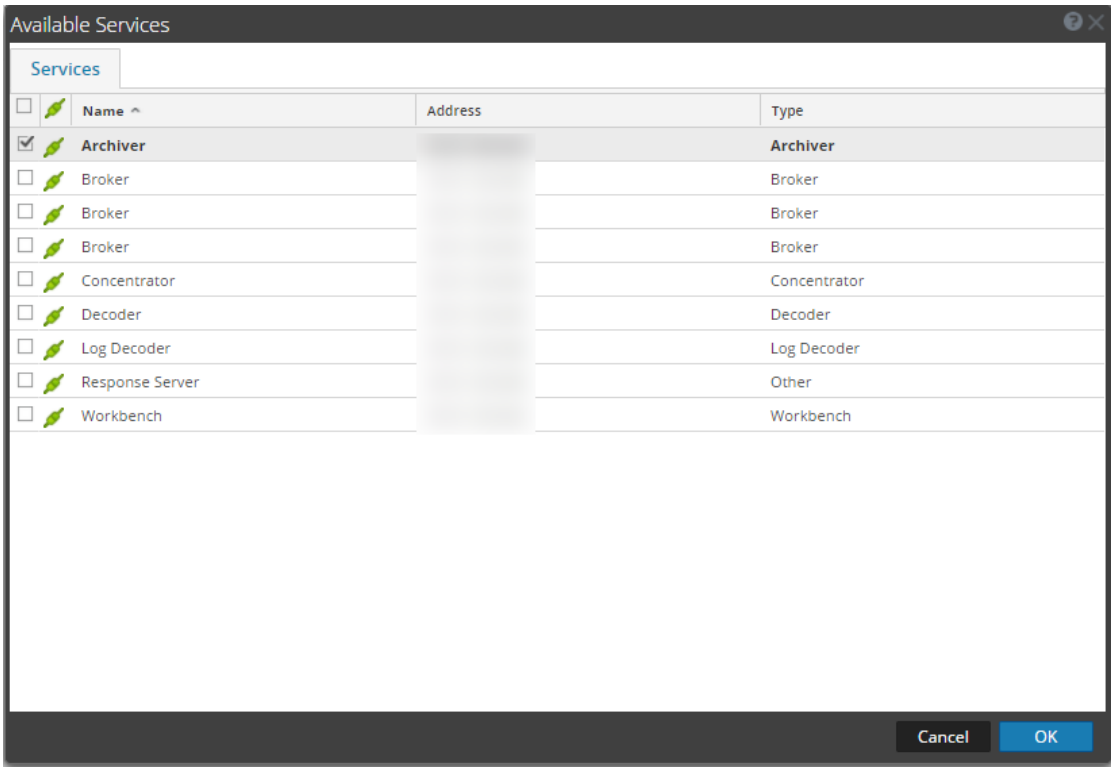
1. Installed the Archiver host in your network environment.
2. Installed and configured a Log Decoder Decoder in your network environment.
3. Verified that Reporting Engine and Archiver services are active.

Procedure

To associate an Archiver data source with Reporting Engine:

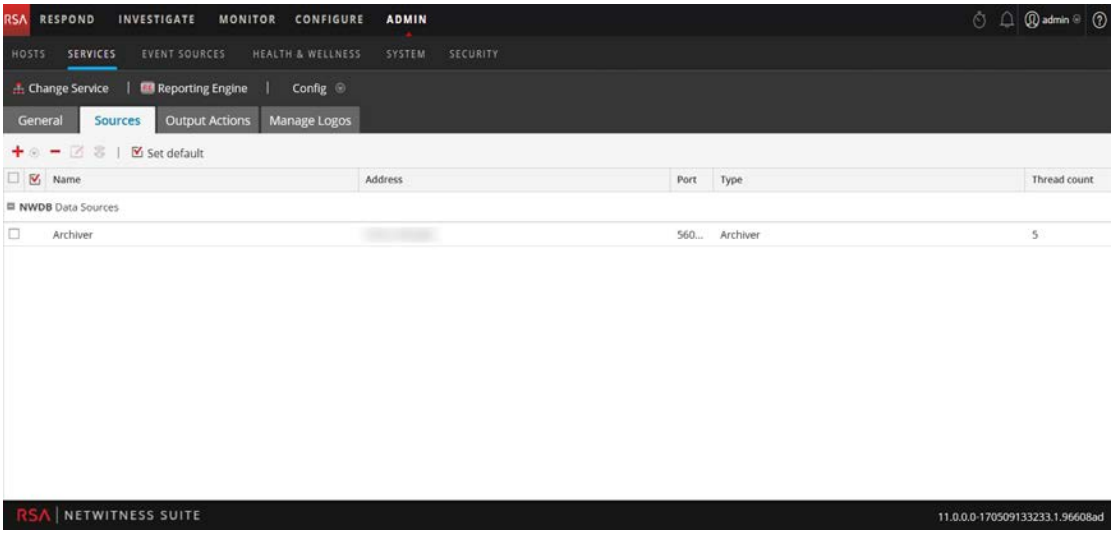
1. Go to **ADMIN > Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. In the **Actions** column, select **View > Config**.
4. Select the **Sources** tab.
5. Click + and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Archiver that you want to add as data source to the Reporting Engine and click **OK**.
7. In the Service Information dialog, type the username and password for the Archiver.
8. Click **OK**.

   The selected Archiver is listed in the NWDB Data Sources category.



You can now create reports on the data collected by Archiver.

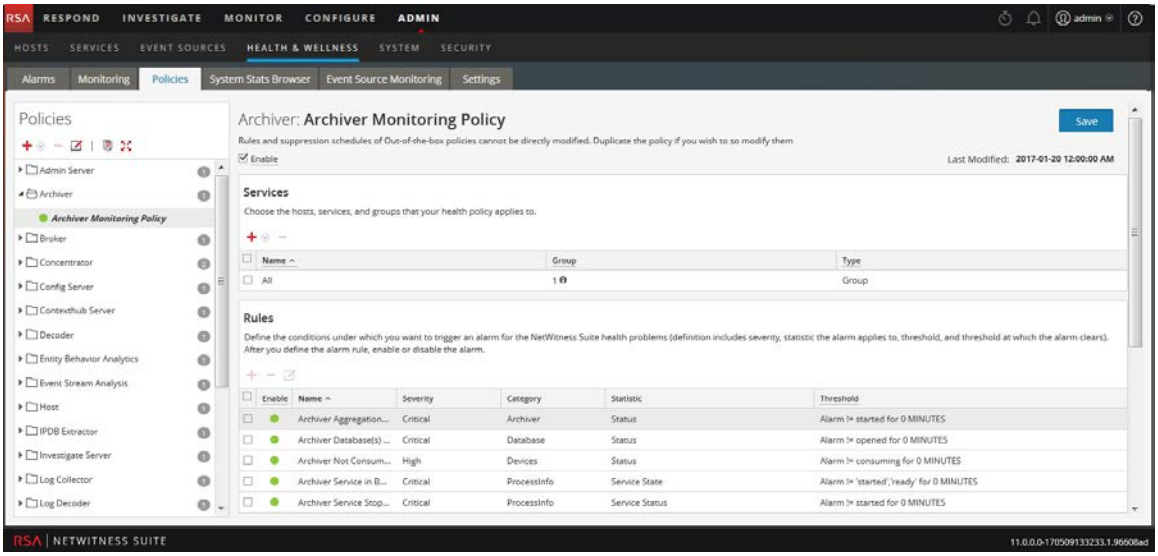
Next Step

Configure alerts for archive storage.

Configure Archiver Monitoring

Health & Wellness enables you to automatically generate notifications when critical thresholds are met.

Review the Health & Wellness policies for Archiver and Host in the Health & Wellness Policies section. Make updates as required.



For detailed information, see **Manage Policies** in the *System Maintenance* guide.

Additional Archiver Configuration

This topic is a collection of individual procedures, which an Administrator may perform at any time and they are not required to complete the initial setup of Archiver. These procedures are presented in alphabetical order.

Use this section when you are looking for instructions to perform a specific task after the initial setup of Archiver.

Topics

- Configuring Data Backup and Restore
- Retrieve Hash Information

Configuring Data Backup and Restore

This topic provides information on the Data Backup and Restore feature for an Archiver. You can use this feature to back up Archiver data and retrieve the backed up data.

You can back up the data in the following ways:

- Use scripts to copy files from cold storage backup folders onto an offline storage.
- Use backup software to copy files from cold storage backup folders onto an offline storage.
- Run EMC Networker or other backup software on Archiver and have it do daily incremental backup of the database files.

Note: For details on the procedure to back up data using Networker, see the *Administration Guide for Networker*.

Once you have the data backup, you have to perform the following tasks to restore the backed up data that is installed on the Archiver.

Action	Description
1. Restore your data to a location accessible by the Archiver.	Refer to Create Collection
2. Create a collection in Archiver that uses that location.	Refer to "Manage Collections" topic in the *Workbench Configuration Guide*.
3. Add the Archiver service as a data source on Reporting Engine to generate reports for the data restored on the Archiver service.	Refer to Add Archiver as a Data Source to Reporting Engine

Add Archiver Service

The NetWitness Suite Archiver service enables you to create collections with restored data from Archiver offline (cold) storage. This procedure is only required if you do not have the Archiver service installed.

Prerequisites

Make sure you have added an Archiver host and applied a license to it.

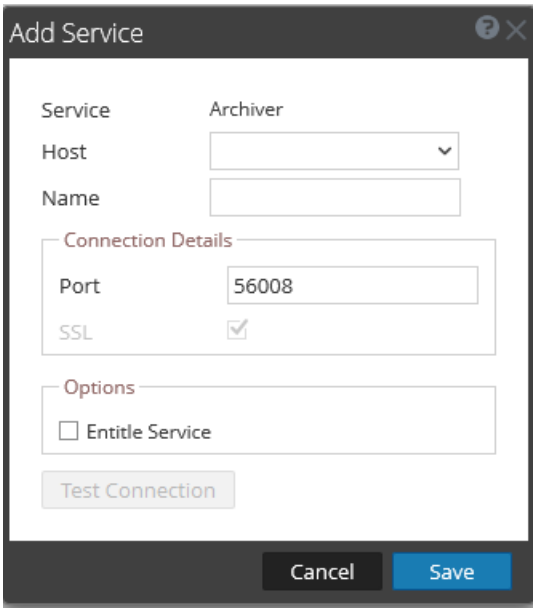
Procedure

Note: This procedure is only required if you do not have Archiver service installed.

Perform the following steps to add the Archiver service:

1. Go to **ADMIN > Services**.
2. In the **Services** panel, select + **>Archiver**.

   The Add Service dialog is displayed, as shown below.



3. Provide the following details.

Field	Description
Host	Select an Archiver host from the drop-down menu.
Name	Type a name for the service.
Port	Default port is 50007.
SSL	Select **SSL** if you want NetWitness Suite to communicate with the service using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. **Note:** If you select SSL, ensure SSL is enabled in the System Configuration panel.
Username	(Optional) Type the username for the service.
Password	(Optional) Type the password for the service.

4. Click **Test Connection** to determine if NetWitness Suite connects to the service.
5. When the result is successful, click **Save**.
   The added service is now displayed in the Services panel.

Note: If the test is unsuccessful, edit the service information and retry.

Create Collection

This topic provides information on how to create a collection on an Archiver service.

You can create a collection using data restored from the backed-up data or an existing subset of data. When you recover the backed-up data, you have to place it in the collection folder created on the Archiver service to enable you to generate the required reports for the retrieved data. For example, if you have backed up the data using EMC Networker at <*location*>, you can use the restore options in Networker to restore the backed-up data to the collection folder created on the Archiver service. For restore procedure using EMC Networker, see the *Administration Guide for Networker*.

Prerequisites

Ensure that you have:

- Archiver service installed on an Archiver host.
- Ensure the Archiverservice has enough space to hold the collection.

- The backed-up data placed in a known location on your local host, if you are creating a collection using the data restored from the backed-up data.

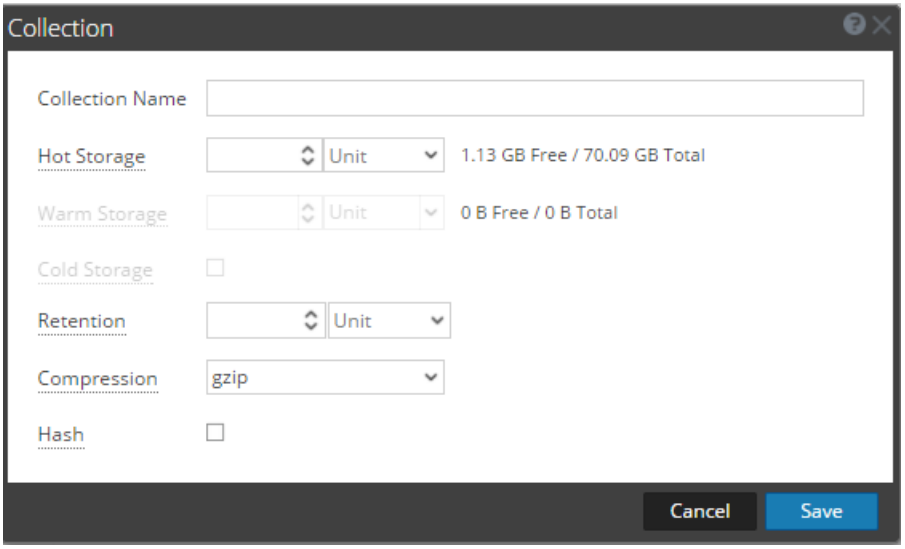
Procedure

The Data Retentions tab enables Administrators to restore and save data that is restored from a backup or from an existing set of data.

Note: The Administrator can point the source path to the location of the database files and the restore command copies them to the Archiver. The Administrator needs to mount those directories to the Archiver before a restoration collection can be created.

To create a collection using data restored from the backed-up data or existing subset of data:

1. Go to **ADMIN > Services > Archiver**.
2. From the **Services** grid, select **>View > Config**.
   The **General** tab is displayed.
3. Select the **Data Retentions** tab and click in the **Collections** panel to add a collection.
   The **Collection** dialog is displayed.



5. Provide the following information:
   - **Collection Name:** Name of the Archiver collection that you want to restore.
   - **Hot Storage:**Enter the number of Archiver database files and unit size (either Gigabytes or Terabytes) that have been moved from cold storage.
   - **Retention:** Select the number of days or hours that you want to store the collection.
   - **Compression:** Select the compression type for the collection.

6. Click **Save** to restore the collection.

   Note: Target is the location where the collection is created.

   Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:
   "The source path does not exist '/xxx/xxx/'."
   If there is insufficient storage to restore your collection, the following error is displayed:
   "Error during disk space checking. Insufficient disk space in location '/xxx/xxx'."

   The Schedule Job dialog is displayed with the following message:
   "Restoring data into a new collection. Check the jobs page for progress."

7. Click **Jobs** icon in the top right area of the main menu to expand the list of restoration collection jobs with their current status.

Note: When restoring a collection, the larger the dataset that you have to restore, the longer the restoration will take. If you are restoring a collection containing hundreds of gigabytes or more, restoration may take several hours.

Add Archiver Service as a Data Source to Reporting Engine

This topic provides instructions on how to add the Archiver service as a data source to Reporting Engine to generate reports for the data restored onto the Archiver.

Prerequisites

Ensure that you have:

- Installed the Archiver service on the Archiver host.
- Added a collection on the Archiver service.

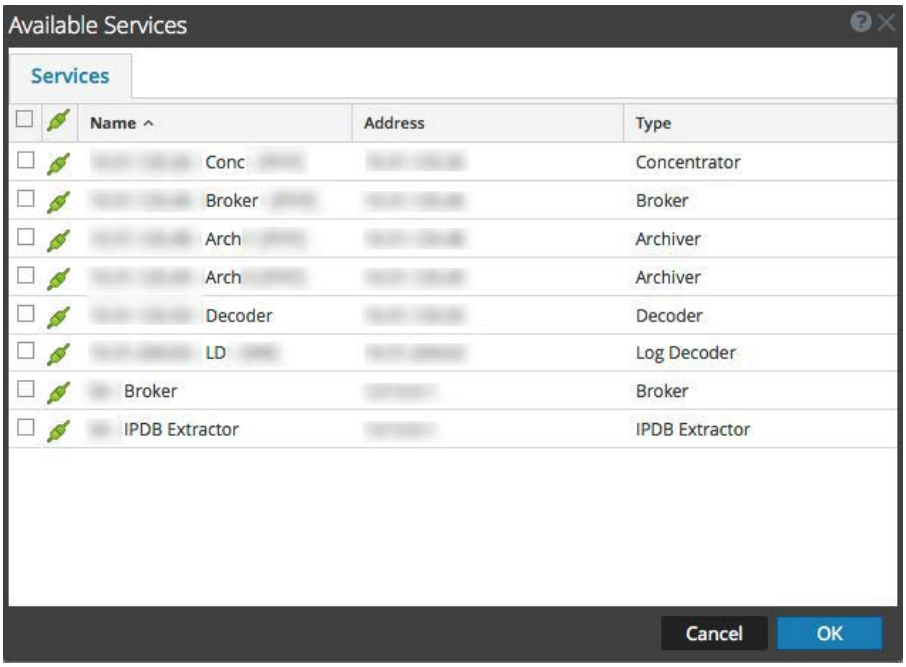
Procedure

Perform the following steps to add the Archiver service as a data source to Reporting Engine:

1. Select **ADMIN > Services**.
2. In the **Services** panel, select a Reporting Engine service.
3. In the **Actions** column, select **View > Config**.
4. Select the **Sources** tab.

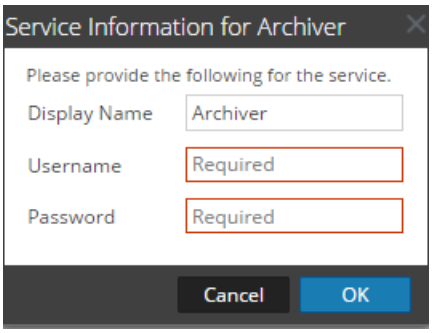
5. Click + and select **Available Services**.

   The Available Services dialog is displayed.



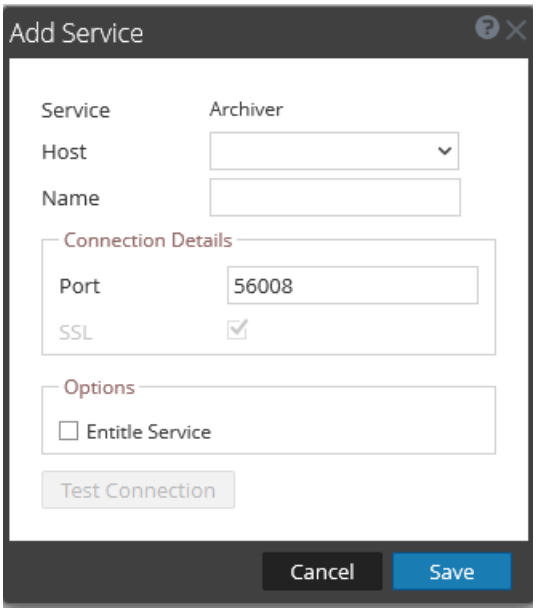
6. Select the Archiver service and click **OK**.

   If the Archiver service is using a Trust Model, the Service Information dialog for the selected service is displayed with the username and password fields required. If the service is not using a Trust Model, these fields will be optional.



7. Type the username and password for admin credentials for the service.

8. Click **OK**.
   The Add Service dialog is displayed.



9. Select a host from the drop-down list and click **Save**.
   The Archiver service is now added as a data source to the Reporting Engine and is listed in the NWDB Data Sources list.

Note: This procedure has to be performed for each collection.

An Administrator can create and delete Workbench collections. and view Workbench statistics and logs. This topic provides all of these procedures and an example procedure for restoring a collection for Reporting and Investigation.

- Mount Archiver Directories
- Create a Collection
- Delete a Collection
- Investigate a Collection
- View Workbench Collection Statistics
- View Workbench Logs

Mount Archiver Directories

If data is in offline storage or cold-tier storage, you need to mount the Archiver directories in order to restore the data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select an **Archiver** from the Services grid and select **> View > Explore**.
   The Explorer view for the Archiver is displayed
3. Right-click on the **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
4. Run the **manifest** command for a time range, for example, 2015-April-01 to 2015-April-10.
   The search returns all files that need to be restored for the selected query.

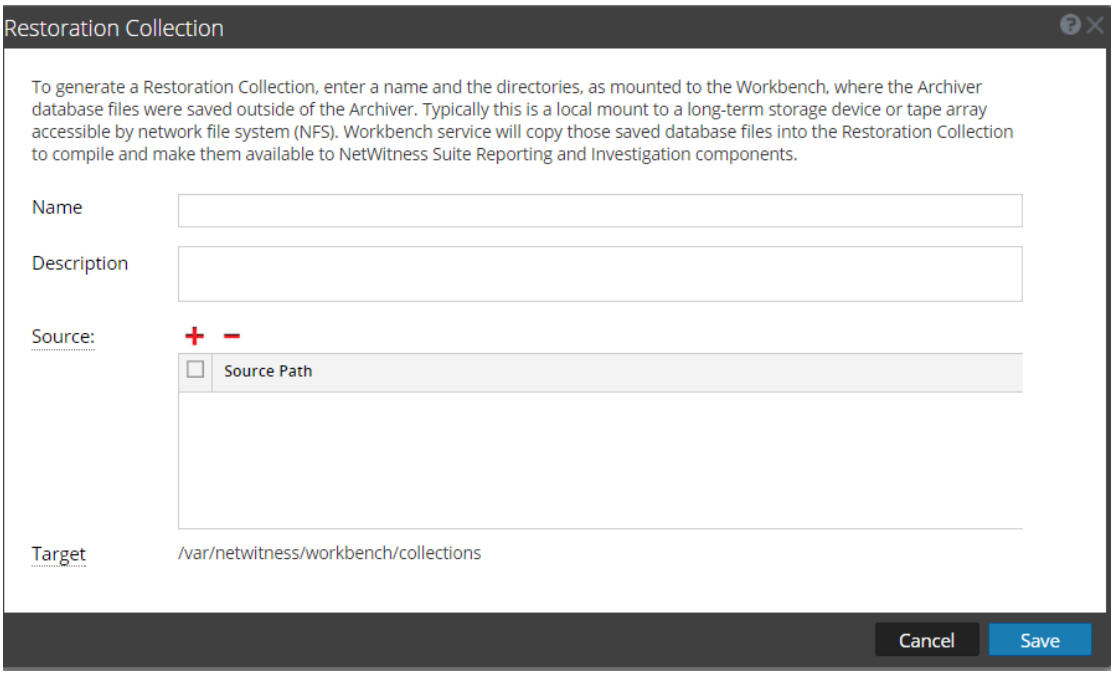
Create a Collection

Administrators can create collections of restored data from a backup or from an existing set of data.

Note: You can point the source path to the location of the database files and the restore command copies them to the Archiver. You need to mount those directories to the Archiver (where the Workbench is installed) before a restoration collection can be created.

To create a collection using data restored from the backed up data or existing subset of data:

1. Go to **ADMIN> Services.**
2. In the Services view, select a **Workbench**, then select **> View > Config**.
   The Services Config view is displayed with the General tab open.
3. Click the **Collections** tab.
   The Collections grid is displayed.
4. Click in the toolbar.
   The Restoration Collection dialog is displayed.



5. Provide the following information:
   - **Name:** Name of the Workbench collection that you want to restore.
   - **Source:** Location where the Archiver database files have been moved from cold storage.

   Note: Target is the location where the collection is created.

6. Click **Save** to restore the collection.

   Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:
   `The source path does not exist '/xxx/xxx/'.`

   If there is insufficient storage to restore your collection, the following error is displayed:
   `Error during disk space checking. Insufficient disk space in location '/xxx/xxx'.`

   The Schedule Job dialog is displayed with the following message:
   `Restoring data into a new collection. Check the jobs page for progress.`

7. Click the **Jobs** icon in the NetWitness Suite toolbar to expand the list of restoration collection jobs with their current status.

Note: Restoring a collection that is larger than 550 GB may take several hours to process.

Delete a Collection

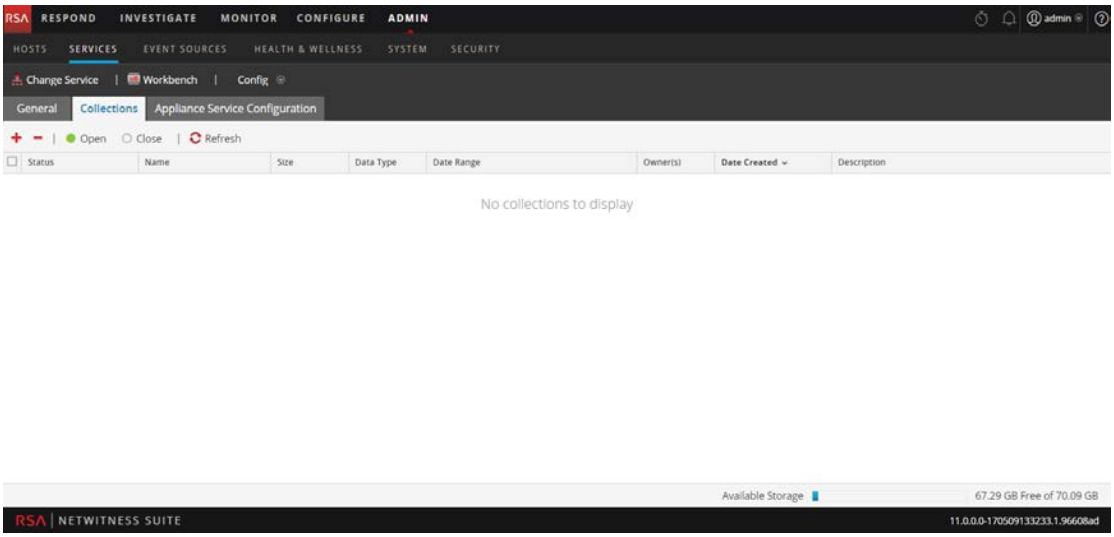
Administrators can delete collections from the Workbench service.

Perform the following steps to delete a collection:

1. Go to **ADMIN > Services.**
2. From the Services view, select a **Workbench** and click **> View > Config**.

   The Services Config view opens with the General tab displayed.
3. Select the **Collections** tab.

   The Collections grid is displayed.



4. In the Collections grid, select the collection that you want to delete.
5. Click from the toolbar.

   A warning dialog requests confirmation.
6. If you want to delete the collection, click **Yes**.

   The collection is removed from the Workbench service.

Example Procedure: How to Restore a Collection for Reporting and Investigation

The following steps illustrate how to restore data for reporting and investigation purposes that is in offline storage or cold-tier storage. In the following example, data is restored for the time range beginning on 2015-April-01 through 2015-April-10.

To restore data for reporting and investigation purposes:

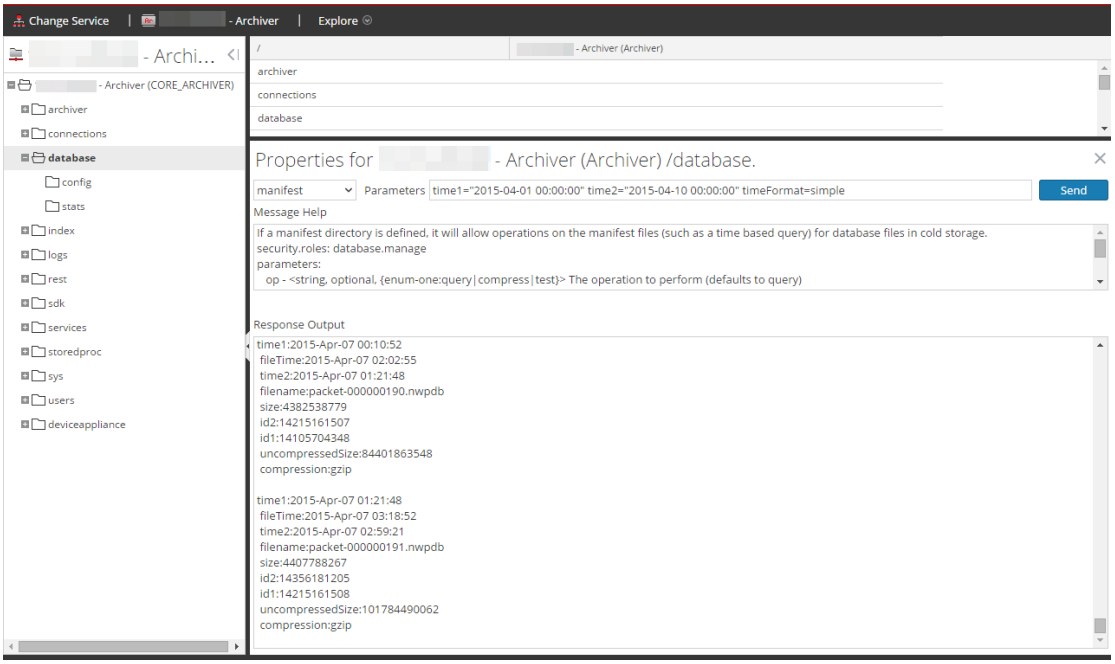
1. Go to **ADMIN > Services**.
2. Select the **Archiver**from the Services grid.
3. Navigate to the Explorer view of the Archiver appliance by selecting **> View > Explore**.

   The Explorer view for Archiver is displayed
4. Right click on **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
5. Run the **manifest** command for the selected time range 2015-April-01 to 2015-April-10.

   The search returns all files that need to be restored for your selected query.

   Example Search:

   ```
   time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
   timeFormat=simple
   ```



6. Go to **ADMIN > Services**.
7. In the Services view, select a **Archiver**, then select **> View > Config**.

   The Services Config view is displayed with the General tab open.
8. Select the **Collections tab.**
9. Create a restoration collection with the source path pointing to files listed in the manifest command output.

10. Save the collection.
    After successfully creating a collection, you can use this collection for reporting and investigation purposes.

Investigate a Collection

To perform an investigation on an Archiver collection:

1. Select **Investigate**.
   The Investigate dialog is displayed.
2. Click the **Collections** tab in the Investigate dialog.
3. Select an Archiver service in the left panel.
4. Select the collection you want to investigate in the right panel.
5. Click **Navigate**.

The Navigate view is displayed showing data pertaining to the Archiver collection that you selected.

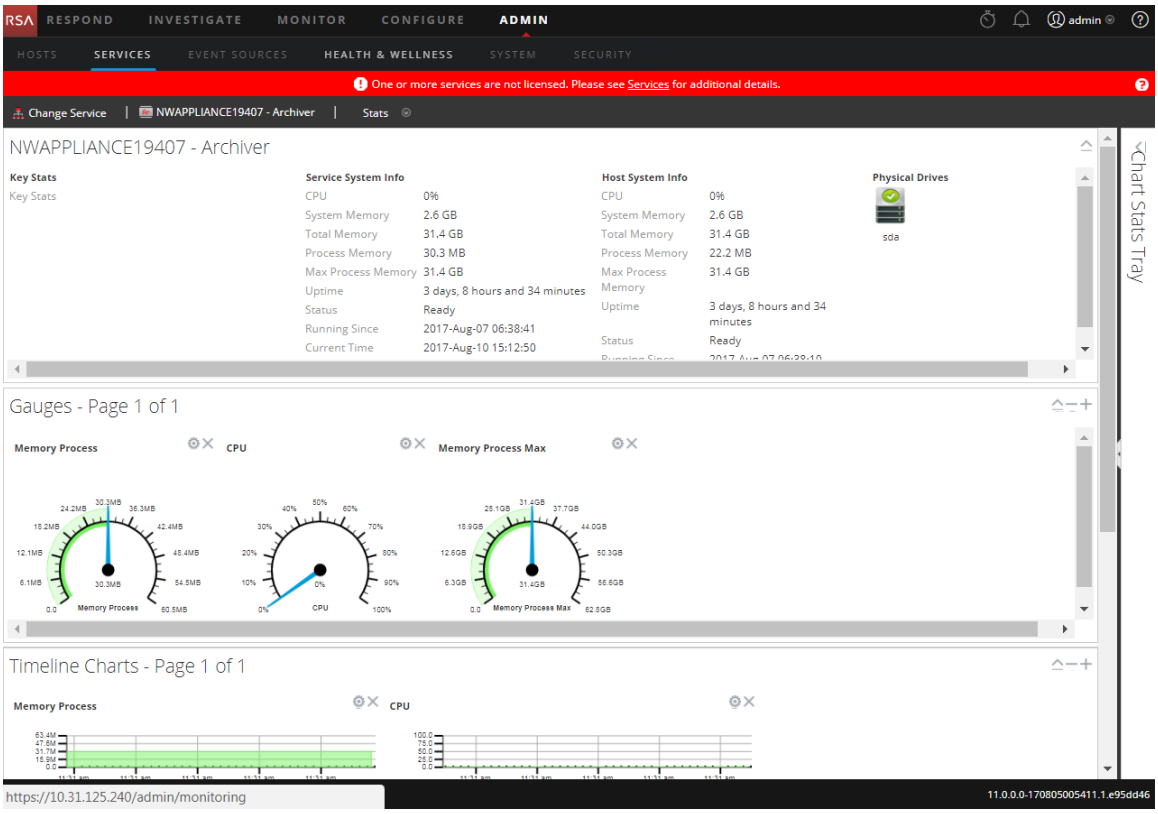
Note: For detailed information about using Investigation, see the *Investigation and Malware Analysis Guide*..

View Archiver Collection Statistics

The same statistics available for other services are provided for the Archiver service. The Services Stats view displays key statistics and system information that pertain to your selected Archiver service. The information is displayed in several different sections within the Stats view: Archiver, Gauges, Timeline Charts and Chart Stats Tray. The Chart Stats Tray lists all available statistics for the Archiver. Any statistic in the Chart Stats Tray can be displayed in a gouge or a timeline chart.

Perform the following steps to view Archiver statistics:

1. Go to **ADMIN > Services**.
2. In the Services view, select an Archiver, then select **> View > Stats**.
   The Services Stats view is displayed.



Note: For more information about Archiver statistics, see the *Host and Services Getting Started Guide*.

View Archiver Logs

Perform the following steps to view logs on an Archiver service:

1. Go to **ADMIN > Services.**
2. In the Services view, select a **Archiver**, then select **> View > Logs**.
   The Services Logs grid is displayed.

Note: For information about viewing and configuring audit logs, see "Configure Global Audit Logging" topic in the *System Configuration Guide* .

Add Archiver Service as a Data Source to Broker

Adding the Archiver service as a data source to Broker is useful when you have more than one collection and you want a report on the archived data. To do this, you can add more than one collection as a downstream service to a Broker and then generate a report on it.

Prerequisites

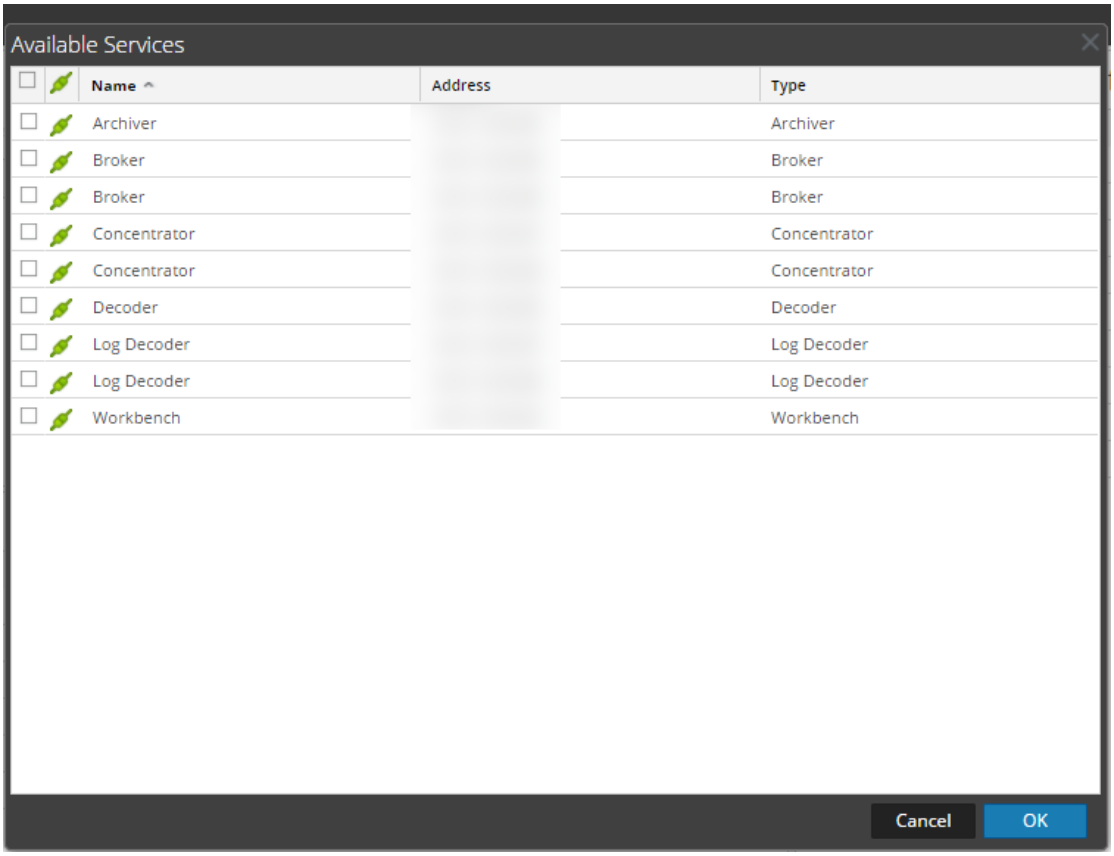
Ensure that you have:

- Installed the Archiver service on the Archiver host.
- Added a collection on the Archiver service.

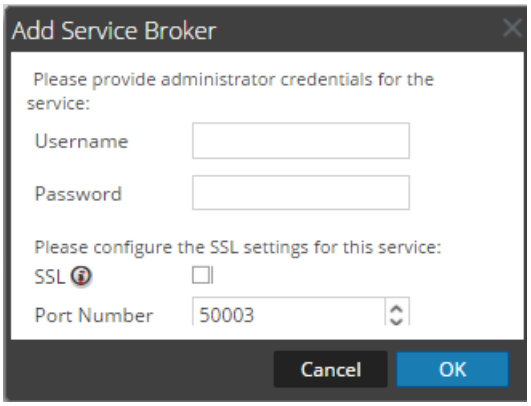
Procedure

To add an Archiver service as a data source on the Broker:

1. Select **ADMIN > Services**.
2. In the **Services** panel, select a Broker service.
3. In the **Actions** column, select > **View** > **Config**.
   The Config view is displayed with the General tab open.
4. In the **Aggregate Services** section, click +.
   The Available Services dialog is displayed.

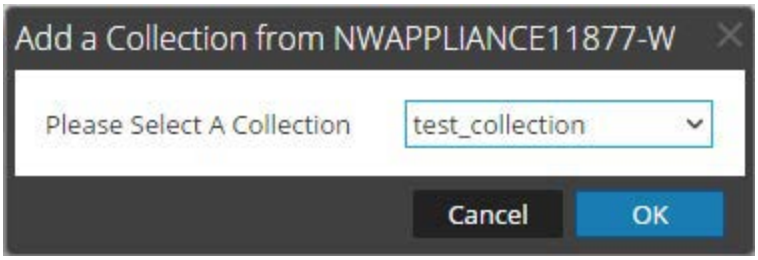


6. Select the Broker service and click **OK**.
7. If the Archiver service is using a Trust Model, a Service Information dialog for the selected service is displayed.



8. Type the username and password for admin credentials for the service.
9. Click **OK**.

   The Add Collection dialog is displayed.



10. Select a collection from the drop-down list and click **OK**.

    The Archiver service is now added as a data source to the Broker.

Note: This procedure has to be performed for each collection.

Retrieve Hash Information

Archiver provides a command, **hashInfo**, which you can use to retrieve the hash information for each session, meta, and packet database that meets the session list or date range criteria. The hash information retrieved is in the form of a list of string parameters, each string parameter corresponding to the hash information for a single database file. You can retrieve the hash information of the database files using the Archiver Service Explore view or REST interface of the Archiver service. The hash information thus retrieved is used to compare the database files in the original location and the exported location to validate data integrity.

The following table lists the criteria that you can use to retrieve the hash files from the database.

Criteria	Description
sessions	You can retrieve the hash information of the database files by specifying the sessions that exist or read from the session database to determine the associated meta and packet id required to determine which meta and packet database files are needed to retrieve the hash information. **For example:** sessions=100 - Retrieves the hash information of all database files that contain the constituent components(session, meta, content) of session 100. sessions=100,500000 - Retrieves the hash information of all database files that contain the constituent components(session, meta, content) of session 100 and 500000
beginDate	You can specify a begin date as a filter against the database files. This finds the hash information for the files created after the specified date. The begin date specified has to be in the format YYYY-MM-DD HH:MM:SS.
endDate	You can specify an end date as a filter against the database files. This finds the hash information for the files created before the specified date. The end date specified has to be in the format YYYY-MM-DD HH:MM:SS **For example:** beginDate: “2014-Mar-25 05:52:00” endDate=”2014-Mar-27 05:52:00” – Retrieves the hash information of all the database files in between March 25, 2014 and March 27, 2014 in the specified time range on those days.

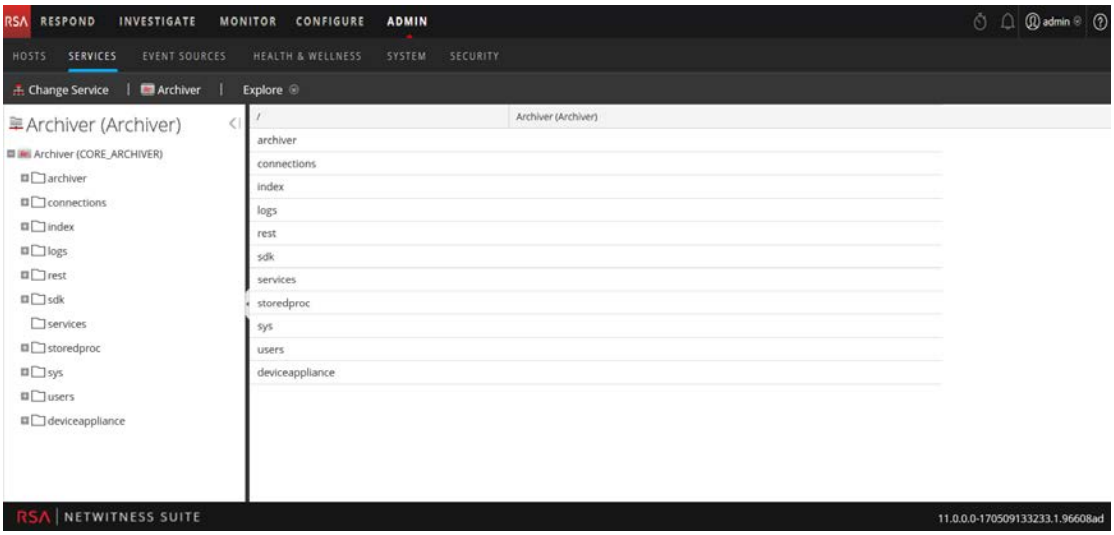
Criteria	Description
directories	By default, the hash information files are stored with the database files they were created for. You can also store the hash information file in different location by defining multiple locations in the hash.dir configuration parameter. You can define the location as a filter and retrieve the hash information files for the configured location. **For example:** directories="/home/hash" – Retrieves the hash information of the database files from the location /home/hash

Procedure

To retrieve hash information of the database files:

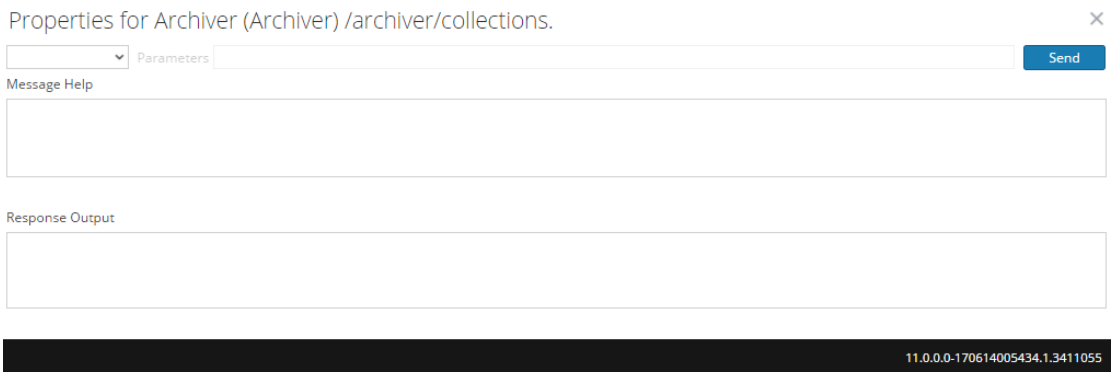
1. Select **ADMIN > Services**.
2. Select an Archiver service.
3. In the **Actions** column, select **View > Explore**.

   The Explore view of the Archiver service is displayed.



4. In the node tree, right-click on **archiver** and select **Properties**.

   The Properties dialog is displayed.



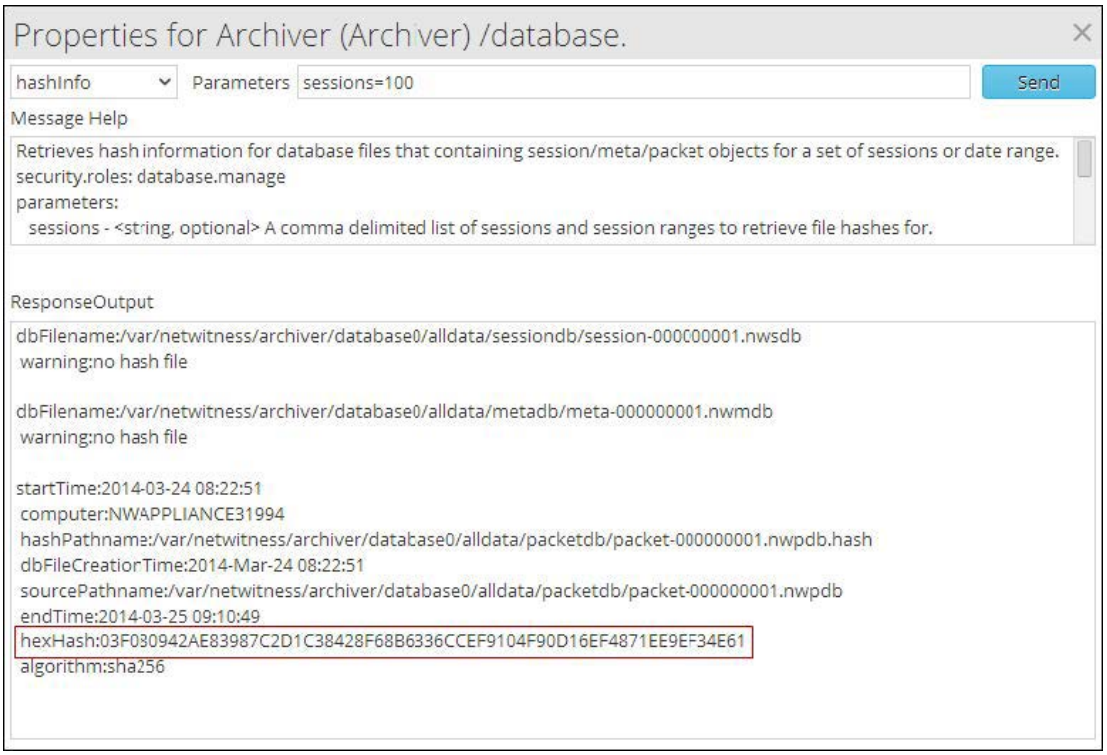
5. In the drop-down menu, select **hashInfo**.
6. In the **Parameters** field, type the criteria that you want to use to retrieve the hash information from the database.
7. Click **Send**.

   The output of the command is displayed in the ReponseOutput textbox. In the output, the hash information is shown in the hexHash parameter. You can use this hash information to verify data integrity manually.

Examples

Retrieve the hash information of the database files for the sessions that exist.
Criteria: sessions=100

Output

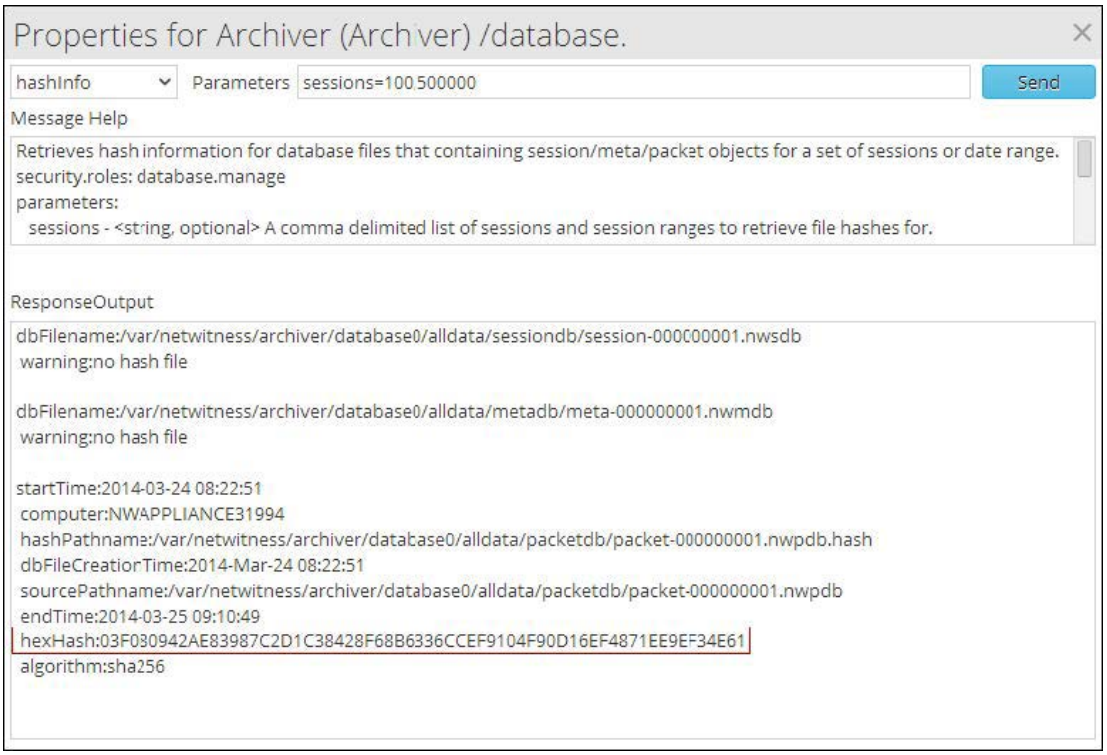


The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for session 100.

Retrieve the hash information of the database files for the session ranges that exist.

Criteria: sessions=100,500000

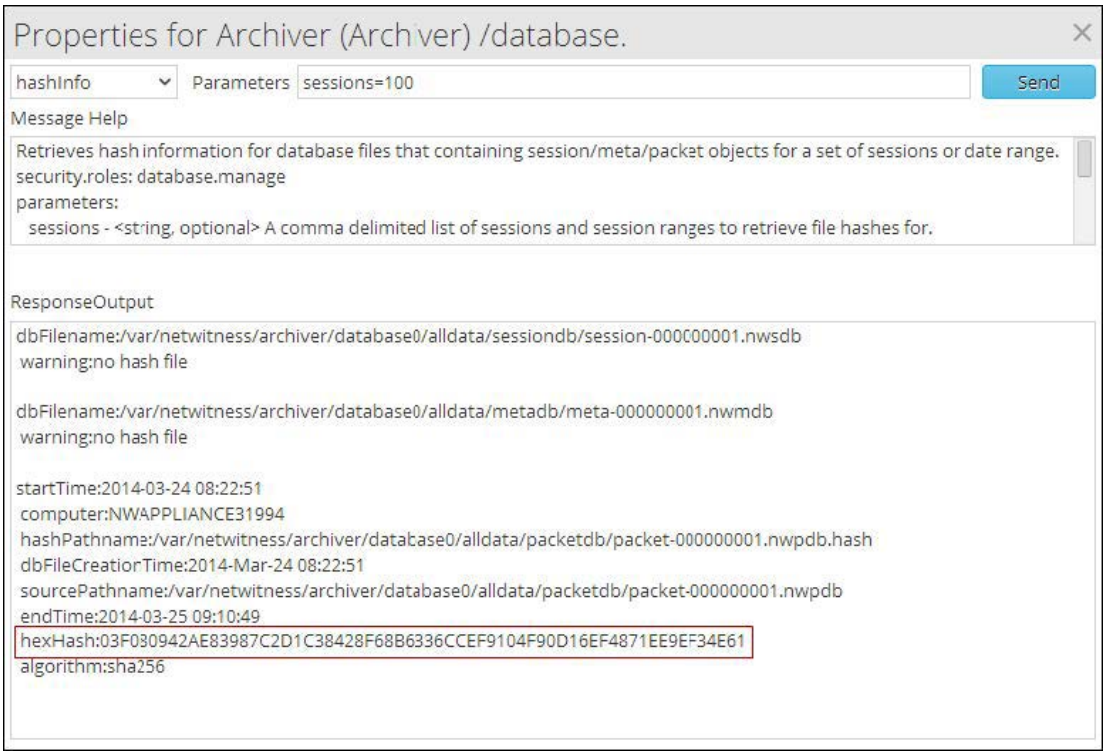
Output



The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for session range 100 - 500000

Retrieve the hash information of the database files created in the specified date range
Criteria: beginDate="2017-Mar-25 05:52:15" endDate="2017-Mar-27 05:52:15"

Output



The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for the date range specified.

References

This topic is a collection of references, which describe the user interface for Archiver in NetWitness Suite.

Topics

- Archiver Collection Dialog
- Archiver Service Configuration
- Data Retention Tab - Archiver
- Archiver Services Config View - General Tab
- Services Config View - Archiver

Archiver Collection Dialog

On the ADMIN > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Collection dialog, which is accessible from the Collections section, you can define individual storage collections to use for different log types. For example, you may want to create collections for compliance reasons or to selectively retain critical logs.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.

What do you want to do?

Role	I want to...	Show me how...
Administrator	Add an Archiver service	Add the Archiver Service
Administrator	Add a Log Decoderas a source to the Archiver	Add Log Decoder as a Data Source to Archiver
Administrator	*Configure Archiver Storage and Log Retention	Configure Archiver Storage and Log Retention
Administrator	Add an Archiver as a Data Source to the Reporting Engine	Add Archiver as a Data Source to Reporting Engine
Administrator	Configure Archiver Monitoring	Configure Archiver Monitoring

*You can perform this task here.

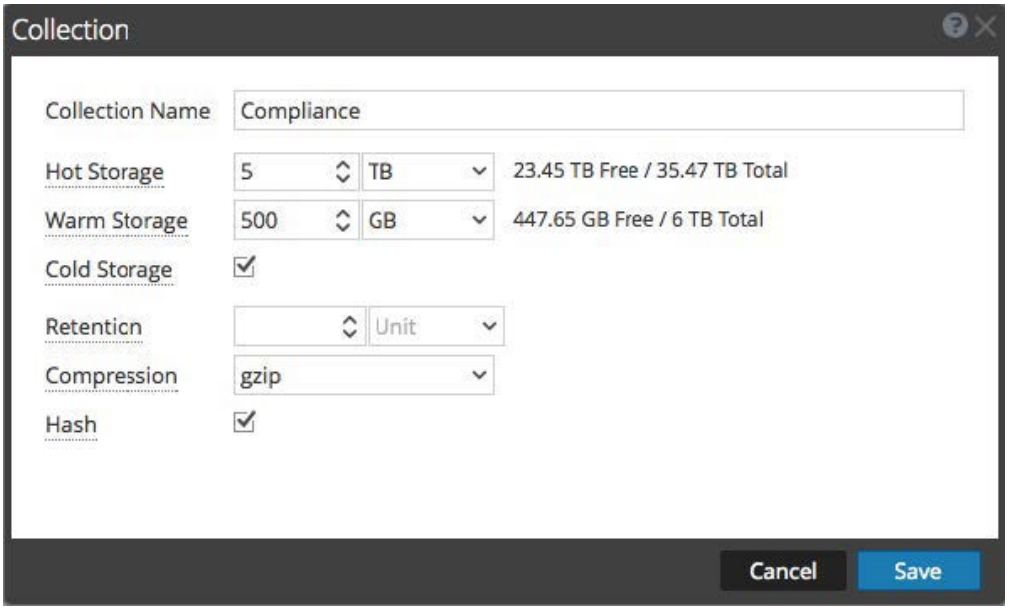
Related Topics

Configuring an Archiver

Quick Look

To access the Collection dialog:

1. Go to **ADMIN > Services.**
2. Select an Archiver service and > View > Config.
3. In the Services Config view for the service, click the Data Retention tab.
4. In the Collections section, click +.
   The Collection dialog is displayed.



Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

The following table describes the fields in the Collection Dialog.

Field	Description
Collection Name	Specify a name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage are shown next to this field. When the size of the logs reach the maximum hot storage size, the logs are removed or they roll to the next available storage tier (warm or cold).

Field	Description
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage are shown next to this field. When the size of the logs reach the maximum warm storage size, the logs are removed or they roll to available cold storage.
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside of the specified size and retention limits roll over to cold storage. If you do not use cold storage, logs outside of the specified size and retention limits are removed.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved.

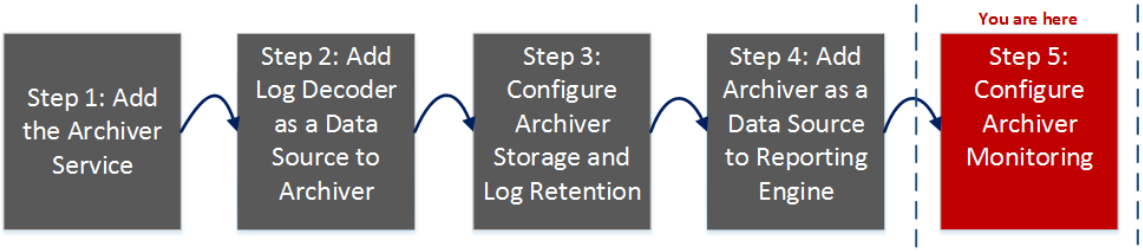
Archiver Services Config View - General Tab

The General tab for an Archiver in the Services Config view helps manage basic service configuration, configure the aggregate service, and configure the aggregation process between an Archiver and the aggregate service.

To access the General tab, go to ADMIN > Services, select an Archiver service, then select View > Config.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.



Configuring the aggregate service (whose data is consumed and aggregated) includes:

- Adding, editing, and deleting Archivers as aggregate services
- Toggling an aggregate service online and offline
- Monitoring statistics for aggregate services
- Starting and stopping aggregation

Configuring the aggregation process includes setting:

- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service

What do you want to do?

Role	I want to...	Show me how...
Administrator	Add an Archiver service	Add the Archiver Service

Role	I want to...	Show me how...
Administrator	Add a Log Decoder as a Data Source to an Archiver	Add Log Decoder as a Data Source to Archiver
Administrator	Configure Archiver Storage and Log Retention	Configure Archiver Storage and Log Retention
Administrator	Add an Archiver as a Data Source to a Reporting Engine	Add Archiver as a Data Source to Reporting Engine
Administrator	*Configure Archiver Monitoring	Configure Archiver Monitoring
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Aggregate Services Section
Administrator	Manage System Configuration	System Configuration Section

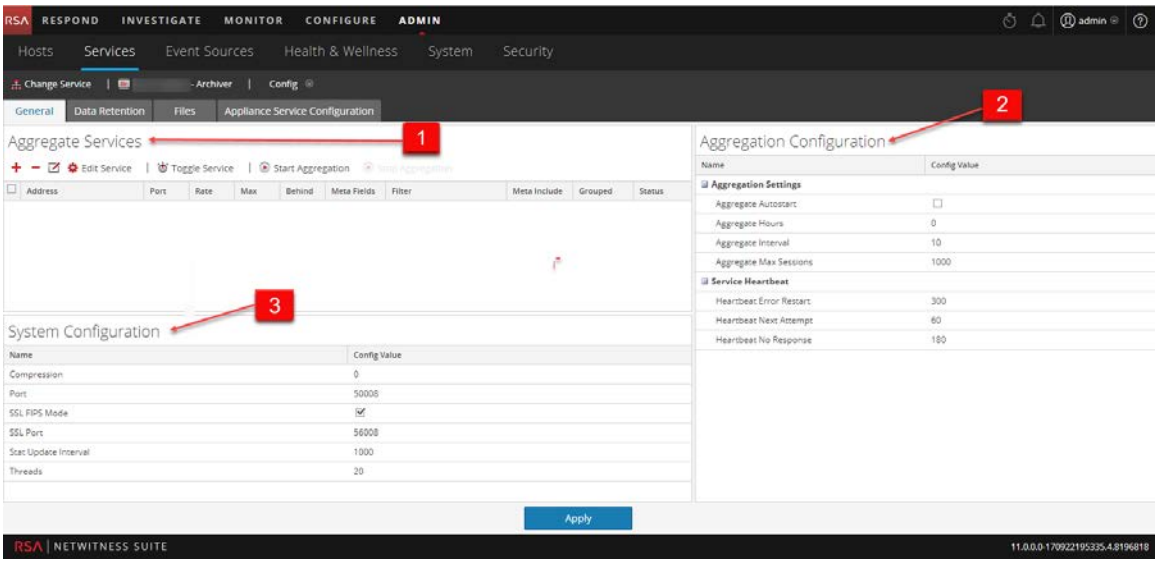
*You can perform this task here.

Related Topics

Configure Log Storage Collections

Quick Look

This is an example of the General tab.



These are the three major sections in the General tab for Archivers:

1. Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service.
2. System Configuration section manages service configuration for a service.
3. Aggregation Configuration section provides configuration settings that affect various aspects of the aggregation process.

Aggregate Services Section

This is an example of the Aggregate Services section for a Concentrator. The Aggregate Services section toolbar offers these options.

Option	Description
+	Opens a dialog in which you can add a Concentrator, Decoder, or Log Decoder as an aggregate service.
−	Removes the selected aggregate service.
	Opens a dialog to edit **Meta Fields** and **Filter** values.
Start Aggregation	When aggregation has been stopped or has not started, starts aggregating data from the online service in the list using the rules defined for the service.
Stop Aggregation	When aggregation is in progress, stops aggregation on the Broker or Concentrator. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.
Toggle Service	Toggles the state of a service between offline and online. Only data from online service is consumed during aggregation.

The Aggregate Services section list has these columns.

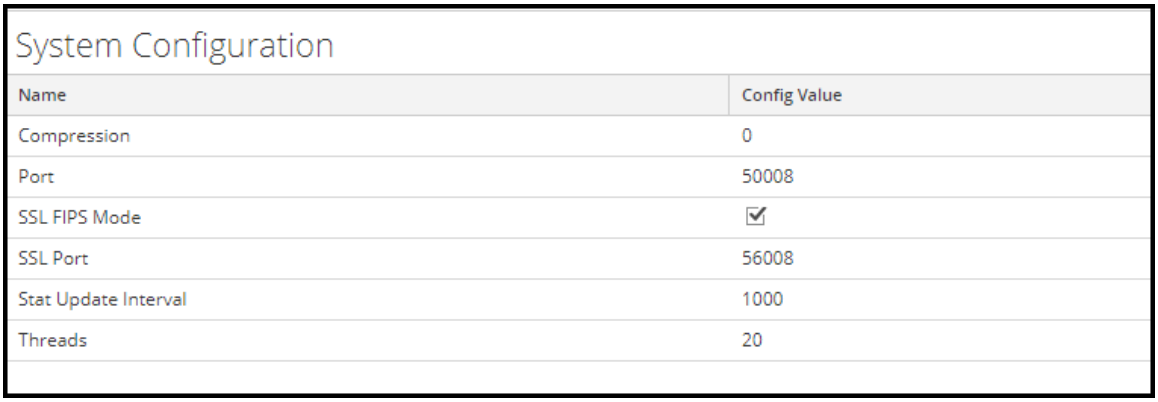
Column	Description
Address	Lists the address of the service.

Column	Description
Port	Lists the port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
Rate	Lists the number of metadata objects being written to the database per second. Values are rolling average samples over a short time period (10 seconds). After capture stops, the rate is reset to **0**.
Max	Lists the maximum number of metadata objects written to the database per second since capture started. Values are rolling average samples over a short time period (10 seconds). After capture stops, **Max** continues to show the maximum value during capture.
Behind	Lists the number of sessions on the service that need to be aggregated.
Collection	For Brokers only, indicates the collection that was selected when the Analyst Workbench service was added to the Aggregate Services section.
Meta Fields	For Concentrators only, lists the types of metadata being consumed by the aggregate service.
Filter	For Concentrators only, lists any filter being applied to the metadata being consumed by the aggregate service.
Meta Include	For Concentrators only, lists the number of types of meta included in the aggregate service.
Grouped	Whether or not the aggregate service is part of a group.

Column	Description
Status	Lists the current status of the service: • online = available to provide data for consumption by the Broker or Concentrator • offline = not available to provide data for consumption by the Broker or Concentrator • consuming = providing data for consumption by the Broker or Concentrator

System Configuration Section

When a service is first added, default values are in effect. You can edit these values to tune performance.



System Configuration

Name	Config Value
Compression	0
Port	50008
SSL FIPS Mode	☑
SSL Port	56008
Stat Update Interval	1000
Threads	20

The System Configuration section has these parameters.

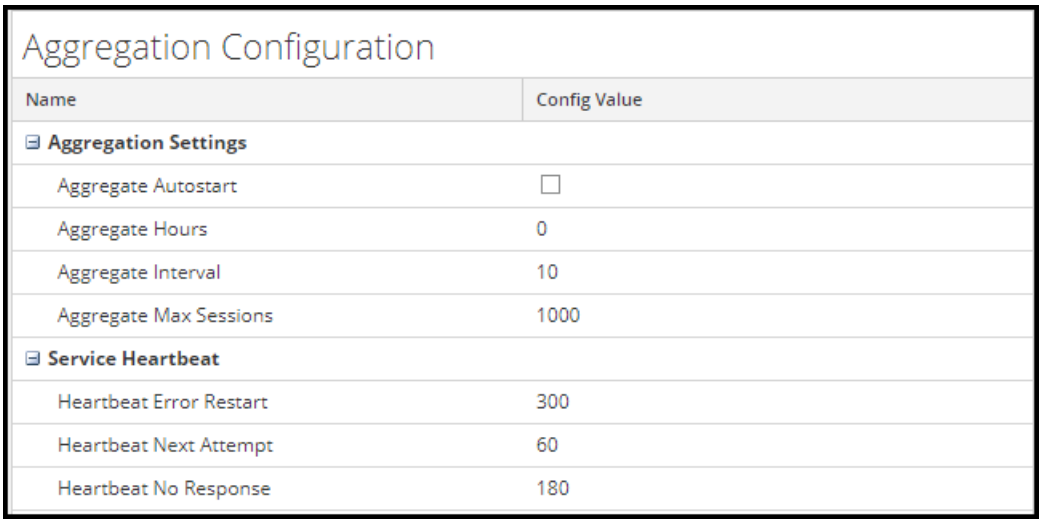
Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of **0** disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.

Parameter	Description
Port	The port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
SSL FIPS Mode	When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
SSL Port	Indicates the SSL port.
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of **0** lets the system decide. The default value is **15**. A change takes effect on service restart.

Aggregation Configuration Section

The Aggregation Configuration Section provides configuration settings for aggregation. When you click **Apply**, the changes are saved; however, not all settings take effect immediately. The tables for Aggregation Settings and Service Heartbeat provide details.

Caution: Do not edit any of these settings without guidance from Customer Support.



Aggregation Configuration

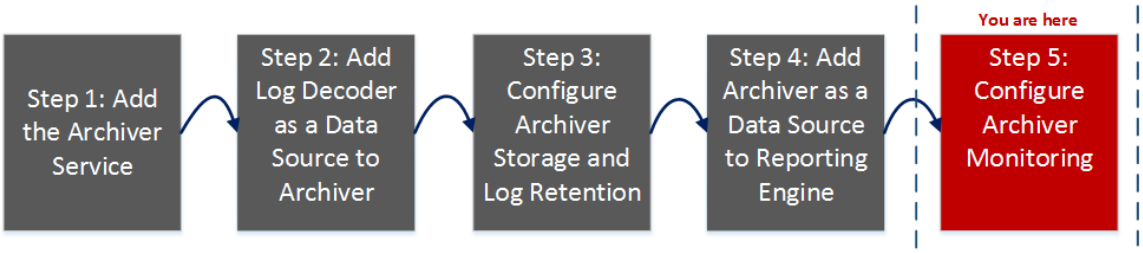
Name	Config Value
Aggregation Settings	
Aggregate Autostart	☐
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	1000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Archiver Service Configuration

This topic lists and describes the available configuration settings for RSA NetWitness Suite Archivers.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver



What do you want to do?

Role	I want to...	Show me how...
Administrator	Add an Archiver service	Add the Archiver Service
Administrator	Add a Log Decoder as a Data Source to an Archiver	Add Log Decoder as a Data Source to Archiver
Administrator	Configure Archiver Storage and Log Retention	Configure Archiver Storage and Log Retention
Administrator	Add Archiver as a Data Source to a Reporting Engine	Add Archiver as a Data Source to Reporting Engine
Administrator	*Configure Archiver Monitoring	Configure Archiver Monitoring
Administrator	Configure Archiver settings	/archiver/config
Administrator	Configure Database settings	/database/config
Administrator	Configure Index settings	/index/config
Administrator	Configure Logs settings	/logs/config
Administrator	Configure REST settings	/rest/config

Role	I want to...	Show me how...
Administrator	Configure SDK settings	/sdk/config
Administrator	Configure Services settings	/services/<service name>/config
Administrator	Configure System settings	/sys/config

*You can perform this task here.

Related Topics

- For more information on configuring Database settings, refer to the "Database Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide.)*
- For more information on configuring Index settings, refer to the "Index Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide.*
- For more information on configuring SDK settings, refer to the "SDK Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide.*

Data Retention Tab - Archiver

From the Admin > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver. From the Data Retention Tab you can configure hot, warm, and cold storage along with configuring multiple storage collections for data retention.

What do you want to do?

Role	I want to...	Show me how...
Administrator	Add the Archiver service.	Add the Archiver Service
Administrator	Add Log Decoder as a Data Source to an Archiver.	Add Log Decoder as a Data Source to Archiver
Administrator	*Configure Archiver Storage and Log Retention.	Configure Archiver Storage and Log Retention
Administrator	Add an Archiver as a Data Source to Reporting Engine.	Add Archiver as a Data Source to Reporting Engine
Administrator	Configure Archiver Monitoring.	Configure Archiver Monitoring

*You can perform these tasks here.

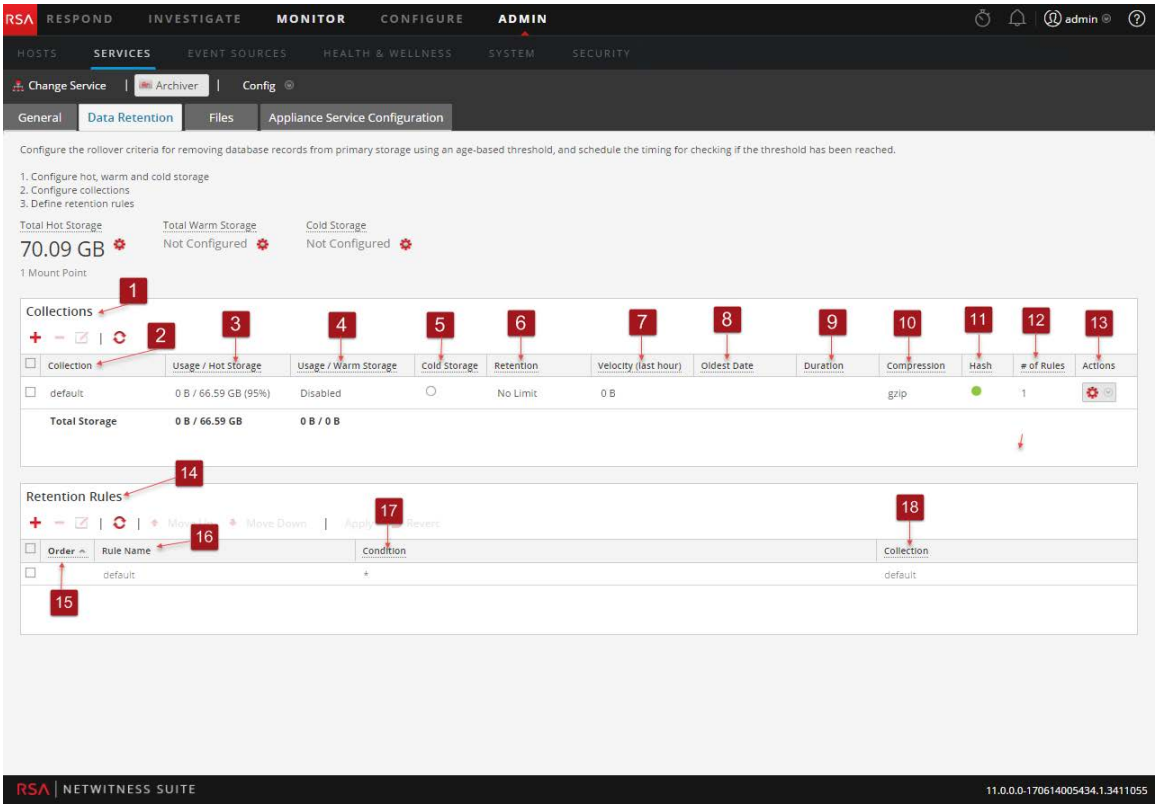
Related Topics

Configuring an Archiver

Configure Hot, Warm, and Cold Storage

Quick Look

As an Administrator, you can configure hot, warm, and cold storage as well as multiple storage collections with different locations and criteria for retaining logs. For example, you can create a Compliance collection that stores logs for a specific time period as required by government regulations. You can create another collection that stores low value logs in hot storage with a much shorter retention period. The flexibility of these collections enables you to have significantly less overall storage requirements.



1	Displays the Collections panel with the Data Retention tab open.
2	Allows you to sort the collections in ascending or descending order.
3	Displays the allocated hot storage space for the collection, as well as the approximate current usage.
4	Displays the allocated warm storage space for the collection, as well as the approximate current usage.
5	Displays whether the collection uses cold storage for long-term backup.
6	Displays the time range used to determine when data is moved to cold storage or discarded.
7	Displays the amount of data written to the collection during the past hour.

8	Displays the date of the oldest data stored in the collection.
9	Displays the approximate age of the oldest data stored in the collection.
10	Displays the compression type used in collection storage.
11	Displays whether or not hashes are used when storing data in the collection.
12	Displays the number of retention rules that use this collection for storing data.
13	Displays the Actions drop-down menu.
14	Displays the Retention Rules panel.
15	Displays the order in which Retention Rules are evaluated in the execution chain.
16	Displays the name of the Retention Rule.
17	Data that satisfies this condition is stored in the corresponding collection.
18	Displays the collection used to store the data that satisfies this particular rule condition.

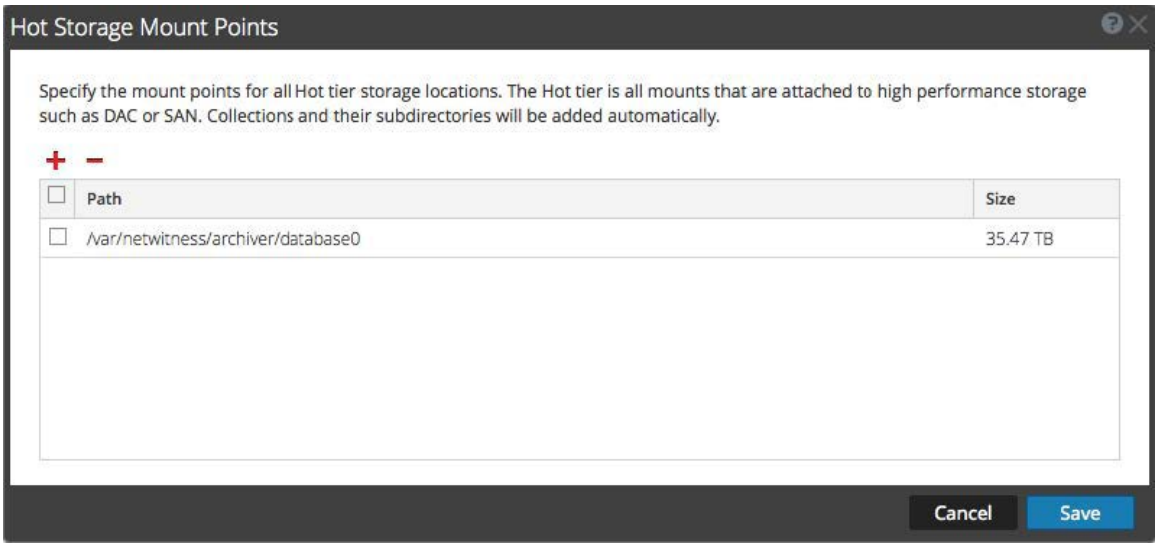
Total Hot, Warm, and Cold Storage

The Total Hot Storage section shows the total amount of Hot storage available and the number of hot storage mount points. The Total Hot Storage section shows the total amount of Warm storage available and the number of warm storage mount points. The Total Cold Storage section shows the total amount of Cold storage and the remaining free space available in Cold storage.

Hot, Warm, and Cold Storage Mount Points Dialogs

In the Hot, Warm, and Cold Storage Mount Points dialogs, you can specify the mount points for your storage locations. You can specify portions of this storage to use for your log storage collections.

To access the Hot, Warm, and Cold Storage Mount Points dialogs, click the icon near the respective section.

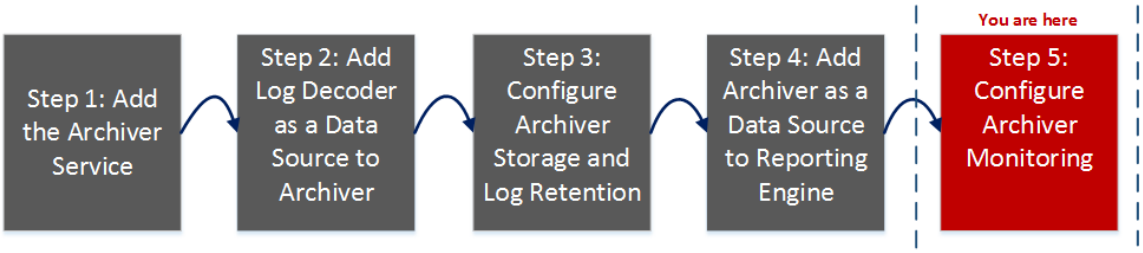

Hot Storage Mount Points
Specify the mount points for all Hot tier storage locations. The Hot tier is all mounts that are attached to high performance storage such as DAC or SAN. Collections and their subdirectories will be added automatically.
Path
Size
/var/netwitness/archiver/database0
35.47 TB
Cancel
Save

Services Config View - Archiver

The Services Config view (ADMIN > Services > select Archiver service and select >View > Config) provides a way to manage basic service configurations, configure aggregate services, configure log retention and storage, edit service configuration files, and configure the appliance service for an Archiver.

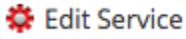
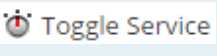
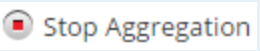
Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Add the Archiver service.	Add the Archiver Service
Administrator	Add a Log Decoder as a Data Source to an Archiver.	Add Log Decoder as a Data Source to Archiver
Administrator	Configure Archiver Storage and Log Retention.	Configure Archiver Storage and Log Retention
Administrator	Add an Archiver as a Data Source to Reporting Engine..	Add Archiver as a Data Source to Reporting Engine
Administrator	Configure Archiver Monitoring.	Configure Archiver Monitoring
Administrator	*Add a Log Decoder as an aggregate service.	Click + in the Aggregate Services section.
Administrator	*Remove the selected aggregate service.	Click − in the Aggregate Services section.

Role	I want to...	Show me how...
Administrator	*Edit Meta Fields and Filter values of the aggregate service.	Click in the Aggregate Services section. You can specify the type of metadata that the Archiver consumes from this service. You can also specify a rule to filter data that the Archiver consumes from this service.
Administrator	*Communicate with the Archiver.	Click  in the Aggregate Services section. This enables you to enter the administrator credentials of the selected aggregate service so that it can communicate with the Archiver.
Administrator	*Toggle the state of a service between offline and online.	Click  in the Aggregate Services section.
Administrator	*Aggregate data using the rules defined for the service.	Click in the Aggregate Services section. Note that it is necessary to start aggregate service after aggregation has been stopped.
Administrator	*Stop aggregation on the Archiver.	Click  in the Aggregate Services section. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.

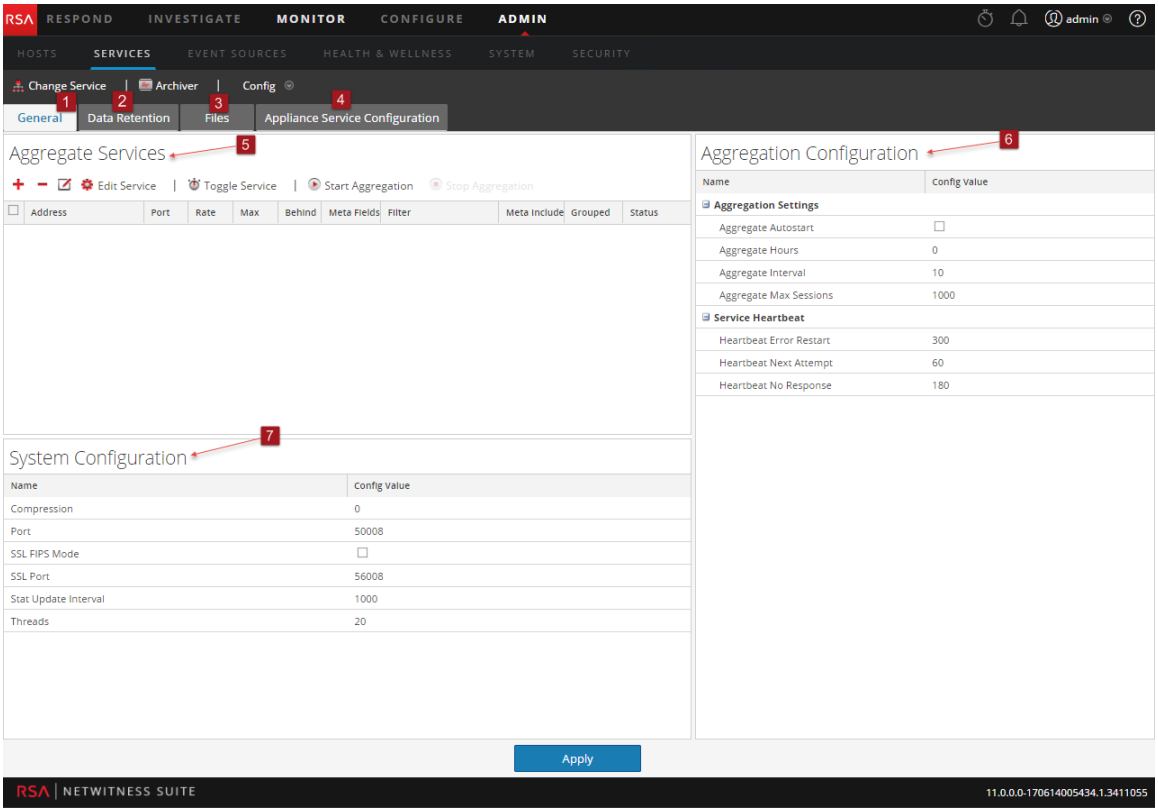
*You can perform this task in the current view.

Related Topics

Configure Log Storage Collections

Quick Look

The Services Config view has four tabs and three panels.



1	General tab provides a way to manage basic Archiver service configuration.
2	Data Retention tab provides a way to view and edit collections and retention rules.
3	Files tab allows you to edit enables you to edit the service configuration files for the Archiver as text files
4	Appliance Service Configuration tab provides a way to configure an Archiver service.
5	Aggregate Services panel provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service.
6	Aggregation Configuration panel provides configuration settings that affect various aspects of the aggregation process.
7	System Configuration panel provides a way to manage service configuration for an Archiver service.

General

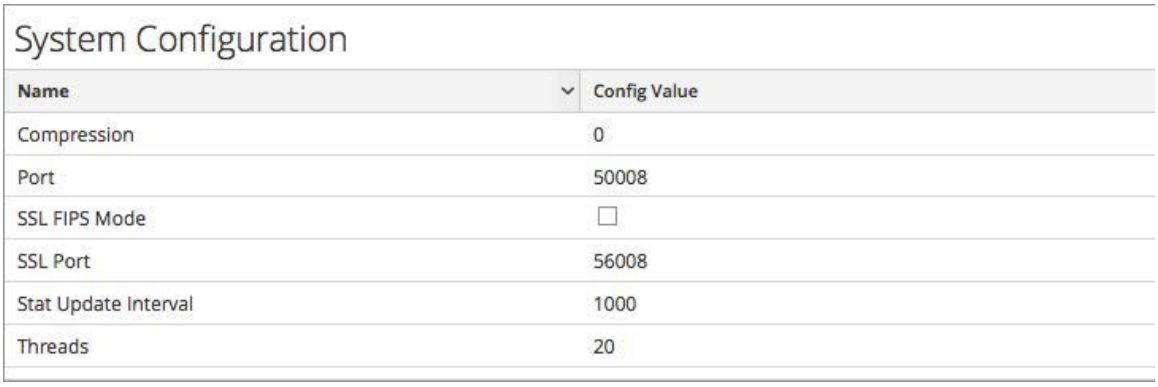
The General tab contains the following sections:

- Aggregate Services
- System Configuration
- Aggregation Configuration

Aggregate Services

The Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service.

System Configuration

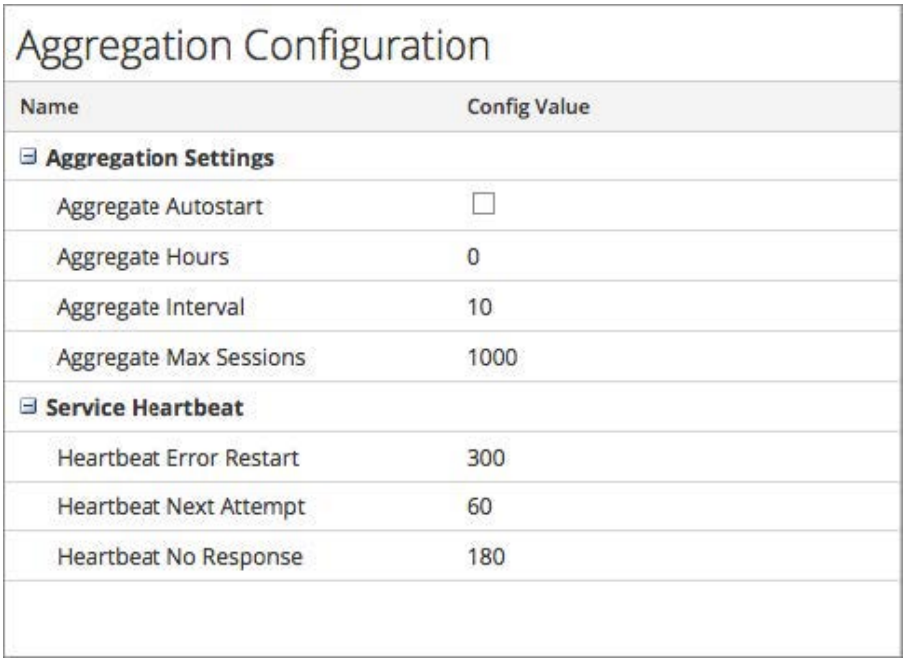


When you add an Archiver service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance. The following table describes the System Configuration parameters.

Task	Description

Task	Description
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.
Port	Determines the port used by the service. **Note:** If you change the port number, ensure that you restart the service.
SSL FIPS mode	If enabled, all the data transferred in the network will be encrypted using SSL.
SSL Port	Indicates the port used for encrypting using SSL.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system.
Threads	Determines the number of threads in the thread pool to handle incoming requests.

Aggregation Configuration



The Aggregation Configuration section contains the following sections:

- Aggregation Settings
- Service Heartbeat

Aggregation Settings

The Aggregations Settings section has the following parameters.

Parameter	Description
Aggregate Autostart	If enabled, data aggregation will automatically restart after a service restart.
Aggregate Hours	Determines the maximum number of hours a service is allowed to start aggregation.
Aggregate Interval	Determines the minimum number of milliseconds before another round of aggregation is requested.
Aggregate Max Sessions	Determines the number of sessions to aggregate on each round.

Service Heartbeat

The Service Heartbeat section has the following parameters.

Parameters	Description
Heartbeat Error Restart	Determines the number of seconds to wait after a service error before attempting a service reconnect.
Heartbeat Next Attempt	Determines the number of seconds to wait before attempting a service reconnect.
Heartbeat No Response	Determines the number of seconds to wait before taking unresponsive service to offline.

Files

The **Files** tab in the Service Config view enables you to edit the service configuration files for the Archiver as text files. The files available to edit vary depending upon the type of service being configured.

The following files are common to all core services:

- Service index file
- NetWitness file
- Crash reporter file
- Scheduler file
- Feed definitions file

For more information on the **Files** tab, see the "Files Tab" topic in the *Host and Services Getting Started Guide*.

RSA NETWITNESS® SUITE

Automated Threat Detection Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Suite Automated Threat Detection 4

Automated Threat Detection for Suspicious Domains 4

Suspicious Domains Module Workflow 5

Suspicious Domains Automated Threat Detection on Packets vs. Web Proxy Logs 7

Configuring Automated Threat Detection for Suspicious Domains 8

Prerequisites 8

Configure Automated Threat Detection for Suspicious Domains 9

Step 1: (For Logs Only) Configure Log Settings 10

To Get the Latest Envision Config File: 11

To Verify the Envision Configuration File was Updated Correctly: 12

To Verify the Indices for the index-concentrator.xml File are Updated: 12

Step 2: Create a Domains Whitelist (Optional) 13

Step 3: Configure the Whois Lookup Service 15

Step 4: Map Data Sources to ESA Analytics Modules 15

Step 5: Verify the Suspected Command & Control By Domain Rule is Enabled and Monitor the Rule 15

Step 6: Verify the Incident is grouped by Suspected C&C 17

Result 17

Next Steps 17

Troubleshooting NetWitness Suite Automated Threat Detection 18

Possible Issues 18

NetWitness Suite Automated Threat Detection

RSA NetWitness® Suite Automated Threat Detection uses preconfigured ESA Analytics modules to identify specific types of threats. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics modules reside within ESA Analytics services. The ESA Analytics services use query-based aggregation (QBA) to collect filtered events for the modules from Concentrators. Only the data required by a module is transferred between the Concentrator and the ESA Analytics system.

There are two ESA services that can run on an ESA host:

- Event Stream Analysis (ESA Correlation rules)
- Event Stream Analytics Server (ESA Analytics)

The first service is the Event Stream Analysis service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live. The second service is the ESA Analytics service, which is used for Automated Threat Detection. Because the ESA Analytics service uses preconfigured modules for Automated Threat Detection, you do not have to create or download rules to use Automated Threat Detection.

NetWitness Suite Automated Threat Detection currently has two Suspicious Domain modules available, Command and Control (C2) for Packets and C2 for Logs.

Because each ESA Analytics module has different data requirements, be sure that all module-specific requirements are met before you deploy a module for Automated Threat Detection.

Automated Threat Detection for Suspicious Domains

The Suspicious Domains modules examine your HTTP traffic to detect domains likely to be malware Command and Control servers connecting to your environment. After NetWitness Suite Automated Threat Detection for Suspicious Domains examines your HTTP traffic, it generates scores based on various aspects of your traffic behavior (such as the frequency and regularity with which a given domain is contacted). If these scores reach a set threshold, an ESA alert is generated. This ESA alert is forwarded to the Respond view. The alert in the Respond view is enriched with data that helps you to interpret the scores to determine what mitigation steps to take.

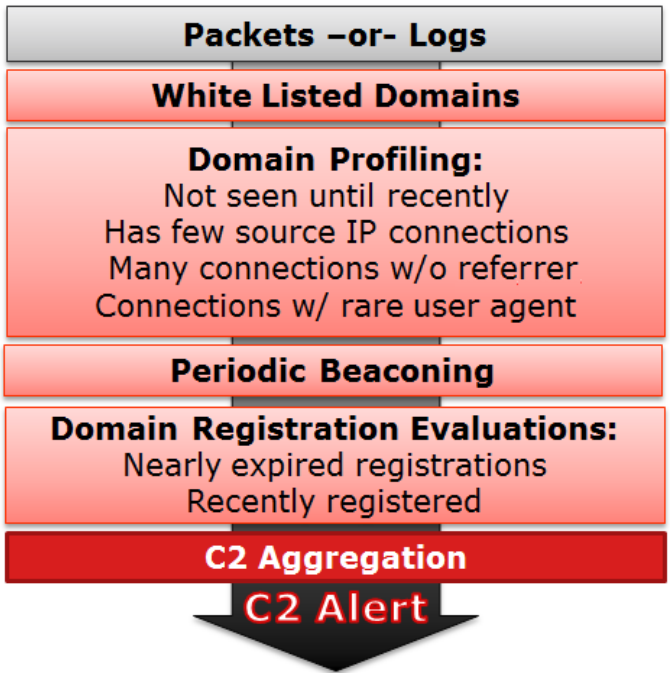
The Automated Threat Detection Suspicious Domain modules provide scoring to detect Command and Control communications. Command and Control communications occur when malware has compromised a system and is sending data back to a source. Often, Command and Control malware can be detected via beaconing behavior. Beaconing occurs when the malware regularly sends communications back to the Command and Control server to notify it that a machine has been compromised and the malware is awaiting further instructions. The ability to catch the malware at this stage of compromise can prevent any further harm from occurring to the compromised machine and is considered a critical stage in the "kill chain."

NetWitness Suite Automated Threat Detection solves several common problems that occur when searching for malware:

- **Ability to use algorithms rather than signatures**. Because many malware creators have begun using polymorphic or encrypted code segments, which are very difficult to create a signature for, this approach can sometimes miss malware. Because NetWitness Suite Automated Threat Detection uses a behavior-based algorithm, it is able to detect malware more quickly and effectively.
- **Ability to automate hunting**. Hunting through data manually is an effective but extremely time-consuming method of finding malware. Automating this process allows an analyst to use his or her time more effectively.
- **Ability to find an attack quickly**. Instead of batching and then analyzing the data, Automated Threat Detection analyzes data as it is ingested by NetWitness Suite, allowing for the attacks to be found in near real-time.

Suspicious Domains Module Workflow

NetWitness Suite Automated Threat Detection works much like a filtering system. It checks to see if certain behavior occurs (or certain conditions exist), and if that behavior or condition occurs, it moves to the next step in the process. This helps to make the system efficient, and frees up resources so that events that are determined to be non-threatening are not held in memory. The following diagram provides a simplified version of the Suspicious Domains module workflow.



1.) **Packets or logs are routed to the ESA**. The HTTP packets or logs are parsed by the Decoder or Log Decoder and sent to the ESA host.

2.) **Whitelist is checked**. If you created a whitelist through the Context Hub, ESA checks this list to rule out domains. If a domain in the event is whitelisted, the event is ignored.

3.) **The domain profile is checked**. Automated Threat Detection checks to see if the domain is newly seen (approximately three days), has few source IP connections, has many connections without a referer, or has connections with a rare user agent. If one or several of these conditions is true, the domain is next checked for periodic beaconing.

4.) **The domain is checked for periodic beaconing**. Beaconing occurs when the malware regularly sends communications back to the command and control server to notify it that a machine has been compromised and the malware is awaiting further instructions. If the site displays beaconing behavior, then the domain registration information is checked.

5.) **Domain registration information is checked**. The Whois service is used to see if the domain is recently registered or nearly expired. Domains that have a very short lifespan are often hallmarks of malware.

6.) **Command and Control (C2) aggregates scores**. Each of the above factors generates a separate score, which is weighted to indicate various levels of importance. The weighted scores determine if an alert should be generated. If an alert is generated, the aggregated alerts appear in the Respond view and can then be investigated further from there. Once the alerts begin to appear in the Respond view, they continue to aggregate under the associated incident. This makes it easier to sort through volumes of alerts that can be generated for a command and control incident.

Analysts can view the alerts in the Respond view.

Suspicious Domains Automated Threat Detection on Packets vs. Web Proxy Logs

RSA NetWitness Suite provides you with the ability to perform Automated Threat Detection for Suspicious Domains using either packets or web proxy logs. While packet data can be streamed directly off of the wire into the NetWitness Suite installation and analyzed directly, if you have the ability to use a web proxy in your installation it may be beneficial to use it. Because some installations use network translation or SSL encryption, the true source IP of an outgoing connection may be masked if you are observing it at the packet level. By using a web proxy you gain the benefit of its ability to accelerate and decrypt SSL traffic as well as its ability to track the true source IP addresses of traffic it monitors.

Both Suspicious Domains for Packets (C2 for Packets) and Suspicious Domains for Logs (C2 for Logs) should produce the same results. From a results point of view, there is no real advantage to using one over the other.

Configuring Automated Threat Detection for Suspicious Domains

This topic tells administrators and analysts how to configure a Suspicious Domains module for NetWitness Suite Automated Threat Detection. The Automated Threat Detection functionality enables you to analyze the data that resides on one or more Concentrators by using preconfigured ESA Analytics modules. For example, using a Suspicious Domains module, an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

There are two types of preconfigured Suspicious Domains modules available in NetWitness Suite: Command and Control (C2) for Packets and C2 for Logs. The Suspicious Domains module defines a subset of events and the activities executed on those events for identifying suspicious C2 domains.

Before you deploy an ESA Analytics module for Automated Threat Detection, it is important to note that there are many potential installation configurations that may be installed on the ESA, including: ESA Analytics, ESA Correlation Rules, and the Context Hub. Each of these may take up resources, so it is important to consider sizing before deploying Automated Threat Detection on your ESA.

Prerequisites

- If you are using Packet data, you must have configured a Decoder for HTTP packet data, and you must have configured an HTTP Lua or Flex parser.
- If you are using web proxy log data, you must have configured the appropriate Log Decoder with the correct parser for your web proxy.
- If you are using web proxy log data, you must have updated to the latest log parsers. The following parsers are supported: Blue Coat Cache Flow (cacheflowelff), Cisco IronPort WSA (ciscoiportwsa), and Zscaler (zscalernss).
- If you are using web proxy log data, for best results you should configure all web proxies the same way (set to the same time zone, use the same collection method -syslog or batch, and if you use batch use the same batching cadence).
- A connection from the ESA host to the Whois service (same location as RSA Live cms:netwitness.com:443) must be opened on port 443. Verify with your System

Administrator that this is complete.

- To whitelist a domain, you need to enable the Context Hub service.

Important: Automated Threat Detection requires a "warm-up" period that acclimates the scoring algorithm to the traffic in your network. You should plan to configure Automated Threat Detection so that the warm-up period can run during normal traffic. For example, starting Automated Threat Detection on a Tuesday at 8:00 am in the timezone that contains the majority of your users allows the module to accurately analyze a day of normal traffic.

Configure Automated Threat Detection for Suspicious Domains

This procedure provides the steps needed to configure an ESA analytics Suspicious Domains module for Automated Threat Detection. ESA analytics modules, such as Suspicious Domains, are considered preconfigured because you do not have to manually create ESA rules for them.

The basic steps required are:

1. **Configure Log settings (for Logs only)**. Before you can use Automated Threat Detection for Logs, you must configure several settings. Skip this step if you plan to use Automated Threat Detection for Packets.
2. **Create a whitelist (optional) using the Context Hub service**. Creating a whitelist allows you to ensure that commonly accessed websites are excluded from any Automated Threat Detection scoring.
3. **Configure the Whois Lookup service**. The Whois service enables you to get accurate data about domains that you connect to. In order to ensure effective scoring, it is important that you configure the Whois Lookup service. Verify that the Whois Service is reachable from your environment.
4. **Map data sources to ESA Analytics modules**. You define how NetWitness Suite Automated Threat Detection should automatically detect advanced threats by mapping a preconfigured ESA analytics module to multiple data sources, such as Concentrators, and an ESA analytics service.
5. **Verify the C2 incident rule is enabled and monitor for activity**. After mapping your Suspicous Domains module, a period of time is required for the scoring algorithm to warm-up. After the warm-up period, verify that the C2 rule is enabled in the Incident Rules and monitor to see if the rule is triggered.
6. **Verify that the incident rules are configured correctly**. When you view incidents in the Respond view, it is helpful if the incidents are grouped by Suspected C&C.

Step 1: (For Logs Only) Configure Log Settings

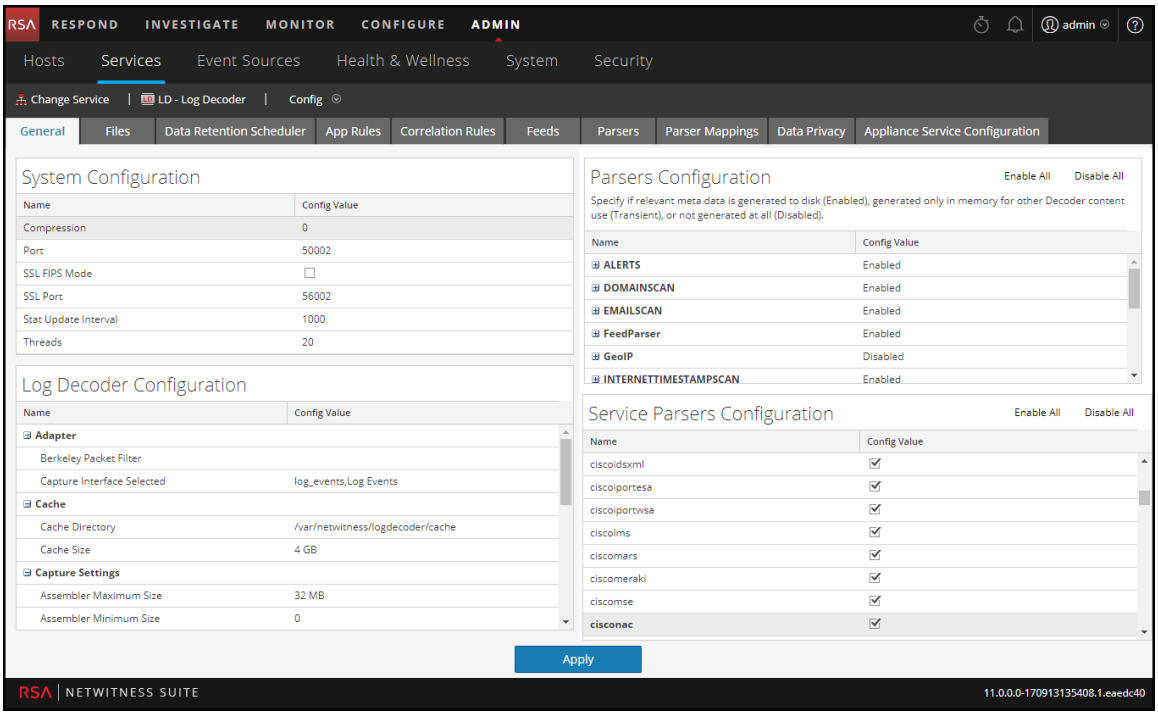
To configure Automated Threat Detection for Logs, you need to complete a few extra configuration steps:

- Verify that the supported parsers are enabled for your Log Decoder.
- Get the latest versions of the appropriate web proxy parser from RSA Live.
- Update the mapping on the Envision config file. This file is required to update the Log Decoder to work with the new meta available via the parsers.
- Verify that the table-map.xml file was updated correctly.
- Verify that the indexes were updated correctly.

To verify your parsers are running on your Log Decoder:

1. Go to **ADMIN > Services**.
2. Select your Log Decoder and select > **View > Config**.

   The Service Parsers Configuration section shows a list of enabled parsers.
3. Verify that the appropriate web proxy parser is enabled.

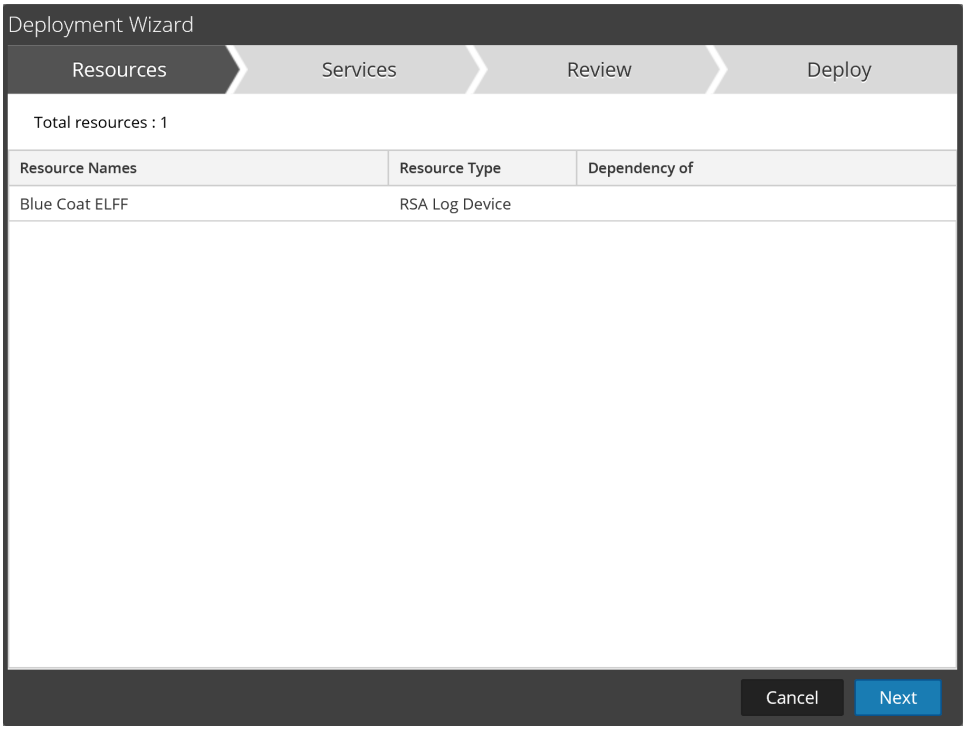


To get the latest parsers from RSA Live:

1. Go to **CONFIGURE > Live Content**.
2. Enter a search term for one of the supported web proxy parsers.
3. Select the appropriate web proxy parser [for example, the Blue Coat ELFF (cacheflowelff) parser].

   Note: You should have taken steps to configure logging to occur on your web proxy parser correctly.

4. Click **Deploy**.
   The Deployment Wizard opens.

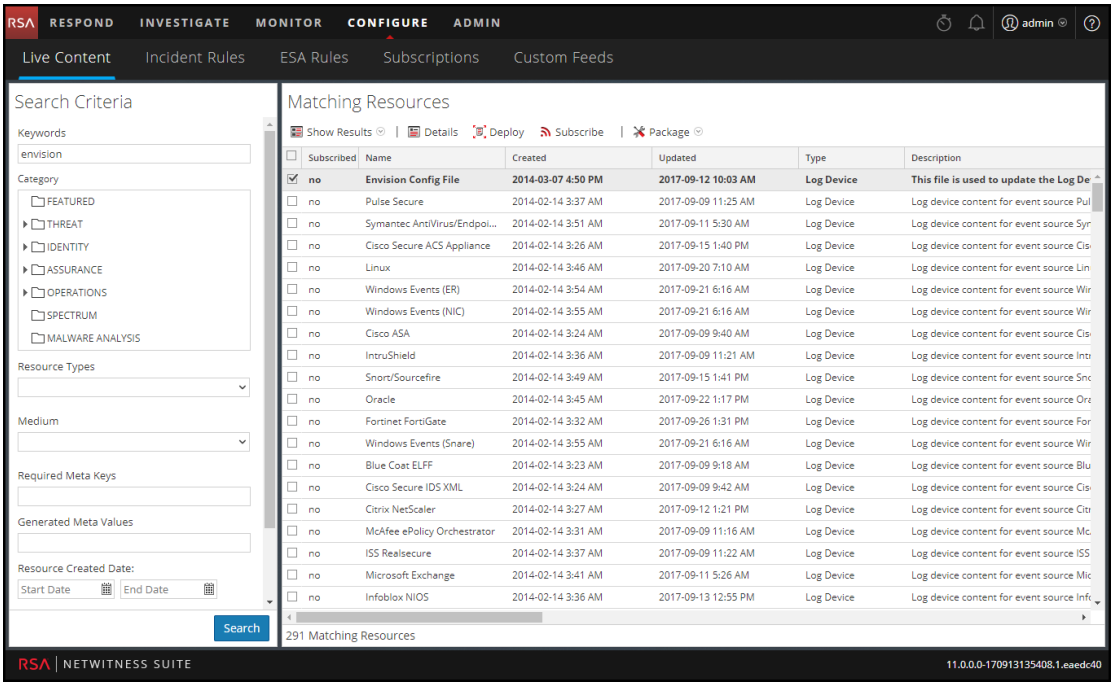


5. Under **Services**, select the Log Decoder as the Service.
6. Click **Deploy** to deploy the parser to your Log Decoder.

To Get the Latest Envision Config File:

1. Go to **CONFIGURE > Live Content**.
2. Enter **envision** as the key word for the search.

3. Select the latest Envision Config file, and click **Deploy**.



4. In the Deployment Wizard, under **Services**, select your Log Decoder.
5. Click **Deploy** to deploy the Envision configuration file to the Log Decoder.

To Verify the Envision Configuration File was Updated Correctly:

1. Go to **ADMIN > Services**, select the Log Decoder, and then select **> View > Config > Files** tab.
   You can see the **table-map.xml** file. This file is modified when you update the Envision Configuration file.
2. Search for the term, *event.time*. The field should now read, *"event.time" flags ="None"*. This means that the event.time meta is now included in the mapping. Similarly, the fqdn flag should be set to "None".

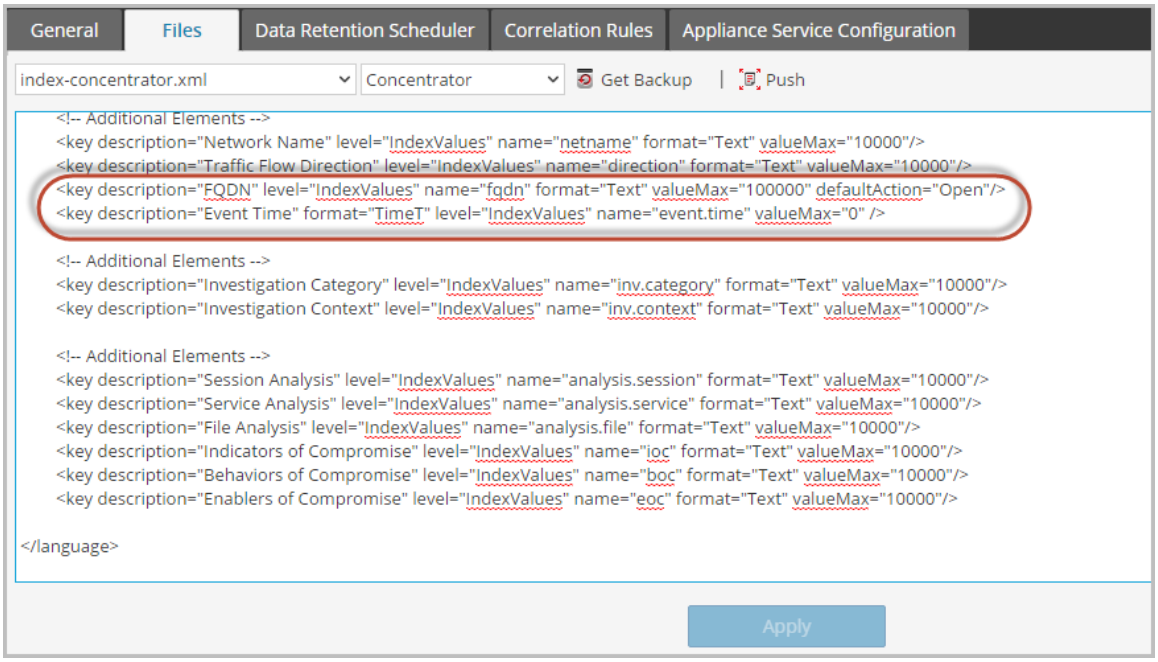
To Verify the Indices for the index-concentrator.xml File are Updated:

You will need to verify that the **index-concentrator.xml** file includes both the event.time and fqdn meta.

1. Go to **ADMIN > Services**, select your Concentrator, and then select **> View > Config**.
2. On the Files tab, search for the **index-concentrator.xml** file.

3. Verify that the following entry exists in your index-concentrator.xml file. If not, you will need to ensure your Concentrator is upgraded to the correct version:

```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text"
valueMax="100000" defaultAction="Open"/><key description="Event Time"
format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```



Step 2: Create a Domains Whitelist (Optional)

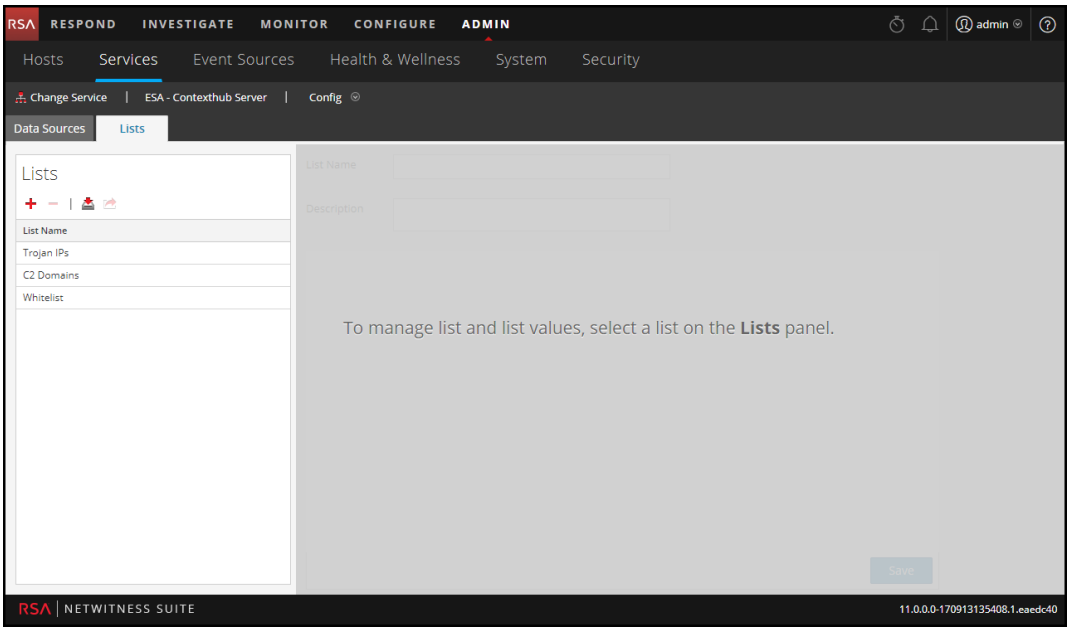
This procedure is used when working with Automated Threat Detection to ensure that certain domains do not trigger a threat score. Sometimes, a domain you access regularly may trigger an Automated Threat Detection score. For example, a weather service might have similar beaconing behavior as a Command and Control communication and trigger an unwarranted negative score. When this happens, it is called a false positive. To prevent triggering a false positive with a specific domain, you can add the domain to a whitelist. Most domains do not need to be whitelisted because the solution only alerts on very suspect behaviors. The domains you may want to whitelist are valid automated services that do not have many host connections.

Note: For migrations from 10.6.x, if your previous Automated Threat Detection whitelist (Whitelisted Domains) appears on the Lists tab, you can rename it to **domains_whitelist** to use it for the Suspicious Domains modules.

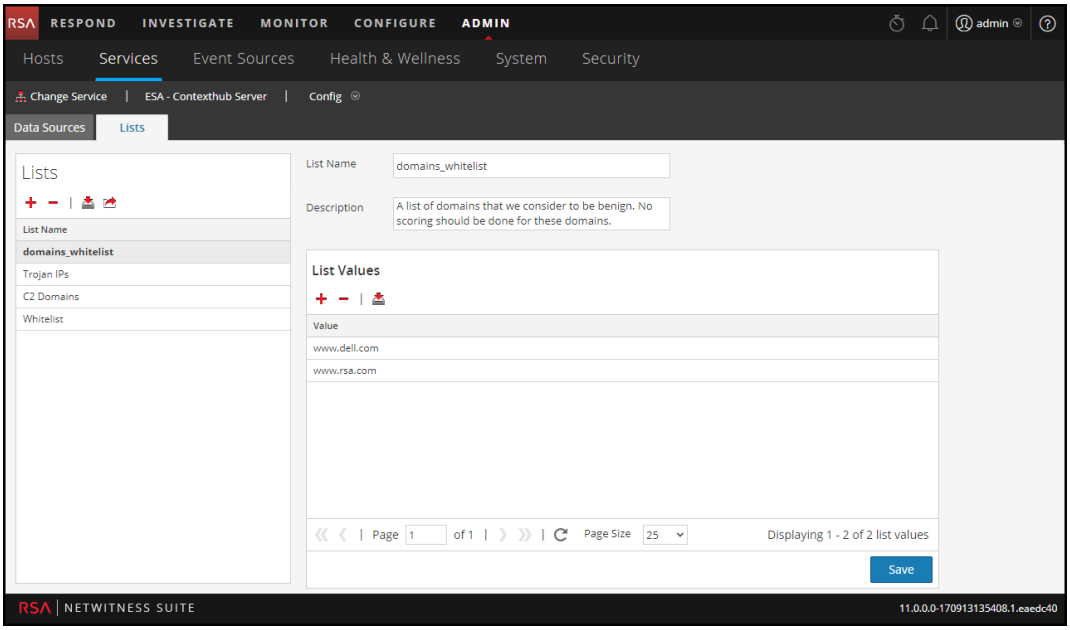
1. Create a whitelist for domains in Context Hub named **`domains_whitelist:`**

   a. Go to **ADMIN > Services**, select the Context Hub Server service, and then select **View > Config > Lists** tab.

   The Lists tab shows the current lists in the Context Hub.



b. In the Lists panel, click + to add a list. In the **List Name** field, type **`domains_whitelist`**. You must use this name in order for the module to recognize it.



2. Manually add domains to the list or import a .CSV file containing a list of domains.
   You can enter full domains, or you can use a wild card to include all sub-domains for a given domain. For example, you can enter *.gov to whitelist all government IP addresses. However, you cannot use other regex functions, such as [a-z]*.gov. This is because using *.gov replaces an entire string, such as www.irs.gov.

a. To add domains manually, in the **List Values** section, click to add domains.

b. To remove a domain, select the domain and click .

c. To import a .CSV file, in the **List Values** section, click , and in the **Import List Values** dialog, navigate to the .CSV file. Choose from the following delimiters: Comma, LF (Line Feed), and CR (Carriage Return) depending on how you have separated the values in your file. Click **Upload**.

3. Click **Save**.
   The **domains_whitelist** appears in the Lists panel. Analysts can add to this list from the Respond view and other parts of Investigation. The *Context Hub Configuration Guide* provides additional information.

Step 3: Configure the Whois Lookup Service

See the "Configure Whois Lookup Service" topic in the *ESA Confguration Guide*.

Step 4: Map Data Sources to ESA Analytics Modules

See the "Mapping ESA Data Sources to Analytics Modules" topic in the *ESA Confguration Guide*.

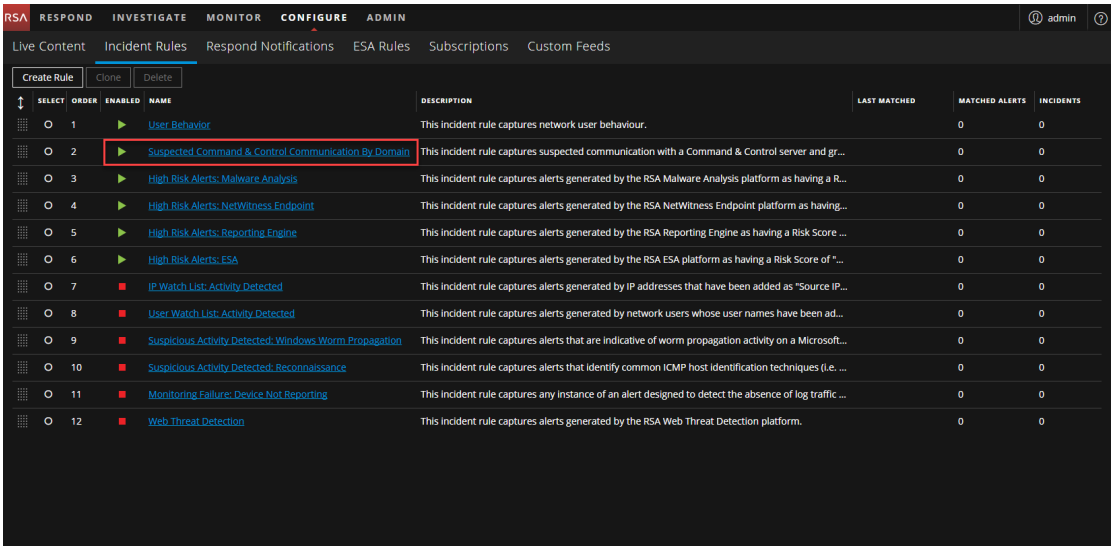
Step 5: Verify the Suspected Command & Control By Domain Rule is Enabled and Monitor the Rule

Note: The information in this procedure applies to version 11.1 and later

Verify and monitor the Suspected Command & Command Control by Domain rule in the Incident Rules list.

1. Go to **CONFIGURE > Incident Rules**.

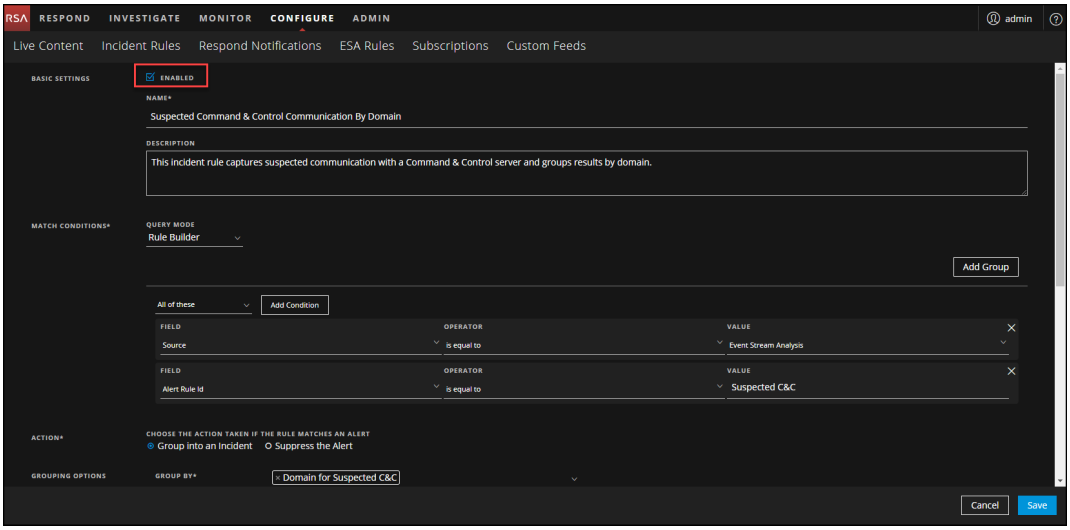
2. In the Incident Rules list, locate the **Suspected Command & Control Communication by Domain** rule and verify that it displays a green Enabled icon (▶) next to the rule name.



3. If the rule is not enabled:

   a. Click the link in the NAME field to open it.

   b. In the Incident Rule Details view, select **Enabled** and click **Save**.



4. In the Incident Rules list, monitor the statistics in the following fields to see if the rule is triggered:

   - **Last Matched**: Shows the time when an alert was successfully matched with the rule.
   - **Matched Alerts**: Displays the number of alerts that matched the rule.
   - **Incidents**: Displays the number of incidents created by the rule.

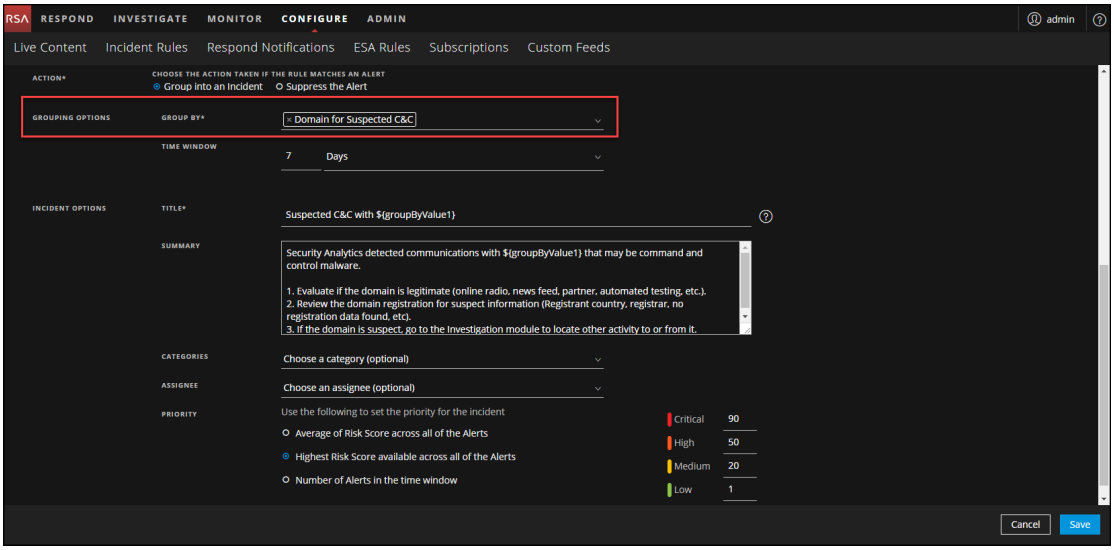
By default, these values reset to zero every 7 days. For more information, see "Set Counter for Matched Alerts and Incidents" in the *NetWitness Respond Configuration Guide*.

Step 6: Verify the Incident is grouped by Suspected C&C

Note: The information in this procedure applies to version 11.1 and later

In order to group incidents correctly in the Respond view, set the Group By condition to Domain for Suspected C&C.

1. Go to **CONFIGURE > Incident Rules**.
2. In the Incident Rules list, locate the **Suspected Command & Control Communication by Domain** rule and click the link in the NAME field to open it.
3. In Grouping Options section, verify that the **Group By** field is set to *Domain for Suspected C&C*.



This will aggregate alerts and incidents will be created for "Suspected C&C".

Result

After you deploy the ESA Analytics Suspicious Domains module mapping for Automated Threat Detection, your ESA will begin to perform analytics on the HTTP traffic. You can view detailed information for each incident in the Respond view.

Next Steps

Monitor the Respond view to see if the rule is triggered. The *NetWitness Respond User Guide* provides additional information.

Troubleshooting NetWitness Suite Automated Threat Detection

NetWitness Suite Automated Threat Detection is an analytics engine that examines your HTTP data. It also makes use of other components, such as the Whois and Context Hub services, which can add complexity to your installation. This topic provides suggestions to help you find issues if your Automated Threat Detection deployment does not provide the results that you expect.

Possible Issues

Problem	Possible Causes	Solutions
I'm seeing too many alerts (false positives).	Several	One possible cause is that the Whois Lookup service is failing or is not configured. The Whois lookup is helpful in determining whether a URL is valid, and if the connection fails or is not properly configured, it can result in false positives. See the "Configure Whois Lookup Service" topic in the *ESA Confguration Guide*.
		You may need to whitelist URLs. Sometimes the legitimate behavior for a URL triggers an alert. One way to prevent this from occurring is to add the URL to the whitelist. See the "Add an Entity to a Whitelist" topic in the *NetWitness Respond User Guide*.
I'm not seeing any alerts.	The ESA host requires a "warm-up" period when you deploy an ESA Analytics Module Mapping for Automated Threat Detection.	When you deploy an ESA analytics module mapping for Automated Threat Detection, there is a "warm-up" period, during which no alerts are viewable. Each module type has a default warm-up period and you need to wait until the warm-up period is complete. For more information, see the "Mapping ESA Data Sources to Analytics Modules" topic in the *ESA Configuration Guide*.

Problem	Possible Causes	Solutions
I'm seeing performance issues (more resource usage or a drop in throughput).	Several	If you are having performance issues on an ESA host that is running both Automated Threat Detection (ESA Analytics) and ESA rules, follow the troubleshooting steps for rules. For these troubleshooting steps, go to "Troubleshoot ESA" in the *Alerting with ESA Correlation Rules User Guide*.

RSA NETWITNESS® SUITE

Broker and Concentrator Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Broker and Concentrator Basics **4**

Overview of Broker and Concentrator **5**

Broker and Concentrator Configuration **7**

Basic Configuration Checklist 7

Step 1. Verify Service System Configuration 8

Step 2. Configure the Aggregation Process 10

Step 3. Configure Aggregate Services 13

Add Aggregate Services to a Broker or Concentrator 13

Remove Aggregate Services from a Broker or Concentrator 15

Edit Aggregate Services on a Concentrator 16

Toggle a Service 18

Step 4. (Optional) Configuring Group Aggregation 18

RSA Group Aggregation Deployment Recommendations 18

Advantages of Using Group Aggregation 18

Configure Group Aggregation 20

Step 5. Start and Stop Aggregation 26

Start and Stop Data Aggregation in the Services System View 26

Start and Stop Aggregation in the Services Config View 27

Broker and Concentrator Configuration References **30**

Services Config View - Broker or Concentrator General Tab 31

What do you want to do? 31

Related Topics 31

General tab 31

Aggregate Services Section 33

Aggregation Configuration Section 36

Services System View - Broker or Concentrator 40

What do you want to do? 40

Related Topics 40

Services System View 40

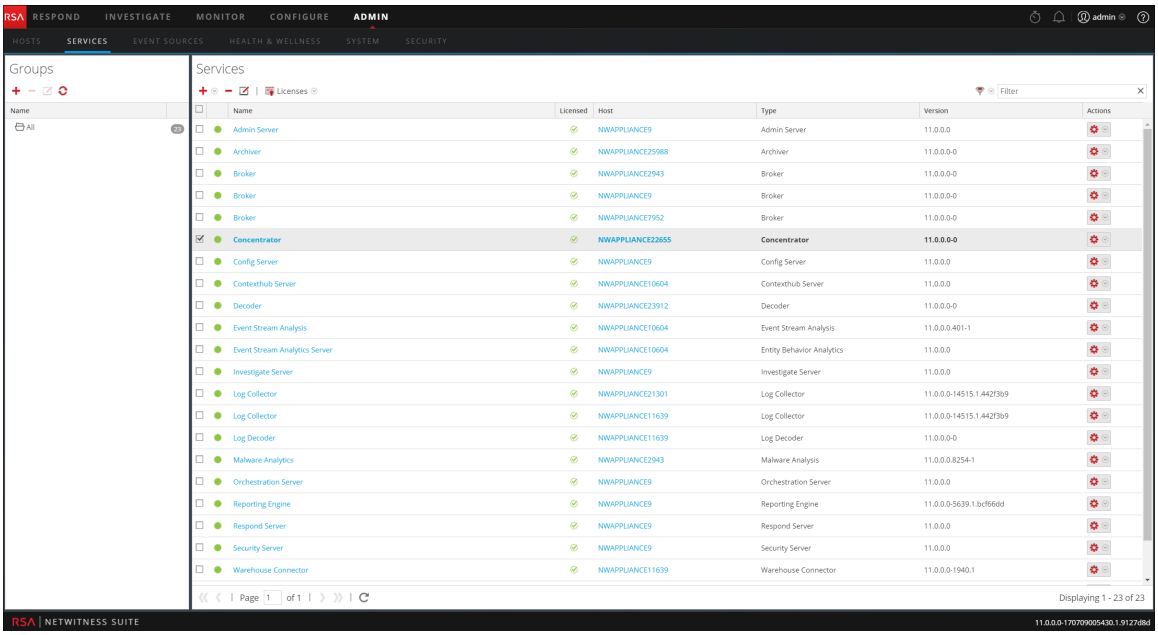
Broker and Concentrator Basics

Concentrators and Brokers aggregate data captured or aggregated by other services unlike Decoders, which capture data,

NetWitness Suite supports the Broker and Concentrator services:

- Brokers - aggregate data across entire infrastructure from configured Concentrators. You can have multiple concentrators aggregating into one broker. You can also have multiple brokers aggregating into a single broker.
- Concentrators - aggregates and analyzes data across multiple capture locations from Decoders. Indexes and directs queries.

You can configure various Brokers and Concentrators together under a Broker. Brokers are able to pull in data quickly from the Concentrators because they acquire index information only. This configuration is done using the NetWitness Suite user interface. Most of the configuration is performed in the Administration Services view (Admin > Services).



You can also configure the aggregate services and perform the whole aggregation process using the Services view. This helps setup Aggregation autostart, Timing and performance parameters, maximum number of open meta and session files. In addition to this, you can also time the attempts to restart, reconnect, or take offline a non-responsive aggregate service. Configuring Aggregate services includes managing Concentrators and Decoders as aggregate services. You can also limit the data being consumed from an aggregate service using meta fields and filters. The aggregation tasks are performed in the General tab of Administration Services view (Admin > Services)

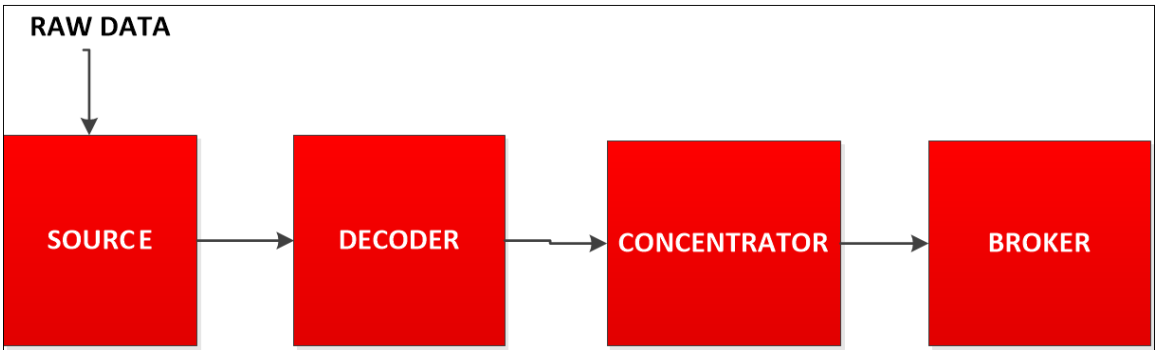
Overview of Broker and Concentrator

Brokers and Concentrators work in conjunction with Decoders and Log Decoders in the NetWitness Suite network. Unlike the two types of Decoders, which capture packets and logs, Concentrators and Brokers aggregate the data captured or aggregated by other services. Brokers aggregate data from configured Concentrators; Concentrators aggregate data from Decoders. A complete overview of the NetWitness Suite network is provided in the *NetWitness Suite Getting Started Guide*.

Note: Go to the Master Table of Contents in RSA Link to find and view referenced documents.

As raw data is entered in the system from the source for analysis, it has to be collected and parsed. This raw data is collected, parsed, and stored using a Decoder. The packet data is then indexed, stored, and parsed by the Concentrator. Parsed packet data is also provided as an endpoint for queries. Eventually, the Broker routes queries across multiple Decoder and Concentrator appliances. Here is how information flows to a Concentrator and Broker.

In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance.

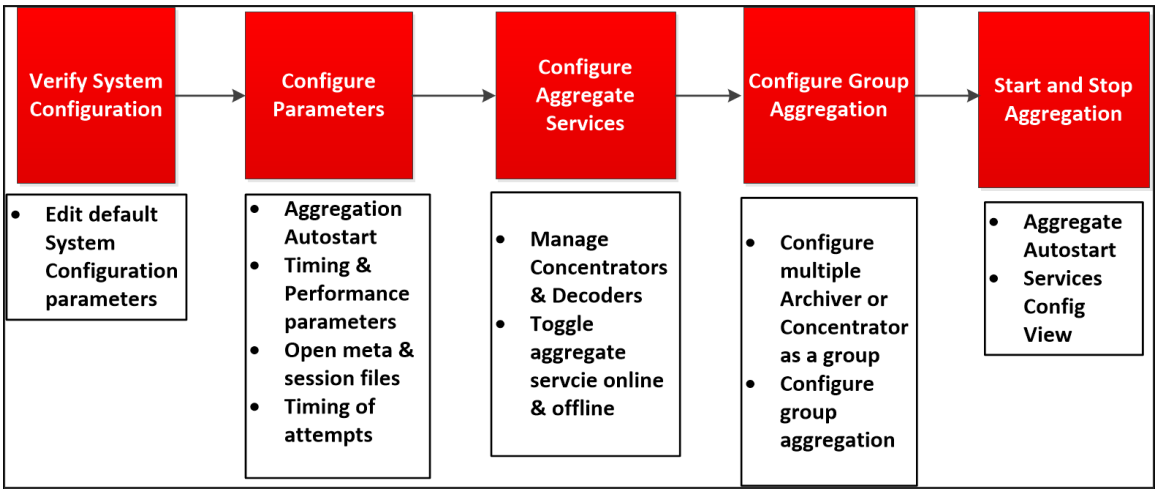


- Concentrator: is required for any large environment to store the Meta data that is generated by the parsers and feeds being triggered by packets and logs ingested into the decoders. l
- Broker: The Broker service is similar to the Concentrator service except that it indexes the collected information. It performs virtual mapping of indices on all connected concentrators. Due to the less internal processing performed, the response time is fast. To allow investigation, multiple brokers and/or concentrators report data into a broker.

Broker and Concentrator Configuration

Setting up a Broker or Concentrator involves configuring the basic system parameters, the aggregate services, and the aggregation process between a Broker or Concentrator and the aggregate services.

These are the required configuration steps for a new Broker or Concentrator, and also for changing the configuration of an existing Broker. Perform the steps in the section in the sequence they are given.



Basic Configuration Checklist

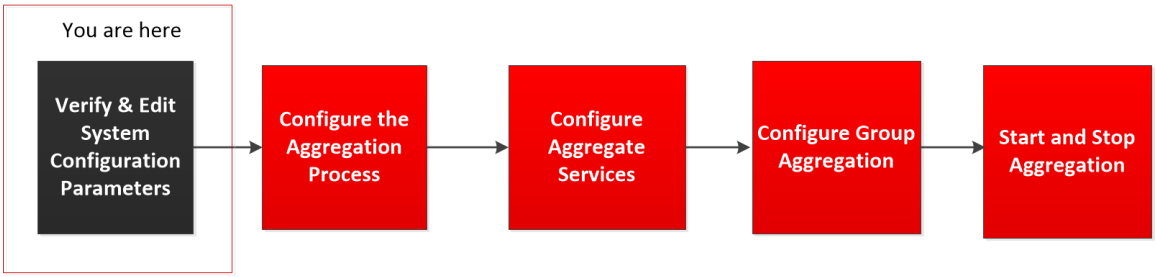
The following checklist provides the sequence for tasks that are required to configure a Broker or Concentrator that has been added to NetWitness Suite in accordance with the *Hosts and Services Guide*.

Configuration Step	Description
Step 1 - Verify System Configuration	Verify system configuration default values for the host and service are appropriate as described in Step 1. Verify Service System Configuration
Step 2 - Configure Parameters	Configure parameters that govern the overall aggregation process as described in Step 2. Configure the Aggregation Process

Configuration Step	Description
Step 3 - Configure Aggregate Services	Configure aggregate services as described in Step 3. Configure Aggregate Services
Step 4 - Configure Group Aggregation	(Optional) Configure group aggregation as described in Step 4. (Optional) Configuring Group Aggregation
Step 5 - Start and Stop Aggregation	Start and stop aggregation as described in Step 5. Start and Stop Aggregation

Step 1. Verify Service System Configuration

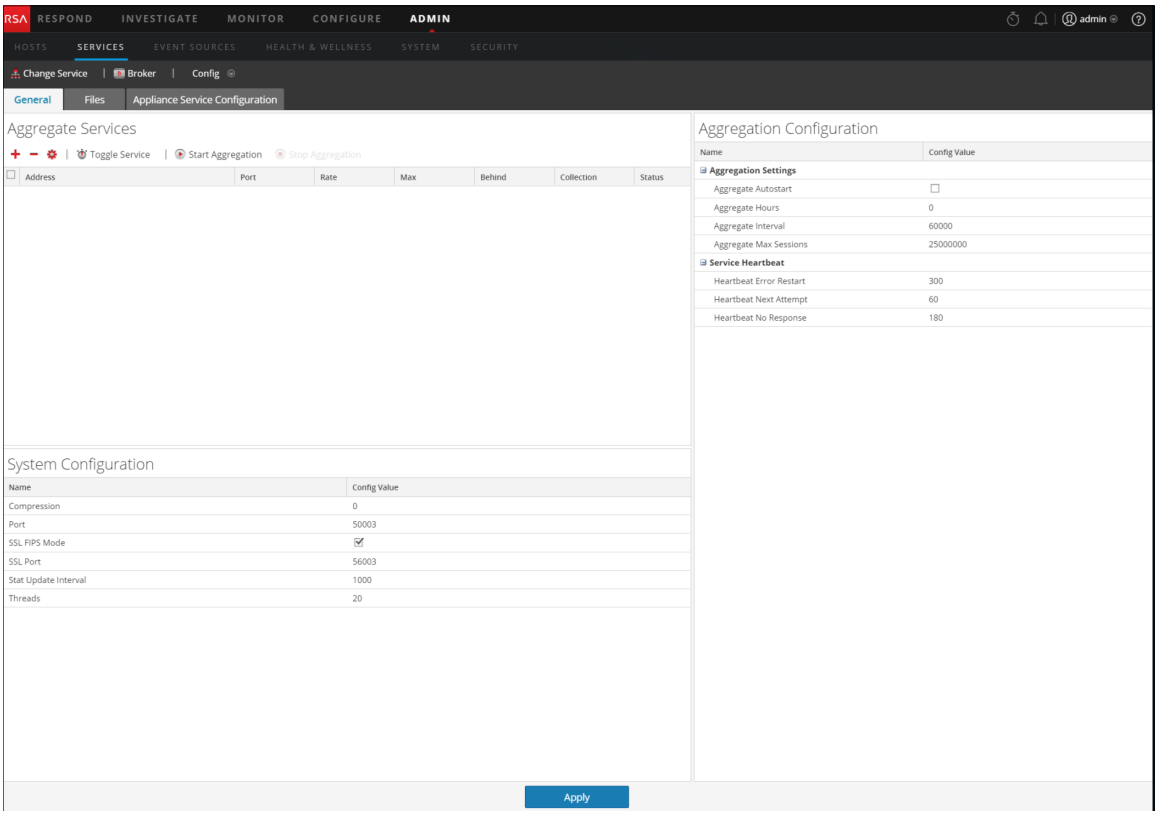
When a service is first added to NetWitness Suite, default values for the system configuration parameters are in effect. You can edit these values to tune performance.



In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance.

To edit system configuration parameters for a Broker or Concentrator:

1. In the **main menu**, select ADMIN > **Services**.
2. In the **Services** view, select a Broker or Concentrator, and in the Actions column, select > **View** > **Config**.
   The Services Config view for the selected service is displayed.

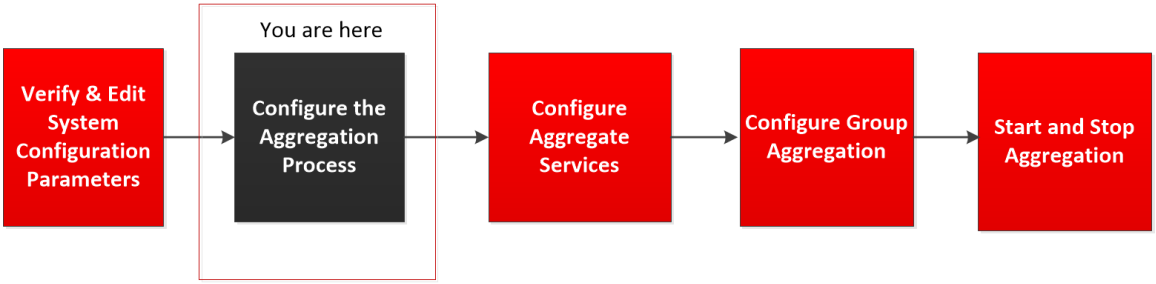


3. Under System Configuration, click a field that you want to edit, and type a new value.
4. When finished editing, click Apply.

Step 2. Configure the Aggregation Process

Configuring the aggregation process for a Broker or Concentrator includes setting:

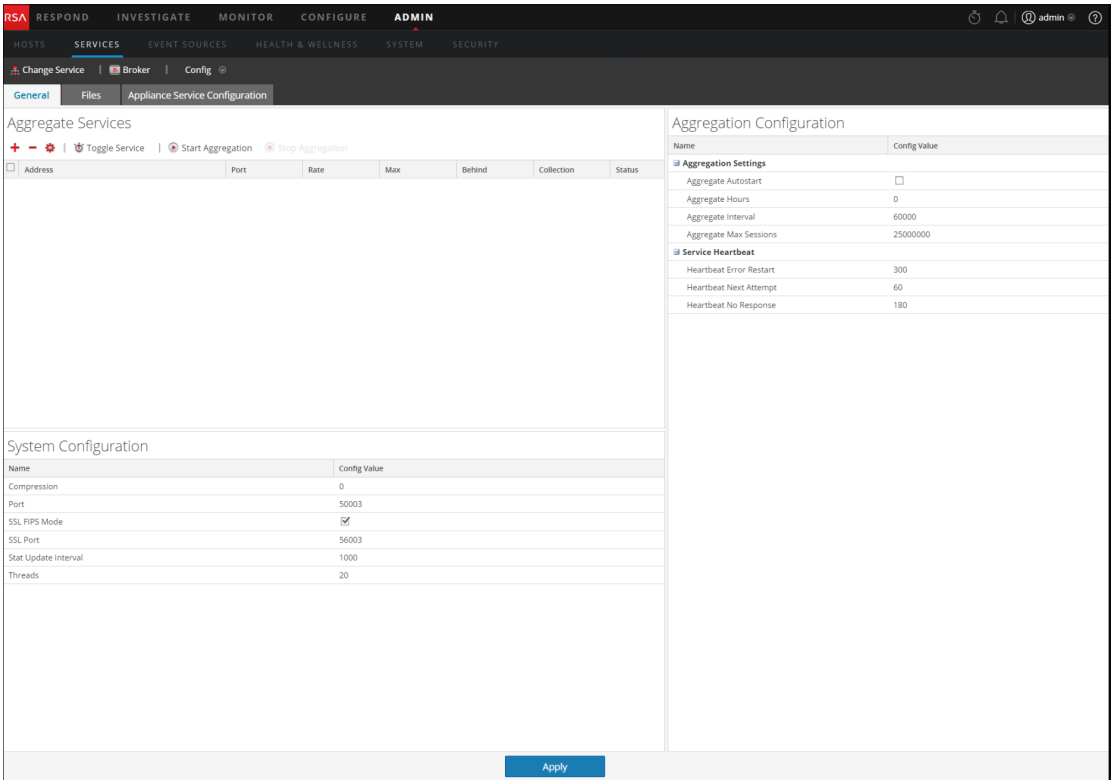
- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- Maximum number of open meta and session files
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service



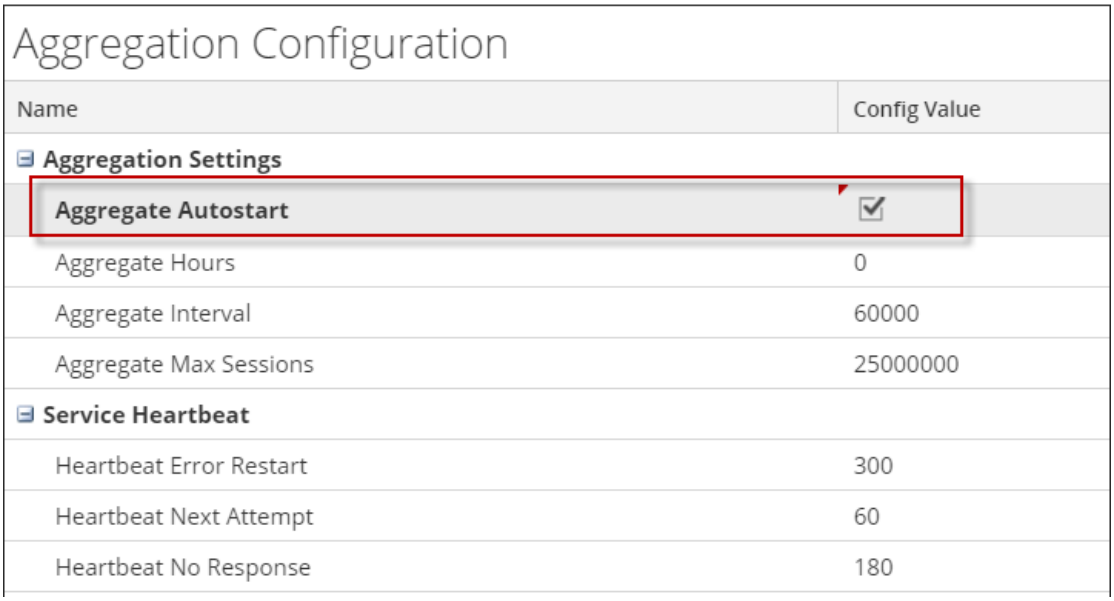
To configure the aggregation process on a Broker or Concentrator:

1. In the **main menu**, select ADMIN > **Services**.
2. In the **Services** view, select a Broker or Concentrator, and select > **View** > **Config**.
   The Services Config view, which includes the Aggregation Configuration section, is

displayed.



3. (Optional) Select **Aggregate Autostart** to enable automatic start of aggregation when a service is online.



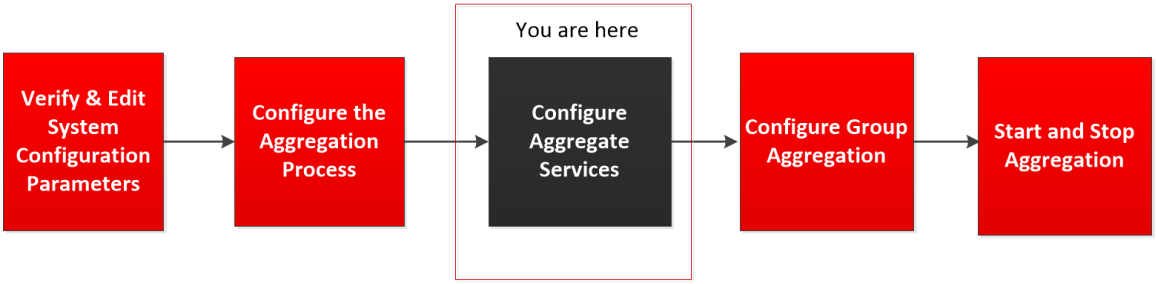
4. (Optional) Edit any of the aggregation settings: the hours back to begin aggregation, the milliseconds between rounds of aggregation, and maximum number of sessions per aggregation round.
5. (Optional) Edit any of the Service Heartbeat settings, which specify the timing of the first attempt to reconnect to a service after an error, the next attempt to reconnect, and taking the service offline after failure to reconnect.
6. When finished editing the settings, click **Apply**.
   The settings become effective immediately

Step 3. Configure Aggregate Services

This topic introduces basic tasks related to data aggregation on Brokers and Concentrators. For information on the optional setup of group aggregation, see Step 4. (Optional) Configuring Group Aggregation.

Configuring the aggregate services (whose data is consumed and aggregated) includes:

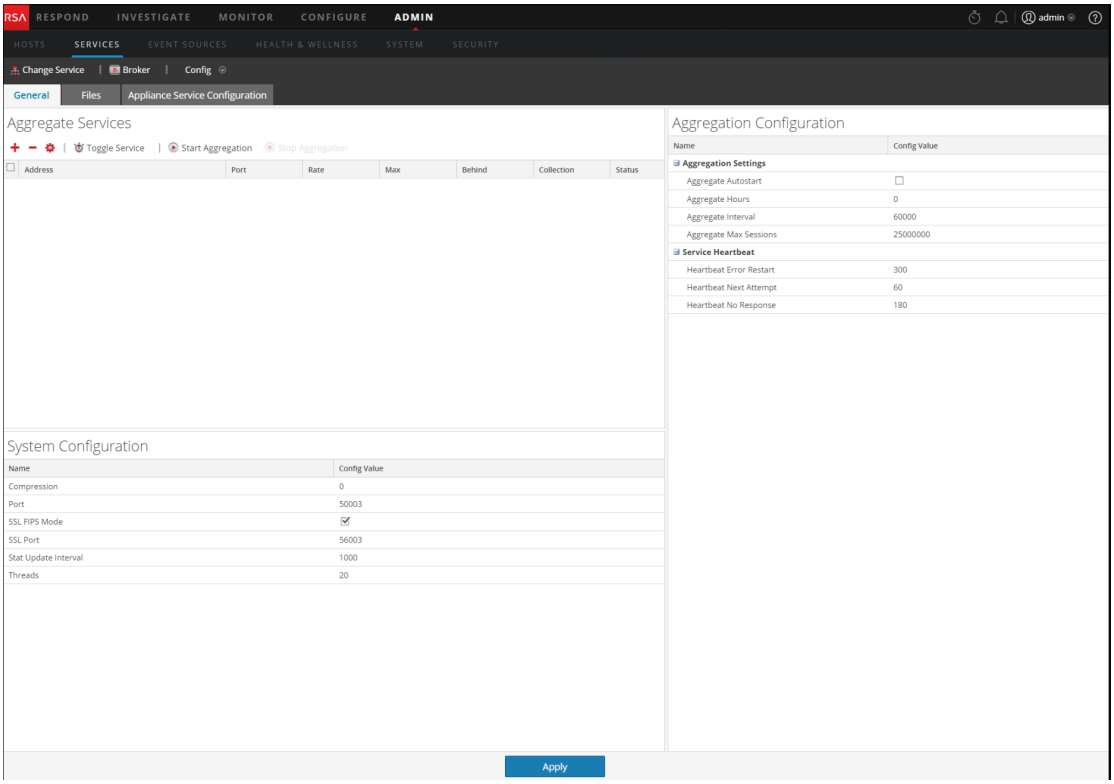
- Adding, editing, and deleting Concentrators and Decoders as aggregate services
- Toggling an aggregate service online and offline



Add Aggregate Services to a Broker or Concentrator

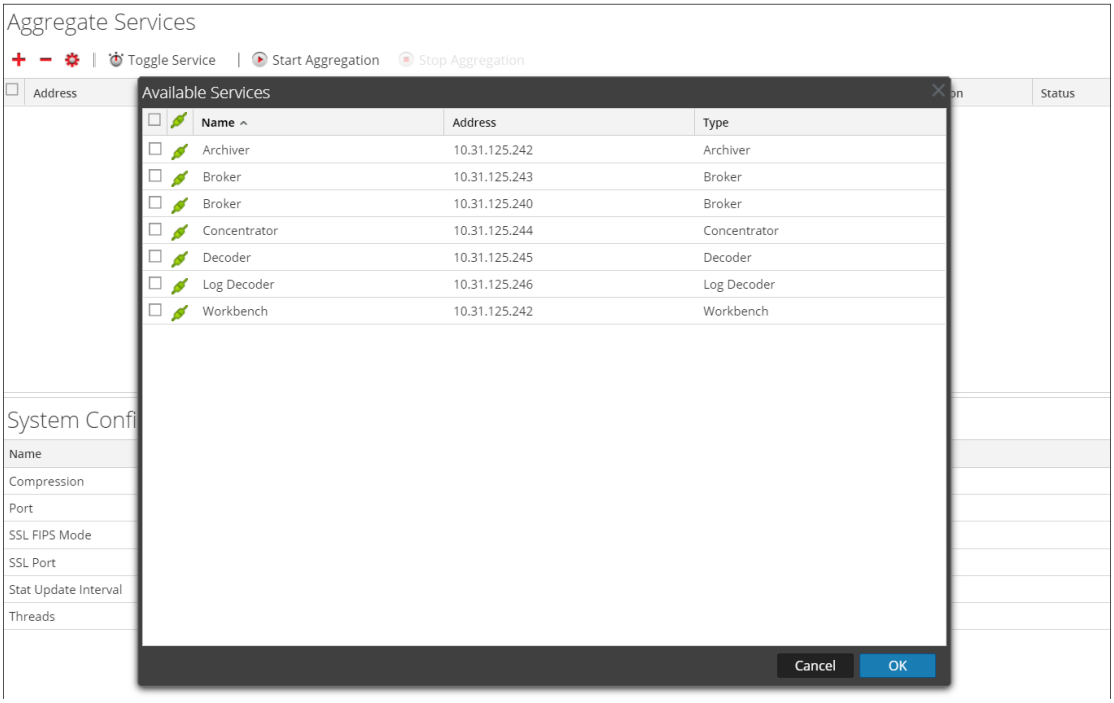
1. In the **main menu** menu, select **ADMIN > Services**.
2. In the **ADMIN Services** view, select a Broker or Concentrator, and select **> View > Config.**

The Services Config view for the selected service is displayed.

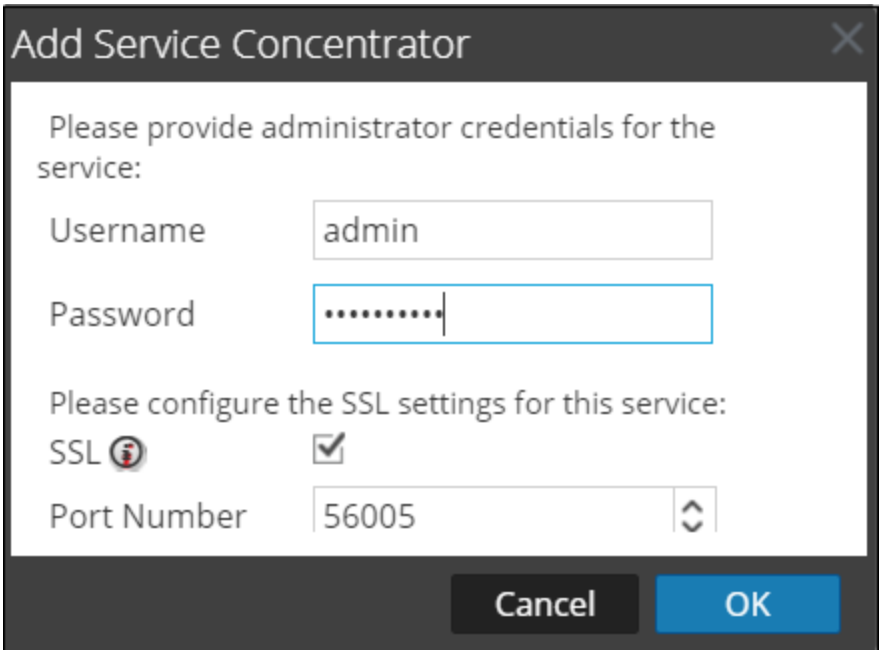


3. Click + in the **Aggregate Services** toolbar.

The Available Services dialog is displayed.



4. Select one or more services to be added and click **OK**.
5. Enter the Administrator username and password to authenticate adding a service.



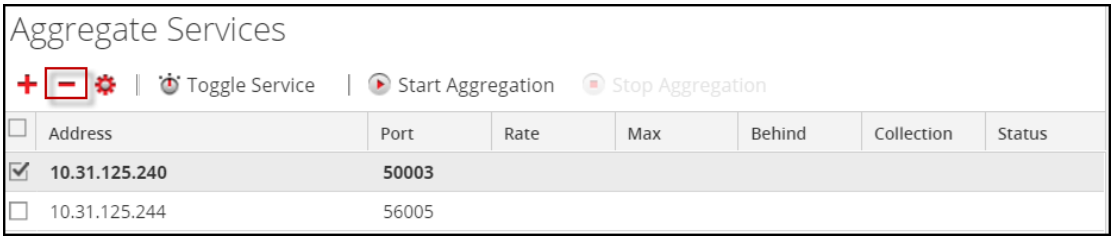
The added services are listed in the Aggregate Services list.

6. To save the changes, click **Apply**.

Remove Aggregate Services from a Broker or Concentrator

Note: This option applies only to offline services. If the aggregate service is online, you must first toggle the service offline.

1. In the **Aggregate Services** list, select one or more services.
2. Click − in the toolbar.



The service is removed from Aggregate Services list.

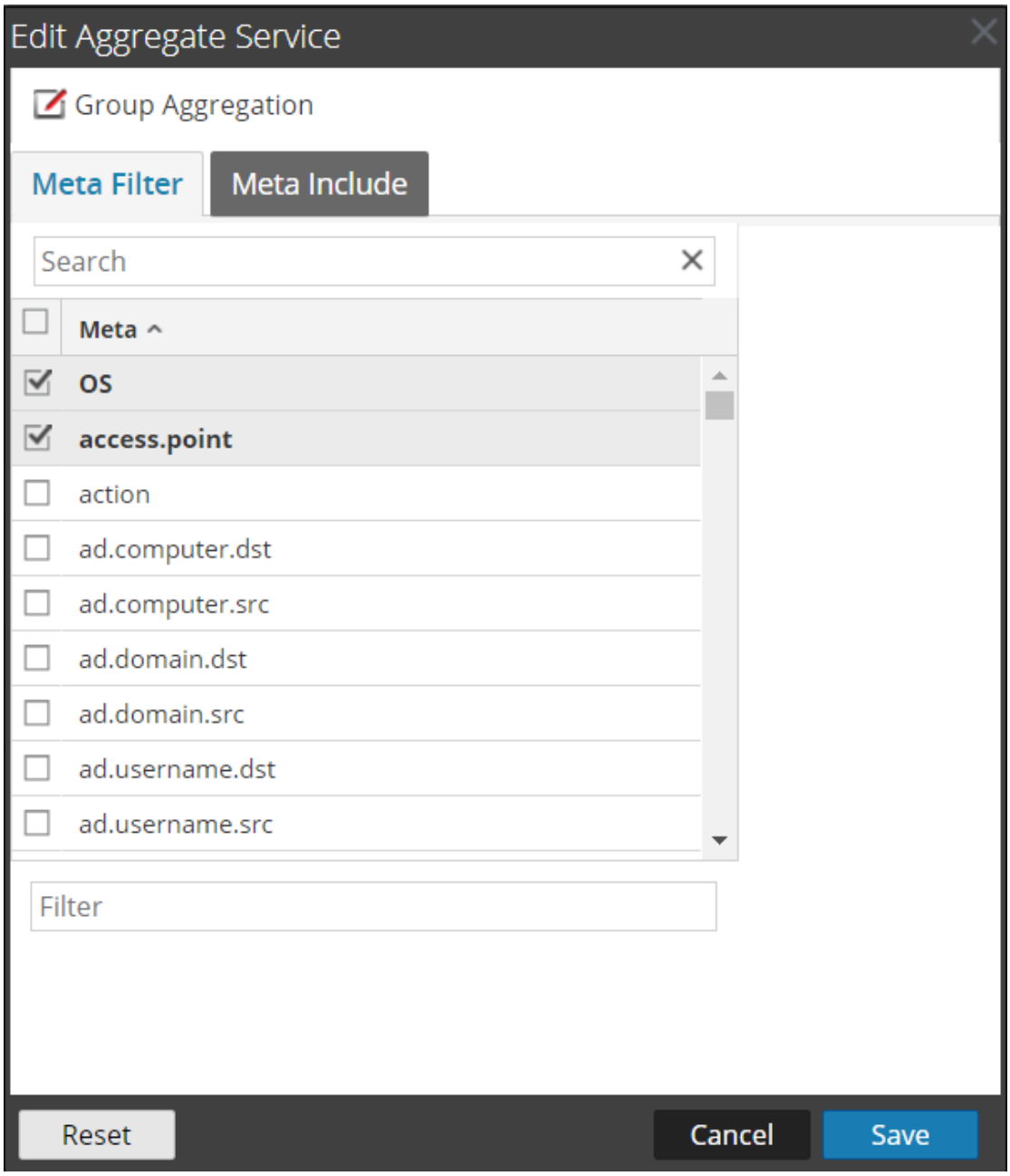
3. To save the change, click **Apply**.

Edit Aggregate Services on a Concentrator

Note: This option applies only to offline services. If the aggregate service is online, you must first toggle the service offline. You can edit only one service at a time.

You can limit the data being consumed from an aggregate service using meta fields and filters. To configure this:

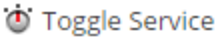
1. Click **Change Service** to change the service to Concentrator.
2. In the **Aggregate Services** list, select one or more services.
3. Click in the toolbar. Enter the authentication information in the pop up dialog box.
   - If the service was added on a different instance of NetWitness Suite, you must add it to this instance of NetWitness Suite in order to edit. A warning dialog allows you to add the service. If you click **Yes**, the Add Service dialog is displayed.
   - If the service is online, a dialog notifies that the service must be offline and requests confirmation that you want to continue. If you click **Yes**, NetWitness Suite takes the service offline and the Edit Aggregate Service dialog is displayed.
   - If the service is offline, the Edit Aggregate Service dialog is displayed with the editable properties for an aggregate service on a Concentrator.
4. Click a type of metadata in the **Meta Include** tab to select the type of metadata for the Concentrator to consume from this service. Click **Save**.



5. To specify a rule to filter data that the Concentrator consumes from this service, compose a rule in the **Meta Filter** tab. Click **Save**.
6. Click **Close**.
   The Edit Aggregate Service dialog closes and the changes are shown in the Aggregate Services list. In this example, two meta were selected on the Meta Include tab. When you click the information icon in the Meta Include field, it shows the selections.
7. To save the changes, click **Apply**.

Toggle a Service

When data aggregation starts, Brokers and Concentrators consume data from aggregate services that are online. When first added to a Broker or Concentrator, aggregate services are offline. To toggle a service between online and offline:

1. Select a service in the **Aggregate Services** list.
2. Click 

.

   The status is changed.

Step 4. (Optional) Configuring Group Aggregation

You use Group Aggregation to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them. You can configure multiple Archiver services or Concentrator services to efficiently aggregate from multiple Log Decoder services to improve query performance on the data:

- Stored in the Archiver.
- Processed through the Concentrator.

RSA Group Aggregation Deployment Recommendations

RSA recommends the following deployment for Group Aggregation.

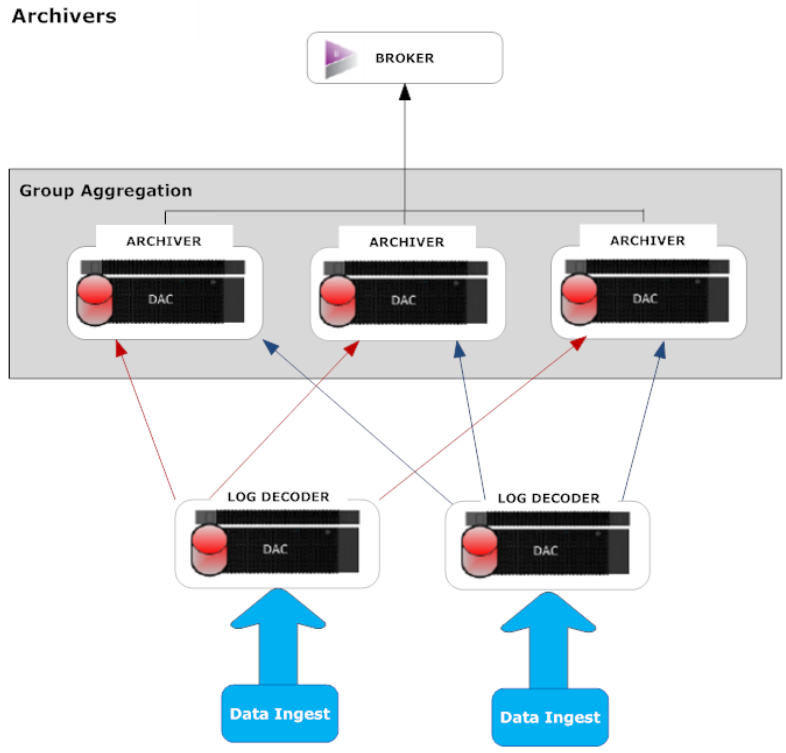
- 1 - 2 Log Decoders
- 3 - 5 Archivers or Concentrators

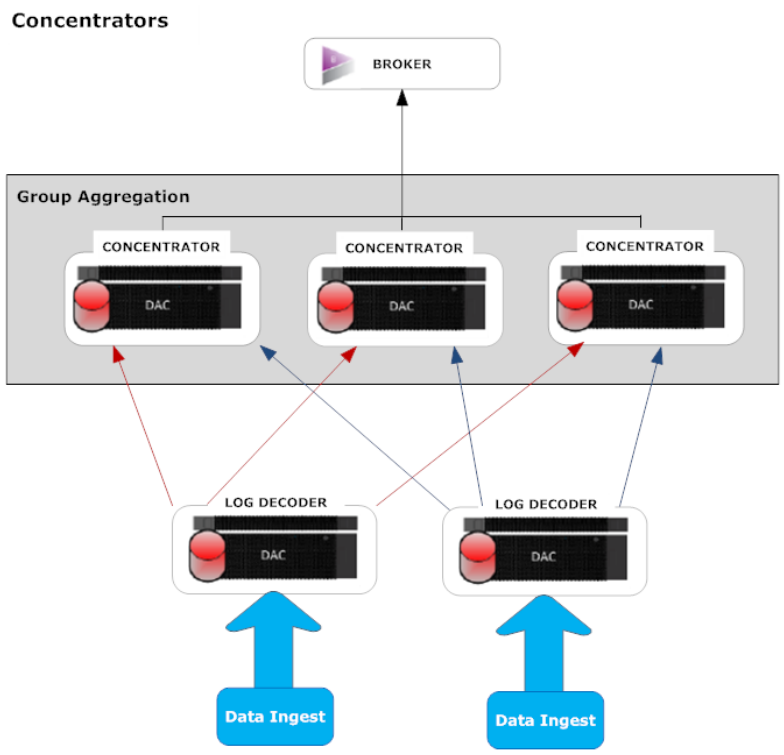
Advantages of Using Group Aggregation

Group Aggregation:

- Increases the speed of Security Analytics queries.
- Improves the performance of aggregate queries (Count and Sum) on the environment.
- Enhances investigation service performance.
- Gives you the option of storing data for a longer duration for investigation purposes.

The following diagram illustrates Group Aggregation.


Archivers
BROKER
Group Aggregation
ARCHIVER
ARCHIVER
ARCHIVER
DAC
DAC
DAC
LOG DECODER
LOG DECODER
DAC
DAC
Data Ingest
Data Ingest


Concentrators
BROKER
Group Aggregation
CONCENTRATOR
CONCENTRATOR
CONCENTRATOR
DAC
DAC
DAC
LOG DECODER
LOG DECODER
DAC
DAC
Data Ingest
Data Ingest

You can have any number of Archivers or Concentrators grouped together and form an aggregation group. The Archiver or Concentrator services in the group divide all the aggregated session between them based on the number of sessions defined in the Aggregate Max Sessions parameter.

For example, in an aggregation group containing two Archiver services or two Concentrator services with the Aggregate Max Sessions parameter set to 10000 the services would divide the session between themselves as illustrated in the following table.

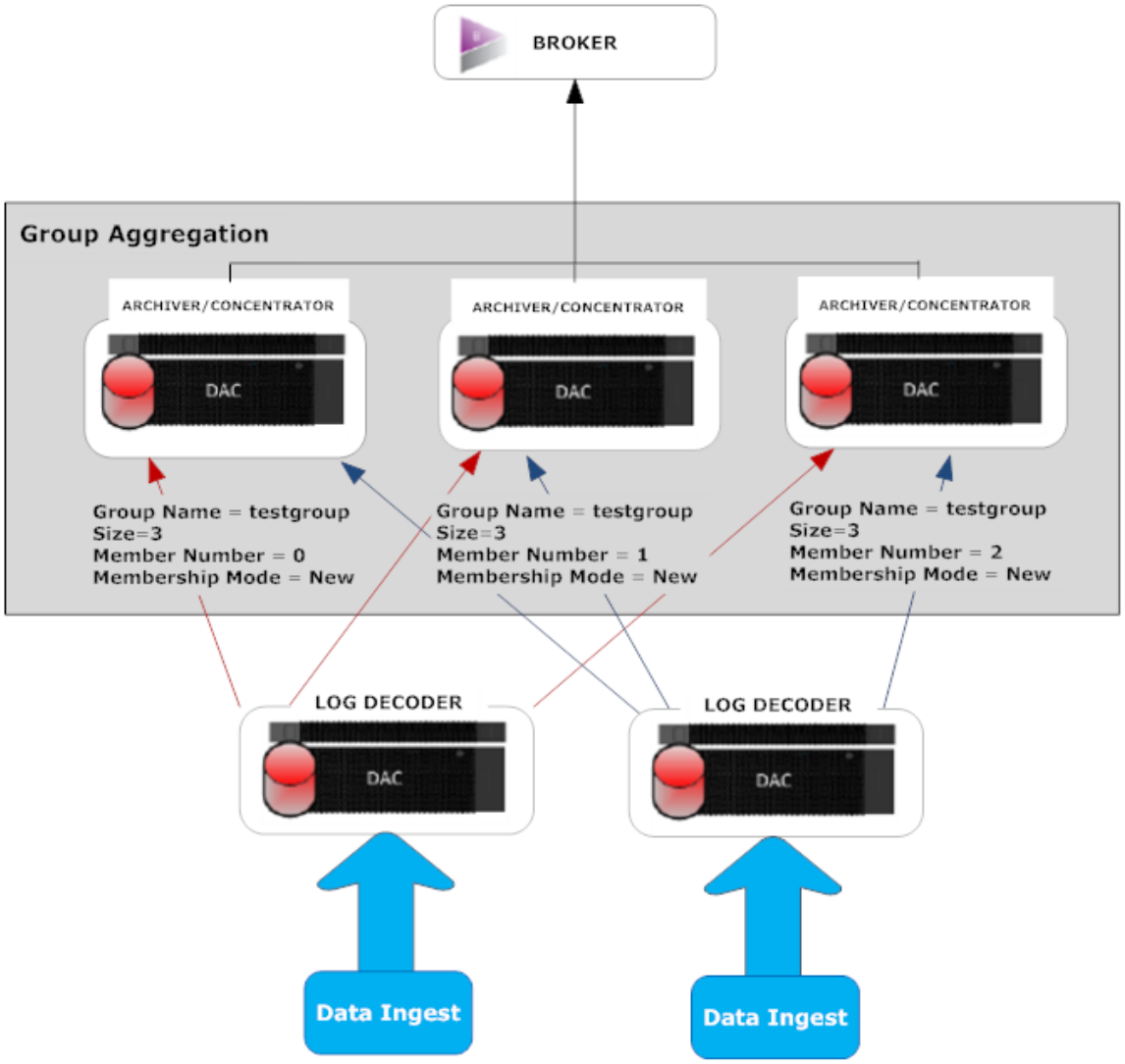
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

Configure Group Aggregation

Complete this procedure to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.

Prerequisites

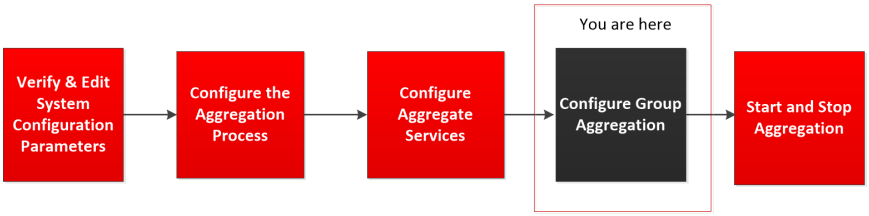
Plan the network design for group aggregation. The following figure is an example of a group aggregation setup.



Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

Parameter	Description
Group Name	It determines the group to which the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All Archiver or Concentrators services in the group should have the same group name.

Size	It determines the number of Archiver or Concentrator services in the aggregation group.
Member Number	It determines the position of the Archiver or Concentrator in the aggregation group. For a group of size N, member number from 0 to N-1 must be set on each of the Archiver or Concentrators services in the aggregation group. For example: If the size of the aggregation group is 2, the member number of one of the Archiver or Concentrator service should be set to 0 and the member number of the other Archiver or Concentrator should be set to 1.
Membership Mode	There are two membership modes: New and Replace. New: Adding a new Archiver or Concentrator service as a member to the existing aggregation group or creating an aggregation group. The Archiver or Concentrator service does not aggregate any existing sessions from the service as other members of the group would have already aggregated all the sessions on the service. This Archiver or Concentrator service will only aggregate new sessions as they appear on the service. Replace: Replacing an existing aggregation group member. The Archiver or Concentrator will begin aggregation from the oldest session available on the service it is aggregating from. **Note:** This parameter has an effect only when no sessions have been aggregated from the service. After some sessions are aggregated, this parameter has no effect.



Set up Group Aggregation

Complete the following procedure to set up group aggregation.

1. Configure multiple Archiver or Concentrator services in your environment. Make sure that you add the same Log Decoder as data source to all the services.
2. Perform the following on all the Archiver or Concentrator services that you want to be part of aggregation group:

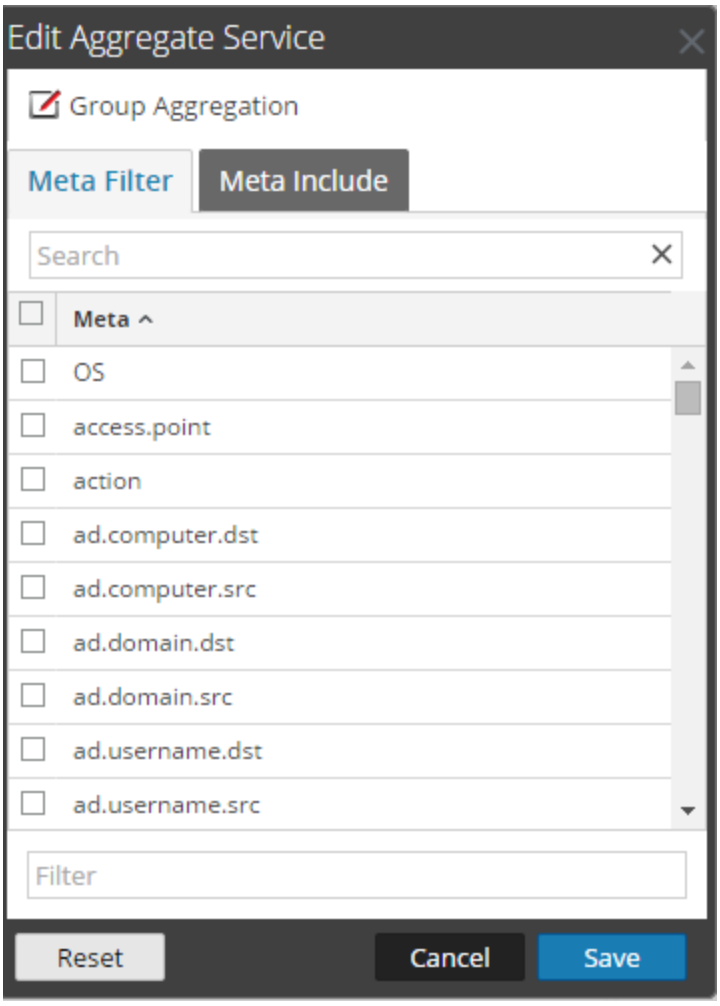
a. In the **main menu**, select **ADMIN > Services**.

b. Select the Archiver or Concentrator service, and in the **Actions** column, select **View > Config**.
The Device Config view of the Archiver or Concentrator is displayed.

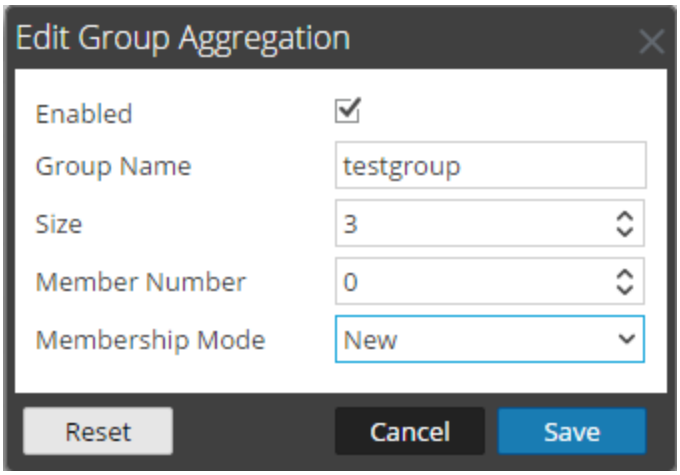
c. Under **Aggregate Services** section, select the Log Decoder device.

d. Click Toggle Service to change the status of the Log Decoder to offline if it is online.

e. Click .
The **Edit Aggregate Service** dialog is displayed.



f. Click Group Aggregation.
The **Edit Group Aggregation** dialog is displayed.



g. Select the **Enabled** checkbox and set the following parameters:

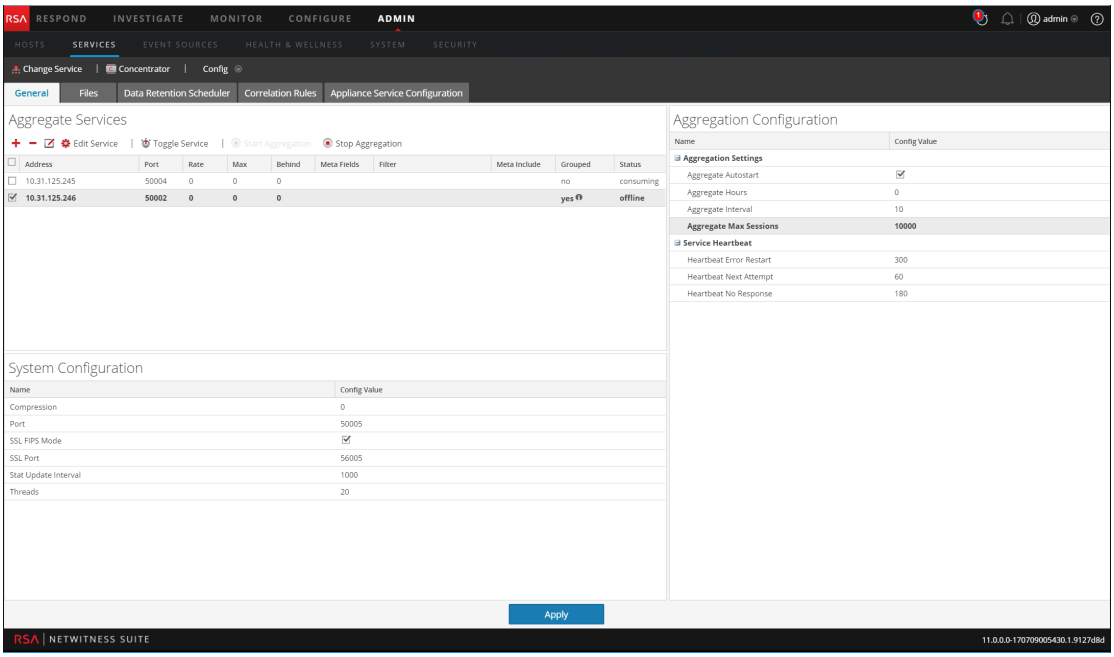
   In the **Group Name** field, type the group name.
   In the **Size** field, select the number of Archiver or Concentrator services in the aggregation group.
   In the **Member Number** field, select the position of the Archiver or Concentrator in the aggregation group.
   In the **Membership Mode** drop-down menu, select the mode.

h. Click **Save**.

i. In the Device Config View page, click **Apply**.

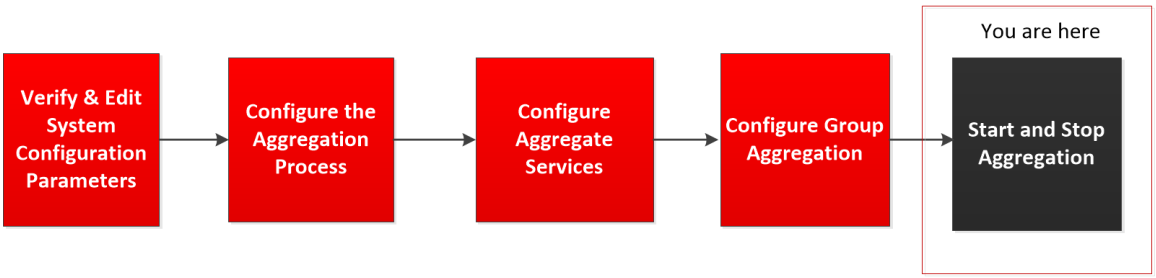
j. Perform **Step b** to **Step i** on all other Archiver or Concentrator services that need to be part of group aggregation.

3. In the **Aggregation Configuration** section, set the **Aggregate Max Sessions** parameter set to **10000**.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Config
General
Files
Data Retention Scheduler
Correlation Rules
Appliance Service Configuration
Aggregate Services
Edit Service
Toggle Service
Start Aggregation
Stop Aggregation
Address
Port
Rate
Max
Behind
Meta Fields
Filter
Meta Include
Grouped
Status
10.31.125.245
50004
0
0
0
no
consuming
10.31.125.246
50002
0
0
0
yes
offline
Aggregation Configuration
Name
Config Value
Aggregation Settings
Aggregate Autostart
Aggregate Hours
0
Aggregate Interval
10
Aggregate Max Sessions
10000
Service Heartbeat
Heartbeat Error Restart
300
Heartbeat Next Attempt
60
Heartbeat No Response
180
System Configuration
Name
Config Value
Compression
0
Port
50005
SSL FIPS Mode
SSL Port
56005
Stat Update Interval
1000
Threads
20
Apply
RSA | NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

Step 5. Start and Stop Aggregation

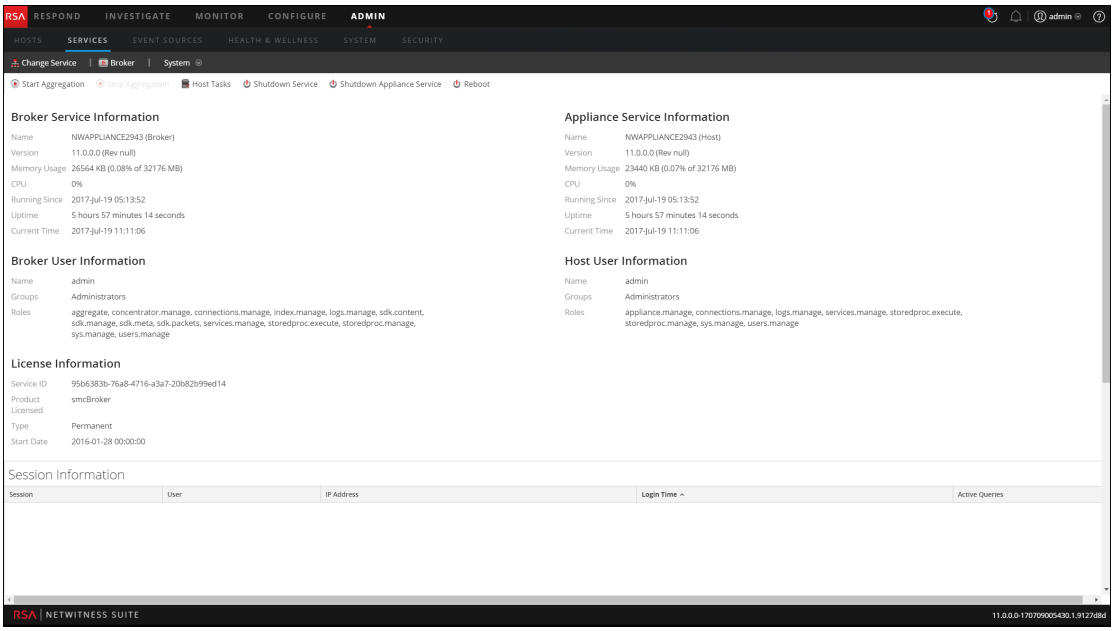
When a Broker or Concentrator starts up, it automatically begins aggregating data if Aggregate Autostart is enabled. When autostart is not enabled, you can start and stop data aggregation manually.



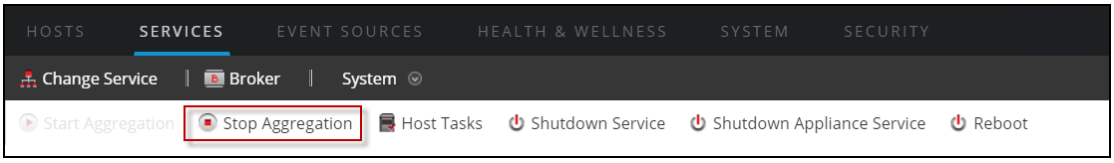
Note: The Aggregate Configuration Settings in the Services Config View for a Broker or Concentrator determine whether Aggregate Autostart is enabled, as well as the size of a round of aggregation and time between rounds.

Start and Stop Data Aggregation in the Services System View

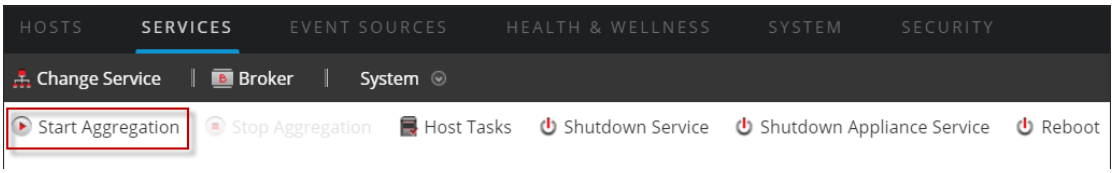
1. In the **main menu**, select **ADMIN > Services**.
2. In the **ADMIN Services** view, select a Broker or Concentrator, and select > **View** > **System.**



3. To stop a Broker or Concentrator that is capturing data, click **Stop Aggregation** in the toolbar.
   The service stops aggregating data and the **Stop Aggregation** option in the toolbar is unavailable. The **Start Aggregation** option becomes active.

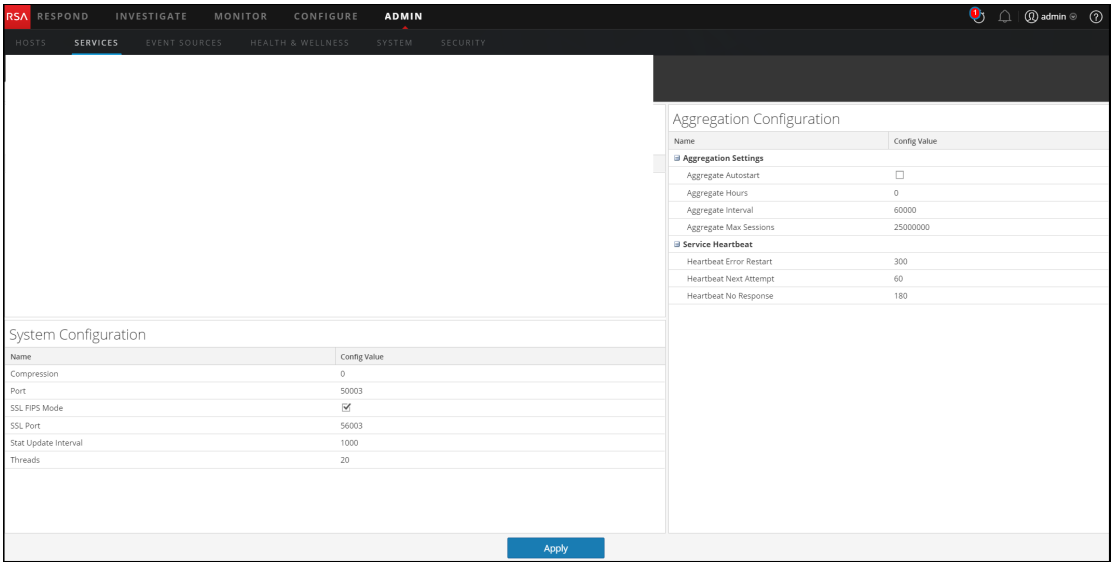


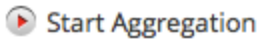
4. If you want the service to start aggregating data again, click **Start Aggregation**.
   You can now investigate the captured data in the Investigation module.



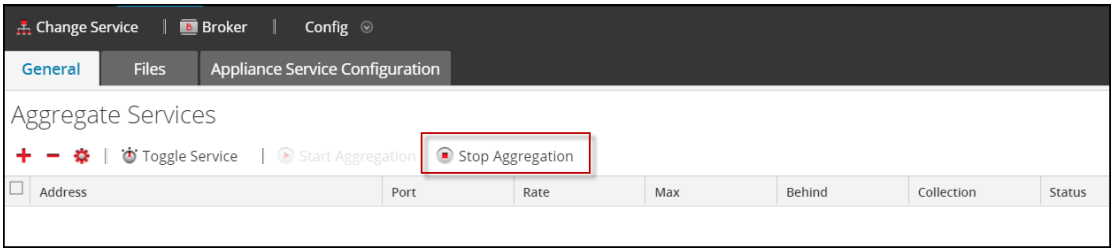
Start and Stop Aggregation in the Services Config View

1. In the **main menu**, select **ADMIN > Services**.
2. In the **Admin Services** view, select a Broker or Concentrator, and select **> View > Config**.
   The Services Config view, which includes the Aggregate Services section, is displayed.



3. To start aggregation on the selected Broker or Concentrator, click  in the **Aggregate Services** toolbar.
   When aggregation starts, the status of all online aggregate services changes to **consuming**. The Start Aggregation button is disabled and the Stop Aggregation button is enabled.

4. To stop aggregation, click in the **Aggregate Services** toolbar.
   When aggregation stops, the status of all consuming aggregate services changes to **online**. The Stop Aggregation button is unavailable and the Start Aggregation button is available.



Broker and Concentrator Configuration References

You can configure Brokers and Concentrators using the NetWitness Suite user interface.

In addition to the views described here, you can view the complete service nodes in a tree form in the Services Explore view, see the "Services Explore View" topic in the *Hosts and Services Getting Started Guide*.

Topics

- Services Config View - Broker/Concentrator General Tab
- Services System View - Broker

Services Config View - Broker or Concentrator General Tab

The General tab for a Broker or Concentrator in the Services Config helps manage basic service configuration, configure the aggregate service, and configure the aggregation process between a Broker or Concentrator and the aggregate service.

Configuring the aggregate service (whose data is consumed and aggregated) includes:

- Adding, editing, and deleting Concentrators and Brokers as aggregate services
- Toggling an aggregate service online and offline
- Monitoring statistics for aggregate services
- Starting and stopping aggregation

Configuring the aggregation process includes setting:

- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service

What do you want to do?

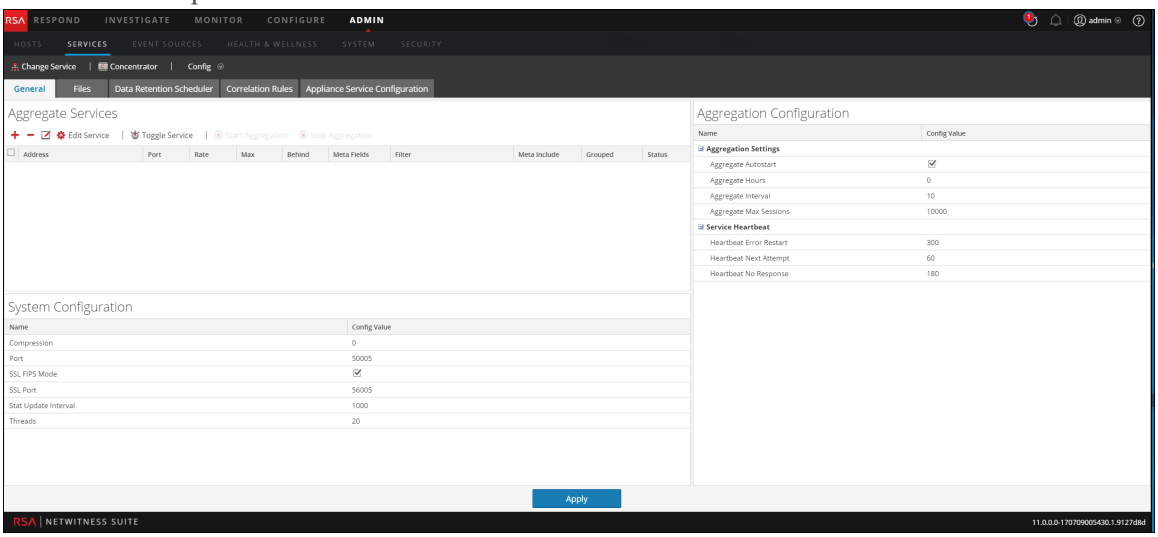
Role	I want to...	Refer to...
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Aggregate Services Section
Administrator	Manage System Configuration	System Configuration Section

Related Topics

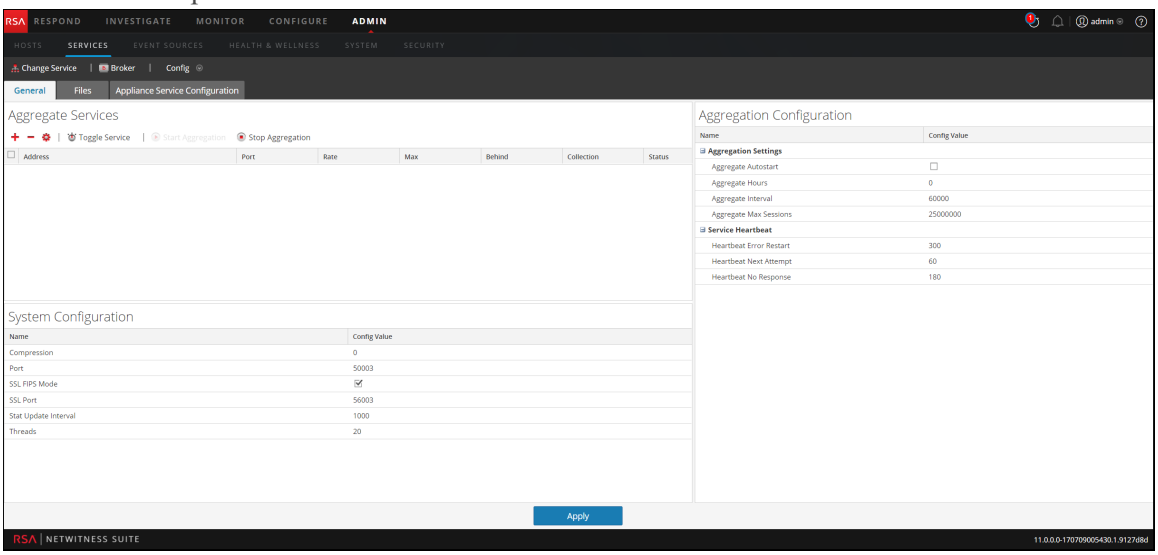
- Broker and Concentrator Basics
- Broker and Concentrator Configuration

General tab

This is an example of the General tab for a Concentrator.



This is an example of the General tab for a Broker.

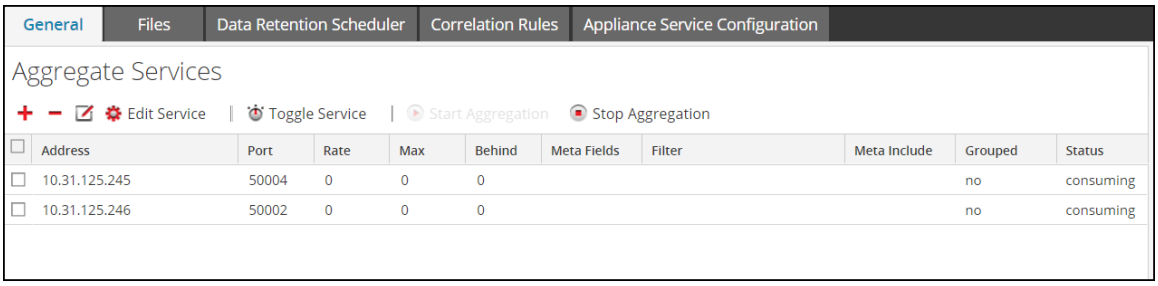


These are the three major sections in the General tab for Brokers and Concentrators:

- Aggregate Services
- System Configuration
- Aggregation Configuration

Aggregate Services Section

The Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service. This is an example of the Aggregate Services section for a Concentrator.



The Aggregate Services section toolbar offers these options.

Option	Description
+	Opens a dialog in which you can add a Concentrator, Decoder, or Log Decoder as an aggregate service.
−	Removes the selected aggregate service.
	For Concentrators only, opens a dialog to edit **Meta Fields** and **Filter** values for the Concentrator.
Edit Service	Enables you to enter the administrator credentials of the selected aggregate service so that it can communicate with the Broker or Concentrator.
Start Aggregation	When aggregation has been stopped or has not started, starts aggregating data from the online service in the list using the rules defined for the service.
Stop Aggregation	When aggregation is in progress, stops aggregation on the Broker or Concentrator. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.
Toggle Service	Toggles the state of a service between offline and online. Only data from online service is consumed during aggregation.

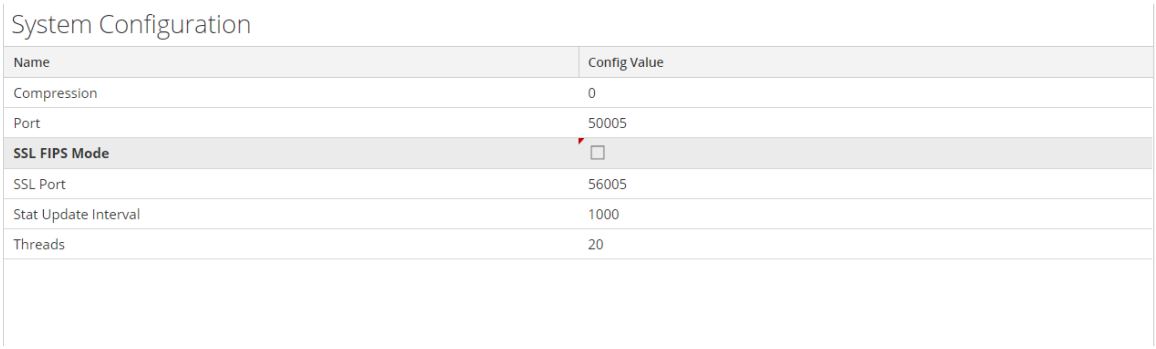
The Aggregate Services section list has these columns.

Column	Description
Address	Lists the address of the service.
Port	Lists the port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
Rate	Lists the number of metadata objects being written to the database per second. Values are rolling average samples over a short time period (10 seconds). After capture stops, the rate is reset to **0**.
Max	Lists the maximum number of metadata objects written to the database per second since capture started. Values are rolling average samples over a short time period (10 seconds). After capture stops, **Max** continues to show the maximum value during capture.
Behind	Lists the number of sessions on the service that need to be aggregated.
Collection	For Brokers only, indicates the collection that was selected when the Analyst Workbench service was added to the Aggregate Services section.
Meta Fields	For Concentrators only, lists the types of metadata being consumed by the aggregate service.
Filter	For Concentrators only, a rule expression (as used in a 'where' clause) can be used to filter the results. You must add a meta key along with an operator and a value, for example `ip.src !=127.0.0.1 && word exists`

Column	Description
Meta Include	For Concentrators only, lists the number of types of meta included in the aggregate service.
Grouped	Whether or not the aggregate service is part of a group.
Status	Lists the current status of the service: • online = available to provide data for consumption by the Broker or Concentrator • offline = not available to provide data for consumption by the Broker or Concentrator • consuming = providing data for consumption by the Broker or Concentrator

System Configuration Section

The System Configuration section manages service configuration for a service. When a service is first added, default values are in effect. You can edit these values to tune performance.



The System Configuration section has these parameters.

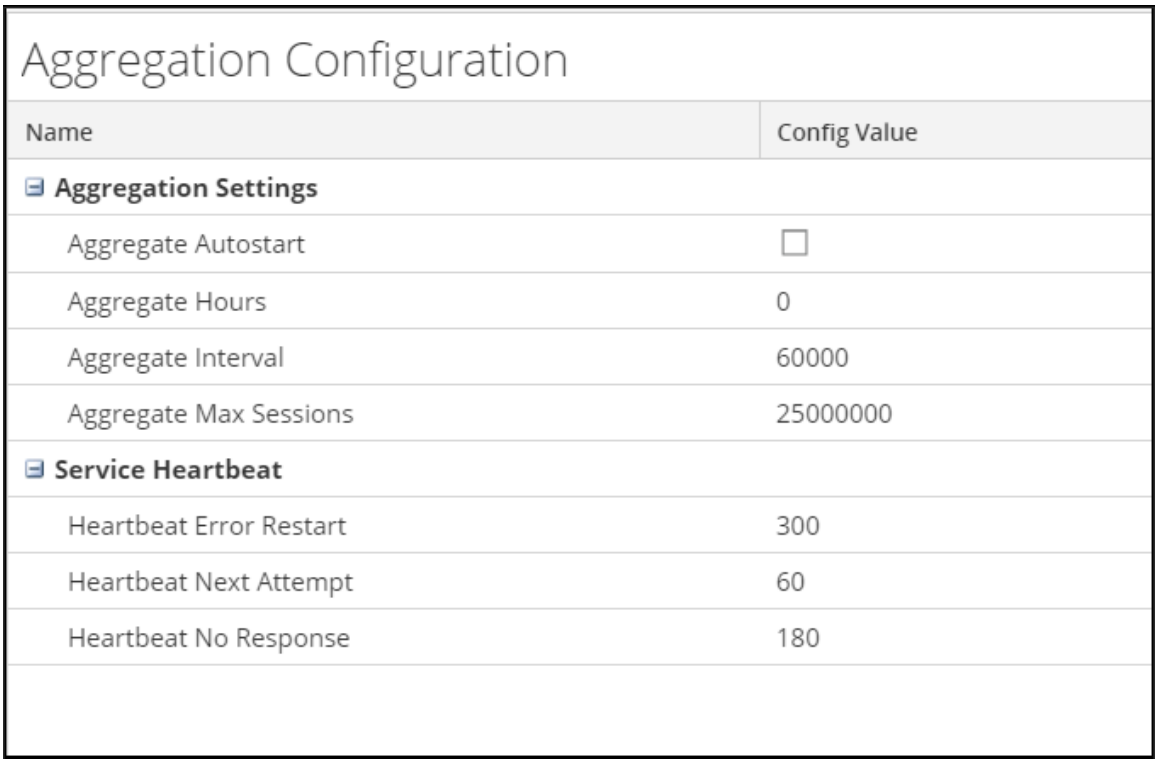
Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of **0** disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.

Parameter	Description
Port	The port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
SSL FIPS Mode	When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
SSL Port	Indicates the SSL port.
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of **0** lets the system decide. The default value is **15**. A change takes effect on service restart.

Aggregation Configuration Section

The Aggregation Configuration section provides configuration settings that affect various aspects of the aggregation process. When you click **Apply**, the changes are saved; however, not all settings take effect immediately. The tables for Aggregation Settings and Service Heartbeat provide details.

Caution: Do not change any of these settings unless guided by the Developers or the Customer Support team. Contact the Customer Support, for any questions before editing any of these settings.



Aggregation Settings

Setting	Description
Aggregate Autostart	Option to start aggregation automatically each time the Broker or Concentrator is started. Checked means yes, unchecked means no. This change takes effect immediately.

Setting	Description
Aggregate Hours	The number of hours back for each service that the Concentrator or Broker attempts to recover at the beginning of aggregation. This change takes effect immediately. • If the value is set to 0, aggregation for each service starts where it last left off, no matter the number of hours behind. • If the value is any positive integer, the Concentrator or Broker only consumes sessions less than that number of hours back. For example, if a service's most current session is +10 hours from the last session, this is what happens with two different Aggregate Hours values: • With a value of 12, the Concentrator or Broker starts consuming where it left off. • With a value of 4, all sessions between 5 and 10 hours back are skipped and the Concentrator or Broker starts consuming the session that started 4 hours back.
Aggregate Interval	The number of milliseconds between rounds of service aggregation. All services managed by the Broker or Concentrator request additional rounds of session and metadata to be aggregated. If a Broker or Concentrator is still consuming the previous round of data, it cannot request more until it finishes. Change takes effect immediately.
Aggregate Max Sessions	The maximum number of sessions that the Broker or Concentrator requests in a given round of data aggregation. Change takes effect after restart.

Service Heartbeat

In communicating with each aggregate service, Brokers and Concentrators monitor the heartbeat of the service. These parameters specify the timing of the first attempt to reconnect to a service after an error, the next attempt to reconnect, and taking the service offline after failure to reconnect.

Setting	Description
Heartbeat Error Restart	After a heartbeat error is detected on an aggregate service, specifies the number of seconds for a Broker or Concentrator to wait before attempting a service reconnect.
Heartbeat Next Attempt	After a failed attempt to reconnect to an aggregate service, specifies the number of seconds for a Broker or Concentrator to wait before attempting another service reconnect. Change takes effect immediately.
Heartbeat No Response	After failing to reconnect to an unresponsive service, specifies the number of seconds for the Broker or Concentrator to wait before taking the unresponsive service offline. Change takes effect immediately.

When editing parameters in the General tab, you must click **Apply** to save changes.

Services System View - Broker or Concentrator

The Services System view displays information specific to specific to Brokers and Concentrators.

While information displayed in this view is the same for all types of Core services, several options in the toolbar are relevant only for Brokers and Concentrators.

What do you want to do?

Role	I want to...	Refer to...
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Services System View - Broker or Concentrator
Administrator	Manage System Configuration	Services System View - Broker or Concentrator

Related Topics

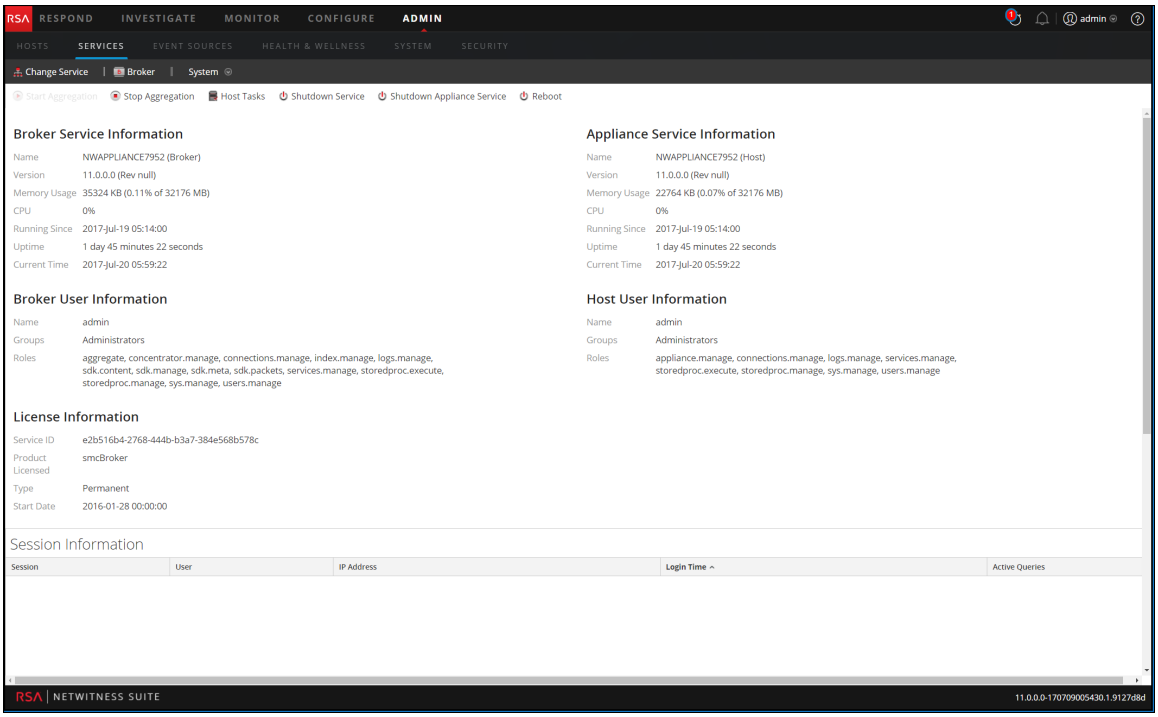
- Broker and Concentrator Basics
- Broker and Concentrator Configuration

Services System View

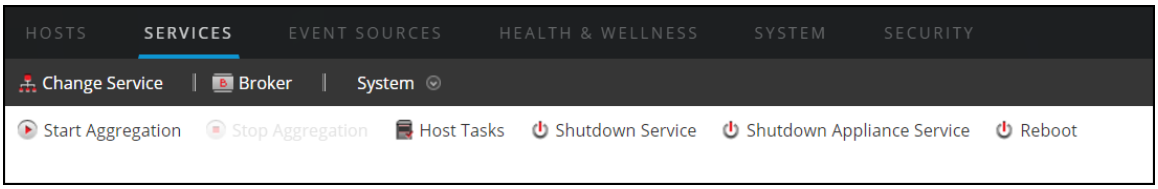
You can access this view by doing the following:

1. In the **main menu**, select **ADMIN > Services.**
2. Select a Concentrator or Broker, and select **> View > System**.

   The System view for the selected Concentrator or Broker is displayed.



The following figure is an example of the toolbar for a Broker or Concentrator.



Host Tasks, Shutdown Service, Shutdown Appliance Service or (Shutdown Appliance), and Reboot are common to all services and are described in the **Services System view** topic in the *Host and Services Getting Started Guide*.

This table describes toolbar options that apply only to a Concentrator or Broker. Both buttons are unavailable until aggregator services are configured and consuming data.

Action	Description
Start Aggregation	Starts aggregation of data being consumed on a Concentrator or Decoder configured as an aggregation service for the selected Broker or Concentrator. The Start Aggregation button is available only when aggregator services are configured and consuming data.
Stop Aggregation	Stops aggregation of data being consumed on a Concentrator or Decoder configured as an aggregation service for the selected Broker or Concentrator. The Stop Aggregation button is available only when aggregation is occurring.

RSA NETWITNESS® SUITE

Cloud Behavioral Analytics Gateway Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

RSA Cloud Behavioral Analytics 4

Provision a Cloud Gateway 5

Mapping Cloud Gateway Analytic Streams 9

Considerations 9

Analytic Stream Deployment Example - Two Gateways 9

Analytic Stream Deployment Example - One Gateway 10

Prerequisites 12

Create Cloud Gateway Analytic Stream Mappings 12

Deploy Cloud Gateway Analytic Stream Mappings 17

Update a Mapping 17

Undeploy a Mapping 18

Delete a Mapping 18

Change the Lag Time 19

Monitor the Cloud Gateway 20

Cloud Gateway References 22

Cloud Gateway Config View Certificate Tab 23

What do you want to do? 23

Related Topics 23

Certificate Tab 23

Toolbar Actions 26

Cloud Gateway Analytic Stream Mappings 27

Workflow 27

What do you want to do? 28

Related Topics 28

Quick Look 28

Analytic Stream Settings 33

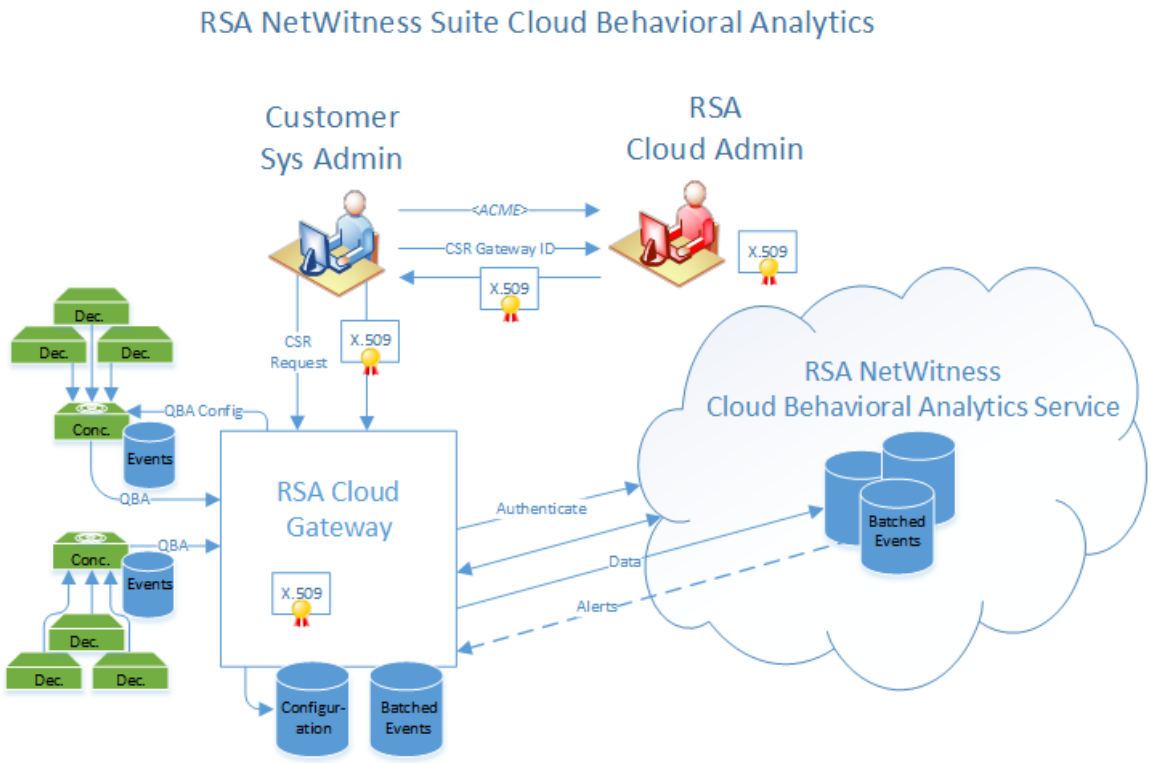
What do you want to do? 33

Related Topics 33

Analytic Stream Settings 33

RSA Cloud Behavioral Analytics

RSA NetWitness® Suite Cloud Behavioral Analytics (CBA) provides the ability to analyze your data in the cloud, instead of on your premises, and send alerts of potential threats. With data analysis in the cloud, RSA Data Scientists can study the effectiveness of the data models used to perform the analysis and update them more frequently to better respond to current threats.



To prepare a secure data connection to the RSA NetWitness Cloud Behavioral Analytics service, you will need to provision the RSA Cloud Gateway service. To do this, you create a Certificate Signing Request (CSR) for the Cloud Gateway. You then provide the CSR and the Gateway ID to the RSA Cloud Administrator. The RSA Cloud Administrator will provide you with a signed certificate for you to install on the NetWitness Suite host where your gateway service is installed. See the following step-by-step instructions to provision the Cloud Gateway.

Note: RSA NetWitness® Suite Cloud Behavioral Analytics is a pre-General Availability release. If you are interested in participating as a design partner to help shape and improve CBA for General Availability, please contact your Sales Representative.

The procedures in this guide should be completed by a NetWitness Suite Administrator.

Provision a Cloud Gateway

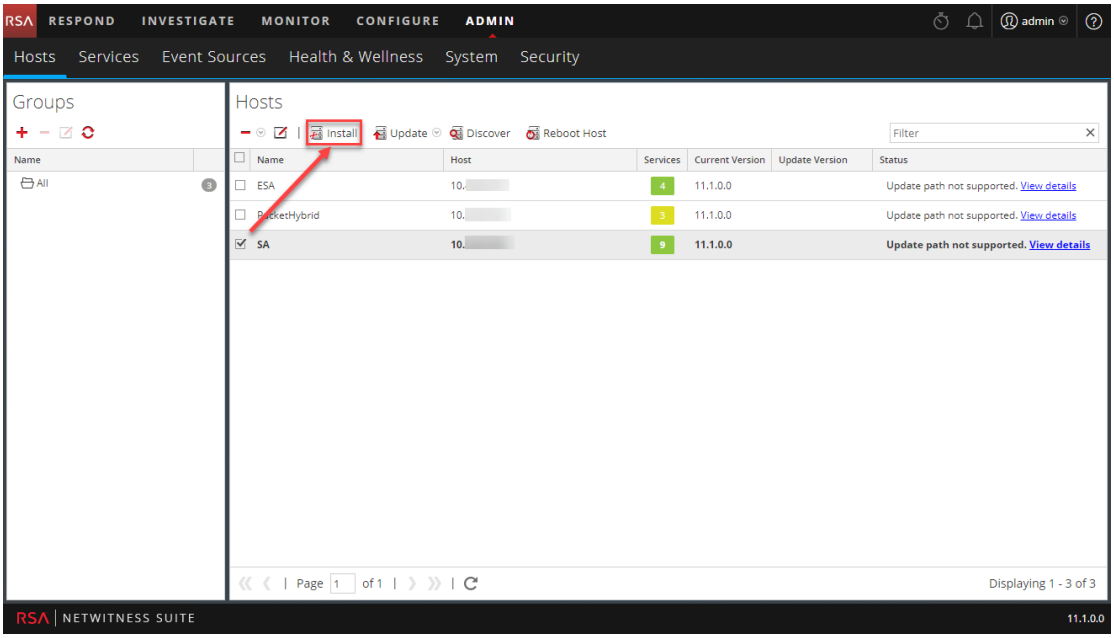
RSA Cloud Gateway Server services must be provisioned before using them for Cloud Behavioral Analytics. This is a one-time procedure per gateway service.

You can install the Cloud Gateway service on any NetWitness Suite host. RSA recommends using a dedicated host that you provision for your Cloud Gateway, but it is not required. The following list shows the preferred locations for the Cloud Gateway in order of preference:

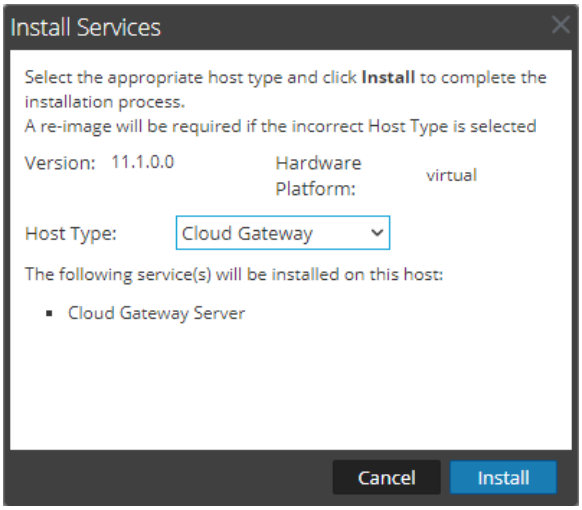
- Provision your own dedicated host
- ESA Host
- NetWitness Server Host

Follow these instructions to install a Cloud Gateway and create a Certificate Signing Request (CSR) for the Cloud Gateway. You will need to provide the CSR and the Gateway ID to the RSA Cloud Administrator. The RSA Cloud Administrator will provide you with a signed certificate to install in your Cloud Gateway service.

1. To install the Cloud Gateway, log in to NetWitness Suite and go to **ADMIN > Hosts**.
2. In the Hosts view, select the NetWitness host where you want to install the Cloud Gateway Server service and click **Install**.

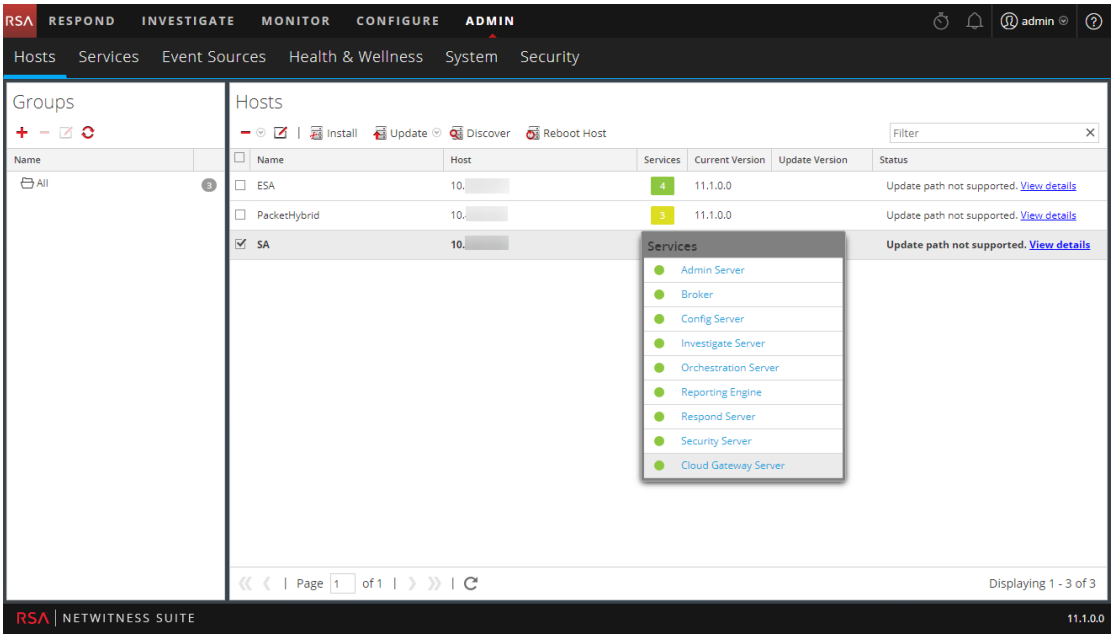


3. In the Install Services dialog, in the **Host Type** field, select **Cloud Gateway**.



4. Click **Install** to install the Cloud Gateway Server on the selected host.

5. To verify the installation, in the Hosts view, click the box in the **Services** column of the selected host.



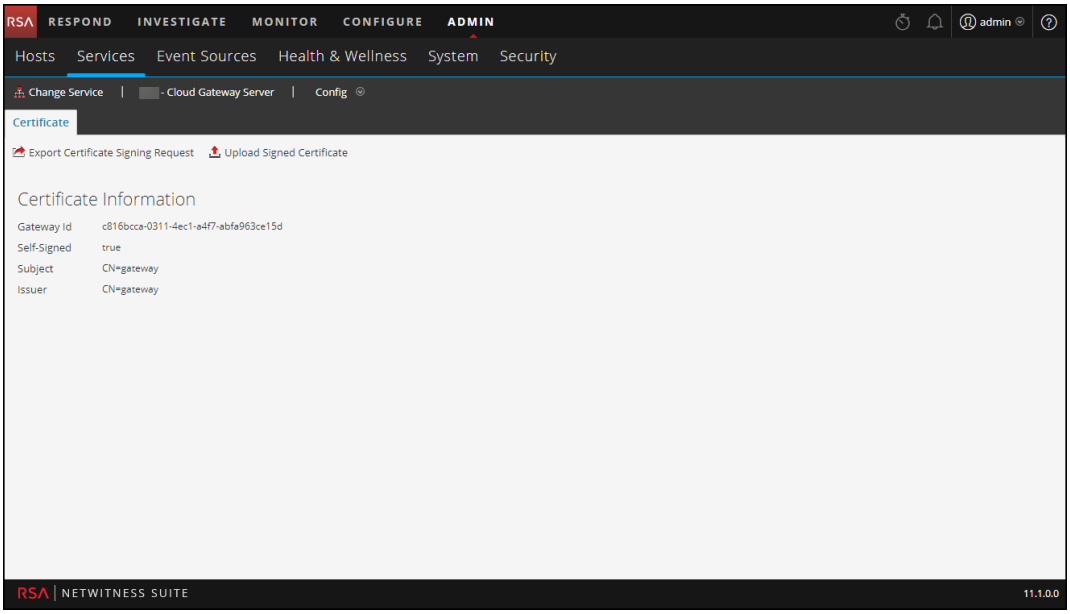
You should see the Cloud Gateway Server service in the services list for that host.

6. Click the **Cloud Gateway Server** service in the list to go to the Services view (**ADMIN > Services**).

7. To get the CSR for the gateway:

   a. In the Services view, select the Cloud Gateway Server service and then select > **View > Config**.

   In the Services Config view, you will see the **Gateway ID** listed.



   b. Click **Export Certificate Signing Request**.

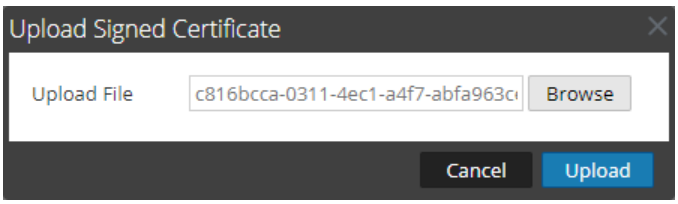
   The service creates and downloads the CSR file for you.

Caution: Do not generate multiple Certificate Signing Requests. The signed certificate file received in step 8 must match the CSR generated in this step. If there is a mismatch, the uploading of the signed certificate file will fail.

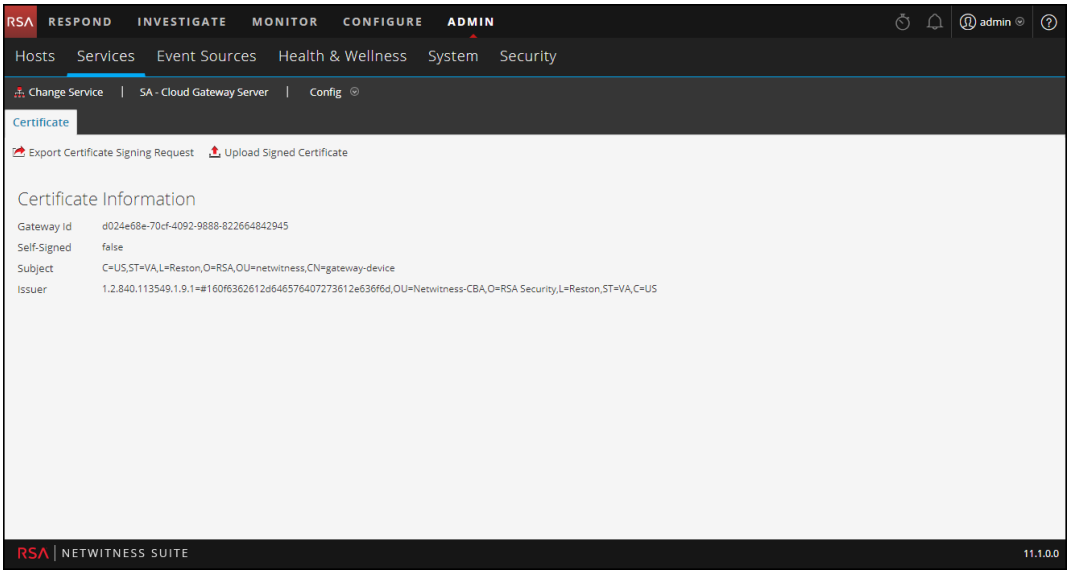
8. Send the CSR file and Gateway ID to the RSA Cloud Administrator, who will provide you with a signed certificate file.
9. Copy the signed certificate file to the NetWitness Suite host where the Cloud Gateway Server service is installed.
10. To install the signed certificate in your Cloud Gateway Server service:

    a. In the Services Config view, click **Upload Signed Certificate**.

    b. In the Upload Signed Certificate dialog, select your signed certificate and click **Upload**.



The following example shows the results of setting the signed certificate on the Cloud Gateway.



After a signed certificate file is properly uploaded to the Cloud Gateway, the **Self-Signed** field shows as **false**, which indicates that the installed certificate is now properly signed by **Netwitness-CBA**.

Mapping Cloud Gateway Analytic Streams

You can configure the RSA Cloud Gateway to automatically upload Analytic Streams from one or more Concentrators to Cloud Behavioral Analytics (CBA). An *Analytic Stream* is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.

When you deploy your mapping, the selected Cloud Gateway service uses query-based aggregation to collect the appropriate filtered events for the selected Analytic Stream from the Concentrators. Query-based aggregation is a predefined query that only transfers data for the selected Analytic Stream. Only the data required by the Analytic Stream is transferred from the Concentrator to Cloud Behavioral Analytics.

Considerations

When creating and deploying your Analytic Stream mappings, keep the following important considerations in mind:

1. Each Analytic Stream that you deploy places an additional load on the Internet egress points on the network.
2. Every Analytic Stream that you add impacts the Concentrators.
3. Ensure that you map Analytic Streams to Concentrators that actively collect that type of information. For example, HTTP Analytic Streams should only be activated on Concentrators that collect HTTP activity.

Analytic Stream Deployment Example - Two Gateways

To take advantage of your additional Concentrator capacity, you can map an Analytic Stream to a Cloud Gateway service and deploy it to analyze data from multiple data sources at the same time.

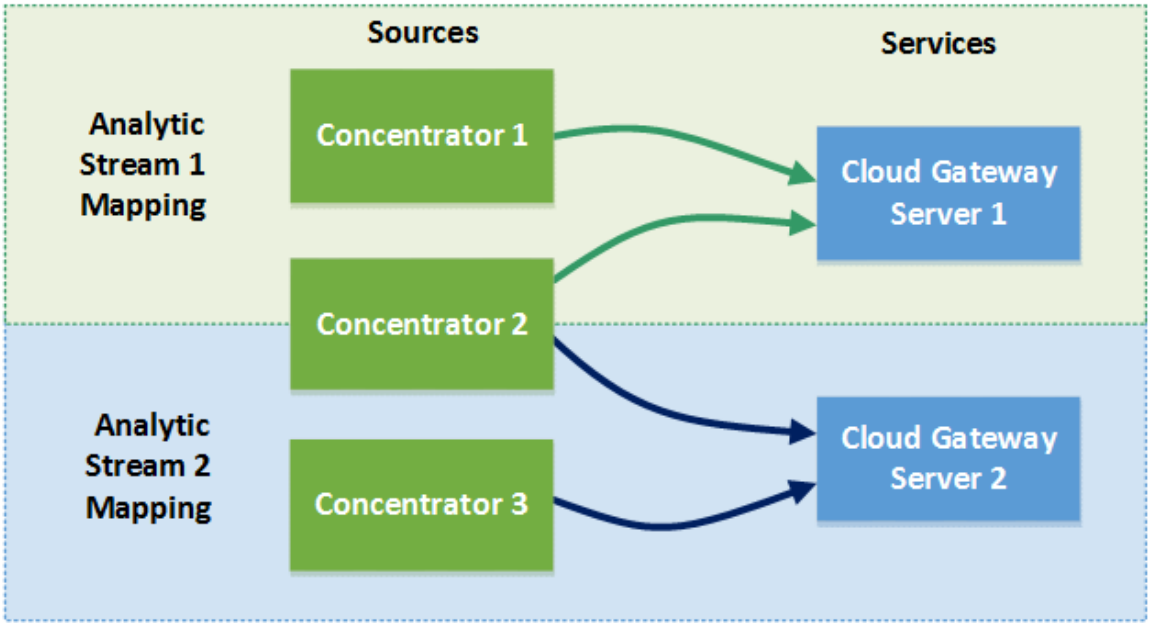
For example, if you have three Concentrators and two Cloud Gateway services, you can create and deploy the following mappings:

- Map Analytic Stream 1 to the Concentrator 1 and 2 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 sends Analytic Stream 1 filtered traffic from Concentrators 1 and 2 to CBA in the Cloud.

- Map Analytic Stream 2 traffic to the Concentrator 2 and 3 sources and the Cloud Gateway Server 2 service. Cloud Gateway Server 2 sends Analytic Stream 2 filtered traffic from Concentrators 2 and 3 to CBA in the Cloud.

In this example, Analytic Stream 1 represents an Analytic Stream, such as HTTP, and Analytic Stream 2 represents another Analytic Stream, such as FTP in another location. Concentrator 1 collects HTTP activity, Concentrator 2 collects HTTP and FTP activity, and Concentrator 3 collects FTP activity.

Analytic Stream Deployment Example – Two Gateways



This example shows how both services can process data from the same Concentrator. Notice that Cloud Gateway services 1 and 2 can both process data from Concentrator 2. Cloud Gateway Server 1 queries data for Analytic Stream 1 HTTP traffic and Cloud Gateway Server 2 queries different data for Analytic Stream 2 FTP traffic.

Analytic Stream Deployment Example - One Gateway

In addition to creating Analytic Stream mappings that are processed by different Cloud Gateway services, you can map more than one Analytic Stream to the same Cloud Gateway service.

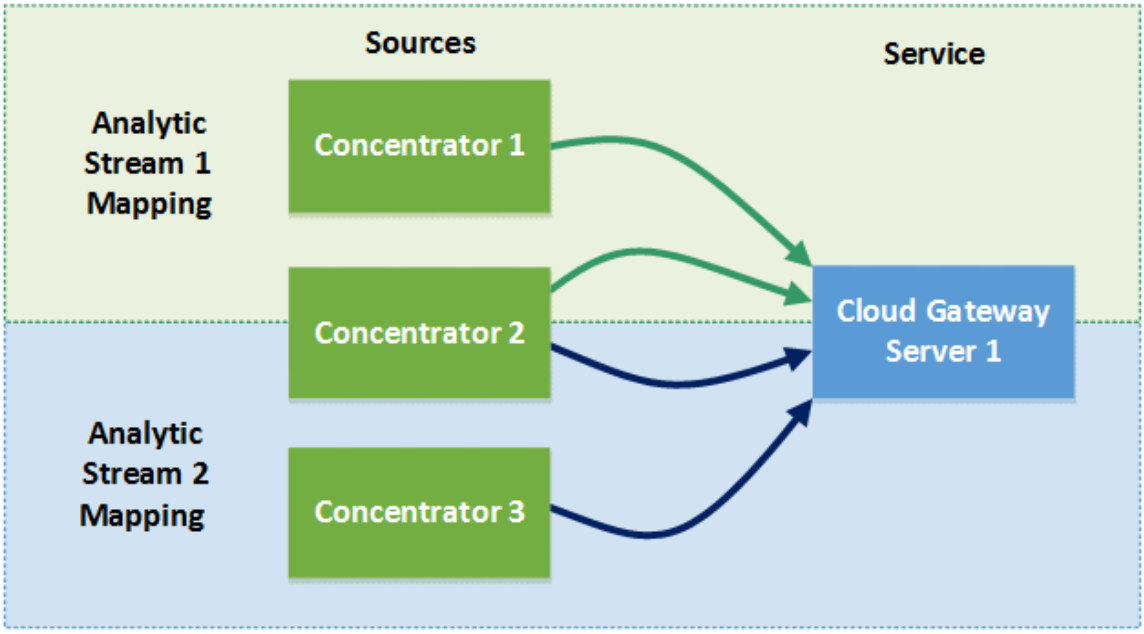
For example, if you have three Concentrators and one Cloud Gateway service, you can create and deploy the following mappings:

- Map Analytic Stream 1 to the Concentrator 1 and 2 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 sends Analytic Stream 1 filtered traffic from Concentrators 1 and 2 to CBA in the Cloud.

- Map Analytic Stream 2 to the Concentrator 2 and 3 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 also sends Analytic Stream 2 filtered traffic from Concentrators 2 and 3 to CBA in the Cloud.

In this example, Analytic Stream 1 represents an Analytic Stream, such as HTTP, and Analytic Stream 2 represents another Analytic Stream, such as FTP in another location. Concentrator 1 collects HTTP activity, Concentrator 2 collects HTTP and FTP activity, and Concentrator 3 collects FTP activity.

Analytic Stream Deployment Example – One Gateway



This example shows how one service can process data from more than one Analytic Stream. Notice that Cloud Gateway Server 1 can process data from Concentrators 1 and 2 for Analytic Stream 1. It also processes data from Concentrators 2 and 3 for Analytic Stream 2. Cloud Gateway Server 1 queries data for Analytic Stream 1 HTTP traffic and queries different data for Analytic Stream 2 FTP traffic and then sends that data to CBA in the Cloud for analytics processing.

Caution: Ensure that all NetWitness Suite host services are in sync with a consistent time source.

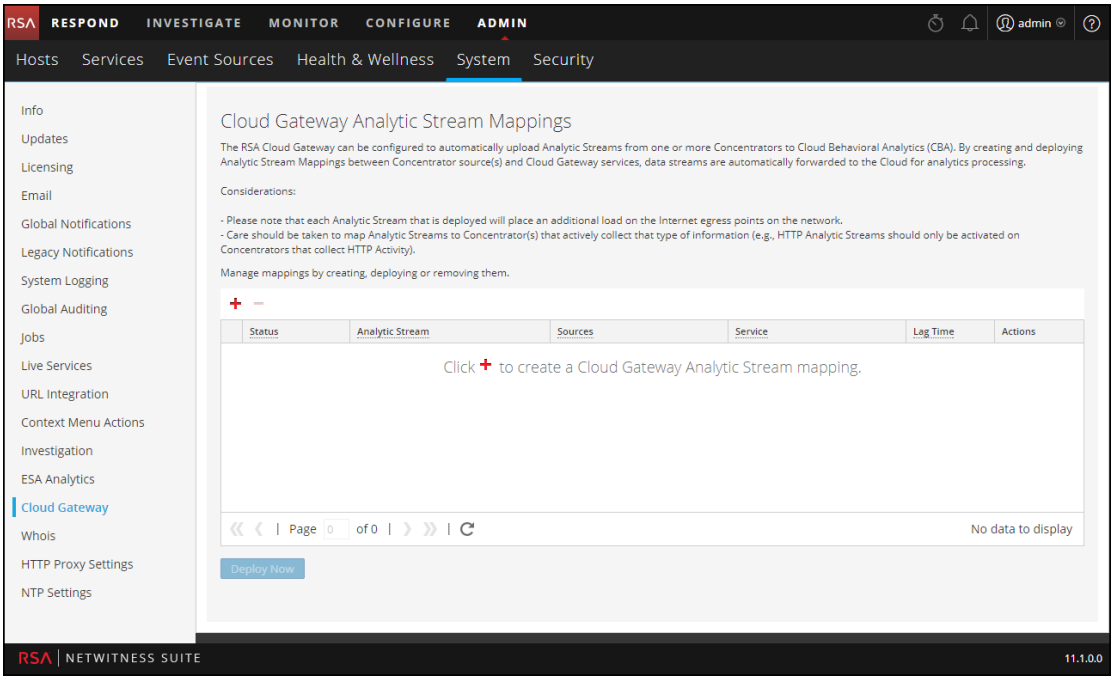
Prerequisites

- All NetWitness Suite host services must be in sync with a consistent time source.
- The Concentrator hosts and services must be discovered and available in the NetWitness Suite user interface.
- The Cloud Gateway Server service must be provisioned. See Provision a Cloud Gateway.

Create Cloud Gateway Analytic Stream Mappings

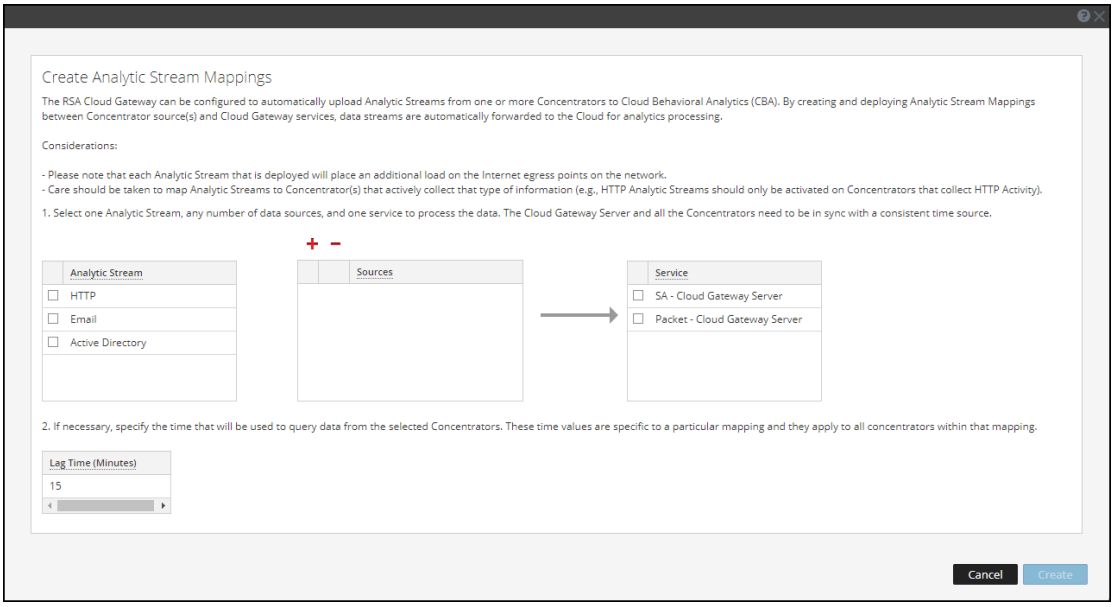
The following procedure tells you how to map Analytic Streams to sources and services. After creating and reviewing the mappings, you deploy them so that they can start aggregating data.

1. Go to **ADMIN > System**, and in the options panel, select **Cloud Gateway**.
   The Cloud Gateway Analytic Stream Mappings panel is displayed.



2. Click + to create an Analytic Stream mapping. Create a separate mapping for each Analytic Stream.

The **Create Analytic Stream Mappings** dialog is displayed.



3. In the **Analytic Stream** list, select an Analytic Stream.

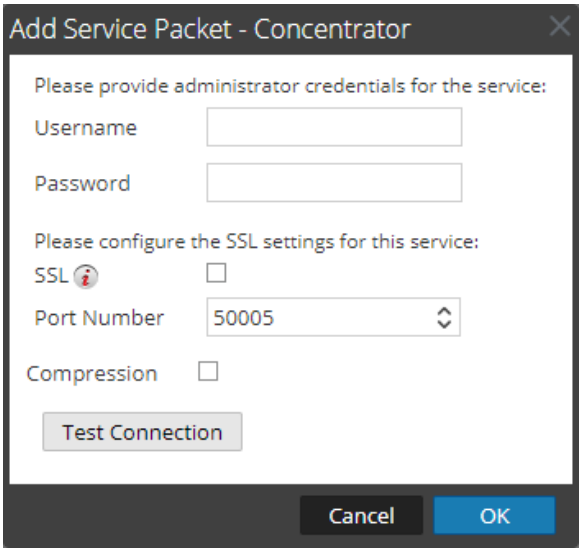
4. Configure one or more data sources (Concentrators) for your mappings. Do the following for each Concentrator:

   a. Click .

   The Available Services dialog shows the data sources that are available from the ADMIN > Services view.

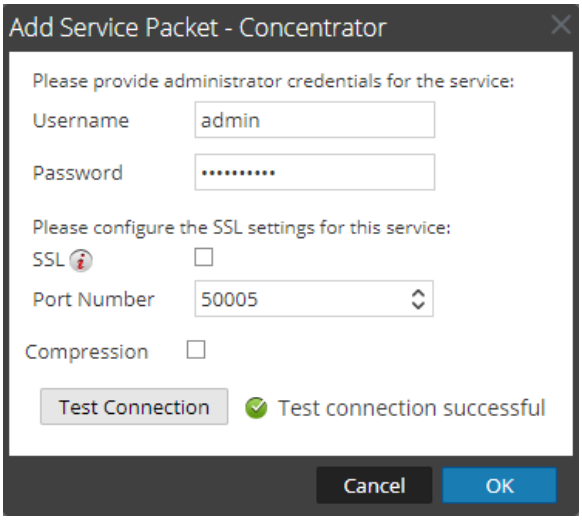
   b. In the **Available Services** dialog, select a Concentrator and click **OK**.

   The Add Service dialog is displayed.



   c. In the **Add Service** dialog, type the Administrator username and password for the Concentrator.

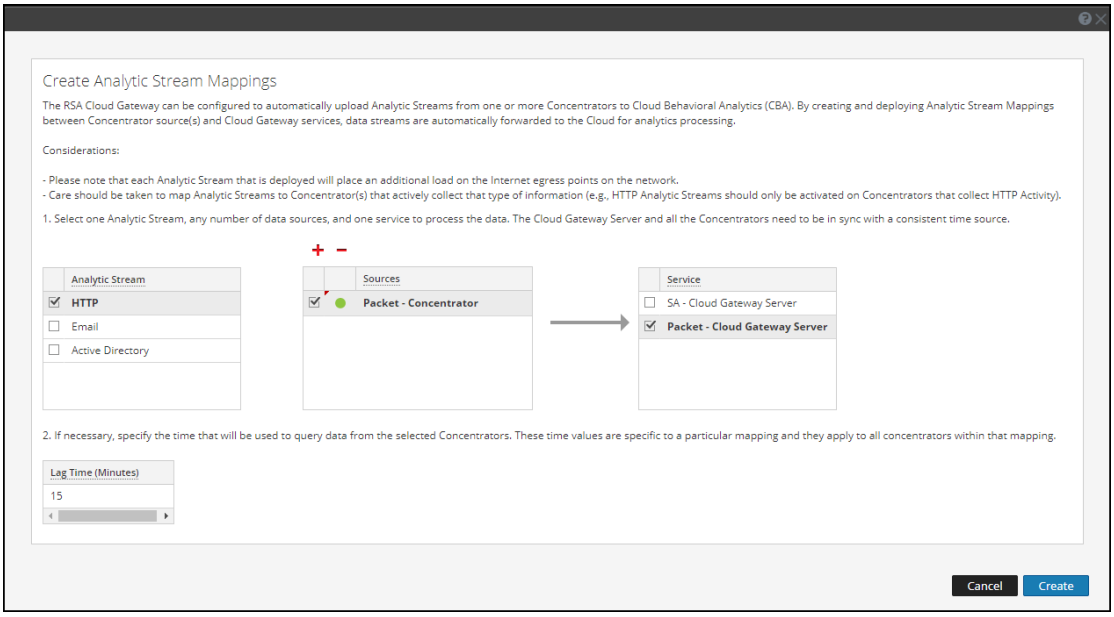
d. Click **Test Connection** to make sure that it can communicate with the Cloud Gateway service.



e. Click **OK**.

After you configure your data sources and they appear in the Sources list, you can reuse them for additional mappings.

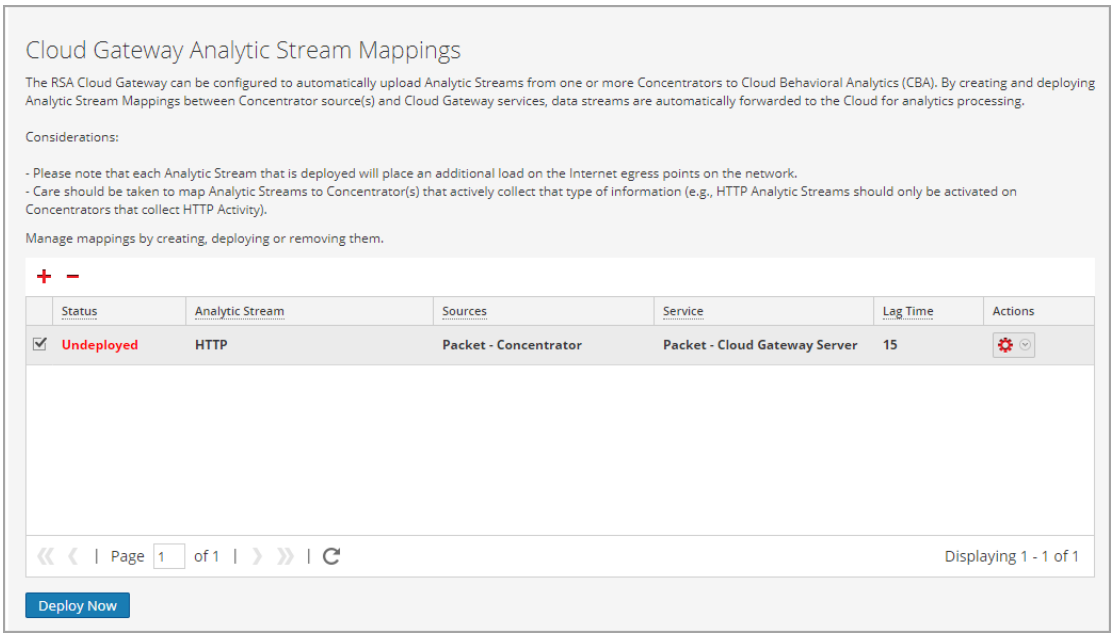
5. In the **Sources** list, select one or more data sources to aggregate the data for the Analytic Stream.



A solid colored green circle indicates a running service and a white circle indicates a stopped service.

6. In the **Service** list, select a Cloud Gateway service to process the data for the Analytic Stream.
7. If necessary, specify the Lag Time that will be used to query data from the selected Concentrators.
   Lag Time (Minutes) specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay.
   The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data.
   Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by CBA.
   For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on.
   Important: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data.

   Caution: RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation.
8. Click **Create**.
   The mappings that you create appear in the list of existing mappings with a status of **Undeployed**.



Important: To start an Analytic Stream so that it starts aggregating data, you need to deploy it.

Deploy Cloud Gateway Analytic Stream Mappings

After you create your mappings, you need to deploy them in order to start aggregating data for the Analytic Streams.

1. In the list of mappings, verify that the status of the mappings that you want to deploy show as **Undeployed**.
2. Select one or more mappings with a status of Undeployed and select **Deploy Now**.
   All selected mappings in the Undeployed state start to aggregate data as configured in the mapping. The mapping status changes to **Deployed**.
   You cannot deploy a mapping that has already been deployed.

Update a Mapping

You can only have one mapping per Analytic Stream. If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that Analytic Stream.

You can make the following updates to a deployed mapping without deleting it:

- Undeploy the mapping
- Change the Lag Time

You can also change the Lag Time for an undeployed Analytic Stream mapping.

Undeploy a Mapping

If you want to stop aggregating data for an Analytic Stream mapping, but you do not want to delete the mapping, you can undeploy it. This gives you the option of deploying it at a later time. When you undeploy a mapping, the specified Cloud Gateway service stops pulling data from the data source for that Analytic Stream.

Caution: Undeploying a mapping with a status of Deployed will affect data aggregation for that Analytic Stream.

To undeploy a mapping:

1. In the Cloud Gateway Analytic Stream Mappings panel, select the deployed mapping that you want to undeploy.
2. In the **Actions** column, select > **Undeploy**.

   The status changes from Deployed to Undeployed and data aggregation stops.

Delete a Mapping

You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not running, it does not affect data aggregation.

You should undeploy a mapping with a status of Deployed before deleting it. Undeploying and deleting a mapping clears the configuration on the Cloud Gateway Server, reverts the deployment for that mapping, and stops pulling data from the data source for that Analytic Stream.

Caution: Undeploying and deleting a mapping will affect data aggregation for that Analytic Stream.

To delete a mapping:

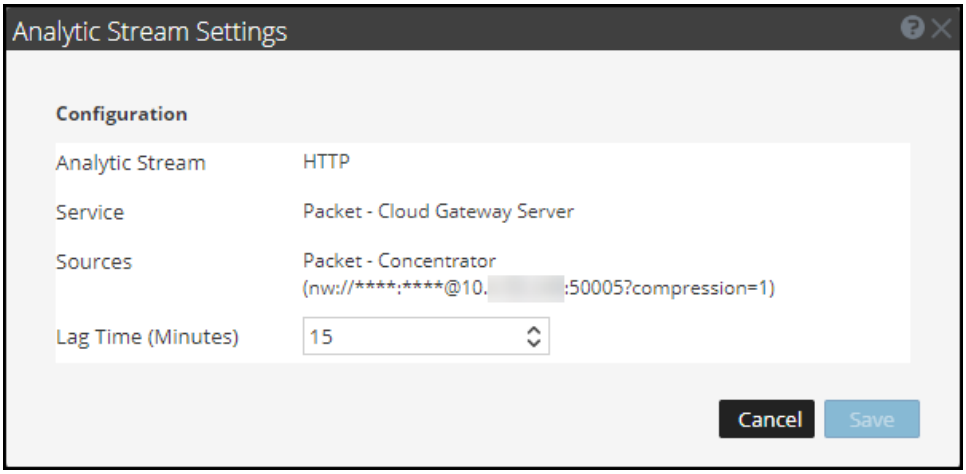
1. In the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to delete. You can only delete one mapping at a time.
2. Click .

Change the Lag Time

If necessary, you can change the Lag Time for the Analytic Stream. The Lag Time defines the buffer between the current (system) time and the time when the Analytic Stream ingests the data.

1. In the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to change and in the **Actions** column, select > **Edit stream**.

   The Analytic Stream Settings dialog shows the selected Analytic Stream, Cloud Gateway service, and data sources for the mapping. The data sources show the URLs used to communicate with the Cloud Gateway service.



2. If necessary, you can adjust the **Lag Time (Minutes)** to give the Concentrators in the mapping additional time to finish aggregating all of the data.
3. Click **Save**.

   Changes DO NOT take effect immediately. For the settings to take effect, you need to undeploy and re-deploy the mapping.
4. To undeploy the mapping, in the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to undeploy and then select > **Undeploy**.

   Data aggregation stops for the selected mapping.
5. To re-deploy the mapping, select the mapping that you want to deploy and then select > **Deploy**.

   The selected mapping deploys and starts to aggregate data as configured in the mapping.

Monitor the Cloud Gateway

You can monitor the RSA Cloud Gateway service statistics in NetWitness Suite.

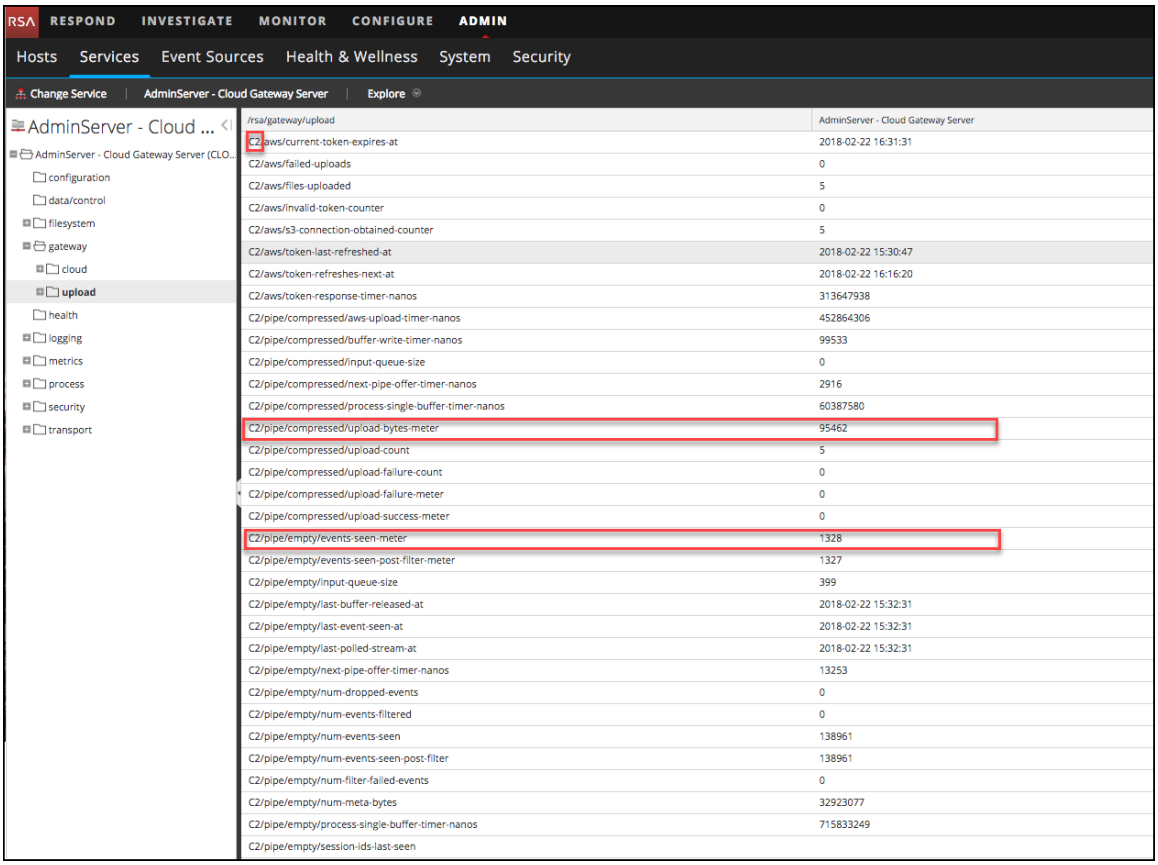
In the Services view, select the Cloud Gateway Server service and then select > **View** > **Explore**. In the Explore view, you will see important statistics that you should monitor for the Cloud Gateway. You can adjust your Analytic Stream Mappings as required.

The following figure shows two important statistics that you will want to look at for each stream:

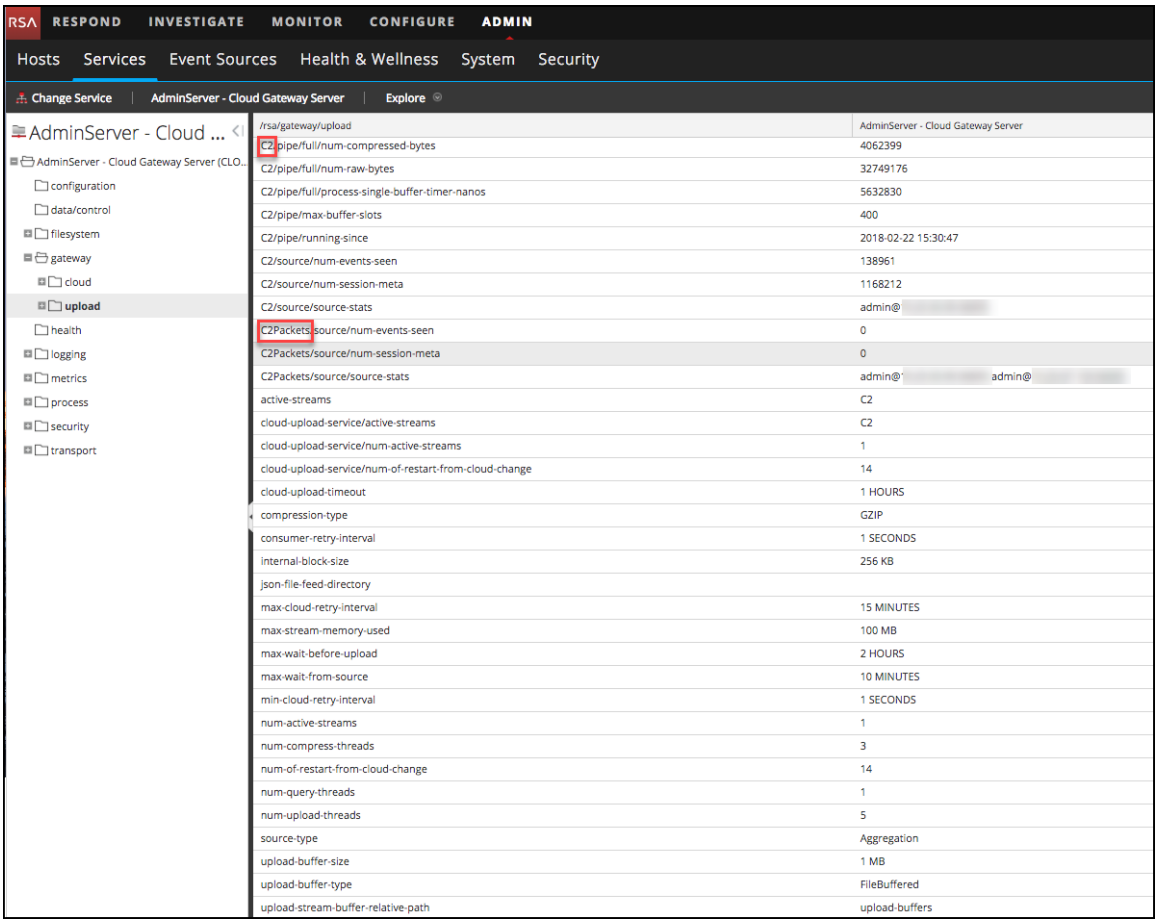
- **upload-bytes-meter**: This statistic shows the average bytes uploaded per second. It is the upload rate (bytes).
- **events-seen-meter**: This statistic shows the number of events pulled from the Concentrator per second. It is the reading rate (number).

The first part of the statistic name shows the Analytic Stream name, in this example the Analytic Stream Name is **C2**:

C2/pipe/compressed/upload-bytes-meter



If you scroll down, you can see the rest of the statistics. If you have more than one Analytic Stream, you will see statistics for that stream, too. In this example, you can see statistics for the **C2** and **C2Packets** Analytic Streams.



Note:
- Each Analytic Stream that you deploy places an additional load on the Internet egress points on the network. Look at the upload statistics, such as **upload-bytes-meter**.
- Every Analytic Stream that you add impacts the Concentrators. Look at the **events-seen-meter** statistic and see the "Monitor Service Details" topic in the *System Maintenance Guide*.
- Ensure that you map Analytic Streams to Concentrators that actively collect that type of information. For example, HTTP Analytic Streams should only be activated on Concentrators that collect HTTP activity.

Cloud Gateway References

This section contains reference information for Cloud Gateway.

See the following topics for details:

- Cloud Gateway Config View Certificate Tab
- Cloud Gateway Analytic Stream Mappings
- Analytic Stream Settings

Cloud Gateway Config View Certificate Tab

An RSA Cloud Gateway must be provisioned before it can be used for Cloud Behavioral Analytics (CBA). The Services Config view Certificate tab for the Cloud Gateway Server service enables you to provision the Cloud Gateway and view the status of the provisioning. After you provision the gateway, you can map data sources to Analytic Streams, such as HTTP or FTP traffic.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Provision the Cloud Gateway.	Provision a Cloud Gateway
Administrator	Configure data aggregation for the Cloud Gateway.	Mapping Cloud Gateway Analytic Streams
Administrator, Analyst	View detected threats.	See *NetWitness Respond User Guide* and *NetWitness Investigate User Guide*.

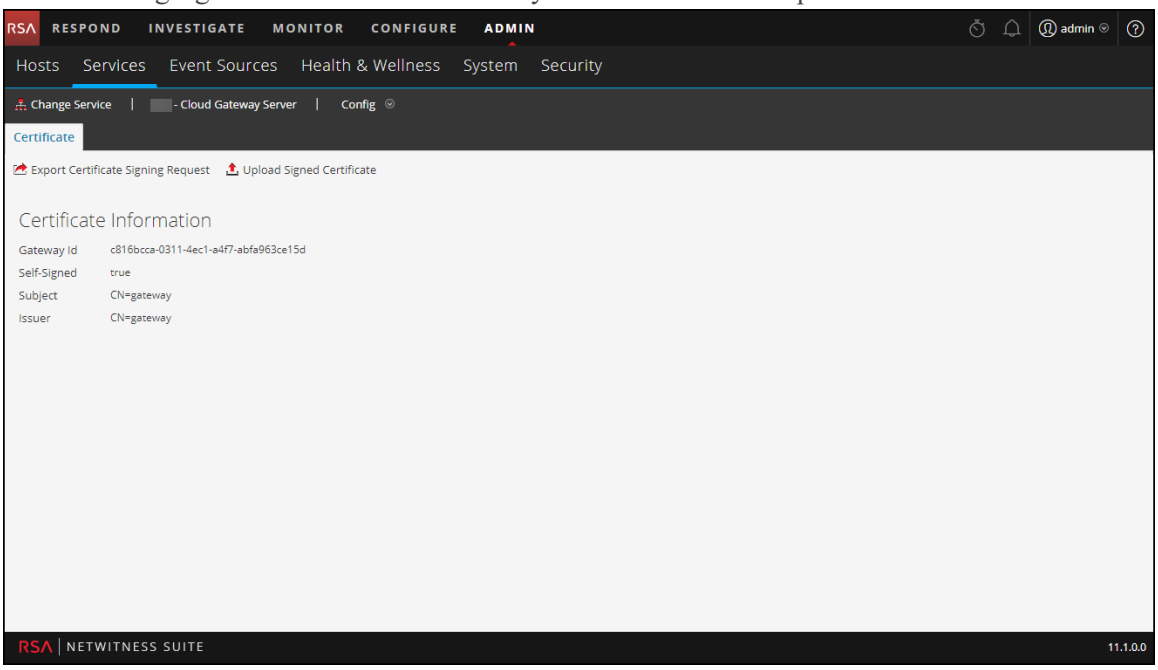
Related Topics

- RSA Cloud Behavioral Analytics
- Cloud Gateway Analytic Stream Mappings

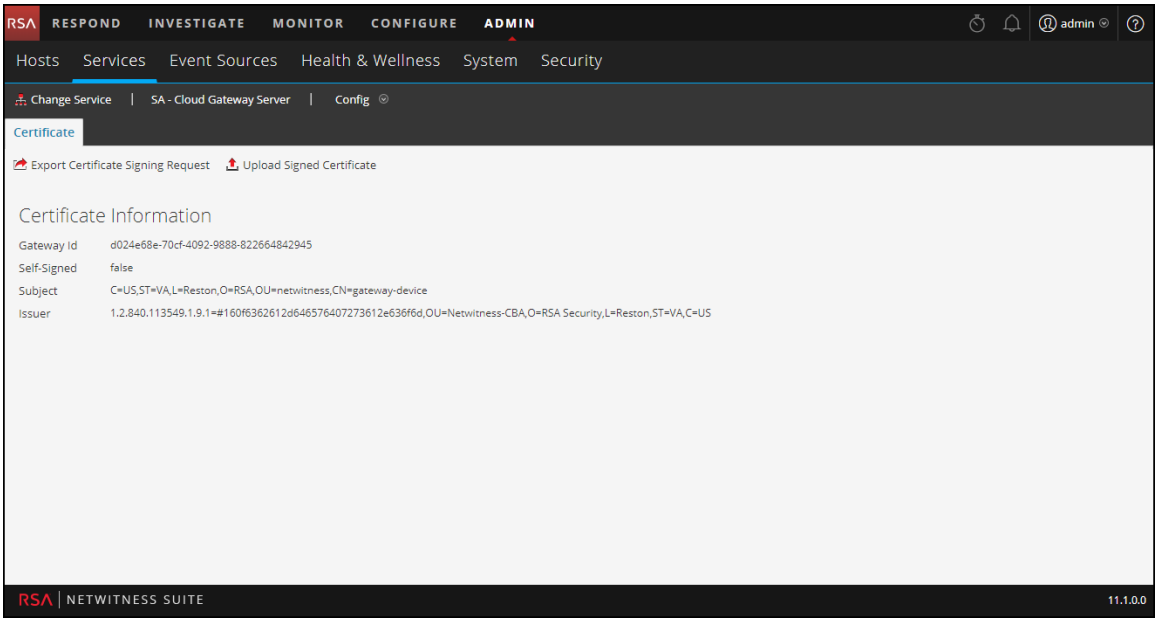
Certificate Tab

To access the Services Config view Certificate tab, in the Services view (ADMIN > Services), select the Cloud Gateway Server service and then select **> View > Config**.

The following figure shows a Cloud Gateway service that is NOT provisioned.



The following figure shows a provisioned Cloud Gateway service.



Certificate Information

The Certificate Information section enables you to view the provisioning status of the Cloud Gateway service.

The following table describes the Cloud Gateway Certificate Information fields.

Field	Description
Gateway ID	The Gateway ID, also known as the Service ID, identifies the gateway for RSA. You send the Gateway ID along with the CSR file to the RSA Cloud Administrator, who will provide you with a signed certificate file.
Self-Signed	If **true**, it indicates a default generated certificate. If **false**, it indicates a signed-certificate provided by RSA.
Subject	The Subject shows "CN=gateway" when the Cloud Gateway is not provisioned. It shows more detailed information when it is provisioned: • **C** = Country (for example, US) • **ST** = State or Province Name (for example, VA) • **L** = Locality Name (for example, Reston) • **O** = Organization Name (for example, RSA) • **CN** = Common Name (for example, gateway-device)
Issuer	The Issuer shows the provider of the certificate. The Issuer shows "CN=gateway" when the Cloud Gateway is not provisioned.

Toolbar Actions

This table lists the toolbar actions available in the Cloud Gateway Config view Certificate tab.

Option	Description
Export Certificate Signing Request	Click this link to create and download the Certificate Signing Request (CSR) file for your Cloud Gateway. Provide the CSR file and the Gateway ID to the RSA Cloud Administrator, who will provide you with a signed certificate.
Upload Signed Certificate	Click this link to install the signed certificate that you received from the RSA Cloud Administrator in your Cloud Gateway Server service.

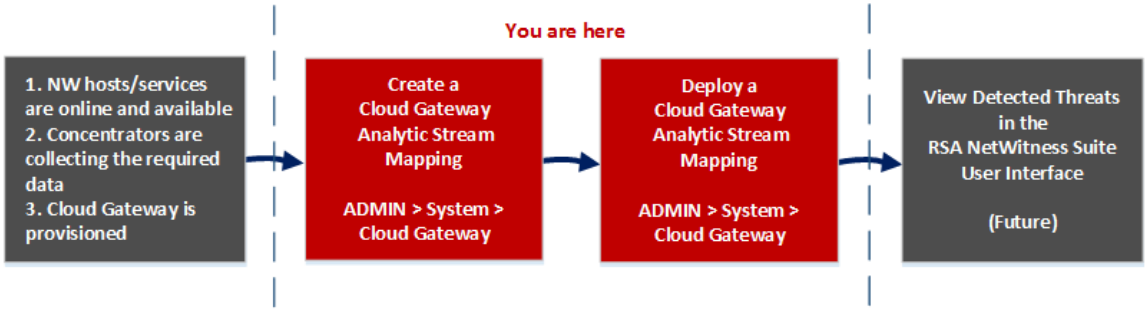
Cloud Gateway Analytic Stream Mappings

In the Cloud Gateway Analytic Stream Mappings panel (ADMIN > System > Cloud Gateway), you define the resources that RSA NetWitness Suite Cloud Behavioral Analytics (CBA) uses to automatically detect advanced threats.

You can configure the RSA Cloud Gateway to automatically upload Analytic Streams from one or more Concentrators to Cloud Behavioral Analytics (CBA). An *Analytic Stream* is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.

Workflow

This workflow shows the process for creating and enabling a Cloud Gateway Analytic Stream mapping to start automatically detecting advanced threats.



Before you create a Cloud Gateway Analytic Stream Mappings mapping, ensure that the NetWitness Suite hosts and services that you want to use for your mappings are online and available. All of the services need to be in sync with a consistent time source. Ensure that the Concentrators are collecting the required data. Cloud Gateway services must be provisioned to enable Cloud Behavioral Analytics.

When you create a mapping, you select an Analytic Stream to map, such as HTTP. Then you select the data sources, such as Concentrators, to use for that Analytic Stream along with a Cloud Gateway service to process the data. When you are ready to start aggregating data, you deploy the mapping. (Future) Analysts can view detected threats for that Analytic Stream in the NetWitness Suite user interface (UI).

What do you want to do?

Role	I want to ...	Show me how
Administrator	Verify that the NetWitness Suite hosts and services are online and available.	ADMIN > Hosts and ADMIN > Services See *Hosts and Services Getting Started Guide*.
Administrator	Ensure that the Concentrators are collecting the required data.	See *Broker and Concentrator Configuration Guide*
Administrator	Provision the Cloud Gateway.	Provision a Cloud Gateway
Administrator	Create Cloud Gateway Analytic Stream mappings*	Mapping Cloud Gateway Analytic Streams
Administrator	Deploy Cloud Gateway Analytic Stream mappings*	Mapping Cloud Gateway Analytic Streams
Administrator, Analyst	View detected threats.	See *NetWitness Respond User Guide* and *NetWitness Investigate User Guide*.

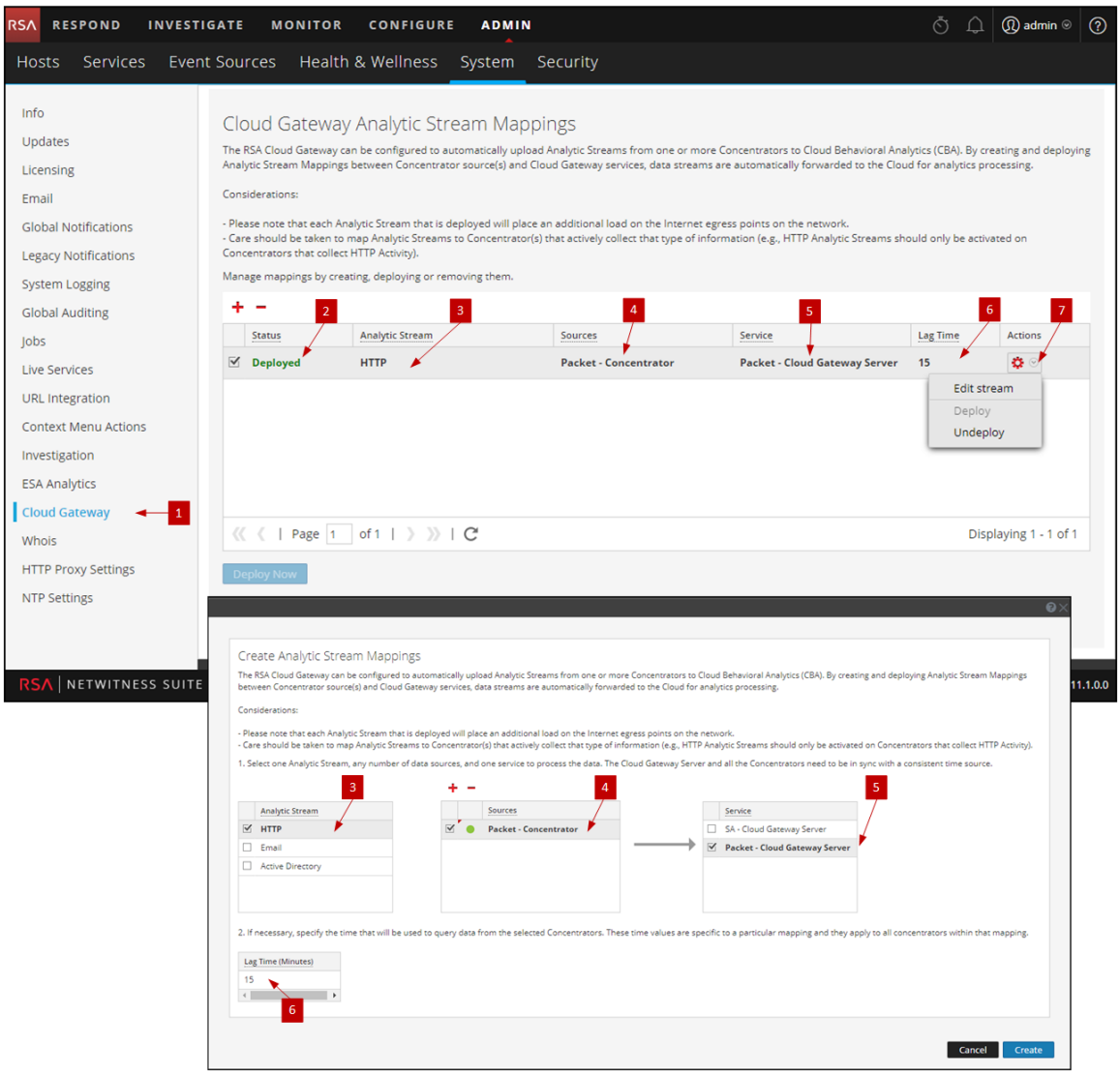
*You can complete these tasks here (that is in the Cloud Gateway Analytic Stream Mappings panel).

Related Topics

- RSA Cloud Behavioral Analytics
- Cloud Gateway Config View Certificate Tab
- Update a Mapping
- Undeploy a Mapping
- Delete a Mapping
- Change the Lag Time
- Analytic Stream Settings

Quick Look

The following example illustrates a Cloud Gateway Analytic Stream mapping. The configuration defines the data sources for the selected Analytic Stream and the Cloud Gateway service that will process the events from those data sources.



1	Displays the Cloud Gateway Analytic Stream Mappings panel.
2	Shows the status of the mapping.
3	The name of the Analytic Stream that is mapped.
4	Data sources, such as Concentrators, assigned to the mapping.
5	Cloud Gateway service that processes the data for the mapping.
6	Lag Time configuration (in minutes) on the data sources for the mapping.
7	Actions for changing Analytic Stream settings, deploying mappings, and undeploying mappings.

Toolbar

The following table describes the toolbar actions.

Icon / Button	Descripton
	Opens the Create Mappings dialog where you can create a mapping. Create a separate mapping for each Analytic Stream. After creating and reviewing the mappings, you deploy them.
	Deletes a Mapping. • You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not deployed and is not running, it does not affect data aggregation. • Deleting a deployed mapping clears the configuration on the host server, reverts the deployment for that mapping, and stops pulling data from the data source for that Analytic Stream. You should undeploy a mapping with a status of Deployed before deleting it.
Deploy Now	After you create your mappings, you need to deploy them in order to start aggregating data for the Analytic Streams. You can select one or more mappings with a status of Undeployed to deploy.

Note: If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that Analytic Stream.

Cloud Gateway Analytic Stream Mappings

The following table describes the listed Cloud Gateway Analytic Stream mappings.

Icon / Field	Description
	To select an individual mapping, select the checkbox next to the mapping.

Icon / Field	Description
Status	Shows the status of the mapping. There are two statuses: **Undeployed** - An undeployed mapping maps an Analytic Stream to sources and a Cloud Gateway service. It does not start aggregating data for the Analytic Stream until you deploy the mapping. **Deployed** - A deployed mapping is deployed and running. In a deployed mapping, the selected Cloud Gateway service uses query-based aggregation to collect the appropriate filtered traffic for the selected Analytic Stream from the Concentrators.
Analytic Stream	Indicates the selected Analytic Stream. An Analytic Stream is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.
Sources	Sources are the data sources, such as Concentrators, from which the Cloud Gateway will aggregate the data for the specified Analytic Stream.
Service	Indicates the Cloud Gateway service that will process the data for the specified Analytic Stream. The selected service needs to be in sync with a consistent time source.

Icon / Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data. Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by CBA. For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation.
	Enables you to select additional actions for the selected Analytic Stream mapping: • **Edit stream** - Enables you to configure the Lag Time for the selected mapping. • **Deploy** - Deploys the selected mapping. The specified Cloud Gateway service starts pulling data from the data sources for that Analytic Stream. • **Undeploy** - Undeploys the selected mapping. The specified Cloud Gateway service stops pulling data from the data sources for that Analytic Stream. **Caution:** Undeploying a mapping with a status of Deployed will affect data aggregation for that Analytic Stream.

Analytic Stream Settings

After you create or deploy an Analytic Stream mapping in the Cloud Gateway Analytic Stream Mappings panel (ADMIN > System > Cloud Gateway), you have the option to change some Analytic Stream configurations for that mapping.

What do you want to do?

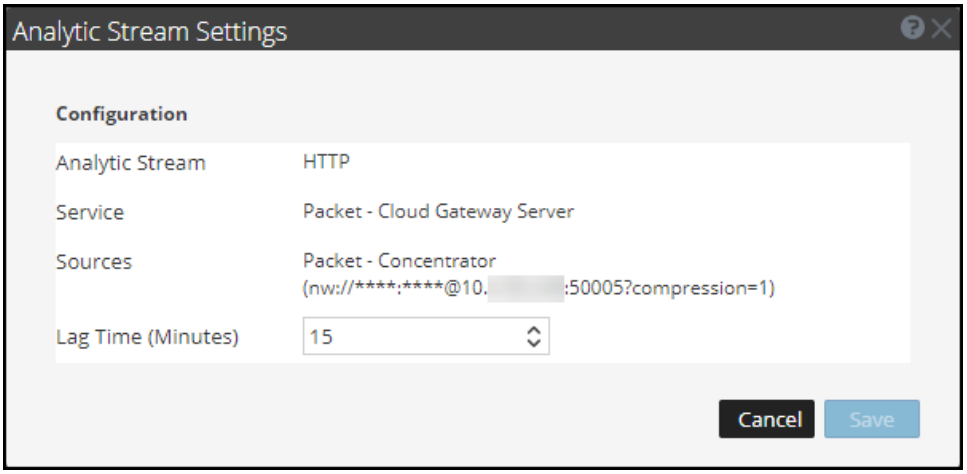
Role	I want to ...	Show me how
Administrator	Change the Lag Time for a Cloud Gateway Analytic Stream mapping.	Change the Lag Time
Administrator	Undeploy and redeploy an Analytic Stream mapping.	Change the Lag Time

Related Topics

- Mapping Cloud Gateway Analytic Streams
- Cloud Gateway Analytic Stream Mappings

Analytic Stream Settings

To access the Analytic Stream settings, in the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to change and in the **Actions** column, select **> Edit stream**.



Configuration

The Configuration section enables you to view the Analytic Stream configuration and change the Lag Time setting.

The following table describes the settings available for a Cloud Gateway Analytic Stream mapping.

Field	Description
Analytic Stream	Shows the name of the mapped Analytic Stream.
Service	Shows the Cloud Gateway service that processes the data for the mapping.
Sources	Shows the mapped data sources and the URLs used to communicate with the Cloud gateway.

Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data. Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by CBA. For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data. The Lag Time value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two Analytic Streams with different Lag Times, the Concentrator uses separate Lag Time values for each Analytic Stream mapping. **Caution:** RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. To determine the correct Lag Time, add together the following to get an environmental Lag Time: 1. **Log or Packet Latency** - This is the time it takes for the Log Decoder to receive the logs or the (Packet) Decoder to receive packets. For example, the Log Decoder may get logs every 20 minutes. In this case, you would want to set Lag Time to at least 20 minutes, preferably 25 minutes, so that you do not miss events. 2. **Aggregation Latency** - This is the time it takes to get the data from the Log Decoder to the Concentrator. 3. **Other Buffer** - Add in any additional time delay specific to your environment.

RSA NETWITNESS® SUITE

Context Hub Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

7

How Context Hub Works 8

Overview of Context Hub Configuration 9

Configure Lists as a Data Source 10

Prerequisites 10

Add List data source using Local File Store 11

Add List data source using HTTP(S) 13

Next Steps: 15

Configure Archer as Data Source 16

Prerequisites 16

Configure Active Directory as a Data Source 20

Prerequisites 20

Configure Netwitness Endpoint as a Data Source 24

Prerequisites 24

Configure Respond as a Data Source 28

Prerequisites 28

Configure Live Connect as a Data Source for Context Hub 30

Prerequisites 30

Enable or Disable Live Connect Data Source 30

Edit Live Connect Data Source Settings 33

Configure Context Hub Data Source Settings 36

Import or Export Lists for Context Hub 41

Import a List 41

Import Single-Column List 41

Import Values to an existing List 43

Export List for Context Hub 43

Configure Meta Type Mapping for Context Hub 45

Context Hub References **49**
Context Hub Data Sources Tab 50
Workflow 50
What do you want to do? 50
Related Topics 51
Quick Look 51
Context Hub Lists Tab 54
Workflow 54
What do you want to do? 54
Related Topics 55
Quick Look 55
Troubleshooting **59**
Possible Issues 59

How Context Hub Works

Context Hub service provides enrichment lookup capability in the Respond and Investigate views. An Administrator can configure the Context Hub service and the data sources to enable an Analyst to perform the context lookup for the required data sources.

By default, the Context Hub service supports enrichment lookups for meta types such as IP address, User, Domain, MAC address, File Name, File Hash, and Host.

The following data sources are supported by NetWitness Suite and provide enriched data when configured.

Lists- Provides contextual information from a list of blacklists, whitelists, or watchlists.

RSA Archer- Provides Criticality information of a device or specific asset based on the IP or Host which needs constant monitoring.

Active Directory - Provides contextual information of a user to help determine if the user is suspicious or not.

RSA NetWitness® Endpoint - Provides context information for endpoint module and machine indicators and to help determine if any of the Endpoint devices are compromised.

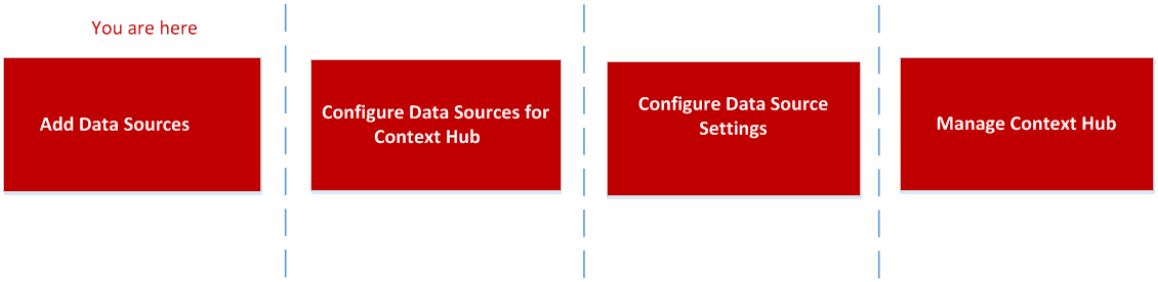
Respond- Provides contextual information of a specific meta available in respond and enables analyst to respond faster based on context data.

Live Connect - Provides contextual information for IP addresses, Domains and File Hashes from RSA Live Connect Threat intelligence community server.

Overview of Context Hub Configuration

The Administrator needs to perform each step in the proper sequence to configure the services to perform the context lookup effectively. In the **ADMIN**> **Services**. Services Config view of Context Hub service, an administrator can configure data sources for Context Hub Service. The administrator can also configure Context Lookups for custom meta keys, if required and also import lists or export lists.

The workflow below describes how the Context Hub service can be configured:



Context Hub service is pre-installed on primary ESA host, and automatically added to the Netwitness Suite.

Note: You can have only one Context Hub service instance enabled in your NetWitness Suite deployment. If there are multiple ESA service in NetWitness Suite, you must choose the appropriate ESA host for Context Hub. A minimum of 8GB space is required to configure Context Hub on ESA host.

Configure Lists as a Data Source

Lists as a Data Source use the Context Hub service to fetch contextual information for meta types that support context lookup. You can create one or more lists and add relevant list values to the list. Make sure that you create meaningful lists such as blacklisted IPs, whitelisted IPs, and so on. The lists can contain supported entities such as IP address, MAC address, User name, Host name, Domain name, File name or File hash. You can import a single-column list or a multi-column list from the Data Source tab.

List values are in CSV format available in an external location and can be accessed through the following two methods:

- **Local File Store**: You can share a file from a local location.
- **HTTP(S)**: You can share a file using a web server location.

Note: You can also set up recurring job to fetch data on regular intervals by using the Prefetch settings while configuring meta mapping.

Prerequisites

Before you configure Lists data source, ensure that:

- User should have admin permissions.
- Context Hub service is available in **ADMIN**> **Services** view of NetWitness Suite.
- If you are using Local File Store or HTTP(S) server, the path mentioned should contain the CSV file

  In case of remote Local File Store, the file must be mounted or placed on the local drive location `/var/lib/netwitness/contexthub-server/data`.
- The NetWitness user must have read permission to access the file.

Caution: If you are creating a Context Hub list for use as an enrichment source in ESA, the list name cannot include any spaces or special characters, or start with a number. If you do not follow this naming convention, when you attempt to add the list as an enrichment source in ESA, an error message will be displayed and you will not be allowed to add the list.

Add List data source using Local File Store

To add a List as a data source:

1. Go to **ADMIN > Services**.

   The services view is displayed.

2. Select the Context Hub service and click > **View** > **Config**.

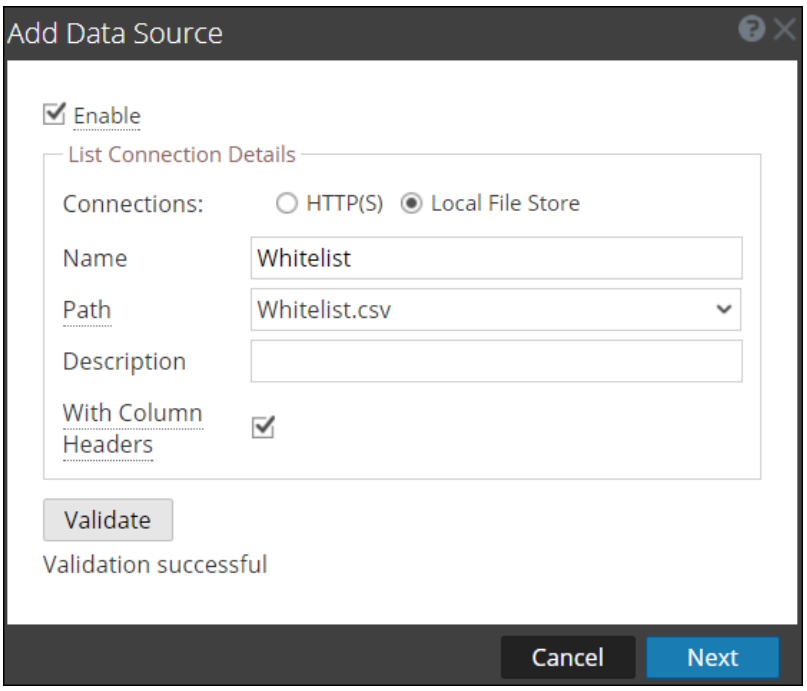
   The Services Config View of Context Hub is displayed.

3. In the **Data Sources** tab, click > **LISTS**.

   The **Add Data Source** dialog is displayed

4. By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, view the list in the list tab and view the contextual information.

5. Select the **Local File Store** Connection Type.



6. Provide the following database connection details. Enter the following fields for Local File Store Connection Type:

   - **Name:** Provide a name for the list data source.
   - **Path:** This field displays all the data files available in the data folder `/var/lib/netwitness/contexthub-server/data`, where context hub service is

running. Select the file name from the drop-down.
A maximum of 32 columns of CSV file are supported that adhere to the RFC1480 standards.

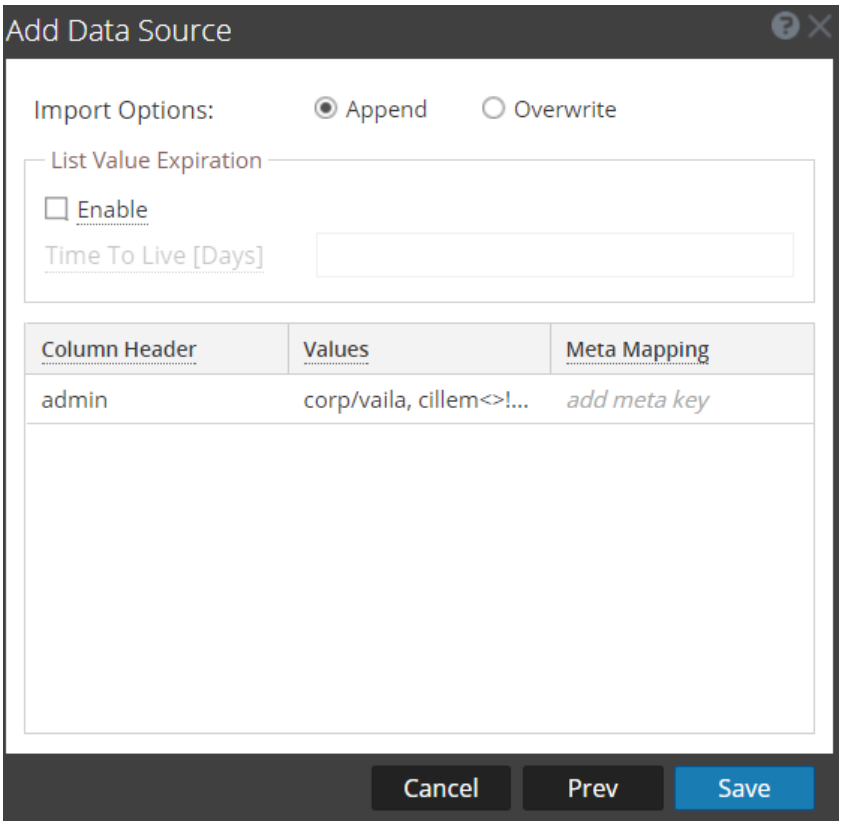
- (Optional) **Description**: Add a description for the selected file.
- **With Column Headers**: Select this option to consider the first row as column headers from the CSV file. If you don't select this option, you need to enter the column headers in the next screen.

7. Click **Validate**.

   If the validation fails, you cannot add the data source.

8. Click **Next**.

   The next dialog is displayed.



9. Select any one of the following options:

   - **Append** - Select this option to add the imported values to an existing list.
   - **Overwrite** - Select this option to replace the values in an existing list with the imported values.

10. In the **List Value Expiration** section, the **Enable** option is unchecked, by default. If you want to store the looked up list values in the cache for a specified number of days then select the **Enable** checkbox and enter the number of days in the **Time to Live (days)** field for the list values to be retained.
11. In the next screen, map at least one meta key with one or more meta types by mapping a column header with a meta. The description for each field is as follows:
    - **Column Header**: Display headers of the CSV file which must be mapped to a meta type.
    - **Meta Mapping**: Maps a column header field to a meta type.
    - **Values**: Displays the first three values from the imported list.
12. Click **Save**.

Add List data source using HTTP(S)

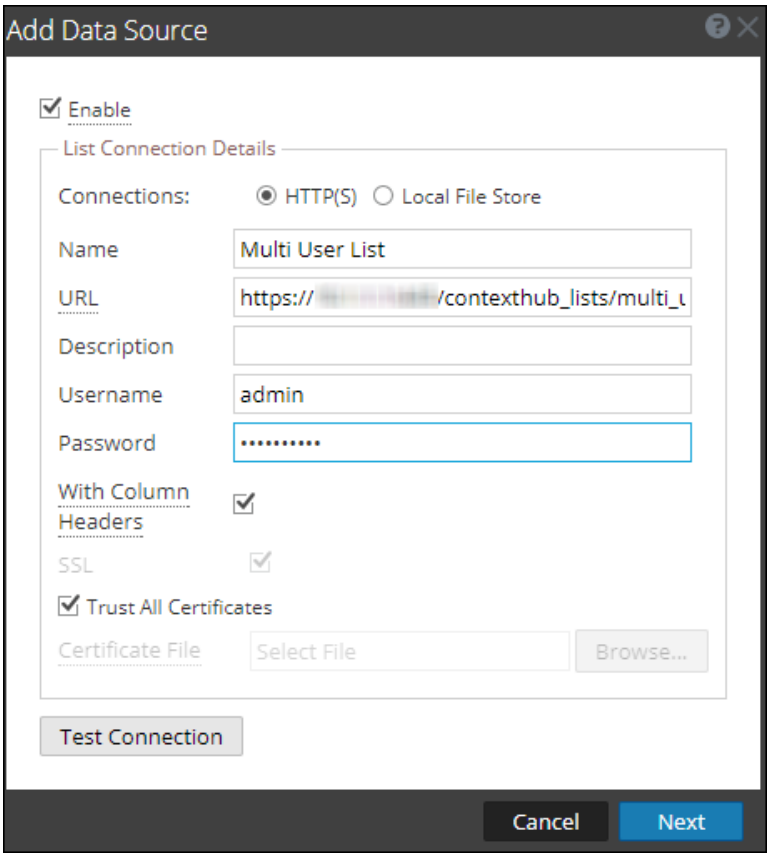
To add List as a data source:

1. Select **ADMIN** > **Services**.

   The services view is displayed.
2. Select the Context Hub service and click > **View** > **Config**.

   The Services Config View of Context Hub is displayed.
3. In the **Data Sources** tab, click > **LISTS**.

   The **Add Data Source** dialog is displayed.
4. Select the HTTP(S) Connection Type.

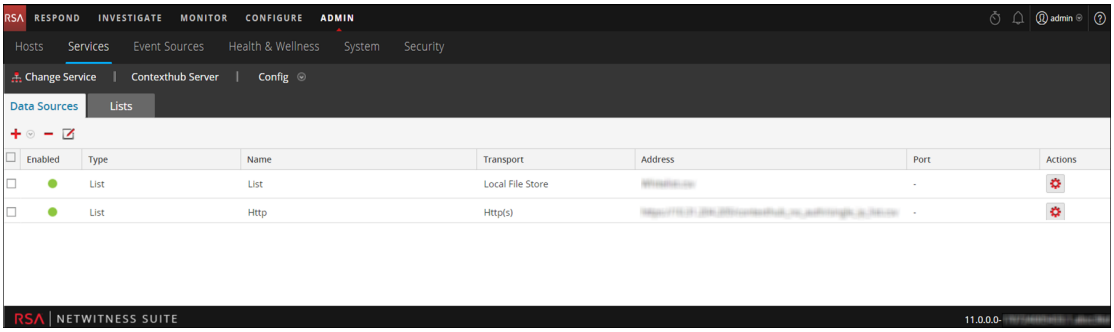


- Enter the following fields for HTTP(S) Connection Type:
  - **Name:** Provide a name for the list data source.
  - **URL**: Enter the path of the CSV file available on the HTTP(S) location along with the host name or IP address of the remote machine where the list is stored. The URL must be of the format: `https://<Hostname or IP-address of the HTTP (S)server>:<Port on which the HTTP(S) server is hosted>/<Absolute path of CSV file>`. For example, `https://10.1.1.1:443/contexthub_lists/multi_user_list.csv`
  - (Optional) **Description**: Add a description for the selected file.
  - (Optional) **Username:** Enter the username to connect to the HTTP(S) server requires basic authentication.
  - (Optional) **Password:** Enter the password to connect to the HTTP(S) server requires basic authentication.

- **With Column Headers**: Select this option if you want to import a CSV file with headers. If this option is selected and you import the CSV without headers, the first row will be considered as a header which can be edited.
- **SSL:** If you enter a URL with HTTPS in this field, then this is selected automatically. If you enter a URL with HTTP, then this checkbox is unselected.
- **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid .cer or .crt format HTTP(S)server certificate for the connection to be successful.

5. Click **Test Connection** to test the connection between Context Hub and the data source.
6. Click **Save** to save the settings.

   List is added as a data source for the configured Context Hub and is displayed in the **Data Sources** tab.



Next Steps:

- Add, edit, or remove values from a specific list.
- Configure the data source settings to determine the data source fields to be displayed in the Context panel. For instructions, see Configure Context Hub Data Source Settings .
- Import and export a list. For more information, see Import or Export Lists for Context Hub.
- View the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA NetWitness Respond User Guide* and *RSA NetWitness Investigation and Malware Analysis User Guide*.

Configure Archer as Data Source

You can configure Archer as a data source for Context Hub and use the Context Hub service to fetch contextual information from Archer. Use the procedures in this topic to add Archer as a data source for Context Hub service and configure the settings (if required) for Archer.

Prerequisites

Before you configure Archer data source, ensure that:

- Context Hub service is available in **ADMIN**>**Services** view of NetWitness Suite.
- Archer is installed with Licensed Devices application.

To add Archer as a data source for Context Hub:

1. Go to **ADMIN** > **Services**.

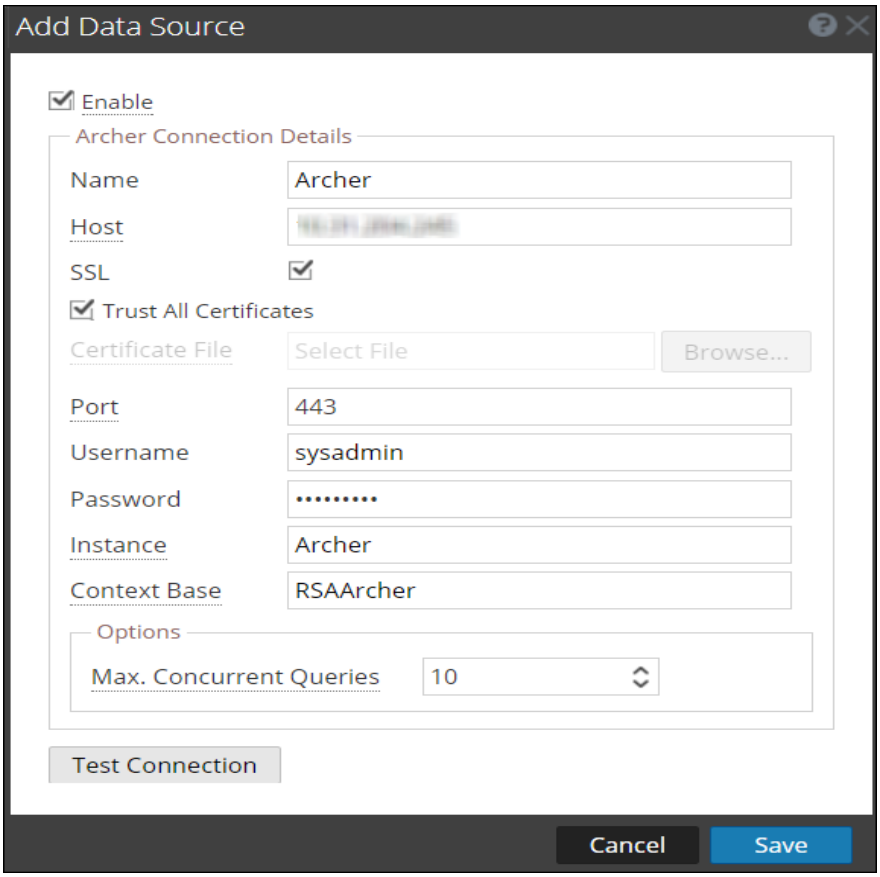
   The Services view is displayed.

2. Select the Context Hub service, and click > **View** > **Config**

   The Services Config view is displayed.

3. In the **Data Sources** tab, click > **Archer**.

   The **Add Data Source** dialog is displayed.

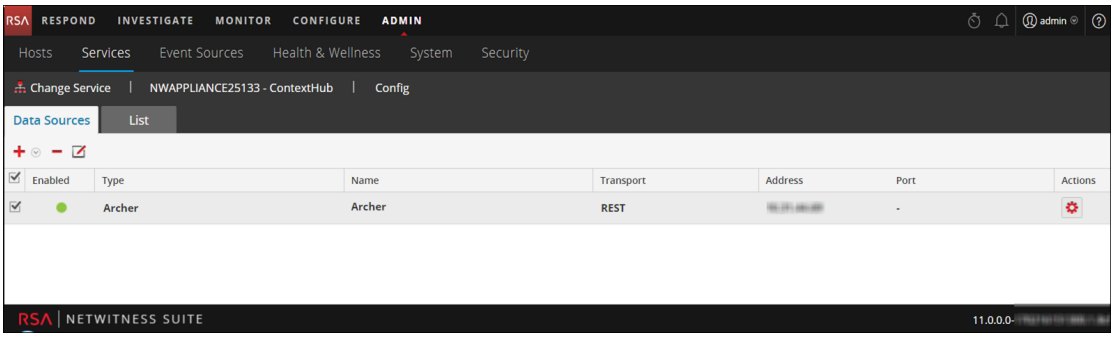


4. Provide the following information:

- By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
- Enter the following fields:
  - **Name**: Enter a name for Archer data source.
  - **Host**: Enter the hostname or IP address where Archer server is installed.
  - **SSL**: By default this option is selected and enables SSL communication to Archer .
  - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid Endpoint server certificate for the connection to be successful.
  - **Port**: The default port is 443.
  - **Username**: Enter the Archer Server username.
  - **Password**: Enter the Archer Server password.
  - **Instance**: Enter the Instance name from which you want to extract data. An RSA Archer instance is a single set up that includes unique content in a database, the connection to the database, the interface, and log-in. You might have individual instances for each office location or region or for development, test, and production environments. The Instance Database stores the RSA Archer content for a specific instance.
  - **Context Base**: Enter the virtual directory name where the files are stored. For example, rsaarcher located at the RSA Archer web address https://archer.company.com/**rsaarche**r/default.aspx. If the files are stored in the IIS default web address https://archer.company.com/default.aspx, then this field must be empty.
  - **Max. Concurrent Queries**: You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 10.
5. Click **Test Connection** to test the connection between Context Hub and the Archer data source.

6. Click **Save**.

   Archer is added as a data source for Context Hub and is displayed in the **Data Sources** tab.



After adding the data source, you can configure data source settings. For instructions, see Configure Context Hub Data Source Settings . And View the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, see the *Netwitness Respond User Guide* and *Investigation and Malware Analysis User Guide*

Configure Active Directory as a Data Source

You can configure Active Directory (AD) as a data source for Context Hub using LDAP and use the Context Hub service to fetch contextual information from AD. Use the procedures in this topic to add AD as a data source for Context Hub service and configure the settings(if required) for AD.

Prerequisites

Before you configure Active Directory data source, ensure that:

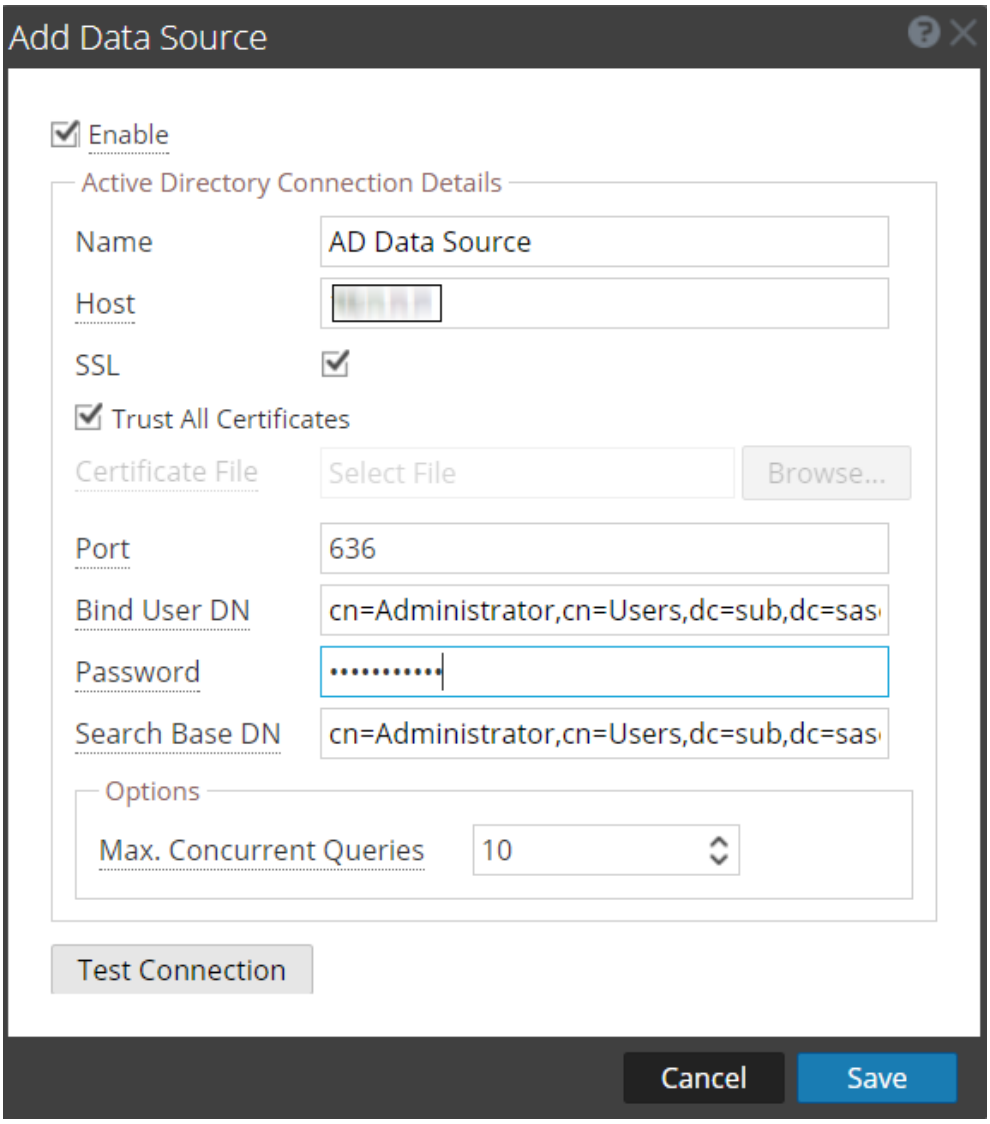
- Context Hub service is available in **ADMIN** > **Services** view of NetWitness Suite.
- AD is available and is running on Windows versions 2003, 2008, and 2012 are supported.

To add AD as a data source for Context Hub:

1. Go to **ADMIN** > **Services**.
   The services view is displayed.
2. Select the Context Hub service and click > **View** > **Config**.
   The Services Config View of Context Hub is displayed.

3. In the **Data Sources** tab, click + > **AD**.

   The **Add Data Source** dialog is displayed.



You need to configure the Active Directory schema to replicate the following attributes to view the data in the RESPOND page:

- Employee ID
- Department
- Company
- Title
- Postal Code

All the other attributes replicate automatically.

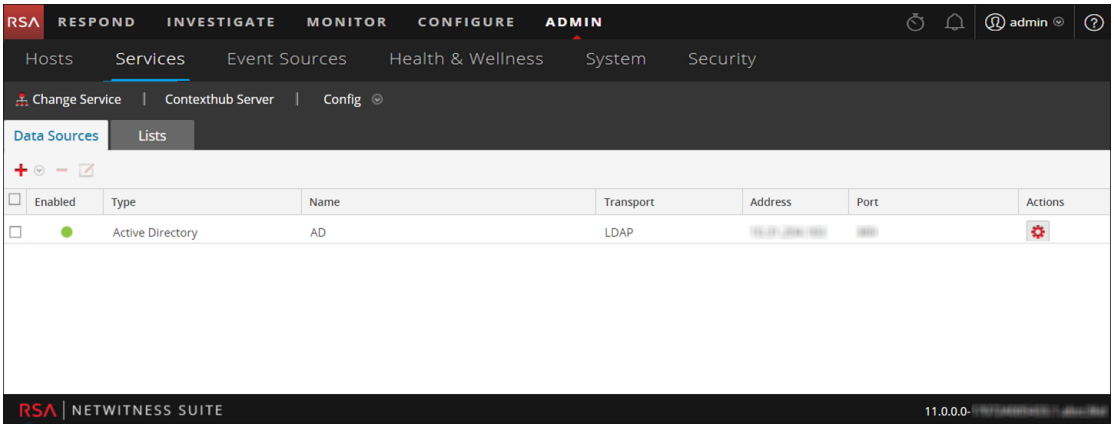
6. Provide the following database connection details:

   - By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
   - Enter the following fields.
     - **Name:** Enter a name for the AD data source.
     - **Host:** Enter the host name or IP address of the AD.
     - **SSL:** By default this will be checked with 636 port number which will connect to the data source using Secure Sockets Layer (SSL) connection.
     - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid .cer or .crt format Active Directory server certificate for the connection to be successful. If you add multiple AD data sources with ssl, you should configure all the data sources with either a valid certificate or a Trust All Certificates.
     - **Port:** The default port is 636 with SSL and 389 without SSL.
       If you want to fetch data from multi-domains you can configure a single data source with the Global catalog port (3269 with SSL or 3268 without SSL).
       Alternately, for multi-domain, you can configure a single data source for each domain with the default port (389 with SSL or 636 without SSL).

       Multi-forest is a collection of multi-domains. If you want to fetch data from multi-forest you need to configure each forest with the Global catalog port (3269 with SSL or 3268 without SSL).
     - **Password:** Enter password of the user DN used to bind with AD.
     - **Bind User DN:** The distinguished name of the user that will authenticate to the search directory. For example, cn=Administrator,cn=Users,dc=sub,dc=saserver,dc=local.
     - **Search Base DN:** The base distinguished name, or base DN, identifies the entry in the directory from which searches are initiated; the base DN is often referred to as the search base. For example, dc=sub,dc=saserver,dc=local.

7. Click **Test Connection** to test the connection between Context Hub and the data source.
8. Click **Save**.
   AD is added as a data source for the configured Context Hub. The added AD data source is

displayed in the **Data Sources** tab.



After adding the data source, you can configure the data source settings. For instructions, see Configure Context Hub Data Source Settings .

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, see the **Navigate to Context Summary Panel and View Additional Context** topic in the *Investigation and Malware Analysis Guide*.

Configure Netwitness Endpoint as a Data Source

You can configure NetWitness Endpoint as a data source for Context Hub and use the Context Hub server to fetch contextual information from NetWitness Endpoint. Use the procedures in this topic to add NetWitness Endpoint as a data source for Context Hub service and configure the settings (if required) for NetWitness Endpoint.

Prerequisites

Before you configure NetWitness Endpoint data source, ensure that:

- Context Hub service is available in **Admin** > **Services** view of NetWitness Suite.
- NetWitness Endpoint (v4.1.1 to 4.3.0.5) is installed and configured.
  For more information on how to install, configure and for detailed information on NetWitness Endpoint, see the NetWitness Endpoint documents available at RSA Link.

To add NetWitness Endpoint as a data source for Context Hub:

1. Go to **Admin** > **Services**.

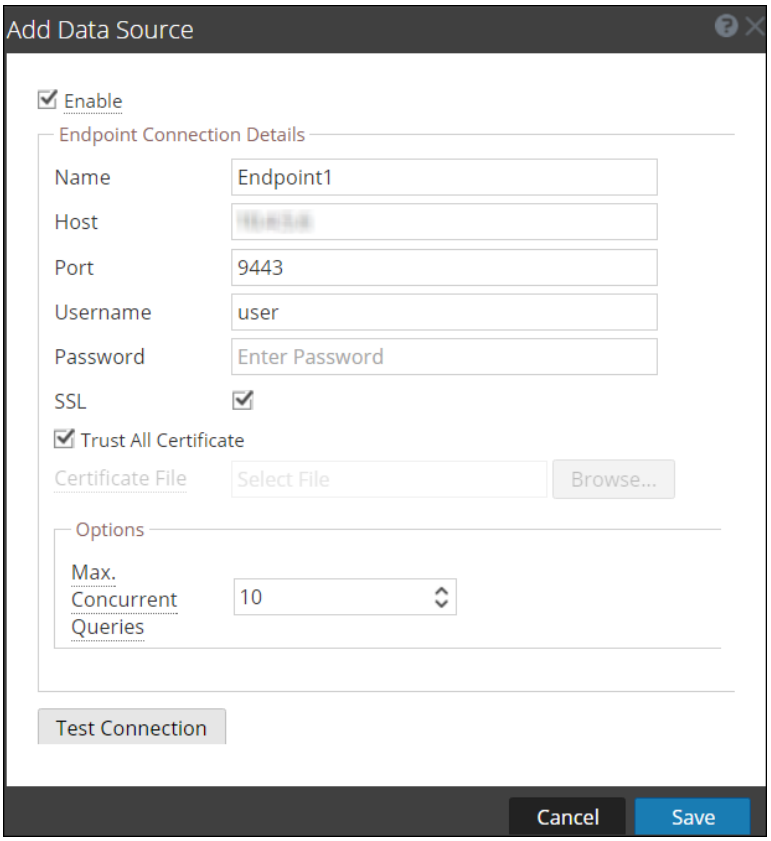
   The Services view is displayed.

2. Select the Context Hub service, and click > **View** > **Config**.

   The Services Config view is displayed.

3. In the **Data Sources** tab, click > **RSA Endpoint**.

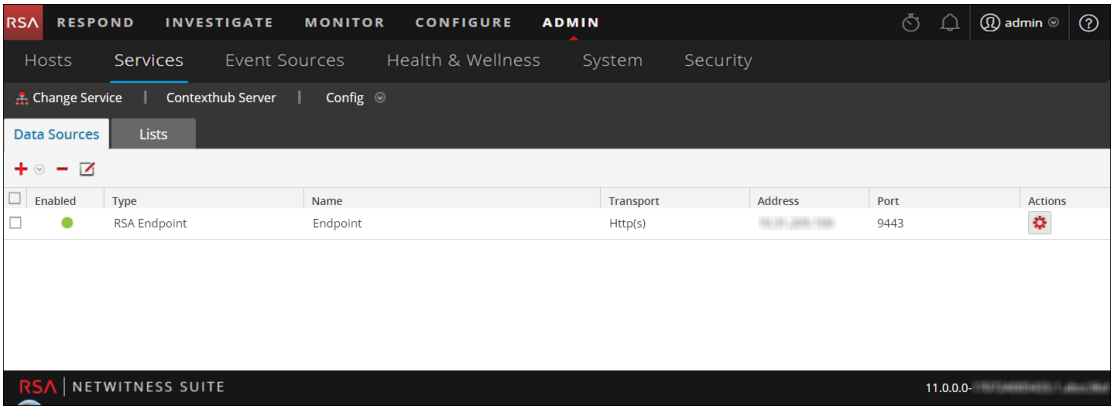
   The **Add Data Source** dialog is displayed.



4. Provide the following information:

- By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
- Enter the following fields:
  - **Name**: Enter a name for NetWitness Endpoint data source.
  - **Host**: Enter the hostname or IP address where NetWitness Endpoint API server is installed.
  - **Port**: The default port is 9443.
  - **SSL**: Select SSL if you want NetWitness Suite to communicate with the host using SSL. This is enabled by default.
  - **Username**: Enter the NetWitness Endpoint API Server username.
  - **Password**: Enter the NetWitness Endpoint API Server password.
  - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid server generated or CA certificate to authenticate the connection with the supported formats of .cer or .crt of Base64 [PEM] encoded or DER encoded.
  - **Max. Concurrent Queries**: You can configure the maximum number of concurrent queries to be run against the configured data sources. The default value is 10.

5. Click **Test Connection** to test the connection between Context Hub and the NetWitness Endpoint.
6. Click **Save**.
   NetWitness Endpoint is added as a data source for Context Hub and is displayed in the **Data Sources** tab.



Next steps

After adding the data source, you can configure the settings. For more information, see Configure Context Hub Data Source Settings .

Also you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA NetWitness Respond User Guide* and the *RSA Netwitness Investigation and Malware Analysis Guide*

Configure Respond as a Data Source

You can configure Respond as a data source for Context Hub and use the Context Hub service to fetch contextual information from Respond service. If Respond service is already configured, the configuration details are pre-populated while adding Respond as a data source. Use the procedures in this topic to add Respond as a data source for Context Hub service and configure the settings.

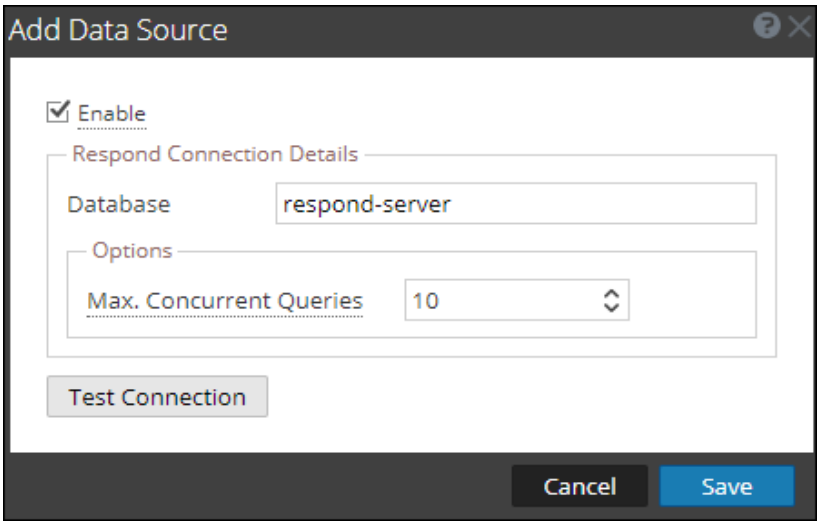
Prerequisites

Before you configure Respond data source, ensure that:

- Context Hub service is available in **ADMIN**> **Services** view of NetWitness Suite.
- Respond service is available.

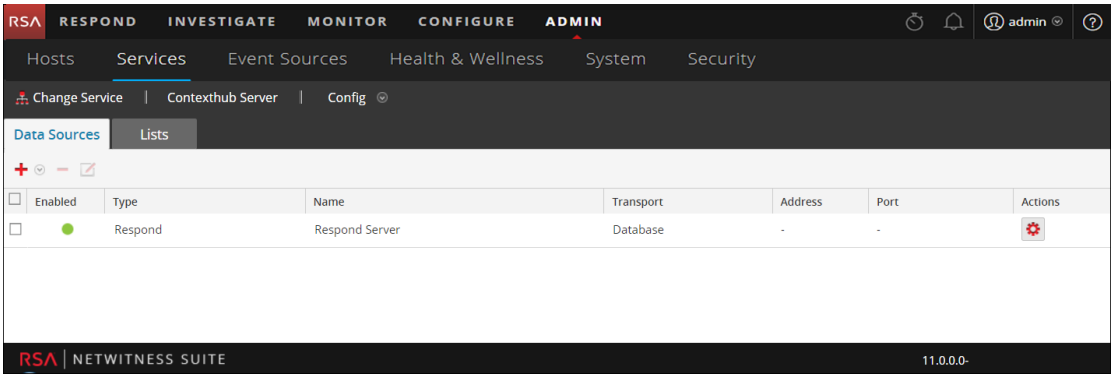
To add Respond as a data source for Context Hub:

1. Go to **Admin** > **Services**.
   The services view is displayed.
2. Select the Context Hub service and click > **View** > **Config**.
   The Services Config View of Context Hub is displayed.
3. In the **Data Sources** tab, click + > **Respond**.
   The **Add Data Source** dialog is displayed.



The required fields to configure the Respond data source are automatically updated.

4. Click **Test Connection** to test the connection between Context Hub and the data source.
5. Click **Save**.
   Respond is added as a data source for the configured Context Hub. The added Respond data source is displayed in the **Data Sources** tab.



After adding the data source, you can configure the settings. For more information, see Configure Context Hub Data Source Settings .

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA Netwitness Respond User Guide* and the *RSA Netwitness Investigation and Malware Analysis Guide*.

Configure Live Connect as a Data Source for Context Hub

This topic describes the procedure to configure Live Connect data source for Context Hub.

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA NetWitness® Suite and RSA NetWitness® Endpoint customer community.

RSA Live Connect is a part of Live Services and can be configured from the System View > Live Services Configuration panel. For more information about configuring Live Services, see the **Configure Live Services Settings** topic in the *System Configuration* Guide.

RSA Live Connect Threat Insights provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by analysts during the investigation process. By default, **Threat Insights** is enabled in **Additional Live Services**. If Context Hub service is configured, Live Connect is automatically added as a data source for Context Hub.

Prerequisites

Ensure that:

- Context Hub is enabled and the service is available in Admin > Services view of NetWitness Suite.
- RSA Live Account is available.

Note: To create a Live Account, see the **Step 1. Create Live Account** topic in the *Live Services Management Guide*.

By default, **Threat Insights** is enabled in **Additional Live Services** section. Before setting up Live Connect data source, make sure that you have signed in to your Live account with your Live Account Credentials and Context Hub is enabled. Live Connect is automatically added as a data source for context hub.

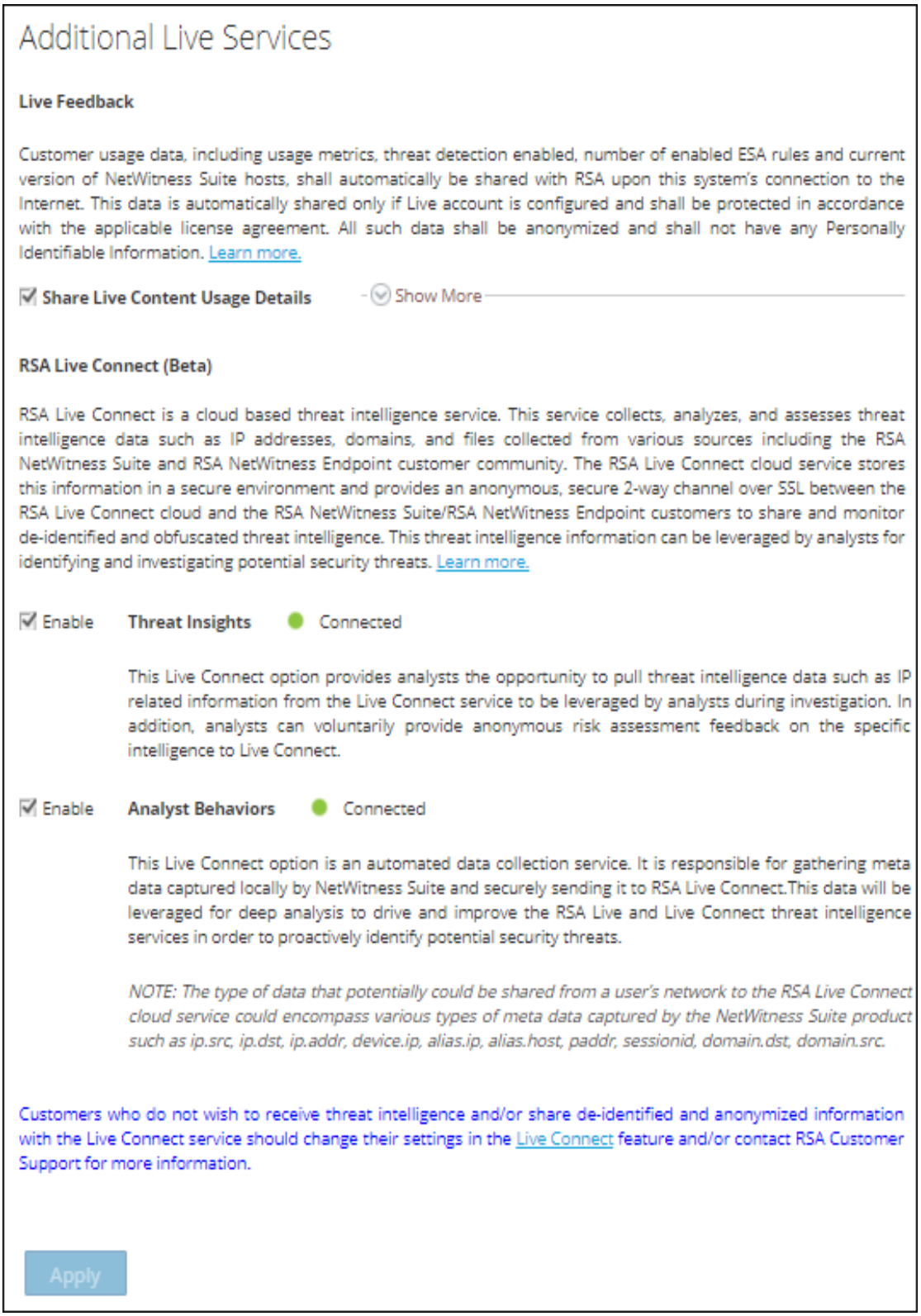
For information about configuring Live Account and Live Services, see the **Configure Live Services Settings** topic in the *System Configuration Guide*.

For information about configuring Context Hub service, see the **Step 1. Add the Context Hub Service** topic in the *Context Hub Configuration Guide*.

Enable or Disable Live Connect Data Source

To enable or disable Live Connect data source for Context Hub:

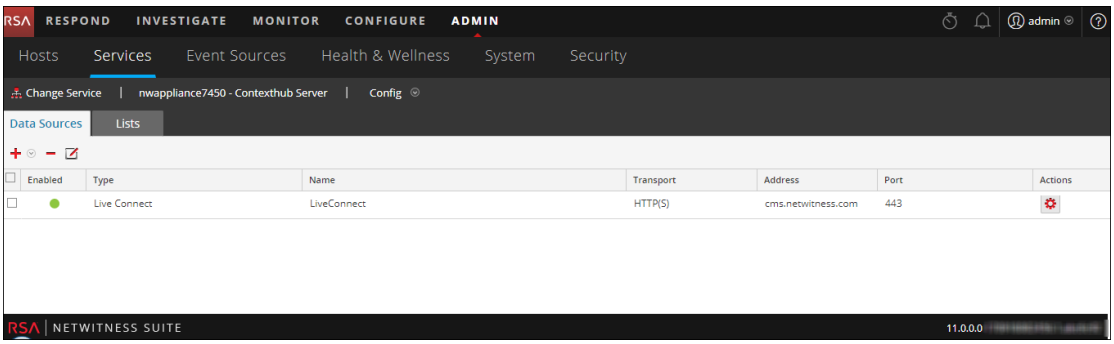
1. Go to **ADMIN > System**.
2. In the left navigation pane, select **Live Services**.
3. In the **Additional Live Services** section, enable **Threat Insights**.



4. Click **Apply**.

   Live Connect data source is enabled for Context Hub service.

5. To verify, go to the **Data Sources** tab and view the available sources.
   Live Connect source must be added to the list of available sources and the **Enabled** field must be a solid green circle ( ).



6. To disable Live Connect data source, disable **Threat Insights** in Additional Live Services panel and click **Apply**.

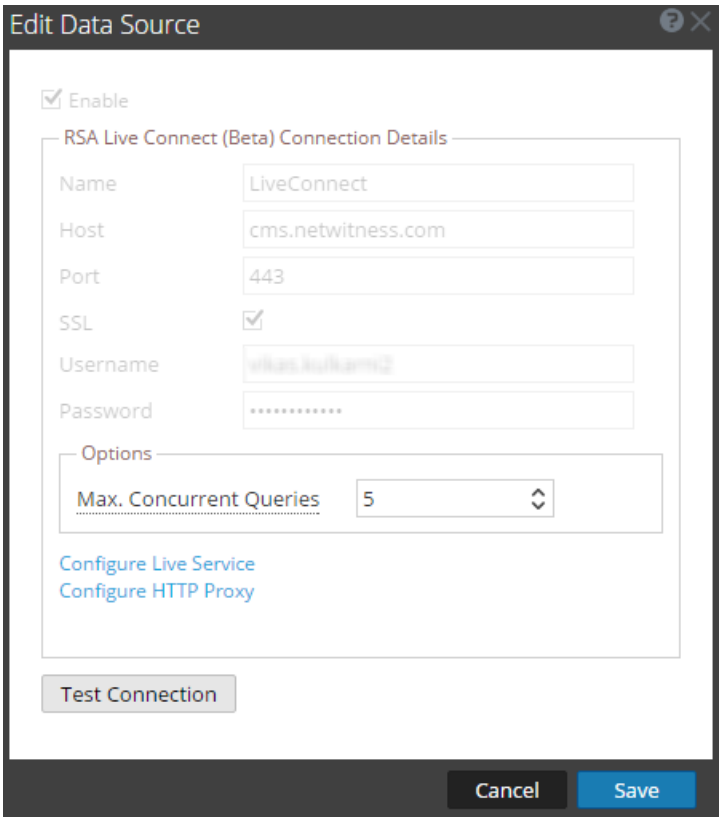
   Live Connect data source is disabled for Context Hub service.

   Note: If Threat Insights is disabled, the Context Lookup panel for Live Connect (in the Investigation Navigate view and Events view) displays a message to configure the Live Connect data source. To view contextual data for Live Connect, you must enable Threat Insights.

Edit Live Connect Data Source Settings

To edit live connect data source for Context Hub:

1. In the main menu, select **Admin > Services**.
   The Services view is displayed.
2. In the **Services** panel, select the Context Hub service, and > **View** > **Config**.
   The Services Config view is displayed.
3. In the **Data Sources** tab, select the live connect data source and click .
   The **Edit Data Source** dialog is displayed.



4. Edit the required fields:

Field	Description
Max. Concurrent Queries	You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 25.

5. To edit the Live Connection and Proxy settings, do the following:
   - To edit the Live Connection settings, see the **Live Services Configuration Panel** topic in the *System Configuration Guide*.
   - To edit the proxy settings, see **the HTTP Proxy Settings Panel** topic in the *System Configuration Guide*.
6. Click **Test Connection** to test the connection between Context Hub and the data source.
7. Click **Save** to save the settings.

Next steps

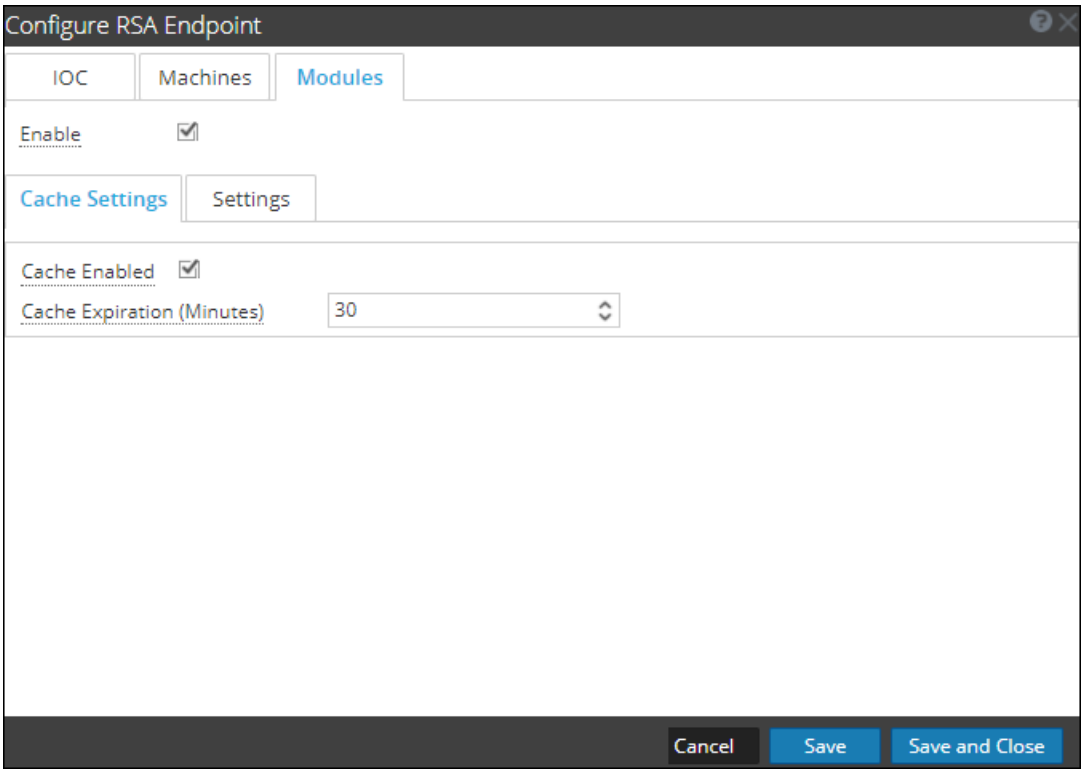
After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA Netwitness Respond User Guide* and the *RSA NetWitness Investigation and Malware Analysis Guide*.

Configure Context Hub Data Source Settings

After you have configured the required data sources you can customize the settings for the data sources based on your requirement.

To access and configure settings:

1. Go to **ADMIN**> **Services**.
   The services view is displayed.
2. In the Services panel, select the Context Hub service and click > **View** > **Config**.
   The Services Config view of Context Hub is displayed.
3. Select the data source for which you want to configure the settings and click in the Actions column.
   The following screenshot is an example of the NetWitness Endpoint settings dialog:



4. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and can be used to enable or disable the response from the selected data source.
Cache Settings	Any lookup from Context Hub can be stored in the Context Hub cache for a configured time. Response to any subsequent matching request will be fetched from the Context Hub cache. Use this section to define the following cache settings for query lookup: • **Cache Enabled**: By default, this checkbox is selected and the query response is cached. • **Cache Expiration (Minutes)**: The maximum time the query lookup is retained in cache. The default time is 30 minutes and maximum is 7200 minutes that you can configure.
List value Expiration	**Enable**: Select Enable to define the number of days the list values must be available. By default, this option is disabled and the values are retained. **Time to Live (Days)**: Enter the number of days you want to the list values to be retained.
Meta Mapping	Any list stored in Context Hub should be made available for a lookup. The lookup in Context Hub is performed based on meta type or entities. Examples IP, HOST, MAC ADDRESS, DOMAIN, FILE_NAME, FILE_HASH, USER. **Meta Type**: Entities available in Context Hub. **Context Hub Fields**: Column headers from CSV file you have added when adding List Data Source.
Minimum IIOC Score	The minimum IIOC score to be considered for fetching contextual information of Netwitness Endpoint modules.
Query Last (Days)	The duration (in days) for which the Context Data must be queried.
Limit	The maximum number of records to be displayed when Context Lookup is performed.
Recur Every	Configure recurring schedule to fetch and store contextual data for the required intervals.

5. Click any one of the following options:

   - **Cancel** - select this option to cancel the changes.
   - **Save** - select this option to save the changes.
   - **Save and Close** - select this option to save and close the dialog.

Based on the data source you select, the Response Groups differ. The following table describes the response groups for every data source.

Data Source (Connection)	Response Supported Groups	Field Settings
List	List	Meta Mapping Meta Type Context Hub Fields Settings Data Prefetch Settings Schedule Recurrence List Value Expiration Cache Settings Cache Enabled Cache Expiration (Minutes) [Min is 30 minutes Max is 7200 minutes]
RSA Archer	Archer	Cache Settings Cache Enabled Cache Expiration (Minutes)

Data Source (Connection)	Response Supported Groups	Field Settings
Active Directory	Users	Meta Mapping Meta Type Context Hub Fields Settings Data Prefetch Settings Schedule Recurrence List Value Expiration Cache Settings Cache Enabled Cache Expiration (Minutes)[Min is 30 minutes Max is 7200 minutes]
RSA Endpoint	IOC Machines Modules	Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Context Panel Settings Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Context Panel Settings Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Minimum IIOC Score Context Panel Settings

Data Source (Connection)	Response Supported Groups	Field Settings
Respond	Alerts Incidents	Context Panel Settings Data Prefetch Settings Query Last [Days Cache Settings Cache Enabled Cache Expiration (Minutes)
Live Connect	Domain File IP	Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Context Panel Settings

Note: After you configure the data source settings, you can configure the Context Hub configuration parameters by navigating to **ADMIN**> **Services**> **View** > **Explore** view. Make sure you restart the Context Hub service if you make any configuration changes in the Explore view.

Import or Export Lists for Context Hub

As an administrator you can import or export a list that is configured in the Context Hub service which can be used by an analyst. The file to be imported or exported is a CSV file and you can add multiple lists as Data Sources.

Prerequisites

Ensure that Context Hub is enabled and the service is available in **Admin** > **Services** view of NetWitness Suite.

Import a List

After you have imported a list, you can perform the following tasks:

- Import values to an existing list
- Add row to a list
- Edit a list name and description
- Edit a value from a list
- Delete a list
- Delete row from a list

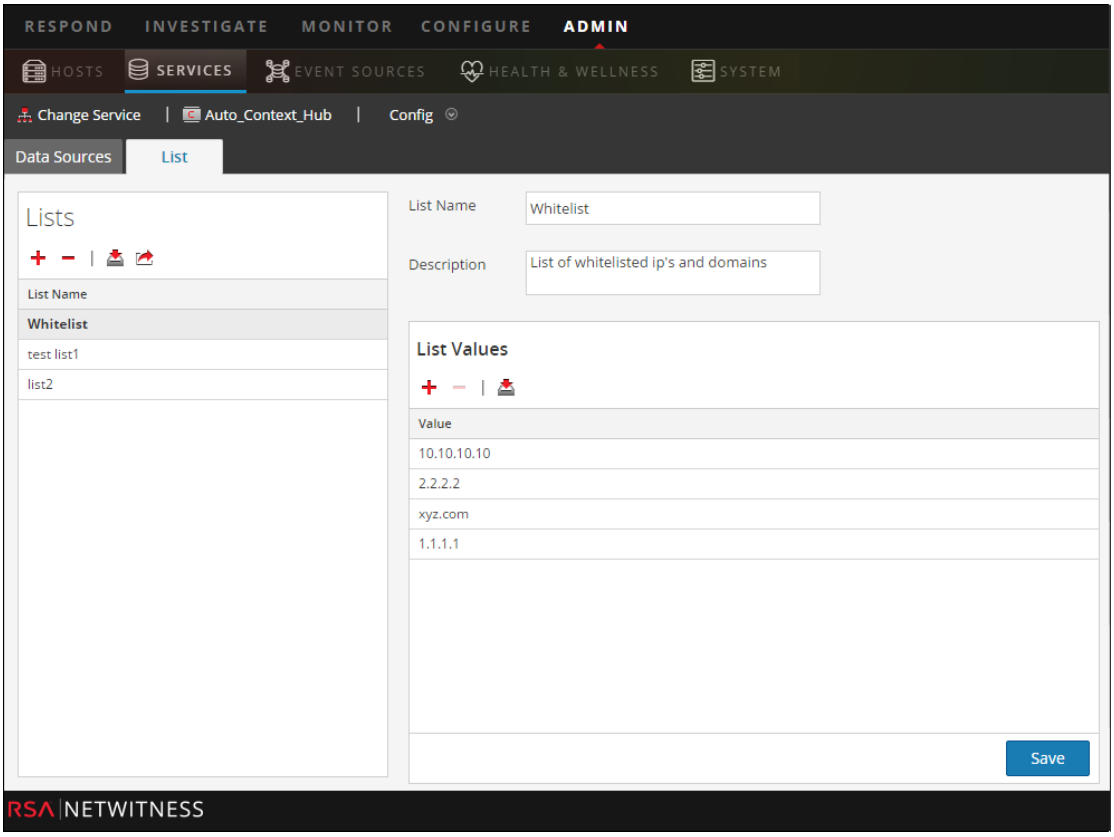
Note: You have to make the same changes to the relevant .CSV file, so that the changes get reflected the next time the schedule recurs. Otherwise, when you import values into an existing single-column or multi-column list, the data is overwritten from the source file the next the schedule recurs.

Import Single-Column List

To import a list:

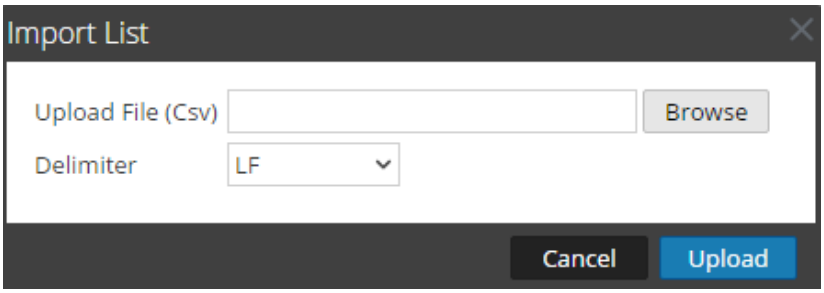
1. Select ADMIN > **Services**.
   The services view is displayed.
2. In the **Services** panel, select the Context Hub service and click > **View** > **Config**.
   The Services Config View of the Context Hub service is displayed.
3. Click the **Lists** tab.
   The Lists tab consists of the **Lists** panel and **List Values** panel.

The below image is an example of single-column list.



4. Click on the **Lists** panel.

   The **Import List** dialog is displayed.



5. In the **Import List** dialog, complete the following steps:

   a. In the **Upload File (.CSV)** field, browse and select the `CSV` file.

   b. In the **Delimiter** field, select the delimiter to separate the values in a list from the options—**Comma**, **CR** (Carriage Return), and **LF** (Line Feed).

6. Click **Upload** to upload the CSV file to Context Hub.

These lists are considered as data sources for retrieving contextual information. But you can append to an existing multi-column list. The data will be appended only if the number of columns match.

Note: You cannot create a new multi column list by importing. For information on how to import multi-column list, see Configure List Data Source for Context Hub.

Import Values to an existing List

When you are importing into existing multi- column list the data is overwritten from the source file when the schedule recurs.

To import values to a list:

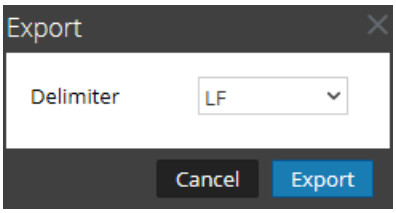
1. Go to **ADMIN** > **Services**.
   The services view is displayed.
2. Service and click > **View** > **Config**.
   The Services Config View of the Context Hub service is displayed.
3. Click the **Lists** tab.
   The Lists tab consists of the **Lists** panel and **List Values** panel.
4. In the Lists panel, select a list for which you want to import the values.
5. Click on the **List Values** panel.
   The **Import List** dialog is displayed.
6. In the **Import List** dialog, complete the following steps:
   a. In the **Upload File (Csv)** field, browse and select the `CSV` file.
   b. In the **Delimiter** field, select the delimiter to separate the values in a list from the options—**Comma**, **CR**(Carriage Return), and **LF**(Line Feed).
7. Click **Upload** to upload the CSV file to NetWitness Suite.

The list values are imported to the selected list. These lists are considered as data sources for retrieving contextual information. But you can append an existing multi column list. The data will be appended only if the number of column match.

Export List for Context Hub

To export a list:

1. On the **Lists** tab of the Services Config view of the Context Hub service, click .
   The **Export** dialog is displayed.



2. In the **Delimiter** field, select the delimiter to separate the values in an exported list from the drop-down [**Comma**, **CR** (Carriage Return), and **LF** (Line Feed)].
3. Click **Export**.

In case of a single-column list, you can select the delimiter. And, in case of a multi-column list, the list is exported as CSV file. to the local machine.

Configure Meta Type Mapping for Context Hub

As an administrator you manage the mapping of Context Hub meta types with Netwitness meta keys.

The Context Hub service provides context lookup for meta values in the Respond and Investigation views. These meta values are grouped into meta types based on the category they belong to. For example, meta keys of NetWitness Suite Respond and Investigation like `ip.src` and `ip.dst`are grouped into the meta type `IP` in Context Hub. The meta type `IP` is in turn mapped to metas like `alert.events.source.device.ip_address` and `alert.events.destination.device.ip_address` in the RESPOND database.

In the **ADMIN**> **System** > **Investigation** view, the Context Lookup tab enables the administrator to configure the Netwitness meta keys and meta type mapping. The administrator can add or remove meta keys to the list of meta types supported by Context Hub.

The Context Hub service is pre-configured with default meta type and meta key mapping, which is expected to work with most deployments, unless there are some custom mappings created for your specific deployment.

Note: You cannot add a new Meta Type.

The default mapping is given below:

Meta Type Name	Meta Keys
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
MAC_ ADDRESS	eth.dst, eth.src, alias.mac
FILE_ NAME	filename, sourcefile
FILE_ HASH	checksum

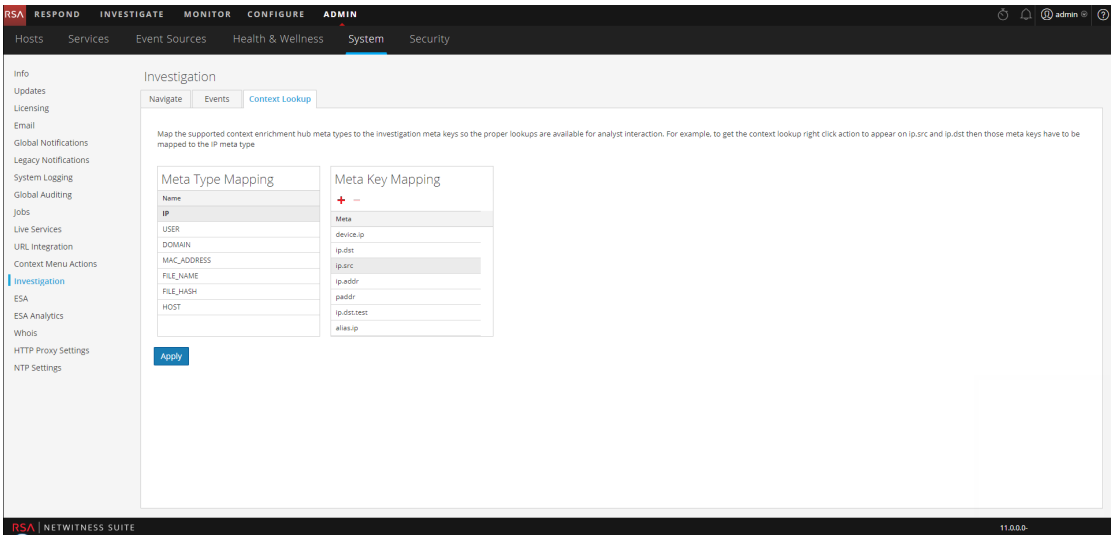
Meta Type Name	Meta Keys
HOST	device.host, alias.host, host.src, host.dst

Procedure

To manage Investigation meta keys mapping:

1. Go to ADMIN > **System**.
2. In the options panel, select **Investigation**.

   The Investigation Configuration panel is displayed.
3. Select the **Context Lookup** tab.



4. Select a meta type to view the default meta keys that are mapped with this meta type.
5. To add a meta key, click + and enter the meta key.
6. To remove a meta key, select the meta key and click −.
7. To save the changes, click **Apply**.
8. In order to add a new meta, they need to be included in the Concentrator's custom index file. For example, if you want to add a meta "**fqdn**" then you need to add an new entry: **<key name="fqdn" description="Fully Qualified Domain Name="IndexValues" format="Text" valueMax="100" />** in the index file. For more information on how to include a new meta in the index file, see Index Customization topic in the *Core Database Tuning*

Guide. After you add the new meta, you can view the contextual information on clicking the Pivot to investigate option in the Respond view.

In case a new meta key is added, the Context Lookup menu option is enabled for the meta values under that meta key. For more information, see the "Investigation Configuration Panel" topic in the *System Configuration Guide*

Context Hub References

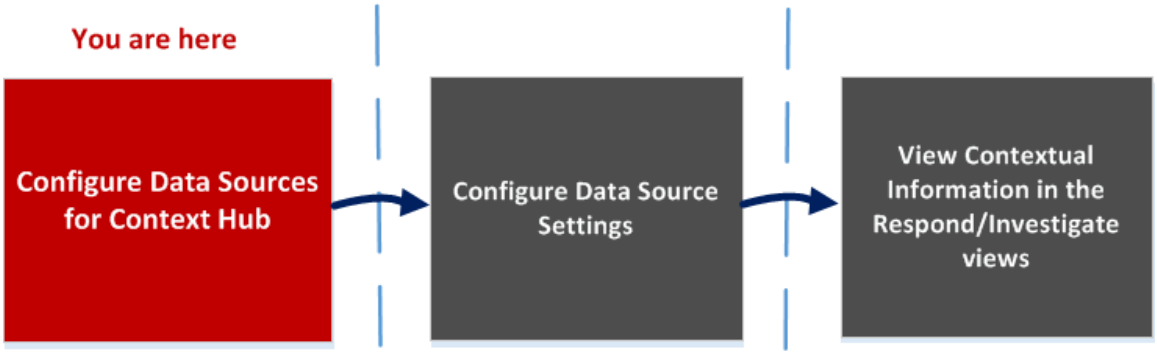
After you have configured the Context Hub service and the required data source, you can manage the settings for each data source. This will help in optimizing and customizing the lookup results.

Context Hub Data Sources Tab

In the **Data Sources** tab, you can configure one or more data sources for Context Hub service. Navigate to **ADMIN** > **SERVICES** > Select Context Hub service > **View** > **Config** > **Data Sources** tab.

Workflow

This workflow shows the procedure to configure data sources for Context Hub service to view contextual information in the Respond / Investigate views.



- The first task is to add a data source
- The second task is to configure data sources settings to enhance your deployment. This task is optional as the settings for each data source is already configured with default values for optimal performance.
- And the third task is to view and analyze the contextual information in the Context Summary panel of the Respond or Investigate views.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Data Sources for Context Hub*	Configure Data Sources for Context Hub
Administrator	Configure Hub Data Settings*	Configure Context Hub Data Source Settings

Role	I want to ...	Show me how
Analyst	View Contextual Information in Respond View	See the *NetWitness Respond User Guide*.
Analyst	Add, create and delete list from the Respond or Investigate View	See the *NetWitness Respond User Guide*. See the *Investigation and Malware Analysis User Guide*.
Analyst	Add or delete an entry from an existing list	See the *NetWitness Respond User Guide*.

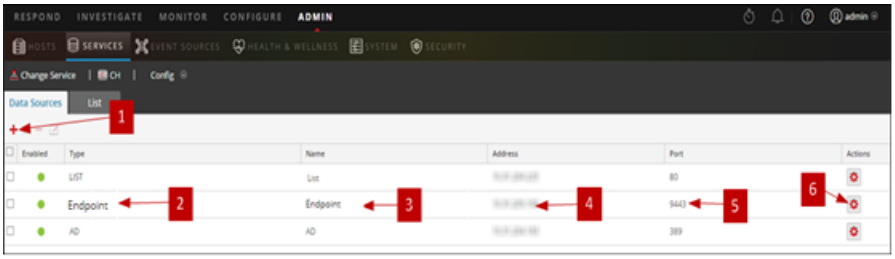
*You can complete this task here (that is in the Context Hub Data Sources Tab.)

Related Topics

- Configure Lists as a Data Source
- Configure Archer as Data Source
- Configure Active Directory as a Data Source
- Configure Netwitness Endpoint as a Data Source
- Configure Respond as a Data Source
- Configure Live Connect as a Data Source for Context Hub

Quick Look

The following example illustrates how to add a data source for Context Hub service.



1 Click + to display the **Add Data Source** dialog.

2 Displays the type of Data Source.

3 Name that identifies the Data Source.

4	The IP address or hostname of the data source.
5	The connection port for the data source.
6	Opens the **Configure Settings** dialog. You can view and edit the settings to be displayed on the Context Summary panel in the Respond or Investigate views.
7	Click **Test Connection** to verify that the host is connected to the Context Hub service.

Toolbar

The following table describes the toolbar actions.

Feature	Description
	Opens the Add Data Source dialog so that you can add a data source. You can add only one data source of each type. Except in case of Lists and Active Directory data sources which can be added in multiples. For detailed instructions to add a data source, see Configure Lists as a Data Source.
	Delete a data source. If you delete a data source, Context Hub does not consider the deleted service as a data source. All contextual information fetched previously will not be available.
	Opens the Edit Data Source dialog. For description of each field in Edit Data Source panel, see Configure Live Connect as a Data Source for Context Hub.
	Opens the Configure Settings dialog. You can view and edit the settings for the data sources. For description of each field in Configure Responses dialog, see Configure Context Hub Data Source Settings .

Data Source Configurations

The following table describes the listed configurations.

Feature	Description
Enabled	Indicates whether the data source is enabled or disabled. A solid colored green circle indicates that data source is enabled ( ). An blank white circle indicates that data source is disabled.

Feature	Description
Type	The type of data source. For example, Lists, Archer, Active Directory, Endpoint, Respond, or Live Connect.
Name	The unique name to identify the data source. For example, Respond \.
Address	The IP address or hostname of the data source.
Port	The connection port for the data source and vary based on the data source being added. For example, for Endpoint the port is 9443, for Lists the port is 80 and so on.

Context Hub Lists Tab

In the **Lists** tab, you can create and configure lists for Context Hub. Navigate to **ADMIN** > **SERVICES** > Select Context Hub service > **View** > **Config** > **Lists** tab.

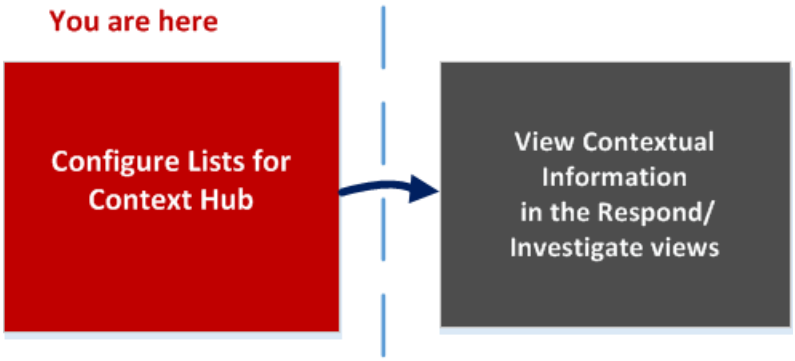
The Lists tab of the Context Hub service allows you to create one or more lists and add relevant list values to the list. These lists are automatically considered as data sources for the Context Hub service.

These lists may be populated with items either by importing CSV files or by adding meta values by using the option Add/Remove from List in Investigation and Respond views.

Note: You can also create lists and add list values from Respond and Investigation views. For more information, see the *RSA NetWitness Respond User Guide* and the *RSA Netwitness Investigation and Malware Analysis Guide*.

Workflow

This workflow shows the procedure to configure lists for Context Hub service and to view contextual information in the Respond and Investigate views.



Creating one or more list is the first task in this workflow. The lists can contain supported metas such as an IP address, User, Host, Domain, MAC address, File Name or File Hash. The next task is to analyze or use the list data to view contextual data in Respond and Investigate views.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure List Data Source for Context Hub*	Configure Lists as a Data Source

Role	I want to ...	Show me how
Administrator/ Analyst	View Contextual Information in Respond View	See the *NetWitness Respond User Guide*.
Administrator/ Analyst	"Manage Lists and List Values in Investigation	See the *Investigation and Malware Analysis User Guide*.
Administrator/ Analyst	Create a list	See the *NetWitness Respond User Guide* and *Investigation and Malware Analysis User Guide*
Administrator/ Analyst	Update a list	See the *NetWitness Respond User Guide* and *Investigation and Malware Analysis User Guide*
Administrator/ Analyst	Delete list	See the *NetWitness Respond User Guide* and *Investigation and Malware Analysis User Guide*
Administrator/ Analyst	Import a list	Import or Export Lists for Context Hub
Administrator/ Analyst	Export list	Import or Export Lists for Context Hub

*You can complete this task here (that is in the Context Hub Lists Tab).

Related Topics

- Context Hub Data Sources Tab
- Troubleshooting NetWitness Investigate

Quick Look

The following example illustrates how to add lists for Context Hub service.

The List tab consists of the **Lists** panel and **List Values** panel. The **Lists** panel has a toolbar with options to add, delete, import, and export lists. The entries under **List Name** are lists that are added or imported for the Context Hub service.

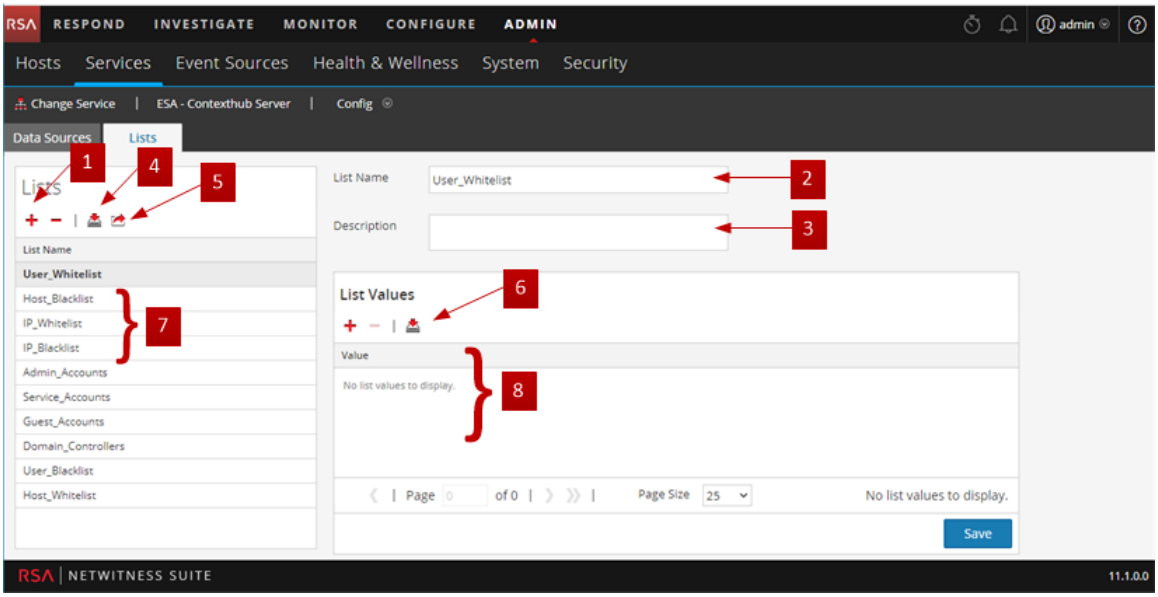
By default, 10 empty single-column lists are available in RSA NetWitness Suite11.1. These lists are empty and you need to add information to these lists. The out of the box 10 list names are used in ESA rules, for more information on ESA rules, see the *Alerting with ESA Correlation Rules User Guide*. For users upgrading from previous versions, they will be able to view these new lists in addition to their previously created lists. The lists available by default are:

- Admin_Accounts
- Guest_Accounts
- Service_Accounts
- User_Blacklist
- User_Whitelist
- Host_Whitelist
- Domain_Controllers
- IP_Blacklist
- IP_Whitelist
- Host_Blacklist

Note: If a list with the same name already exists prior to updating to or installing RSA NetWitness Suite11.1, then that list will be retained. Either rename that list before updating to 11.1 or update the contents in such a way that it can be used in ESA rules.

The lists are available in ESA rules tab in CONFIGURE > ESA Rules > Settings > Enrichment Sources. For more information on ESA rules, see the *Alerting Using ESA Guide for Version 11.1*.

The **List Values** panel has a toolbar with options to add, delete, and import list values to the selected list. The entries under **Value** identify each list entry included in the list.



1 Click + to add a new list.

2	Name that identifies the list.
3	Description of the list.
4	Click to import list(s) to Context Hub.
5	Click to export a list to the local machine.
6	Click to import list values to selected list.
7	Displays the custom list(s) that are added to Context Hub.
8	Displays the list values that are added to the selected list.

Toolbar

The following table describes the toolbar actions.

Feature	Description
	Add a new list. For more information, see Configure Lists as a Data Source.
	Delete a list. If you delete a list from Context Hub, the list is no longer considered as a data source for retrieving contextual information.
	Import lists to Context Hub. For more information, see Import or Export Lists for Context Hub.
	Export a list to the local machine. For more information, see Import or Export Lists for Context Hub.

List View Options

The following table describes the Lists configurations.

Feature	Description
List Name	Unique name to identify the list.
Description	Description of the list.

Feature	Description
Save	Saves the changes made to the list.

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, **Navigate to Context Summary Panel and View Additional Context** topic in the *Investigation and Malware Analysis User Guide*.

Troubleshooting

This topic provides information about possible issues that NetWitness Suite users may encounter when setting up their Context Hub service in NetWitness Suite.

Possible Issues

Problem	Solutions
Prefetch for list fails if the list is created in append mode. The following error message is displayed in logs indicating that, entries in list exceeds the max allowed. `Error setting data source entries com.rsa.asoc.contexthub.exception.ContextHubException: total.entries.exceed.max` Also, Health & Wellness sets the stat - `Contexthub.Datasource.Health.Data-Sources-Health` to `Unhealthy` and displays the names of the lists for which prefetch has failed. For example, number of entries in the list are 50001 and number of records in the CSV file are 50001 (user did not change the csv since last prefetch.). Upper limit on number of entries in list is 100k. Now on prefetch, Context Hub will try to append 50001 entries to the list but since 50001 + 50001 > 100k, prefetch fails.	You should add only those entries in the .csv file which they wish to append to the existing .csv file. If, you do not want to append any entries to the list then perform one of the options, as applicable: • If you created the list with headers: remove all rows from the csv except the header. • If you created list without headers: you should have 0 rows in csv.
SSL handshake with Archer certificate fails while adding it as a data source.	Use an archer generated certificate with the Trust All Certificates option configured.

Problem	Solutions
Pivot to Investigate option on the Respond page does not navigate to the correct link.	When you stop and restart the RabbitMQ server, the Pivot to Investigate option available on the respond screen is not visible. And the context panel for Pivot to Investigate reopens the same page. You need to restart the jetty service on the Netwitness Server, login to the Netwitness Server Host and enter the service jetty restart command.

RSA NETWITNESS® SUITE

Core Database Tuning Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Core Database Introduction 7

NetWitness Suite Products Covered by this Guide 7

Frequently Used Terms 7

NetWitness Core Database History 8

Core Database Strengths and Weaknesses 9

Basic Database Configuration 11

Find Help within the Core Service 11

Packet, Meta, and Session Storage 11

Index Storage 11

Tiered Database Storage 12

Archiver 13

Manifests 13

Search Historical Manifests 15

Advanced Database Configuration 17

Database Configuration Nodes 17

packet.dir , meta.dir , session.dir 17

packet.dir.warm , meta.dir.warm , session.dir.warm 18

packet.dir.cold , meta.dir.cold , session.dir.cold 19

packet.file.size , meta.file.size , session.file.size 19

packet.files , meta.files , session.files 20

packet.free.space.min , meta.free.space.min , session.free.space.min 20

packet.index.fidelity , meta.index.fidelity 20

packet.integrity.flush , meta.integrity.flush , session.integrity.flush 20

packet.write.block.size , meta.write.block.size , session.write.block.size 21

packet.compression , meta.compression 21

packet.compression.level , meta.compression.level 21

hash.algorithm 21

hash.databases 22

hash.dir 22

Index Configuration Nodes 22

index.dir 22

index.dir.warm 22
index.dir.cold 22
index.slices.open 22
page.compression 23
save.session.count 23
reindex.enable 23
SDK Configuration Nodes 23
max.concurrent.queries 24
max.pending.queries 24
cache.window.minutes 24
max.where.clause.cache 24
max.unique.values 24
query.level.1.minutes , query.level.2.minutes , query.level.3.minutes 25
query.timeout 25
max.where.clause.sessions 25
max.query.groups 25
packet.read.throttle 26
cache.dir , cache.size 26
parallel.values 26
parallel.query 26
Per-User Configuration Nodes 27
query.prefix 27
query.level 27
query.timeout 27
session.threshold 27
Scheduler 27
Example 28
Rollover 29
Synchronous Rollover 29
Asynchronous Rollover 29
Example 30

Queries 31

query Syntax 31
where Clauses 33
Query Operators 34
values call 40

Parameters 41
values Flags 43
values Call Example 43
Values call and bucketing mode 44
Suggestion Mode 44
msearch Call 44
msearch Flags 45
msearch Index Search Mode 46
Text Search Syntax 46
Search Syntax And Index Modes 46
msearch Tips 47
Stored Procedures 47
Use of Quotes in Query Syntax 47

Index Customization 49

Index Configuration File Locations 49
Index configuration entries 49
Meta names 50
Data Types 50
Index Levels 51
Value Max 52
maxLength 52
minLength 53
ngrams 53
Numeric Bucketing 53
Key Value Aliases 54
Key Renaming 54
Entities 55
Entity Definition Rules 56
Entities in Brokers 56

Rebuilding the Index 57

Activating the Background Reindexer 57
Controlling the Background Reindexer 57
Background Reindexing Algorithm 57
Background indexer status 58
Effects on Aggregation 58

Forcing A Reindex 58

Optimization Techniques 59

Thresholds 59
Complex where Clauses 59
AND and OR 60
Use Case: Match a Large Subnet 60
Use Case: Substring Matching 61
Index Saves 61
Affects of Increasing the Save Interval 62
Affects of Decreasing the Save Interval 62
Working with valueMax 63
Parallelize Workloads 63
Index Rebuild 63
Scaling Retention 64
Increasing Packet and Meta Retention 64
Increasing Index Retention 64
Scaling Horizontally 64
Grouping Workloads 65
Cache Window 65
Time Limits 66

Appendix A: Statistics 67

Statistics in /database/stats 67
Statistics in /index/stats 68
Statistics in /sdk/stats 68
Per-query Statistics 69

Appendix B: Index Inspect 71

Parameters 71
Response 71
Slice Summary 71
Per-Index Summary 71
Slice Summary Footer 72

NetWitness Core Database Introduction

This topic provides an overview of the NetWitness Core database. The NetWitness Core services contain a proprietary database developed specifically for use within the NetWitness Suite products. It bears little resemblance to traditional relational databases, and is not based on any off-the-shelf database technology. As such, many users find that there is a steep learning curve to understanding how the Core database works, and how to make best use of it. The purpose of this guide is to help NetWitness Suite users understand the database and use it to its fullest potential.

As a System Administrator, you can use this information to help plan your NetWitness Suite deployment, and to tune it for best performance. As an Analyst, you can use this guide to structure your analysis in ways that will return reports faster. As a Content Developer, you can use this guide to help write content that will be processed efficiently by the database system.

NetWitness Suite Products Covered by this Guide

This guide covers the capabilities of NetWitness Suite 11.0. The following NetWitness Suite components contain the Core database:

- Concentrator
- Archiver
- Decoder
- Log Decoder
- Workbench

Frequently Used Terms

Definitions for terms that are used throughout this document are presented here. The terms are listed in the order in which they enter the NetWitness Suite system:

- **Packet DB** : The packet database contains the raw captured data. On a Decoder, the packet database contains packets as captured from the network. Log Decoders use the packet database to store raw logs. The raw data stored in the packet database is accessible by a Packet ID, however, this ID is typically never visible to the end user.
- **Packet ID** : A number used to uniquely identify a packet or log in a packet database.

- **Meta DB** : The meta database contains items of information that are extracted by a Decoder or Log Decoder from the raw data stream. Parsers, rules, or feeds can generate meta items.
- **Meta ID** : A number used to uniquely identify a meta item in the meta database.
- **Meta Key** : A name used to classify the type of each meta item. Common meta keys include ip.src, time, or service.
- **Meta Value** : Each meta item contains a value. The value is what each parser, feed, or rule generates.
- **Session DB** : The session database contains information that ties the packet and meta items together into sessions.
- **Session** : On a packet Decoder, a session represents a single logical network stream. For example, a TCP/IP connection is one session. On a Log Decoder, each log event is one session. Each session contains the references to all the Packet IDs and Meta IDs that refer to the session.
- **Session ID** : A number used to uniquely identify sessions in the Session DB.
- **Index** : The index is a collection of files that provides a way to look up Session IDs using Meta Values.
- **Core Database** : This refers to the combination of the Packet, Meta, Session, and Index.

For syntax definitions, this document uses EBNF grammar definitions.

NetWitness Core Database History

NetWitness (now RSA) developed the Core database for use in packet capture systems. Early in the history of NetWitness, developers identified that existing database technologies would not be able to keep up with the high ingest rate inherent in full packet capture. Contemporary database technologies were not anywhere close to being able to keep up with capturing the number of sessions received every second, much less sorting every packet. Likewise, the volume of data meant that packet storage would need to be discarded and reused just as quickly as it was consumed. This was also a weakness of databases at the time. Thus, NetWitness created a database consisting of the packet, session, and meta databases.

In order to provide the analytical capabilities of NetWitness Investigator, a meta index was added to the NetWitness database. The index shared the same design goals as the original databases. It was designed to sustain a very high insert rate into a high number of very large indices.

The index has evolved considerably over the years. Early versions of the index were only capable of providing summary estimates about how many unique meta values were present in the meta database. Other versions have had great challenges in meeting acceptable query performance. For example, NetWitness 9.0 more frequently measured report times in minutes rather than seconds. The current version of the index is derived from the NetWitness 9.0 index, but has evolved considerably in order to meet performance expectations and to add new features.

Core Database Strengths and Weaknesses

Strengths:

- High sustained insert rates, without needing down time for bulk inserts.
- Decent query performance simultaneous with high insert rates.
- Automatic cleanup and rollover of old data with minimal fragmentation.
- Extremely high number of meta value indices: more than 100 enabled by default on a Concentrator.
- Ability to scale to Petabyte database sizes and Terabyte index sizes within a single node.
- Using meta key-value pairs, it is very flexible for storing arbitrary meta items within a session. Thus a session can be used to represent nearly any kind of data record.

Weaknesses:

- The query functionality is limited and low level.
- The packet, meta, and session DB schema is fixed, and all customization is done through custom meta keys and values.
- The database provides no transaction atomicity guarantees as you might expect to find in a SQL database.

Basic Database Configuration

This topic covers basic database configuration settings of NetWitness Core services. For information on how to configure the Core services by editing configuration files, see "Service Configuration Settings" in the *Host and Services Getting Started Guide* .

This document assumes that the reader has some familiarity with adjusting the configuration of a NetWitness Core service. To use this document, you should be familiar with one of the mechanisms for modifying the configuration tree of Core services. Examples of such mechanisms include the Explorer view of the Administration pages within the NetWitness Suite user interface, or the REST interface accessible on each service through a web browser.

Find Help within the Core Service

Each configuration item within a Core service has a built-in help description of what the item does. You can view this help information by hovering your mouse over the configuration item in the Explorer view. Each configuration item also indicates whether it can be changed without restarting or if a restart of the service is needed for the change to take effect.

Developers using the REST API can retrieve the help text for each configuration item by sending the `help` message to the configuration node path.

Packet, Meta, and Session Storage

Each of the packet, meta, and session databases are configured through the `/database/config` folder on each NetWitness Core service. Each database has a configurable parameter to specify where the Core service stores data. Packet, meta, and session databases follow a predictable pattern for all of their configuration entries. Configuration items for the packet database start with the prefix `packet` , meta database configuration starts with the prefix `meta` , and the session database configuration items start with the prefix `session` .

Index Storage

The index configuration is stored in the `/index/config` folder on each Core service.

Topics

- Tiered Database Storage
- Manifests

Tiered Database Storage

This topic describes tiered database storage and provides recommendations for Hot, Warm, and Cold tier storage.

Starting with version 10.4, the Archiver service has the capability to be configured to use tiered storage. The concept of tiered storage is to put the most recent data on a Hot tier, which is the fastest storage available on the Archiver.

All services use the Hot tier by default.

The next tier is known as Warm and is typically cheaper and slower storage, such as a network-attached storage (NAS). The Warm tier contains older data; how old depends upon how much storage is allocated on the Hot tier and the average ingest rate. When the Hot tier reaches max utilization, the natural progression is to move the oldest data from the Hot tier to the Warm tier. When configured correctly, this happens automatically and is invisible to the end user. Queries and data access happen automatically no matter what tier (Hot or Warm) the data resides on. However, there can be a performance impact when accessing data on the Warm tier as compared to the Hot tier, because access times on the Warm tier are typically slower.

In addition to Hot and Warm, there is also a Cold tier. The Cold tier is only used as a staging area for offline backup. NetWitness Core services do not access data on the Cold tier. NetWitness Core services move the oldest data to the Cold tier and consider it abandoned (the service no longer accesses the data). This data can then be backed up to long-term storage like tape for possible restoration months or even years later, depending on requirements. The backing up and subsequent removal of data on the Cold tier must be handled outside of NetWitness Core services via scripts or other processes.

If the Cold tier becomes full because external processes are not removing data in a timely manner, this causes the NetWitness Core service to eventually stop the ingestion of new data until the problem is corrected.

When moving data to the Cold tier, RSA recommends that the directory remain on the same mount point as where it is being moved from. Therefore, if the files are coming from the Warm tier, it is far better for performance reasons to set the Cold tier directory on the same file system. The reason for this is that the service attempts to simply move the file and directory to the Cold tier, which is a nearly instantaneous operation on the same file system. If the move fails, the fallback is to copy the data to the Cold tier, which takes more processing time and causes additional I/O contention on the tier from which it is being copied.

Archiver

The tiers of storage capabilities are used by the Archiver. You can configure Archiver to only use Hot storage (the default), Hot and Warm, or all three (Hot, Warm and Cold). All services must use Hot, you cannot configure a service to only use Warm. Data flows from Hot to Warm and finally to Cold. You can also skip Warm and go from Hot to Cold. If Cold (offline) storage is not configured, the oldest data is deleted on the last configured tier, which has been the standard operating procedure.

The typical Archiver deployment sets all the databases to unlimited size (packet.dir, meta.dir, session.dir, index.dir, and optionally the Warm tier variants), which means that the size specifier is left off or set to zero. This lets the databases and index grow unbounded. Instead of each database managing their own size and rolling out only when each individual database exceeds their configured size, Archiver rolls out everything together using the `/index sizeRoll` command. This enables the databases and index to roll out in unison. For more information on sizeRoll, see "Asynchronous Rollover" in Rollover .

Archiver is typically configured to place the index, session, meta, and packet (log) DB on the same volume, instead of multiple volumes like a Concentrator or Decoder. Although this can potentially cause more I/O contention when concurrent reads happen across multiple databases, it also maximizes overall retention. Because all databases are on the same volume, they are configured to roll out together, which minimizes orphaning of data. Decoder and Concentrator are configured for maximum I/O speed, but can suffer from estimates on the proper volume sizing.

For example, if the session DB is too large, it may have enough storage for six months of retention, whereas the meta DB and index only have retention for four months. Because the session, meta DB, and index are intricately tied together, the shortest retention period for all three define the overall retention period (in this case, four months). Retention of individual databases is mostly affected by factors beyond our control, such as traffic captured, meta generated (parsers, feeds, rules) and filtering. The databases are easily resized by a simple configuration change, but this usually also involves changes at the hardware and file system level to adjust partitions, which complicates dynamic resizing. Archiver avoids these problems by using a single volume for everything, with the trade-off of somewhat slower I/O speed.

Manifests

This topic describes manifest files and provides an example manifest for a meta DB file. It also describes manifest searching and provides an example manifest search.

Manifest files are created with every session, meta, and packet (log) DB file and index slice directory. A manifest file is a file that describes several key pieces of information about the data to which it refers. Manifest files are written as a JSON record. Manifest files travel with the data they represent from tier to tier. If the data they represent is deleted, the manifest file is also deleted, except in the following special case. If the service has `/database/config/manifest.dir` configured to a valid directory, at the point when the manifest data is deleted, a copy of the manifest file is placed into the directory pointed at by `manifest.dir` (the directory is created if it does not exist). This enables a NetWitness Suite feature called historical manifest searching.

The intention of this process is to keep historical manifest files for years, in one location for offline querying. As you might imagine from a service running for many years, this can potentially generate hundreds of thousands of files. This should not be a concern however, as the service automatically compresses files into a single archive in order to save space when they grow too numerous. Manifest files are very small and compress well.

Example manifest (`meta-000000023.nwmdb.manifest`) for a meta DB file:

```
{
    "filename" : "meta-000000023.nwmdb",
    "size" : 185153768,
    "fileTime" : 1403903940,
    "id1" : 150814110,
    "id2" : 159341086,
    "session1" : 4023382,
    "session2" : 4250442,
    "time1" : 1403903879,
    "time2" : 1404739851
}

filename  = The filename for the db file the manifest represents
size      = The size in bytes of the db file
fileTime  = The time the file was created
id1       = The starting id in the file (for this example, the starting
meta ID)
id2       = The last id in the file (for this example, the last meta ID)
session1  = The starting session ID of the first meta in the file
session2  = The last session ID of the last meta in the file
time1     = The POSIX time of the first "time" meta found in the file
time2     = The POSIX time of the last "time" meta found in the file
```

In this example manifest, the most important fields are `fileTime` , `time1` and `time2` . All three fields are written in POSIX time. `time1` and `time2` are the starting and stopping times of the meta recorded in the meta DB file `meta-000000023.nwmdb` . In particular, `fileTime` is always the time in which the file was created (not last modified). `time1` and `time2` are representative of the min and max range of the parsed data within the meta DB file. When doing historical searches by time, `time1` and `time2` are preferred over `fileTime` , when they are present. Manifest files for the other databases and index contain some different fields, but all have enough information to perform time based queries.

Search Historical Manifests

When manifests are collected in the directory pointed to by `manifest.dir` , it is assumed that the data they refer to was copied to the Cold tier and eventually backed up to offline storage. Because the historical manifests are still accessible by the service, this allows time-based queries to be performed on offline data, in order to determine what data needs to be restored for a given time range.

You can search manifests using the `/database manifest` command:

```
manifest: If a manifest directory is defined, it will allow operations
on the manifest files (such as a time based query) for database files in
cold storage.
security.roles: database.manage
parameters:
   op - <string, optional, {enum-one:query|compress}> The operation to
perform (defaults to query)
   time1 - <date-time, optional> The beginning time (UTC) for matching
offline database files
   time2 - <date-time, optional> The ending time (UTC) for matching
offline database files
   timeFormat - <string, optional, {enum-one:posix|simple}> Specify the
time format that is returned (posix, simple), default is posix
```

Example search:

```
/database manifest time1="2014-04-20 11:00:00" time2="2014-04-11
11:20:00" timeFormat=simple
```

The search returns all manifests that match the query:

```
[ filename=meta-000001691.nwmdb size=4843826176 fileTime="2014-Apr-20
11:06:34" id1=301555027452 id2=301733101896 session1=15352020201
session2=15361024200 time1="2014-Apr-20 11:05:34" time2="2014-Apr-20
```

```
11:16:34" compression=gzip ]
[ filename=session-000001865.nwsdb size=268439552 fileTime="2014-Apr-20
11:06:35" id1=14674145801 id2=14682041000 metaId1=288217522208
metaId2=288370660984 packetId1=11733872441 packetId2=11741745303 ]
[ filename=session-000001866.nwsdb size=268439552 fileTime="2014-Apr-20
11:18:31" id1=14682041001 id2=14689936200 metaId1=288370660985
metaId2=288520616949 packetId1=11741745304 packetId2=11749618589 ]
```

The returned results can be used to correlate which files should be restored from backup for the given time range. For NetWitness Suite 10.4 and later, a service called Workbench can be used to take the restored files and provide a query interface over the restored data using one or more collections.

Setup of the Workbench service is beyond the scope of this document. For more information, see "Configure Data Backup and Restore" in the *Archiver Configuration Guide* .

Advanced Database Configuration

This topic explains the advanced configuration options of the NetWitness Core database.

The configuration options of the NetWitness Core database may change from one release to the next. However, many of the configuration items do not change frequently and are documented here. This is not an exhaustive list, since new features are added in every release, and they may require new configuration items. For the most up-to-date documentation, refer to the built-in help functionality of the NetWitness Core service.

Topics

- Database Configuration Nodes
- Index Configuration Nodes
- SDK Configuration Nodes
- Per-User Configuration Nodes
- Scheduler
- Rollover

Database Configuration Nodes

This topic describes database configuration nodes. The following database configuration nodes are some of the advanced database configuration items of the NetWitness Core database that do not change frequently.

packet.dir,meta.dir,session.dir

This is the primary configuration entry for each database (also known as the Hot tier). It controls where in the file system the respective databases are stored. This configuration entry understands a complex syntax for specifying many directories as storage locations.

Configuration syntax:

```
config-value = directory, { ";" , directory } ;
directory    = path, [ ( "=" | "==" ) , size ] ;
path         = ? linux filesystem path ? ;
size         = number size_unit ;
size_unit    = "t" | "TB" | "g" | "GB" | "m" | "MB" ;
number       = ? decimal number ? ;
```

Example:

```
/var/lib/netwitness/decoder/packetdb=10
t;/var/lib/netwitness/decoder0/packetdb=20.5 t
```

The size values are optional. If set, they indicate the maximum total size of files stored there before databases roll over. If the size is not present, the database does not automatically roll over, but its size can be managed using other mechanisms.

The use of = or == is significant. The default behavior of the databases is to automatically create directories specified when the Core service starts. However, this behavior can be overridden by using the == syntax. If == is used, the service does not create any directories. If the directories do not exist when the service starts, the service does not successfully start processing. This gives the service resilience against file systems that are missing or unmounted when the host boots.

If you modify the size of a directory in use, the size takes effect immediately, as long as it is larger. If the size is smaller, it is ignored if it is more than 10 percent smaller than the existing size. This prevents an accidental mistype that causes a enormous loss of data. For example, if the packet database was configured for `12 TB` and someone mistyped it as `12 GB` , the database would end up deleting over 11 TBs of data in order to shrink it down to just 12 GB. Instead, the database ignores the `12 GB` setting and logs a warning, so that the error can be caught quickly. Of course, if the size specified is actually correct and more than a 10 percent difference from the existing size, the only recourse for it to take effect is to restart the service. When it starts back up, it assumes the size is correct and adjusts the database to the new size by rolling out the oldest data until the new size is reached. If you actually do want to adjust the size downward and by more than 10 percent without restarting the service, you need to modify the size multiple times, each time adjusting it by less than 10 percent. Watch the service logs to know when the database has adjusted to the new size, as it only adjusts the total database size when the latest file being written has been closed.

If new directories get added or deleted (semicolon separated), they do not take effect until the service restarts.

packet.dir.warm,meta.dir.warm,session.dir.warm

These settings are optional and are used for Warm tier storage on an Archiver. By default, they are blank and unused. If configured, they follow the same format and behavior as `packet.dir` , `meta.dir` , and `session.dir` (see _ `packet.dir` , `meta.dir` , and `session.dir` _ above). When configured, the oldest file on the Hot tier moves to the Warm tier when no available space remains in the Hot tier.

packet.dir.cold,meta.dir.cold,session.dir.cold

These settings are optional and are used to move files from either a Hot or Warm tier storage system to the Cold tier directory specified. Specifically, this setting is nothing more than a directory, there are no size specifiers. However, the defined path name has a few special format specifiers that you can use to name the directory with the date of the data in it.

```
%y   = The year of the data being moved to the cold tier
%m   = The month of the data being moved to the cold tier
%d   = The day of the data being moved to the cold tier
%h   = The hour of the data being moved to the cold tier
%##r = A block of time within a day. So %12r would create two blocks, 00
and 01\. 00 for all data in the AM, 01 for all PM data
```

Example setting:

```
packet.dir.cold = /var/lib/netwitness/archiver/database1/alldata/cold-
storage-%y-%m-%d-%8r
```

For the setting above, if a log database file was about to be moved to cold storage and it was created on `2014-03-02 15:00:00`, it would be moved to the following directory on the Cold tier:

```
/var/lib/netwitness/archiver/database1/alldata/cold-storage-2014-03-02-
01
```

The last number `01` needs some explanation. The `%8r` specifier breaks the hours of the day into 24 / 8 = 3 parts. The first eight hours of the day would be block `00`, so 12 a.m. to 8 a.m. The next eight hours are from 8 a.m. to 4 p.m. and are assigned block `01`. Since the data being moved to cold storage was created at 3 p.m., it falls into block `01`. The `%r` format specifier is useful for backing up files with a granularity somewhere between a day `%d` and a single hour `%h`. The Cold storage directory is created on demand and is defined by the data being moved when the format specifiers are used.

The ability to add a date to the path of the data is just a convenience added for backup and restore. It is a way of tagging the data with a date in the path.

packet.file.size,meta.file.size,session.file.size

This controls the size of the files created with each database. It is normally not necessary to change these values as the default values typically work well. This setting takes effect immediately for subsequent files.

packet.files,meta.files,session.files

This setting controls the number of files held open by the database. You can increase this value to improve performance: however, the operating system has an overall limit on the number of files that service can keep open. If this limit is exceeded, an error is reported and the service does not function. This setting takes effect immediately.

In NetWitness Suite 10.6 and later, the default value for packet.files, meta.files, and session.files is `auto` and the service manages the number of open files based on this criteria:

1. Number of collections
2. Amount of system memory

When set to `auto` , the number is dynamic and you can view it in the logs when it changes. For NetWitness Suite 10.6, RSA recommends that you set this value to `auto` and do not change it to a specific number.

packet.free.space.min,meta.free.space.min, session.free.space.min

This setting provides a safety limit on the minimum free space that exists on the paths specified by the packet.dir, meta.dir, and session.dir directories, respectively. This setting is used to prevent the service from running out of space in the event that other programs have filled up the space that should be dedicated to each of the databases. This setting takes effect immediately.

packet.index.fidelity,meta.index.fidelity

This setting controls how frequently packet ID locations and meta ID locations are indexed. This setting can be increased to reduce the amount of space needed by each packet or meta nwindex file, but increasing the setting reduces the speed at which individual packets or meta items can be located. This setting takes effect immediately.

The session database does not have a fidelity setting because it does not generate index files.

packet.integrity.flush,meta.integrity.flush, session.integrity.flush

This setting controls whether the database forces a sync operation on the file system when it is finished writing a file. The default value is `sync` , which means when a file is closed there will be a significant delay while the data writes to non-volatile storage. It may be necessary to set this to `normal` in order to achieve higher sustained write rates, especially on a Decoder. This setting takes effect on the next file created. Therefore, it is expected that at least one more sync will happen if the value was just changed to `normal` .

If packet drops are occurring and packet.integrity.flush is set to `sync` , set it to `normal` and monitor. Keep the session and meta flush settings on `sync` . If packet drops are still problematic, then set all three to `normal` and monitor.

packet.write.block.size,meta.write.block.size, session.write.block.size

The block size represents how much data is allocated at a time within each database file. Larger block sizes can provide higher throughput and compression ratios, and can improve the rate at which items can be retrieved from the database sequentially. However, larger block sizes have a detrimental impact on random read speed for compressed packet and meta items. This setting takes effect immediately.

packet.compression,meta.compression

These parameters control whether the databases compress data. Compression reduces the amount of storage needed by each database, but it can have a major detrimental impact on the speed at which items are written to the database, and the speed at which items are retrieved from the database. Changes take effect immediately on the next file creation.

As of NetWitness Suite 10.4, the valid values for this parameter are `gzip` , `bzip2` , `lzma` , or `none` . `gzip` is the preferred algorithm when compression is used, because it provides a good balance between performance and space savings. Both `bzip2` and `lzma` can achieve better space savings, but the tradeoff in speed is substantial and likely should only be considered for low ingest speeds and when storage space is at a premium.

packet.compression.level,meta.compression.level

You can use these settings to further refine how the compression algorithms behave. They have no effect when compression is disabled. The valid values are between 0–9\. The default value of zero means let the software pick the best setting for speed and compression. The values between 1 and 9 are used as a sliding scale between performance (1) and compression (9). The value of 9 typically gives you the best compression for a given algorithm, but the worst performance. Somewhere in the middle is usually the best setting, which is what zero picks.

hash.algorithm

This setting controls how the database files are hashed. The default value is `none` , so no hashing is performed. The valid values are `none` , `sha256` , `sha1` , or `md5` . Database files can be hashed to provide evidence that they have not been tampered with since they were closed. Hashing is time intensive and affects ingest performance when enabled. This change takes effect immediately.

hash.databases

This setting controls which databases are hashed. Valid values are `session` , `meta` , and `packet` and are comma separated when hashing multiple databases. This change takes effect immediately.

hash.dir

This setting is normally empty, which means the hash file is created in the same directory as the database file that was hashed. If this setting is defined, the hash file is written to the directory specified instead. This could be some form of write-once storage for resilience against hash tampering.

Hash files are small XML files containing the hex encoded hash along with metadata about the database file that was hashed.

Index Configuration Nodes

This topic describes index configuration nodes. The following index configuration nodes are some of the advanced database configuration items of the NetWitness Core database that do not change frequently.

index.dir

The `index.dir` setting controls where the files used by the index are stored. This setting supports the same syntax as the `packet.dir` , `meta.dir` , and `session.dir` settings.

index.dir.warm

The Warm tier storage for index slices. This setting supports the same syntax as `packet.dir.warm` , `meta.dir.warm` , and `ession.dir.warm` .

index.dir.cold

The Cold tier storage for index slices. This setting supports the same syntax as `packet.dir.cold` , `meta.dir.cold` , and `session.dir.cold` .

index.slices.open

This setting controls the number of index slices held open by the index. Index slices are opened automatically as needed by queries. When queries complete, the index engine may hold the slices open so that subsequent queries execute faster. The most recently created slices are the slices that will be held open, since they are mostly likely to be used by queries.

If queries against the index require the index to open slices, then they will execute slower than if the slices were already open. Therefore, this parameter should be tuned such that most queries executed against the index will work on open slices. However, each open index slice consumes some resources, such as file handles and memory. If there are too many index slices open, the overall performance of the service can suffer.

You should set this parameter so that the open index slices will cover most of the time ranges that most queries will need. For example, if most queries are over the past two weeks, and there are index slices created every 8 hours, then there are 14 days x 3 slices per day, or 42 slices created over the past two weeks. Thus, you could set index.slices.open to 42 so that only slices that are likely to be used are held open.

If this parameter is set to 0, then all slices are held open until the next index save. In this scenario, the only thing limiting the number of slices open in the process is the number of slices in the index.

`page.compression`

Deprecated. Versions of the NetWitness Core index between 9.8 and 10.2 supported two different index compression algorithms, and you can choose between them using this setting. As of 10.3, the only recommended value is the default of `huffhybrid` .

`save.session.count`

This setting controls how often the index is automatically saved when new sessions are inserted. If the value of save.session.count is greater than 0, any time more than `save.session.count` sessions are added to the index, the index automatically saves itself. If the `save.session.count` is set to 0, this feature is disabled and the index will not automatically save itself when new sessions are added to the index.

`save.session.count` can be used to implement an automatic save pattern that is based on the volume of data that enters the index. This is useful because it allows a lightly loaded system to generate save points less often.

For more information on the topic of index saves, see the section in this guide on Optimization Techniques .

`reindex.enable`

This setting controls the operation of the background reindexer .

SDK Configuration Nodes

This topic describes the SDK configuration nodes that affect the database. There are some additional configuration items in each Core service that affect the database, but do not actually affect how the database stores or retrieves data. These settings exist in the `/sdk/config` folder.

max.concurrent.queries

This setting controls how many query operations are allowed on the database simultaneously. Allowing more simultaneous query operations can improve overall responsiveness for more users, but if the query load of the Core service is very I/O bound, having a high max.concurrent.queries value can have a detrimental effect. The recommended value is near the number of cores on the system, including hyper threading. Thus, for an appliance with 16 cores, the value should be somewhere close to 32\. Subtract a few for aggregation threads and general system response threads. Subtract a few more if this is a hybrid system (for example, both a Decoder and Concentrator running on the same appliance). There is no magic number, but somewhere between 16 and 32 should work well.

max.pending.queries

This setting controls the backlog size for the query engine of the database. Larger values allow the database to queue more operations for execution. A queued query does not make progress on its execution, so it may be more useful to make the system produce errors when the queue is full, rather than allowing the queue to grow very large. However, on a system that is primarily performing batch operations such as reports, there may be no detrimental effect to having a large queue.

cache.window.minutes

This setting controls a feature of the query engine that is intended to improve query responsiveness when there are a large number of simultaneous users. For more information on cache window, see Optimization Techniques .

max.where.clause.cache

The where clause cache controls how much memory can be consumed by query operations that need to produce a large temporary data set to evaluate sorting or counting. If the where clause cache size is overflowed, the query still works, but it is much slower. If the where clause cache is too large, it is possible for queries to allocate so much memory that the service would be forced into swap or run out of memory. Thus, this value multiplied by the max.concurrent.queries should always be much less than the size of physical RAM. This setting understands sizes in the form of a number followed by a unit, for example `1.5 GB` .

max.unique.values

The maximum unique values limits how much memory can be consumed by the SDK Values function. SDK Values produces a sorted list of unique values. In order to produce accurate results, it may need to merge together large numbers of unique values from many slices. This merged set of values must be held in memory, so this parameter exists to put a limit on how much memory the merged value set can consume. The default value will limit memory usage to approximately 1/10th of total RAM.

query.level.1.minutes,query.level.2.minutes, query.level.3.minutes

These settings are available in NetWitness Suite 10.4 and earlier versions.

In NetWitness Suite 10.4 and earlier, the Core database supports three query priority levels. Each user is assigned to one of the priority levels. Therefore, there are up to three groups of users that can be defined for the purposes of performance tuning. These settings control how long each user level is allowed to execute the queries. For example, lower privileged users may have a lower value so that they are not able to use all the resources of the Core service with long-running queries.

query.timeout

This setting is available in NetWitness Suite 10.5 and later versions.

Query levels have been replaced in NetWitness Suite 10.5 and later with per user account query timeouts. For trusted connections, these timeouts are configured on the NetWitness Suite server. For accounts on Core services, there is a new config node under each account called `query.timeout` , which is the maximum amount of time in minutes that each query can run. Setting this value to zero means no query timeout will be enforced by the Core service.

max.where.clause.sessions

This setting is available in NetWitnes Suite 10.5 and later versions.

This setting imposes a limit on how many sessions can be scanned by a single query. For example, if a user selects all meta from the database, the database stops processing results once the number of sessions read for the query reaches this configuration value. The value of 0 disables this limit.

The number of sessions needed to fully process a query is equal to the number of sessions that match the WHERE clause of the query, assuming that all terms in the where clause have a suitable index. If there are terms in the where clause that are not indexed, the database has to read more sessions and meta, and reaches this limit sooner.

max.query.groups

This setting is available in NetWitness Suite 10.5 and later versions.

This setting imposes a limit on the number of unique groups collected in a single query. For example, if a query has a group by clause with multiple metas that have high unique value counts, the amount of memory needed for that query could easily outpace the amount of RAM available on the server. Thus, this limit exists to prevent out-of-memory conditions from happening.

Setting a value of 0 disables this limit.

packet.read.throttle

This is a decoder-only setting that affects the access to the packets database. When packet.read.throttle is set to a value greater than 0, the decoder attempts to throttle packet reads when it detects packet contention on the packet database. Higher numbers provide more throttling. Changes takes effect immediately.

cache.dir,cache.size

All NetWitness Suite Core services maintain a small file cache of raw content extracted from the device. These parameters control the location (cache.dir) and size (cache.size) of this cache.

parallel.values

This setting is available in NetWitness Suite 10.5 and later versions.

This setting allows SDK-values operations to be executed in parallel. If this is set to 0, it will disable parallel execution. If it is set to a value greater than 0, it represents the number of threads created when each SDK-values operation is executed. The maximum value is the number of logical CPUs available when the process started.

Setting a higher value for parallel.values is useful when there are small numbers of simultaneous users, since it will allow for more complex Investigations to be executed more quickly. If there are many simultaneous users, it is better to use a low value here, since there will be many independent SDK-values operations executed simultaneously.

parallel.query

This setting is available in NetWitness Suite 10.5 and later versions.

This configuration is similar to the parallel.values setting in that the maximum value is the number of logical CPUs. Setting parallel.query to a specific value should take into account the number of simultaneous users to maximize CPU utilization without consistently exceeding available resources.

Setting a higher value for parallel.query is useful when there are small numbers of simultaneous users and queries, since it will allow more complex queries to be executed more quickly. If there are many simultaneous users and queries, it is better to use a low value, since there will be many independent SDK-query operations executed simultaneously.

Query operations are limited by the meta database read rate, so setting parallel.query to a value higher than 4 is unlikely to produce dramatically better results than the default value of 0\. The best number to use for parallel.query will depend on the type of storage attached. Experiment with different values of parallel.query to determine the best results for your storage system.

Per-User Configuration Nodes

This topic describes the per-user configuration nodes. There are settings that influence the actions users are allowed to perform on the database. These settings are stored in the configuration tree at `/users/accounts/<username>/config` , where `<username>` is the name of the user to which the settings apply.

query.prefix

A query prefix applies a filter to every query operation that the user performs. This is implemented by taking the `query.prefix` values and appending it the the where clause of each query using the logical && (and) operator. For more information on Where Clauses, see Queries .

query.level

This setting is available in NetWitness Suite 10.4 and earlier versions.

The query.level setting assigns the query level that the users have for every query they perform. These influence whether their queries are limited by the query.level.1.minutes, query.level.2.minutes, or query.level.3.minutes.

query.timeout

This setting is available in NetWitness Suite 10.5 and later versions.

The query.timeout setting assigns the maximum amount of time in minutes that a user can run each query. For trusted connections, these timeouts are configured on the NetWitness Suite server. For accounts on Core services, this setting is stored in the configuration tree at `/users/accounts/<username>/config` , where `<username>` is the name of the user to which the setting applies. When this value is set to zero, the Core service does not enforce the query timeout.

session.threshold

The session.threshold setting assigns a maximum session threshold for the user. If set, this threshold value is assigned to all values calls that the user performs. A detailed discussion of both the values call and thresholds is covered in this guide.

Scheduler

This topic provides a brief introduction to the scheduler and explains how to schedule commands. All NetWitness Core services come with a built-in scheduler found under `/sys/config/scheduler` . To use the scheduler, you add the command you want to run periodically using one of two messages:

`/sys/config/scheduler addInter` - Add a command to run at the specified interval (every N hours, minutes or seconds)

or

`/sys/config/scheduler addMil` - Add a command to run at the specified time of day or even specific days of the week

Example

For example, suppose that you have a use case to delete all packet data that is greater than seven days old. Since you cannot configure the packet.dir setting to rollout data based on a time interval, you need to schedule the `/database timeRoll` command to run every so often. For this example, create a timeRoll to run every 20 minutes:

```
addIter minutes=20 pathname=/database msg=timeRoll params="type=packet
days=7"
```

This command adds a scheduled task (it is persisted between restarts of the service) to run every 20 minutes, on the `/database` node, and ages out all packet data older than seven days. The `params` parameter is used to pass all the parameters to the command specified (in this case `timeRoll`). Notice how it quotes all the embedded parameters (`type` and `days`) so they are not interpreted as parameters to be passed to the outer `addIter` command. If the parameters inside `params` need to use quotes, you must escape the inner quotes with a backslash. You can rewrite it with embedded quotes, which does not alter the command in any way:

```
addIter minutes="20" pathname="/database" msg="timeRoll"
params="type=\"packet\" days=\"7\""
```

This command works identically to the original, but demonstrates how to escape complicated parameter passing. Additional useful scheduler commands are:

`/sys/config/scheduler print` - Print all scheduled commands (you can also see them by doing an `ls` on the scheduler node).

`/sys/config/scheduler delSched` - Delete a scheduled command by passing in the identifier shown in the `print` (or `ls`) command.

This is a brief introduction to the scheduler. For more information on command parameters, send the `help` message to the scheduler node and pass in the command name via the `msg` parameter. For more information, see the "Services Explore View" topic in the *Host and Services Getting Started Guide* .

Rollover

This topic describes the two rollover mechanisms. The database operates as a first-in, first-out (FIFO) queue. New data is always appended to the database, and the oldest data is automatically removed as needed. Data that is in the middle of the database is immutable, meaning it cannot be modified.

There are two mechanisms to for rollover: synchronous and asynchronous.

Synchronous Rollover

Synchronous rollover refers to rollover settings that are applied in response to a write operation on the database. That means data is removed from the database in direct response to the need to write new data. Synchronous rollover is configured by setting size values on the configuration for `packet.dir` , `meta.dir` , `session.dir` , and `index.dir` .

Synchronous rollover on the packet, meta, and session databases can occur within any write operation. Synchronous rollover on the index occurs when the index is saved.

Asynchronous Rollover

Asynchronous rollover refers to database file removal that occurs when an explicit rollover command is issued to the database. Most commonly this type of rollover is scheduled to run periodically using the built-in scheduler of the Core service. The user can also explicitly request it.

The asynchronous rollover command is the `sizeRoll` message present on the `/index` and `/database` nodes of the configuration tree. The message on the `/database` node does size rollover on packet, meta, and session databases only, while the message on the `/index` node can do simultaneous rollover on both the index and the packet, meta, and session databases.

The `sizeRoll` command has the following parameter syntax:

```
size-roll-params    = {type-param, space}, (max-size-param | min-free-
param | max-percent-param), {max-size-warm-param, space}
type-param          = "type=", {type-flag} , { ",", type-flag } ;
type-flag           = "packet" | "meta" | "session" ;
max-size-param      = "maxSize=", number, {space}, unit ;
max-percent-param   = "maxPercent=", number, {space}, unit ;
min-free-param      = "minFree=", number, {space}, unit ;
max-size-warm-param = "maxSizeWarm=", number, {space}, unit ;
unit                = "t" | "TB" | "g" | "GB" | "m" | "MB" ;
```

```
number              = ? decimal number ? ;
percentage          = ? number between 0 and 100 ? ;
```

The `type` parameter controls the databases to consider for removing the oldest data based on total size or space remaining. If type is not specified on the `/index` sizeRoll, only the index is considered for rollover operations.

The `maxSize` parameter sets a current maximum size of the database or index. If the database is larger than this size, oldest data is deleted first (or moved to the Warm or Cold tier, depending on the configuration) until total size is less than `maxSize` . The `sizeRoll` operation determines which data is oldest out of all the databases and the index based on session IDs. Sessions or index entries with lowest session IDs are deleted first, possibly including removing meta and packet databases that are orphaned by removing entries from the session database. The index data is rolled out if the sessions that it refers to are removed.

The `maxSizeWarm` parameter sets a current maximum size on the *Warm* tier, but otherwise behaves identically to the `maxSize` parameter. When data is rolled out on the Warm tier, it is moved to the Cold tier (if configured) or deleted.

The `maxPercent` parameter sets a maximum percentage of all the volumes of all databases passed in `type` parameter combined. When exceeded, oldest data is deleted first until total size is less than maxPercent of total volumes.

The `minFree` parameter sets a minimum allowed free space on the volumes before oldest data is deleted.

Each call to the sizeRoll operation provides a single pass through the database to delete files. When the operation completes, the current size utilization of the database will have met the criteria specified by the `maxSize` , `maxPercent` , or `minFree` parameters and the optional `maxSizeWarm` . Therefore, this operation can be scheduled periodically to ensure that the database can continue to operate uninterrupted.

Example

The following example shows a typical sizeRoll scheduler entry for an Archiver:

```
pathname=/index minutes=5 msg=sizeRoll params="type=meta,session,packet
maxSize=25TB maxSizeWarm=150TB"
```

This scheduler entry specifies that every five minutes the database ensures that the max size of the meta, session, packet, and index does not exceed 25 terabytes on the Hot tier and does not exceed 150 terabytes on the Warm tier.

Queries

This topic covers the database query syntax. There are three main mechanisms for performing queries in the database, the `query` , `values` , and `msearch` calls on the `/sdk` folder on each Core service.

The `query` call returns meta items from the meta database, possibly using the index for fast retrieval.

The `values` call returns groups of unique meta values sorted by some criteria. It is optimized to return a subset of the unique values sorted by an aggregate function such as count.

The `msearch` call takes text search terms as it's input, and returns matching sessions that match the search terms. It can search within indexes, meta, raw packets, or raw logs.

`query` Syntax

The `query` message has the following syntax:

```
query-params     = size-param, space, query-param, {space, start-meta-
param}, {space, end-meta-param};
size-param       = "size=", ? integer between 0 and 1,677,721 ? ;
query-param      = "query=", query-string ;
start-meta-param = "id1=", metaid ;
end-meta-param   = "id2=", metaid ;
metaid           = ? any meta ID from the meta database ? ;
```

The `id1` , `id2` , and `size` parameters form a paging mechanism for returning a large number of results from the database. Their usage mostly benefits developers who are writing applications directly against the NetWitness Core database. Normally, results are returned in the order of oldest to newest data (higher meta IDs are always more recent). In order to return results from most recent to oldest, reverse the IDs such that `id1` is larger than `id2` . This has a slight performance penalty, because the where clause must be completely evaluated before processing in reverse order can begin.

When size is left off or set to zero, the system streams back all results without paging. For the RESTful interface, this results in the full response to be returned with chunked-encoding. The native protocol returns the results over multiple messages.

The `query` parameter is a `query` command string with its own NetWitness-specific syntax:

```
query-string      = select-clause {, where-clause} {, group-by-clause {,
order-by-clause } } ;
select-clause     = "select ",  ( "*" | meta-or-aggregate {, meta-or-
```

```
aggregate} ) ;
where-clause      = " where ",  { where-criteria } ;
meta-or-entity    = (meta_key | entity) ;
meta-or-aggregate = meta-or-entity | aggregate_func, "(", meta-or-
entity, ")" ;
aggregate_func    = "sum" | "count" | "min" | "max" | "avg" | "distinct"
| "first" | "last" | "len" | "countdistinct" ;
group-by-clause   = " group by ", meta-key-list
meta-key-list     = meta-or-entity {, meta-key-list}
order-by-clause   = " order by ", order-by-column
order-by-column   = meta-or-aggregate { "asc" | "desc" } {, order-by-
column}
```

The `select` clause allows you to specify either `*` to return all the meta in all the sessions that match the where clause, or a set of meta field names and aggregate functions to select a subset of the meta with each session.

The `select` clause may contain entity names in the place of meta key names. If an entity name is in the select clause, meta items returned by the query will have their key name set to the entity name, rather than their actual meta key name stored in the session. Thus, the names of the meta items returned in the query will match the names of the metas in the select clause. For example, if there is an entity `ip` that consists of `ip.dst` and `ip.src` , then a query containing `select ip` will only return `ip` fields, with nothing to distiguish `ip.dst` meta items from `ip.src` meta items in the result set.

The `select` clause may contain renamed meta key names. Any fields appearing in the result set as a result of a renamed key in the `select` clause will be returned with the meta key name matching the name used in the `select` clause. For example, if the key `port_src` is used to rename `tcp.srcport` , then a query containing `select port_src` will only return `port_src` fields, even if the underlying meta had type `tcp.srcport` .

The aggregate functions have the following effect on the query result set.

Function	Result
`sum`	Add all meta values together; only works on numbers
`count`	The total number of meta fields that would have been returned
`min`	The minimum value seen
`max`	The maximum value seen
`avg`	The average value for the number
`distinct`	Returns a list of all unique values seen

`countdistinct`	Returns the number of unique values seen. `countdistinct` is equivalent to the number of metas that would have been returned by the distinct function.
`first`	Returns the first value seen
`last`	Returns the last value seen
`len`	Converts all field values to a UInt32 length instead of returning the actual value. This length is the number of bytes to store the actual value, not the length of the structure stored in the meta database. For example, the word "NetWitness" returns a length of 10\. All IPv4 fields, like `ip.src` , return 4 bytes.

`where` Clauses

The `where` clause is a filter specification that allows you to select sessions out of the collection by using the index.

Syntax:

```
where-criteria    = criteria-or-group, { space, logical-op, space,
criteria-or-group } ;
criteria-or-group = criteria | group ;
criteria          = (meta-key | entity), ( unary-op | binary-op meta-
value-ranges ) ;
group             = ["~"], "(" where-clause ")" ;
logical-op        = "&&" | "||" ;
unary-op          = "exists" | "!exists" ;
binary-op         = "=" | "!=" | "<" | ">" | ">=" | "<=" | "begins" |
"contains" | "ends" | "regex" ;
meta-value-ranges = meta-value-range, { ",", meta-value-range } ;
meta-value-range  = (meta-value | "l" ), [ "-", ( meta-value | "u" ) ] ;
meta-value        = number | quoted-value | ip-address | mac-address |
relative-time ;
number            = ? any numeric value ? | ( '"' text '"' )
quoted-value      = ( '"' text '"' ) | ( '"' date-time '"' ) ;
relative-time     = "rtp(" , time-boundary , "," ,  positive-integer ,
time-unit, ")" ;
```

```
time-boundary     = "earliest" | "latest" ;
positive-integer  = ? any non-negative integral number ?
time-unit         = "s" | "m" | "h" ;
```

When specifying rule criteria, the `meta-value` part of the clause is expected to match the type of the meta specified by the `meta-key` . For example, if the key is `ip.src` the `meta-value` should be an IPv4 address. Entity names are allowed in any location where a meta-key name is required.

Queries using a `meta-key` name will match meta items corresponding both to the `meta-key` name as well as to the names of any "renames" specified for the key. See "Key Renaming" under the Index Customization topic for details on key renaming.

Query Operators

The following table describes the function of each operator.

Operator	Function
=	Match sessions containing the meta value exactly. If a range of values is specified, any of the values is considered a match.
!=	Matches all sessions that would not match the same clause as if it were written with the = operator.
<	For numeric values, matches sessions containing meta with the numeric value less than the right side. If the right side is a range, the first value in the range is considered. If multiple ranges are specified, the behavior is undefined. For text metas, a lexicographical comparison is performed.
<=	Same behavior as < , but sessions containing meta that equals the value exactly are also considered matches.
>	Similar to the < operator, but matches sessions where the numeric value is greater than the right side. If the right side is a range, the last value in the range is considered for the comparison.
>=	Same behavior as > , but sessions containing meta that equals the value exactly are also considered matches.
`begins`	Matches sessions that contain text meta value that starts with the same characters as the right side.
`ends`	Matches sessions that contain text meta that ends with the same characters as the right side.

`contains`	Matches sessions that contain text meta that contains the substring given on the right side.
`regex`	Matches sessions that contain text meta that matches the regex given on the right side. The regex parsing is handled by boost::regex.
`exists`	Matches sessions that contain any meta value with the given meta key.
`!exists`	Matches sessions that do not contain any meta value with the given meta key.
`length`	Matches sessions that contain text meta values of a certain length. The expression on the right side must be a non-negative number.

Text Values

The system expects quoted text values. Unless it can be parsed as a time (see below), a quoted value is interpreted as text.

> It is also important to quote any text value that may contain - so that it is not interpreted as a range.

IP Addresses

IP addresses can be expressed using standard text representations for IPv4 and IPv6 addresses. In addition, the query can use CIDR notation to express a range of addresses. If CIDR notation is used, it is expanded to the equivalent value range.

MAC Addresses

A MAC address can be specified using standard MAC address notation:
`aa:bb:cc:dd:ee:ff`

Numeric Values

In a where clause, you can specify numeric search values. Numbers should not be surrounded by quotes.

Bucketed Numeric Indexes

Meta keys indexed with bucketing can be used like any other numeric search value. Under most situations such searches will return sessions that have a meta value that exactly matches the requested search criteria.

Special behavior is invoked for queries that select only `sessionid` , for example a query of the form `select sessionid where size = 2048` . Selecting `sessionid` explicitly bypasses all meta database read operations, and only returns index information. If selecting `sessionid` only, and if the numeric value specified is exactly equal to one of the bucket values, then the system will return all sessions that match somewhere in the bucket, rather than an exact match. For example, the search term `size = 2048` will match all sessions in the 2 KB bucket, which is the range from 2048 to 3171 bytes. However, if the search values does not match a bucket values, then the system will return only matches for the exact byte value. For example, the search term `size = 2049` will only match sessions with a size meta value exactly 2049. In this mode of operation, specifying a non-bucket value in a where clause is slower than searching within a bucket value. The 'where' clause parameter to the `values` API also invokes this optimization.

Using bucketed values in other forms of `query` does not invoke special behavior. The same is true for the `msearch` API. For those APIs, the use of a bucketed index in the where clause is evaluated accurately, without special meaning applied to bucket values. To search within an entire bucket using these APIs, specify the bucket range explicitly. For example `size=2048-3171` .

More information on how to tell if an index is bucketing is in the topic Index Customization .

Numeric Value Aliases

For numeric values, aliases specified in the index can be used in a query as a quoted string in place of where a literal numeric value would be used; e.g.,

```
select * where service = "NFS"
```

Numeric value aliases can be used anywhere a numeric literal might be used: as a single value, as the beginning or end of a range, or in a comma-delimited list of values (and/or ranges).

Refer to the topic Index Customization for details of how value aliases can be specified in the index.

Date and Time Expressions

In NetWitness Suite, dates are represented using Unix epoch time, which is the number of seconds since Jan 1, 1970 UTC. In queries, you can express the time as this number of seconds, or you can use the string representation. The string representation for the date and time is `"YYYY-mmm-DD HH:MM:SS"` . A three-letter abbreviation represents the month. You can also express the Month as a two-digit number, 01-12.

Time values must be quoted.

All times specified in queries are expected to be in UTC.

Relative Time Points

Relative time points allow a where clause to reference a value at some fixed offset relative to the earliest or latest time metas seen in the collection.

A relative time point expression has the syntax `rtp(boundary, duration)` .

The boundary is either `earliest` or `latest` .

The duration is an expression of hours, minutes, or seconds. For example, `24h` , `60m` , or `60s` .

Relative time points can only be used in SDK operations, where there is a collection from which to get the boundaries for earliest and latest time metas.

Relative time points only work on indexed meta types. The default indexed meta types are `time` and `event.time` .

Examples:

```
Last 90m of collection time:
time = rtp(latest, 90m) - u


First 2 days of event time:
event.time = l - rtp(earliest, 48h)
```

Special Range Values

Ranges are normally expressed with the syntax * `smallest` * - * `largest` *, but there are some special placeholder values you can use in range expressions. You can use the letter `l` to represent the lower-bound of the all meta values as the start of the range, and `u` to represent the upper bound. The bounds are determined by looking at the smallest or largest meta value found in the index out of all the meta values that have already entered the index.

If you use the `l` or `u` tag, it should be unquoted.

For example, the expression `time = "2014-may-20 11:57:00" - u` would match all time from that 2014-may-20 11:57:00 to the most recent time found in the collection.

Notice that it is easy to confuse a range expression with a text string. Make sure that text values that contain - are quoted, and that hyphens within range expressions are not within quoted text.

`group by` Clause (since 10.5)

The query API has the ability to generate aggregate groups from the results of a query call. This is done using a `group by` clause on the query. When `group by` is specified, the result set for the query is subdivided into groups. Each group of results is uniquely identified by the meta values indicated in the group by clause.

For example, consider the query `select count(ip.dst)` . This query returns a count of all ip.dst metas in the database. However, if you add a `group by` clause, like this: `select count(ip.dst) group by ip.src` , the query returns a count of the ip.dst metas found for each unique ip.src.

As of NetWitness Suite version 10.5, you can utilize up to 6 meta fields in a `group by` clause.

The `group by` clause shares some of the same functionality as the `values` call, but it offers significantly more advanced groups at the expense of longer query times. Producing the results of a grouped query involves reading the meta from the meta database for all sessions that match the `where` clause, while a values call can produce its aggregates by reading the index only.

The contents of each group returned by the query are defined by the `select` clause. The `select` clause can contain any of the aggregate functions or meta fields selected. If multiple aggregates are selected, the result of the aggregate function is defined for each group. If nonaggregate fields are selected, the meta fields are returned in batches for each group.

The result set of a `group by` query is encoded with the following rules:

1. All meta items associated with a group are delivered with the same group number.
2. The first meta items returned to the group identify the group key. For example, if the `group by` clause specifies `group by ip.src` , then the first meta item of each group will be an `ip.src` .
3. The normal, nonaggregate meta items are returned after the `group key` , but they all will have the same group number as the group key metas.
4. The aggregate result meta fields for each group are returned next.
5. All fields within a group are returned together. Different group results will not be interleaved.

If one of the `group by` meta items is missing from one of the sessions matched by the `where` clause, that meta field is treated as a NULL for the purposes of that group. When the results for that group are returned, the NULL-valued parts of the group key will be omitted from the group's results, since the database has no concept of NULL.

The semantics of a `group by` query differ from a SQL-like database in terms of what meta fields are returned. SQL databases require you to select the `group by` columns explicitly in the `select` clause if you want them to be returned in the result set. The NetWitness Core database always implicitly returns the group columns first.

A query with a `group by` clause honors the result set `size` parameter if one is provided. However, due to the nature of the grouping, it puts an additional burden on the caller to page and reform groups if a fixed-size result set is requested. For this reason, you should not specify an explicit result size when making a `group by` call. By not specifying an explicit size, the entire result set will be delivered as partial results.

`group by` clauses allow results to be grouped by an entity definition.

The following table describes the database honors configuration parameters that limit I/O or memory impact of a group by query.

Parameter	Function
`/sdk/config/max.query.groups`	This is the limit on how many groups

	can be held in memory to calculate aggregates. This parameter allows you to limit the overall memory usage of the query.
`/sdk/config/max.where.clause.sessions`	This is the limit on how many sessions from the where clause can be processed in a query. This parameter allows you to set a limit on the number of sessions that have to be read from the meta and session databases to resolve a query.

`order by` Clause (since 10.5)

An `order by` clause can be added to a query that contains a `group by` clause. The `order by` clause causes the set of grouped results to be returned in sorted order.

An `order by` consists of a set of items to sort by in ascending or descending order. Sorting can be performed on any data field that will be returned in the result set. This includes meta specified by the `select` clause, aggregate function results specified by the `select` clause, or `group by` meta fields.

The `order by` clause can sort over many columns. There is no limit on the number of `order by` columns allowed in the query; but a practical limit exists in that each of the `order by` columns must refer to something returned by the `select` clause or `group by` clause. The multiple column sort is imposed lexicographically, meaning that if two groups have equal values for the first column, then they are sorted by the second columns. If they are equal in the second column, they are sorted by the third column, and so on for however many `order by` columns are provided.

The NetWitness Core database is unique in that the groups of results returned by a query may each have many values for a selection. For example, it is possible to select all meta items that match a meta type and organize them into groups, and it is possible to use the `distinct()` function to return groups of distinct meta values. If an `order by` clause references one of the fields in the group that has multiple values, the sorting order is applied as follows:

1. Within each group, the fields with multiple matching values are ordered by the ordering clause
2. All the groups are sorted by comparing the first occurrence of the ordered field found within each group

The `order by` clause is only available in queries that have a `group by` clause, since groups are required to organize the meta fields into distinct records. If you wish to sort an arbitrary query as if there were no grouping applied, use `group by sessionid` . This ensures that results are returned in groups of distinct sessions or events.

`group by` clauses are naturally returned in ascending group key order; but, an `order by` clause can be used to return groups in a different order.

If an `order by` column does not specify `asc` or `desc` , the default ordering is ascending.

Examples:

```
select countdistinct(ip.dst) GROUP BY ip.src ORDER BY countdistinct
(ip.dst)
select countdistinct(ip.dst) GROUP BY ip.src ORDER BY countdistinct
(ip.dst) desc
select countdistinct(ip.dst),sum(size) GROUP BY ip.src ORDER BY sum
(size) desc, countdistinct(ip.dst)
select sum(size) GROUP BY ip.src, ip.dst ORDER BY ip.dst desc
select user.dst,time GROUP BY sessionid ORDER BY user.dst
select * GROUP BY sessionid ORDER BY time
```

`values` call

The index provides a low-level `values` function to access the unique meta values that have been stored in the index. This function allows developers to perform more advanced operations on groups of unique meta values.

The `values` call parameter syntax:

```
values-params          = field-name-param, space, where-param, space,
size-param, {space, flags-param} {space, start-meta-param}, {space, end-
meta-param}, {space, threshold-param}, {space, aggregate-func-param},
{space, aggregate-field-param}, {space, min-param}, {space, max-param} ;
field-name-param       = "fieldName=", (meta-key | entity) ;
where-param            = "where=", where-clause ;
size-param             = "size=", ? integer between 1 and 1,677,721 ? ;
start-meta-param       = ? same as query message ?
end-meta-param         = ? same as query message ?
flags-param            = "flags=", {values-flag, {"," values-flag} } ;
values-flag            = "sessions" | "size" | "packets" | "sort-total" |
```

```
"sort-value" | "order-ascending" | "order-descending" ;
threshold-flag        = "threshold=", ? non-negative integer ? ;
aggregate-func-param  = "aggregateFunction=", { aggregate-func-flag } ;
aggregate-func-flag   = "count" | "sum" ;
aggregate-field-param = "aggregateFieldName=", ( meta-key | entity ) ;
min-param             = "min=", meta-value ;
max-param             = "max=", meta-value ;
```

The `values` call provides the function of returning a set of unique meta values for a given meta key. For each unique value, the `values` call can provide an aggregate total count. The function used to generate the total is controlled by the flags parameter.

Parameters

The following table describes the function of each parameter.

Parameter	Function
`fieldName`	This is the meta key name for which you retrieve unique values. For example, if `fieldName` is `ip.src` , this function returns the unique source IP values in the collection. Entities can be used for the field name, in which case the result is defined as the combined set of field values for all the referenced meta keys. If the `fieldName` refers to a key with rename references, the result is defined as the combined set of field values for the given meta key name plus all of the references' meta keys.
`where`	This is a `where` clause which filters the set of sessions for which the unique values are returned. For example, if the `fieldName` is `ip.src` , and the `where` clause is `ip.src = 192.168.0.0/16` , only values in the range of `192.168.0.0` to `192.168.255.255` are returned. For information on the `where` clause syntax, see *Where Clauses* .
`size`	The size of the set of unique values to return. This function is optimized to return a small subset of the possible unique values in the database.
`id1` , `id2`	These optional parameters limit the scope of the search for unique

	values to a specific region of the meta database and the index. Setting the `id1` and `id2` parameters to a limited range of the meta database is very important to running searches quickly on large collections.
`flags`	Flags control how the values are sorted and totaled. Flags are described in the following Values Flags section.
`threshold`	Setting the `threshold` parameter allows the `values` call to short-cut collection of the total associated with each value once the threshold is reached. By providing a threshold, the caller can reduce the amount of index and meta items that must be retrieved from the database. If the `threshold` parameter is omitted or set to 0, this optimization is not used.
`aggregateFunction`	Optional parameter used to change the default behavior from counting sessions, packets, or size to counting or summing the numeric field defined by `aggregateFieldName` . Both parameters must be specified when either is defined. Pass either `sum` or `count` to specify which behavior to perform.
`aggregateFieldName`	The meta field on which to perform the `aggregateFunction` . Both `aggregateFunction` and `aggregateFieldName` parameters must be specified when the `aggregate` flag is set. Performing a `values` call using one of the aggregate functions can be significantly slower than a `values` call that collects totals of sessions, packets, or size. The reason for this is that each session that matches the `where` clause must be retrieved from the meta database. This scan causes a large portion of the query to be I/O bound on the meta DB volumes. The time taken to run an aggregate `values` call is linearly proportional to the number of sessions that match the `where` clause.
`min` , `max`	The minimum and maximum value that should be returned from the call. These parameters are used to iterate (or page) over an extremely large number of values, typically more values than could be returned from a single call. Primarily used in conjuction with the

flags `sort-value,sort-ascending` such that the highest value returned would be used in a subsequent call as the `min` parameter value. The values are exclusive. If `min="rsa"` was specified and `rsa` was a valid value, `rsa` would not be returned; instead, the next highest value would be returned.

`values` Flags

The `flags` parameter controls how the values call operates. There are three groups of flags that correspond to the different modes of operation as shown in the following table.

Flag	Description
`sessions` , `size` , `packets`	The `values` call allows you to specify one of these flags to determine how the total for each value is calculated. If the flag is `sessions` , the `values` call returns a count of sessions that contain each value. If the flag is `size` , the `values` call totals the size of all sessions that contain each unique value, and reports the total size for each unique value. If the flag is `packets` , the values call totals the number of packets in all sessions that contain each unique value, and then reports that total for each unique value.
`sort-total` , `sort-value`	These flags control how results are sorted. If the flag is `sort-total` , the result set is sorted in order of the totals collected. If the flag is `sort-value` , the results are returned in order of the sorting order of the values.
`order-ascending` , `order-descending`	These flags control the sort order of the result set. For example, if sorting by total in descending order, the values with the greatest total are returned first.
`suggest`	Enables suggestion mode for the values API. All other flags are ignored if this flag is set

`values` Call Example

The `values` call is used extensively by the Navigation view in NetWitness Suite. The default view generates calls that look like this:

```
/sdk/values id1=198564099173 id2=1542925695937 size=20
flags=sessions,sort-total,order-descending threshold=100000
```

```
fieldName=ip.src where="time=\"2014-May-20 13:12:00\"-\"2014-May-21
13:11:59\""
```

In this example, the Navigation view requests unique values for `ip.src` . It requests unique values of `ip.src` in the time range given. It asks for the count of sessions that match each `ip.src` , and the results are the top 20 `ip.src` values when sorted by the number total count of sessions in descending order. In addition, the Navigation view has a meta ID range in order to provide an optimization hint to the query engine.

Values call and bucketing mode

When a values call is executed with a `fieldName` parameter that specifies a bucketed indexed meta, the system will only return the bucket values present within the rest of the criteria. This has the side effect of producing counts and totals that represent all sessions within each returned bucket. This is useful because it summarizes size meta into groups that represent human-readable ranges like 1 MB, 2 MB, and so one.

When the number of sessions scanned by the values call drops below 1000 sessions, the values call operates in meta-scanning mode, and at that point it returns exact values for numeric value indexes, regardless of the bucketing setting on the index.

Suggestion Mode

The `values` call has an additional execution mode that is used to provide suggested search values. In this mode of operation, the `values` call only identifies unique values stored with the given meta key name. It provides these results within milliseconds. To achieve this it does not provide any session counts, it will not utilize any other sort flags. The suggestion mode does utilize the `where` parameter to refine suggestions, but it only utilizes the time range clause if provided. Other portions of the `where` clause are not utilized to refine suggestion.

Suggestion mode is enabled by setting the `suggest` flag in the `flags` parameter.

Suggestion mode gives special meaning to the `min` parameter. The `min` parameter can contain the starting point for the suggested values. The return values of `suggest` mode will only include values that start with the text provided in the `min` parameter.

`msearch` Call

The index provides a low-level `msearch` function to perform text searches against all meta types. This type of search does not require users to define their queries in terms of known meta types. Instead, it searches all parts of the database for matches. `msearch` is used by the Events view text search. See the "Filter and Search Results in the Events View" topic in the *Investigation and Malware Analysis Guide* for detail on the accepted search forms and examples.

`msearch` parameters:

```
msearch-params  = search-param, {space, where-param}, {space, limit-
param}, {space, flags-param};
search-param    = "search=", ? free-form search string ? ;where-param
 = "where=", ? optional where clause ? ;
limit-param     = "limit=", ? optional session scan limit ? ;flags
    = "flags=", {msearch-flag, {"," msearch-flag} };
msearch-flag    = "sp" | "sm" | "si" | "ci" | "regex" ;
```

The `msearch` algorithm works as follows:

1. A set of sessions is identified from the index by finding the intersection of three sets:
   - (Set 1) All sessions in the database
   - (Set 2) Sessions that match the `where` clause parameter
   - (Set 3) If the `si` flag is specified, sessions that indexed values that match the search string parameter.
2. If the search specifies the `sm` parameter, all meta items from the set of sessions identified in step 1 are read and scanned to see if they match the search string parameter. The meta items will be read from the service nearest to the point where the search was executed. For example, if the search is performed on a Broker, the meta items may be read from the Concentrator nearest to the broker, but if the search is performed on an Archiver the meta items will be read from the Archiver itself.
3. If the search specifies the `sp` parameter, all raw packet or log entries from the set of sessions identified in step 1 are read and scanned to see if they match the search string parameter. The packets will be read from the service nearest to the point where the search was executed. For example, if the search is performed on a Concentrator, the packet data will be read from the Decoder, but if the search is performed on an Archiver, the packet data will be read from the Archiver itself.
4. Matches from step 2 and step 3 are returned as they are found, up to the point where the `limit` parameter is reached. Limit specifies the maximum number of sessions for which meta and packet data will be scanned. If limit is not specified, the entire set of sessions determined in step 1 is scanned.

`msearch` Flags

Flag	Description
`sp`	Scans raw packet data

`sm`	Scans all meta data
`si`	Does index lookups for all search parameters before scanning meta
`ci`	Performs a case insensitive search. Returned results are case-preserving.
`regex`	Treats the search parameter as a regular expression. Only a single regular expression can be specified, but the regular expression may be arbitrarily complex.

`msearch` Index Search Mode

Using the index search mode, specified by using the `si` flag, causes results to be returned significantly faster than any other mode. The main limitation of this mode is that it only returns matches on text terms that match value-indexed meta values.

- The `si` parameter must be combined with the `sm` flag. The `si` parameter implies the search only matches indexed meta.
- The `si` parameter can be used with regex searches, however only text indexed values will match. IP addresses and numbers will not match the regex.

Text Search Syntax

The search parameter given to `msearch` is composed of 1 or more words, separated by whitespace. For example, searching for `foo` returns sessions that contain the word foo.

If multiple terms are provided for the search, they are implicitly considered to be an AND operation. For example, searching for `foo bar` returns sessions that contain both foo AND bar. Sessions that contain only foo or only bar are filtered out. If you want to search for sessions containing any of two or more terms, you must explicitly separate the terms with the word OR. For example, searching for `foo OR bar` returns sessions that contain either foo or bar.

Search Syntax And Index Modes

The searches given to the `msearch` command are interpreted according to the index level on all the indexes. `msearch` works on the value-indexed keys in the index. Search terms provided to `msearch` will find values that are an exact match to values that were indexed.

As of version 11.1, there are new index modes available that allow `msearch` to locate text that is not an exact match to the search input. `msearch` supports wildcard searches on the word meta index, if the word meta index has the ngram option enabled. For details on the ngram option, see the topic Index Customization .

The wildcard search allows the use of the `*` and `?` characters as wildcards in search terms. The `*` can stand for 0 or more characters, while the `?` may stand for any single character. To search for those characters in an N-gram enabled index, you may escape them with a backslash character.

If the word index has the 'edge' N-gram option enabled, then it can be used to locate searches that end in a wildcard. This means it is only useful for finding text that begins with a known prefix.

If the word index has the 'all' N-gram option enabled, then wildcards may appear anywhere in the search term.

This table summarizes the relationship between word index level, and the types of searches that `msearch` will locate.

Search input	Non-indexed	IndexValues	IndexValues with Edge N-grams	IndexValues with All N-grams
"foo"	no match	"foo"	words starting with "foo"	words containing "foo"
"foo*"	no match	literal "foo*"	words starting with "foo"	words starting with "foo"
"*foo"	no match	literal "*foo"	no match	words ending with "foo"
"*foo*"	no match	literal "*foo*"	words staring with foo	words containing "foo"
"foo*"	no match	literal "foo*"	literal "foo*"	literal "foo*"

`msearch` Tips

- Always use the `where` clause to specify a time range for the search.
- To search for IP address ranges, specify them in the `where` clause.
- Use the `limit` parameter when not using the index search mode. Without it, there will be an extremely large amount of data read by the meta and packet databases.

Stored Procedures

The `query` and `values` calls provide more low-level search functionality. For more advanced use cases, server-side stored procedures exist.

Use of Quotes in Query Syntax

The query parser does not care whether you use single or double quotes within a query statement. A single- or double-quoted value is treated as text meta.

The query parser attempts to make sense of whatever you put in the statement. It is not very strict about what it will accept.

For example:

```
reference.id=4752
```

This clause identifies sessions that have a `reference.id` meta value that has a *numeric* value of 4752.

`reference.id='4752'` or `reference.id="4752"`

This clause identifies sessions that have a `reference.id` meta value that has a *string* value of `4752` .

However, the query engine implicitly compares numbers and strings that look like numbers as equal when the values are semantically the same. So it works with either syntax.

For most efficient performance, however, it is always a good idea to construct the queries such that the query syntax matches the data types generated by the parser.

For example, if the parser is creating `reference.id` as a numeric data type (such as `uint32` or `uint64`), then use the numeric syntax.

If the parser is creating `reference.id` as a text data type, then use the string syntax.

Index Customization

This topic describes how to use the custom index file to customize the index. Each NetWitness NextGen service is installed with a default index configuration that is intended to cover the index needs for most users of the product. However, it is possible to index new meta keys in order to use the index with custom content that generated custom meta.

Index Configuration File Locations

The index customization is accomplished by making changes to the custom index file. The location of this file is **/etc/netwitness/ng/index-<servicename>-custom.xml** , where **<servicename>** corresponds to the name of the product that you are customizing. For example, the Concentrator custom index file is /etc/netwitness/ng/index-concentrator-custom.xml.

Concentrator products also include a file that describes the default index configuration: **/etc/netwitness/ng/index-concentrator.xml** . This file is useful as a template to show how the custom index file is formatted.

If you make customizations to the index in the custom index file, those customizations override any conflict with the default index configuration.

You can make changes to the custom index file while the service is running. When the service receives an index save command, the changes to the custom index file are read and applied to the index.

Changes to the index can only be applied to new incoming data. Data cannot be retroactively reindexed with a new custom index configuration, except by rebuilding the index .

Index configuration entries

The custom index file is an XML document. The root element of this document is the `language` element, and inside there are elements for each meta key to describe each custom index. Each element of the custom index configuration looks like this:

```
<key name="did" description="Decoder Source" level="IndexValues"
format="Text" valueMax="100"  />
```

Definitions for each attribute in this element:

Attribute	Description
name	The name of the meta key that will be indexed
description	A human-readable description for the meta type
level	The type of index that will be created for this meta key

valueMax	The maximum unique values that will be stored for this key per slice
format	The format of the data held by all meta items with this meta key name
bucket	Enable size bucketing
ngrams	Enable ngram generation
defaultAction	Default Navigate view action for this key: Open, Closed, Auto, Hidden

The next few sections examine these parameters in greater detail.

Meta names

The meta name used by the index refers to the meta key name present within every meta item in the meta database. These meta names are generated by the Decoders when parsing. Parsers can choose to generate meta with any meta key name. Therefore, the custom index allows you to choose which of the meta items generated by the Decoder are indexed.

Meta key names can be 16 characters long, and contain only letters or the '.' character.

Data Types

When the Decoder generates meta items, it assigns a data type. Each parser can choose the data type of the meta it generates. However, there are recommended and standard data types for each of the default meta keys. For example, ip.src and ip.dst are stored as the IPv4 meta type, and alias.host is stored as the Text meta type. Each parser must agree on the data format for each meta key generated by the Decoder.

When adding a custom index to the Concentrator, the data type of the custom index must match the format of the data generated by the Decoder. If the types do not match, the Concentrator attempts to convert the meta generated into the type specified for the custom index. However, these conversions sometimes fail, and the resulting index can produce undefined results.

Likewise, when many Decoders and Concentrators work together as part of a NetWitness installation, they must all agree on the types for each meta key. Conflicts of meta types between NetWitness NextGen services can lead to undefined behavior.

The following table shows the metadata types supported by the NetWitness NextGen services.

Type	Size in bytes	Description
Int8	1	Signed 8-bit integer
UInt8	1	Unsigned 8-bit integer
Int16	2	Signed 16-bit integer
UInt16	2	Unsigned 16-bit integer
Int32	4	Signed 32-bit integer
UInt32	4	Unsigned 32-bit integer

Int64	8	Signed 64-bit integer
UInt64	8	Unsigned 64-bit integer
UInt128	16	Unsigned 128-bit integer
Float32	4	32-bit floating point number, single precision
Float64	8	64-bit floating point number, double precision
TimeT	8	Unix epoc timestamp
Binary	1-255	Arbitrary binary data
Text	1-255	UTF-8 Encoded text data
IPv4	4	IPv4 address bytes
IPv6	16	IPv6 address bytes
MAC	6	MAC Address bytes

When defining a custom index, it is important to use the best data type for the meta. For example, never store IP addresses as Text, since the Text representation takes more bytes than the IPv4 representation.

Index Levels

There are three levels, or types, of indexing: IndexNone, IndexKeys, and IndexValues.

IndexNone

This type of custom index is not really an index at all. Custom index entries with the IndexNone level exist only to define and document the meta key. IndexNone entries can be used in custom Decoder indices to enforce a specific data type for a meta key across all the parsers on a Decoder.

IndexKeys

This type of custom index indicates that the index only keeps track of sessions that contain meta items with this meta key name. However, it does not index any unique values in the meta database for the meta key.

Key-level indices take much less storage space, memory, and CPU time to manage, but they require a lot more work from the query engine when you perform query or values operations using them.

If used in a where clause, a meta key indexed at the key level can only be used to resolve operations such as exists or !exists.

IndexValues

This type of custom index keeps sessions that contain each individual unique value for the meta key. This type of index is also known as a "full index".

This type of index is needed for efficient processing of most where clauses, and for use of this meta key as the fieldName parameter of a values call.

Value Max

Value max is a parameter that can have a very significant impact on the accuracy and performance of a Value-level index.

As a Decoder parses packets or logs, it is allowed to create meta of any type with any value. Usually, these meta items are created from data copied directly out of the packet or log. Therefore, anyone can create unique meta values in response to nearly any event.

The performance of the index is directly dependent on the number of unique values it has found for each meta key. As the number of unique values increases, the rate at which new meta is indexed can decrease, and the speed with which queries are completed decreases. Since any person can influence the creation of unique meta values, it is possible for any person to affect the performance of the index.

The value max parameter limits the number of unique values that can enter the index. Therefore, a malicious user cannot flood the system with a large number of unique values in an attempt to make the NetWitness system not work.

It is important to set a value max on any meta key that may have its value influenced directly by incoming packets or logs.

The value max applies only to values added since the last index save operation.

The limit for how high value max can be set varies from version to version and on the amount of RAM available to the NetWitness NextGen service. As of 10.3, the recommended ceiling for value max is 5,000,000 for any meta key. If there are a lot of custom indices, then the value max may have to be lower.

maxLength

The max length parameter is used exclusively on the `word` meta type. The meaning of the `maxLength` parameter depends on whether the index is storing N-grams, as indicated by the `ngrams` parameter. The default and recommended value for `maxLength` is 5.

Max Length without N-Grams

If N-Gram support is turned off, then the `maxLength` parameter indicates that search terms need to be truncated so that they will match truncated values in the index and meta database. If this is the case, the `maxLength`**must** be less than or equal to the corresponding setting for **/decoder/parsers/config/token.max.length** on the Log Decoder service that is generating `word` token metas. The index will use the `maxLength` to properly interpret search terms fed into the `msearch` SDK function.

Max Length with N-Grams

If N-Gram support is turned on, by setting `ngrams="Edge"` or `ngrams="All"` , then the maxLength parameter controls the maximum length of N-Grams extracted from the meta item. In this scenario, the maxLength does not have to match the length of `word` meta items generated on the Log Decoder.

minLength

The minimum length parameter is used exclusively on the `word` meta type. It only has an effect when N-grams are generated. It indicates the smallest length N-gram that will be extracted from the `word` meta items. The default and recommended minimum N-Gram length is 3, which means that searches against the `word` index must have at least 3 characters.

ngrams

The `ngrams` parameter is used exclusively on the `word` meta type. N-gram indexes extract information that allow for fast lookup of searches that only match part of the word. For example they allow for finding 'ball' inside the word 'basketball'. If set to the value of `all` , then the index will create entries for all N-grams within the word meta values. The minimum value of N is specified by `minLength` , and the maximum value of N is specified by `maxLength` .

The `ngrams` parameter also supports the value `edge` , which indicates the index will only store N-grams that appear at the beginning of a word. Edge N-grams are useful for type-ahead search matching, and take less space than storing all N-grams. However they are not useful to locate matches inside the word or at the end of the word.

N-gram indexing has a major impact on the functionality of the word index. If enabled the word index will consume approximately 5 times more space than if N-grams were not enabled.

Numeric Bucketing

Indexes on meta formats that are unsigned integers, specifically UInt32 and UInt64, can make use of size bucketing to improve performance.

Size bucketing rounds down the size values in the index to their nearest traditional byte unit of information. Enabling this option on a numeric index reduces the number of unique values to track in the index, which improves aggregation and query performance.

The bucketing option is enabled by the boolean parameter `bucket` on the key element. `bucket` may have the value `0` , for off or `1` for on. The default is `0` .

Examples of bucket number values:

Raw Value	Value Stored in Index	Explanation
0 - 1,023	0 - 1,023	Values 0-1023 are stored unmodified
1,024 - 1,048,575	1 KB, 2 KB, 3 KB ... 1,023 KB buckets	Values under 1 MB are stored in 1 KB

1,048,576 - 1,073,741,823	1 MB, 2 MB, 3 MB ... Values under 1 GB are stored in 1 MB 1,023 MB buckets
1,073,741,824 - 1,099,511,627,775	1 GB, 2 GB, 3 GB ... Values under 1 TB are stored in 1 GB 1,023 GB buckets

Key Value Aliases

Value aliases can be specified for keys. Value aliases are text representations that correspond to specific values for a key. These text representations may be easier to remember and more convenient to display. Aliases can be used in the rule/query language (see Queries and are accessible via the SDK.

Value aliases are specified using the `aliases` and `alias` elements:

```
<key description="Service Type" format="UInt32" level="IndexValues"
name="service" valueMax="75" defaultAction="Open">
       <aliases>
              <alias format="$alias" value="0">OTHER</alias>
              <alias format="$alias" value="20">FTPD</alias>
              <alias format="$alias" value="21">FTP</alias>
              <alias format="$alias" value="22">SSH</alias>
              <alias format="$alias" value="23">TELNET</alias>
              <alias format="$alias" value="25">SMTP</alias>
              ⋮
       </aliases>
</key>
```

Key Renaming

The index language supports the concept of key renaming. This feature is used to provide backwards compatibility for new key names to deprecate and replace old key names. A renaming is achieved by adding `rename` elements to the key. This has the effect of indicating the parent key renames the key in the rename element. For example, the key definition below defines a new key named `port_src` that renames the key `tcp.srcport` .

```
<key name="port_src" description="Source Port" format="UInt16"
level="IndexValues">
       <rename name="tcp.srcport"/>
</key>
```

The rename element indicates to the database that uses of the parent key, in this case `port_src` , will include both meta items with type port_src and meta items with type tcp.srcport. Thus, new meta items can be added to the database and queried using `port_src` , and such queries will return information that was previously stored in tcp.srcport as well.

The rename element accepts a single attribute, `name` , that refers to a previously defined key.

Keys referred by rename elements must have the same type as the parent key.

Keys referred by rename elements must have the same index level as the parent key.

If a key is redefined in a custom index file, and the redefined key contains rename elements, then those rename elements replace any previously defined rename elements.

Entities

The index configuration is used to define entities. Entities provide a convenient way to work with several meta keys at the same time. An entity definition is an alias that groups together the results from other meta keys. You can use an entity definition anywhere you would use a normal meta name. The primary use for entities is to organize similar meta types into a single, easier to use, meta type. For example, the default NextGen database language includes distinct meta types for IP source and IP destination. You could define an entity that represents the combined set of all IP sources and destinations using an `entity` element:

```
<entity name="ip.all" description="any ip entity">
       <keyref name="ip.src"/>
       <keyref name="ip.dst"/>
</entity>
```

The `entity` element accepts the following attributes:

Name	Description
name	(Required) The name of the entity
description	(Optional) A description of the entity
defaultAction	(Optional) Navigate view action for this entity: Open, Closed, Auto, Hidden

Entity definitions create new entries in the NextGen service language. Since they are returned in the SDK `language` call, they can be used by older client applications that are not directly aware of the concept of entities.

Each entity definition must contain one or more `keyref` elements. The keyref element only allows a single `name` attribute that must refer to a real meta `key` element defined somewhere else in the device's language. The `keyref` is also allowed to refer to meta types defined in the default language.

Meta entities can be utilized in application rules, but are not supported in network rules as meta available is too limited.

Entity Definition Rules

- All the keys referenced by an entity must have the same data type
- All the keys referenced by an entity must have the same index level
- An entity name cannot conflict with any existing meta type
- Keyrefs must refer to meta key names that are defined earlier in the index configuration

Entities in Brokers

Brokers will inherit entity definitions from up-stream devices, in the same way that meta key definitions are inherited. If the upstream devices attached to the broker do not all have the same set of entities defined, the Broker will log a warning. All upstream devices should have the same entity configuration. A broker operating with mismatched entity definitions may produce undefined behavior.

Rebuilding the Index

Under normal operation, changes made to the index configuration for a service are only applied to new data that enters the collection. Rebuilding the index over all the data in the collection is a time-consuming process because it requires all of the meta database storage to be read from disk.

In version 11.0 and later, it is possible to rebuild the index while the service is online. Version 11.0 services rebuild indexes in the background whenever the service detects that part of the session and meta databases is unindexed.

Activating the Background Reindexer

The background reindexer is activated whenever the service starts. During startup, the indexer checks for gaps between sessions that are indexed and sessions that are present in the session and meta database. If any gaps are found, the background reindexer begins reindexing the session and meta database on the service.

Examples of events that may activate the background reindexer:

1. A power failure or crash occurred, rendering the last slice of the index corrupt. The corrupt data is deleted at startup, leaving a gap in the index.
2. Index data is forcibly deleted, either by doing an index reset or deleting files from the filesystem.

Controlling the Background Reindexer

The operation of the background indexer is controlled by the configuration node `/index/config/reindex.enable` . If `reindex.enable` is set to true, the next time the service starts the reindexer will operate. If `reindex.enable` is set to false, the reindexer will not start the next time the service starts, but will continue to operate until the service is restarted.

Background Reindexing Algorithm

The operation of the background indexer is as follows:

1. The index examines the ranges of sessions that are present in the index and compares them to the ranges of sessions that have valid meta data. Any discrepancies between the two are considered gaps.

2. The gaps in the index are subdivided into slices based on the current value of `/index/config/save.session.count`.
3. For each slice that is missing, a temporary index is created in one of the directories specified by `/index/config/index.dir`. The slices are reindexed in reverse numerical order. Thus, the most recently collected sessions are indexed first.
4. Once the slice is completely reindexed, it is moved into its valid location in the online index. If the reindexed slice belongs on the warm tier, it is moved to the warm tier.
5. The newly indexed data appears as part of the collection.

Background indexer status

The stat node `/index/stats/updater.state` indicates the current state of the background reindexer. This node will say `running`, `not running`, or `failed`. If the status is `failed`, check the service log for more diagnostic information.

Effects on Aggregation

Services that perform aggregation utilize the index to keep track of sessions that have already been aggregated. If the index does not have enough information to begin aggregation, aggregation will be offline until enough slices have been reindexed. During this time the aggregation status for the upstream device will indicate that it is waiting on aggregation.

Forcing A Reindex

To force the index on a service to be rebuilt:

1. Ensure that `/index/config/reindex.enable` is true.
2. Reset the index by using the `reset` message on the service. For example: `/concentrator/reset index=1` will restart the service and delete all the index files.
3. Wait for the service to restart. Background reindexing will start.
4. The most recently collected data will be available for queries as soon as the index slice representing those sessions has been reindexed.

Optimization Techniques

This topic describes optimization techniques for the NetWitness Core database. The NetWitness Core database is set up to work with a wide variety of work loads by default. However, like any database technology, its performance can be very sensitive to both the nature of the data being ingested, and the nature of the searches that the user performs against the database.

Thresholds

Thresholds are a useful optimization that can have a dramatic effect on how fast results are returned to the NetWitness Suite Navigate view. Thresholds are applied to the `values` call. For more information about the `values` call, see Queries .

The threshold defines a limit to how much of the database is retrieved from disk in order to produce a count. For most queries, the number of sessions that match the `where` clause is very large. For example, selecting all the log events for just one hour running at 30,000 events per second matches 108,000,000 sessions.

RSA introduced the threshold feature based on the observation that most cases where a count of sessions is required do not have to have results that are accurate down to the very last session. For example, when looking at the top 20 IP addresses present over the past hour, it is not very important if the report indicates that an IP value matched 10,000,000 or 10,000,001 sessions exactly. The estimate is good enough. In these scenarios, we can make an estimate for the value of the count returned when our count exceeds the threshold parameter. When the threshold is reached, the remaining count is estimated, and the results are sorted based on the estimated counts, if necessary.

Complex `where` Clauses

The amount of time it takes for the NetWitness Core database to produce a result is dependent on the complexity of the query. Queries that align directly with the indexes present on the meta can be resolved quickly, but it is very easy to write queries that cannot be resolved quickly. Sometimes, queries that cannot be returned quickly can be processed by the Core database and the index differently to produce much more satisfying results for the customer.

It is useful to know the relative *cost* of each part of the `where` clause. A clause with a high cost takes longer to execute. In the following table, the query operations are ordered in terms of their relative cost, from lowest to highest.

Operation	Cost
exists, !exists	Constant
= , ! =	Logarithmic in terms of the number of unique values for the meta key, linear in

	terms of the number of unique elements that match a range expression
< , > , <= , >=	Logarithmic in terms of unique value lookup, but more likely to be linear since the expression matches a large range of values
begins , ends , contains	Linear in terms of the number of unique values for the meta key
regex	Linear in terms of the number of unique values for the meta key with a high per-value cost

AND and OR

When constructing a where clause, keep in mind that constructing many terms using the AND operator can have a beneficial affect on the performance of a query. Any time that multiple criteria can be used to filter down the set of sessions matching the where clause, there is less work for the query to do. Likewise, each OR clause creates a larger set of sessions to process for each query.

As a general rule of thumb, the more AND clauses in the query, the faster it completes, but the more OR clauses in the query, the slower it completes.

Use Case: Match a Large Subnet

It is common for users to construct queries that attempt to include or exclude a class-A subnet. This type of query is common because the users are trying to include or exclude some large portion of their internal network from their investigation.

It is a problem for the query engine to resolve this query using the ip.src or ip.dst indices alone. The issue arises from the fact that a where clause such as this:

```
ip.src = 10.0.0.0/8
```

Actually must be interpreted as:

```
ip.src = 10.0.0.0 || ip.src = 10.0.0.1 || ip.src = 10.0.0.2 || ... ||
ip.src = 10.255.255.255
```

Thus, the index could have to create a where clause with more than 16 million terms.

The solution to this problem is to use the Decoder to tag common networks of interest using application rules. For example, you could create meta items with an application rule that looks like this:

```
name=internal rule="ip.src = 10.0.0.0/8" order=3 alert=network
```

This rule creates meta items in the meta key network with the value internal for any IP address in the 10.0.0.0/8 network.

The `where` clause could be expressed as:

```
network = "internal"
```

Assuming there is a `value-level` index on the network meta data, the index does not have to expand this query into anything more complex, and the sessions matching the desired subnet are matched very quickly.

Use Case: Substring Matching

Using the operators `begins` , `ends` , `contains` , and `regex` in a `where` clause can be very slow if there are a large number of unique values for the meta key. Each of these operators is evaluated independently against each unique value. For example, if the operator is `regex` , the `regex` must be run independently against each unique value.

To work around this, the most effective strategy is to reorganize the meta items such that the user does not have to use a substring match.

For example, consider if the users are attempting to find the host name within a URL somewhere in the session. The users might write a `where` clause such as:

```
url contains 'www.rsa.com'
```

In this scenario, it is likely that the `url` meta key contains one unique value for every session that was captured by the Decoder, and therefore has a huge number of unique values. In this case, the contains operation is slow.

The best approach is to identify the part of meta data they are attempting to match, and move the matching into the content parser.

For example, if there is meta data being generated for each URL, a parser could also break down the URL into its constituent components. For example, if the Decoder generates URL meta data with the value `http://www.rsa.com/netwitness` , it could also generate `alias.host` meta data with the value `www.rsa.com` . Queries could be performed using:

```
alias.host = 'www.rsa.com'
```

Since the substring operator is no longer needed, the query is much faster.

Index Saves

The Core index is subdivided by save points, also known as slices. When the index is saved, all the data in the index is flushed to disk, and that portion of the index is marked as read-only. Saves serve two functions:

- Each save point represents a place where the index could be recovered in the case of a power failure.
- Periodically saving can ensure that the portion of the index that is actively being updated does not grow larger than RAM.

Save points have the effect of partitioning the index into independent, non-overlapping segments. When a query must cross over multiple save points, it must re-execute parts of the query and merge the results together. This ultimately makes the query take longer to complete.

By default, for NetWitness Suite 10.5 and later installations, a save is performed on the Core index every time 600,000,000 sessions are added to the database. This interval is set by the index configuration parameter `save.session.count` . For more information, see Index Configuration Nodes .

Older versions of NetWitness Suite, or systems that have been upgraded from NetWitness Suite versions prior to 10.5, use a time-based save schedule that saves the index every 8 hours. You can see the current save interval by using the scheduler editor in the NetWitness Admin UI for the service. The default entry looks like this:

```
hours=8 pathname=/index msg=save
```

By adjusting the interval, you can control how often saves are created.

Affects of Increasing the Save Interval

By increasing the save interval, save points are created less frequently, and therefore fewer save points exist. This has a positive effect on query performance, because it becomes less likely that queries traverse slices, and when slices do have to be traversed, there are not as many to traverse.

There are downsides to increasing the save interval though. First, the Concentrator is more likely to hit the `valueMax` limit set on any of the indices. Second, the recovery time in the event of a forced shutdown or power failure is increased. And third, the aggregation rate may suffer if the index slice grows too large to fit in memory.

Affects of Decreasing the Save Interval

By decreasing the save interval, it is possible to avoid hitting the `valueMax` limits while maintaining a full value index for meta data that contains a large number of unique values. Decreasing the save interval does have a detrimental impact on query performance, since more slices are created.

Working with `valueMax`

The `valueMax` limitation can be frustrating to customers who want to index all possible unique meta. Unfortunately that is not possible in the general case. Meta keys exist that can have arbitrary random data from anywhere on the Internet, and all unique values cannot be indexed.

However, it is possible to work around some of the limitations of `valueMax` by using key level indices instead of value indices. Key level indices are not influenced by `valueMax` .

It is possible to use the Navigate view on a meta key indexed at the key level. The database uses value level indices in the `where` clause where possible, but meta database scanning is used to resolve unique values for the `values` call. This approach works well when the `where` clause provides an effective filter to limit search scope to a small number of sessions, perhaps less than 10,000 sessions.

In cases where the `valueMax` is reached, the users can perform a database scan on their queries to ensure no relevant values were dropped. This feature is accessible in the Investigator 9.8 client via the right-click menu on the Navigation view. Although the meta database scan takes a long time, it reassures the customer that they are not missing anything in their reports.

Parallelize Workloads

When the customer is using a lot of reports, ensure that they are making full use of the parallel executing options within Reporting Engine. Likewise, ensure that the number of `max.concurrent.queries` is appropriate for the hardware.

The NetWitness Suite Navigate view has the ability to run the components of its output in parallel, which can have a significant impact on the perceived performance of the NetWitness Core service.

Index Rebuild

In rare cases, a Core service might benefit from an index rebuild. Examples:

- The NetWitness Core service has index slices created by a very old version of the product and has not rolled out any data in more than six months.
- The index was configured incorrectly, and the customer wants to re-index all meta with a new index configuration.
- The traffic load into the Core service was very light, and the save interval was large, causing more slices than needed to be generated.

In these cases, an index rebuild may provide performance improvements. To do so, you must send the message `reset` with the parameter `index=1` to the `/decoder` folder on a Decoder, the `/concentrator` folder on a Concentrator, or the `/archiver` folder on an Archiver.

Be aware that a full reindex takes days to complete on a fully loaded Concentrator, and possibly weeks on a full Archiver.

Scaling Retention

There are several ways to improve the retention of the NetWitness Core database. Retention refers to the period of time that is covered by data stored in the database.

The first step in analyzing retention is to determine which part of the database is the limiting factor in terms of retention. The packet, meta, and session databases provide the `packet.oldest.file.time` , `meta.oldest.file.time` , and `session.oldest.file.time` stats in the `/database/stats` folder to show the age of the oldest file in the database. The index provides the `/index/stats/time.begin` stat to show the oldest session time stored in the index.

Increasing Packet and Meta Retention

The primary mechanism for increasing retention on these databases is adding more storage. If adding more storage to the NetWitness Core service is not possible, then it may be necessary to use the compression options on the packet and meta database to reduce the amount of data each database writes.

If meta retention is a concern, you may want to remove unneeded content from the Decoder generating meta. Many parsers generate meta that the customer does not need to store long term.

Increasing Index Retention

Usually the index has longer retention than the databases, but with a complex custom index the index retention may be shorter. Usually the easiest course of action is to remove unneeded value-level indices from the custom config, or perhaps override some of the default value-level indices with key-level indices.

It is also possible to scale the index by adding additional index storage. However, the index storage should be extended using solid-state drives only.

Scaling Horizontally

Starting in version 10.3, Concentrators and Archivers have the ability to be clustered using group aggregation. Group aggregation allows a single Decoder to feed sessions to multiple Concentrators or Archivers in a load-balanced manner. Group aggregation enables the query and aggregation workload to be split among an arbitrarily large pool of hardware.

For more information, see the "Group Aggregation" topic in the *Deployment Guide* .

Grouping Workloads

The NetWitness Core database works much better when all the users of the system are working within the same region of the database. Since the database is fed data from the Decoder with a first-in-first-out scheme, data in the database typically is clustered together according to the time it was captured and stored. Therefore, the database works better when all users are working on the same time period of data.

It is not always possible for all users to be working on the same time period simultaneously. The NetWitness Core database can handle that use case, but it is slow to do so because it must alternate between having different periods of time in RAM. It is not possible to have all of the time periods in RAM at the same time. Typically less than 1 percent of the database and less than 10 percent of the index fits in RAM.

To make NetWitness Suite work for the customer, it is important to get the customer to organize their users into groups that tend to work on the same time ranges. For example, users who do daily monitoring over the most recent data may be one user group. Perhaps there is another user group that does queries further back in time as part of an investigation. And perhaps another set of users do reports over large periods of time. Attempting to serve all the groups from a single database can lead to frustration and long wait times for results to be produced. However, if the different use cases can be spread to different Concentrator hardware, the perceived performance can be much better. In this case, it may be beneficial to utilize more Concentrator services with less RAM and CPU power rather than a single large and expensive Concentrator intended to meet all needs.

Cache Window

Consider this sequence of events:

1. At 9:00 a.m., user "kevin" logs in to a Concentrator and requests a report on the last one hour of collection time.
2. The Concentrator retrieves reports for the time range 8:00 a.m. to 9:00 a.m.
3. At 9:02 a.m., user "scott" logs in to the same Concentrator and also requests a report on the last one hour of collection time.
4. The Concentrator retrieves reports for the time range 8:02 a.m. to 9:02 a.m.

Notice that even though both users were looking at time ranges that were close together, the work done by the Concentrator to produce reports for Kevin could not be re-sent to Scott, since the time ranges are slightly different. The Concentrator had to re-calculate most of the reports for Scott.

The setting `cache.window.minutes` on the `/sdk` node allows you to optimize this situation. When a user logs in, the point in time representing the most recent data for the collection only moves forward in increments of the the number of minutes in this setting.

For example, assume the `/sdk/config/cache.window.minutes` is 10\. Re-evaluating the above action changes the sequence of events.

1. At 9:00 a.m., user "kevin" logs in to a Concentrator and requests a report on the last one hour of collection time.
2. The Concentrator retrieves reports for the time range 8:00 a.m. to 9:00 a.m.
3. At 9:02 a.m., user "scott" logs in to the same Concentrator and also requests a report on the last one hour of collection time.
4. The Concentrator retrieves reports for the time range 8:00 a.m. to 9:00 a.m.
5. At 9:10 a.m., user "scott" re-loads the reports for the last one hour of collection time.
6. The Concentrator retrieves reports for the time range 8:10 a.m. to 9:10 a.m.

The report returned in step 3 falls in the cache window, so it is returned instantaneously. This gives Scott the impression that the Concentrator is very fast.

Thus, larger `cache.window` settings improve perceived performance, at the cost of introducing small delays until the latest data is available to search.

Time Limits

When a query is running on the NetWitness Core database for a very long time, the Core service dedicates more and more CPU time and RAM to that query in order to get it to complete faster. This can have a detrimental impact on other queries and aggregation. In order to prevent lower privileged users from using more than their share of the Core service resources, it is a good idea to put time limits on the queries run by normal users.

Appendix A: Statistics

This topic describes statistics used to monitor system operation. The Core services provide a very large number of statistics for monitoring the operation of the system. Some of them are useful for monitoring performance, while some of them exist for monitoring the operation of the system or for debugging purposes.

Statistics in /database/stats

The following table shows the meaning of the statistics in **/database/stats** .

Statistic	Meaning
`meta.bytes` , `packet.bytes` , `session.bytes`	The total size of data (in bytes) stored in each database
`meta.first.id` , `packet.first.id` , `session.first.id`	The first meta ID, packet ID, and session ID, respectively, stored in the database
`meta.last.id` , `packet.last.id` , `session.last.id`	The last meta ID, packet ID, and session ID, respectively, stored in the database
`meta.oldest.file.time` , `packet.oldest.file.time` , `session.oldest.file.time`	The creation date of the oldest file in each database
`meta.rate` , `packet.rate` , `session.rate`	The count of the number of meta, packet, and session objects added to each database over the last second
`meta.total` , `packet.total` , `session.total`	The total number of meta, packet, and session objects within each database
`meta.volume.bytes` , `packet.volume.bytes` , `session.volume.bytes`	The approximate total volume size (in bytes) for all directories used by each database
`meta.free.space` , `packet.free.space` , `session.free.space`	The approximate total unused space (in bytes) across all directories used by each database

Statistics in /index/stats

The following table shows the meaning of the statistics in **/index/stats** .

Statistic	Meaning
`checkpoint.page` , `checkpoint.summary`	The last objects stored the last time an index save was created (debugging)
`index.bytes`	An approximate measure of how much disk space is required by index files
`index.last.load.time`	The timestamp when the current index configuration was loaded from the index configuration files
`memory.used`	An approximate measure of how much memory is occupied by the index
`page.first.id` , `summary.first.id`	The first page and summary object stored in the index (debugging)
`page.last.id` , `summary.last.id`	The last page and summary object stored in the index (debugging)
`page.total` , `summary.total`	Number of pages and summaries in the index (debugging)
`session.first.id`	The ID of the first session indexed
`session.last.id`	The ID of the last session indexed
`sessions.since.save`	The number of sessions currently held by the current index slice
`values.added`	The number of unique values added to the current index slice
`slices.total`	The number of slices in the index
`time.begin`	The oldest time meta indexed
`time.end`	The most recent time meta indexed
`updater.state`	The status of background reindexer

Statistics in /sdk/stats

The following table shows the meaning of the statistics in **/sdk/stats**

Statistic	Meaning
cache.window.time.begin	The beginning of the current time enforced by cache.window.minutes
cache.window.time.end	The end of the current time enforced by cache.window.minutes
queries.active	The number of queries currently executing in the index
queries.queued	The number of queries waiting for execution
values.calls	The number of calls made to the "values" function since the process was started
values.calls.cached	The number of calls made to the "values" function that were resolved by the values call result cache

Per-query Statistics

SDK operations, such as query and values, provide information about their execution status in /sdk/config/stats/queries/<handleid> , where <handleid> is a unique identifier for the query operation.

The following table shows the meaning of per-query statistics.

Statistic	Meaning
channel.path	This stat provides a link to the connection channel over which the operation is communicating. This channel is used to communicate results back to the client.
query.type	The type of operation being performed, such as queries or values
query	The complete set of parameters given to the query
query.progress	The percentage of the query execution that has completed
query.status	A message describing what stage of the query execution is currently occurring
running.since	The time at which the query began execution
user	The user name that executed the query

Appendix B: Index Inspect

The NetWitness Core database index has a built-in debugging feature called `inspect` that provides detailed information about the composition of its indexes. The index inspect feature is located at `/index/inspect` in every Core service configuration tree. Services that do not actually have an index, like Broker, do not have the `/index/inspect` feature.

Parameters

Options

Type: String This parameter may be set to the value `all-slices` to collect inspect information about every slice in the index. If it is not set, information on the current, most recently created slice is returned.

Collecting information on all slices may take a very long time to complete if there are many index slices.

Response

Inspect returns many rows of key value pairs that represent the state of the index.

Slice Summary

The first row returned for every slice is a summary with the following values.

`session1`	The first session ID indexed in the slice
`session2`	The last session ID indexed in the slice
`meta1`	The first meta ID in the first session indexed in the slice
`meta2`	The last meta ID in the last session indexed in the slice

Per-Index Summary

There will be per-index summary rows returned for each index. Only value-level indexes are reported.

`key`	The meta key name for the index
`pathname`	The path on disk to this index
`values`	The number of unique values stored in this index
`summaries`	The number of summary entries occupied by this index in the summary.db file

`pages`	The number of page entries occupied by this index in the page.db file
`sessions`	The number of sessions that had a value that was inserted into this index
`size`	The cumulative "size" meta values for all sessions that inserted a value into this index
`packets`	The cumulative count of packets for all sessions that inserted a value into this index
`summary1`	The first summary ID used by this index
`summary2`	The last summary ID used by this index
`session1`	The first session ID referenced by this index
`session2`	The last session ID referenced by this index

Slice Summary Footer

The last row in each inspect report contains cumulative statistics for all the indexes in the slice.

`totalKeys`	The number of indexed meta types
`totalValues`	The number of unique values tracked by all indices in this slice
`totalMemory`	An approximate total of the memory needed to open this index slice

RSA NETWITNESS® SUITE

Decoder and Log Decoder Configuration Guide

for Version 11.0

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2018

Contents

Decoder and Log Decoder Quick Setup 9

Perform Initial Quick Setup 11

Configure Common Settings on a Decoder 13

Configure Capture Settings 15

Select a Network Adapter 15

Configure a Decoder to Begin Capturing Data Automatically 17

Configure Optional Capture Settings 18

(Optional) Configure System-Level (BPF) Packet Filtering 19

(Optional) Configure a Decoder to Capture Data Across All Types of Network Interfaces 22

(Optional) Preserve VLAN Tags When Using the Packet MMAP Capture Interface 25

Enable and Disable Parsers and Log Parsers 29

Start and Stop Data Capture 32

Configure Decoder Rules 33

Rule Processing 34

Rule and Query Guidelines 34

Rule Examples 35

Invalid Rules 35

General Syntax Guidelines 36

Capture Rule Syntax 36

Configure Capture Rules 40

Import Rules from a File and Export Rules 42

Push Rules to Other Services 44

Change Execution Order of Rules 46

Restore a Rule Snapshot from History 46

Configure Application Rules 48

Monitor Application Rules 51

Configure Correlation Rules 52

Configure Network Rules 56

Supported Meta Keys in Network Rule Conditions 56

Fix Rules with Invalid Syntax 61

Decoder Commands for Managing Rules 63

add Command 63
merge Command 64
Methods of Sending a List of Rules to a Service 65
Ordering Rules When Pushing 66
replace Command 67
clear Command 68
delete Command 68
validate Command 68

Configure Feeds and Parsers 69

Configure Parsers 69
Configure Feeds 70
Custom Feed Definition File Structure 71
Sample Feed Definition File 71
Feed Definition Equivalents for Custom Feed Wizard Parameters 72
Sample Files for a MetaCallback Feed Using CIDR Index Range for IPv4 and IPv6 75
Create a Custom Feed 77
Create a STIX Custom Feed 89
Create an Identity Feed 100
Import the SSL Certificate 109
Cannot Verify Identity Feed URL 110
Edit, Upload, or Remove a Feed 112
Create Custom Meta Keys Using a Custom Feed 117
Add a Custom Meta Key in the Log Decoder 117
Deploy a Log Decoder Feed in Live 117
Add the Custom Meta Key Entry in the Concentrator Custom Index file 123
Investigate on the Custom Meta Key 124
Additional Procedures 125
Upload and Delete Custom Parsers 129
Upload Parsers to a Decoder or Log Decoder 129
Manage Upload Jobs 131
Delete Deployed Parsers 131
Enable and Configure the Entropy Parser 132
Entropy Parser Configuration in the Concentrator Custom Index File 135

Decoder and Log Decoder Additional Procedures 137

Configure 10G Capability 138

Hardware Prerequisites 138
Software Prerequisites 139
Install the 10G Decoder 139
Configure the 10G Decoder 140
Storage Considerations 142
Parsing and Content Considerations 142
Optimize Read/Write Operations When Adding New Storage 145
Configure a Log Decoder to Accept Protobuf 148
Configure Session Split Timeouts 150
Configure Syslog Forwarding to Destination 153
Configure Transaction Handling on a Decoder 156
Transaction Handling 156
Decrypt Incoming Packets 158
Performance Considerations 159
Encryption Keys 162
Upload Multiple Premaster and Private Keys 163
Parameters for Managing Keys 165
Return Values 165
Viewing Unencrypted Traffic 166
Supported Cipher-Suites 166
Edit Decoder System Configuration 185
Enable CPU Usage Statistics for Installed Content 187
Enable Parser Mappings 188
Enable IP Address to Event Source Mapping 188
Update IP to Event Source Mapping 189
Read IP to Event Source Type Mappings 190
Edit an IP to Event Source Type Mapping 191
Delete an IP to Event Source Type Mapping 191
Sort the Hostname or Event Source Type 191
Import IP to Event Source Mapping Entries 192
Export IP to Event Source Mapping Entries 193
Search IP to Event Source Mapping Entries 193
Enable or Disable Lua and Flex Parsing Systems 194
Map IP Address to Service Type for Log Parsing 195
Map an IP Address to a Service Type 195
Map an IP Address to a Time Zone 196

Obtain Log Files a from Pre-11.0 Log Decoder 197
Upload a Log File to a Log Decoder 200
Upload a Packet Capture File 202

Feed and Parser References 204

Feed Definitions File 205
feed-definitions.xml 205
Flex Parsers 206
NwFlex.xml 206
Arithmetic Functions 208
Common Parser Operations 210
General Functions 213
Logging Functions 216
Nodes 217
Payload Functions 224
Regex 227
String Functions 228
Geo IP Parser 232
GeoPrivate.ipl 232
Lua Parsers 233
List of Lua Parsers 233
Search Parser 234
search.ini 234
search.ini Search String Syntax 235
Wireless LAN Configuration 237
wlan-config.xml 237

Decoder and Log Decoder References 239

Services Config View - Data Privacy Tab 240
What do you want to do? 240
Related Topics 240
Quick Look 241
Services Config View - Data Retention Scheduler 242
What do you want to do? 242
Related Topics 242
Quick Look 242
Services Config View - Feeds Tab 244

What do you want to do? 244
Related Topics 244
Quick Look 244
Upload Feeds Dialog 246
What do you want to do? 246
Related Topics 246
Quick Look 246
Services Config View - Files Tab 249
What do you want to do? 249
Related Topics 249
Quick Look 249
Services Config View - General Tab 251
Workflow 251
What do you want to do? 251
Related Topics 251
Quick Look 251
Services Config View - Parsers Tab 260
What do you want to do? 260
Related Topics 261
Quick Look 261
Services Config View - Parser Mappings Tab 263
What do you want to do? 263
Related Topics 263
Quick Look 263
Services Config View - Rules Tabs 266
Workflow 266
What do you want to do? 266
Related Topics 267
Quick Look 267
App Rules Tab 270
What do you want to do? 270
Related Topics 270
Quick Look 270
Correlation Rules Tab 274
What do you want to do? 274
Related Topics 274

Quick Look 274
Network Rules Tab 277
What do you want to do? 277
Related Topics 277
Quick Look 277
Services System View - Decoders 282
Workflow 282
What do you want to do? 282
Related Topics 283
Quick Look 283

Decoder and Log Decoder Quick Setup

A basic RSA Network Suite network includes at minimum Brokers, Concentrators, and Decoders. Brokers aggregate data from Concentrators, and Concentrators consume data from at least one Packet Decoder or Log Decoder. The basic network may include both types of Decoders. Packet Decoders are usually referred to as Decoders, and they capture network data in packet form. Log Decoders capture log data as events.

Adding a Decoder makes it visible and available for use with NetWitness SuiteAdministration, Live Services, and Investigate. To add a service in NetWitness Suite, you select the service type, provide service connection information, and validate that the service can be reached. The *Hosts and Services Getting Started Guide* provides the information you need to understand and install all NetWitness Suite services.

After the services are added, you need to configure each service. This is the preferred order for configuring your system:

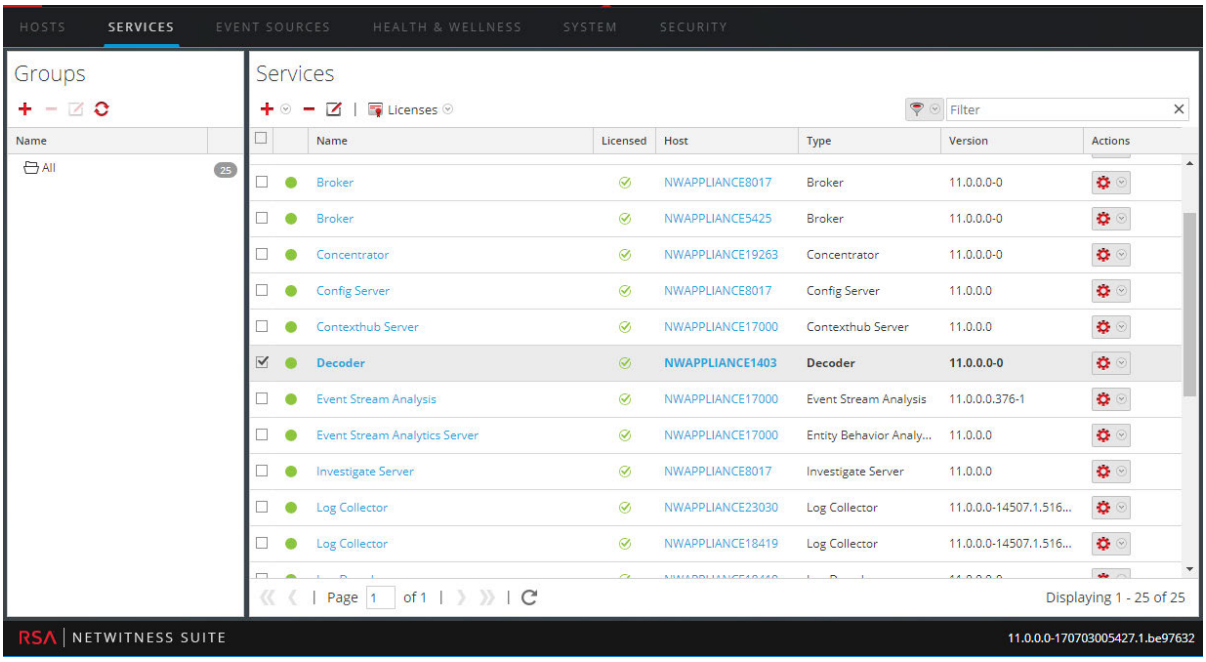
1. Decoders
2. Log Decoders
3. Concentrators (refer to the *Broker and Concentrator Configuration Guide*)
4. Brokers (refer to the *Broker and Concentrator Configuration Guide*)

Note: A Log Decoder is a special type of Decoder, which is configured and managed in a similar way to a Decoder. Most of the information in this guide refers to both types of Decoders. "Decoder" refers to both types of Decoders. Information that applies exclusively to Packet Decoders or Log Decoders is clearly identified.

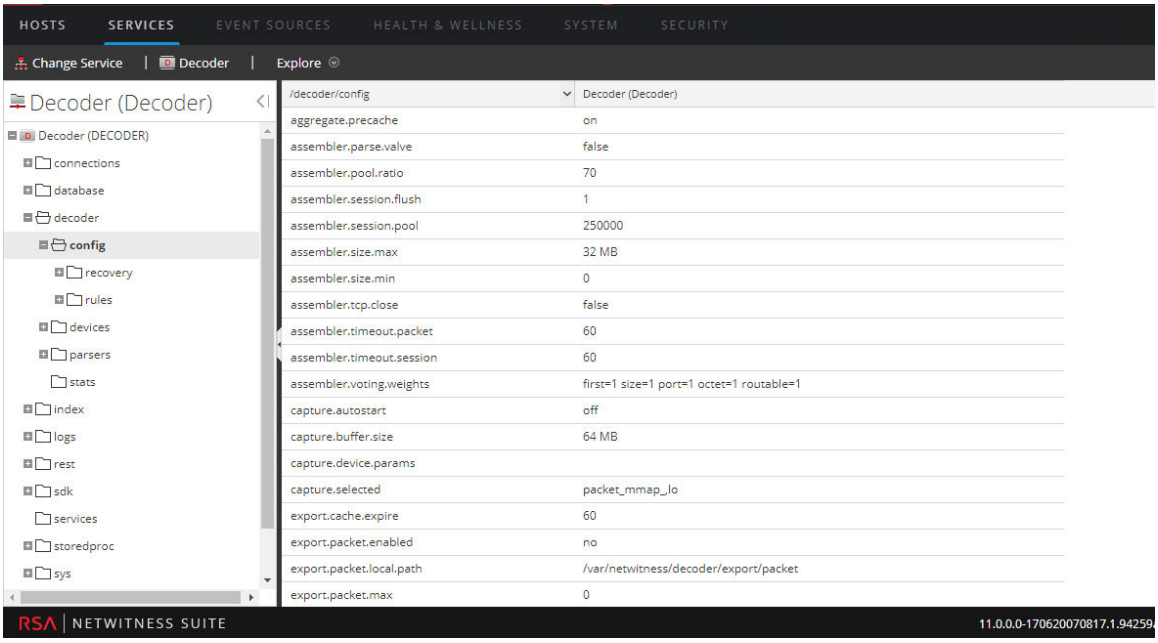
Basic Configuration of the Decoder involves selecting a network adapter interface and starting data capture.

In addition, you can configure each Decoder to control the type of traffic captured using rules, feeds, and parsers. Advanced configuration tasks enable additional features that are relevant to specific applications. For example, configure a 10G Decoder, create custom meta keys, or decrypt incoming packets.

The easiest way to configure all of the required Decoder and Log Decoder settings is to use the options in the NetWitness Suite user interface. For the most part, configuration is performed in the Administration Services view (ADMIN > Services).



Administrators who feel comfortable working outside of the user interface can configure the basic parameters as well as advanced settings by editing database nodes in the Decoder node tree using the Services Explore view.

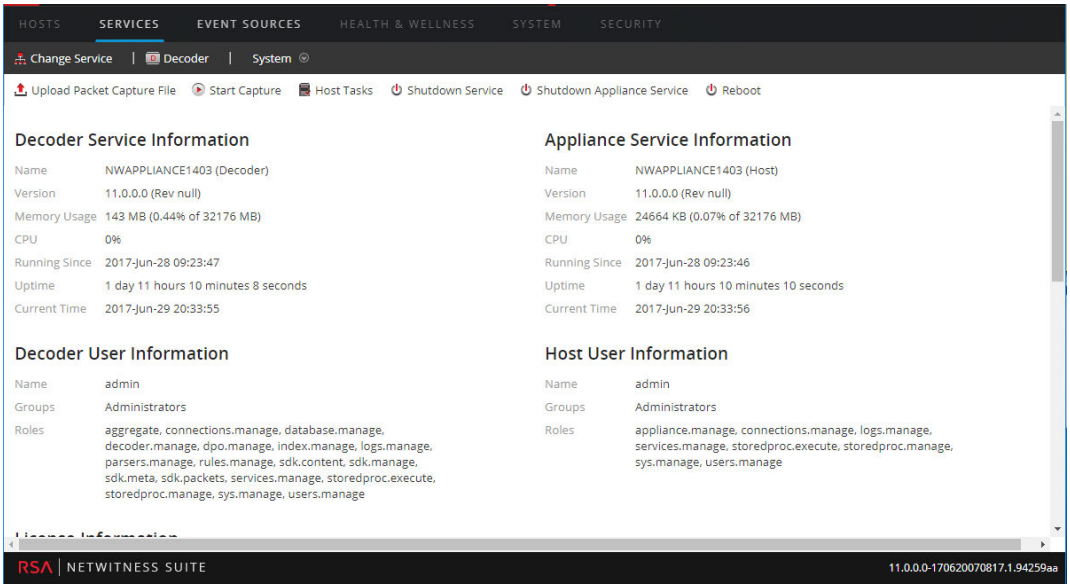


Perform Initial Quick Setup

This procedure accomplishes the initial, basic configuration of a Decoder, and starts data capture. When the basic setup is complete, the Decoder begins capturing data for the Concentrator to consume.

To configure a Decoder and start capturing data:

1. Assign a network interface for capturing data. For details, see "Select a Network Adapter" in Configure Capture Settings.
2. Do one of the following:
   a. To start capture, select the Decoder and > **View** > **System**. In the toolbar click Start Capture.



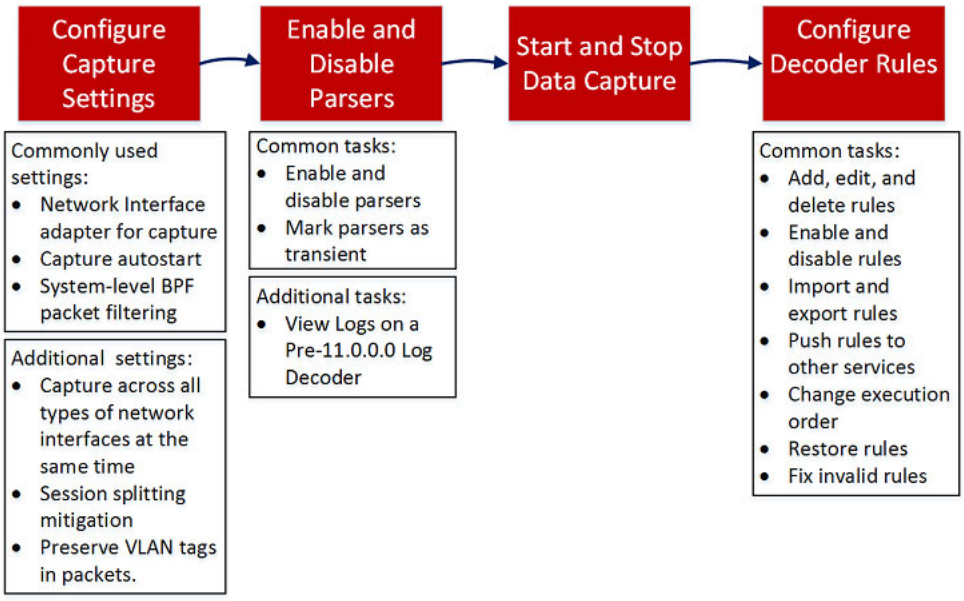
   b. To enable Capture Autostart, see "Configure a Decoder to Begin Capturing Data Automatically" in Configure Capture Settings.
   The Decoder begins capturing data for consumption by a Concentrator. For additional configuration options, refer to Configure Common Settings on a Decoder and Decoder and Log Decoder Additional Procedures

Configure Common Settings on a Decoder

This section introduces commonly used configuration settings on a Decoder with procedures and background information. After you have completed Decoder and Log Decoder Quick Setup, you can refine your configuration by using parsers, feeds, and rules to limit the captured data.

Note: A Log Decoder is a special type of Decoder, which is configured and managed in a similar way to a Decoder. Most of the information in this guide refers to both types of Decoders. "Decoder" refers to both types of Decoders. Information that applies exclusively to Packet Decoders or Log Decoders is clearly identified.

The following workflow illustrates commonly used settings and breaks the configuration process into four steps.

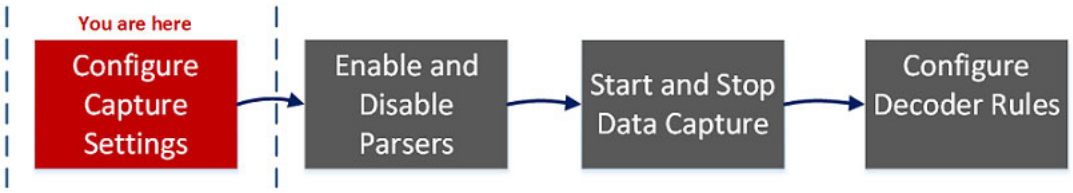


Configuration Step	Description
Configure Capture Settings	When initially setting up the Decoder, configuring the network adapter interface is required. Additional optional capture settings are available; one that is frequently used is Capture Autostart.
Enable and Disable Parsers and Log Parsers	View the parsers that have been downloaded and deployed from Live, and manage which ones are enabled or disabled.

Configuration Step	Description
Start and Stop Data Capture	When a Decoder starts up, it automatically begins aggregating data if Capture Autostart is enabled. When autostart is not enabled, you can start and stop data capture manually.
Configure Decoder Rules	Capture rules can add alerts or contextual information to sessions or logs. They can also define which data a Decoder or Log Decoder filters out. By default, no capture rules are defined when you first configure NetWitness Suite. Unless rules are specified and the rules are valid, the packets are not filtered. You can deploy the latest rules from Live as described in the *Live Services Management Guide*. You can define capture rules at any time, and you can fix rules that use invalid syntax (Fix Rules with Invalid Syntax).

Configure Capture Settings

When initially setting up the Decoder, configuring the network adapter interface is required. Additional optional capture settings are available; two that are frequently used are the Berkeley Packet Filter, and Capture Autostart.



Besides the basic network adapter interface setup, you may decide to use one of the special-purpose configurations described in (Optional) Preserve VLAN Tags When Using the Packet MMAP Capture Interface or (Optional) Configure a Decoder to Capture Data Across All Types of Network Interfaces

The rest of the capture settings have default values chosen to be effective in most cases (see a detailed list in Services Config View - General Tab). You can adjust these in some circumstances, for example, if Customer Support advises a change. You can edit the capture settings at any time.

Select a Network Adapter

The table below describes the Netword Adapter settings for a Decoder. The system administrator sets the default network adapters when the Decoder is installed. Consult your System Administrator for more information.

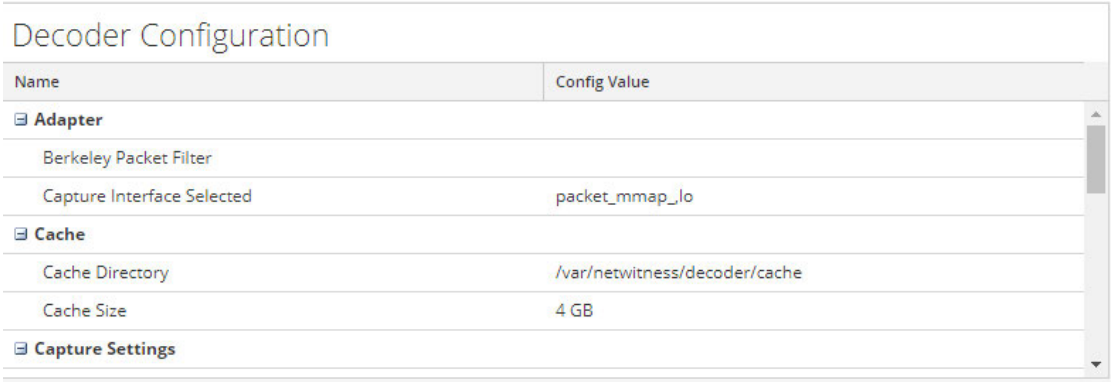
Adapter Parameter	Description
Berkley Packet Filter	Berkeley Packet Filters (BPF) are applied to the packet stream before the packets are copied to the Decoder adapter for analysis. This allows unwanted traffic to be efficiently discarded. However, any packets discarded are not accounted for in any Decoder statistics (capture rate, packets dropped, and packets filtered and total packets).

Adapter Parameter	Description
Capture Interface Selected	Select an adapter through which the Decoder captures packets. For the lower speed internal capture interface, use the `packet_mmap_,7,eth1` adapter, which corresponds to the monitor port located on the motherboard. There are six additional capture ports: • `packet_mmap_,1,lo (bpf)` • `packet_mmap_,2,eth2 (bpf)` • `packet_mmap_,3,eth3 (bpf)` • `packet_mmap_,4,eth4 (bpf)` • `packet_mmap_,5,eth5 (bpf)` • `packet_mmap_,8,ALL (bpf)` There are three wireless capture services available: • `packet_netmon_ (Microsoft Netmon)` • `packet_mac80211_ (Linux mac80211)` • `packet_airport_ (Mac OS X AirPort)`
Capture Interface Selected for Log Decoder	The following capture service is available: • `log_events,Log Events`

To configure the network adapter on a Decoder:

1. Go to **ADMIN > Services**.

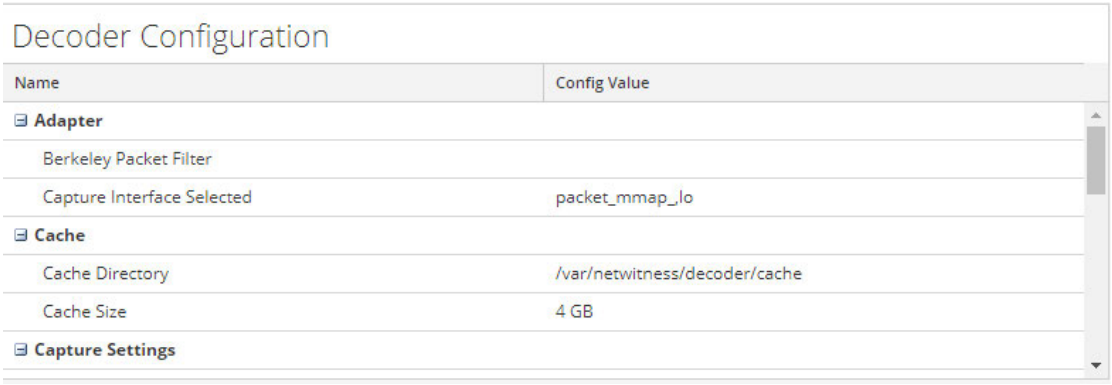
2. In the **Administration Services view**, select the Decoder and ⚙ > **View** > **Config.**
   The Services Config view is displayed with the General tab open.



3. In the **Capture Interface Selected** field, select the network adapter that best suits the Decoder.
4. To save the changes, click **Apply.**
5. If necessary to put the changes into effect, navigate back up to the **Administration Services view**, select the Decoder, and select ⚙ > **Restart**.

Configure a Decoder to Begin Capturing Data Automatically

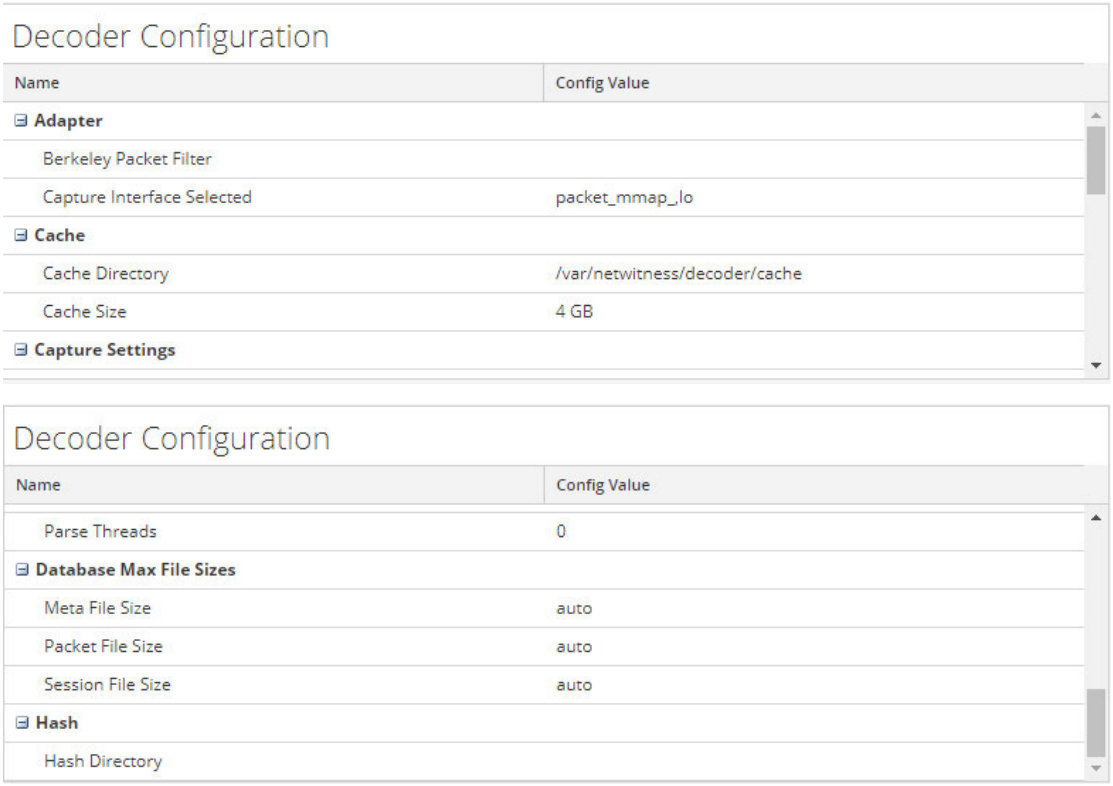
1. Go to **ADMIN** > **Services**.
2. In the **Administration Services view**, select the Decoder and ⚙ > **View** > **Config.**
   The Services Config view is displayed with the General tab open



3. Under **Capture Settings**, select the **Capture Autostart** checkbox.
4. To save the changes, click **Apply.**
5. If necessary to put the changes into effect, navigate back up to the **Administration Services view**, select the Decoder, and select ⚙ > **Restart**.

Configure Optional Capture Settings

1. Go to **ADMIN > Services**.
2. In the **Administration Services view**, select the Decoder and **> View > Config.**
   The Services Config view is displayed with the General tab open.



3. If you want to apply a system-level filter to the packet stream before the packets are copied to the Decoder adapter for analysis, configure the Berkeley Packet Filter as described in (Optional) Configure System-Level (BPF) Packet Filtering.
4. In the **Capture Settings** sections, review the default values. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change. See Services Config View - General Tab for an explanation of these settings.
5. In the **Database Max File Sizes** section, review the default values. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change. See Services Config View - General Tab for an explanation of these settings.

6. In the **Hash** section, define a directory for hash files if you are using this feature. See Services Config View - General Tab for an explanation of these settings.

(Optional) Configure System-Level (BPF) Packet Filtering

You can use Berkeley Packet Filters to control which packets and logs are processed by a Decoder.

Berkeley Packet Filters (BPF) are applied to the packet stream before the packets are copied to the Decoder adapter for analysis. This allows unwanted traffic to be efficiently discarded. These discarded packets are not accounted for in any Decoder statistics (capture rate, packets dropped, and packets filtered and total packets).

The Decoder also supports system-level packet filtering defined using `tcpdump/libpcap` syntax. Specifying a `Libpcap` filter can efficiently reduce packet volume based on Layer 2 - Layer 4 attributes. A `Libpcap` filter is appropriate for use when a Decoder is receiving a traffic volume that is placing a load against the physical resources of the platform. In this scenario, the Decoder may consistently drop packets and have a large number of capture pages available (`/decoder/stats/capture.pagefree` is high).
The following is an example of a `libpcap` filter to keep only packets that do not have both source and destination addresses in the 10.21.0.0/16 subnet.

```
not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)
```

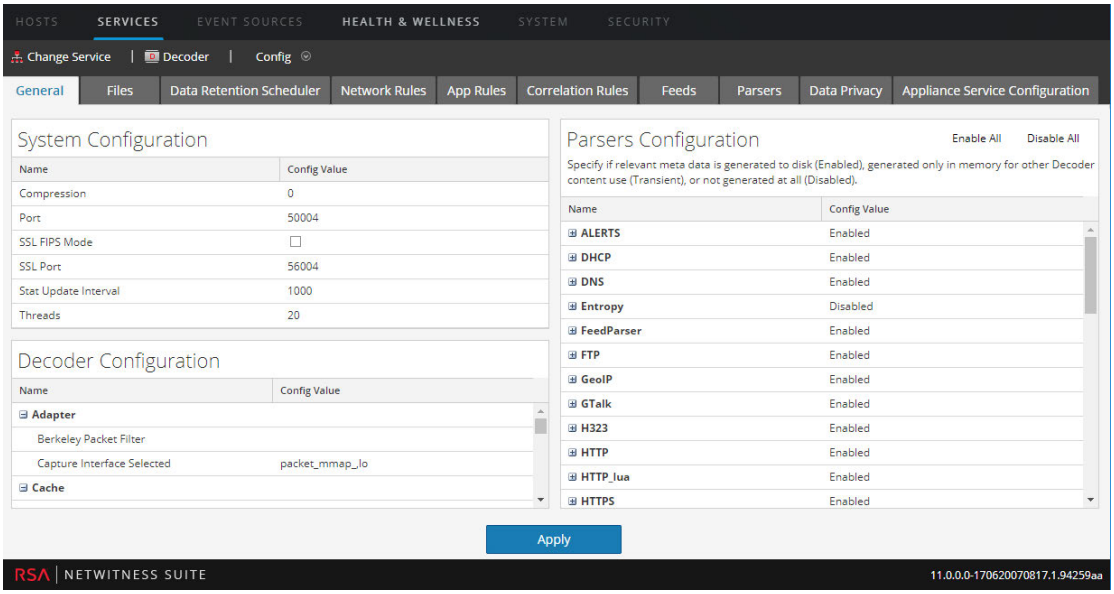
For a full reference of the `Libpcap` filter syntax, see the main pages for:

- tcpdump (http://www.tcpdump.org/tcpdump_man.html).
- pcap-filter (http://www.unix.com/man-page/FreeBSD/7/pcap-filter/).

To add a system-level Berkeley Packet Filter:

1. Go to ADMIN > **Services.**

2. In the Administration Services view, select a Decoder service and > **View** > **Config.**
   The Services Config view is displayed with the General tab open.



3. In the **Decoder Configuration Section**, under **Adapter**, click in the field next to **Berkeley Packet Filter**.
4. Type only one filter in the field. If you want to filter multiple items, join multiple expressions using `and`. Several examples are provided below.
   The user interface validates input at the time you enter your filter string.
5. To save the filter, click **Apply**.
   If the syntax is correct, a confirmation message is displayed.
   If the syntax is incorrect, a **Packet filter is not valid** message is displayed and a corresponding log message will follow in the log messages on the Decoder:
   `164474800 2015-May-01 19:03:08 warning Decoder Failed to parse filter 'example_badrule': syntax error`
6. To activate the filter, you must stop and start capture on the Decoder:
   a. Change the **Config** view to the **System** view.
   b. Click **Stop Capture**.
   c. Click **Start Capture**.
      The active filter will be displayed in the Decoder logs.

Examples

These are several filter examples:

- Drop packets to or from any address in the 10.21.0.0/16 subnet:
  `not (net 10.21.0.0/16)`
- Drop packets that have both source and destination addresses in the 10.21.0.0/16 subnet:
  `not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`
- Drop packets that are from 10.21.1.2 or are headed to 10.21.1.3.
  `not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Combine both IP and HOST:
  `not (host 192.168.1.10) and not (host api.wxbug.net)`
- Drop all port 53 traffic, both TCP & UDP:
  `not (port 53)`
- Drop only UDP port 53 traffic:
  `not (udp port 53)`
- Drop all IP protocol 50 (IPSEC) traffic:
  `not (ip proto 50)`
- Drop all traffic on TCP ports 133 through 135.
  `not (tcp portrange 133-135`

The following filters combine some of the above to demonstrate how to put multiple directives into one filter:

- Drop any port 53(DNS) traffic sourced from 10.21.1.2 or destined to 10.21.1.3.
  `not (port 53) and not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Drop any traffic using IP proto 50 or port 53 or any traffic from net 10.21.0.0/16 destined to net 10.21.0.0/16
  `not (ip proto 50 or port 53) or not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`

Caution: The use of parentheses can have a large and potentially disruptive effect on the use of Packet Filters. As a best practice, keep "not" operations outside of parentheses and always test your rules before deploying them. Failure to properly format your rules (despite input validation) can cause a packet filter to drop ALL traffic or behave in other unexpected ways. This is due to the way packet `Libpcap` filters work and is not the result of any logic within NetWitness Suite software.

Testing

BPF filters can and should be tested using either `tcpdump` or `windump` to ensure that they will provide the expected behavior before implementing them. This example shows a test of a filter using windump:

```
windump -nni 2 not (port 53 or port 443) or not (ip proto 50)
```

Conversions

If for the sake of performance, you have decided that an existing network rule filter would be better running as a System-Level Packet Filter, you can convert it. There are a few things to remember when doing conversions.

- `&&` becomes `and`
- `ip.addr` becomes `host` if a single host or **net** if a network.
- `ip.src` becomes `src host` if a single host or `src net` if a network.
- `ip.dst` becomes `dst host` if a single host or `dst net` if a network.
- Use CIDR notation when listing a network (that is, 10.10.10.0/24).
- `||` becomes `or`
- `!` becomes `not`
- Multiple rules must be joined with `and`.

The manual for TCPDump also gives examples of filters and strings that can be used: http://www.tcpdump.org/tcpdump_man.html

Additionally, the following site provides an excellent reference for BPF-style packet filters: http://biot.com/capstats/bpf.html

Caution: If you are capturing `vlan` tagged packets, above standard bpf filter may not work. For example, if you use `not (udp port 123)` to filter `vlan` tagged NTP traffic on udp port 123, it will not work. This is because the bpf filter machinery is simple and does not account for protocols not referenced in the rule. So the OS executing the bpf filter will look for the `udp port` values at the byte offset they would occur in a standard Ethernet/udp packet; but the optional `vlan` tag fields in the Ethernet header pushes those values by 4 bytes, thus the bpf filter rule will fail. To fix it, you need to change the bpf filter to: `not (vlan and udp port 123)`.

(Optional) Configure a Decoder to Capture Data Across All Types of Network Interfaces

The `packet_mmap_,ALL` adapter is capable of capturing across all types of network interfaces at the same time. For example, this can include things like physical network interfaces over different media types and tunnel interfaces.

The default behavior of the ALL adapter is to capture from all interfaces from the system, except for the hard-coded defaults of lo, eth0, and em1.

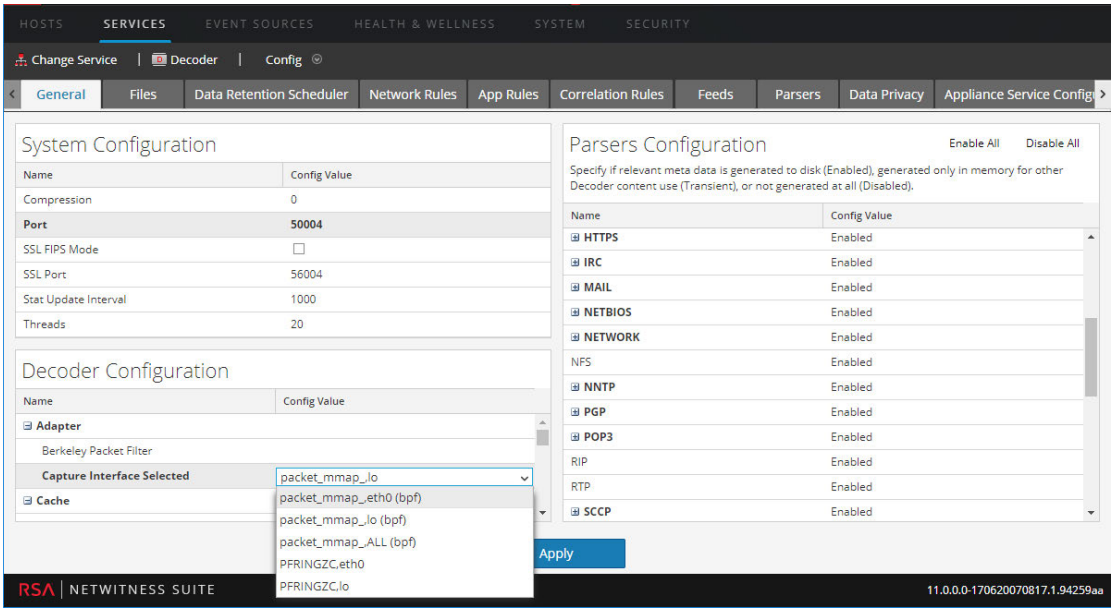
In NetWitness Suite 11.0, you can select any subset of the capture interfaces by editing the Decoder configuration node /decoder/config/capture.device.params to include an interfaces= parameter. The interfaces parameter contains a comma-separate list of interfaces that are used for capture. Instead of using all interfaces for capture, only the specified interfaces are used.

For example, if you want to force capture on interfaces em1, em2, and em4, and ignore em3, you can select the packet_mmap_,ALL adapter, and then add this line to capture.device.params: interfaces=em1,em2,em4

Note: Using the interfaces parameter to select eth0, lo, or em1 overrides the default behavior, which is to drop traffic from those ports.

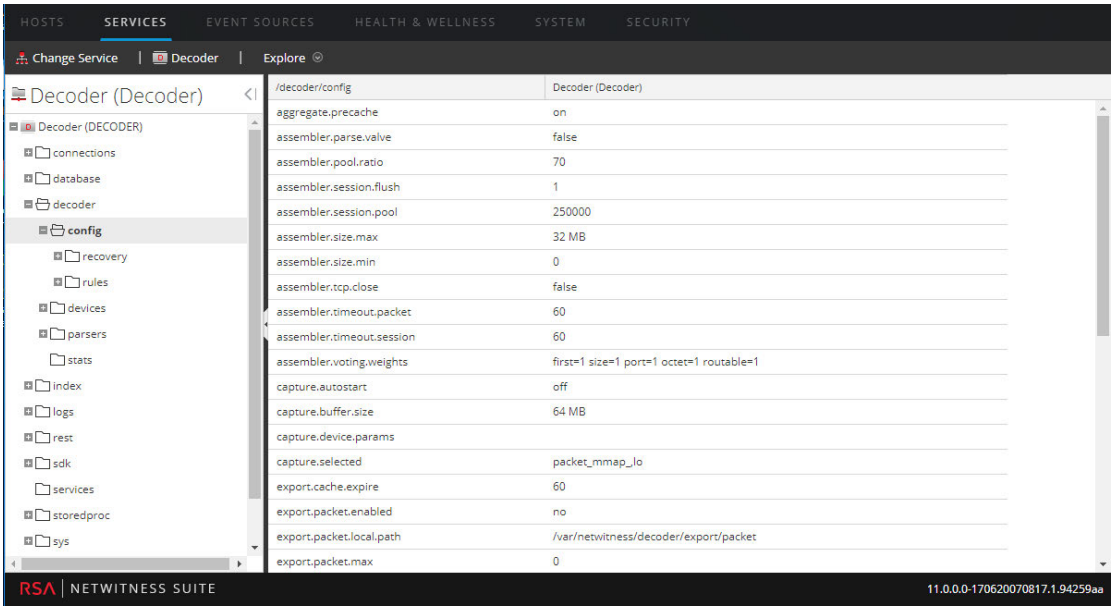
To configure the packet_mmap_,ALL adapter to capture from specific interfaces instead of all interfaces:

1. In the **Administration Services view**, select the Decoder service and > **View** > **Config.**
2. In the **Services Config view**, set **Capture Interface Selected** to packet_mmap_,ALL adapter.

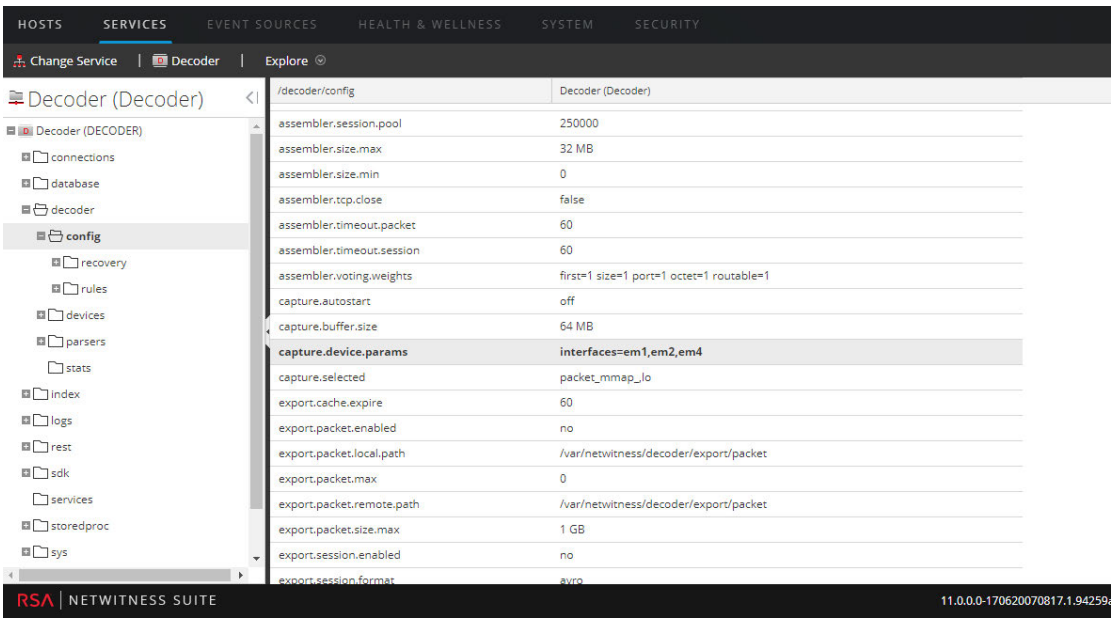


3. To go to the Services Explore view, click **Config** in the toolbar and select **Explore** in the drop-down list.

4. In the Services Explore view, select **decoder** > **config**.



5. Click in the values column next to `capture.device.params`, type `interfaces=em1,em2,em4`, and press **Enter**.



The change goes into effect immediately; only traffic on `em1`, `em2`, and `em4` interfaces is captured.

(Optional) Preserve VLAN Tags When Using the Packet MMAP Capture Interface

When capturing traffic containing VLAN tags, you may need to configure the Packet MMAP capture interface to preserve the VLAN tags in the packets (VLAN fixup). By default, the network capture hardware removes the tags. Performing this procedure preserves the tags in the packets, and the tag values are parsed into VLAN meta data for further analysis.

There are two mechanisms for enabling the VLAN fixup.

- Option 1: Set `vlan-fix=true` within `capture.device.params`. This option performs the VLAN fixup on all traffic entering the Decoder. This option is appropriate in most cases, since it is assumed that all the traffic will be VLAN tagged.This mechanism works on either single-interface mode, or on all-interfaces mode. This option overrides the VLAN fixup settings on individual interfaces; even interfaces that are not configured to do VLAN fixup will have the feature enabled.
- Option 2: Use the `interfaces` parameter within `capture.device.params` on a per-device basis. The `interfaces` parameter accepts a comma-separated list of interface names on which to capture packets. By adding `:vlan` to an interface name, you can enable the VLAN fixup on individual interfaces. If the interface does not have the `:vlan` suffix added, then it will not perform the VLAN fixup.

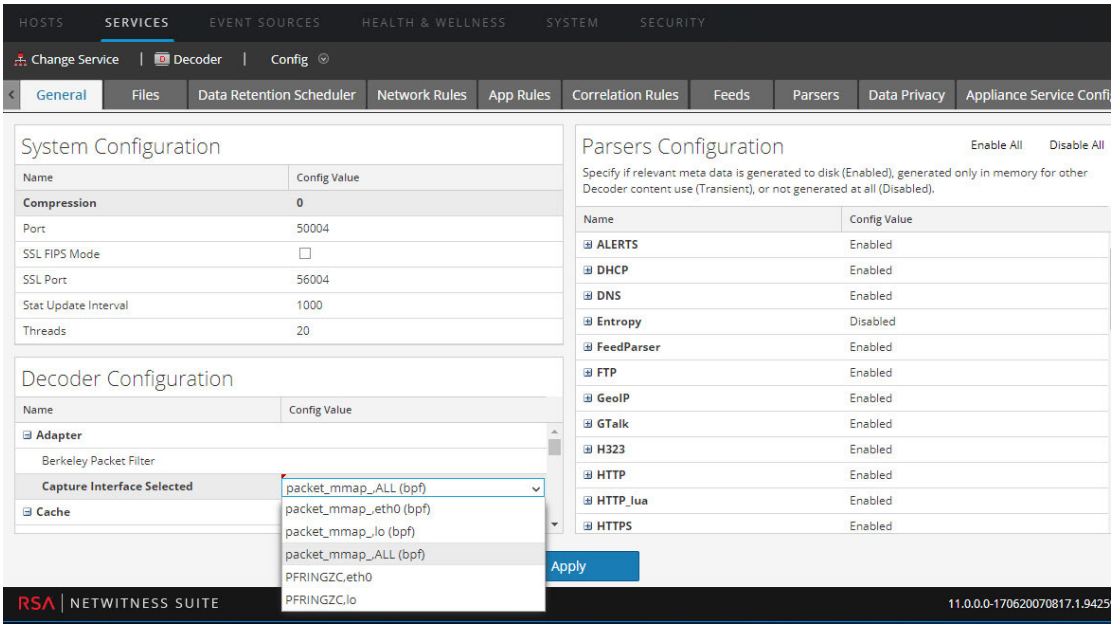
After editing this parameter, you must restart capture on the Decoder in order for changes to `capture.device.params` to take effect.

These are `vlan` examples of both options. If you need to pass multiple settings for `capture.device.params`, use the following synax. Notice that quotes are needed for values with whitespace, see *Core Database Tuning Guide*.
`name1="value1" name2="value2"`.

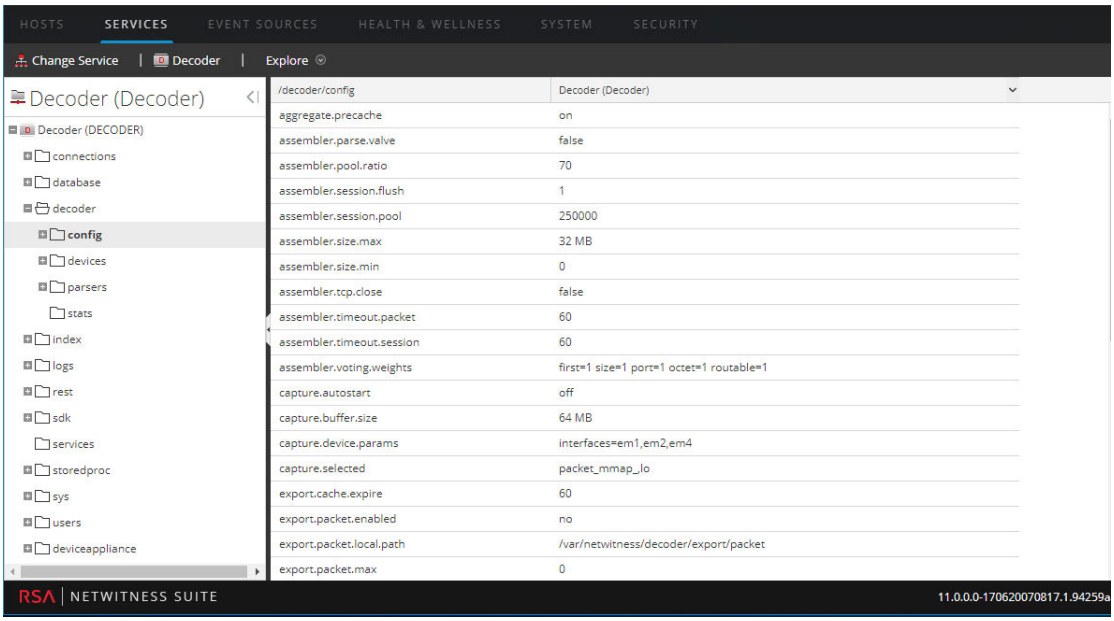
Parameter	Value	Effect
`capture.device.params`	`vlan-fix=true`	VLAN fixup always performed on all interfaces. The default value is `vlan-fix=false`.
`capture.device.params`	`interfaces=eth0:vlan,eth1`	VLAN fixup performed on traffic capture on `eth0` interface only
`capture.device.params`	`interfaces=eth0:vlan,eth1 vlan-fix=true`	VLAN fixup always performed because the `vlan-fix` setting overrides the interfaces setting.

To configure the `packet_mmap_` adapter to preserve the VLAN tags in packets:

1. In the **Administration Services view**, select the Decoder service and > **View** > **Config.**
2. In the **Services Config view**, set **Capture Interface Selected** to `packet_mmap_,ALL` adapter.

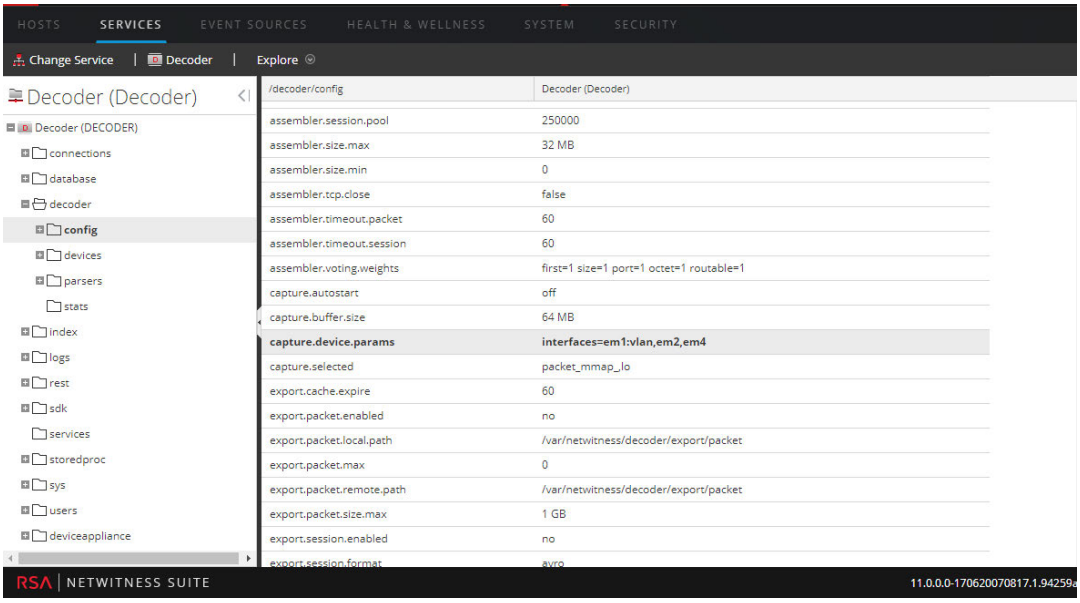


3. To go to the Services Explore view, click **Config** in the toolbar and select **Explore** in the drop-down list.
4. In the Services Explore view select **decoder** > **config**.



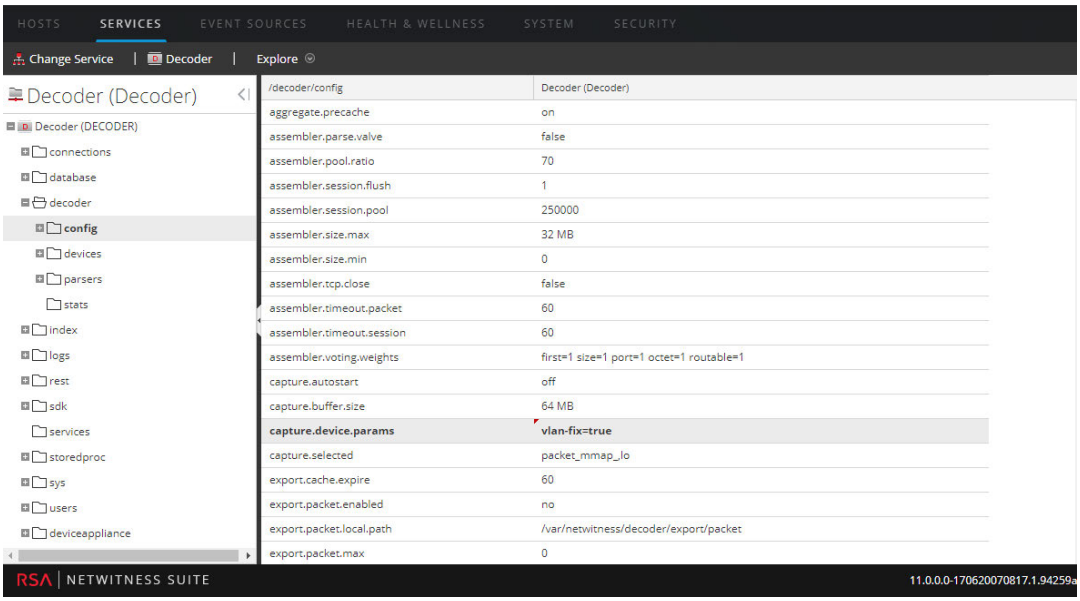
5. Click in the values column next to `capture.device.params`, and do one of the following:

   - To preserve VLAN tags on an interface in the interfaces list, add **`:vlan`** after the interface name and press **Enter**. For example, this specifies that VLAN tags are preserved on `em1`, but not on `em2` and `em4`:
     `interfaces=em1:vlan,em2,em4`



   The change goes into effect immediately; only traffic on `em1` has the VLAN tags preserved.

   - To preserve VLAN tags on all interfaces, enter the following and press **Enter**:
     `vlan-fix=true`.

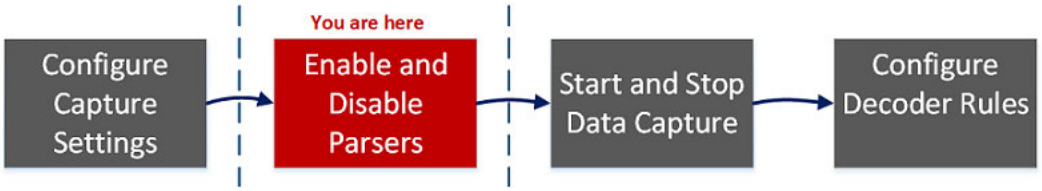


The change goes into effect immediately; VLAN tags are preserved on all capture interfaces.

Enable and Disable Parsers and Log Parsers

Administrators can see which parsers have been downloaded from Live and deployed on a Decoder or Log Decoder, see which of these have been enabled, and enable or disable parsers and log parsers.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see Decoder and Log Decoder Quick Setup.



You should only download and deploy the parsers you need for the following reasons:

- There is an impact on performance as you increase the number of deployed parsers.
- The more parsers you deploy, the more meta data created, which impacts data retention
- Not having extra (unnecessary) log parsers deployed reduces the potential for misidentification of messages.

The Parsers Configuration panel provides a way to select parsers to use on the Decoder. Within some parsers, you can also configure the metadata that the parser creates. These are the options in the Parsers Configuration panel.

Option	Description
Enable All **Disable All**	These options provide a way to quickly select either all parsers or no parsers.
Name	The names of parsers available to the Decoder. A plus sign indicates that the metadata generated by the parser is configurable. Clicking the plus sign displays the metadata that the parser can create.

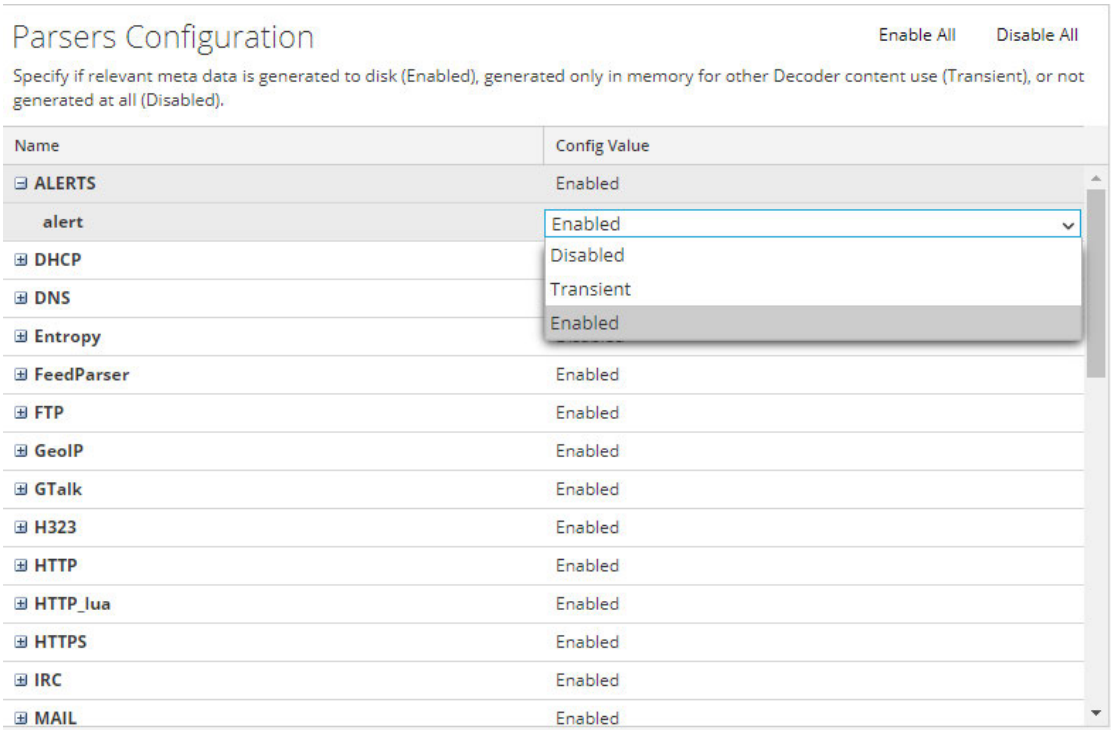
Option	Description
Config Value	A drop-down list changes the setting for the parser or metadata to **Enabled**, **Disabled**, or **Transient**. • When **Enabled**, the Decoder is using the parser to filter traffic. • When **Transient**, the Decoder is using the parser to filter traffic, and the generated metadata is not stored on disk. The transient metadata is available in memory to additional content (that is, parsers, feeds, and application rules) on that Decoder. This helps administrators to protect certain data and is usually done as part of a data privacy plan (see the *Data Privacy Management Guide*). • When **Disabled**, the Decoder is not using the parser. If the generated metadata for the parser is configurable, clicking the plus sign to expand the parser displays configurable meta keys and the same drop-down list selects the meta key the parser will create.

Note: For a Log Decoder You must have previously deployed log parsers from Live, See the **Find and Deploy Live Resources** topic in the *Live Services Management* Guide for details. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

To enable or disable an parser, or to view the status for each parser:

1. Go to **ADMIN** > **Services**.
2. In the **Administration Services view**, select a Log Decoder or a Decoder, and **>View** > **Config**.

3. In the **Parsers Configuration** panel, look for the Decoder parser or the Log Decoder event source parser.



4. In the **Config Value** column, note the current status for your parser.

   You can update the status of any individual parser by selecting its **Config Value** and selecting **Disabled**, **Transient**, or **Enabled** from the drop-down menu. Alternatively, you can select **Enable All** or **Disable All** to update the status for all of your log parsers at once.

5. Click **Apply**.

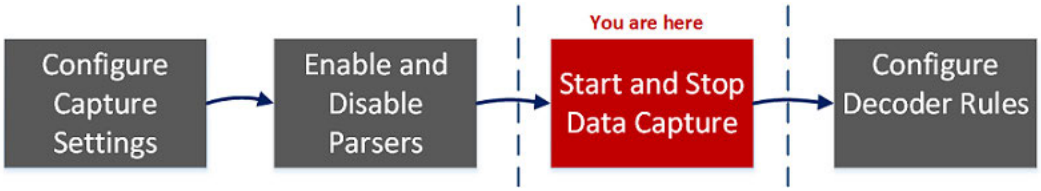
When you click **Apply**, note that all parsers are reloaded into NetWitness Suite. The status for each parser is updated, based on your selections.

Start and Stop Data Capture

When a Decoder starts up, it automatically begins aggregating data if **Capture Autostart** is enabled. When autostart is not enabled, you can start and stop data capture manually.

Note: The Capture Configuration Settings in the Service Config view for a Decoder determine whether Capture Autostart is enabled.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see Decoder and Log Decoder Quick Setup. You may want to stop and start capture at other times, for example, before you shut down the service.



To start and stop capture:

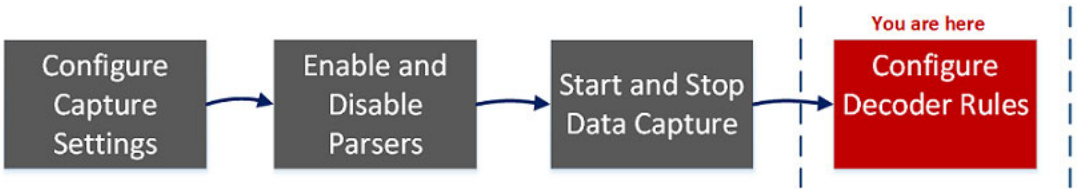
1. Go to **ADMIN > Services.**
2. In the **Admin Services** view, select a Decoder or Log Decoder service, and select > **View** > **System**.
3. In the toolbar, click **Start Capture**.
   If the service is a Decoder, it begins capturing packets. If the service is a Log Decoder, it begins capturing logs.
   When packet or log capture is in progress, the option in the toolbar changes to **Stop Capture**, and the option to upload a file is unavailable.
4. Whenever you want to discontinue traffic capture on a Decoder, click **Stop Capture**.
   Packet or log capture ceases, and the option to upload a file to the service is again available.

Note: When you stop the Log Decoder service while capture is running, all events currently in Log Decoder memory will be processed and persisted. Should an issue arise where it is necessary to quickly shutdown the service, use the Services Explore view to stop capture (**/decoder stop**), passing the parameters ***flush=false*** before stopping the Log Decoder service. For further information, see the "Services Explore View" in the *Host and Services Getting Started Guide*.

Configure Decoder Rules

This topic provides procedures for creating and managing rules for Decoder or Log Decoder traffic capture in the Services Config view > Rules tabs . Services Config View - Rules Tabs provides details about the Rules tab options.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see Decoder and Log Decoder Quick Setup.



Capture rules can add alerts or contextual information to sessions or logs. They can also define which data is filtered out by a Decoder or Log Decoder. Rules are created for specific metadata patterns, which result in predefined actions when matches are found. For example, to keep all traffic that fits certain criteria, but discard all other traffic, you can create a rule to perform the necessary actions. When applied, rules affect both packet capture file importing, as well as live network capture.

Rule and Query Guidelines provides guidelines that all queries and rule conditions in NetWitness Suite Core Services must follow.

By default, no rules are defined when you first install NetWitness Suite. Until rules are specified, the packets are not filtered. You can deploy the latest rules from Live. You can define three types of rules: Network Rules, Application Rules, and Correlation Rules.

- Network rules are applied at the packet level and are made up of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied to the Decoder. Rules can be applied to multiple layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules are only available on packet Decoders.
- Application rules are applied at the session level. If the first rule listed is not a match, the Decoder then attempts to match the next rule listed, until a match is found.
- Correlation rules are applied over a configurable sliding time window. When a match is found, the service creates a new super session that identifies other sessions that match the rule, then creates a session list for analysis.

The two most common uses of rules are:

- To alert, and thereby create a custom alert meta value, when certain conditions are found.
- To filter out certain types of traffic that do not add value to the analysis of the data.

Groups of capture rules form rule sets, which you can import and export. This feature enables use of multiple rule sets for various scenarios. You can import the exported rule set, in the form of an .nwr file, to other NetWitness Suite services, simplifying the deployment and configuration of multiple services.

Rule Processing

These are the principles governing capture rule processing:

- Multiple rules can be applied to the Decoder.
- Capture rules are executed one after the other, in sequence.
- Rule processing stops when all rules are processed or after a rule configured to stop rule processing is matched.
- A default rule can be used to either include or exclude all traffic not otherwise selected by a rule. A default rule, if used, must always be placed at the bottom of the rule list. Otherwise, rule processing stops as soon as the default rule is evaluated since, by definition, all traffic is selected by the default rule.
- When rule processing stops, the session is saved using the configured session options and debug options.

Rule and Query Guidelines

All queries and rule conditions in RSA NetWitness Core services must follow these guidelines:

All string literals and time stamps must be quoted. Do not quote numbers, MAC, or IP addresses.

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Note: The space on the right and the left of an operator is optional. For example, you can type a rule as `service=80` or `service = 80`.

Rule Examples

The following table shows examples of rule conditions. You can use rule conditions for log retention collections in an Archiver and for application, network, and correlation rules on a Decoder, Log Decoder, or Concentrator. Rule conditions are also used in all `WHERE` clauses in all Core database queries.

For detailed information on rule syntax in NetWitness Suite, see "`WHERE` Clauses" in the "Queries" section of the *Core Database Tuning Guide* .

Rule Name	Condition
ComplianceDevices	`device.group='PCI Devices' || device.group='HIPPA Devices'`
HighValueWindows	`device.group='Windows Compliance'`
MediumValueWindows	`device.type='winevent_nic' && msg.id='security_4624_security'`
LowValueWinLogs	`device.type='winevent_nic' && msg.id='security_4648_security'`
LowValueProxyLogs	`device.class='proxy' && msg.id='antivirus_license_expired'`
GeneralWindows	`device.type='winevent_nic'`

Invalid Rules

NetWitness Suite uses a rule parser that strictly defines valid syntax for rules and queries. When a Core service encounters invalid syntax, it writes a warning in the NetWitness Suite logs indicating the error.

Note: NetWitness Suite 11.0 does not support parsing of legacy syntax rules (as NetWitness Suite 10.6 did). After you update to NetWitness Suite 11.0, rules with invalid syntax are highlighted in the user interface, and no rules will be applied until the invalid rules are corrected. The Rule Editor provides additional tooltips. After you fix the rules, the highlights disappear. See Fix Rules with Invalid Syntax.

The `/decoder/config/rules/rule.errors` and `/concentrator/config/rules/rule.errors` stats, contain the count of rules with errors. If `rule.errors` is nonzero, NetWitness Suite generates a Health and Wellness alert to indicate that you need to fix the rules.

General Syntax Guidelines

- All text values must quote literal values. Example: `username = 'user1'`
- Quotes can use single or double quotes; but they must match. (You cannot start with a single quote and finish with a double quote.)
- If the literal value has a quote, you can escape it (using a backslash) or use a different starting quote character. Both of the following examples are valid: `username = "User's"`, `username = 'User\'s'`

The following are valid syntax rules:

- To use a backslash in a literal string, escape it using an extra backslash: `\`
- All time values should use quotes for dates in this form:
  `time = 'YYYY-MM-DD HH:MM:SS'`
- All time values that are the number of seconds since EPOCH (Jan 1, 1970), should not be quoted.
  Example: `time = 1448034064`
- **Everything** else is unquoted: IP addresses, MAC addresses, numerics, and so on. Example:
  `service = 80 && ip.src = 192.168.1.1/16`

Capture Rule Syntax

Capture rules compare fields to values or to other fields. This is an example of a simple expression with a meta key on the left side of the operator and a value on the right side.

```
ip.dst=192.168.1.1
```

The syntax allows a meta key on the right side of the operator in Decoders and Log Decoders for application and network rules. Meta key comparison does not apply in the `where` clause in queries. This is an example of a simple expression with a meta key on the left side of the operator and a meta key on the right side.

```
ip.src=ip.dst
```

Rules that include a meta key comparison support renamed meta keys; if a rule queries a meta key that has been renamed, the rule is parsed for the renamed meta key. For example, if the meta key `ip_dst` is used in a rule, it is transparently mapped to the renamed meta key: `ip.dst`. Existing rules that include original keys will trigger alerts that include data for the renamed meta key.

This is an example of a rule that finds packets having the same `ip.src` address and `ip.dst` address on a Decoder, and generates an alert on the Concentrator.

```
alert=alert.id name=testRule8 rule="ip.src=ip.dst" order=38
```

This rule would generate an error because `eth.src` and `ip.src` are incompatible formats.

```
rule="eth.src=ip.src" name="testRule99" alert=alert.id
```

Values can be expressed as discrete values, a range of values, an upper or lower bound, or a combination of these three. You can create a greater than or less than comparison, and test equality or inequality against a range of values or an upper/lower bound.

`key 0-5` (a range of values)

`key = 0-u` is the same as `key >= 0` (upper bound, greater than or equal to)

The following table summarizes the operators on meta keys.

Left Operand Format	Operator	Right Operand Format	Description
any	=	compatible with left operand	Equality operator. You can use values or meta keys on the right side of the equality operator.
any	!=	compatible with left operand	Inequality operator. You can use values or meta keys on the right side of the inequality operator.
any	<	compatible with left operand	Less than operator. You can use values or meta keys on the right side of this operator.
any	<=	compatible with left operand	Less than or equal to operator. You can use values or meta keys on the right side of this operator.
any	>	compatible with left operand	Greater than operator. You can use values or meta keys on the right side of this operator.

Left Operand Format	Operator	Right Operand Format	Description
any	>=	compatible with left operand	Greater than or equal to operator. You can use values or meta keys on the right side of this operator.
text	contains	text	Find values that contain the right operand. You can use meta keys or values on the right side of this operator.
text	begins	text	Find values that begin with the right operand. You can use meta keys or values on the right side of this operator.
text	ends	text	Find values that end with the right operand. You can use meta keys or values on the right side of this operator.
text	length	integer	Find strings of a certain length. You can use meta keys or values on the right side of this operator.
any	count	integer	Find values with a specific number of occurrences within the session. You can use meta keys or values on the right side of this operator.
any	ucount and unique	integer	Finds a number of uniquely occurring values. You can use meta keys or values on the right side of this operator. For example, if the results include instances of a meta key with 5 unique values and 3 of the same value, the ucount is 6.
N/A	exists	any	Finds any values for the meta key. You can use meta keys or values on the right side of this operator.
N/A	!exists	any	Finds any sessions in which the meta key does not occur. You can use meta keys or values on the right side of this operator.

Left Operand Format	Operator	Right Operand Format	Description
text	`regex`	text	Finds values matching a regular expression. You can use values on the right side of this operator.

The following table summarizes other syntax elements used in rules.

Syntax element	Description
*	Default rule. By using an asterisk (*) as the sole character in a rule, that rule will select all traffic.
`u`	Upper bound of a range a range of times, IP addresses, or numeric formats. For example, to select all TCP ports above 40000, the syntax would be: `tcp.port = 40000-u`
`l`	Lower bound of a range of times, IP addresses, or numeric values. For example, to select all TCP ports below 40000, the syntax would be: `tcp.port = l-40000`
- (dash)	Denotes a range. This is only applicable to time values, IP or MAC addresses, or numeric values. Separate the lower and upper bounds of the range with a dash (-) character. For example, to select TCP ports between 25 and 443, the syntax would be: `tcp.port = 25-443`
, (comma)	Denotes a list of ranges or values or meta keys. Single values may be used as well as any combination of ranges and upper or lower bounds. Single meta keys may be used in a list. Meta keys and literal values cannot both appear on the right-hand side of an operator. For example, the following is valid syntax: `tcp.port = 1-10,25,110,143-225,40000-u`

Syntax element	Description
`( )`	Grouping operator. An expression can be enclosed in parentheses to create a new logical expression. For example, the following would select traffic on port 80 to/from 192.168.1.1 OR traffic on port 443 to/from 10.10.10.1: `(ip.addr=192.168.1.1 && tcp.port=80) || (ip.addr=10.10.10.1 && tcp.port=443)`
`~`	Logical NOT operator, a negation of an expression.
`&&`	Logical AND operator, a conjunction of two expressions.
`||`	Logical OR operator, a disjunction of two expressions.

Configure Capture Rules

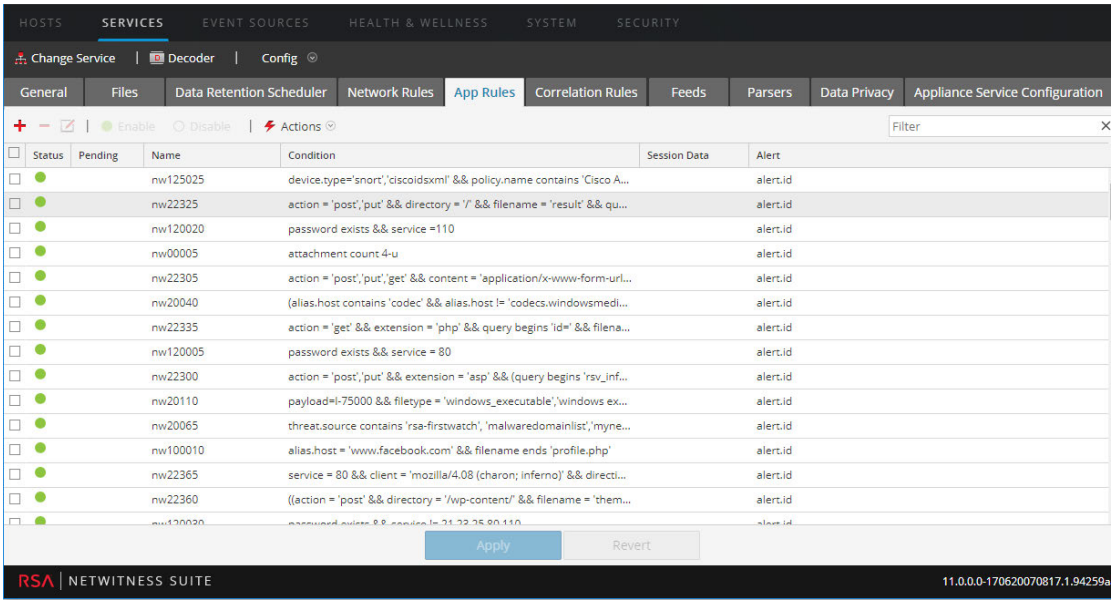
The Decoder and Log Decoder rules are editable in the Services Config view. While each type of rule (network, application, and correlation) has its own tab; the functions are similar for all types of rules. You can:

- Add, edit, and delete rules
- Enable and disable rules
- Change the execution sequence of rules
- Import rules from a file
- Export rules to a file
- Push rules to another service
- Revert or apply rule changes
- Restore one of the last ten rule configurations from a snapshot

To configure rules in the Rules tabs

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Decoder service and **> View > Config**.
3. In the **Services Config** view, select one of the Rules tabs: Network Rules, App Rules, or Correlation Rules.

The rules list for the selected rule type is displayed.



Each type of rule has a list with slightly different columns and different parameters. Several basic guidelines apply to all rule management activities:

- The rules are executed in the sequence they are displayed in the list. To change the execution sequence of rules, drag and drop rules to the appropriate location in the list or use the context menu options to arrange the rules in the list.
- To select a single row, click the row.
- To select a group of adjacent rows, click the first, then shift-click the row at the end of the group.
- To select multiple non-adjacent rows, click the first, then control-click the others.
- When editing rules in the Rules tab, you must apply the configuration changes in order to activate.
- Until changes are applied, you can discard edits to the list and revert to the unedited rules.
- Once rules are applied, you can recover the last ten rules configurations using the **History** option in the **Actions** menu.

To add a rule in any Rules tab, do one of the following:

- Click **+**.
- Right-click a rule, and select **Insert Above** or **Insert Below** from the context menu. The Rule Editor dialog for that type of rule is displayed.

To remove a rule:

1. From any Rules tab, select the rules to remove from the rules list.
2. Click −.

   The selected rules are removed from the list, but still exist on the service.

To edit a rule

1. From any Rules tab, select the rule to edit.
2. Click or double-click the rule row.

   The Rule Editor dialog for that type of rule is displayed.

To disable a rule:

1. From any Rules tab, select the rules to disable.
2. Click Disable.

   The status changes to disabled in the rules list, but the rule is still enabled on the service.

To enable a rule:

1. From any Rules tab, select the rules to enable.
2. Click Enable.

   The status changes to enabled in the rules list, but the rule is still disabled on the service.

Import Rules from a File and Export Rules

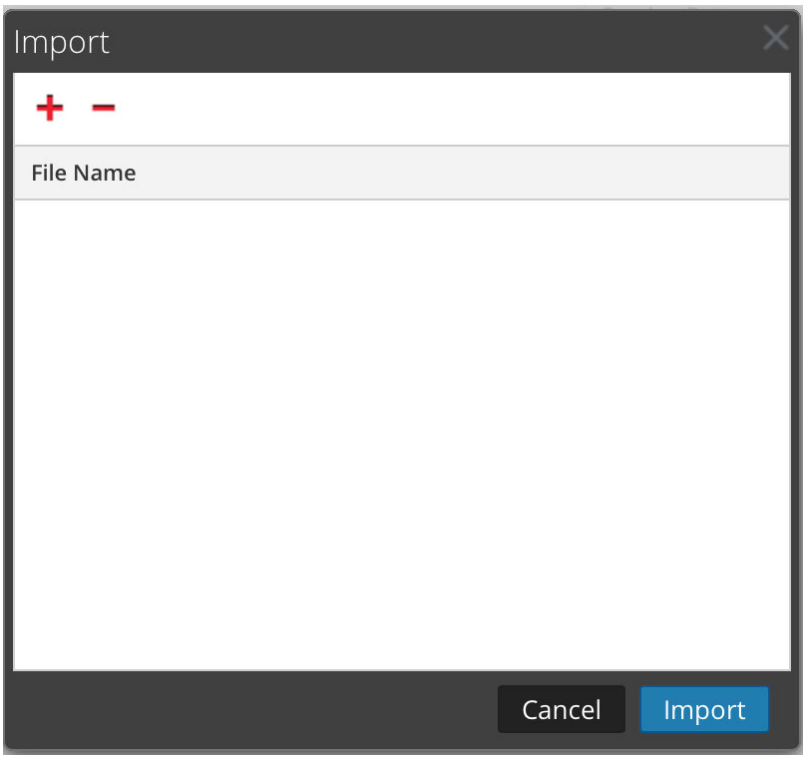
You can import network, application, and correlation rules to a Decoder from a file that contains rules of the same type. After the rules are imported, you can edit and manage them as you would any other rules.

When you attempt to import a group of rules, NetWitness Suite Administration checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, the rules are not imported. You must re-import the rules under the correct tab or select another file to import.

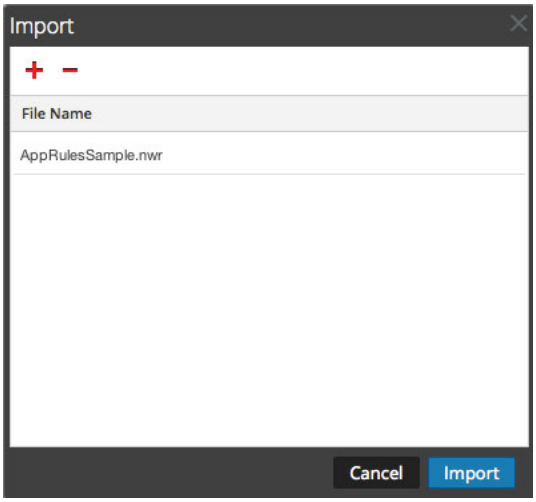
To import rules to a service:

1. From any Rules tab, select Actions > Import.

   The Import dialog is displayed.



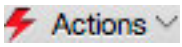
2. Click +.
   A view of the directory structure is displayed.
3. Choose one or more NetWitness rules (.nwr) files to import, and click **Open**.
   The file is added to the list in the Import dialog.



4. Click **Import**.
   The rules are imported into the user interface. Imported rules have a red corner in each edited column.
5. Edit or reorder the rules if needed.

6. To save the rules to the service, click **Apply**.
   The rules for the service are updated with the changes.

To export a rule to a file:

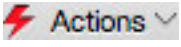
1. To export a subset of the rules, select the rules to be exported.
2. Do one of the following:
   - In the toolbar, select 

 > Export > Selection. (**Export > All** exports all rules in the rules listeven if you have a subset selected for export.)
   - Right-click the selected rules and select **Export Selection**.
     A prompt for the filename is displayed.
3. Enter the filename and click **Export**.
   The .**nwr** file is downloaded.

Push Rules to Other Services

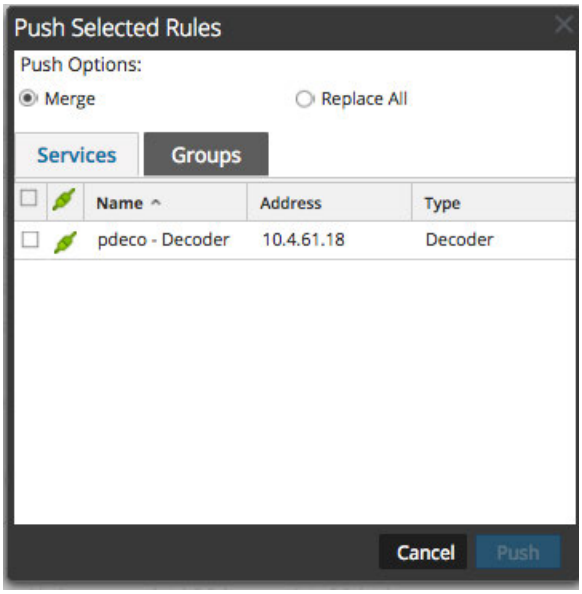
You can apply (push) rules or selected rules to other services (Decoders or Log Decoders) or service groups. When you push all rules to other services, all rules on the target services are removed and replaced with all of the rules on the source service.

To push selected rules from this Decoder to other Decoders:

1. From any Rules tab, select the rules that you want to push to another Decoder.
2. Do one of the following:
   - Select 

 > Push > Selection.

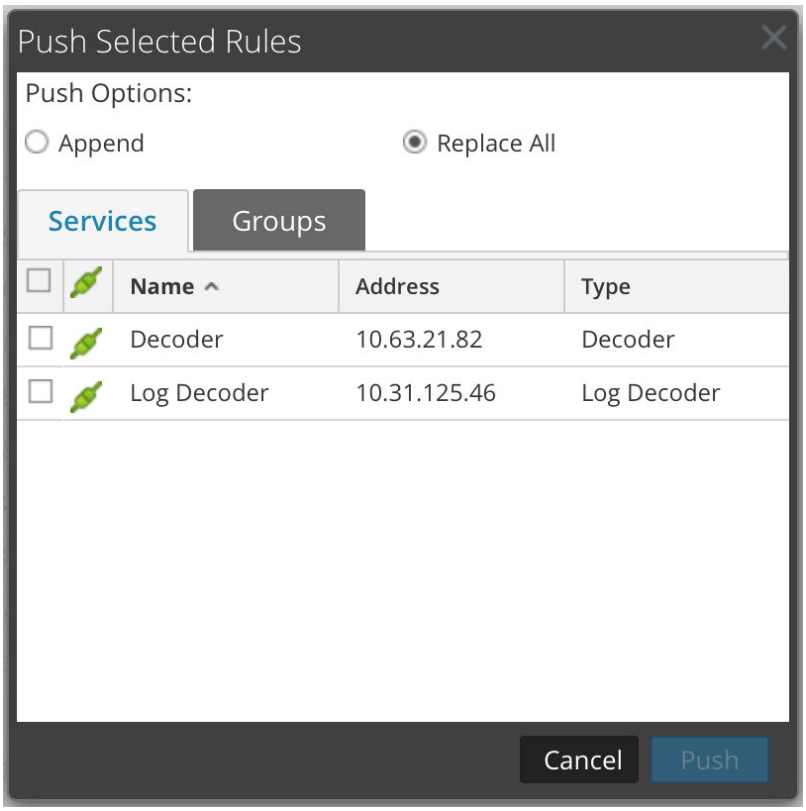
- Right-click the selected rules and select **Push Selected Rules**.
  The Push Selected Rules dialog is displayed.



3. Select a Push Option:
   - Select **Replace All** to delete all rules on the target services and replace them with the selected rules. This is the default selection.
   - Select **Merge** to merge the selected rules with the existing rules on the target services.
4. On the **Services** tab, select the target services to receive the pushed rules, or select the groups of services from the **Groups** tab.
5. Click **Push**.
   The rules are pushed to the selected services and become effective immediately.

To push all rules from this Decoder to other Decoders:

1. From any Rules tab, select Actions > **Push** > **All**.
   (**Push** > **All** pushes all rules in the rules list even if you have a subset selected to push.) The Push Selected Rules dialog is displayed.



2. On the **Services** tab, select the target services to receive the pushed rules, or select the groups of services from the **Groups** tab.
3. Click **Push**.
   All rules from the target services are deleted and replaced with all of the rules from source service. The rules become effective immediately.

Change Execution Order of Rules

Capture rules are applied in the order they are displayed in the rules list. To reorder rules, use either of these methods:

- Drag and drop the rules in the appropriate location in the rules list.
- Right-click a rule to display the context menu, and use the **Cut** and **Paste** options.

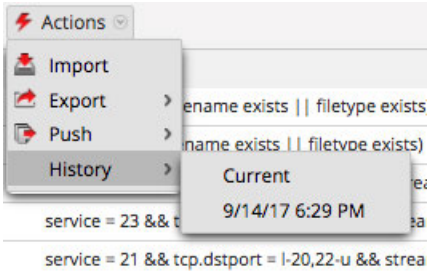
Restore a Rule Snapshot from History

NetWitness Suite keeps the last ten snapshots of rules applied to a service.

To restore a rules snapshot from history:

1. Select Actions > **History**.

   A submenu of snapshots is displayed.



2. Select the snapshot time from the submenu.

   The rules from the snapshot are loaded into the rules list, replacing the current set. But the current set is still in use on the service.

3. To apply the rules to the service, click **Apply**.

   The rules are applied to the service.

Configure Application Rules

Application layer rules are applied at the session level. The following are sample application rules.

To truncate packets carried via Server Message Block protocol (SMB), create a rule as follows:

- Rule Name: Truncate SMB
- Condition: `service=139`
- Rule Action: Truncate All

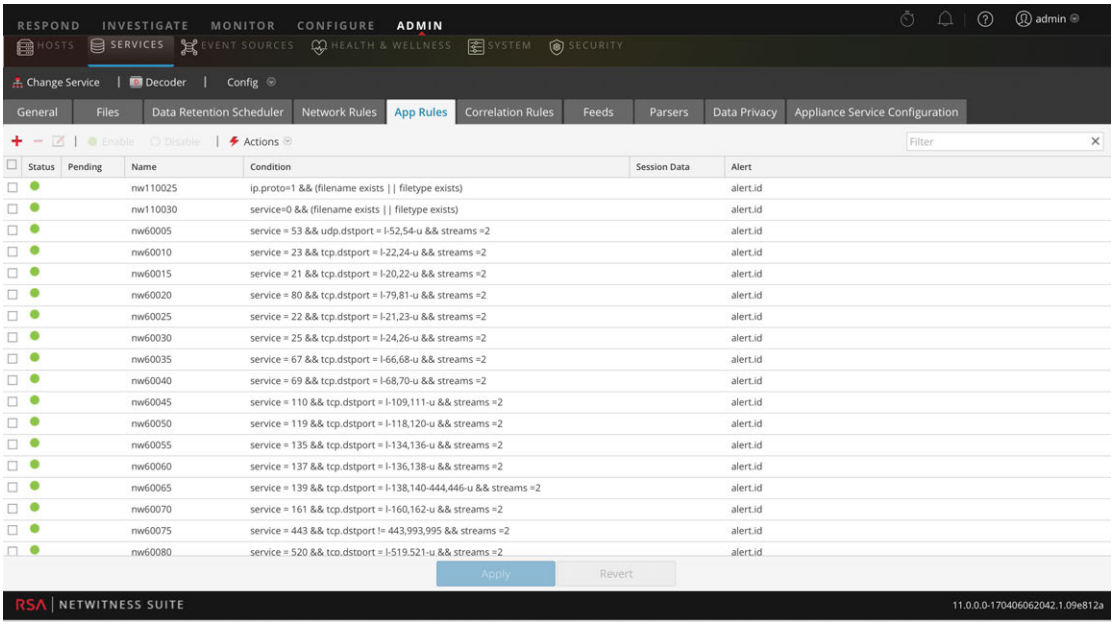
To retain email to and from a specific e-mail address, create a rule as follows:

- Rule Name: Email Filter Tom Jones
- Condition: `email='Tom.Jones@TheShop.com'`
- Rule Action: Filter

To add or edit an application rule:

1. Go to **ADMIN > Services.**
2. Select a Decoder or Log Decoder service and > **View** > **Config**.

   The Systems Config view for the selected service is displayed.
3. Select the **App Rules** tab.



4. Do one of the following:

   If adding a new rule, click + .

   If editing a rule, select the rule from the rules list and click .
5. The Rule Editor Dialog is displayed with application rule parameters.

   (add a capture with example data)

   a. In the **Rule Name** field, type a name for the rule. For example, for a rule that truncates all SMB, type **Truncate SMB**.
   b. In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, NetWitness Suite displays syntax errors and warnings. For example, to truncate all SMB, type **service=139**.

      All string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details.
   c. If you want rule evaluation to end with this rule, check the **Stop Rule Processing** checkbox.
   d. In the **Session Data** section, choose one of the following actions to apply when a matching packet is found:

      Keep: The packet payload and associated meta are saved when they match the rule.

Filter: The packet is not saved when it matches the rule.

Truncate: Select a truncate option to execute when a packet matches the rule. The example uses the **All** option.

-**Truncate All** to save the packet headers and associated metadata, and do not save the packet payload.

-**Truncate After First <n> Bytes** to save the packet headers and associated metadata, and do not save the packet payload after the specified first <n> bytes, where <n> is a number of bytes.

-**Truncate SSL/TLS Handshake** to truncates the payload for all sessions except in the case of an SSL/TLS session, where the SSL exchange is preserved, but the rest of the payload is not saved. This option is for use with SSL parsers.

e. In the **Session Options** section, do any of the following:

- **To generate a custom alert** when a session metadata matches the rule, enable the Alert flag and select the name of the alert meta from the **Alert On** drop-down list.
- **To perform syslog forwarding** when the log matches the rule, enable the **Forward** flag. Make sure that:
  - You have enabled both the Alert and Forward flags to carry out syslog forwarding.
  - The name of the rule mentioned in the Rule Editor dialog matches the syslog forwarding destination name specified in the Log Decoder > View > Explore > `/decoder/config/logs.forwarding.destination` parameter
- **To prevent the alert metadata that is created from being written to the disk**, enable the **Transient** flag.

6. To save the rule and add it to the grid, click **OK**.
   The rule is added at the end of the grid or inserted where you specified in the context menu. The plus sign is displayed in the **Pending** column.
7. Check that the rule is in the correct execution sequence with other rules in the grid. If necessary, move the rule.
8. To apply the updated rule set to the Decoder or Log Decoder, click **Apply**.
   NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder and removes the pending indicator from the rules that were pending.

Monitor Application Rules

The Decoder and Log Decoder keep track of how many times each application rule matches a session. These stats can be viewed by connecting to the Decoder or Log Decoder Explore view and viewing the properties on the `/decoder/config/rules/application` folder. Then, send the command "`statdump`" to that folder. The output of this message is a listing of the number of times each application rule is hit. The listing is ordered in the same order as the contents of the rule definitions in the `/decoder/config/rules/application` folder. For example, on a system with three application rules:

```
0001: hits=6543 loaded=true
0002: hits=9294 loaded=true
0003: hits=43 loaded=true
```

The hit counters for the application rules are reset whenever the parsers are reloaded.

Configure Correlation Rules

Basic Correlation Rules are applied at the session level and alert the user to specific activities that may be occurring in their environment. NetWitness Suite applies correlation rules over a configurable sliding time window. When the conditions are met, alert metadata is created for this activity and there is a visible indicator of the suspicious activity.

The following are sample correlation rules illustrating two use cases and the syntax.

Objective: In sessions where tcp.dstport exists, if there is any combination of ip.src and ip.dst where the count of unique instances of tcp.dstport > 5 within 1 minute, then alert. To achieve this objective, create a rule as follows:

- Rule Name: IPv6 Vertical TCP Port Scan 5
- Rule: `tcp.dstport exists`
- Instance Key: `ip.src,ip.dst`
- Threshold: `u_count(tcp.dstport)>5`
- Time Window: 1 min

Objective: In sessions where `action==login` and `error==fail`, if there is any combination of `ip.src` and `ip.dst` that appears in more than 10 sessions within 5 minutes, then alert. To achieve this objective, create a rule as follows:

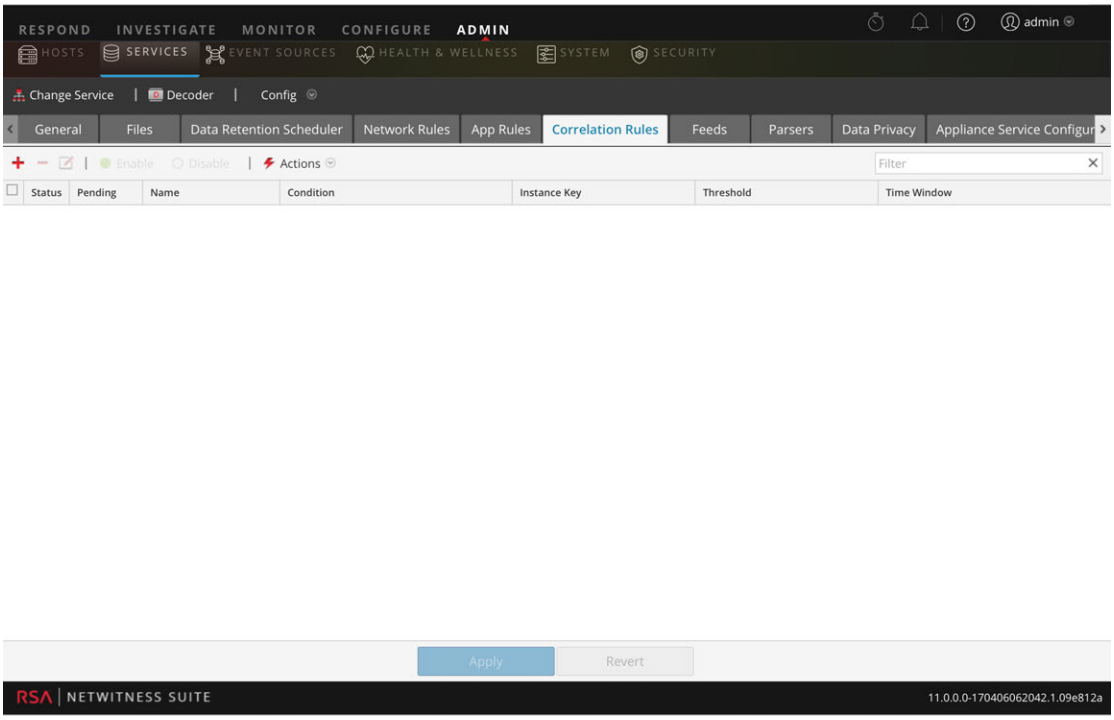
- Rule Name: IPv4 Potential Brute Force 10
- Rule: action=`'login' && error='fail'`
- Instance Key: `ip.src,ip.dst`
- Threshold: `count()>10`
- Time window: 5 mins

Both sample rules have the same instance key: `ip.src` and `ip.dst`. Because we are looking for unique combinations of `ip.src` and `ip.dst` that match the correlation condition, **`ip.src`** and **`ip.dst`** are **primary keys**.
Threshold can include an **associated key** that identifies the meta type that we are counting to determine if the condition is satisfied. In the first example, the associated key specified in Threshold is `tcp.dstport`. We are counting unique instances of `tcp.dstport` for every `ip.src/ip.dst` pair. In the second example, the associated key is not specified in the Threshold because it is merely a count of sessions. It is helpful to think of this scenario as counting unique session IDs and the associated meta is implicitly session.id. We are counting unique `session.id` for every `ip.src/ip.dst` pair.

Invalid use case: In sessions where (rule), if there is any combination of `ip.src` and `ip.dst` that have a unique count of `ipv6.dst > 5` within (time window), then alert. This case does not work because the associated key `ipv6.dst` is an IPv6 meta type. IPv4 and IPv6 meta types are not permitted to be used as associated keys.

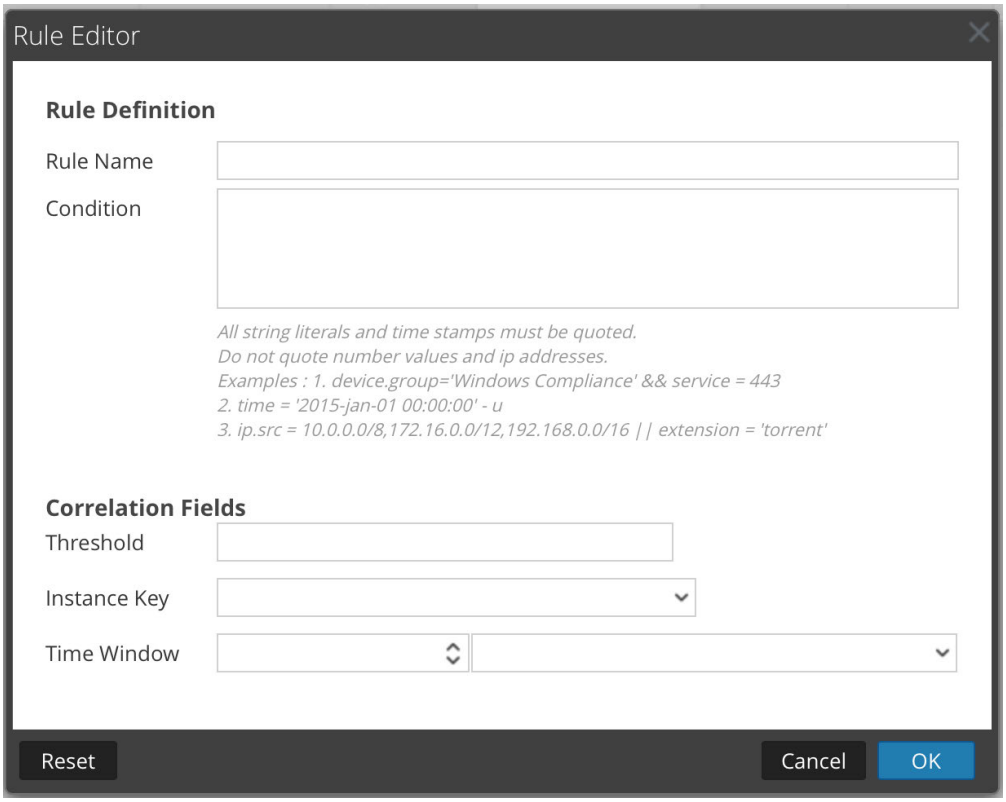
To add or edit a correlation rule

1. Go to **ADMIN > Services,** select a service, and **> View > Config**.
   The Service Config view for the selected service is displayed.
2. Select the **Correlation Rules** tab.



3. In the **Correlation Rules** tab, do one of the following:
   - If adding a new rule, click .

- If editing a rule, select the rule from the rules grid and click .
  The Rule Editor dialog is displayed with correlation rule parameters.



4. In the **Rule Name** field, type a name for the rule. For example, to create the sample rule, **IPv6 Vertical TCP Port Scan 5**.
5. In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, syntax errors and warnings are displayed by NetWitness Suite. For example, to create the sample rule, type **tcp.dstport exists**. When this condition is matched, the session data action is performed.
   All string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details.
6. In the **Threshold** field, use one of the threshold parameters to specify the minimum number of occurrences required to create a correlation session and an associated key if required. The associated key cannot be an IPv4 or IPv6 meta type.
   - u_count(associated_key) = the count of unique values of the specified key
   - sum(associated_key) = the values of the specified key
   - count = number of sessions (no associated key is specified)

7. In the **Instance Key** field, select the target indicator to base the event upon. This can be a single key or a compound key (two primary keys, separated by a comma).
8. In the **Time Window**, set the duration during which the threshold must be reached to create a correlation session.
9. To save the rule and add it to the grid, click **OK**.
   The rule is added at the end of the grid or inserted where you specified in the context menu. The plus sign is displayed in the **Pending** column.
10. Check that the rule is in the correct execution sequence with other rules in the grid. If necessary, move the rule.
11. To apply the updated rule set to the service, click **Apply**.
    NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder or Log Decoder.

Configure Network Rules

Network rules are applied at the packet level on a Decoder and are made up of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied at the packet level to a Decoder. Network rules can apply to multiple network layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules do not apply to Log Decoders, they apply only to packet Decoders.

You can create and manage network rules in the Services Config view > Network Rules tab.

Supported Meta Keys in Network Rule Conditions

The following table describes the meta keys that NetWitness Suite supports for use in network rule conditions.

Meta Key	Description
eth.addr	Ethernet source or destination address. Commonly known as the MAC address.
eth.dst	Destination Ethernet address. This is the same as the Ethernet address field except that it selects only packets where the destination address matches the selected value(s).
eth.src	Same as Ethernet destination except that it focuses on the source address.
eth.type	Ethernet frame type.
hdlc.type	Frame type of the HDLC frame.
ip.addr	IPv4 source or destination address in standard form. IP addresses can be entered in CIDR notation for subnets.
ip.dst	Destination IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets.
ip.proto	IPv4 protocol field.
ip.src	Source IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets.

Meta Key	Description
ipv6.addr	IPv6 source or destination address in hex format. Generally IPv6 addresses are written as eight groups of four hex digits, thus expressing the entire 128 bit address length. Supports notation to represent multiple blocks of 0000 in an address. Does not support CIDR notation.
ipv6.dst	Destination IPv6 address in hex format.
ipv6.proto	IPv6 protocol field. This maps to the Next Header field in the IPv6 header and uses the same values as the IPv4 protocol field.
ipv6.src	Source IPv6 address in hex format.
tcp.dstport	Destination TCP port.
tcp.port	TCP source or destination port.
tcp.srcport	Source TCP port.
udp.dstport	Destination UDP port.
udp.port	UDP source or destination port.
udp.srcport	Source UDP port.

The following are sample network rules.

To truncate all SSL from the source port, create a rule as follows:

- Rule Name: Truncate SSL
- Condition: `tcp.srcport=443`
- Rule Action: Truncate

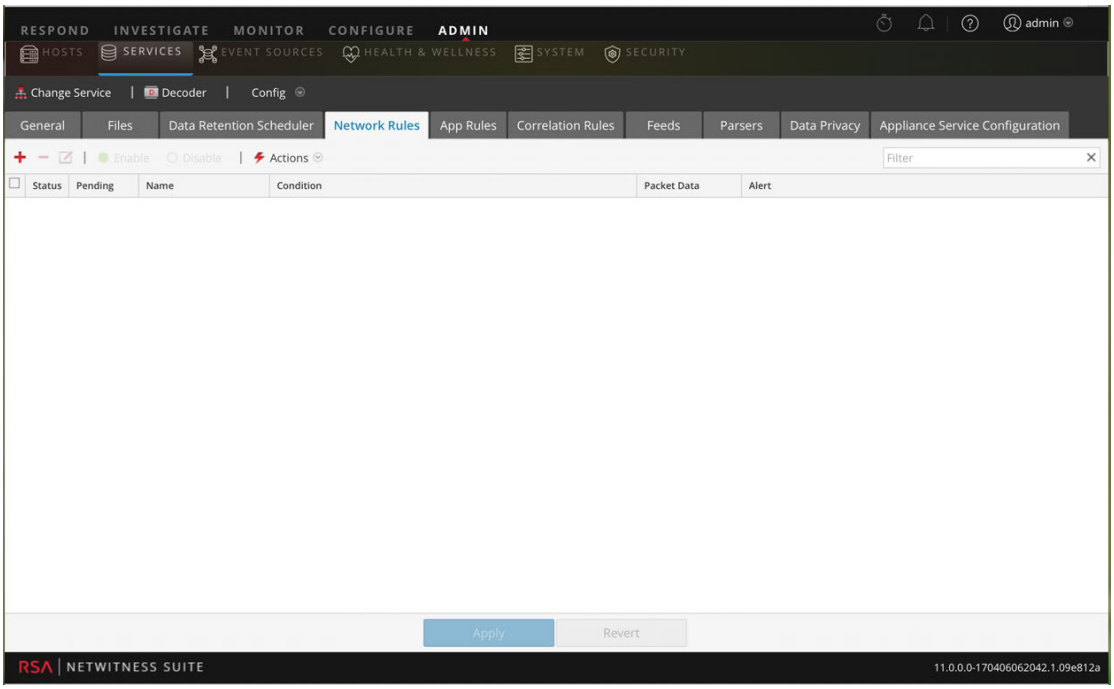
To filter subnet traffic, create a rule as follows:

- Rule Name: Subnet Filter
- Condition: `ip.addr=192.168.2.0/24`
- Rule Action: Filter

Meta entities, which provide a way to work with several meta keys at the same time, can be used in application rules, but are not supported in network rules as the metadata available are too limited. For more information on meta entities, see the *Core Database Tuning Guide*.

To add or edit a network rule:

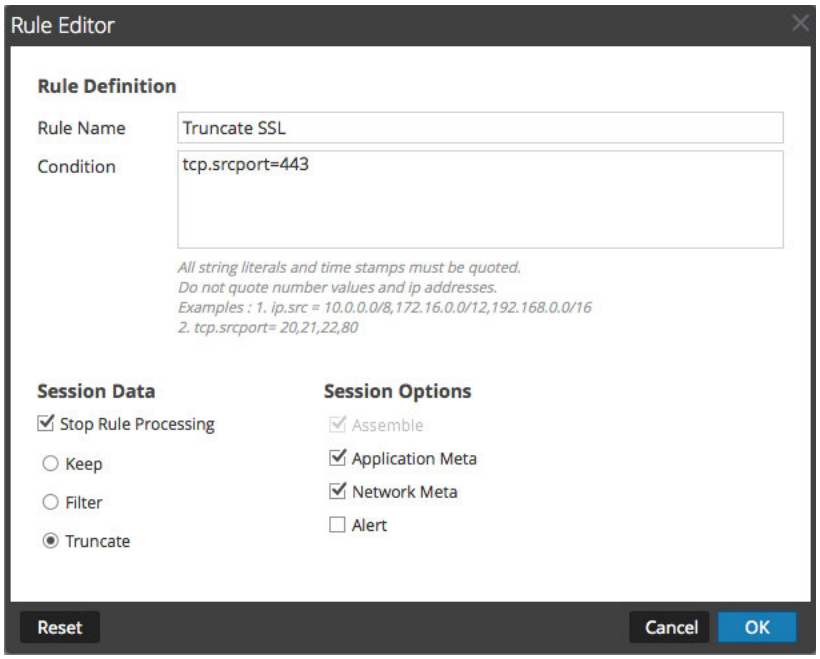
1. Go to **ADMIN > Services,** select a Decoder service, and > **View** > **Config**.
   The Services Config view for the selected service is displayed.
2. Select the **Network Rules tab**.
   The Network Rules tab is displayed.



3. In the **Network Rules** tab, do one of the following:
   - If adding a new rule, click .

- If editing a rule, select the rule from the rules list and click .

  The Rule Editor dialog is displayed.



4. In the **Rule Name** field, provide a name for the rule. For example, for a rule that truncates all SSL from the source port, type **SSL Truncate**.
5. In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, NetWitness Suite displays syntax errors and warnings. For example, to truncate all SSL from the source port, `tcp.srcport=443`.
   All string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details. Supported Meta Keys in Network Rule Conditions describes the meta keys that NetWitness Suite supports for use in network rule conditions.
6. If you want rule evaluation to end with this rule, select the **Stop Rule Processing** checkbox.
7. In the **Session Data** section, choose one of the following actions to apply when a matching packet is found:
   - **Keep**: The packet payload and associated meta are saved when they match the rule.
   - **Filter**: The packet is not saved when it matches the rule.
   - **Truncate**: The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.
8. In the **Session Options** section, select all options that apply of these four.

- **Assemble**: The assembler assembles the packet chain when it matches the rule.
- **Network Meta:** The packet generates network metadata when it matches the rule.
- **Application Meta**: The packet generates application metadata when it matches the rule.
- **Alert**: The packet generates a custom alert when metadata matches the rule.

9. To save the rule and add it to the rules list, click **OK**.
   The rule is added at the end of the list or inserted where you specified in the context menu.
10. Check that the rule is in the correct execution sequence with other rules in the list. If necessary, move the rule.
11. To apply the updated rule set to the Decoder, click **Apply**.
    NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder and removes the pending indicator from the rules that were pending.

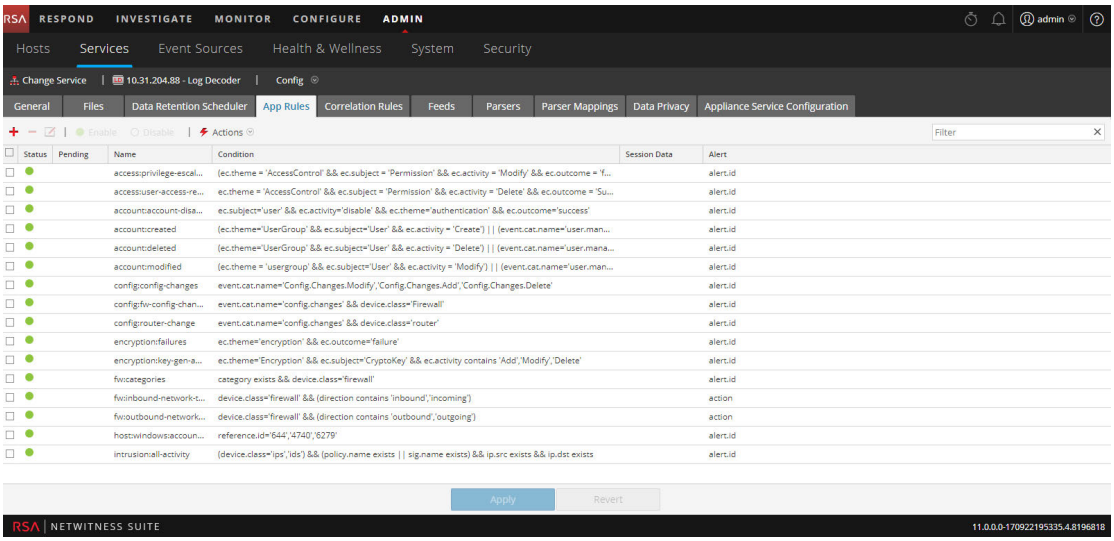
Fix Rules with Invalid Syntax

After an update to NetWitness Suite 11.0, the user interface highlights any rules with invalid syntax. The Rule Editor provides additional tooltips. After you fix the rules, the highlights disappear. Configure Decoder Rules provides guidelines that all queries and rule conditions in NetWitness Suite must follow.

To correct rules with invalid syntax:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Decoder and > **View** > **Config**.
3. In the **Services Config** view, select one of the Rules tabs: Network Rules, App Rules, or Correlation Rules.

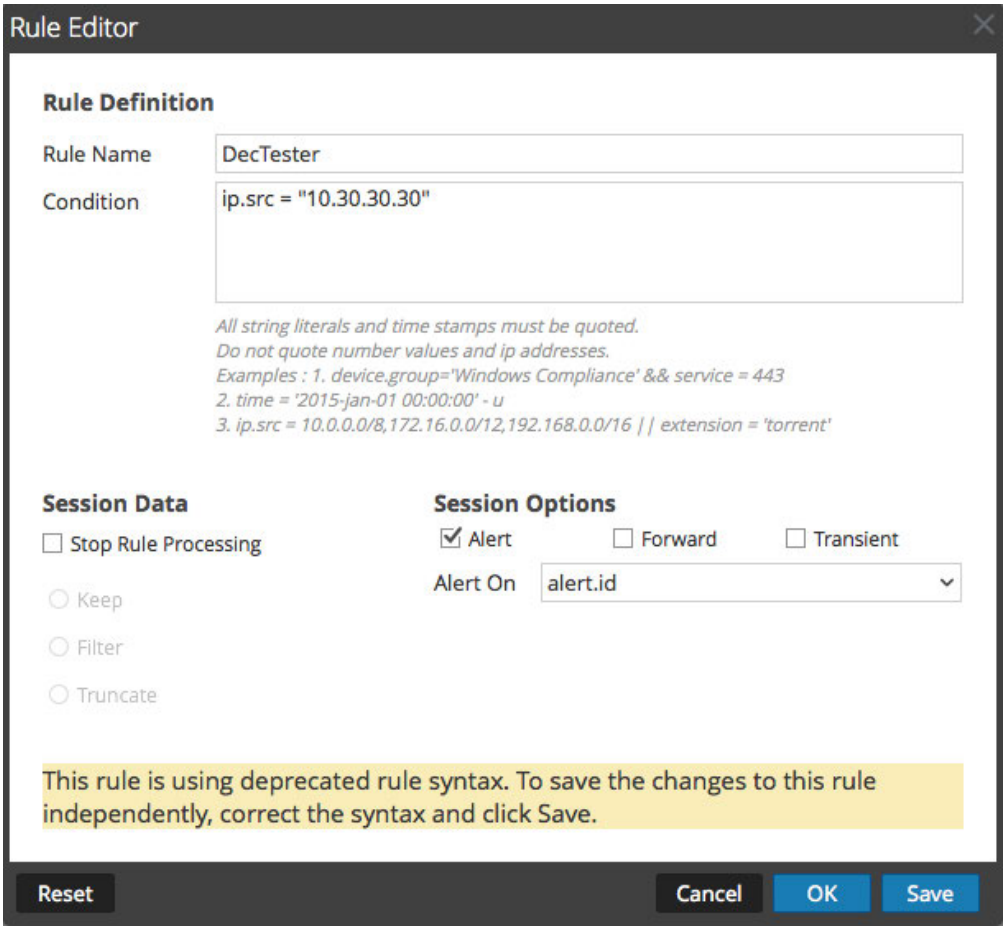
   The Rules tab for the selected rule type shows the number of rules using invalid syntax and the invalid rules are highlighted.



4. Select an invalid rule and click .

   The Rules Editor shows additional information for the invalid rule and it includes an

additional Save option.



5. In the **Condition** field, correct the rule syntax.
   All string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details.
   For example, if the invalid rule condition is `ip.src="10.30.30.30"`, correct the syntax by removing the quotes: `ip.src=10.30.30.30`
6. Do one of the following:
   - To correct the rule individually, click **Save**.
     The corrected rule is applied independently to the Decoder. The corrected rule appears on the Rules tab without highlights.
   - To correct the rule and apply the rule to the Decoder later with other rules, click **OK**.
     The corrected rule appears on the Rules tab without highlights. The rule is not applied to the Decoder.

Decoder Commands for Managing Rules

In the NetWitness Core database, the Rules tree holds the main functionality related to managing rules for all Core services that have rules: Concentrators, Decoders, Log Decoders, and Archivers. Although you can manage rules in the NetWitness Suite user interface, advanced users may prefer to manage rules using a command line to add, merge, replace, delete, and validate rules on a service. This section provides a brief overview of the commands and their usage. These are the available commands:

- `add` - Adds a single rule at the specified position.
- `clear` - Deletes all existing rules in the current node on the service. For example, using the command in `/decoder/config/rules/application` node deletes all existing application rules on the Decoder.
- `delete` - Deletes one or more rules at a specified position and count.
- `merge` - Merges a pushed rule set with an existing rule set. Existing rules that match the incoming rules (by name or rule) are replaced; otherwise, rules are inserted by the position indicated as described in merge Command.
- `replace` - Deletes all existing rules and replaces them with the incoming rule set.
- `validate` - Validates the syntax of a rule, but does not validate the meta keys.

add Command

The `add` command adds the rule to the existing rule set. Formatting is important because the API uses double quotes in the rule language and also uses double quotes as parameters to all RSA NetWitness® Suite APIs. Therefore, you must escape any double quotes in the rule itself by preceding it with a backslash (\) character. This is the syntax of the command:

```
add rule=<string> name=<string> alert=<string, optional> atPos=<<uint32, optional>
```

- `rule` is the rule to add. Be sure to place double quotes around any rules with white space and to escape any double quotes that are part of the rule with a backslash.
- `name` is the name of the rule.
- `alert` is the alert for the rule (if any).
- `atPos` is the position at which the rule should be added (1 based). Zero is the top of the list and any number larger than the current size of the list is appended to the list.

This is an example of command to add a rule using NwConsole

```
send /decoder/config/rules/application add rule="ip.src exists" order=1
alert=alert.id name=testrule
```

For example, take the following rule:

```
alias.host = "myPC" && country.src="china","russian federation"
```

To add this as a rule, you would need to send the parameters as follows:

```
rule="alias.host = \"myPC\" && country.src=\"china\",\"russian
federation\"" name=myRule filter
```

Notice how all the double quotes had to be escaped inside the rule parameter. A simple trick to make this more readable is to use single quotes inside the rule. Single and double quotes are interchangeable in the rule and query language, but not in parameters for the API (only double quotes are supported there). Therefore, this is more readable:

```
rule="alias.host = 'myPC' && country.src='china','russian federation'"
name=myRule filter
```

merge Command

The `merge` command is used to merge an incoming list of rules with the existing rules on the service. This is how it works:

- It finds existing rules that match via the name OR via a matching rule, updates the existing rule name, and keeps the same position.
- It inserts new rules into the rule list based on the NUMBER position. If the number is zero, it goes to the top of the list.
- It processes the rules in the order received so if you have two rules numbered zero, the second rule is processed after the first and claims the top spot. All existing rules are pushed down two places. Any numbers higher than existing rule positions are appended after the last existing rule and numbered in sequence.
- Any non-numbered rule is appended after the last existing rule and numbered in sequence.

This is the syntax of the merge command:

```
merge --file-data=<string> --file-format<string>
```

- `file-data` is the full path and name of the rules file to merge.
- `file-format` is the format of the rules file. Valid values are `params-list`, `string`, `params`, `binary`, and `params-binary`.

Methods of Sending a List of Rules to a Service

There are two ways to send a list of rules. You can send them as a `.nwr` (NetWitness Rule) file or as a numbered set of parameters, each number indicates the position to insert the rule at as well as the encoded rule. If you want to see the current list of rules on a service, you need to run the `ls` command on the rule category (for instance, application rules on a Decoder are found in `/decoder/config/rules/application`).

This is an example of commands to list the existing rules using NwConsole:

```
login <hostname>:50004 <username> <password>
cd /decoder/config/rules/application
ls
```

This is another example to list existing rules in NwConsole:

```
send /decoder/config/rules/application ls
```

This is an example of the command to point to network rules in the RESTful port, which supports a basic `admin HTML` app.

```
http[s]://<decoder>:50104/decoder/config/rules/network
```

Send a NetWitness Rule File

Let's start with an example `nwr` file, each rule must be on a separate line:

```
rule="ip.src=192.168.0.1" name=first keep
rule="ip.src=192.168.1.1" name=second alert=risk.info
rule="ip.src=192.168.2.1" name=third filter
```

To push and merge rules using NwConsole, use the following commands:

```
login <hostname>:50004 <username> <password>
send /decoder/config/rules/application merge --file-data=/root/App_Rules.nwr --file-format=params-list
```

To replace the existing rules with the rules in the file, instead of using the `merge` command , use the `replace` command.

```
send /decoder/config/rules/application replace --file-data=<pathname> --file-format=params-list
```

To merge the rules in an `nwr` file using the RESTful port, you can use a `curl` command that pushes the rules:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary @<pathname> -X POST "http://<hostname>:50104/decoder/config/rules/application?msg=merge"
```

The examples are pushing application rules. To push network rules, send the rules to `/decoder/config/rules/network`. For correlation rules, send the rules to `/decoder/config/rules/correlation`.

Send Numbered Parameters

The other way to send a list of rules is to send them as numbered parameters. The difficulty with this method is remembering to escape the quotes within each numbered rule. Though it is only a problem if you are trying to do it by hand. For instance, to send the same rules above as parameters via NwConsole, use the following command:

```
send /decoder/config/rules/application merge 1="rule=\"ip.src=192.168.0.1\"
name=first keep" 2="rule=\"ip.src=192.168.1.1\" name=second alert=risk.info"
3="rule=\"ip.src=192.168.2.1\" name=third filter"
```

This command is hard to read because you have to escape the inner quotes with a backslash (\). Otherwise, these two commands accomplish the same thing. Merging or adding three rules in positions 1, 2 and 3. If you think the above was hard to read, this is what the equivalent `curl` command looks like:

```
curl -u "<username>:<password>"
"http://<hostname>:50104/decoder/config/rules/application?msg=merge&1=rule%3D%22ip.src%3D
192.168.0.1%22%20name%3Dfirst%20keep&2=rule%3D%22ip.src%3D192.168.1.1%22%20name
%3Dsecond%20alert%3Drisk.info&3=rule%3D%22ip.src%3D192.168.2.1%22%20name%3Dthird
%20filter"
```

For more details on how to escape double quotes inside parameters, see add Command.

Ordering Rules When Pushing

Pushed rules are ordered in one of two ways. When passing as parameters, the number of each parameter determines the insertion order. If it is not actually a number, `merge` checks for an `order` parameter within the rule itself and uses that value if found.

Note: Using `order` is the only way to set the order with a `.nwr` file. If neither a number nor an `order` parameter is found, there are no guarantees of the insertion order.

Example

A Decoder has the following application rules installed; notice the numbering is ALWAYS consecutive and starts at 1:

0001 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep

0002 : rule="ip.src=192.168.1.1" name=second alert=risk.info

0003 : rule="ip.src=192.168.2.1" name=third filter

And you want to merge the following four rules:

rule="ip.src=192.168.3.1" name=third keep

rule="ip.dst=192.168.4.1" name=NewRule filter order=0

rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append

rule="service=80,443" name=web filter order=3

Use any method to push your rules and this is what you end up with:

0001 : rule="ip.dst=192.168.4.1" name=NewRule filter order=1

0002 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep order=2

0003 : rule="service=80,443" name=web filter order=3

0004 : rule="ip.src=192.168.1.1" name=second alert=risk.info order=4

0005 : rule="ip.src=192.168.3.1" name=third keep order=5

0006 : rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=6

Are there any surprises here? This is how each rule was processed.

1. rule="ip.src=192.168.3.1" name=third keep

This rule had the same name as an existing rule on the Decoder (third). So the rule updated the existing rule, `changing _filter_ to _keep_`.

2. rule="ip.dst=192.168.4.1" name=NewRule filter order=0

This rule is new and had `order=0` in it, which means insert at the very top.

3. rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append

This rule had a non-number `append` for `order`, therefore, it went to the end of the list. You can accomplish the same thing by giving a very large number, like `999999`.

`4. rule="service=80,443" name=web filter order=3`

This rule is last but has `order=3`, therefore, if it does not match an existing rule by name or the text of the rule itself, it should be placed in position 3. And there it is, the third rule in the list. Any rules that follow were pushed further down.

replace Command

The `replace` command removes all existing rules and replaces them with the incoming rule list. Refer to merge Command for details on how to format the incoming rule list and how ordering works.

This is an example of the `replace` command using a Netwitness Rule File :

send /decoder/config/rules/application replace --file-data=/root/Decoder-AppRules.nwr --file-format=string

This is an example of the `replace` command using Numbered Parameters :

send /decoder/config/rules/application replace 1="rule=\"ip.src exists\" name=\"test rule\" order=1 alert=alert.id"

clear Command

The `clear` command removes all existing rules on the service. This is an example of the command:

```
send /decoder/config/rules/application clear
```

delete Command

The `delete` command deletes one or more rules on the service.

delete atPos <uint32> count <uint32, optional>

- `atPos` deletes the rule at the given position. Rules are numbered starting with 1 and go in sequential order.
- `count` deletes one or more rules starting `atPos`. This is an optional parameter defining the number of rules to delete starting `atPos`. The default value is 1.

This example of the command deletes four rules beginning at position 0003:

```
send /decoder/config/rules/application delete atPos=0003 count=4
```

validate Command

The `validate` command takes the provided rule and verifies that it parses correctly. Keep in mind that this command cannot verify whether language keys and entities are valid.

validate rule <string>

`rule` - is the name of the rule to validate. Make sure to place double quotes around any rules with white space.

Configure Feeds and Parsers

Feeds and parsers are responsible for analyzing the packets and logs when captured or imported in a Decoder or Log Decoder. Most commonly, they are used for static metadata extraction and service identification. The flexible definition allows custom extension of the core defined services to provide extra service type identification and metadata extraction. This is important due to the volume of custom applications that are used on networks.

Note: Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.

Configure Parsers

NetWitness Suite has a set of core parsers that are defined by the system, and also has the ability to add additional parsers. Each parser is configurable in the Services Config View - General Tab. The Parser Configuration panel provides a way to enable or disable parsers to use on the Decoder in addition to limiting the metadata that the parser creates.

In addition, there are several types of custom configurable parsers:

- GeoIP – This parser associates the IP addresses with geographical locations.
- Search – This parser is user -configured to generate metadata by scanning for pre -defined keywords and regular expressions.
- FLEXPARSE (deprecated) – This is a generic parser definition language for extending the existing application protocol support of the Decoder. By default this parser is disabled (see Enable or Disable Lua and Flex Parsing Systems).
- Lua – This parser is defined using the Lua scripting language for extending the existing application protocol support of the Decoder.
- enVision – This application parser supports the Log Decoder and is configured to generate metadata by scanning log files.
- SNORT® – This parser supports the payload detection capabilities of SNORT® IDS rules.

In the Services Config view > Parsers tab, you can view deployed parsers on a Decoder, upload parsers, and delete deployed parsers. The user interface includes an Indicator if the parser originated from Live Services, installed through NetWitness Suite, or uploaded manually. Parsers can be added and removed while a Decoder is running without affecting capture.

In addition, you can download parsers using NetWitness Suite Live Services.

Configure Feeds

NetWitness Suite uses feeds to create metadata based on externally defined metadata values. A feed is a list of data that is compared to sessions as they are captured or processed. For each match, additional metadata is created. This data could identify and classify malicious IPs or incorporate additional information such as department and location based on internal network assignments. Some examples of feeds include threat feeds to identify BOTNets, DHCP mappings, or even active directory information such as physical location or logical department.

You can use the Live module in NetWitness Suite to obtain feeds from outside sources. "Live Content in NetWitness Suite" in the *Live Services Management Guide* provides an overview of the Live content management tool.

Within the NetWitness Suite user interface, you can view the list of currently deployed feeds, along with an indicator if a feed that originated from Live was installed through NetWitness Suite or manually. Feeds can be added, removed, and updated while a Decoder is running without affecting capture.

has a Custom Feed wizard to allow creation and deployment of custom Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides users through the process to create both on-demand and recurring feeds, it is helpful to understand the form and content of a feed file when you create a feed.

NetWitness Suite has a Custom Feed wizard, which streamlines the task of creating and managing custom feeds, as well as populating the feeds to selected Decoders and Log Decoders. In addition, you can download existing feed files and edit the files, then edit the feed or create a new feed using the edited file.

Custom Feed Definition File Structure

The NetWitness Suite Custom Feed wizard allows creation and deployment of custom Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides users through the process to create both on-demand and recurring feeds, it is helpful to understand the form and content of a feed file when you create a feed.

Feed filenames in RSA NetWitness Suite are in the form `<filename>.feed`. To create a feed, NetWitness Suite requires a feed data file in `.csv` or `.xml` format and a feed definition file in `.xml` format, which describes the structure of a feed data file. The Custom Feed wizard can create the feed definition file based on a feed data file, or based on a feed data file and the corresponding feed definition file.

The files that you use to create an on-demand feed must be stored on your local file system. The files used to create a recurring feed must be stored at an accessible URL, whence NetWitness Suite can fetch the most current version of the file for each recurrence. After a NetWitness Suite feed is created, you can download the feed to your local file system, edit the feed files, and then edit the NetWitness Suite feed to use the updated feed files.

Sample Feed Definition File

This is an example of a feed definition file named `dynamic_dns.xml`, which NetWitness Suite creates based on your entries in the Custom Feed wizard. It defines the structure of the feed data file named `dynamic_dns.csv`.

Note: The feed file path should be `.csv` regardless of the Feed Type (Default or STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
   truncdomain="true"/>

   <LanguageKeys>
            <LanguageKey name="threat.source" valuetype="Text" />
            <LanguageKey name="threat.category" valuetype="Text" />
```

```
            <LanguageKey name="threat.desc" valuetype="Text" />
    </LanguageKeys>

    <Fields>
    <Field index="1" type="index" key="alias.host" />
    <Field index="4" type="value" key="threat.desc" />
    <Field index="2" type="value" key="threat.source" />
    <Field index="3" type="value" key="threat.category" />
    </Fields>
    </FlatFileFeed>

</FDF>
```

Feed Definition Equivalents for Custom Feed Wizard Parameters

The NetWitness Suite Custom Feed wizard provides options to define the structure of the data feed file. These correspond directly to attributes in the feed definition (.xml) file.

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Feed Tab) Feed Type	Select: **Default** - to define a feed based on a .csv formatted feed data file. **STIX** - to define a feed based on STIX formatted.xml file.
(Define Feed Tab) Feed Task Type	Select: **Adhoc** - to create an on-demand feed. **Recurring** - to update the .csv or .xml file persistently and store it in a location accessible by NetWitness Suite , so NetWitness Suite downloads a file at regular intervals and pushes it to the downstream devices.
(Define Feed tab) **Name**	The custom feed name in the feed data file. It corresponds to the `flatfeedfile name` attribute in the feed definition file. For example, Dynamic DNS Test Feed. **Note:** You can use special characters to define the name of the custom feed.

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Feed tab) **File/ Browse**	This is the name of the feed data file. It corresponds to the `flatfeedfile path` attribute in the feed definition file. For example, `dynamic_dns.csv`.
(Advanced Options tab) **XML Feed File**	The name of the feed definition file. For example, `dynamic_dns.xml`.
(Advanced Options tab) **Separator**	The separator character used to separate attributes in the feed data file. It corresponds to the `latfeedfile separator` in the feed definition file. For example, a comma.
(Advanced Options tab) **Comment**	The character used to identify a comment in the feed data file. It corresponds to the `flatfeedfile comment` attribute in the feed definition file. For example, `#`.
(Define Columns tab, Define Index) **Type**	The type of lookup value in the index position of the feed data file. **IP** means that each row in the feed data file contains an IP address in the lookup value position. The IP value is in dotted-decimal format (for example, 10.5.187.42). **IP Range** means that each row in the feed data file contains a range of IP addresses in the lookup value position. The IP range is in CIDR format (for example, 192.168.2.0/24). **Non IP** means that the each row in the feed data file contains a metadata value other than IP address in the lookup value position. The Service Type and Truncate Domain, and Callback Keys fields become active for a Non IP index.

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Columns tab, Define Index) **CIDR**	Specifies that the IP value in the lookup position is in CIDR format. The **CIDR** attribute sets the IP address format in the field to Classless Inter-Domain Routing (CIDR) notation.
(Define Columns tab, Define Index) **Service Type**	For a Non IP index, the integer service type to filter meta lookups. It corresponds to the `MetaCallback apptype` attribute in the feed definition file. A value of 0 indicates no filtering by service type.
(Define Columns tab, Define Index) **Truncate Domain**	For a Non IP index, for meta values that contain domain names (for example, hostnames), the system can strip off the host specific element in the data. Truncate Domain corresponds to the `MetaCallback truncdomain` attribute. If the value is `www.example.com`, it is truncated to `example.com`. A value of **False** selects no truncation, and **True** selects truncation.
(Define Columns tab, Define Index) **Callback Keys**	For a Non IP index, the available meta keys to match on instead of ip.src/ip.dst (the defaults for IP index type) are selectable from the drop-down list. The Callback Key corresponds to the `MetaCallback name` attribute, and the index column of the csv file must contain data that can match the chosen meta key. For example, if the username meta key is chosen, the index column of the csv file needs to be populated with users to be matched.
(Define Columns tab, Define Index) **Index Column**	Identifies the column in the feed data file that provides the lookup value for the row. Each position in each row of the feed data file is identified by a **Field index** attribute in the feed definition file. A field with an index of **1** is the first entry in a row, the second field has an index of **2**, the third field has an index of **3**, and so on.

NetWitness Suite Parameter	Feed Definition File Equivalent
(DEFINE VALUES) **Key**	The name of the `LanguageKey`, as defined in the feed definition file, for which meta is created from this row of the feed data file. It corresponds to the `Field key` attribute in the feed definition file. A key applies only to a field whose type is set to `value`. In the feed definition file, there is a list of `LanguageKeys` from `index.xml`, or a summary name if Source Name and Destination Name are used. For example, `reputation` is a summary name for `reputation.src` and `reputation.dst`. This value is referenced by the Field key attribute.

Sample Files for a MetaCallback Feed Using CIDR Index Range for IPv4 and IPv6

These sample files demonstrate how to use CIDR index ranges for IPv4 and IPv6 in custom MetaCallback feeds. As with other custom feeds, you must create feed data file in .csv format, and a feed definition file in .xml format.

Note: Using MetaCallback feeds with CIDR index ranges is supported only through the Advanced Configuration wizard or the REST interface.

The following example shows the contents of both a `.csv` file and an `.xml` file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

.csv file:

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
        <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">
                <Meta name="ip.dst"/>
        </MetaCallback>
        <LanguageKeys>
```

```
            <LanguageKey name="alert" valuetype="Text" />
        </LanguageKeys>
        <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
        </Fields>
</FlatFileFeed>
</FDF>
```

Note: To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.

Create a Custom Feed

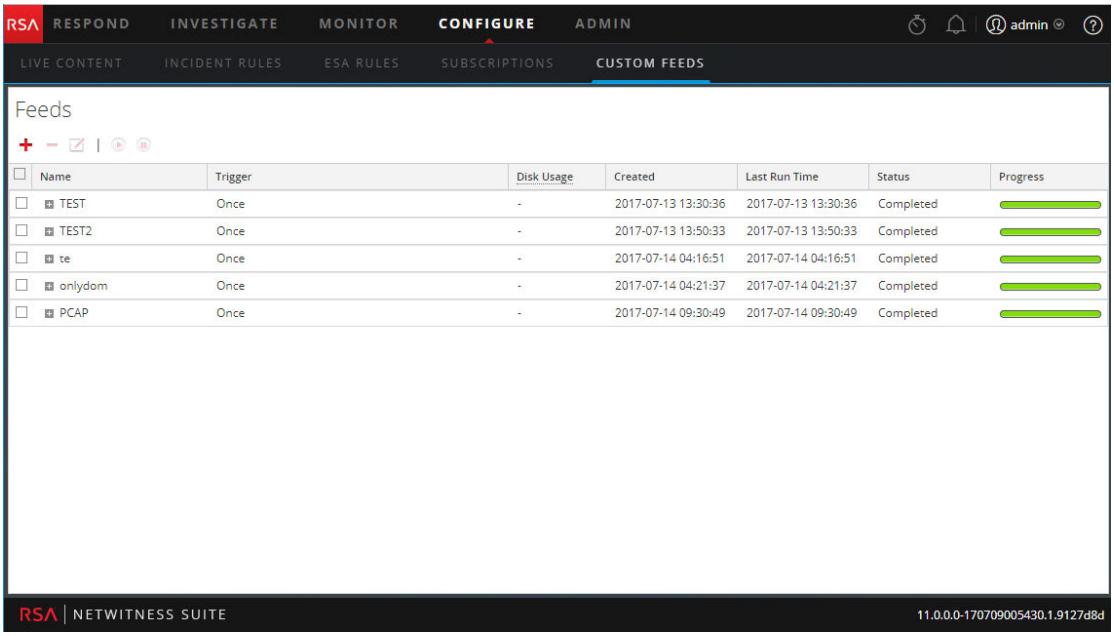
You can create a custom feed using the Custom Feed wizard. To complete this procedure, you need a feed data file in `.csv`or `.xml` format. If you also have an associated feed definition file in `.xml` format, which describes the structure of the feed data file, you can use the feed definition file to create a feed. The Custom Feed wizard can create the feed based on a feed data file, or based on a feed data file and corresponding feed definition file.

Note: From 10.6.1 or later, NetWitness Suite supports Structured Threat Information Expression (STIX). For more information about STIX and creating a STIX custom feed.

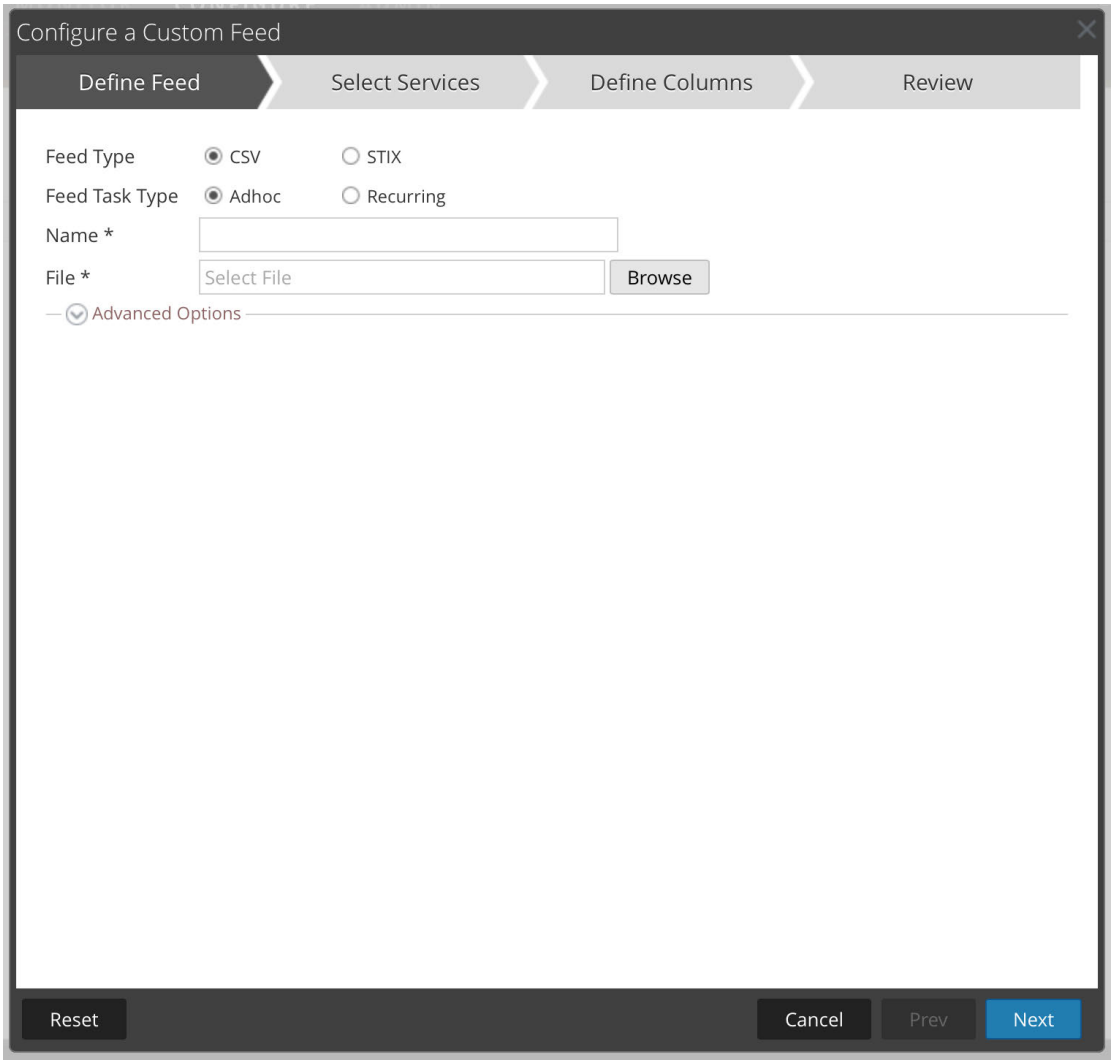
The feed data file and optionally the feed definition file (`.xml`) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness Suite server.

To create a custom feed:

1. Go to **CONFIGURE > Custom Feeds**, and in the **Feeds** panel click **+**.
   The Custom Feeds view is displayed.



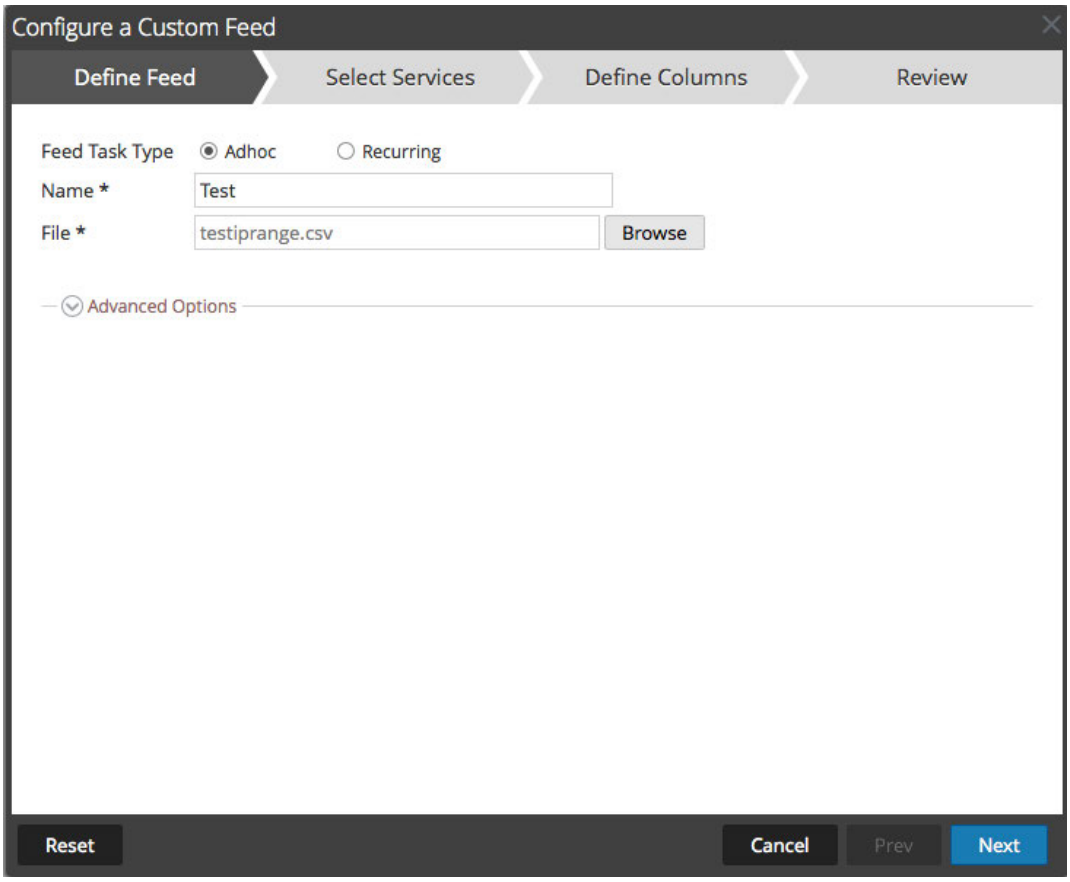
2. Click **Custom Feed** and **Next**.
   The Configure a Custom Feed wizard is displayed, with the Define Feed form open.



3. Select the Feed Type: **CSV** or **STIX**.
4. To define a feed based on a `.csv` formatted feed data file, select **Default** in the **Feed Type** field.

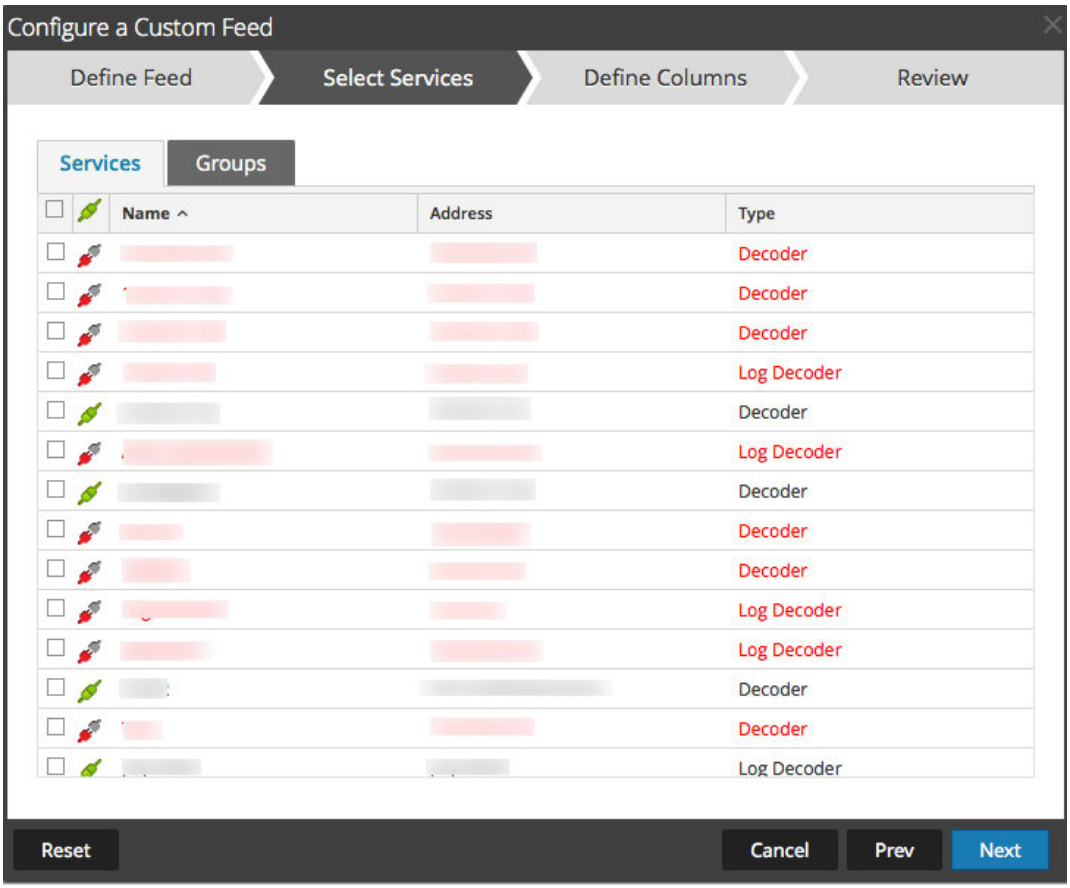
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on a `.csv` formatted feed data file, type the feed **Name**, select a .csv content **File** from the local file system, and click **Next**.
   b. (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

      The Advanced Options are displayed:



c. Select an XML feed file from the local file system, choose the **Separator** (default is comma), and specify the **Comment** characters used in the feed data file (default is #), and click **Next**.

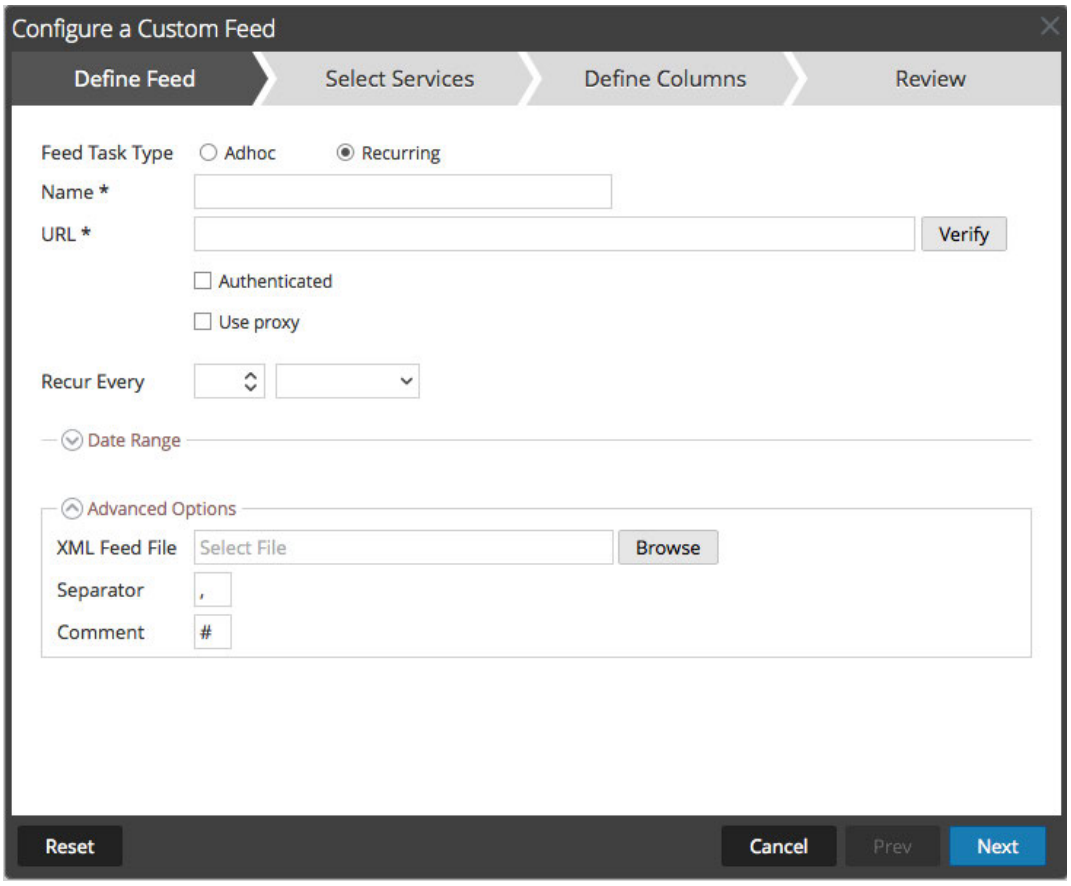
d. The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

a. Select **Recurring** in the **Feed Task Type** field.

The Define Feed form includes the fields for a recurring feed.



b. In the **URL** field, enter the URL where the feed data file is located, for example, `http://<hostname>/<feeddatafile>.csv`, and click **Verify**.

NetWitness Suite verifies the location where the file is stored in order to enable checking for the latest file automatically before each recurrence.

c. (Optional) If the URL has restricted access and requires authentication using your username and password, select **Authenticated**.

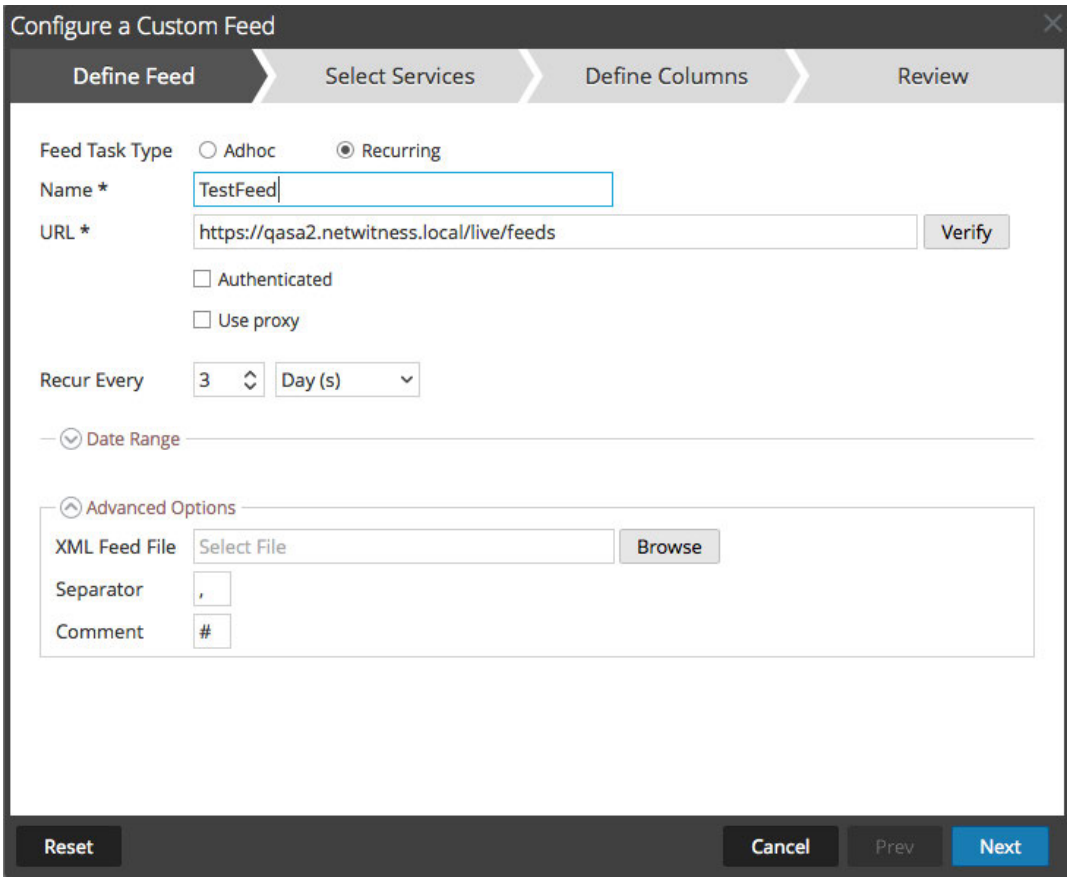
NetWitness Suite provides your user name and password for authentication to the URL.

d. If you want the NetWitness server to access the Feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see "Configure Proxy for NetWitness Suite" in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

e. To define the interval for recurrence, do one of the following:

- Specify the number of minutes, hours, or days between recurrences of the feed.
- Specify recurrence every week, and select the days of the week.

f. To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.



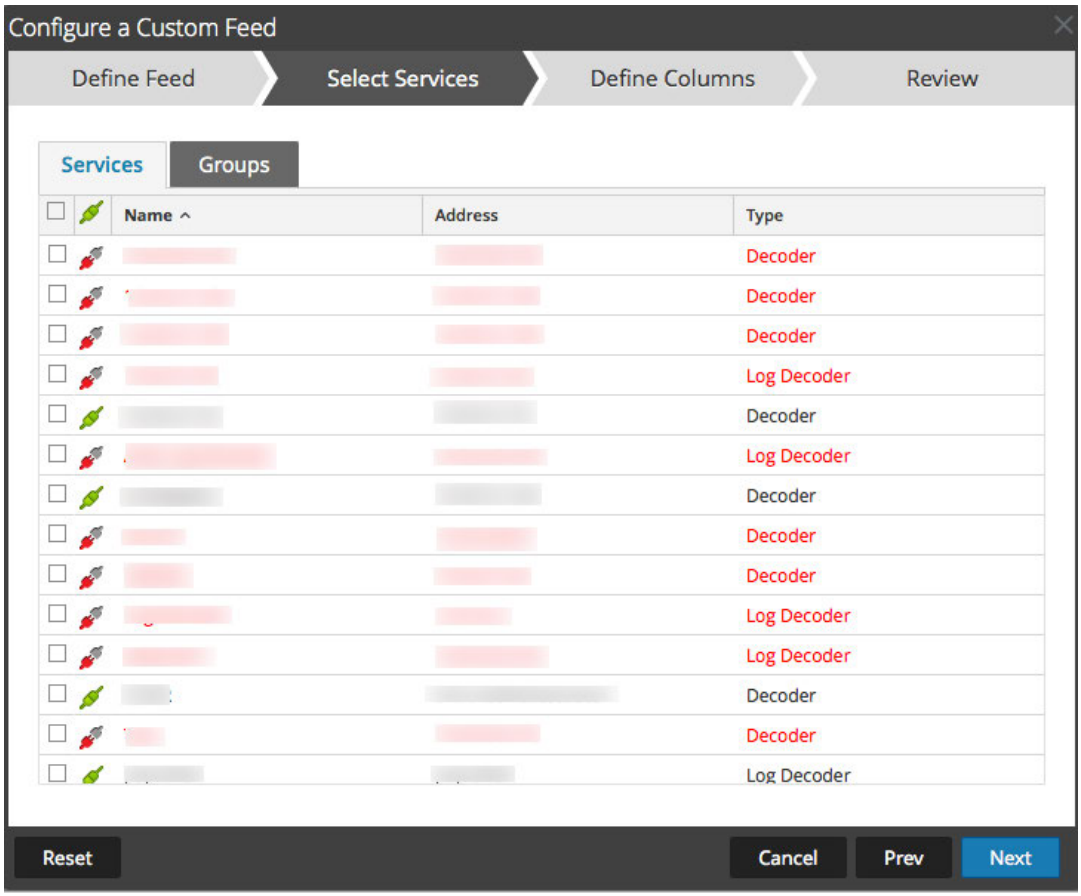
7. (Conditional) If you want to define a feed based on an XML feed file:

- Type the feed **Name**, select **Advanced Options**.

  The Advanced Options fields are displayed.

- Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #) and click **Next**.

  The Select Services form is displayed.



8. To identify services on which to deploy the feed, do one of the following:

   a. Select one or more Decoders and Log Decoders, and click **Next**.

   b. Click the **Groups** tab and select a group. Click **Next**.

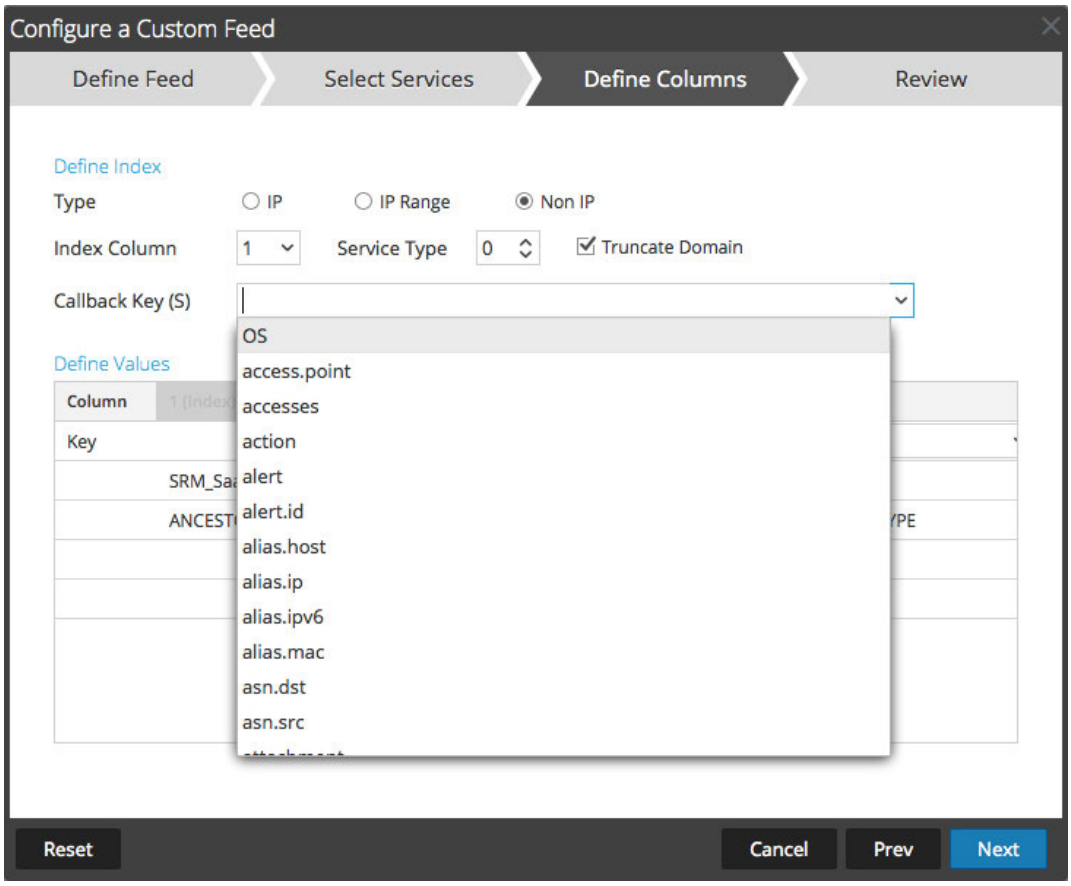
      The Define Columns form is displayed.

9. To map columns in the Define Columns form:

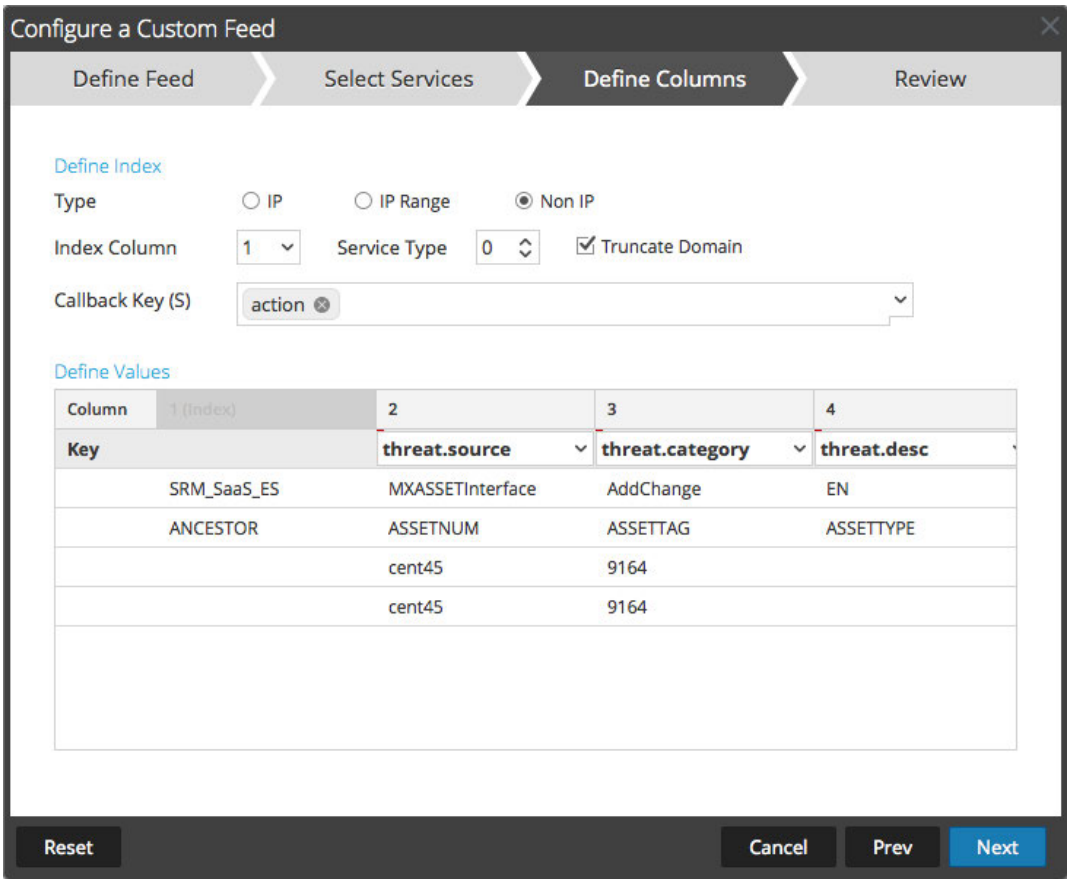
a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.

b. (Conditional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR.**

c. (Conditional) If the index type is **Non IP**, additional settings are displayed. Select the service type and **Callback Keys,** and optionally select the **Truncate Domain** option.

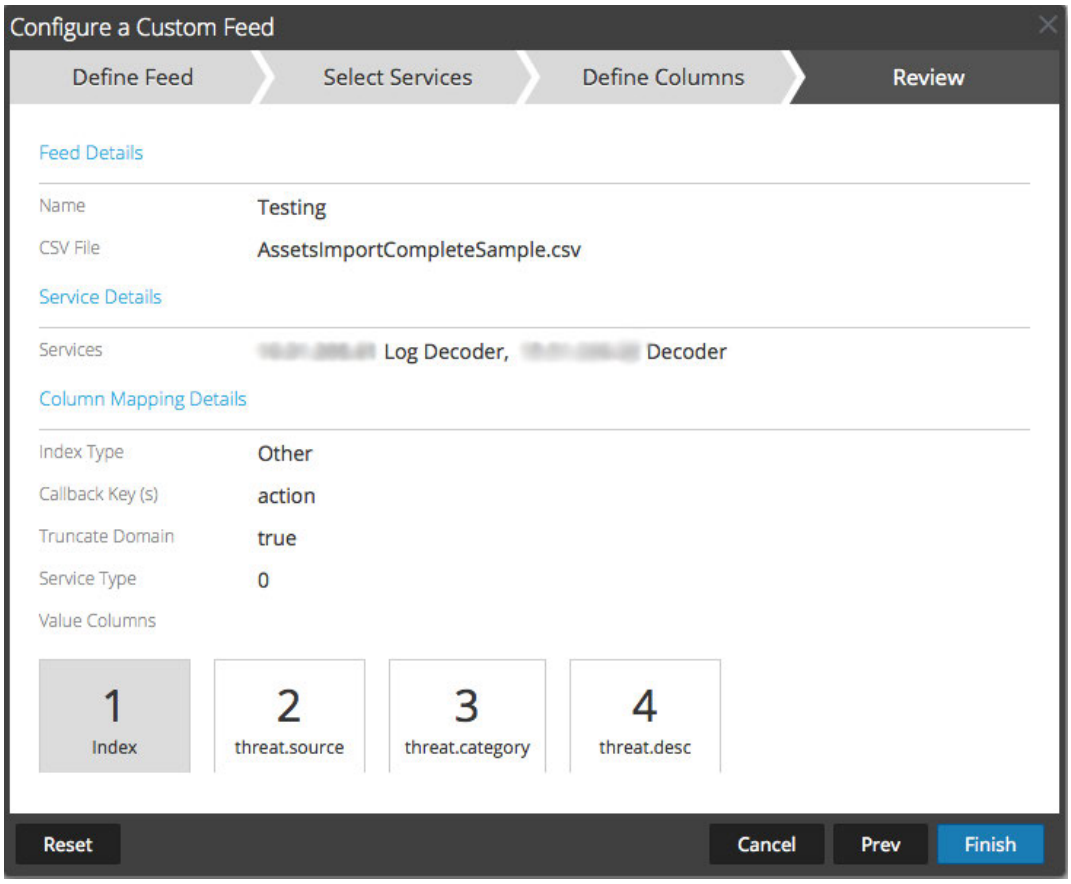


d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.



e. Click **Next**.

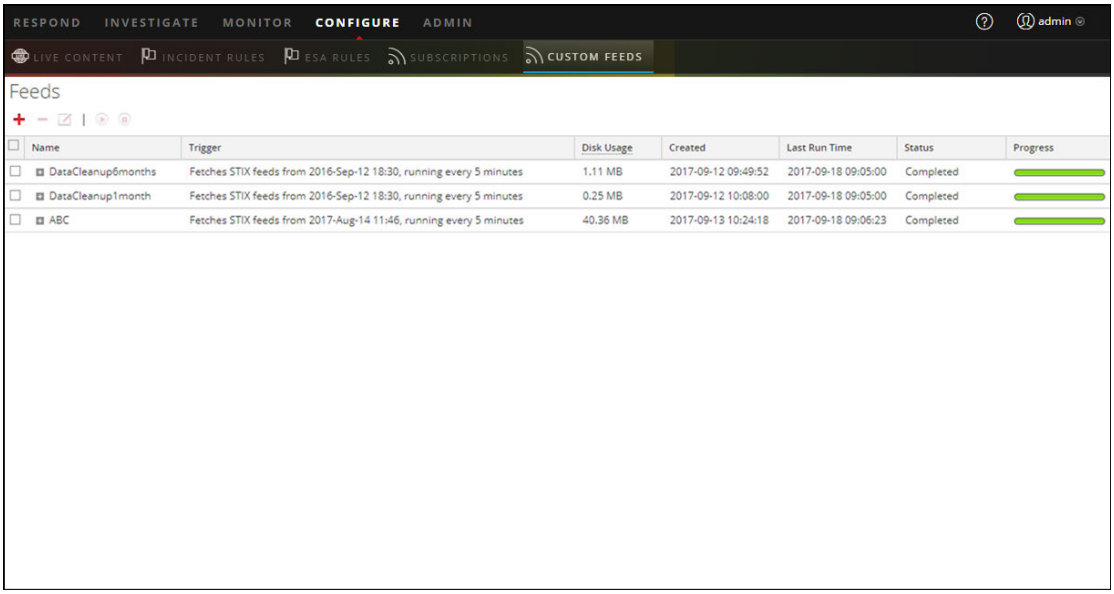
The Review form is displayed.



10. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form)
11. Review the feed information, and if correct, click **Finish**.

12. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.

    ..



Create a STIX Custom Feed

Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. For more information about STIX, see https://stixproject.github.io/.

You can create a custom feed using a STIX-formatted feed data file (`.xml`) in RSA NetWitness Suite. NetWitness Suite supports Structured Threat Information Expression (STIX) 1.0, 1.1 and 1.2 versions only.

Caution: If a STIX recurring feed is configured and you update Security Analytics from 10.6.x to NetWitness Suite 11.0, you must re-configure the STIX recurring feed.

In NetWitness Suite, STIX feeds of type Indicator or Observable that contain properties such as the IP addresses, File hashes, Domain names, URIs and Email addresses are supported. The properties values in the Equals operator are supported. Attributes such as Type and Title are also read from the STIX. A STIX file with a single STIX_Package is supported.

TAXII (Trusted Automated eXchange of Indicator Information) is the main transport mechanism for cyber threat information represented in STIX. Using the TAXII services, organizations can share cyber threat information in a secure and automated manner.

The STIX and TAXII communities work closely together to ensure that they continue to provide a full stack for sharing threat intelligence.

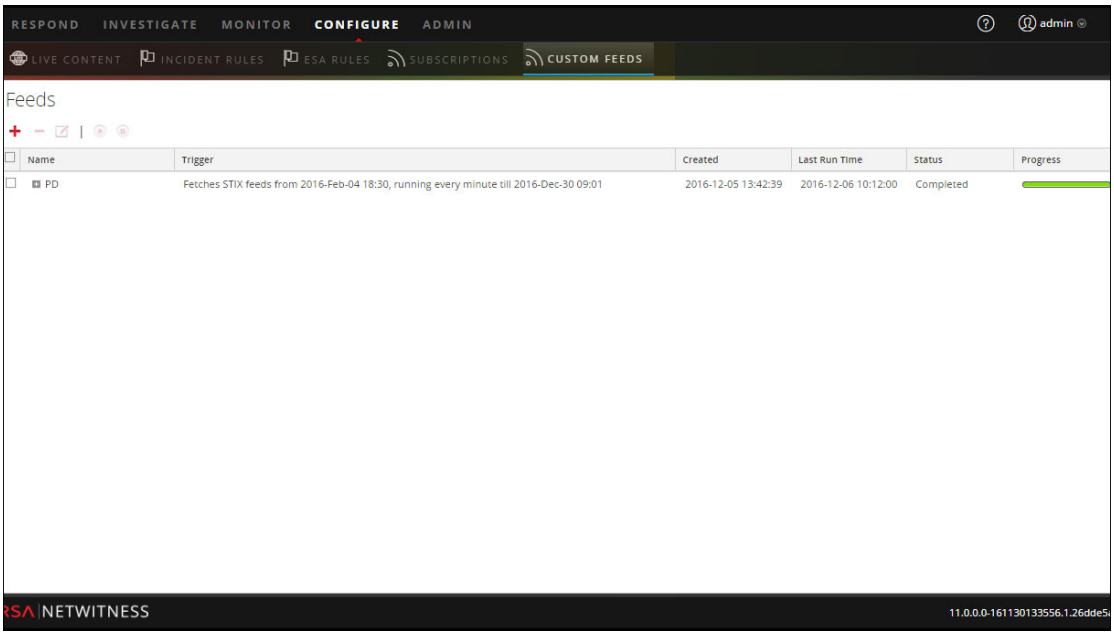
Apart from the TAXII server, STIX data can also reside on a REST server and you can fetch the STIX file from the REST server by providing the URL of the REST server. For example, `http://stixrestserver.internal.com`.

The STIX feed data file and optionally the feed definition file, both in `.xml` format must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness Suite server.

To create a STIX custom feed:

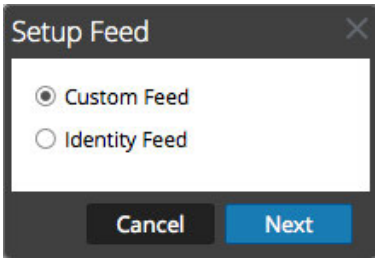
1. Go to **Configure > Custom Feeds**.

   The Custom Feeds view is displayed.



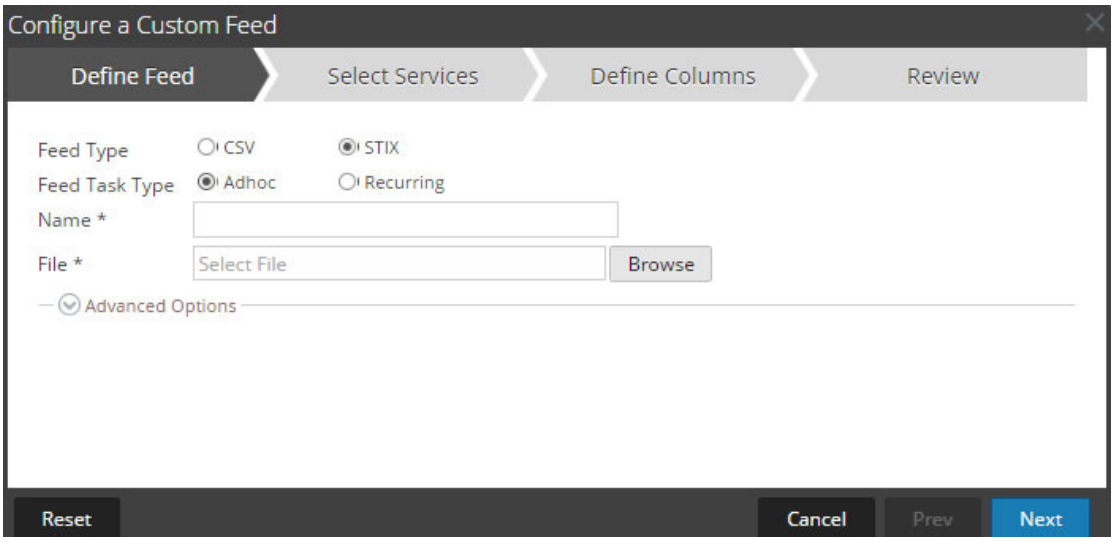
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.



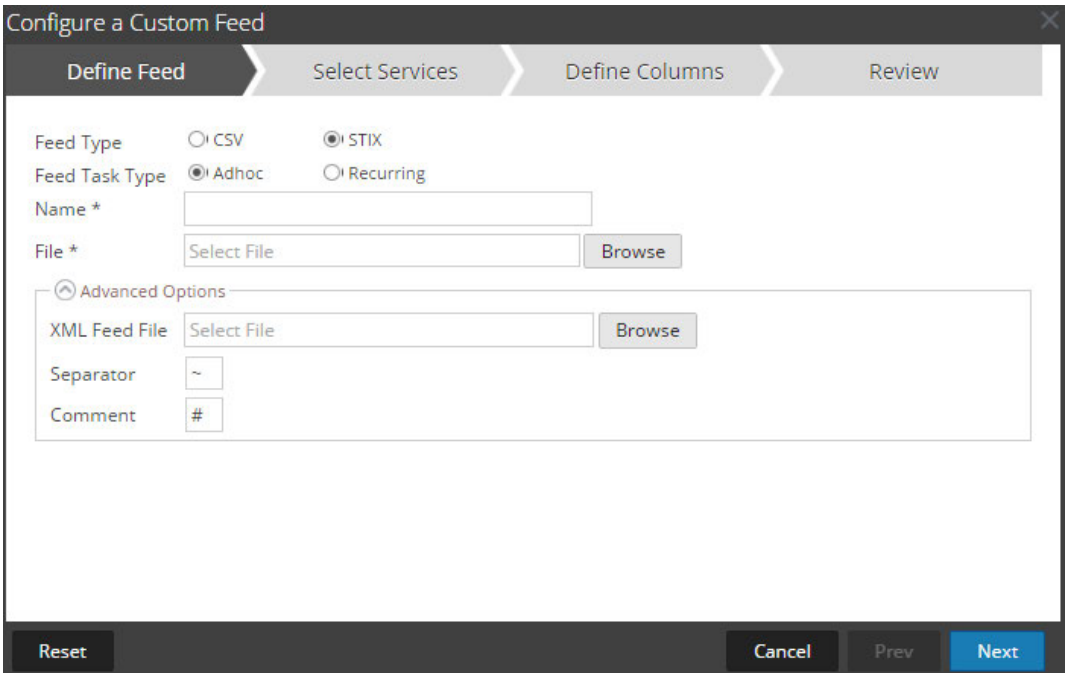
3. To select the feed type, click **Custom Feed** and **Next**.

   The Configure a Custom Feed wizard is displayed, with the Define Feed form open.



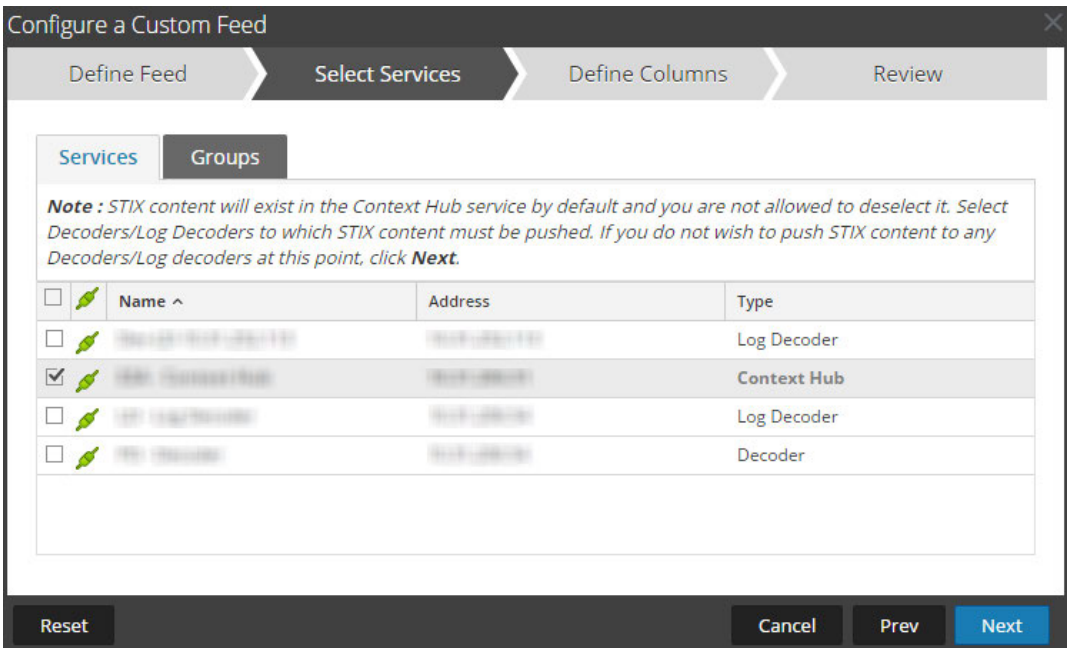
4. To define a feed based on a STIX formatted `.xml` file, select **STIX** in the **Feed Type** field.
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on STIX-formatted `.xml` file, type the feed **Name**, select a STIX formatted `.xml` content **File** from the local file system, and click **Next**.
   b. (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

      The Advanced Options are displayed.



   c. Select an XML feed file from the local file system, choose the **Separator** (default is

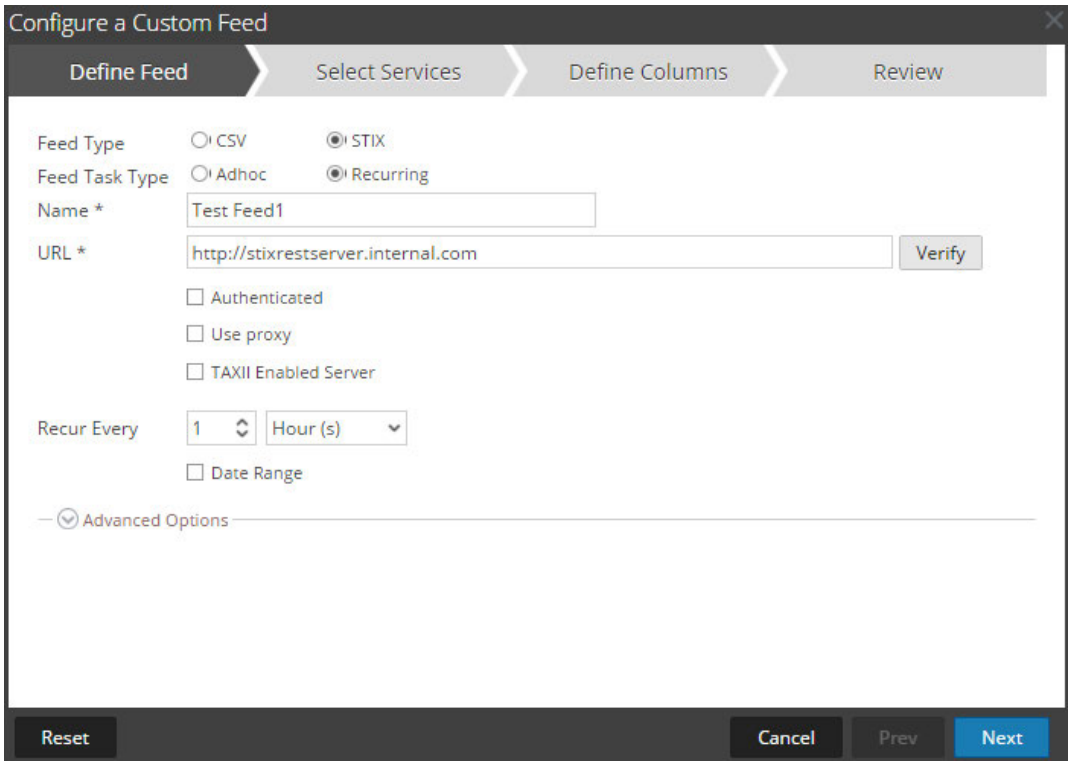
comma), specify the **Comment** characters used in the feed data file (default is #), and click **Next**.
The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

   a. Select **Recurring** in the **Feed Task Type** field.

      The Define Feed form includes the fields for a recurring feed.



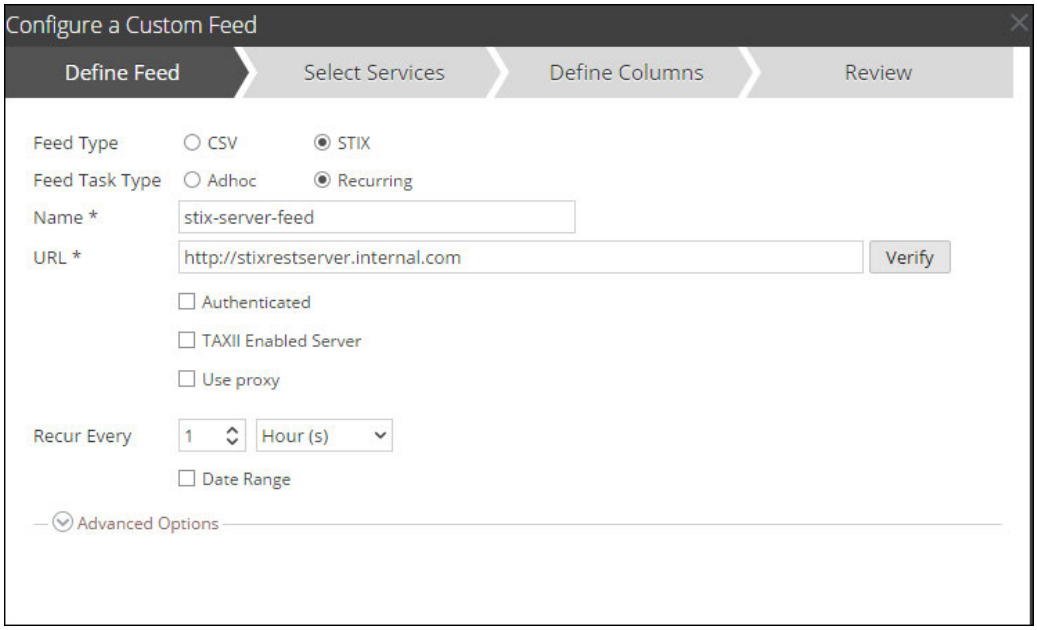
b. In the **URL** field, do one of the following:

- To define a recurring feed based on STIX which pulls STIX packages from a TAXII Server, enter the TAXII server's discovery service URL, for example, `http://hailataxii.com/taxii-discovery-service`.

  Note: A Context Hub service installed on Event Stream Analysis host must be reachable for the specified TAXII server.

- To define a recurring feed based on a STIX-formatted `.xml` file using the REST Server, enter the URL of the REST server where the STIX data file is located, for

example, `http://stixrestserver.internal.com`.



NetWitness Suite verifies the connection to the server, so that NetWitness Suite can check for the latest file automatically before each recurrence.

c. If you do not want NetWitness Suite to verify the REST server's SSL certificate, Select **Trust All Certificate**. This option is enabled by default (checked).

d. For client authentication with the REST URL, in the **Certificate** field, click **Browse** and select the self signed certificate. The supported certificate formats are `.cer`, `.crt` with `Base64` and `DER` encoded files.

e. (Optional) If the URL has restricted access and requires authentication using your username and password, select **Authenticated**.

NetWitness Suite provides your user name and password for authentication to the URL.

f. Select **TAXII Enabled Server**, if you want to select a TAXII collection from the list. For a valid URL, one or more TAXII collections that contains the STIX data file is displayed based on your credentials. Select the required TAXII collection from the list. Only one collection can be added from a TAXII server for a feed.

Note: Though multiple feeds from multiple TAXII servers are supported, only one account (username and password) is supported per TAXII server.

g. If you want the NetWitness Suite server to access the feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see "Configure Proxy for NetWitness Suite" in the *System Configuration Guide*. (Go to the Master Table of

Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.) By default, the **Use Proxy** checkbox is not selected.

h. (Optional) Click **Verify** to test the settings.

> **Note:** Make sure all the required connection parameters such as Authentication, Proxy, Certificate trust, TAXII Enabled Server, and others, are configured before you click Verify.

i. To define the interval of recurrence for pushing to the Decoder or Log Decoder, do one of the following:

- Specify the number of minutes, hours, or days between recurrences of the feed.
- Specify recurrence every week, and select the days of the week.

j. To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time. The Start Date should be defined from when you want to fetch the data.

7. (Conditional) If you want to define a feed based on an XML feed file:

- Type the feed **Name**, select **Advanced Options**.

  The Advanced Options fields are displayed.

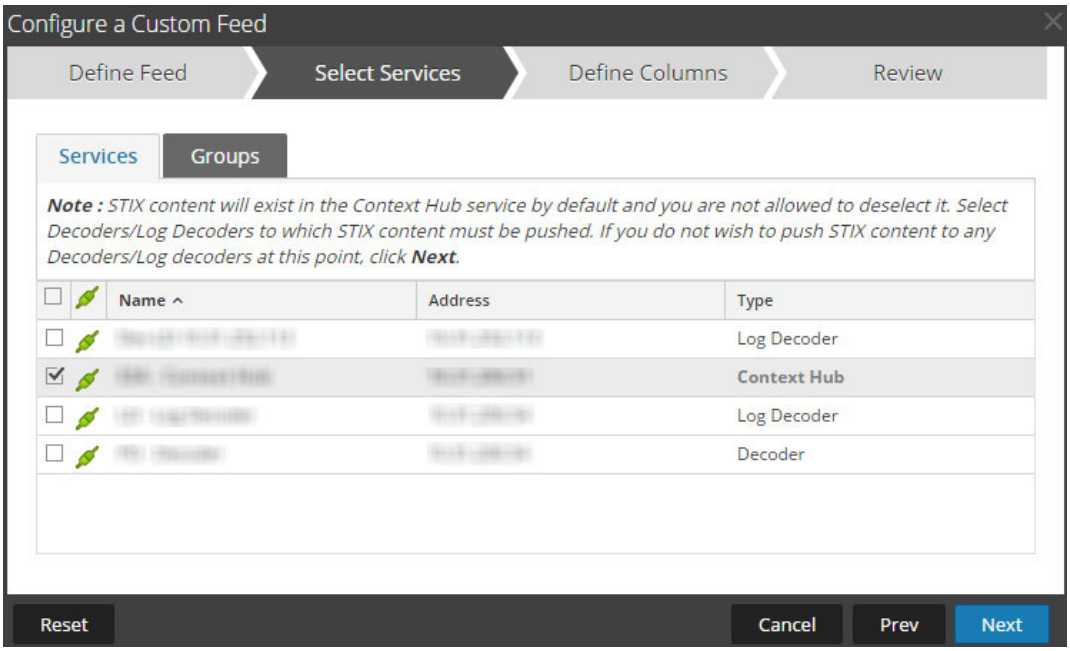
- Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #).
- In the **Remove STIX data older than** field, specify the number of days for which STIX packages pulled from TAXII server is to be stored. The STIX packages older than the specified number of days is deleted automatically.
- Click **Next**.

  The Select Services form is displayed.

8. To identify services on which to deploy the feed, do one of the following:

a. Select one or more Decoders and Log Decoders, and click **Next**.

b. In case of STIX feed, Context Hub will be selected by default and you are not allowed to deselect it. In addition, you can select one or more Decoders and Log Decoders and click **Next** or click the **Groups** tab and select a group. Click **Next**.

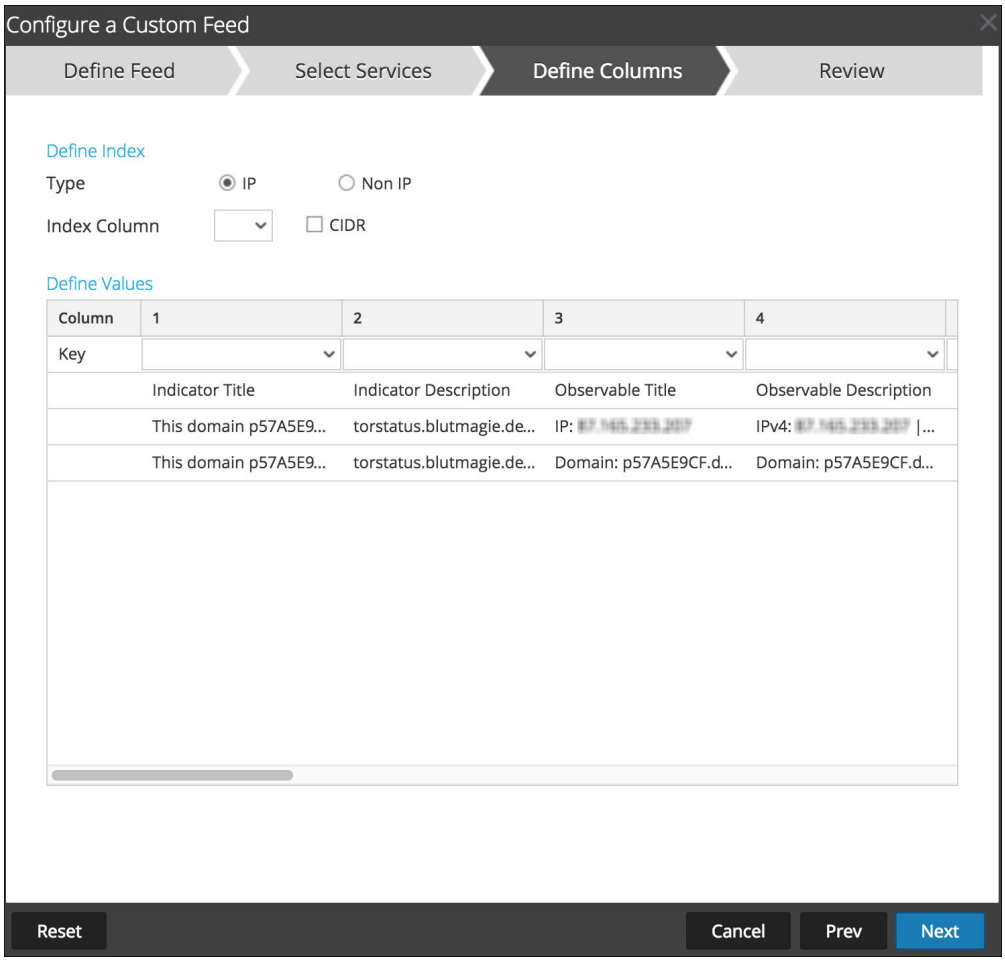


If the data from the STIX server is large, the following message is displayed: "Fetching sample date is taking longer than expected. Choose one of the following options." You have two options: continue to wait or map without sample data.

- If you click **Continue to Wait**, the Feed Wizard continues to wait till the sample data is fetched or a timeout (10 minutes) occurs, whichever is sooner. If there is a timeout, no sample data is retrieved.
- If you click **Map without Sample data**, the mapping column is displayed without any sample data.

The Define Columns form is displayed.

9. To map columns in the Define Columns form:
   a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.
   b. (Conditional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR**.
   c. (Conditional) If the index type is **Non IP**, additional settings are displayed. Select the service type and **Callback Keys,** and optionally select the **Truncate Domain** option.

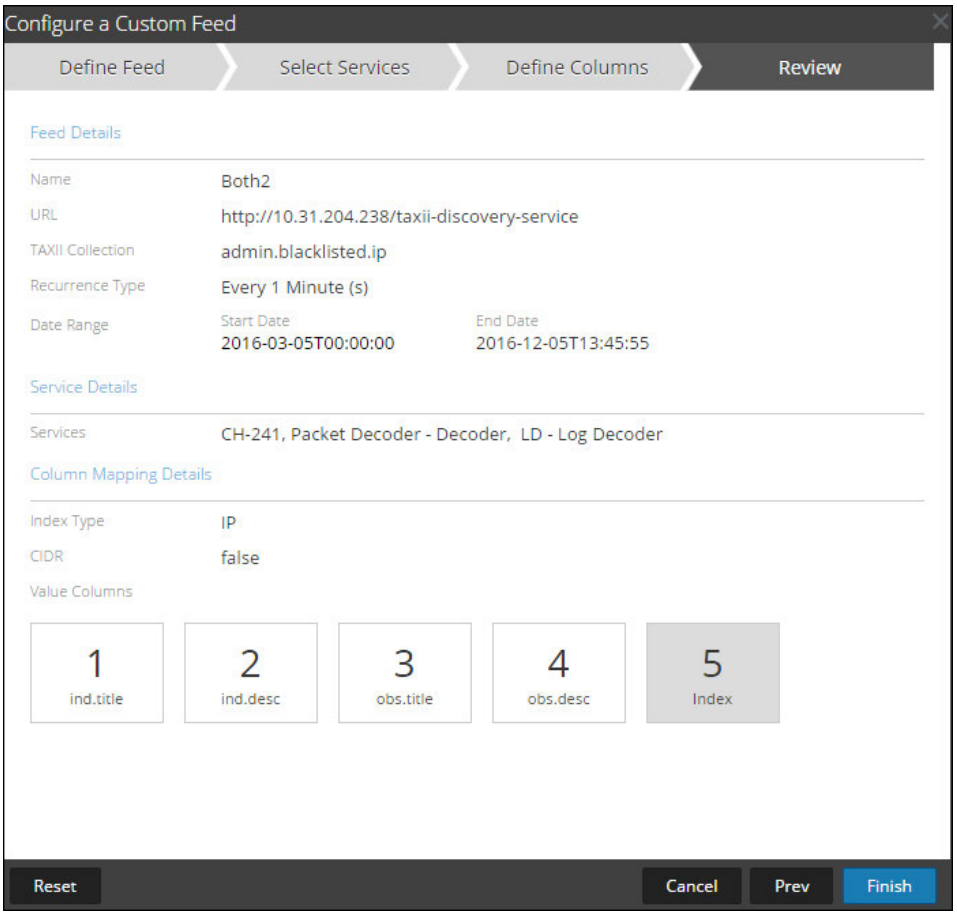


- If the Index Type is Non IP, you can select multiple index columns in the Index Columns. The values from all the selected columns are merged in the first index column that you selected and the merged values are pushed to the Log Decoder for parsing. For example, in the Index Columns if you select 2,4,7 as index columns the values from the 2,4 and 7 columns are merged in the column 2 and the values are pushed to Log Decoder for parsing.
- Indexing cannot be done for columns such as Indicator Title, Indicator Description, Observable Title, Observable Description, as the look up cannot be performed for those columns.

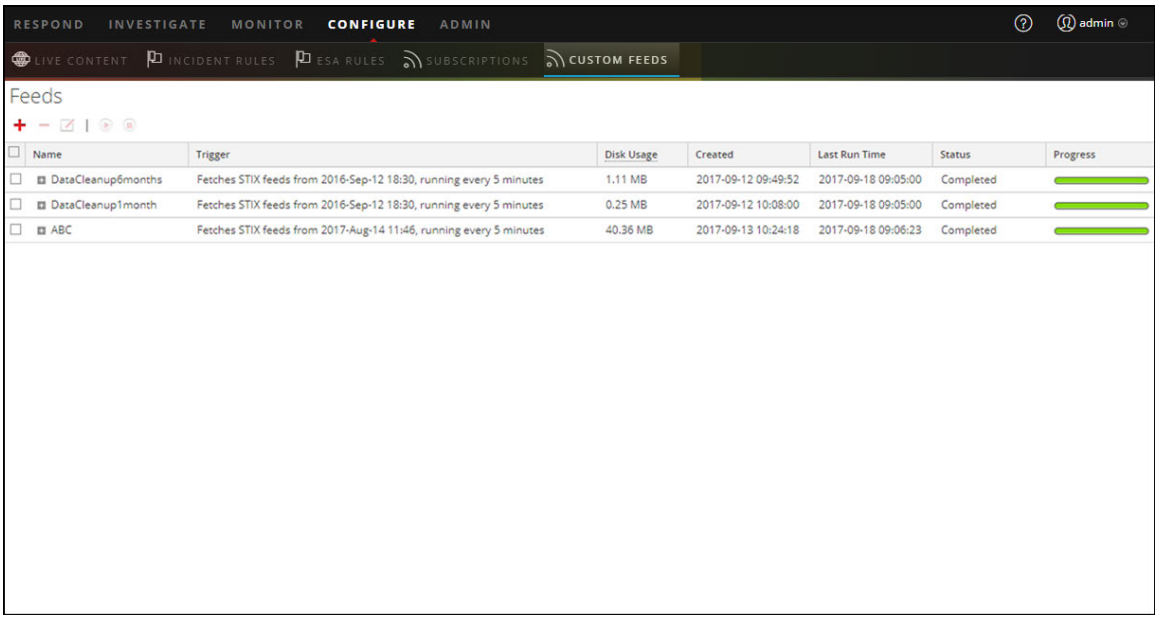
d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.

e. Click **Next**.

The Review form is displayed.



10. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form).
11. Review the feed information, and if correct, click **Finish**.
12. Upon successful creation of the feed definition file, the Create Feed wizard closes, the feed and corresponding token file are listed in the Feed grid, and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.



Note: Health and Wellness raises alerts when the available heap memory of Context Hub server is critically low. If the status of Context Hub server is Unhealthy due to low memory. For more information on how to troubleshoot `OutOfMemoryError` on `Contexthub` Server, refer to "Troubleshooting" in the *Live Services Management Guide*.

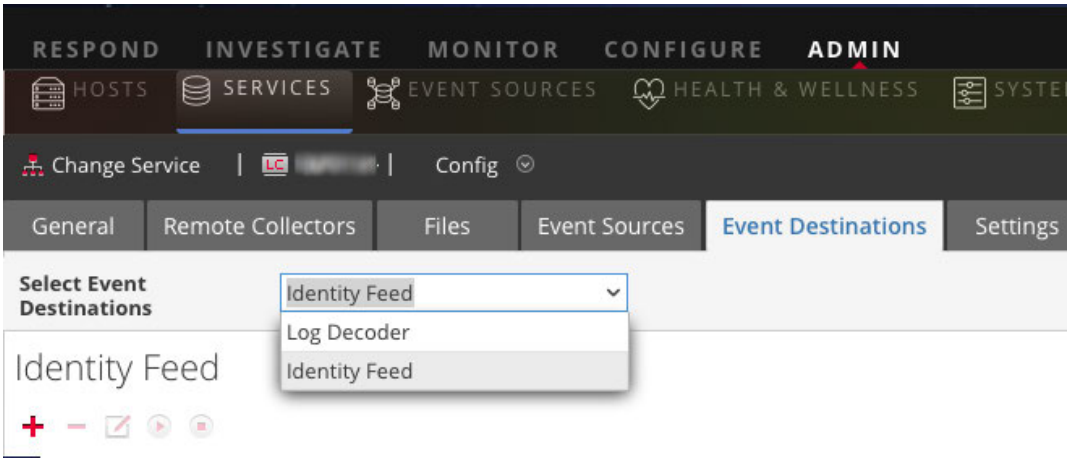
Create an Identity Feed

You can create an Identity feed and populate it to selected Decoders and Log Decoders. In order to create an identity feed, you need to have:

- A Log Collector service with an Identity Feed Event Processor
- A Log Collector service with Windows Collection configured and enabled

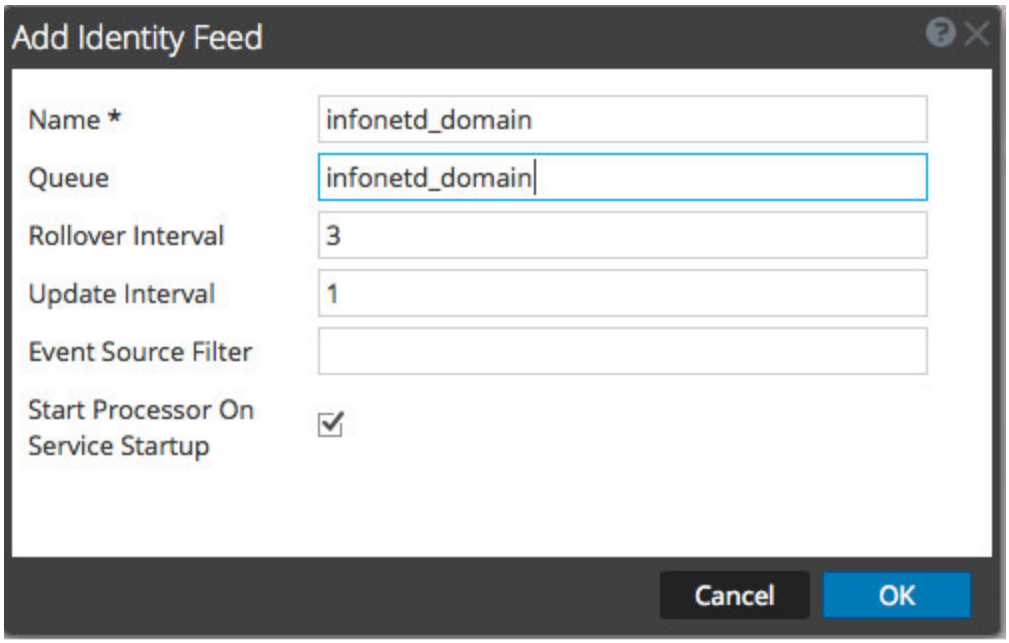
To create an identity feed:

1. Add a destination for the feed.
   a. Go to **ADMIN > Services**, in the **Services** list select a **Log Collector** service, and **View > Config**.
   b. Select the **Event Destinations** tab.
   c. In the Select **Event Destinations** field, select **Identity Feed**.



   d. Click + and enter a unique name for the feed.

      The Queue name identifies the feed within the log collector. Use the name of the feed for the Queue.

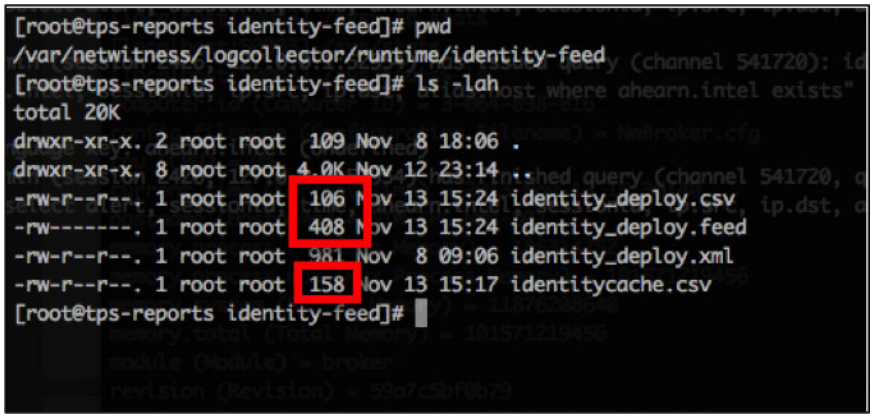


e. Click **OK**.

2. Test generation of messages.

   a. Have users log into Windows boxes on the domain to generate the appropriate log messages on the domain controllers for testing.

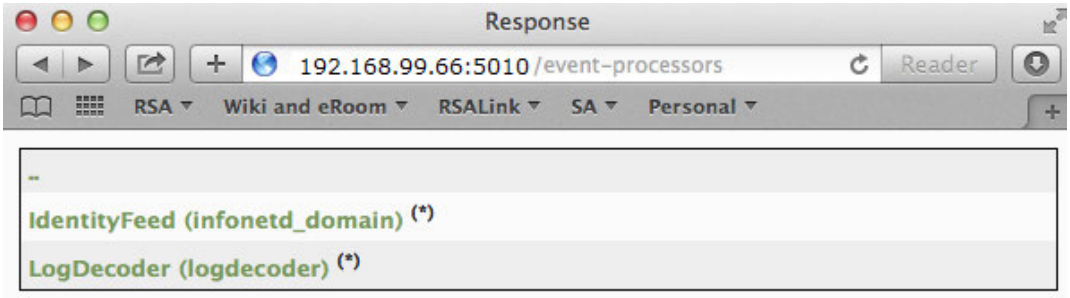
   b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.



   c. Open up a web browser (Non-Internet Explore browsers preferred) and log in to the REST interface of the Log Collector. Use administrative credentials when logging in. For example, if the IP address of your log collector is 192.168.99.66, the URL would be:

- SSL not enabled: **http://192.168.99.66:50101/event-processors**
- SSL enabled: **https://192.168.99.66:50101/event-processors**

The browser screen should look like this:

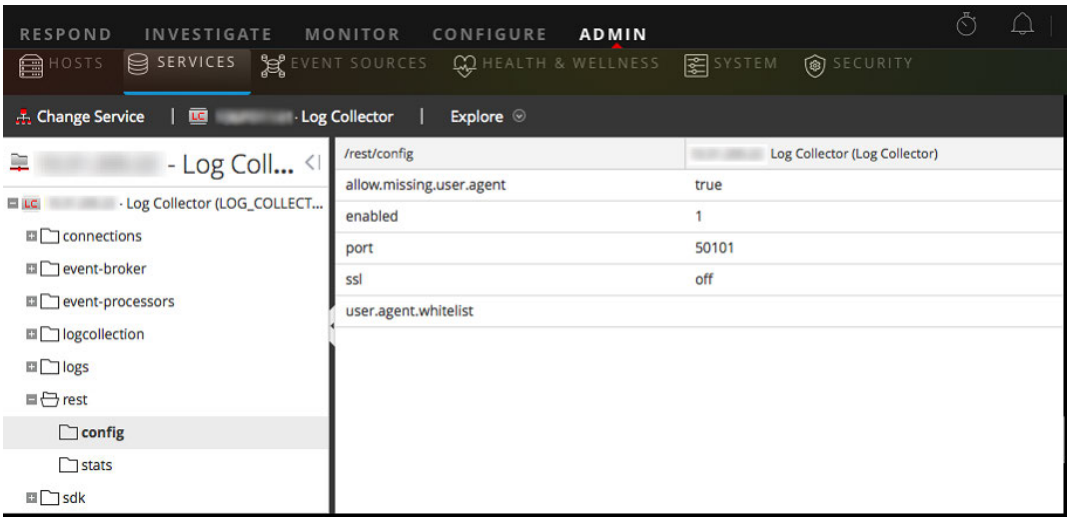


Notice the screen contains the name of the identity feed you created earlier (`infonetd_domain`, in this example).

For the identity feed to function correctly, port 50101 must be active on the Log Collector, and you must determine whether SSL encryption is active.

d. Go to **AdMIN > Services > *<Log Collector being setup>*** **> View > Explore**.

e. In the left pane, expand **rest > config**.



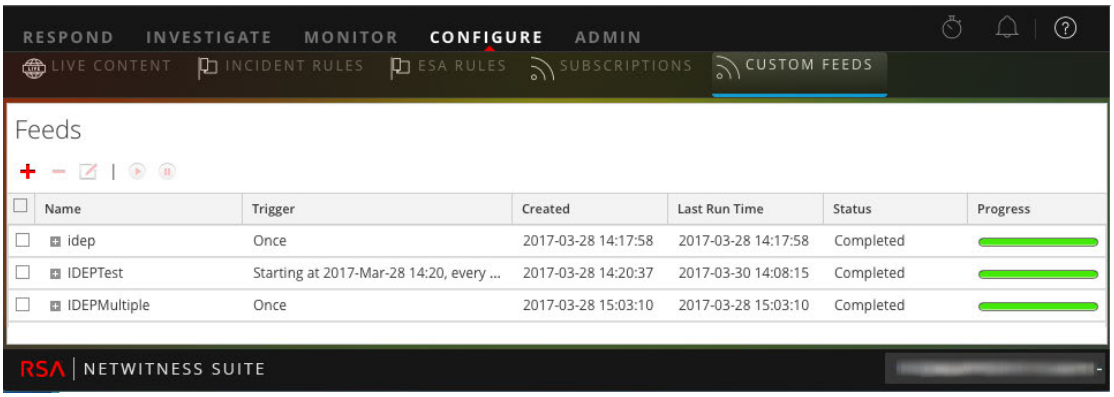
For REST to be active, **enabled** must be set to **1**.

f. Note the value for **ssl**. If SSL should be enabled for your environment, this must be set to **on**.

> **Note:** If you changed the setting for either the **enabled** or **ssl** option you must restart the Log Collector service before moving forward.

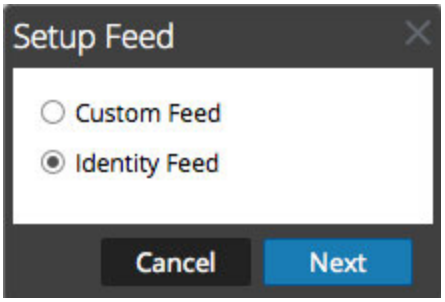
3. Go to **CONFIGURE > Live Content > Custom Feeds**.

   The Feeds grid is displayed.



4. In the toolbar, click +.

   The Setup Feed dialog is displayed.



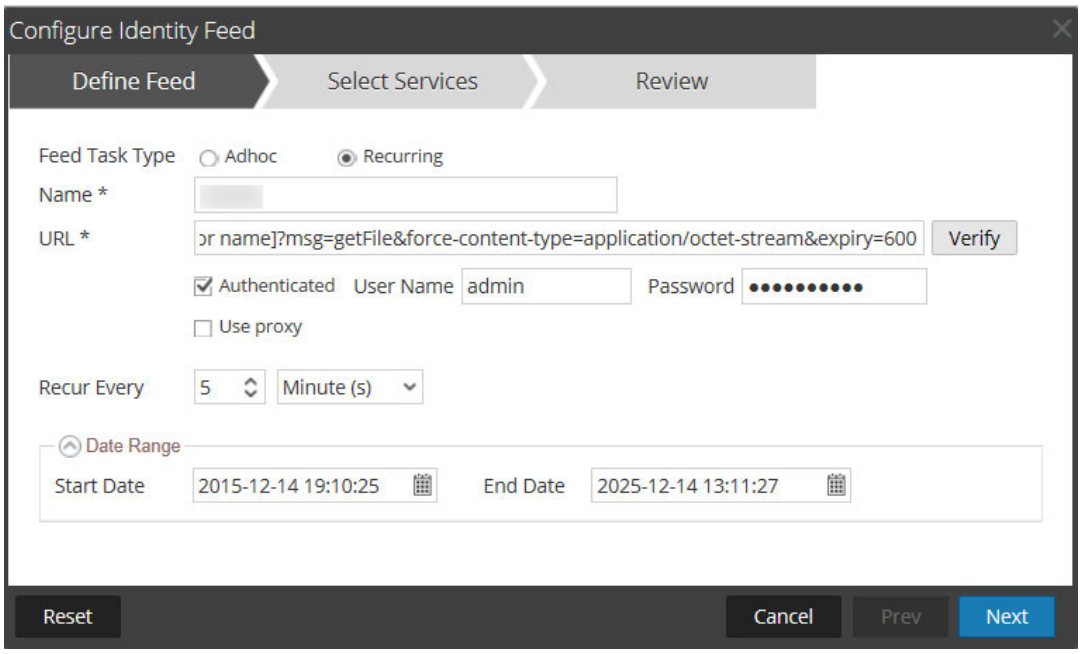
5. Ensure **Identity Feed** is selected and click **Next**.

   The Configure Identity Feed panel opens with the **Define Feed** tab displayed.

6. (Conditional) You can create an on-demand or recurring feed.

   - To define an on-demand Identity feed task that executes once, select **Adhoc** in the **Feed Task Type** field, type the feed **Name**, and browse for and open the feed.
   - To define a recurring Identity Feed task that executes on a recurring basis, select **Recurring** in the **Feed Task Type** field.

     The **Define Feed** form includes the fields for a recurring feed.



Note: RSA NetWitness Suite verifies the location where the file is stored, so that Security Analytics can check for the latest file automatically before each recurrence.

7. Fill in and verify the URL field.

   a. In the **URL** field, enter the URL where the feed data file is located. This is the REST API interface that was setup earlier. You need to know the following information to construct the URL:

   - The IP address of the log collector being used to construct the Identity Feed file.
   - The identity queue name, as set in step 2c.
   - Whether or not SSL is enabled on the log collector REST port, as set in step 2f.

   You construct this value as follows:

   - SSL enabled: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
   - SSL not enabled: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

   So, using our example from earlier, the complete value that you would enter into this field is as follows:

```
http://192.168.99.66:50101/event-processors/infonetd_
domain?msg=getFile&force-content-type=application/octet-
stream&expiry=600?msg=getFile&force-content-
type=application/octet-stream&expiry=600
```

b. For the URL verification to work correctly, it is important that the Security Analytics UI server can access the log collector's REST API port (50101). This can be tested by going to the Security Analytics UI server via SSH. Once there, run the following command:

- SSL enabled: `curl -vk https://<ip of log collector>:50101`
- SSL not enabled: `curl -v http://<ip of log collector>:50101`

If the `curl` command does not connect then there may be a network firewall or routing issue between the Security Analytics UI server and the Log Collector.

Example of Bad connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... No route to host
* couldn't connect to host
* Closing connection #0
curl: (7) couldn't connect to host
```

Example of Good connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... connected
* Connected to 192.168.99.66 (192.168.99.66) port 50105
(#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2
> Host: 192.168.99.66:50105
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Content-Length: 71
< Connection: Keep-Alive
< Pragma: no-cache
```

```
< Expires: -1
< Cache-Control: no-cache, no-store, must-revalidate
< WWW-Authenticate: Basic realm="NetWitness"
< Content-Type: text/xml; charset=utf-8
<
<?xml version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
* Connection #0 to host 192.168.99.66 left intact
* Closing connection #0
```

8. The REST API requires a username and password when attempting to pull the `identity_deploy.csv` file from the log collector. This can be any username and password that is available on the service itself. For details, see the "Services Security View" topic in the *Hosts and Services Guide*.

   To see which accounts are available, go to **ADMIN > Services > <log collector being setup> > Actions > View > Security**.

   Under the Users table, you see all the users that can be used in this step. It is suggested that a separate user account is created specifically for this setup, and is used nowhere else in the environment, for added security. For details, see "Add a User and Assign a Role" in the *System Security and User Management Guide*. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

9. To define the interval for recurrence, do one of the following:

   - Specify the number of minutes, hours, or days between recurrences of the feed.
   - To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.

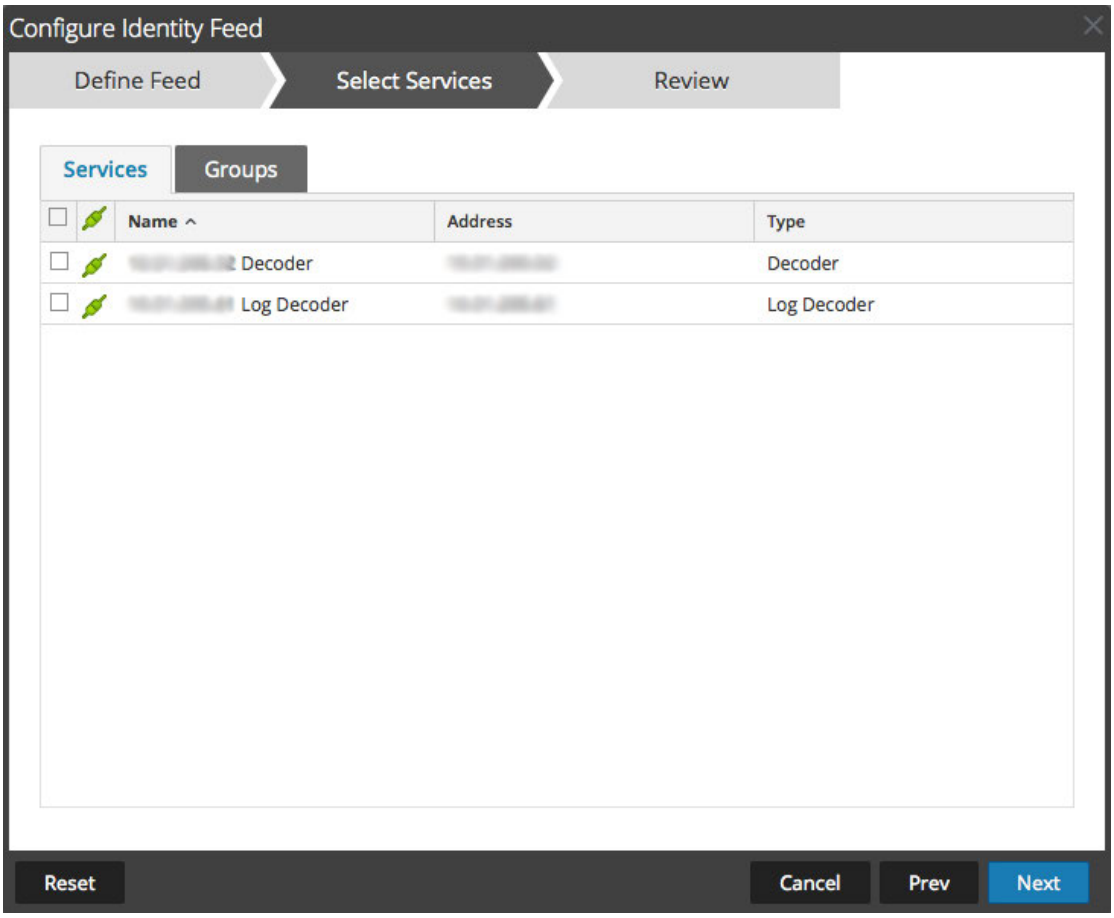
10. If using SSL encryption, you need to install the REST API SSL certificate for the log Collector into the Security Analytics UI server. For details, see Import the SSL Certificate.

    If, after importing the SSL certificate, the verification of the URL still fails, see Cannot Verify Identity Feed URL.

11. Click **Verify** to verify your identity feed configuration before you proceed to the Select Services form.

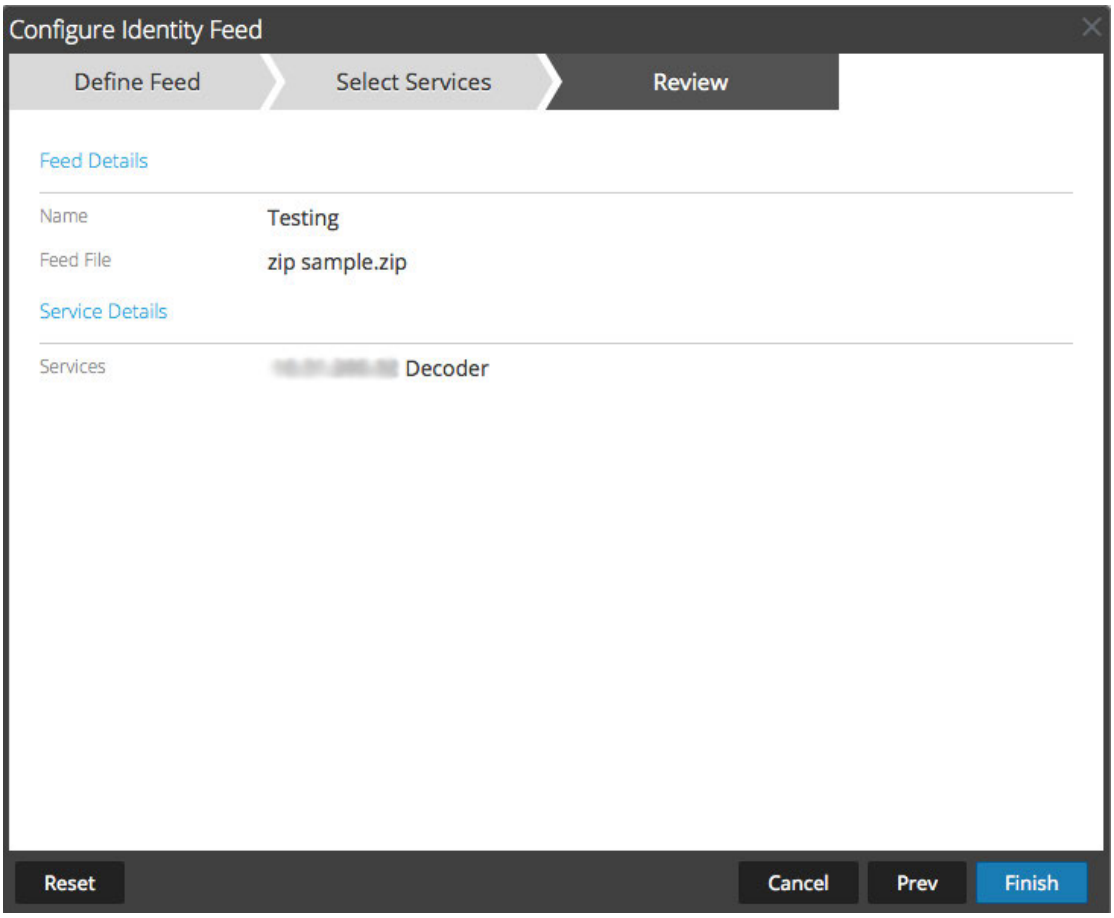
12. Click **Next**.

    The Select Services form is displayed.



13. To identify services on which to deploy the feed, select one or more Decoders and Log Decoders and click **Next**.
14. Click the **Groups** tab, select a group, and click **Next**.

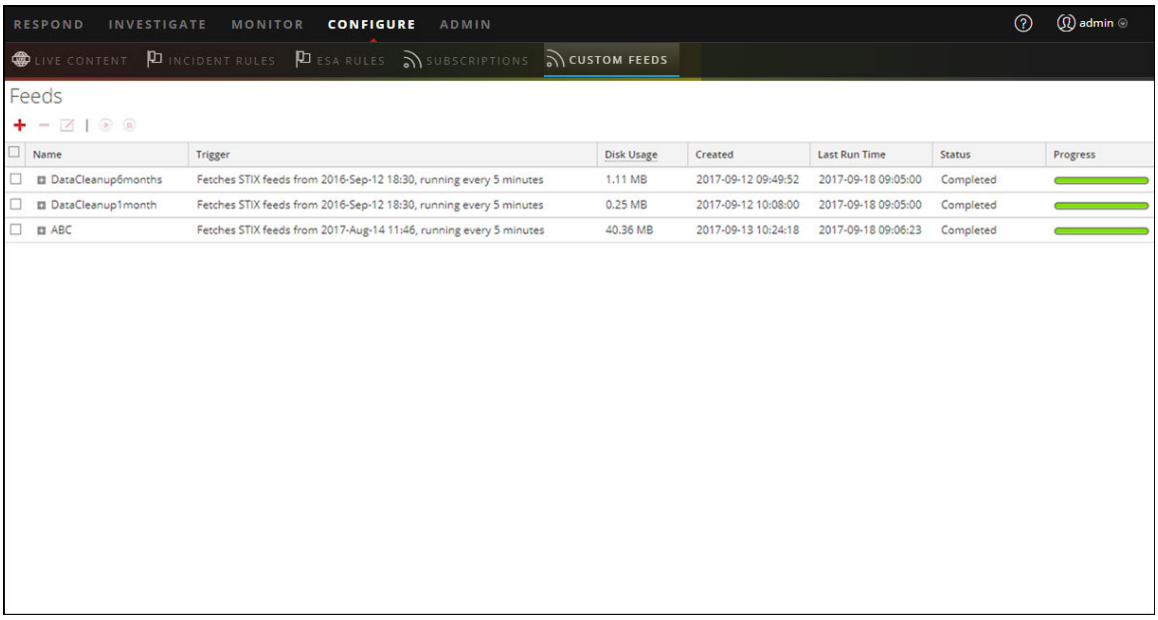
    The Review form is displayed.



Note: If a group of devices with Decoders and Log Decoders is used to create recurring or custom feeds and this group is deleted, you can edit the feed and add a new group to the feed.

15. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form).
16. Review the feed information, and if correct, click **Finish**.

Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.



Import the SSL Certificate

If SSL is configured on the Identity feed's Log Collector, follow these steps to import the Log Collector's SSL certificate into the Security Analytics UI server key store. If this certificate is not imported, the Security Analytics UI server will be unable to pull the Identify feed file from the Log Collector.

1. To pull the SSL certificate off the log collector, SSH into the Security Analytics UI server and run the following command:

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne
   '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/<SERVERNAME>.cert
   ```

   This command saves the SSL certificate to `/tmp/<SERVERNAME>.cert`.

   For example:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed
   -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/logcollector.cert
   ```

2. To import the SSL certificate into the Security Analytics UI server, SSH into the UI server and run the following command:

   ```
   keytool -importcert -alias <name an alias for the cert> -file
   <the cert file pathname> -keystore /etc/pki/java/cacerts
   ```

   For example:

```
keytool -importcert -alias logcollector01 -file
/tmp/logcollector.cert -keystore /etc/pki/java/cacerts
```

3. The system requests a password. Enter the password for the keystore on the Security Analytics UI server, not for the jetty keystore. The default password is **changeit**.
4. Restart **jettysrv** to allow jetty to read the new certificate in the store.

Cannot Verify Identity Feed URL

If the Identity feed URL cannot be verified, and you are using SSL, make sure you followed the steps in Import the SSL Certificate.

If there are still issues, it is possible that the internal name of the certificate does not match the hostname of the log collector. The following procedure checks this.

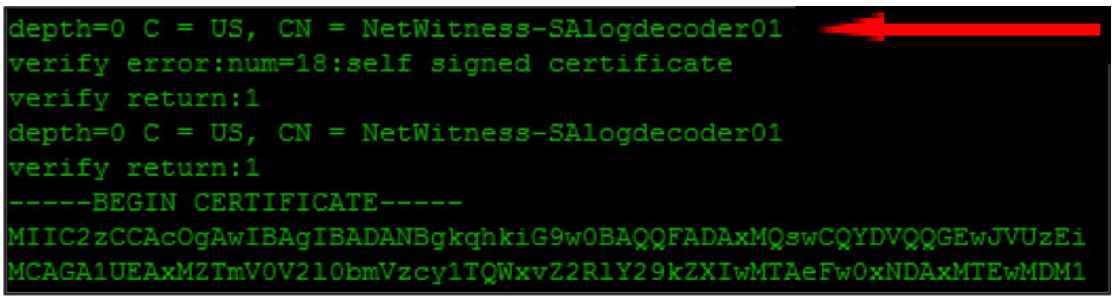
1. SSH to the Security Analytics UI server.
2. Run the following command to output the CN name of the SSL cert:

   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed
   -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

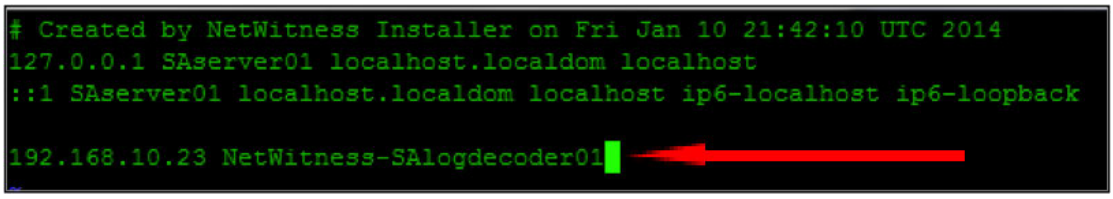
   Example:

   ```
   echo -n | openssl s_client -connect salogdecoder01:50101 |
   sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Retrieve the CN name of the SSL certificate.

4. Edit the `/etc/hosts` file and add the IP address and CN name to the file.

5. Restart the network service on the appliance.

6. Confirm that the name placed in the **/etc/hosts** file is used instead of the FQDN or IP address in the Identity feed URL.
7. Re-verify the Identity feed URL.

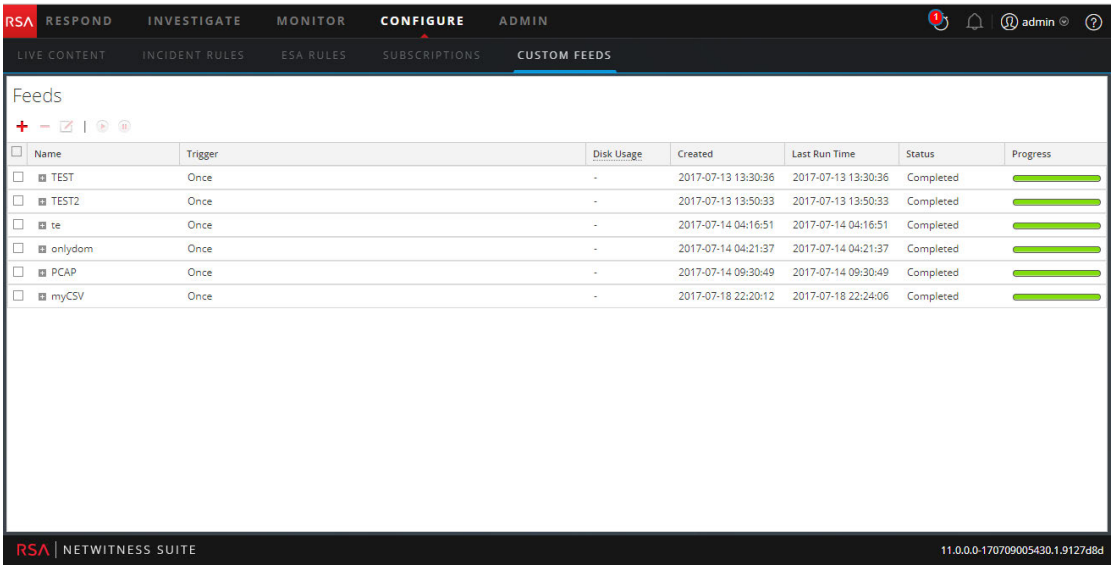
Edit, Upload, or Remove a Feed

You can upload a feed, edit an existing feed, or remove a feed.

To edit an existing feed:

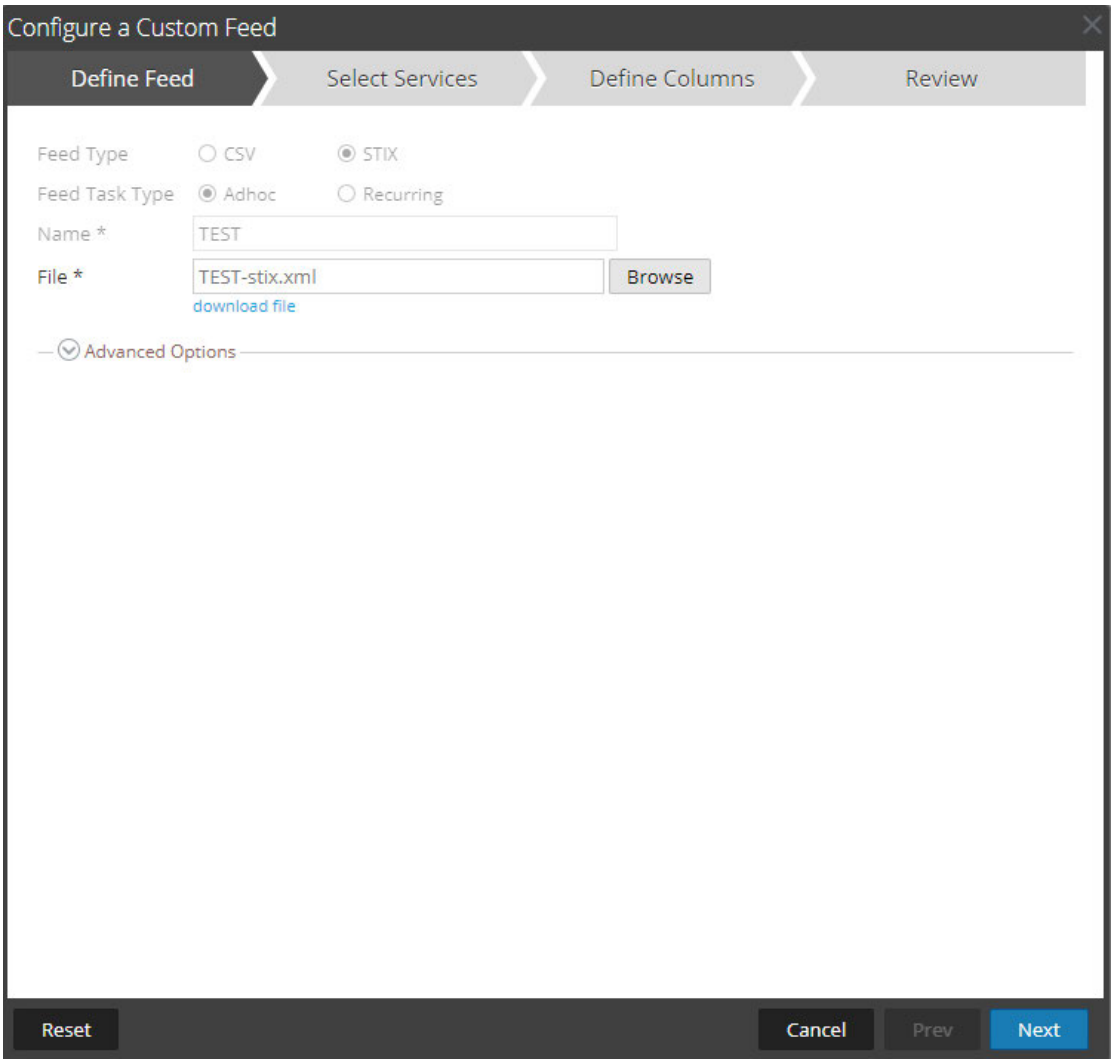
1. Go to **CONFIGURE > Custom Feeds**.

   The Feeds view is displayed.



2. In the toolbar, select a feed and click .

   The Configure Custom Feed or Configure Identity Feed panel opens in the Custom Feed wizard.



3. If you want to edit the feed file:
   a. Click **download file**.

      For an Identity feed, the .zip file is downloaded. For a custom feed, the .csv or .xml file is downloaded to your local file system. For a STIX feed, the .xml file is downloaded to your local file system.

   b. Edit and save the file.

   c. In the **Define Feed** tab, browse for and open the edited file.
4. Edit any other parameters in the **Define Feed** tab, **Select Services** tab, and **Define Columns** tab that apply to the type of feed.
5. Anytime before you click **Finish**, you can:

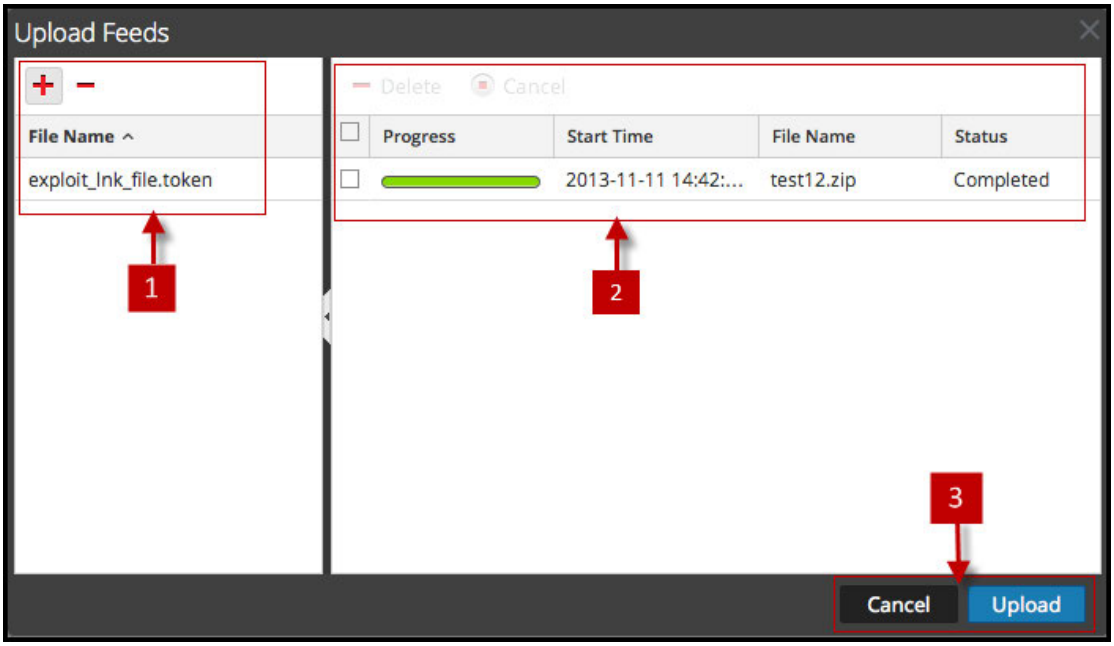
- Click **Cancel** to close the wizard without saving your changes.
- Click **Reset** to clear the data in the wizard.
- Click **Next** to display the next form (if not viewing the last form).
- Click **Prev** to display the previous form (if not viewing the first form).

6. In the **Review** tab, review the feed information, and if correct, click **Finish**.

The feed is recreated with the updated file and new feed specifications. The feed is added to the Feeds list and progress bar tracks completion. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file is listed in the Feeds list. You can expand or collapse the entry to see how many services are included, and which services are successful.

To upload a feed to a Dcoder or Log Decoder:

1. Go to **ADMIN > Services**.
2. Select a service and click > **View** > **Config**.
   The Services Config view is displayed with the General tab open.
3. Select the **Feeds** tab.
4. In the Feeds tab toolbar, click Upload.
   The Upload Feeds dialog is displayed.

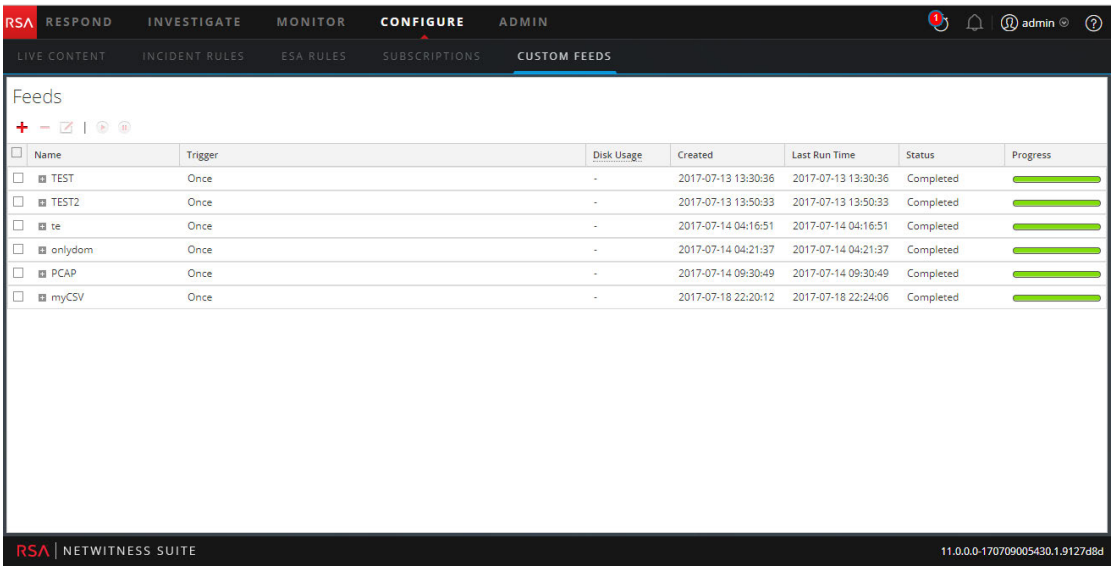


5. In the **File** grid, click + and select a feed file. Supported files are *.feed, *.token, and *.filter.

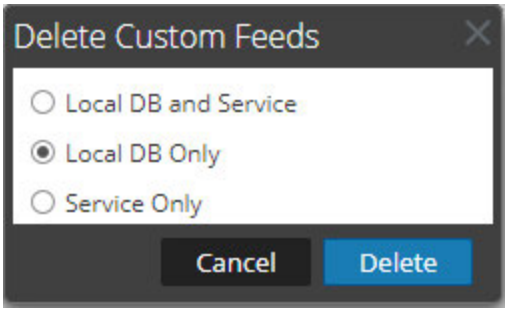
6. Select the feed file from the **File** list and click **Upload**.
   The Upload Job list is updated to show the progress and status of the uploaded feed.

To remove a feed:

1. Go to **CONFIGURE > Custom Feeds**.
   The Custom Feeds view is displayed.



2. In the toolbar, select a feed and click − .
   The Delete Custom Feeds dialog is displayed.



   You can select one of the following options to delete the feed:

   - If you choose to delete the feed from **Local DB and Service**, the feed is deleted from both the service and the local NetWitness Suite box. The deleted feed will no longer seen on the NetWitness Suite user interface.
   - If you choose to delete the feed from **Local DB Only**, the feed is deleted from the local NetWitness Suite box. The deleted feed will not be seen on the NetWitness Suite user

interface; however, the last deployed version of the feeds will be present on the service. The undeployed feeds will be deleted forever.

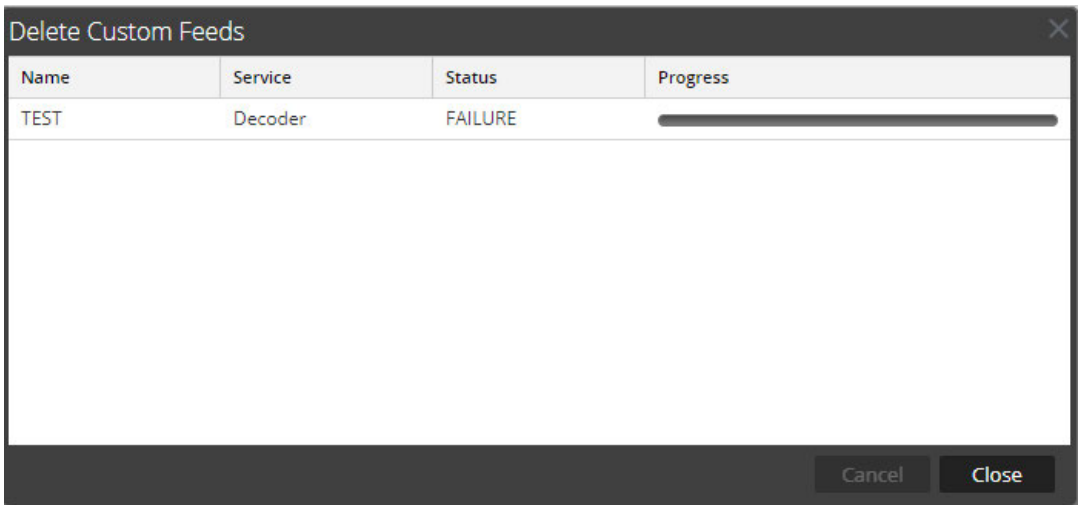
- If you choose to delete the feed from **Service Only**, the feed is deleted from the service. The deleted feed will appear on the NetWitness Suite user interface and can be deployed again

3. Select where you want to delete the feed and click **Delete**.

   A warning dialog is displayed.

4. Click **yes** to confirm that you want to delete the feed from the select areas.

   - If you chose to delete the feed from the **Local DB Only**, the feed is deleted.
   - If you chose to delete the feed from the **Local DB and Service** or **Service Only**, the Delete Custom Feeds view is displayed showing the progress of the deletion on the service.



Create Custom Meta Keys Using a Custom Feed

This topic provides information on how to add custom meta keys, using a custom feed in the Log Decoder.

You can create custom meta keys to retrieve data, to investigate and analyze the logs and packets. Custom meta keys enable you to add an enrichment context for the log and packet data. This document highlights the configuration changes to reflect the custom meta keys in the Concentrator, ESA, Archiver, Warehouse Connector, and Reporting Engine schema.

Here is a example of creating the custom meta key in the Log Decoder. In this scenario, an organization wants to track the location of an asset such as a printer. So, a custom meta key **source location** is introduced, which indicates the location of the asset, for example Printer1, which is located in the 'Fifth Floor A wing'.

Note: Custom meta keys can be created in the Decoder as well. Select the `index-decoder-custom.xml` file when you create a custom meta in the Decoder.

Add a Custom Meta Key in the Log Decoder

To add custom meta keys using custom feed:

1. Go to **ADMIN** > **Services** > **Log Decoder.**
2. Select a service and click > **View** > **Config** > **Files** tab > **index-logdecoder-custom.xml.**

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

3. Restart the Log Decoder service. In the Services view, click > **Restart**.

Deploy a Log Decoder Feed in Live

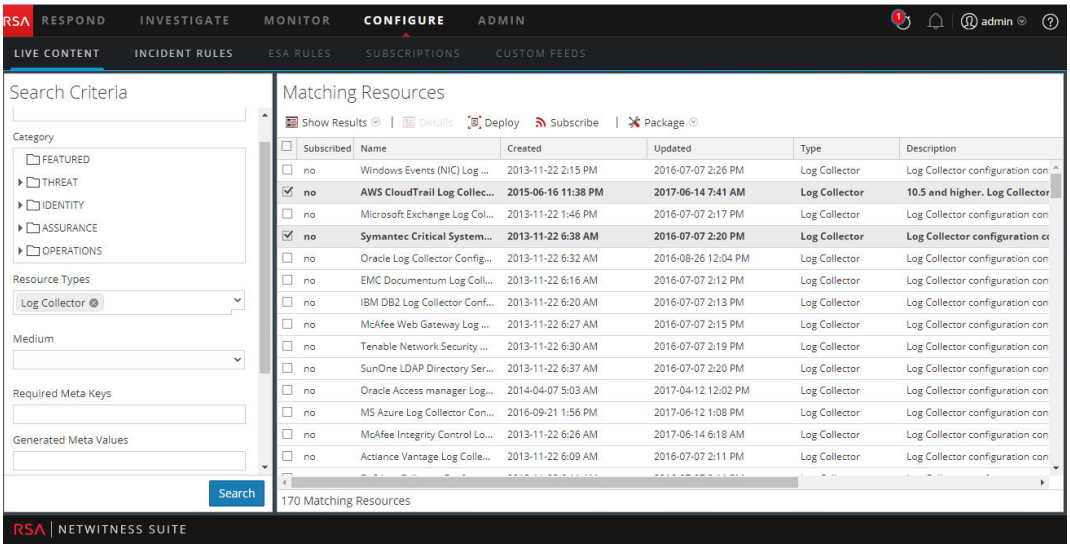
To deploy the feed in the live environment:

1. Go to **CONFIGURE > Live Content.**
2. Select a group of resources, or a previously-created resource package. To select a resource or group of resources:

a. In the **Live Search View,** browse Live resource (for example, search for the **Log Collector** resource Type).

b. In the **Matching Resources** panel, select **Show Results > Grid**.

c. Select the checkbox to the left or the resources that you want to deploy.

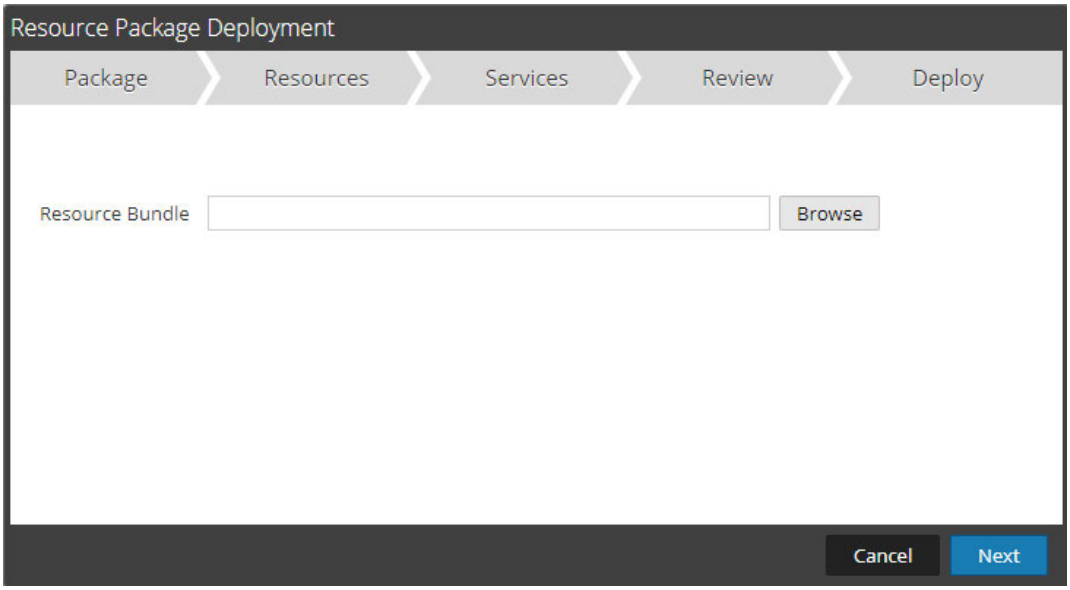


d. In the Matching Resources toolbar, click

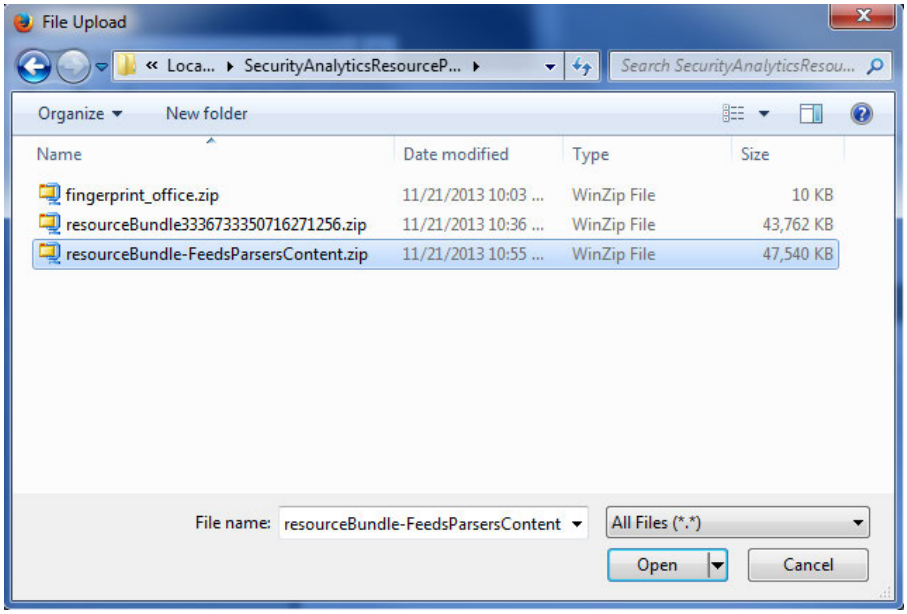
.

3. To select a resource package to deploy:

a. In the **Live Search** view **- Matching Resources** toolbar, select **Package** > **Deploy** : The Package page of the Resource Package Deployment wizard is displayed.



b. Click **Browse** and select a package from your network (for example **resourceBundle-FeedsParsersContent.zip**).



c. Click **Open.**

At this point, whether you are deploying a package or a group of resources, the Deployment Wizard opens, and the Resources page is displayed.

3. Click **Next**.

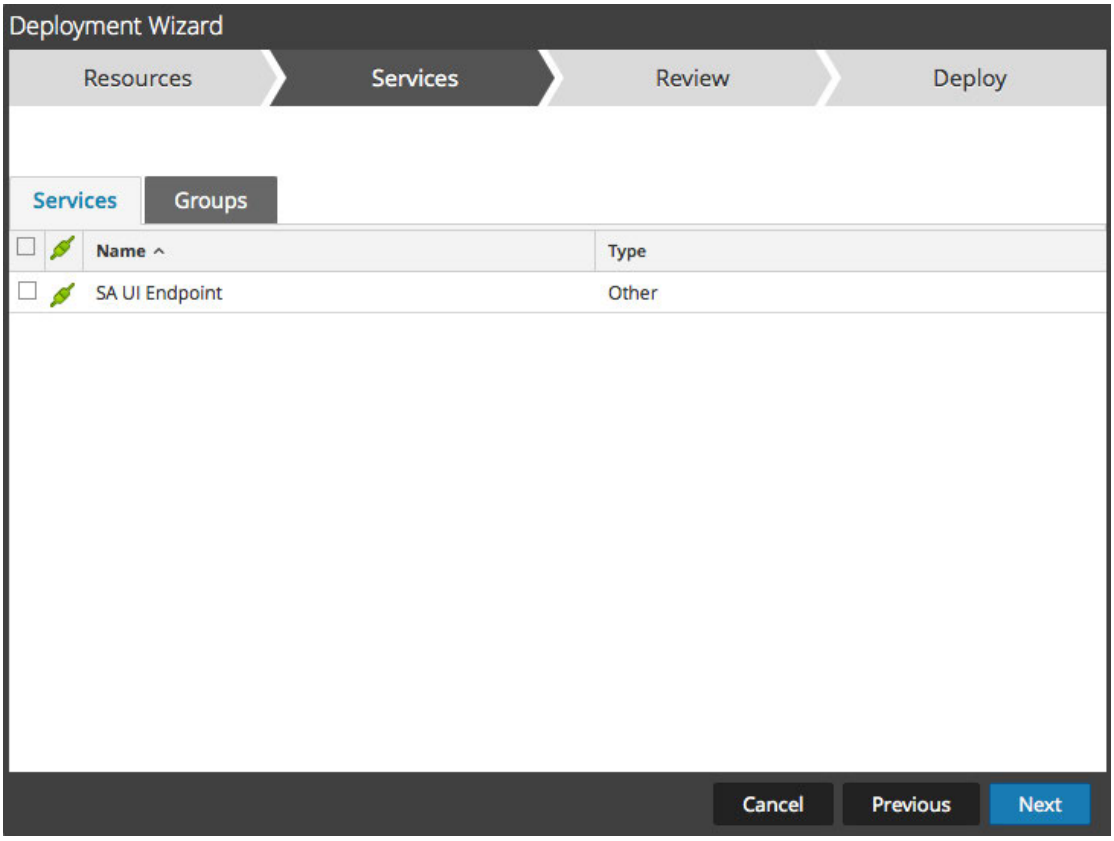
The **Services** page is displayed that has two tabs, **Services** and **Groups**, which provide a list of services and service groups that are configured in the Admin > Services View. The columns are a subset of the columns available in the Services View.

Note: The Live server is "smart" about deploying resources to Services. For example, it does not deploy resources that have a Medium of packets to any Log Decoders. This means that only applicable content resources are deployed to each Service.

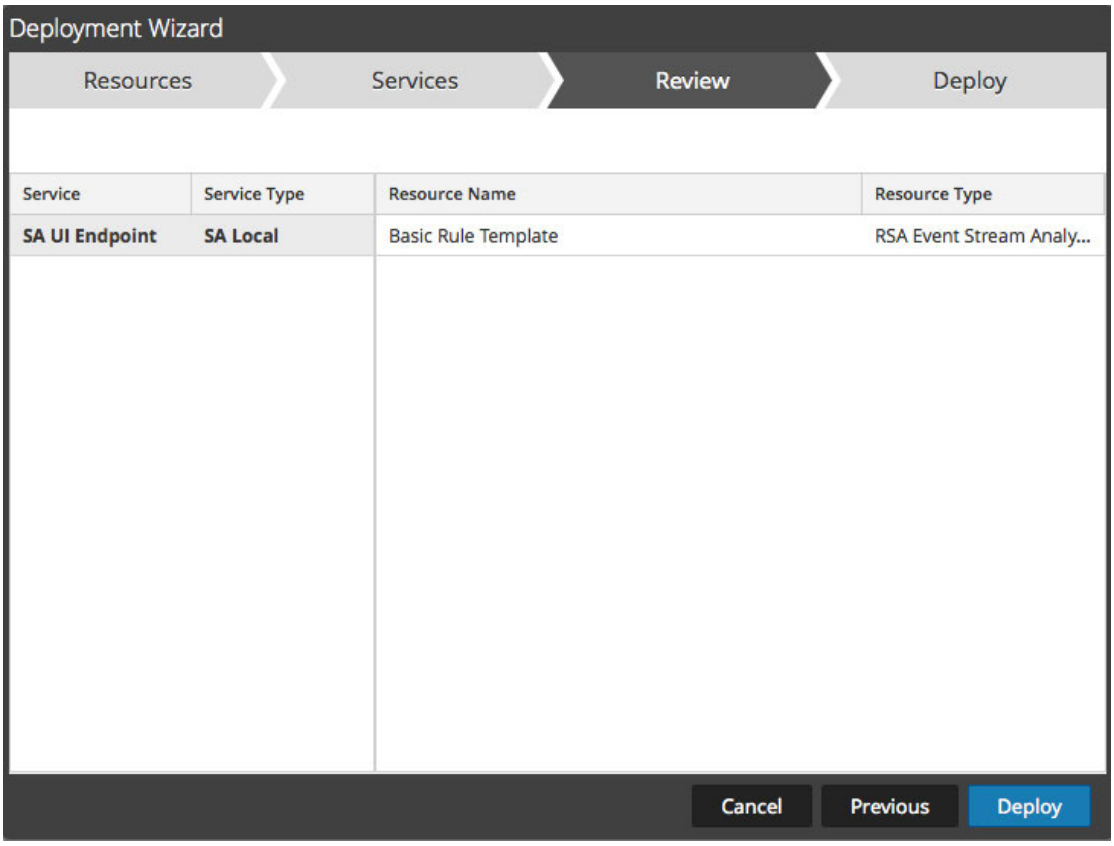
4. Select the services to which you want to deploy the content. You can select any combination of services and service groups.

Use the **Services** tab to select individual services, list of services and service groups that are configured in the Admin Services view.

Use the **Groups** tab to select groups of services.

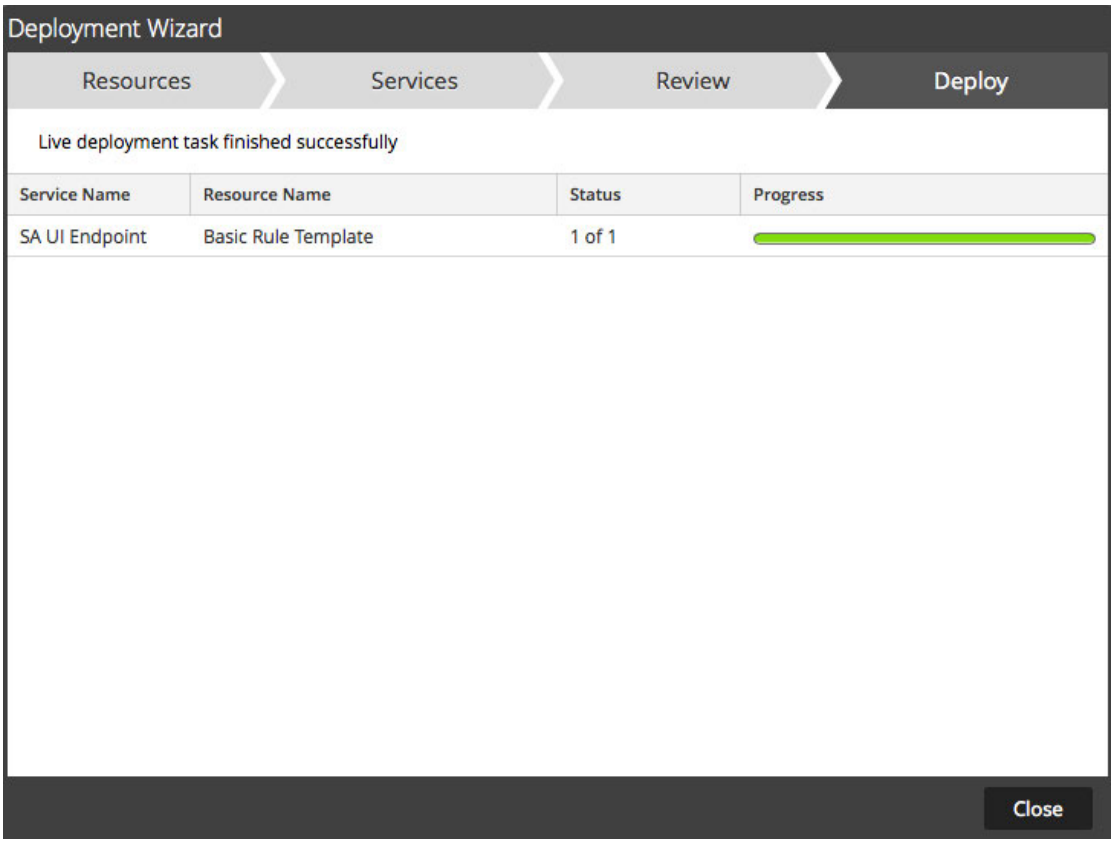


5. Click **Next**.
   The **Review** page is displayed.

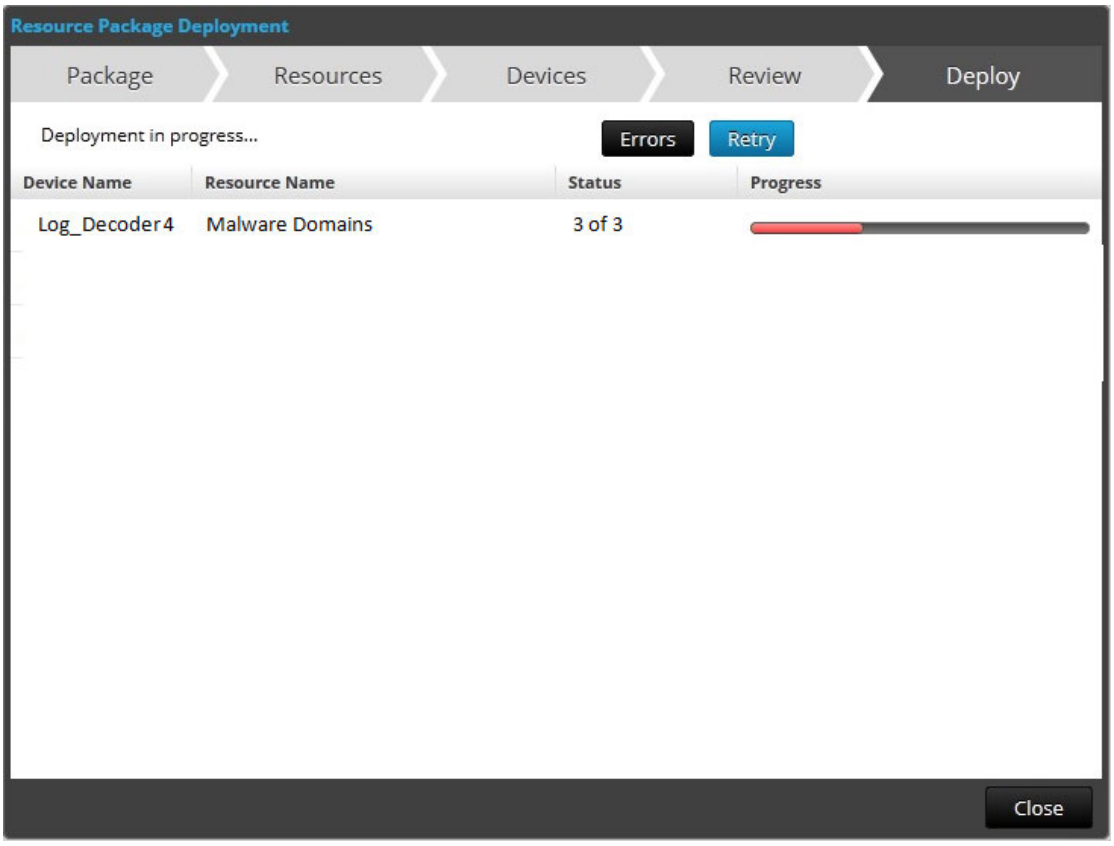


Make sure that you have selected correct resources and the services to which you want to deploy them.

6. Click **Deploy**.
   The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.



If you try to deploy resources and services that are not compatible, NetWitness Suite displays the Errors and Retry buttons, which you click to review the errors and re-attempt the deployment.



7. Click **Close**.

Note: The Source IP should be indexed by selecting the type as 'IP' as the ip.src. and ip.dst are in IPv4 format.

In this scenario, a custom meta key location.src (location source) is added by indexing the hostname (alias.host). In this example, the printer hostname are populated in meta key 'alias.host'. So, select 'alias.host' as callback key, and index type as 'Non IP' in the Feed Wizard as shown below. In the Define Values section, select the custom meta key from the drop down menu.

Add the Custom Meta Key Entry in the Concentrator Custom Index file

To add the custom meta entry in the concentrator custom index file:

1. Go to **ADMIN** > **Services** > **Concentrator**.
2. Click > **View** > **Config** > **Files** tab > **index-concentrator-custom.xml.**
3. Add the custom meta key entry in the Concentrator index file.

```
 <Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
   <!-- Reserved Meta key for Feed -->
   <Key description="Source Location"  level="IndexValues"
name="location.src" format="Text"  valueMax="10000"
defaultAction="Open"/>
  </Language>
```

4. To restart the Concentrator service, in the Services view, click > **Restart**.

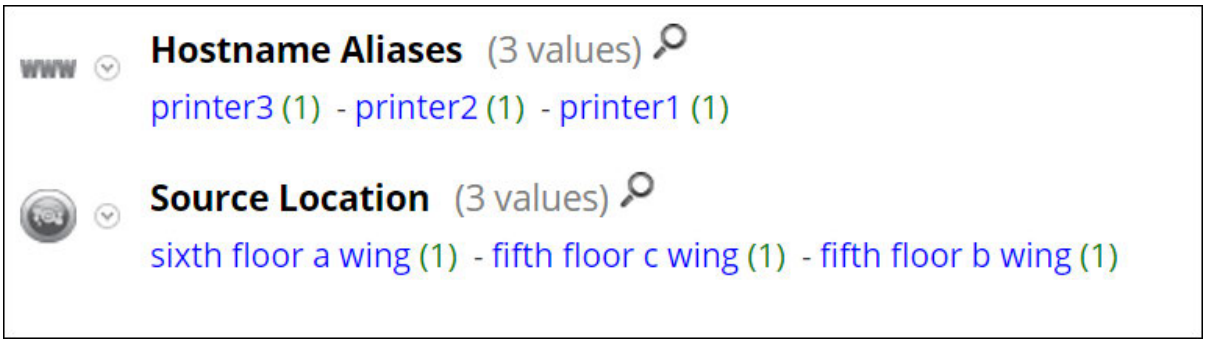
Note: In case of the Broker, the Broker derives its index from the Concentrator from which it aggregates. So you do not need to create custom meta in the broker. If you have not indexed the meta key in the concentrator, the broker will not display in the investigation.

Investigate on the Custom Meta Key

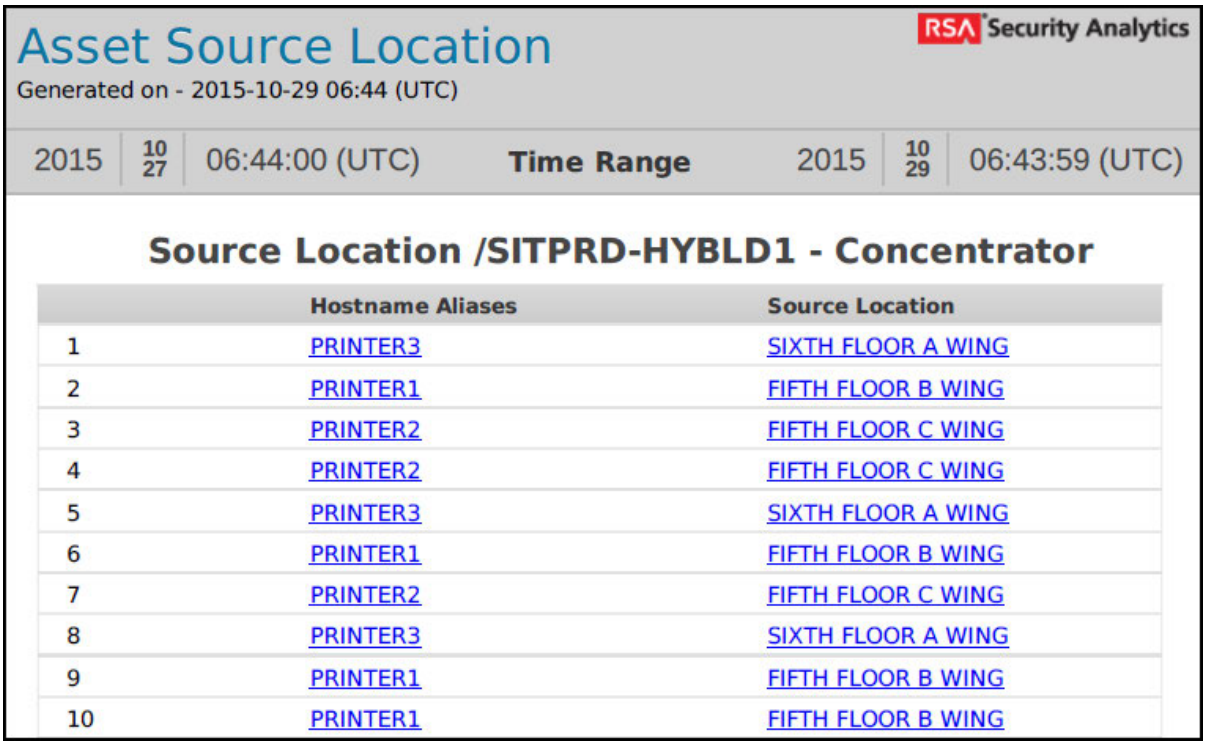
Note: You have to log out and log in from the NetWitness Suite User Interface, before you can view the custom meta key in Investigation.

To investigate on the custom meta key:

1. Go to **INVESTIGATE** > **Navigate**.
2. Select a Concentrator service, and click **Navigate**.



Here is an example of a report executed on the concentrator.



Asset Source Location

RSA Security Analytics

Generated on - 2015-10-29 06:44 (UTC)

2015	10 27	06:44:00 (UTC)	Time Range	2015	10 29	06:43:59 (UTC)

Source Location /SITPRD-HYBLD1 - Concentrator

	Hostname Aliases	Source Location
1	PRINTER3	SIXTH FLOOR A WING
2	PRINTER1	FIFTH FLOOR B WING
3	PRINTER2	FIFTH FLOOR C WING
4	PRINTER2	FIFTH FLOOR C WING
5	PRINTER3	SIXTH FLOOR A WING
6	PRINTER1	FIFTH FLOOR B WING
7	PRINTER2	FIFTH FLOOR C WING
8	PRINTER3	SIXTH FLOOR A WING
9	PRINTER1	FIFTH FLOOR B WING
10	PRINTER1	FIFTH FLOOR B WING

Additional Procedures

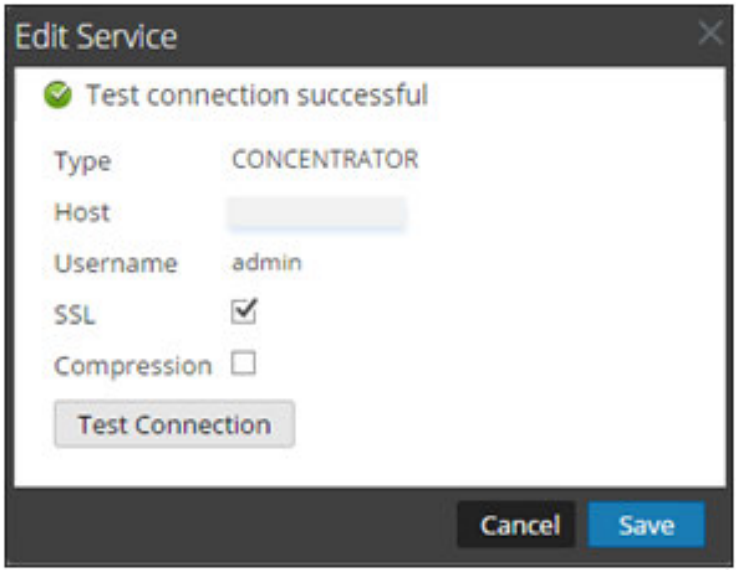
The following procedures must be executed if you have Warehouse Connector, Archiver, Reporting Engine and ESA configured.

Update the Schema in ESA

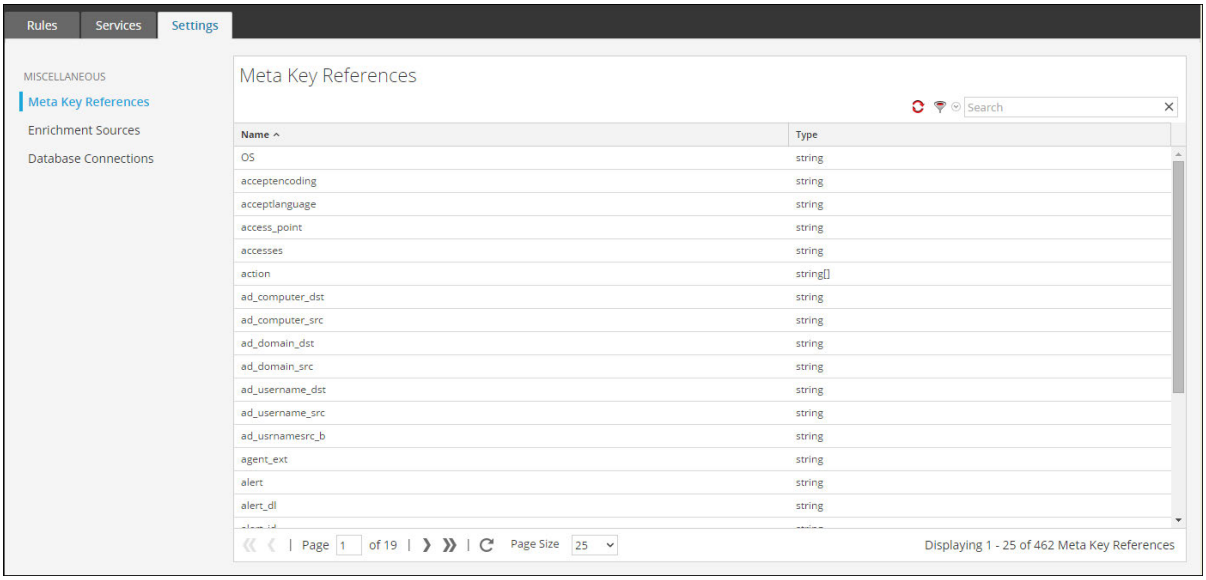
Before you update the schema in ESA, the custom meta key should be indexed in the concentrator.

To update the schema ESA rules and to be able to use the new custom meta keys:

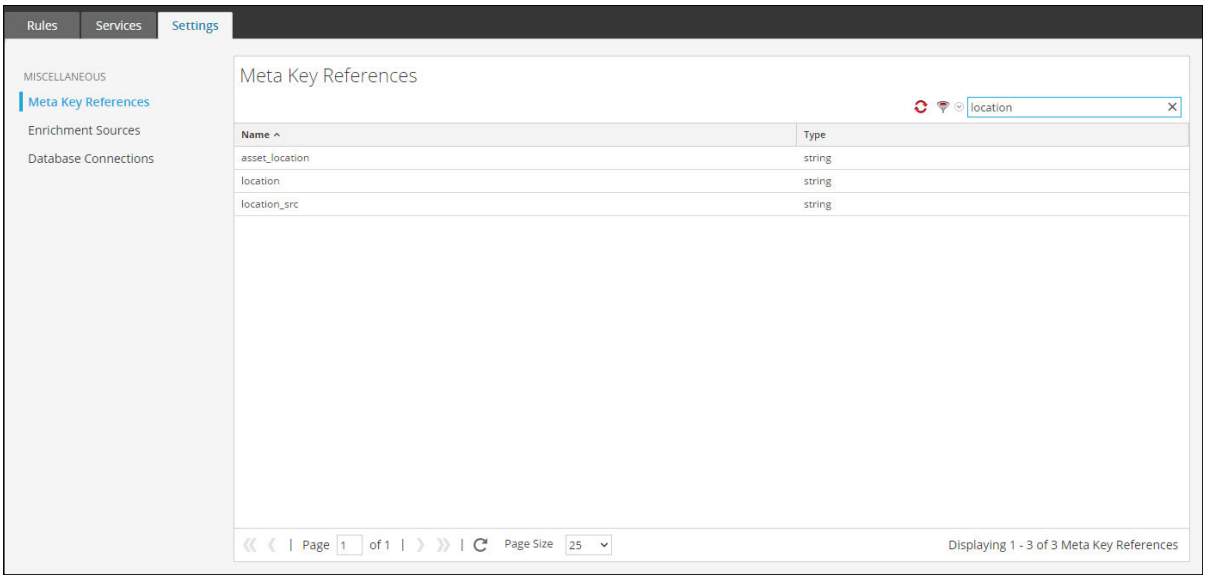
1. Go to **ADMIN** > **Services** > **ESA- Event Stream Analysis** > **View** > **Config**.
2. Edit the Concentrator Datasource.
3. Click **Test Connection.**



4. Click **Save** after the connection is successful.
5. Click **Apply**.
6. Navigate to **Alerts** > **Configure** > **Settings**.



7. Click the **Search** tab and search for the name of the custom meta key.
   The custom meta key name and type is displayed.



Update the Schema in Archiver

If you want to configure the Archiver, using the new custom meta keys, you need to update the Archiver schema in the Reporting Engine. To update the Archiver schema in Reporting Engine:

1. Go to **ADMIN** > **Services** > **Archiver**.
2. Select > **View** > **Config** > **Files** > **index-archiver-custom.xml**.
3. Add the custom meta key entry in the Archiver index file.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexValues"
name="location.src" format="Text"
  valueMax="10000" defaultAction="Open"/>
 </Language>
```

4. To restart the Archiver service, click > **Restart.**

   The Archiver schema is updated with the custom meta key.

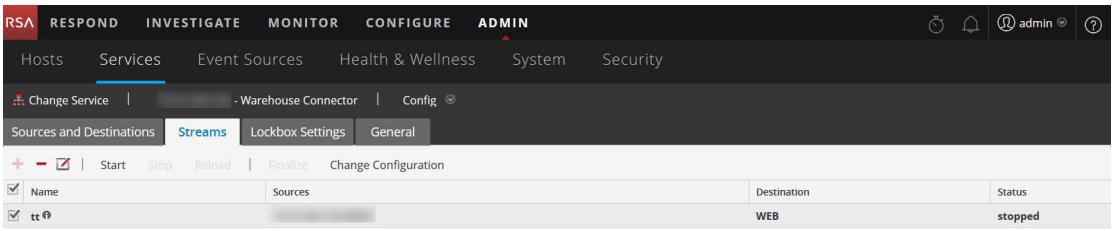
Update the Schema in Warehouse Connector

If you want to configure the Warehouse with custom meta and use it in warehouse report then you need to update the Warehouse schema in the Reporting Engine.

If the Log Decoder or Decoder, where the custom meta key is added, is one of the sources in the Warehouse Connector stream, you need to update the schema in the Warehouse Connector.

To update the Warehouse schema in the Reporting Engine:

1. Go to **ADMIN** > **Services** > **Warehouse Connector**.
2. Click ⚙ > **View** > **Config** > **Files** tab > **index-logdecoder-custom.xml.**
3. Select the stream and click **Reload**.
   The warehouse connector pulls the schema from the downstream devices (Log Decoder/Decoder).



For more information on streams, see "Configure Streams" in the *Warehouse Connector Configuration Guide*.

Update the Schema in Reporting Engine

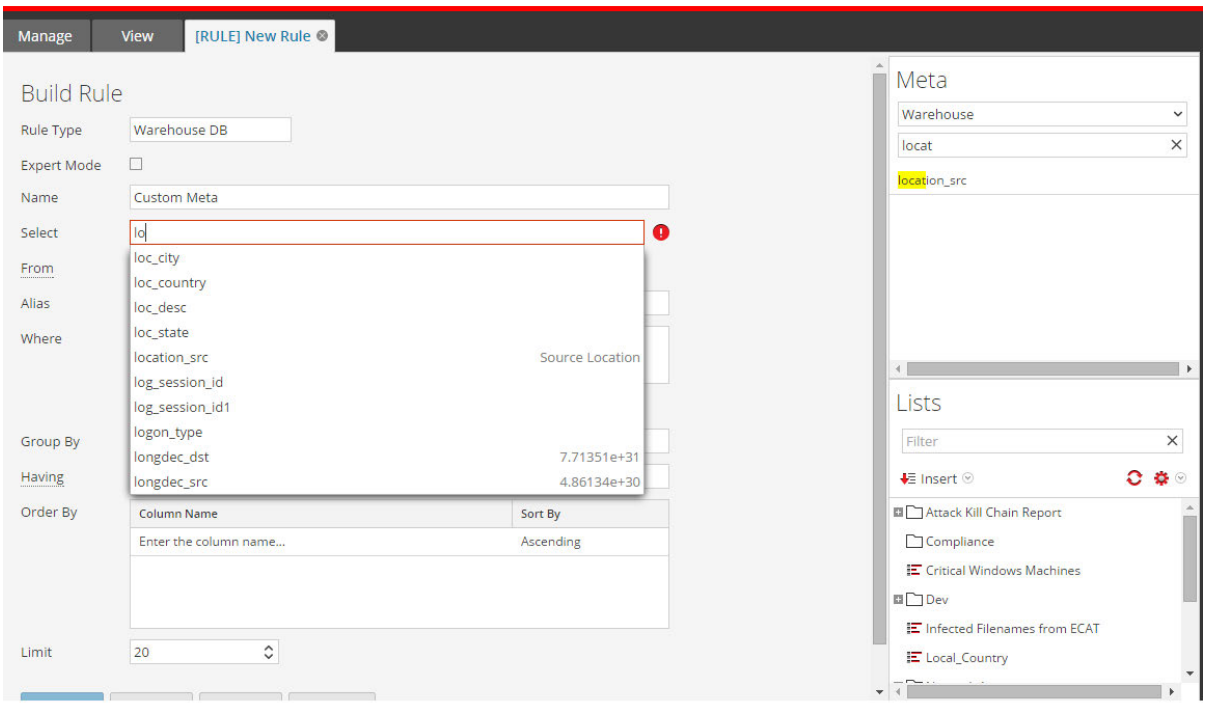
To update the schema in Reporting Engine:

1. Go to **ADMIN** > **Services** > **Reporting Engine.**
2. Click ⚙ > **Restart.**

Note: Restart the Reporting Engine or wait for thirty minutes for the schema to be updated.

To view the custom meta key:

1. Navigate to **Reports** > **Rules**.
2. In the toolbar, click +.
3. Select **Warehouse DB**.
4. In the Build Rule tab, search for the custom meta from the right panel.
   The custom meta key is displayed.



Upload and Delete Custom Parsers

RSA NetWitness Suite has the ability to upload parsers from your local system and delete these parsers.

Upload Parsers to a Decoder or Log Decoder

The Upload option in the Service Config view > Parsers tab displays the Upload Parsers dialog, in which you can manage the uploading of parsers to a Decoder or Log Decoder. In the File list, you prepare a list of parsers for uploading. You can add files from a directory structure, and delete files from the list if you decide that you don't want to upload a particular file. When the list is ready, clicking Upload starts the upload process.

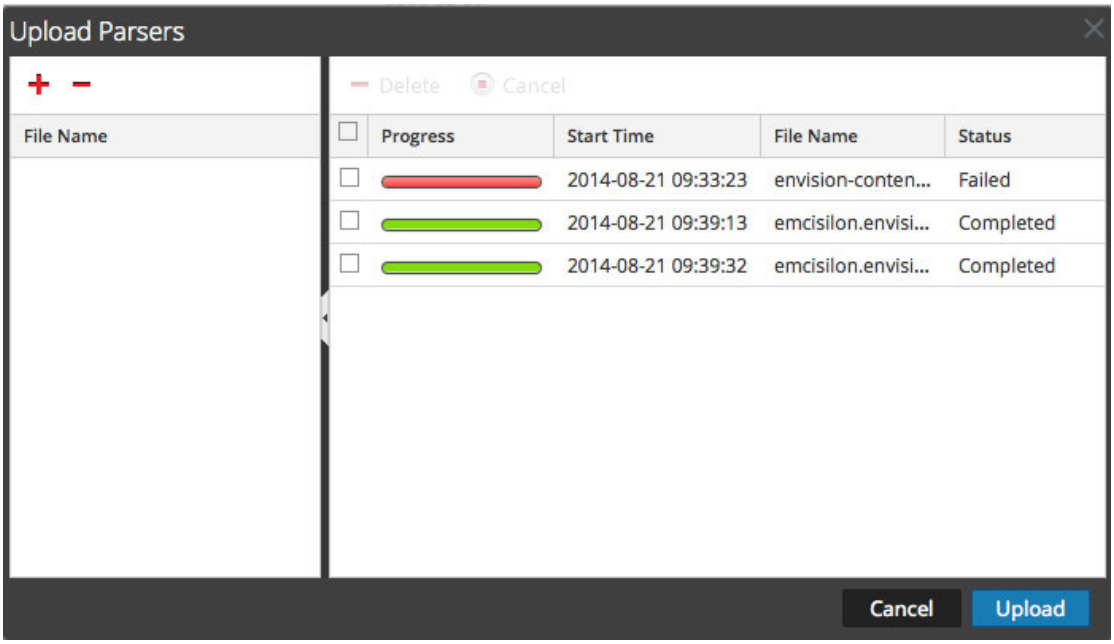
1. Go to **ADMIN > Services**, select a service, and > **View > Config.**

   The Config view for the selected service is displayed.

2. Click the **Parsers** tab.

3. Click Upload.

   The Upload Parsers dialog is displayed.

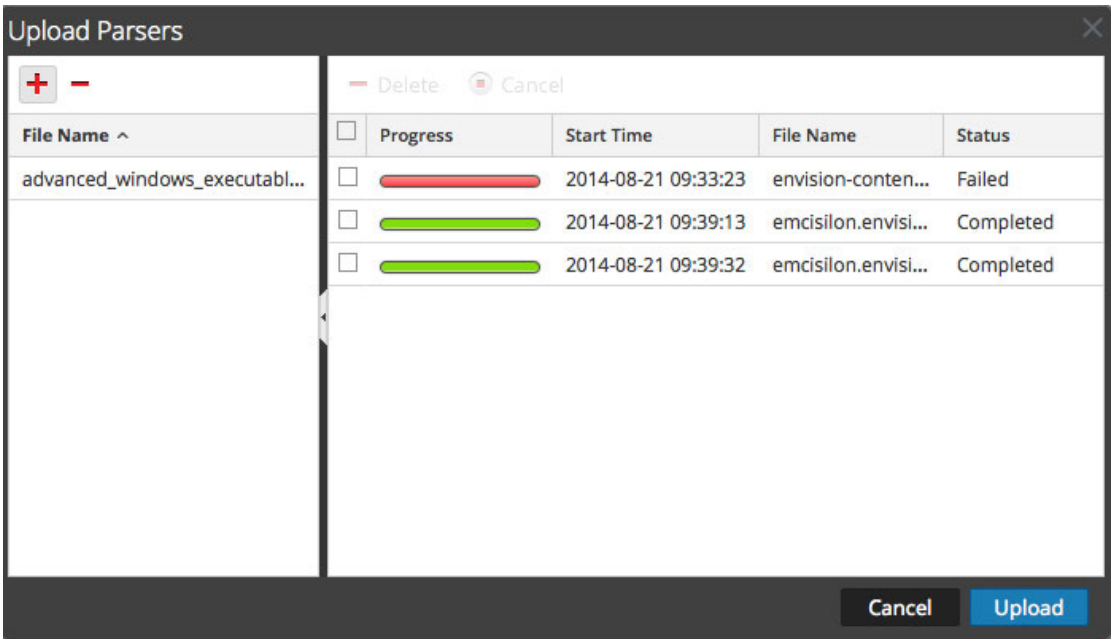


4. Click + .

   A file selection dialog is displayed.

5. Select the **.flex**, **.parser**, and **.lua** files to be updated, and click **Open**.

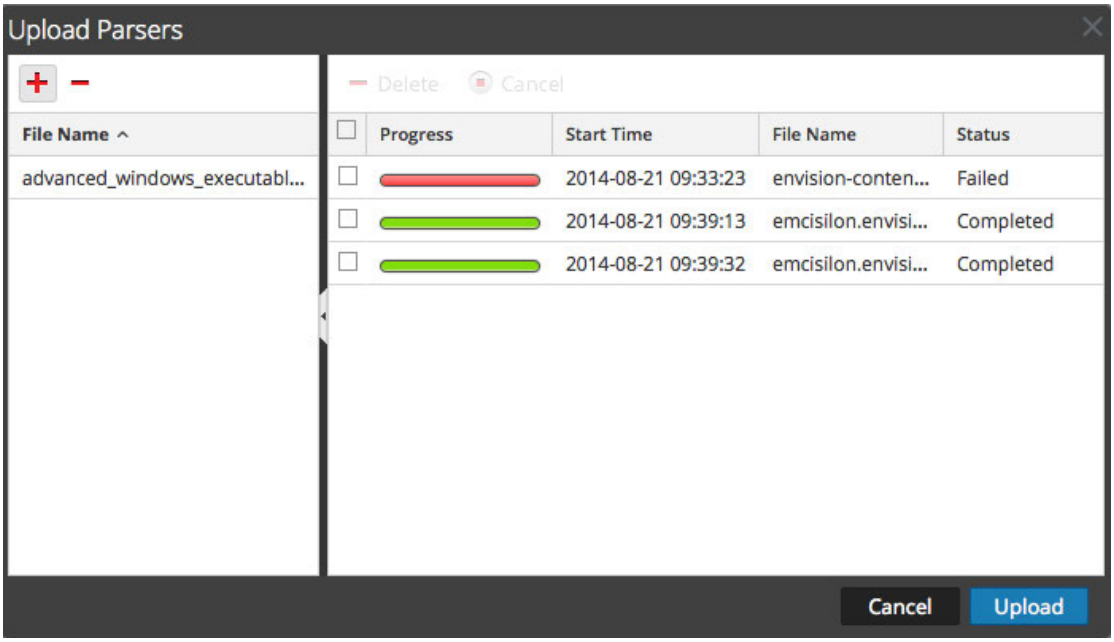
   The dialog closes, and the selected files are displayed in the File list.



6. Click **Upload**.

   The Upload Job grid shows the progress of the upload jobs with each job representing a file

being uploaded.



7. Use any of the Upload grid tools to manage the upload of selected jobs: pause and resume, cancel, and delete.
   Once a job is complete, it is deployed on the Decoder and listed with the deployed parsers in Parsers tab.

Manage Upload Jobs

You can use any of the Upload grid tools to manage the upload of selected jobs: pause, resume, cancel, and delete.

- To cancel uploading a set of parsers while the upload is in queue or progress, click Cancel.
- To pause uploading a set of parsers, if the upload is not yet complete, click Pause.
- To resume uploading a set of parsers after a pause, click Resume.
- To delete an upload job, click .

Delete Deployed Parsers

The Delete option in the Service Config view > Parsers tab provides a way to delete deployed parsers from a Decoder or Log Decoder. Parsers can be added and removed while a Decoder is running without affecting capture.

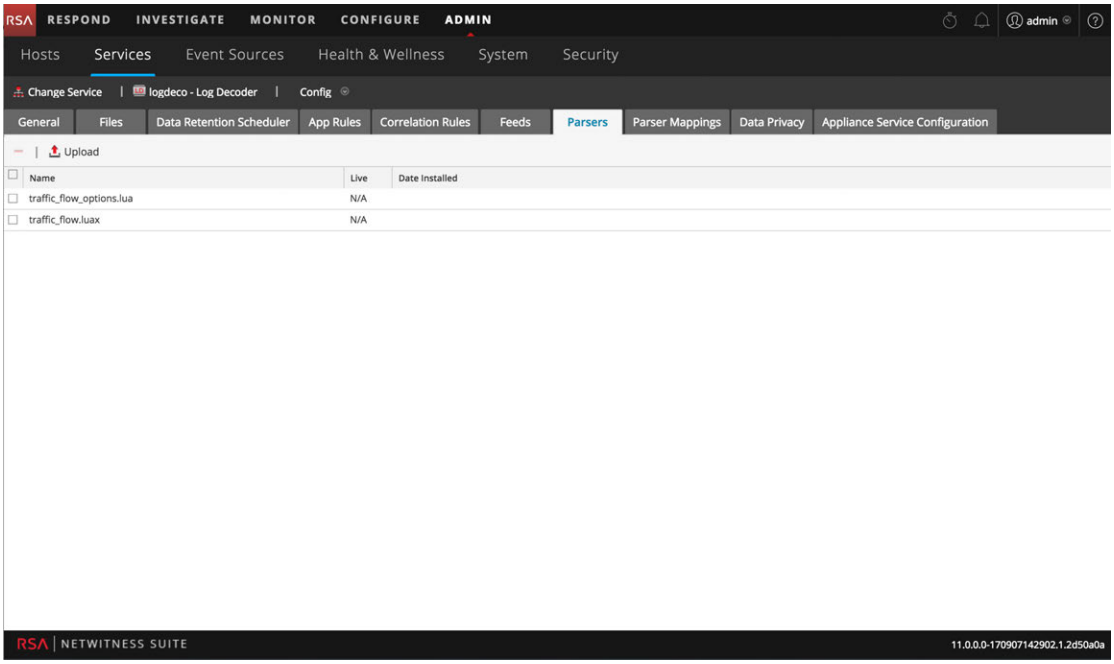
Note: Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.

To delete a parser from a Decoder:

1. Go to **ADMIN > Services**, elect a service, and > **View > Config.**

   The Services Config view for the selected service is displayed.

2. Click the **Parsers** tab.



3. In the **Parsers** tab, select one or more parsers to delete.

4. Click .

   A dialog requests confirmation that you want to delete the parsers.

5. If you want to delete the parsers, click **Yes**.

   The parsers are removed from the Decoder immediately.

Enable and Configure the Entropy Parser

Beginning with NetWitness Suite 11.0, the administrator can configure a Decoder to use a NetWitness native parser, known as the Entropy parser. When the Entropy parser is enabled, analysts have visibility into channels that are trying to blend in with other traffic, but do not follow normal protocol behavior. This helps to identify channels that do not conform to the normal environment traffic baseline, and may, therefore, be worthy of investigation.

The parser creates meta keys, based on statistics collected by the native NetWitness Suite parser, that help to identify behavior of any channel that is getting lots of network traffic. When the parser is first enabled, the analyst needs to become familiar with overall behavior for the different channels seen in a captured session to understand the frequency of bytes and the normal client and server payload. Once the normal behavior is known, analysts can use the meta keys to find behavior that does not match the expected.

By default, the Entropy parser generates 10 additional meta keys that do not add significantly to the load on a Decoder, and are useful for this specialized case. The parser is disabled by default.

Enable indexing if you have interest in exploring interesting sessions based on payload byte analysis of the packets. By default, to make indexing easier, the normal `Float32` value for `entropy.req` and `entropy.res` is multiplied by 10k and stored in a `UInt16` (thus giving four digits of precision, 0 to 10,000).

However, if you define the `entropy.*` fields in the Decoder language to be `Float32`, the Decoder will store it as a float with a range of 0.0 to 1.0. Take care to change the language everywhere if you decide to keep it as a `Float32`.

RSA does not recommend indexing as a `Float32` because of the high unique counts due to minute changes in precision.

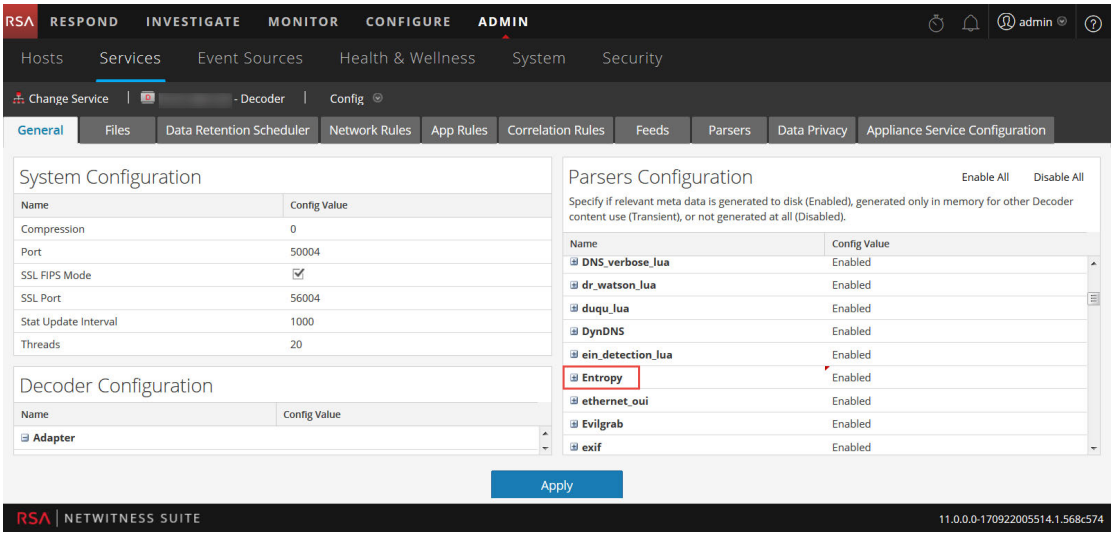
These are the new meta keys generated by the Entropy parser by default:

- `entropy.req` and `entropy.res`: These meta keys capture entropy using the Shannon entropy equation, which has a floating point value as a result. The floating point value of 0 to 1.000 is multiplied by 10000 and written in NetWitness Suite Suite as `UInt 16`, an unsigned integer of 0 through 10000. .
- `mcb.req` and `mcb.res`: The most common byte is simply which byte for each side (0 thru 255) was seen the most.
- `mcbc.req` and `mcbc.res`: The most common byte count is the number of times the most common byte (above) was seen in the session streams.
- `ubc.req` and `ubc.res`: - Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once.

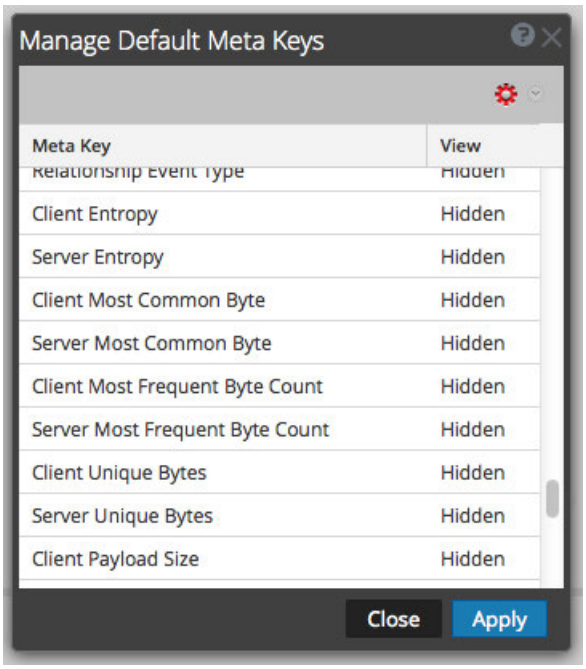
To enable and configure the Entropy parser on a Decoder

1. Log in to RSA NetWitness, and select **ADMIN > Services** in the NetWitness Suite menu.
2. In the Services view, select the Decoder that you want to configure, and then **View > Config**.
   The Services Config view for the selected Decoder is displayed.
3. The Entropy parser is disabled by default. Click the drop-down list under **Config Value** and select **Enabled**. If you want to disable some of the meta keys, click the drop-down list and

select **Disabled** next to the meta key.



4. Click **Apply**
   The Entropy parser is enabled and begins creating the new meta keys as configured in the Concentrator custom index file.
5. In the Service Config view select the Concentrator that is aggregating traffic from this Decoder. Select **View > Files** and open the Custom Index file for the Concentrator. Look for the Entropy parser meta keys to see if they are included and uncommented.
   By default the keys are commented out and therefore not enabled. To enable that part of the language the administrator needs to copy that part of index file into the `index-concentrator-custom.xml` and uncomment the `key description` line for each meta key. An example of the custom index file with the Entropy parser keys and instructions is shown below.
6. With the Entropy meta keys enabled, they are available to analysts in Investigate, but hidden by default. To make the meta keys visible in the Investigate Values view, edit the default meta keys in the Default Meta Keys dialog so that they are open instead of hidden. You can manage these meta key the same way you manage other meta keys.



Entropy Parser Configuration in the Concentrator Custom Index File

The following is an excerpt of the Concentrator Index file lines that the administrator must copy to the custom index file. The comments provide guidance on configuring the parser.

<!-- This section is commented out because it's only used by the Entropy parser which is disabled by default. To enable this part of the language, copy to index-concentrator-custom.xml and uncomment the keys. HOWEVER, take note that depending on how the Entropy parser is configured, the entropy.req and entropy.res format might be a Float32 instead of a UInt16. So make sure to change to the correct type if necessary.-->

<!-- Entropy parser meta - enable indexing if you have interest in exploring this for interesting sessions based on payload byte analysis of the packets. By default, to make indexing easier, the normal Float32 value for entropy.req and entropy.res is multiplied by 10k and stored in a UInt16 (thus giving 4 digits of precision, 0 to 10,000). However, if you define the entropy.* fields in the Decoder language to be Float32, it will store it as a float with a range of 0.0 to 1.0. Take care to change the language everywhere if you decide to keep it as a Float32. We do not recommend indexing as a Float32 because of the high unique counts due to minute changes in precision. -->

<!--

<key description="Entropy Request (Client)" format="UInt16" level="IndexNone" name="entropy.req" valueMax="10001"/>

<key description="Entropy Response (Server)" format="UInt16" level="IndexNone" name="entropy.res" valueMax="10001"/>

-->

<!-- The most common byte is simply which byte for each side (0 thru 255) was seen the most -->

<!--

<key description="Most Common Byte Request" format="UInt8" level="IndexNone" name="mcb.req"/>

<key description="Most Common Byte Response" format="UInt8" level="IndexNone" name="mcb.res"/>

-->

<!-- The most common byte count is the number of times the most common byte (above) was seen in the session streams -->

<!--

<key description="Most Common Byte Count Request" format="UInt32" level="IndexNone" name="mcbc.req" valueMax="500000"/>

<key description="Most Common Byte Count Response" format="UInt32" level="IndexNone" name="mcbc.res" valueMax="500000"/>

-->

<!-- Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once -->

<!--

<key description="Unique Byte Count Request" format="UInt16" level="IndexNone" name="ubc.req"/>

<key description="Unique Byte Count Response" format="UInt16" level="IndexNone" name="ubc.res"/>

-->

<!-- The payload size metrics are the payload sizes of each session side at the time of parsing. However, in order to keep indexing from having high unique counts (bad for performance), the two payload size metas below are indexed in buckets. -->

<!--

<key description="Payload Size Request" format="UInt32" level="IndexNone" bucket="true" name="payload.req" valueMax="500000"/>

<key description="Payload Size Response" format="UInt32" level="IndexNone" bucket="true" name="payload.res" valueMax="500000"/>

-->

Decoder and Log Decoder Additional Procedures

This topic explains the additional procedures an administrator could choose to follow which are not essential for the configuration of the Decoder or Log Decoder.

Topics

- Configure 10G Capability
- Configure a Log Decoder to Accept Protobuf
- Configure Session Split Timeouts
- Configure Syslog Forwarding to Destination
- Configure Transaction Handling on a Decoder
- Create Custom Meta Keys Using a Custom Feed
- Decrypt Incoming Packets
- Edit Decoder System Configuration
- Enable CPU Usage Statistics for Installed Content
- Enable Parser Mappings
- Enable or Disable Lua and Flex Parsing Systems
- Map IP Address to Service Type for Log Parsing
- Obtain Log Files a from Pre-11.0 Log Decoder
- Upload a Log File to a Log Decoder
- Upload a Packet Capture File

Configure 10G Capability

This topic guides administrators in how to tune a Packet Decoder specifically for high speed packet capture using NetWitness Suite 11.0. This applies when capturing packets on a 10G interface card. Packet capture at high speeds requires careful configuration and pushes the Decoder hardware to its limits, so please read this entire topic when implementing a 10G capture solution.

RSA NetWitness Suite provides support for high-speed collection on the Decoder. You can capture network packet data from higher speed networks and optimize your Packet Decoder to capture network traffic up to 8Gb/sec sustained and 10Gb/sec burst, depending on which parsers and feeds you have enabled.

Enhancements that facilitate capture in these environments include the following:

- Utilization of the `pf_ring` capture driver capability to leverage the commodity 10G Intel NIC card for high-speed capture.
- Introduction of `assembler.parse.valve` configuration, which automatically disables application parsers when certain thresholds are exceeded, to limit risk of packet loss. When the application parsers are disabled, network layer parsers are still active. When stats fall below exceeded thresholds, application parsers are automatically re-enabled.

Hardware Prerequisites

- A Series 4S or Series 5 Decoder
- An Intel 82599-based ethernet card, such as the Intel x520. All RSA-provided 10G cards meet this requirement. Two examples are:
  - All SMC-10GE cards provided by RSA.
  - A Dell Network Daughter Card using an Intel controller to provide 10G network interfaces. This is included in all Series 5 hardware.
- For the Series 4S / Dell R620 only: 96 GB of DD3-1600 memory in **dual-rank** DIMMs. Single-rank DIMMs may decrease performance by as much as 10%. To determine the speed and rank of the installed DIMMs, run this command:
  `dmidecode -t 17`.
- Sufficiently large and fast storage to meet the capture requirement. Storage considerations are covered later in this topic.
- Each Packet Decoder configured with a minimum of 2 DACs or SAN connectivity.

Software Prerequisites

- Dell R620-based systems, such as the Series 4S, must have their BIOS updated to v1.2.6 or later.
- The 10G Decoder capability is only supported on RSA-provided Decoder Installation images. All required software is installed by default.
- If upgrading from a previous release, perform the upgrade first before proceeding with configuration

Install the 10G Decoder

Note: You can skip to "Configure the 10G Decoder" if you are starting with new Series 5 hardware.

Perform the following steps to install the NetWitness 10G Decoder:

Download and Update the BIOS

Note: BIOS revisions earlier than v1.2.6 have issues properly identifying the location of the 10G capture card within the system. It is recommended that customers update to the latest v2.2.3 BIOS, but is not required for 10G if they are running v1.2.6 or later.

1. Download BIOS v2.2.3 from the following location:

   http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04
2. Download the Update Package for the Red Hat Linux file.
3. Copy the file to the NetWitness server.
4. Login as `root`.
5. Change the permissions on the file to execute.
6. Run the following file:

   `./BIOS_V7P04_LN_2.2.3.BIN`
7. Reboot the system when execution is complete and a reboot is requested.

Note: The BIOS installation procedure takes approximately 10 minutes.

Locate the 10G Decoder Packages

The packages required to configure the 10G Decoder should already be present on the Decoder installation image. You should not have to install any additional packages.

Verify 10G Decoder Packages Are Installed

Installation of the 10G Decoder packages is handled automatically. Therefore, there should be no action to enable the 10G functionality.

- If you upgraded the kernel packages as part of an upgrade, a reboot is required. The operating system will recompile and install the drivers for the upgraded kernel.
- You can verify that the installation was successful if you see additional `PFRINGZC` interfaces available when selecting the Capture Port Adaper as described below.

Configure the 10G Decoder

Perform the following steps to configure the 10G Decoder:

1. From the **Decoder Explorer** view, right-click **Decoder** and select **Properties**.
2. In the properties drop-down menu, select **reconfig** and enter the following parameters:
   `update=1 op=10g`
   This adjusts the Decoder packet processing pipeline to allow for higher raw data throughput, but less parsing ability.
3. From the **Decoder Explorer** view, right-click **database** and select **Properties**.
4. In the **Properties** drop-down menu, select **reconfig** and enter the following parameters:
   `update=1 op=10g`
   This adjusts the packet database to use very large file sizes and Direct I/O.
5. Select the capture port adapter. Options for this include (in the following examples, "p1p1" and "p1p2" are placeholders and should be replaced with your own interface names):
   - Single port capture - **PFRINGZC,p1p1** or **PFRINGZC,p1p2**
   - Capture off both ports – Select **PFRINGZC,P1P1** and in the **Explorer** view, set `capture.device.params = device=zc:p1p2,zc:p1p1`
6. If the write thread is having trouble sustaining the capture speed, you can try the following:

   Change `/datebase/config/packet.integrity.flush` to `normal`.

   > **Note:** You can adjust the `packet.file.size` to a higher value, but keep the file size under 10 GB, as the whole file is buffered in memory.

7. (Optional) Application parsing is extremely CPU intensive and can cause the Decoder to drop packets. To mitigate application parsing-induced drops, you can set `/decoder/config/assembler.parse.valve` to `true`. These are the results:

- When session parsing becomes a bottleneck, application parsers (HTTP, SMTP, FTP, and others) are temporarily disabled.
- Sessions are not dropped when the application parsers are disabled, just the fidelity of the parsing performed on those sessions.
- Sessions parsed when the application parsers are disabled still have associated network meta (from the network parser).
- The statistic `/decoder/parsers/stats/blowoff.count` displays the count of all sessions that bypassed application parsers (network parsing is still performed).
- When session parsing is no longer a potential bottleneck, the application parsers are automatically re-enabled.
- The assembler session pool should be large enough that it is not forcing sessions.
- You can determine if sessions are being forced by the statistic `/decoder/stats/assembler.sessions.forced` (it will be increasing). Also `/decoder/stats/assembler.sessions` will be within several hundred of `/decoder/config/assembler.session.pool`.

8. (Optional) If you need to adjust the MTU for capture, add the `snaplen` parameter to `capture.device.params`. Unlike previous releases, the `snaplen` does not need to be rounded up to any specific boundary. The Decoder automatically adjusts the MTU set on the capture interfaces.
9. The following configuration parameters are deprecated and no longer necessary
   - The `core= parameter` in `capture.device.params`
   - Any configuration files under `/etc/pf_ring` directory

   Note: An Ethernet device installed post imaging does not require any configuration for use as a capture device. It does require configuration if it is used as a network interface, or for system tools to access it without manual configuration.

Typical Configuration Parameters

Typical configuration parameters are listed below. Actual parameters may vary depending on the amount of memory and CPU resources available.

1. session and packet pool settings(under `/decoder/config`):
   - `pool.packet.pages` = 1000000
   - `pool.session.pages` = 300000
2. Packet write block size under (`/database/config/packet.write.block` size) set to

`filesize`.

Note: This configures the Decoder to buffer the file with huge pages and write using direct I/O for maximum performance.

3. Parse Thread Count (under `/decoder/config`).

   `parse.threads =12`

Storage Considerations

When capturing at 10G line rates, the storage system holding the packet and meta databases must be capable of sustained write throughput of 1400 MBytes/s.

Using the Series 4S Hardware (With Two or More DAC Units)

The Series 4S is equipped with a hardware RAID SAS controller capable of an aggregate 48Gbit/s of I/O throughput. It is equipped with eight external 6 Gbit ports, organized into two 4-lane SAS cables. The recommended configuration for 10G is to balance at least two DAC units across these two external connectors. For example, connect one DAC to one port on SAS card, and then connect another DAC to the other port on the SAS card.

For environments with more than two DACs, chain them off each port in a balanced manner. This may require re-cabling of DACs in an existing deployment, but should not affect data that has already been captured on the Decoder.

If adding new capacity, use the currently available `NwMakeArray` script to provision the DAC units. The script automatically adds one DAC per execution (that means, if adding three DACs, then the script must be run three times), adding the DACs to the `NwDecoder10G` configuration as separate mount points. The independent mount points are important, as this configuration allows the `NwDecoder10G` to segregate write I/O from capture from the read I/O needed to satisfy packet content requests.

Using SAN and Other Storage Configurations

The Decoder allows any storage configuration that can meet the sustained throughput requirement. The standard 8-Gbit FC link to a SAN is not sufficient to store packet data at 10G; in order to use a SAN it may be required to perform aggregation across multiple targets using a software-RAID Scheme. Thus environments using SAN are required to configure connectivity to the SAN using multiple FCs.

Parsing and Content Considerations

Parsing raw packets at high speeds presents unique challenges. Given the high session and packet rates, parsing efficiency is paramount. A single parser that is inefficient (spends too long examining packets) can slow the whole system down to the point where packets are dropped at the card.

For initial 10G testing, start with only native parsers (except SMB/WebMail). Use the native parsers to establish baseline performance and with little to no packet drops. Do not download any Live content until this has been done and the system is proven to capture without issue at high speeds.

After the system has been operational and running smoothly, Live content should be added very slowly - especially parsers.

Best Practices

Whether you are updating a currently deployed system or deploying a new system, it is recommended you use the following best practices to minimize risk for packet loss. One caveat is if you are updating a current 10G deployment but not adding any additional traffic. For example, a current Decoder capturing off a 10G card at 2G sustained should see no difference in performance, unless part of the update also entails adding additional traffic for capture.

- Incorporate baseline parsers (except SMB/Webmail, both of which generally have high CPU utilization) and monitor to ensure little to no packet loss.
- When adding additional parsers, add only one or two parsers at a time.
- Measure performance impact of newly added content, especially during peak traffic periods.
- If drops start occurring when they did not happen before, disable all newly-added parsers and enable just one at a time and measure the impact. This helps pinpoint individual parsers causing detrimental effects on performance. It may be possible to refactor it to perform better or reduce its feature set to just what is necessary for the customer use case.
- Although lesser performance impacts, feeds should also be reviewed and added in a phased approach to help measure performance impacts.
- Application Rules also tend to have little observable impact, though again, it is best not to add a large number of rules at once without measuring the performance impact.

Finally, making the recommended configuration changes outlined in the Configuration section will help minimize potential issues.

Tested Live Content

All (not each) of the following parsers can run at 10G on the test data set used:

- MA content (7 Lua parsers, 1 feed, 1 application rule)
- 4 feeds (alert ids info, nwmalwaredomains, warning, and suspicious)
- 41 application rules
- DNS_verbose_lua (disable DNS)

- fingerprint_javascript_lua
- fingerprint_pdf_lua
- fingerprint_rar_lua
- fingerprint_rtf_lua
- MAIL_lua (disable MAIL)
- SNMP_lua (disable SNMP)
- spectrum_lua
- SSH_lua (disable SSH)
- TLS_lua
- windows_command_shell
- windows_executable

NOT TESTED:

- SMB_lua, native SMB disabled by default
- html_threat

OTHER:

- HTTP_lua reduces the capture rate from >9G to <7G. At just under 5G this parser can be used in place of the native without dropping (in addition to the list above).
- xor_executable pushes parse CPU to 100% and the system can drop significantly due to parse backup.

Aggregation Adjustments Based on Tested Live Content

A 10G Decoder can serve aggregation to a single Concentrator while running at 10G speeds. Deployments using Malware Analysis, Event Stream Analysis, Warehouse Connector, and Reporting Engine are expected to impact performance and can lead to packet loss.

For the tested scenario, the Concentrator aggregates between 45 and 70k sessions/sec. The 10G Decoder captures between 40-and 50k sessions/sec. With the content identified above, this is about 1.5 to 2 million meta/sec. Due to the high volume of session rates, the following configuration changes are recommended:

- Nice aggregation on the Concentrator limits the performance impact on the 10G Decoder. The following command turns on nice aggregation.
  ```
  /concentrator/config/aggregate.nice = true
  ```

- Due to the high volume of sessions on the Concentrator, you may consider activating parallel values mode on the Concentrator by setting `/sdk/config/parallel.values` to `16`. This improves Investigation performance when the number of sessions per second is greater than 30,000.
- If multiple aggregation streams are necessary, aggregating from the Concentrator instead has less impact on the Decoder.
- Further review for content and parsing is required for deployments where you want to use other NetWitness Suite components (Warehouse, Malware Analysis, ESA, and Reporting Engine).

Optimize Read/Write Operations When Adding New Storage

A 10G Decoder is optimized to stagger read and write operations across multiple volumes so that the current file being written is on a different volume from the next file that will be written. This allows maximum throughput on the raid volume when reading data from the last file being written while writing the current file on a different volume. However, if volumes are added after a Decoder has been in use, the ability to stagger is limited because one or more volumes are already full so the new volume is the only place new files can be written.

To remedy this situation, an administrator can run a `stagger` command on an existing NetWitness Suite database (packet, log, meta, or session), that has at least two volumes, to stagger the files across all volumes in the most optimal read/write pattern. The major use case is when new storage is added to an existing Decoder and you want to stagger the volumes BEFORE restarting capture.

The configuration nodes for this command are the session, meta, and packet databases. Each of these lives under `/database/config`, which is usually a root node. The config nodes for a Decoder are:

- `/database/config/packet.dir`
- `/database/config/meta.dir`
- `/database/config/session.dir`

The *NetWitness Suite Core Database Tuning Guide* has information on how those configurations are formatted.

The `stagger` command is typically only useful for a 10G Decoder and usually just for the packet database. Maximum performance is achieved for storing and retrieving packets when multiple volumes are present. In this scenario, the Decoder always fills the volume with the most free space. When the volumes are roughly the same size, this results in a staggered write pattern, which allows maximum throughput for reading and writing across all volumes. However, this only naturally occurs when multiple packet storage volumes are present at the time the Decoder is first deployed.

A typical use case is adding more storage to an existing Decoder to increase retention. However, when adding storage to an deployment that has already filled the existing volumes with stored packets, the Decoder will naturally fill the new storage with packets before rolling out any packets on the existing storage. This results in a suboptimal read/write pattern because most reads will occur on the same volume that is currently being written to. In a 10G deployment, reads are blocked from the volume when writes are occurring. This doesn't stop ALL reads on that volume, because the file is buffered in memory before being written, but it does result in suboptimal read performance.

With the `stagger` command, you can add more storage and then have the service naturally stagger the files across ALL volumes (existing and new) so that read performance is optimized.

Caution: This command should only be performed AFTER the storage is mounted and the Decoder configured to use it (e.g., after adding the mount point(s) to `packet.dir`).

The downside to this command is it can take some time to stagger and the Decoder should not be capturing during the stagger operation.

Recommended workflow:

1. Add all storage and configure mount points.
2. Add new storage mount points to `packet.dir` (or `session.dir`/`meta.dir`) and restart service (very important!).
3. Ensure capture is stopped.
4. Run stagger operation but make sure the connection that initiated the stagger operation is never terminated until the operation is complete. If the connection is terminated, then the stagger operation will be canceled. If the operation is canceled, the files that were already staggered will remain in place. The operation can be resumed by rerunning the same command (the work already done will not need to be done again). If running stagger from NwConsole, run the `timeout 0` command before sending the `stagger` command. This will prevent the normal 30-second command timeout.
5. Start capture after `stagger` command finishes.

The following are the parameters for the command:

- `type` - The database that will be staggered (session, meta, or packet). Typically only the packet database is useful for staggering, but it is possible to do the session or meta database when multiple volumes are present for those databases. Since the session and meta databases write far less data than the packet database, typically staggering those databases results in less noticeable performance gains.

- `dryRun` - If `true` (the default), will only return a description of the operations that would be performed. If `false`, then the files will actually be moved to an optimal read/write pattern. You MUST pass false to actually stagger the files.

Example usage from NwConsole:

```
login <decoder>:50004 <username> <password>
timeout 0
send /database stagger type=packet dryRun=false
```

If you run this command via the RESTful API, please pass the additional parameter `expiry=0` to prevent a timeout from the service. You will also need to ensure the HTTP client does not disconnect before the operation completes.

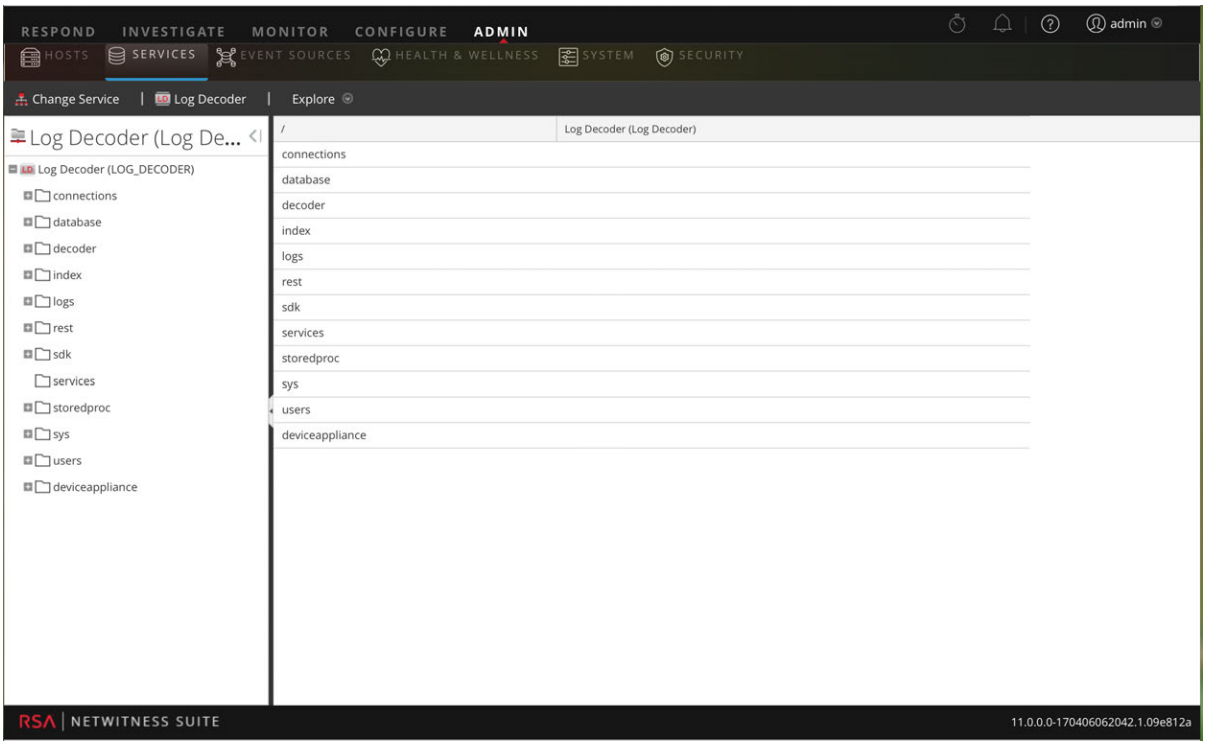
Configure a Log Decoder to Accept Protobuf

There are occasions when you want to analyze log files that are in protobuf (Protocol Buffer) format. You can configure a Log Decoder to accept logs in protobuf (Protocol Buffer) format.

To import a log file to a Log Decoder:

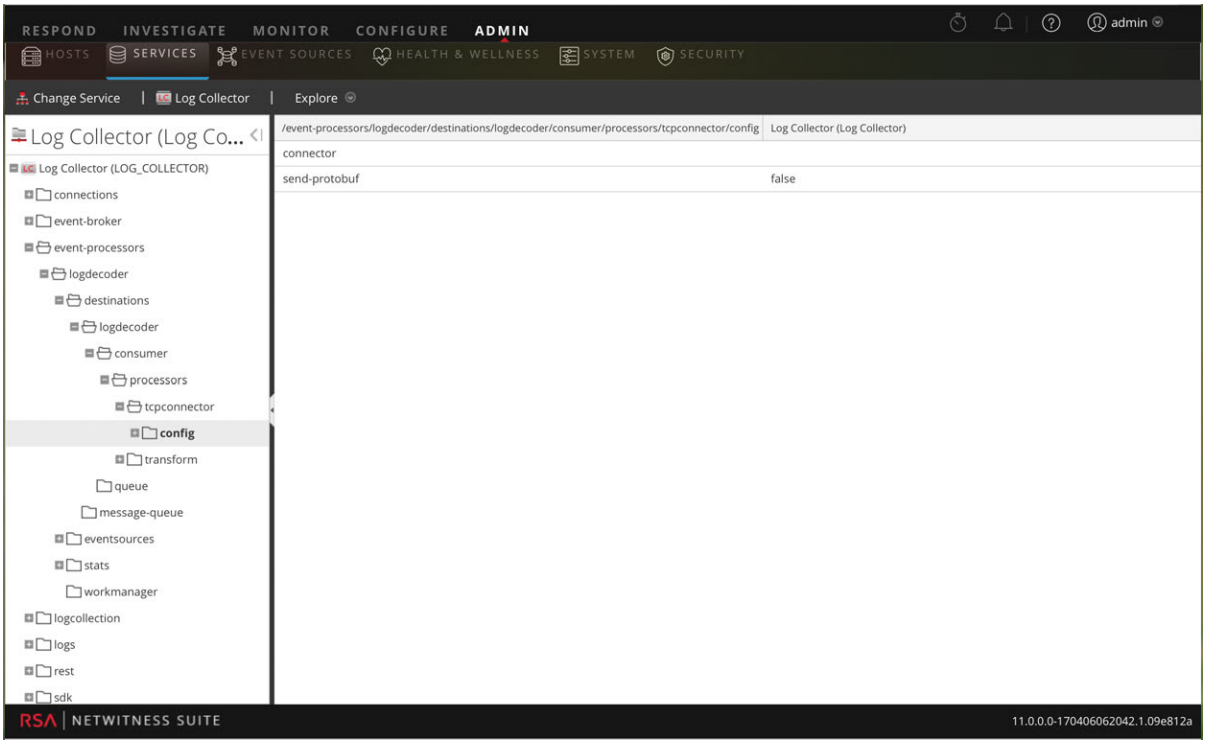
1. Go to **ADMIN > Services**.
2. Select a Log Decoder in the **Service** list, and select > **View** > **Explore**.

   The Explorer view for the Log Decoder is displayed.



3. Navigate to `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config`

Your screen should look similar to the following.



4. For the **send-protobuf** field, select **false**, and change the value to **true.**
5. Navigate to `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp` and change the **port** value to **50202**.
6. Navigate to `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/event` and change the following parameters:
   - Clear the **delimiter** field
   - Change **format** to **%text%**

Configure Session Split Timeouts

The default behavior of the Decoder is to automatically end sessions that exceed a configured size or have been inactive for a period of time. When the session is ended due to timeout, any subsequent packets received in that session appear to be stored in a new session. You can mitigate the effect of session splitting due to long periods of inactivity between packets using this procedure.

When a Decoder session exceeds a configured size (32MB by default, the `/decoder/config/assembler.max.size`) or has been inactive for a period of time, the session is split. NetWitness Suite has the previous packet and the next packet and can propagate session state from the initial session fragment to the subsequent session fragment.

Each session fragment is annotated (`session.split` meta) such that it can be identified and associated with other fragments from the actual network session. Directionality as determined by the initial session reduces the occurrence of fragments having reversed directionality.

If there is a gap in time between packets large enough that there are no longer any packets for the session in memory, the session is removed from the Decoder. If a subsequent packet shows up after this occurs, a new session is created with no context to the preceding session. The issue is the inability to continue a session when we encounter a gap between packets of a session that is larger than the packets we are buffering (based upon available memory and timeout configurations). Once the last packet of a session is removed from memory, the session is also removed, and with it the necessary context for ensuring consistent directionality.

There are two timeout settings in a Packet Decoder, `/decoder/config/assember.timeout.session` and `assembler.timeout.packet`. Both default to 60 seconds. The setting `assembler.timeout.session` controls how long a session lives in Assembler without receiving another packet. The setting `assembler.timeout.packet` controls how long a session waits before getting parsed. If the session is kicked out of Assembler before this timeout, then it automatically goes to parsing.

The session timeout is the number of seconds since the last packet was added to that session. Therefore, this timeout resets on every packet added to that session. The packet timeout is the number of seconds since the very first packet for that session was added (in other words, the packet that created the session). This is never reset and once the timeout expires, the session is parsed.

The important point is a session can be parsed but still remain in Assembler. A session in Assembler can still have packets added to it, even if it has already been parsed. Packets added after the session is parsed will never be seen by parsers, but they will be attached to the session and can be viewed by a subsequent `/sdk content` or `/sdk packets` call.

After a session is parsed, the session AND its metadata are written to disk. At this point, they can be aggregated and "seen" by `sdk` commands. Packets are written in order of capture and are not reordered by what session they belong to. Nor are they necessarily written when the session and meta data are written.

You can disable both timeout nodes, `/decoder/config/assembler.timeout.session` and `assembler.timeout.packet`, by setting them to zero in the Services Explore view.

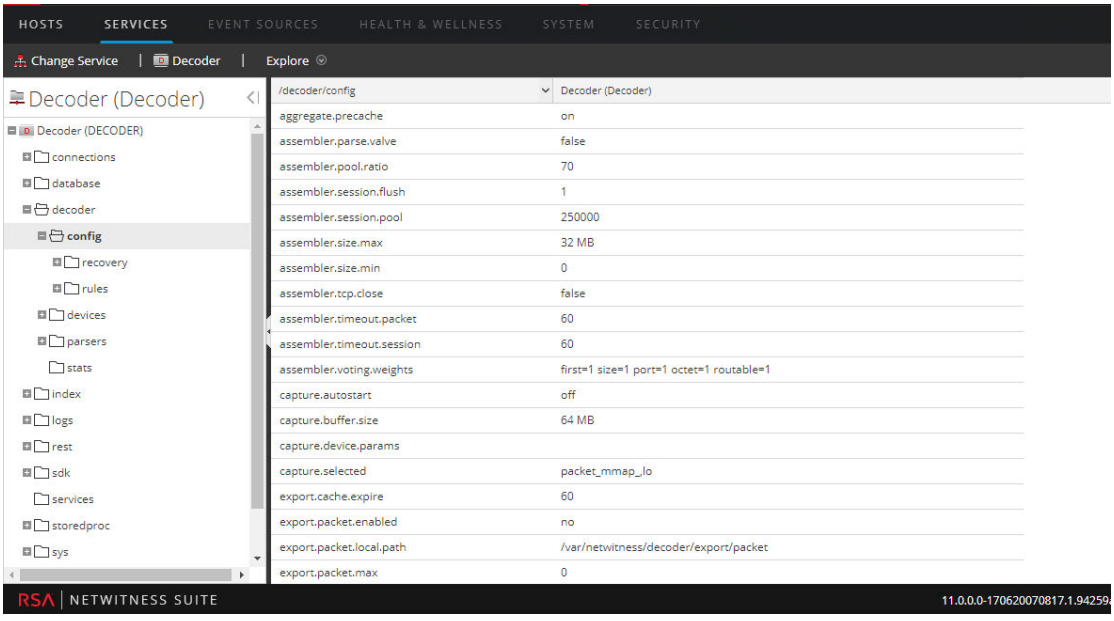
If both timeouts are disabled, the sessions are still split due to time or size expiration. However, the Decoder keeps track of the network stream for as long as it has sufficient memory. Thus, when more packets arrive on the same network stream, the Decoder adds `split` meta items to the subsequent sessions. Using a combination of the `split` metadata and the stream key, it is possible to reconstruct the network stream from the multiple sessions.

The length of time for which sessions are tracked is limited by the number of session pool entries available on the Decoder, and therefore the actual time window varies according to the rate at which new sessions are added. If new sessions are added at a high rate, the size of the time window decreases. The size of the pool is set using the configuration entry `/decoder/config/assembler.session.pool`, which sets the maximum number of sessions that will be tracked at a time.

The `/decoder/stats/assembler.timespan` statistic allows you to see when the Decoder is no longer tracking session splits because the ingest rate is too high and the Decoder does not have enough memory to track. This statistic shows the number of seconds tracked within the session table, which is the effective time window in which the Decoder can link together sessions. Under normal operation this statistic matches the value of `/decoder/config/assembler.timeout.session`, but when running in Time Split mode, the `/decoder/stats/assembler.timespan` statistic grows or shrinks depending on the ingest rate.

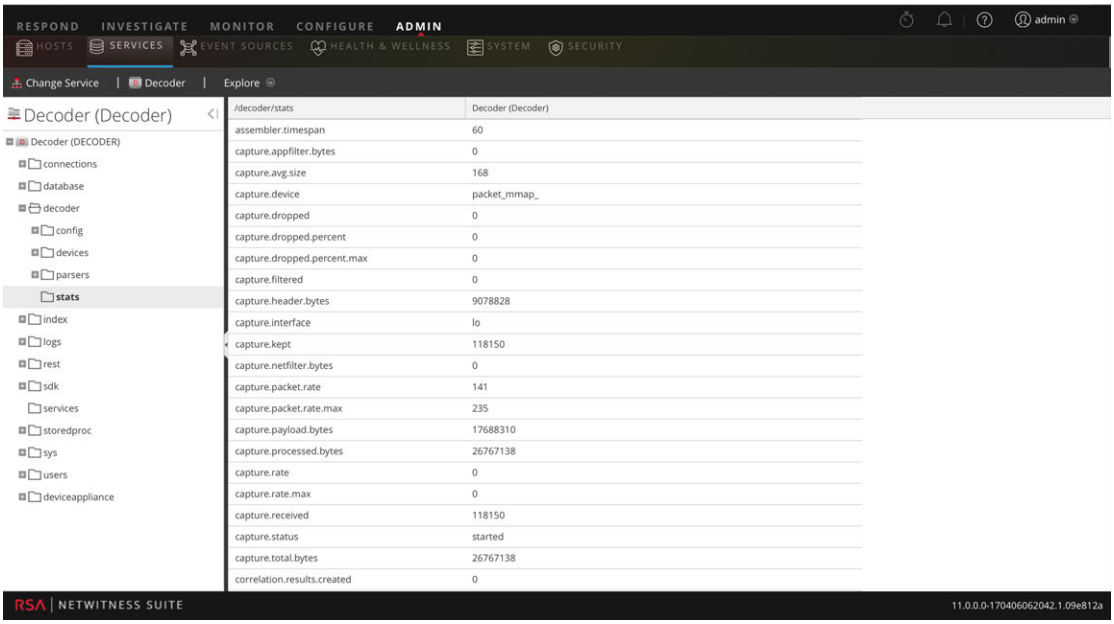
To configure Time Split mode, set the following configuration parameters and restart the Decoder:

1. In the Admin > Services view, select the Decoder service and > **View** > **Explore.**
2. In the Services Explore view select **decoder** > **config**.



3. Click in the **Value** column next to the parameter and set these two parameters :
   `/decoder/config/assembler.session.flush = 0`
   `/decoder/config/assembler.timeout.session = 0`

4. To see when the Decoder is no longer tracking session splits because the ingest rate is too high and the Decoder does not have enough memory to track, view the `/decoder/stats/assembler.timespan` statistic, in the Services Explore view select **decoder** > **stats**.



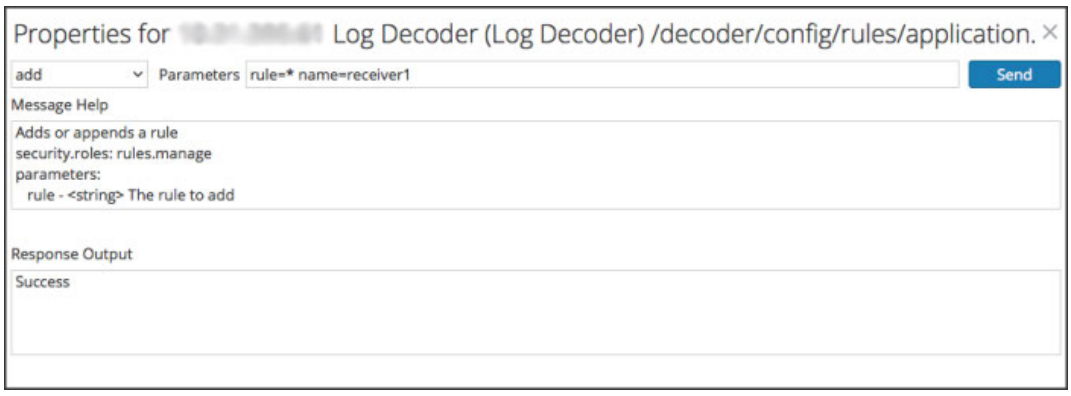
Configure Syslog Forwarding to Destination

In addition to collecting Syslog messages, you can configure the Log Decoder to forward Syslog messages to another Syslog receiver. NetWitness Suite forwards Syslog messages after it has parsed the messages and before it writes the messages to the Log Decoder.

Note: You must configure Syslog Forwarding using the steps defined in this topic under **Procedure** using the **Explore** view.

The Log Decoder must be in the **Started** state before you can configure Syslog Forwarding. To configure Syslog Forwarding:

1. Configure Log Decoder application layer rules (Application rules) to tag Syslog messages with metadata that instructs NetWitness Suite to forward the messages:
   a. In the **Services** view, select a Log Decoder, and in the Actions column, select > **View** > **Explore**.
   b. Go to the **/decoder/config/rules/application** node, right-click **application,** and click **Properties**.
   c. In the **Properties** view, specify the **add** command with the following parameters:
   `rule=<query> name=<name>`
   Example 1: `rule=*name=receiver1`
   Example 2: `rule="device.type='winevent_nic'" name=receiver`)
   d. Click **Send**.



NetWitness Suite creates the `name=receiver1 rule=* order=<n>` rule. NetWitness Suite inserts the order number (for example, `order=49`) based on when you set up the rule.

e. Go to the `/decoder/config/rules/application` node and click the `name=receiver1 rule=* order=49` rule.

f. Add **alert forward** parameters to the rule parameters.

```
rule=* name=receiver1 order=49 alert forward
```

All other rule parameters have the same meaning as they do in other application rules.

The following Application rule example selects all logs with the `*` rule. It creates an alert meta with the value "**`receiver1`**" and tags the entire log for forwarding it to the syslog forwarding destination. You can define as many different forwarding rules as you need with the same name or unique names.

2. Define Syslog forwarding destinations and enable forwarding.

   a. In the **Services** view, select a Log Decoder, and ⚙ > **View** > **Explore**.

   b. Syslog forwarding destinations are defined in the configuration node `/decoder/config/logs.forwarding.destination`.
   This configuration node contains one or more name/value pairs. The name corresponds to the name parameter in the application rule that you used to tag logs with forwarding meta. The value is a colon-separated triple of transport, host, and port followed by an optional formatting parameter.
   `name=(udp|tcp|tls):host:port[:(retainsource|rfc3164)]`
   The first parameter indicates the transport protocol and must be one of udp, tcp, or tls. Specifying udp will forward logs via RFC 3164 / RFC 5426 UDP syslog protocol. Specifying tcp will forward logs via a TCP connection with RFC 6587 framing. Specifying tls will forward logs in accordance with RFC 5425.

   The host is an IPv4 address, IPv6 address, or host name.

   The port is the port to which the logs are sent. This is typically port 514 for UDP syslog, and 6514 for TLS connections. There is no standard port assignment for syslog over TCP.

Optionally, `retainsource` or `rfc3164` can be specified at the and of the destination string to indicate that additional formatting and information should be included with each log forwarded. Specifying `retainsource` will include z-connector headers at the beginning of the log based and will be populated by the `time`, `device.(ip|ipv6|host)`, and `lc.cid` meta and is best used for forwarding to other log decoders. The `rfc3164` option will prepend a valid RFC3164 header to all events forwarded constructed of the `syslog.pri`, `time`, and `device.(ip|ipv6|host)` meta. In both cases, the original log text is unmodified.

Example forwarding destination:

```
gears=tls:gears.netwitness.local:6514
```

Example forwarding over tcp to blackout on port 514 with z-connector headers:

```
fwdrule=tcp:blackout.netwitness.local:514:retainsour
```

In the `/decoder/config/logs.forwarding.destination` parameter, specify the destination. For example:
TLS Connections: `receiver1=tls:receiver1.netwitness.local:6514`
UDP Connections: `receiver1=udp:receiver1.netwitness.local:514`
TCP Connections: ***`receiver1=tcp:receiver1.netwitness.local:514`***

Note:
You can configure:
- Multiple rules to forward logs to the same destination.
- Multiple rules to forward logs to multiple destination.

For TLS connections, the certificate of the forwarding destination must be validated. The certificate authority that signed the destination's certificate must be present in the Log Decoder's CA trust store and the certificate must reside on the destination or Syslog receiver. Refer to "Configure Certificates" in the *Log Collection Configuration Guide* for information about manipulating the Log Decoder's CA trust store. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

c. In the `/decoder/config/logs.forwarding.enabled` parameter, specify **true**.

Configure Transaction Handling on a Decoder

Beginning with 11.0, administrators can configure a Decoder to subdivide incoming sessions into smaller transaction sessions when using LUA parsers designed to create transactions. The feature allows analysts to perform analytics on the split sessions in downstream services such as Investigate.

Transaction Handling

The Decoder service configuration node has a new parameter for configuration of transaction handling: `/decoder/parsers/config/parser.transaction.mode`. This node controls the behavior of the Decoder when a parser defines a transaction within a network session.

The values for `parser.transaction.mode` correspond to the operating modes:

- `off` (transactions off)
- `meta` (transactions represented as meta Items)
- `split` (transactions split sessions)

Transactions Off

When transactions mode is off, any application-level transactions created by parsers are ignored, and nothing is stored in the collection to represent the transaction.

Transactions Represented as Meta Items

In this mode of operation, when a parser generates an application-level transaction, a new meta item of type `{{trans}}` is added to the session in which the transaction occurred. The `{{trans}}` meta item contains a list of other meta items that constitute the transaction.

Transactions Split Sessions

In this mode of operation, when a parser generates an application-level transaction, the session is split. The session splitting is accomplished by:

1. A new session item is created.
2. Network meta items are copied from the parsed session into the new session.
3. Meta items marked in the transaction are moved from the original session to the new session.

The following meta items are duplicated into the split session from the session that was parsed:

- `time`
- `medium`

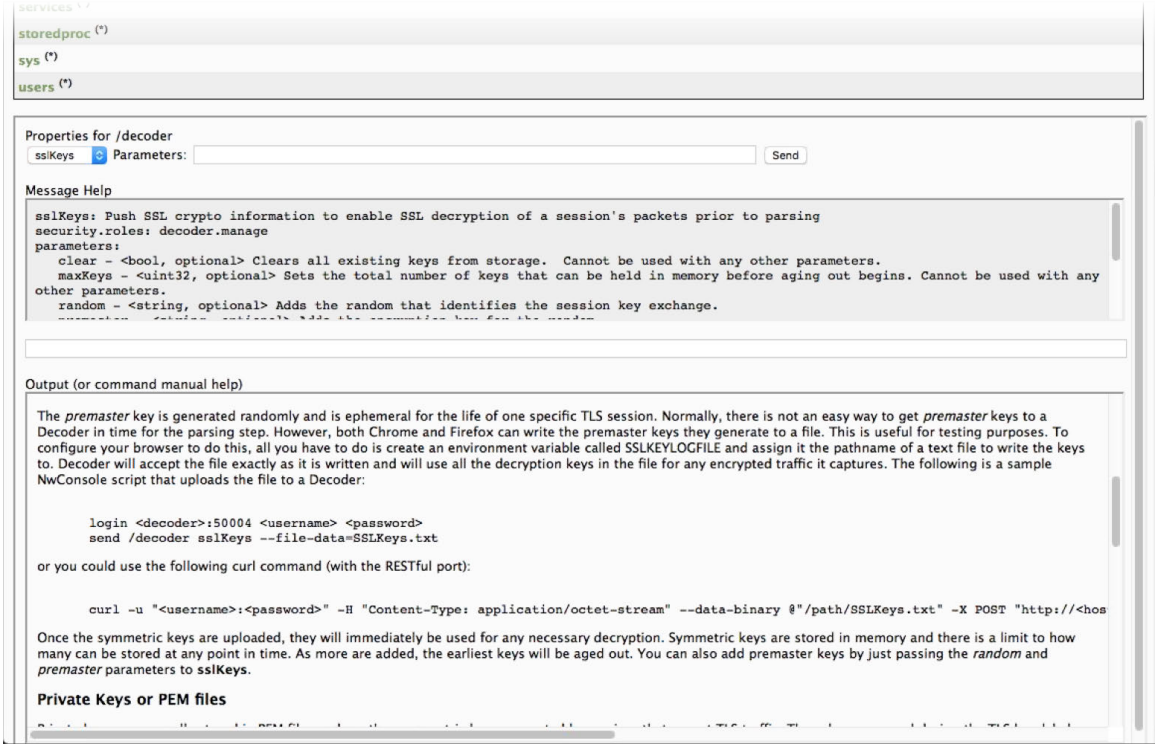
- eth.src
- eth.dst
- eth.type
- ip.proto
- ip.src
- ip.dst
- ipv6.src
- ipv6.dst
- ipv6.proto
- tcp.srcport
- tcp.dstport
- tcp.flags
- udp.srcport
- udp.dstport
- service
- udp.srcport
- udp.srcport
- tls.premaster

Decrypt Incoming Packets

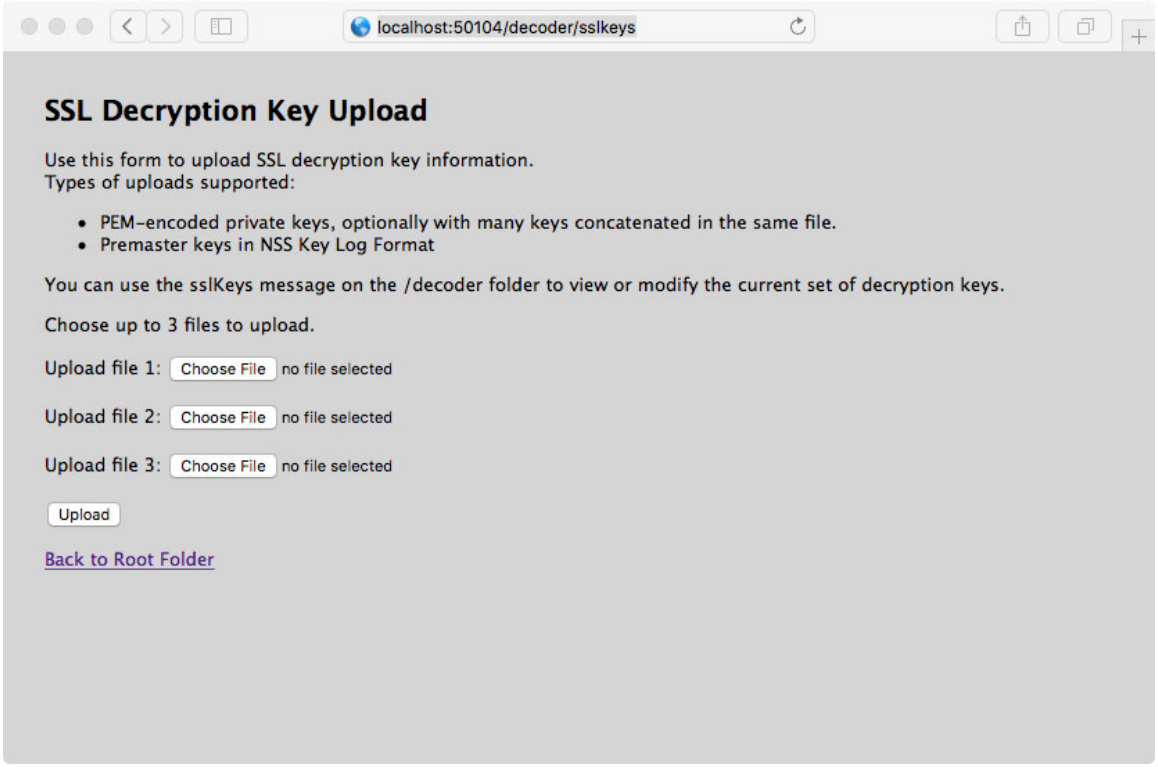
Beginning with NetWitness Suite 11.0, administrators can configure a Packet Decoder to decrypt incoming packets using the `sslKeys` command. Enabled parsers will see the unencrypted packet payload and create metadata accordingly. If the Decoder is not configured to decrypt incoming packets, most enabled parsers will see only encrypted garbage and will fail to create meaningful metadata.

Note: If FIPS is enabled, the list of ciphers for decryption is restricted to only those that are FIPS approved.

The `sslKeys` command provides a way to upload premaster or private keys to the Decoder, so that captured encrypted packets that match the keys can be decrypted before parsing. Administrators configure the Decoder by entering the `sslKeys` command using the NwConsole command line interface or the Decoder RESTful interface.



The RESTful interface form at the path: `/decoder/sslkeys` allows uploading a single PEM-encoded private key, a single file containing multiple private keys concatenated together, or a single file of multiple premaster keys.



Although the packets are decrypted during the parse stage, only the encrypted packets are written to disk. The matching premaster key used for decrypting is written to the `tls.premaster` meta key, which analysts can use to subsequently view unencrypted packets on demand.

Details for administrators to configure decryption of incoming packets, and for analysts to view unencrypted packets on demand are provided below.

Performance Considerations

Decrypting packets in real time requires extra work in the parsing stage. Before implementing this feature, plan carefully to ensure the incoming traffic bandwidth does not overwhelm the available compute power. You may need more Decoders to decrypt traffic than you would need if not decrypting.

Packets captured on a Decoder normally have a timeout of ~60 seconds in the assembly stage before they are sent to the parsing step. If the Decoder is under memory pressure due to very high bandwidth, the lifetime of the packets in Assembler may be shortened. To alleviate this situation, you can configure a longer timeout value and increase the amount of memory available to hold packets in Assembly. Also, in order to perform decryption of the packets, the Decoder must receive the decryption key before the parsing stage.

Note: Currently, only TLS 1.2 and earlier protocols can be decrypted

With no feeds loaded, the following parsers enabled, and 50% of the sessions being decrypted,a Decoder can process traffic at 3 Gbps .

Parser Name	Description
SYSTEM	Session Details
NETWORK	Network Layer
ALERTS	Alerts
GeoIP	Geographic data based on ip.src and ip.dst
HTTP	Hyper Text Transport Protocol (HTTP)
HTTP_Lua	Hyper Text Transport Protocol (HTTP) Lua
FTP	File Transfer Protocol (FTP)
TELNET	TELNET Protocol
SMTP	Simple Mail Transport Protocol (SMTP)
POP3	Post Office Protocol (POP3)
NNTP	Network News Transport Protocol (NNTP)
DNS	Domain Name Service (DNS)
HTTPS	Secure Socket Layer (SSL) Protocol
MAIL	Standard E-Mail Format (RFC822)
VCARD	Extracts VCARD fullname and email information
PGP	Identifies PGP blocks within network traffic
SMIME	Identifies SMIME blocks within network traffic
SSH	Secure Shell (SSH)
TFTP	Trivial File Transfer Protocol (TFTP)
DHCP	Dynamic Host Configuration Protocol (DHCP and BOOTP)
NETBIOS	Extracts NETBIOS computer name information.

Parser Name	Description
SNMP	Simple Network Management Protocol (SNMP)
NFS	Network File System (NFS) protocol
RIP	Routing Information Protocol (RIP).
TDS	MSSQL and Sybase database protocol (TDS)
TNS	Oracle database protocol (TNS)
IRC	Internet Relay Chat (IRC) protocol
RTP	Real Time Protocol (RTP) for audio/video
SIP	Session Initiation Protocol (SIP)
H323	H.323 Teleconferencing protocol
SCCP	Cisco Skinny Client Control Protocol
GTalk	Google Talk (GTalk)
VlanGre	Vlan ID and GRE/EtherIP tunnel addresses
BITTORRENT	BitTorrent File Sharing Protocol
FIX	Financial Information eXchange Protocol
GNUTELLA	Gnutella file sharing protocol
IMAP	Internet Message Access Protocol
MSRPC	Microsoft Remote Procedure Call protocol
RDP	Remote Desktop Protocol
SHELL	Command Shell Identification
TLSv1	TLSv1
SearchEngines	A parser that extracts search terms
FeedParser	External Feed Parser

Encryption Keys

The `sslKeys` command accepts two types of encryption keys:

- Premaster key: the symmetric key used in the TLS payload stream for encryption and decryption.
- Private key: the asymmetric private key used during the TLS handshake that encrypts the premaster.

Premaster Key

The premaster key is generated randomly and is ephemeral for the life of one specific TLS session. Normally, there is not a good way to get premaster keys to a Decoder in time for the parsing step. However, both Chrome and Firefox can write the premaster keys they generate to a file. This is useful for testing purposes. To configure your browser to do this, create an environment variable called SSLKEYLOGFILE and assign it the pathname of a file to which the keys will be written. The Decoder will accept the file exactly as written and will use all the decryption keys in the file for any encrypted traffic it captures.

This is a sample NwConsole script that uploads the file to a Decoder:

```
login <decoder>:50004 <username> <password>

send /decoder sslKeys --file-data=SSLKeys.txt
```

This is an example using a curl command (with the RESTful port) to upload the file to a Decoder:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary @"/path/SSLKeys.txt" -X POST "http://<hostname>:50104/decoder?msg=sslKeys"
```

After the symmetric keys are uploaded, they will immediately be used for any necessary decryption. Symmetric keys are stored in memory and there is a limit to how many can be stored at any point in time. As more keys are added, the earliest keys will be aged out. You can also add premaster keys by just passing the `random` and `premaster` parameters to `sslKeys`.

Private Keys or PEM files

Private keys are normally stored in PEM files and are the asymmetric keys generated by services that accept TLS traffic. These keys are used during the TLS handshake to encrypt the premaster symmetric key that will be used for the rest of the payload encryption.

For example, if you have a web server whose traffic you want visibility into, you need to upload the private key it uses to encrypt traffic. You only need to do this once, as it is stored permanently (or until removed by a delete command). Private keys are automatically encrypted before storing to protect them. After upload, you must issue a parser reload command so that the newly installed key becomes visible to the HTTPS parser. Now, all TLS handshakes that use that private key will be able to be decrypted by the Decoder.

Note: Not all ciphers suites use a "known" private key (for example, Ephemeral Diffie Hellman). Encrypted traffic with those ciphers cannot be decrypted unless the premaster key is uploaded to the Decoder before the session is parsed.

These are some sample commands that upload a PEM file to be used for decryption.

Using NwConsole:

```
send /decoder sslKeys pemFilename=MyKey.pem --file-data=/path/MyKey.pem
```

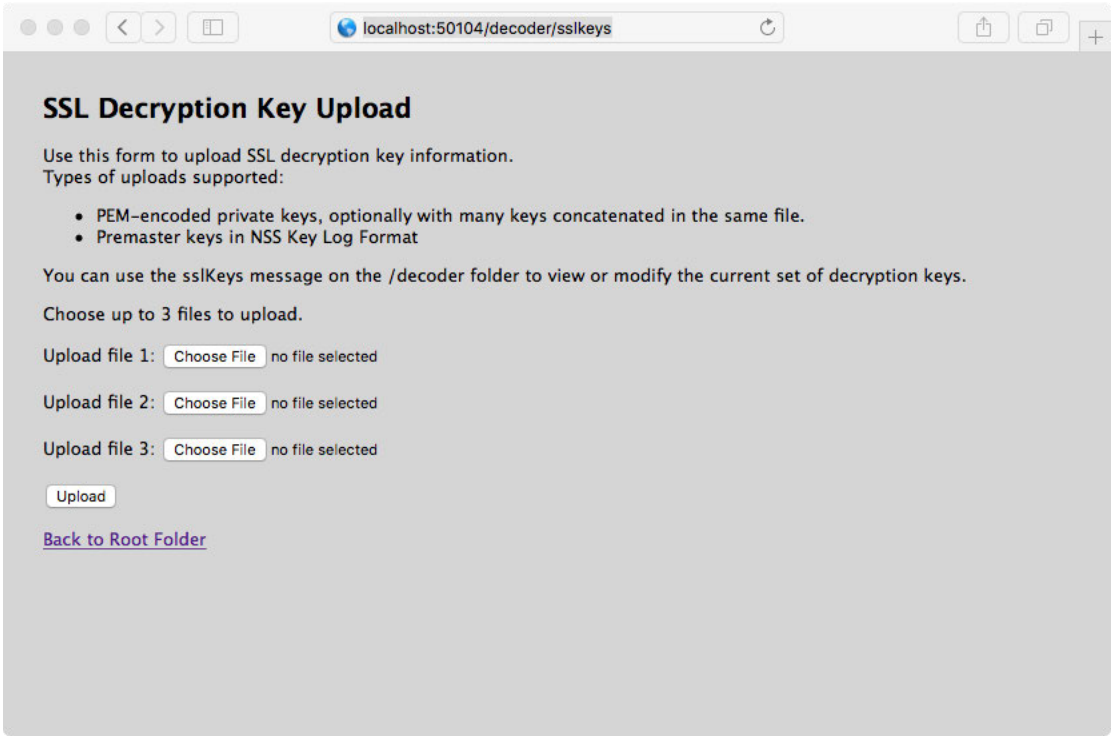
Using the RESTful interface (you must provide the `pemFilename` parameter in the URL):

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary
@"/path/MyKey.pem" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys&pemFilename=MyKey.pem"
```

Upload Multiple Premaster and Private Keys

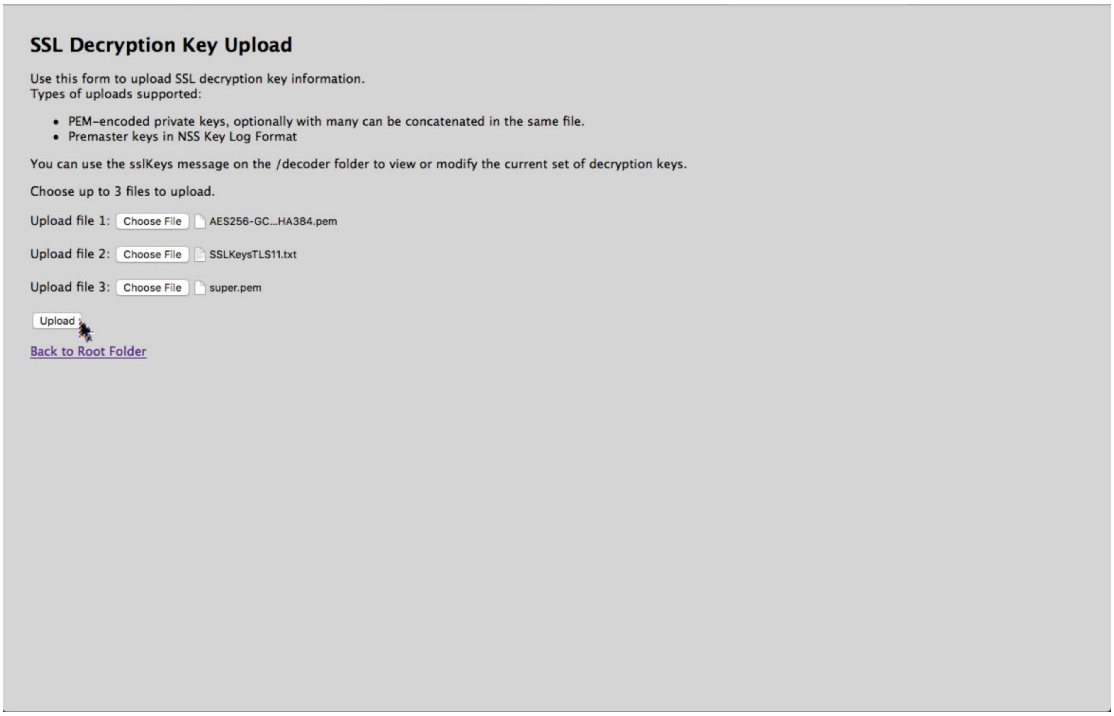
You can use the RESTful interface form to facilitate uploading of multiple keys, both premaster and private at the same time.

1. Open the RESTful API in your browser, and navigate to this path on the Decoder that you want to configure: `/decoder/sslkeys`.



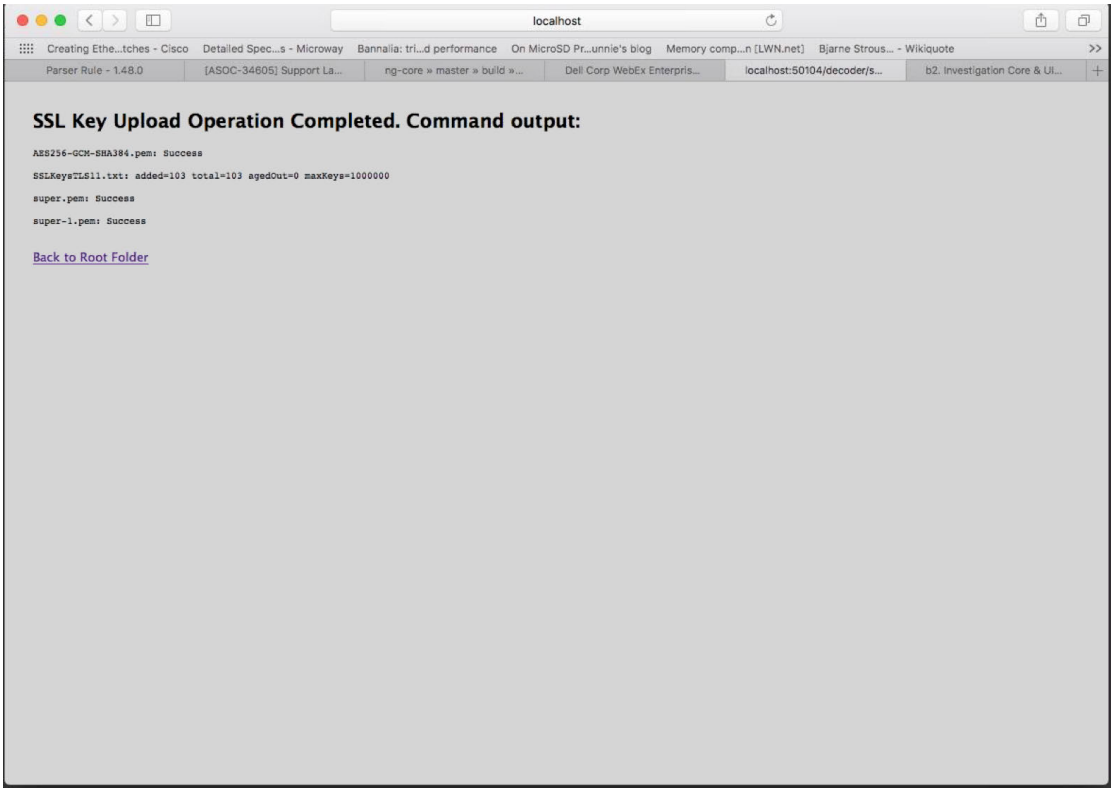
2. Next to **Upload File 1**, click **Choose File** and locate the premaster key file or PEM file that you want to upload on you local file system.

3. (Optional) repeat for **Upload File 2** and **Upload File 3**.



4. Click **Upload**.

   The files are uploaded to the Decoder and results are displayed in the form.



Parameters for Managing Keys

The `sslKeys` command has several parameters for managing premaster and private keys. This is the full list of parameters:

Parameter	Description
`clear`	Removes all premaster keys from memory. Does not delete any PEM files installed on the system.
`maxKeys`	Changes the maximum number of premaster keys that are stored in memory.
`listPems`	Returns a list of all installed private key PEM files.
`deletePem`	Deletes the named PEM file from the file system. You can pass this parameter more than once to remove multiple files.
`random`	The random hash used to identify the premaster key.
`premaster`	The premaster key that will be installed for the previous `random` parameter. They must show up in pairs and `random` must be first.

Return Values

Most `sslKeys` commands return name/value pairs of statistics about the premaster keys in memory. The statistics are listed in the following table.

Name	Description
`added`	The number of premaster keys just added during this command.
`total`	The total number of premaster keys loaded in memory.
`agedOut`	The total number of premaster keys that were removed during this command; this is not a lifetime stat.
`maxKeys`	The current maximum allowed premaster keys

Viewing Unencrypted Traffic

If packets are decrypted during the parse stage, encrypted packets are written to disk, and the matching premaster key used for decrypting is written to the `tls.premaster` meta key, analysts can view the unencrypted packets using the `tls.premaster` meta key.

One Decoder API that you can use to see the unencrypted packets is the /sdk/content RESTful service. You need to know the Session ID of the encrypted packets and the `flags` parameter masked to the value 128 (or 0x80 in hex). Point your browser to the Decoder RESTful interface and type in the following command, substituting the actual Session ID for <id>:

```
http://<decoder>:50104/sdk/content?session=<id>&flags=128&render=text
```

The Decoder returns a simple web page showing the packets after they are decrypted.

If you want to see what the packets look like encrypted, type in one of the following commands, substituting the Session ID for <id>:

```
http://<decoder>:50104/sdk/content&session=<id>&render=text
```

```
http://<decoder>:50104/sdk/content&session=<id>&flags&render=text
```

For more information on the /sdk/content service, see the manual page for /sdk content.

Supported Cipher-Suites

The following table lists which cipher-suites are supported using private keys.

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ ECDHE_ RSA_ WITH_ AES_256_ GCM_ SHA384	ECDHE-RSA-AES256-GCM-SHA384	[0xc030]	TLSv1.2	Kx=ECDH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	[0xc02c]	TLSv1.2	Kx=ECDH	Compliant	Not Supported
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	[0xc028]	TLSv1.2	Kx=ECDH	Compliant	Not Supported
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	[0xc024]	TLSv1.2	Kx=ECDH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	[0xc014]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	[0xc00a]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384	[0xa3]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	[0x9f]	TLSv1.2	Kx=DH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	[0x6b]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256	[0x6a]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	[0x39]	SSLv3	Kx=DH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA	[0x38]	SSLv3	Kx=DH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	[0x88]	SSLv3	Kx=DH	Non-Compliant	Not Supported
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE-DSS-CAMELLIA256-SHA	[0x87]	SSLv3	Kx=DH	Non-Compliant	Not Supported
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384	[0xc032]	SSLv3	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384	[0xc02e]	TLSv1.2	Kx=ECDH/ECDSA	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ ECDH_ RSA_ WITH_ AES_256_ CBC_ SHA384	ECDH-RSA-AES256-SHA384	[0xc02a]	TLSv1.2	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ ECDH_ ECDSA_ WITH_ AES_256_ CBC_ SHA384	ECDH-ECDSA-AES256-SHA384	[0xc026]	TLSv1.2	Kx=ECDH/ECDSA	Compliant	Not Supported
TLS_ ECDH_ RSA_ WITH_ AES_256_ CBC_SHA	ECDH-RSA-AES256-SHA	[0xc00f]	SSLv3	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ ECDH_ ECDSA_ WITH_ AES_256_ CBC_SHA	ECDH-ECDSA-AES256-SHA	[0xc005]	SSLv3	Kx=ECDH/ECDSA	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	[0x9d]	TLSv1.2	Kx=RSA	Compliant	Supported
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	[0x3d]	TLSv1.2	Kx=RSA	Compliant	Supported
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	[0x35]	SSLv3	Kx=RSA	Compliant	Supported
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	[0x84]	SSLv3	Kx=RSA	Non-Compliant	Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	[0xc012]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	[0xc008]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	[0x16]	SSLv3	Kx=DH	Compliant	Not Supported
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA	[0x13]	SSLv3	Kx=DH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	[0xc00d]	SSLv3	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	[0xc003]	SSLv3	Kx=ECDH/ECDSA	Compliant	Not Supported
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	[0x0a]	SSLv3	Kx=RSA	Compliant	Supported
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	[0xc02f]	TLSv1.2	Kx=ECDH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ ECDHE_ ECDSA_ WITH_ AES_128_ GCM_ SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	[0xc02b]	TLSv1.2	Kx=ECDH	Compliant	Not Supported
TLS_ ECDHE_ RSA_ WITH_ AES_128_ CBC_ SHA256	ECDHE-RSA-AES128-SHA256	[0xc027]	TLSv1.2	Kx=ECDH	Compliant	Not Supported
TLS_ ECDHE_ ECDSA_ WITH_ AES_128_ CBC_ SHA256	ECDHE-ECDSA-AES128-SHA256	[0xc023]	TLSv1.2	Kx=ECDH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	[0xc013]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	[0xc009]	SSLv3	Kx=ECDH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256	[0xa2]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	[0x9e]	TLSv1.2	Kx=DH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	[0x67]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256	[0x40]	TLSv1.2	Kx=DH	Compliant	Not Supported
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	[0x33]	SSLv3	Kx=DH	Compliant	Not Supported
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA	[0x32]	SSLv3	Kx=DH	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA	[0x9a]	SSLv3	Kx=DH	Non-Compliant	Not Supported
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA	[0x99]	SSLv3	Kx=DH	Non-Compliant	Not Supported
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	[0x45]	SSLv3	Kx=DH	Non-Compliant	Not Supported
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE-DSS-CAMELLIA128-SHA	[0x44]	SSLv3	Kx=DH	Non-Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ ECDH_ RSA_ WITH_ AES_128_ GCM_ SHA256	ECDH-RSA-AES128-GCM-SHA256	[0xc031]	TLSv1.2	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ ECDH_ ECDSA_ WITH_ AES_128_ GCM_ SHA256	ECDH-ECDSA-AES128-GCM-SHA256	[0xc02d]	TLSv1.2	Kx=ECDH/ECDSA	Compliant	Not Supported
TLS_ ECDH_ RSA_ WITH_ AES_128_ CBC_ SHA256	ECDH-RSA-AES128-SHA256	[0xc029]	TLSv1.2	Kx=ECDH/RSA	Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256	[0xc025]	TLSv1.2	Kx=ECDH/ECDSA	Compliant	Not Supported
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	[0xc00e]	SSLv3	Kx=ECDH/RSA	Compliant	Not Supported
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	[0xc004]	SSLv3	Kx=ECDH/ECDSA	Compliant	Not Supported
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	[0x9c]	TLSv1.2	Kx=RSA	Compliant	Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	[0x3c]	TLSv1.2	Kx=RSA	Compliant	Supported
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	[0x2f]	SSLv3	Kx=RSA	Compliant	Supported
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA	[0x96]	SSLv3	Kx=RSA	Non-Compliant	Supported
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	[0x41]	SSLv3	Kx=RSA	Non-Compliant	Supported
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA	[0x07]	SSLv3	Kx=RSA	Non-Compliant	Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	[0xc011]	SSLv3	Kx=ECDH	Non-Compliant	Not Supported
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	[0xc007]	SSLv3	Kx=ECDH	Non-Compliant	Not Supported
TLS_ECDH_RSA_WITH_RC4_128_SHA	ECDH-RSA-RC4-SHA	[0xc00c]	SSLv3	Kx=ECDH/RSA	Non-Compliant	Not Supported
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	ECDH-ECDSA-RC4-SHA	[0xc002]	SSLv3	Kx=ECDH/ECDSA	Non-Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	[0x05]	SSLv3	Kx=RSA	Non-Compliant	Supported
TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA	[0x15]	SSLv3	Kx=RSA	Non-Compliant	Not Supported
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-DES-CBC-SHA	[0x12]	SSLv3	Kx=DSS	Non-Compliant	Not Supported
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA	[0x09]	SSLv3	Kx=RSA	Non-Compliant	Supported
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA	[0x14]	SSLv3	Kx=DSS	Non-Compliant	Not Supported

Cipher Suite Name (RFC)	Name (OpenSSL)	Cipher Suite	TLS Version	KeyExch.	FIPS	Private Key
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA	[0x11]	SSLv3	Kx=DSS	Non-Compliant	Not Supported
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA	[0x08]	SSLv3	Kx=DES	Non-Compliant	Supported

Edit Decoder System Configuration

When a service is first added to NetWitness Suite, default values for the system configuration parameters are in effect. In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance. You do not need to edit these setting unless an RSA Customer Support technician advises you to change them.

System Configuration

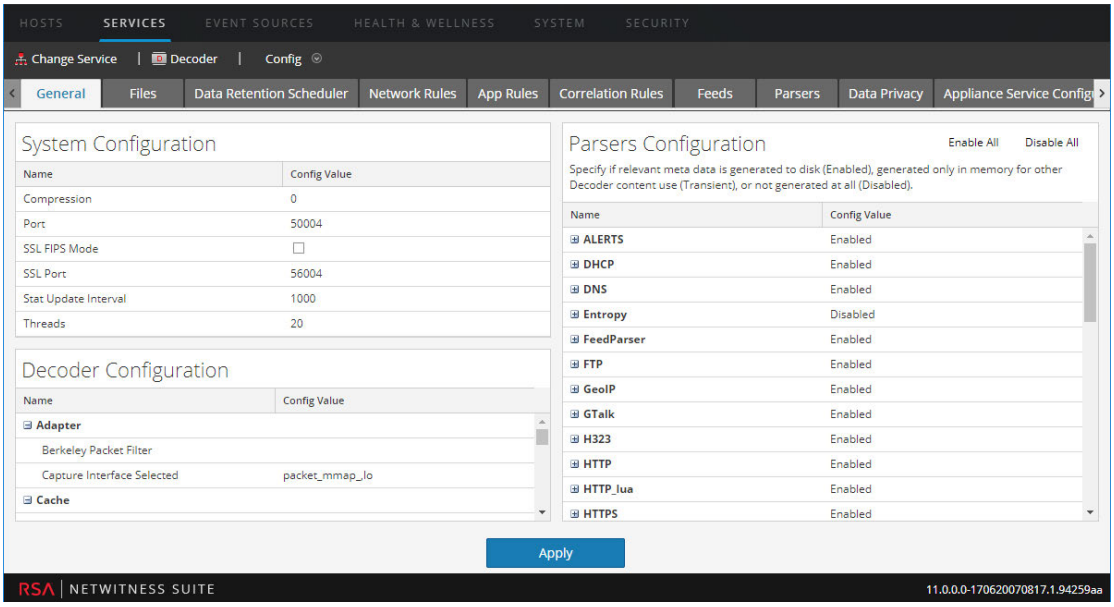
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

One parameter that you may want to change for your environment is the SSL setting, which by default is not enabled. When enabled, the security of data transmission is managed by encrypting information and providing authentication with SSL certificates.

To edit system configuration parameters for a Decoder or Log Decoder:

1. Go to**ADMIN > Services**.
2. In the Admin > System view, select a Decoder or Log Decoder service, and select **> View > Config**.

The Services Config view for the service is displayed with the General tab open.



3. Under **System Configuration**, click in a field that you want to edit **(Compression**, **Port**, **SSL FIPS Mode**, **SSL Port**, **Stat Update Intervals**, or **Threads)**. Type a new value.
4. When finished editing, click **Apply.**
   The settings become effective immediately.

Enable CPU Usage Statistics for Installed Content

Beginning with NetWitness Suite 11.0, the Decoder provides CPU utilization statistics for all installed content, which you can use to reveal how much CPU time is used by parsers, feeds, application rules, and lexical scanning. The statistics are visible as Stat nodes in the service tree from the Explorer view when **/decoder/parsers/config/detailed.stats** is enabled and the Decoder is capturing the stats.

Each piece of content is accounted as a single percentage value (0-100) regardless of the number of parse threads running. The percentage represents an average of the CPU utilization for the content across all threads.

To enable usage statistics monitoring:

1. Navigate to the Decoder Explorer view and select the `/decoder/parsers/config/detailed.stats` parameter.
2. Change the value to **enabled**. If the Decoder is not capturing data, start capture.
   When you open the Decoder Stats node in the Explorer view, the new statistic is visible.

Enable Parser Mappings

This topic tells administrators how to enable event source mapping on a Log Decoder.

The Log Collector discovers the event source type on a per-message basis. If the correct parser is not identified for the event source, a small percentage of logs may be misidentified. The misclassified messages do not populate event source rules and alerts, and the reports do not have the correct data. If there are multiple event source types associated with an IP address, it makes it difficult for the parsers to identify the exact event source from which the logs are generated.

If you map an IP address to its event source type, the Log Decoder can identify the event source from which the log is generated. When messages are delivered to the Log Decoder from a mapped event source, only the assigned parsers are queried to find event matches.

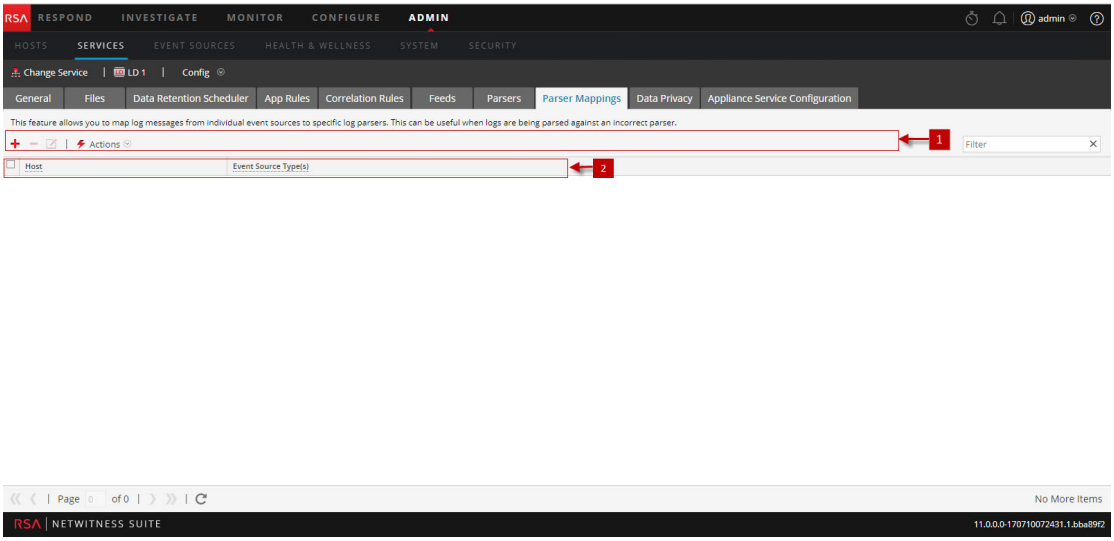
You can assign event source types to IPV4, IPV6, or the hostname value of the event source. You can also assign multiple event source types to a single IP address. You can also use the Log Collector ID when different event source types with the same IP address are sent to different Log Collectors.

Note: You can also enable parser mapping functions by navigating to **ADMIN > Event Sources > Discovery.**

Enable IP Address to Event Source Mapping

To enable an IP address to event source mapping:

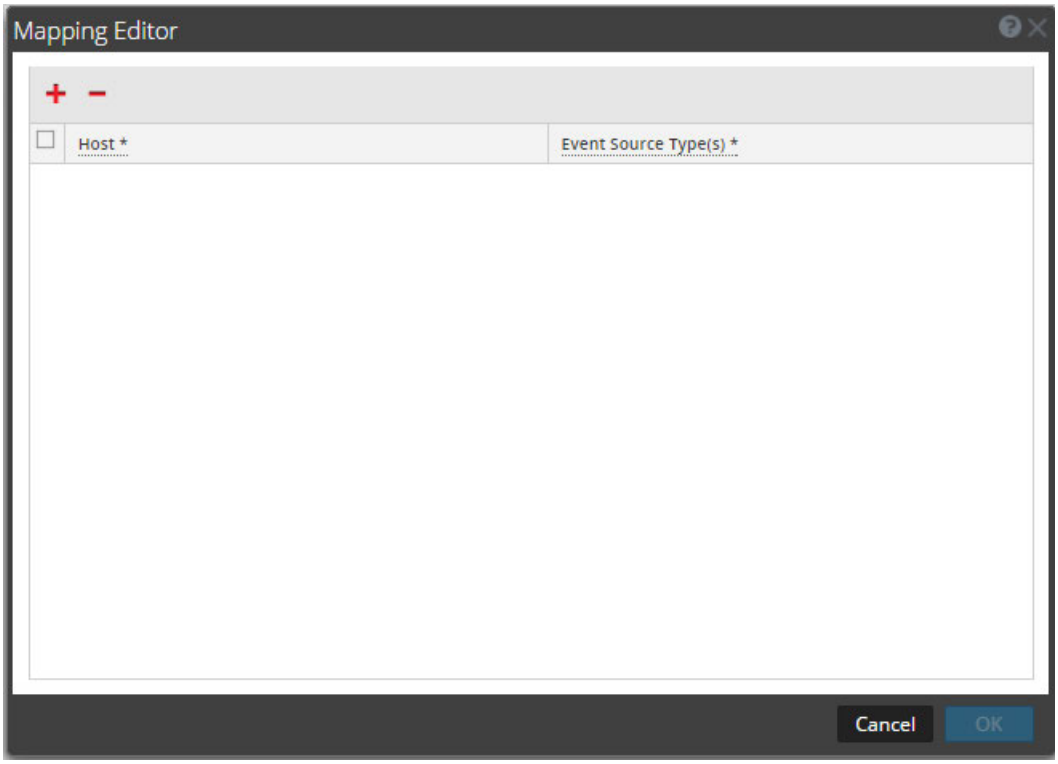
1. Go to **ADMIN > System > Log Parser Mappings**.
2. Select **Decoder**, then select > **View** > **Config**.
3. In the Configuration page, select the **Parser Mappings** tab.
   The Parser Mappings tab is displayed in the Services Config view.



Update IP to Event Source Mapping

To update an IP to event source mapping:

1. Go to **ADMIN > Services**.
2. Select a **Log Decoder**, and in the **Actions** column, select > **View** > **Config**.
   The Services Config view is displayed.
3. Select the **Parsers Mapping** tab.
4. Click .
   The Mapping Editor is displayed.



5. Any of the following mappings can be defined:

One Host and One Event Source Type
- In the **Host** field, enter the hostname.
  For example: `10.0.0.1`
- In the **Event Sources**(s) field, enter the event source type.
  For example: `apache`

One Host and One or More Event Source Types
- In the **Host** field, enter the hostname.
  For example: `10.0.0.1`
- In the **Event Source(s)** field, enter the event source type.
  For example: `apache,sap,aix`

One Host, One Log Collector, and One Event Source Type

- In the **Host** field, enter the hostname and Log Collector ID.
  For example: `10.0.0.1,LC-1`.
- In the **Event Source(s)** field, enter the event source type.
  For example: `apache`

One Host, One Log Collector ID, and One or More Event Source Types

- In the **Host** field, enter the hostname and Log Collector ID.
  For example: `10.0.0.1,LC-1`
- In the **Event Source(s)** field, enter the event source type.
  For example: `apache,sap,aix`

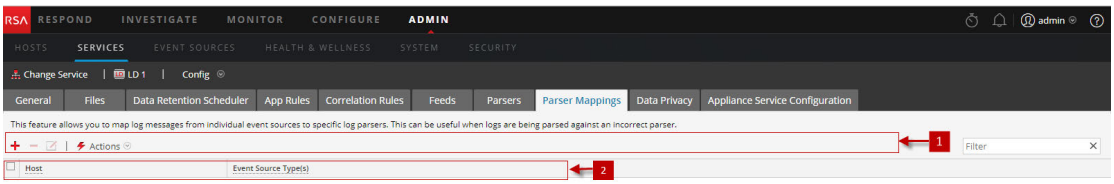
Note: The event source types are processed in the order you enter the parsers and if one or more parsers matches a log, the first parser in the list is queried. The Host/IP can be IPv4, IPv6, or Hostname.

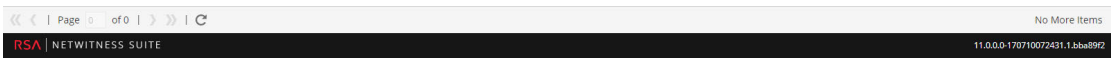
6. Click **OK**.
   The Parser Mapping is added.
7. To cancel the parser mappings selection, click **Cancel**.

Read IP to Event Source Type Mappings

To read an IP to event source type mappings:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select **> View > Config**.
   The Services Config view is displayed.
3. Select the **Parsers Mapping** tab.
   The mappings are displayed.





Edit an IP to Event Source Type Mapping

To edit an IP to event source type mapping:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select **> View > Config**.
   The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mapping you want to edit.
   Note: You can only edit one mapping at a time.
5. Click
6. In the **Event Source(s)** field, modify the event source(s).
   Note: The host is not editable and the field is disabled.
7. Click **OK** to accept the edited Event Source.
8. To cancel the changes, click **Cancel**.

Delete an IP to Event Source Type Mapping

To delete an IP to event source type mapping:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select **> View > Config**.
   The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mapping you want to delete.
5. Click .
   The mapping is deleted and the grid is refreshed.
6. To cancel the changes, click **Cancel**.

Sort the Hostname or Event Source Type

To sort the hostname or event source type:

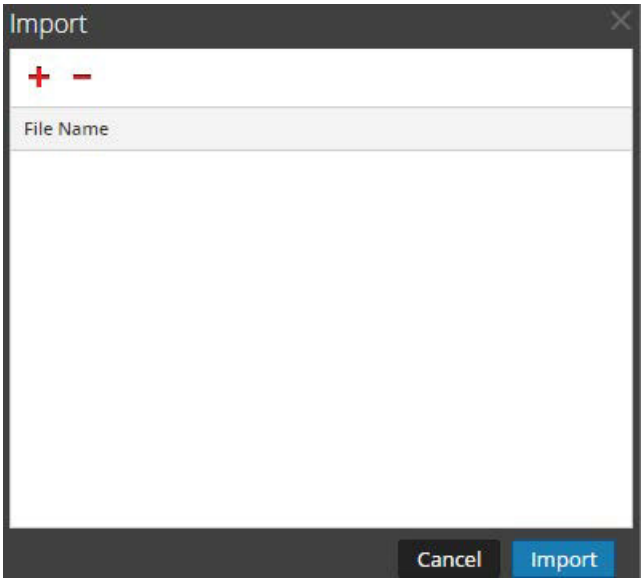
1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select **> View > Config**.
   The Service Config view is displayed.

3. Select the **Parser Mappings** tab.
4. To sort a column, click in the column header.
   Event Source Type(s) are applied for your selected IP address. Logs are parsed against the parsers in the order they are listed.

Import IP to Event Source Mapping Entries

To import IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select **> View > Config**.
   The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select **Actions > Import**.
   The Import dialog is displayed.



5. Click .
6. Select the file you want to import and click **OK**.
7. To load the parser, click **Import**.

Note: You can only import one .csv file at a time.

Export IP to Event Source Mapping Entries

To export IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select > **View** > **Config**.
   The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mappings you want to export.
5. Select **Actions** > **Export** > **Selection**.
   The Export Selection dialog is displayed.

6. Enter the file name and click **Export**.

Search IP to Event Source Mapping Entries

To search IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select > **View** > **Config**.
   The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. In the Parsers Mappings toolbar, enter the Host or Event Source in the **Filter** field.
5. Click **Enter**.
   The Hosts or Event Sources that match the names entered in the **Filter** field are displayed.

Enable or Disable Lua and Flex Parsing Systems

This topic tells administrators how to enable or disable Lua and Flex parsing systems on a Decoder or Log Decoder. Flex parsers are deprecated and disabled by default.

The settings to enable or disable Lua and Flex parsing systems are configured correctly by default and you do not typically have to change them. However, you may need to adjust these settings at the request of RSA Customer Care or for troubleshooting purposes.

In addition to configuring individual parsers, you can enable and disable all Lua parsing as well as all Flex parsing in the Services Explore view. You enable and disable the Lua parsing and Flex parsing systems settings separately, but they work in the same way.

- If you **disable** the Lua or Flex parsing system, the corresponding parsing system is disabled and no parsers are loaded.
- If you **enable** the Lua or Flex parsing system, the corresponding parsing system is enabled and individual parsers are enabled and disabled following the current individual configurations.

To enable or disable Lua and Flex parsing systems on a Decoder or Log Decoder:

1. Go to **ADMIN > Services.**
2. Select a Decoder or Log Decoder and **> View > Explore.**
   The Services Explore view for the selected service is displayed.
3. In the Node list, navigate to and select **/decoder/parsers/config**.
4. In the Monitor panel:
   - To enable the Lua parsing system, in the value field for `lua.enabled`, type **yes**.
   - To disable the Lua parsing system, in the value field for `lua.enabled`, type **no**.
   - To enable the Flex parsing system, in the value field for `flex.enabled`, type **yes**.
   - To disable the Flex parsing system, in the value field for `flex.enabled`, type **no**.

Map IP Address to Service Type for Log Parsing

This topic describes the procedure to map an IP address to a service type for log parsing.

The Log Collector discovers event source type on a per-message basis. If the correct parser is not used for the specific event source, the messages that are common between event source types are misclassified. The misidentified messages will not populate service rules and alerts, and the reports will not have proper information. Also, if there are multiple services associated with an IP address, it can be difficult for the parsers to identify the exact service from which the log is generated.

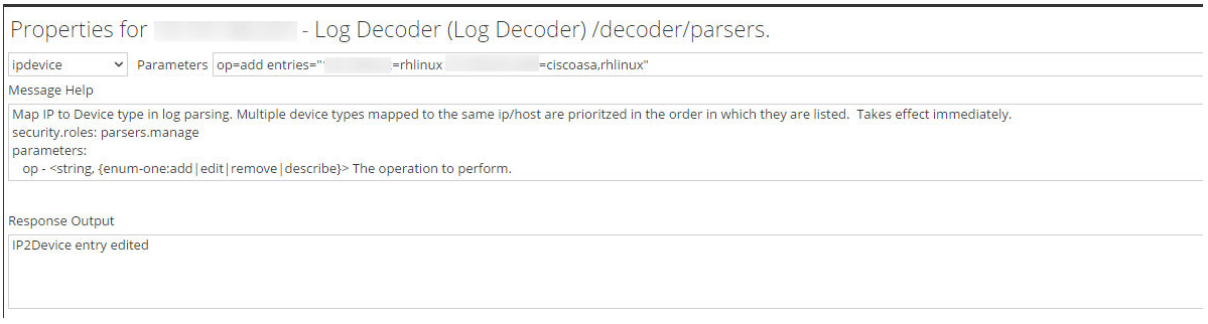
If you map an IP address to its services, the log decoder can identify the service from which the log is generated. When messages come into the log decoder from a mapped service, the assigned parsers are loaded to find event matches.

You can assign service types to IPV4, IPV6 or hostname value of the event source. You can also assign multiple service types to a single IP address. You can also use the CollectorID when different service types with the same IP address are sent to different collectors.

Map an IP Address to a Service Type

To map an IP address to a service type, do the following:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Log Decoder, and in the **Actions** column, select **> View > Explore**.
3. Go to **/decoder/parsers** node, right-click **parsers**, and select **Properties**.
4. In the **Properties** view, specify the **ipdevice** command with the following parameters: `op=add/remove entries="ipaddress=service"` (for example, `op=add entries="10.100.201.300=ciscoasa"`)
5. Click **Send**.



IPdevice Command

In the `ipdevice` command, three operations are available:

- `add`: This operation adds or updates entries in the ipdevice map. Multiple space delimited address/type pairs may be specified.
  `op=add entries="<address>=<service type>"`
- `remove`: This operation removes entries from the ipdevice map. Multiple space delimited address/type pairs may be specified.
  `op=remove entries="<address>"`
- `describe`: This operation returns the values currently in the ipdevice map.

Map an IP Address to a Time Zone

Often times logs do not fully specify timestamps and may be missing time zone information. To properly normalize such timestamps to UTC, the Log Decoder provides the ability to associate devices from a specific address (IPv4 or IPv6) or hostname to a time zone or a fixed offset.

Three time zone formats are currently accepted and are shown in the following examples:

- Olson format: America/Anguilla
- POSIX format: AST2:45ADT0:45,M4.1.6/1:45,M10.5.6/2:45
- Offset by Hours format: = -500

NetWitness Suite maps the device address (IPv4 or IPv6) or hostname to a specific time zone or offset. Event time meta that is parsed from a log that is from a mapped address and does not include an offset or time zone as part of the timestamp is adjusted to UTC according to the mapping.

To map an IP address to a time zone, do the following:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Log Decoder, and in the **Actions** column, select **> View > Explore**.
3. Go to **/decoder/parsers** node, right click **Parsers**, and select **Properties**.
4. In the **Properties** view, specify the `iptmzone` command with the following parameters:
   `op=add entries="ipaddress=timezone" (for example, op=add entries="10.10.10.10=Africa/Addis Ababa")`
5. Click **Send**.

iptmzone Command

In the `iptmzone` command, three operations are available:

- `add`: This operation adds or updates entries in the iptmzone map. Multiple space delimited address/type pairs may be specified.
  `op=add entries="<address>=<time zone>"`
- `remove`: This operation removes entries in the iptmzone map. Multiple space delimited address/type pairs may be specified.
  `op=remove entries="<address>"`
- `describe`: This operation returns the values currently in the iptmzone map.

Examples

The following examples provide instances fro mapping IP addresses to time zones:

- If you want to map two different entries with different IPV4 values and time zone, enter the following parameter in the **iptmzone** command and click **Send**
  `"op=add entries=”10.10.10.10=America/Anguilla 10.10.10.11=Pacific/Rarotonga”`
- If you want to remove an entry for a single IPV4 value and time zone, enter the following parameter in the **iptmzone** command and click **Send**.

```
"op=remove entries=10.5.245.9"
```

- If you want to create a single entry for an IPV6 value and time zone, enter the following parameter in the **iptmzone** command and click **Send**.

```
op=add entries=”2001:DB8:85A3::8A2E:370:7334=America/Anguilla”
```

- If you want to create a single entry to map an IPV4, IPV6, or hostname with the Minute Offset, Olson, or POSIX format,enter the following parameter in the **iptmzone** command and click **Send**.

```
op=add entries="10.168.0.2=America/Anguilla
2001:DB8:85A3::8A2E:370:7334=0500nwappliance21=EST5EDT,M3.2.0/2
,M11.1.0"
```

Obtain Log Files a from Pre-11.0 Log Decoder

NetWitness 11.0. added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available.

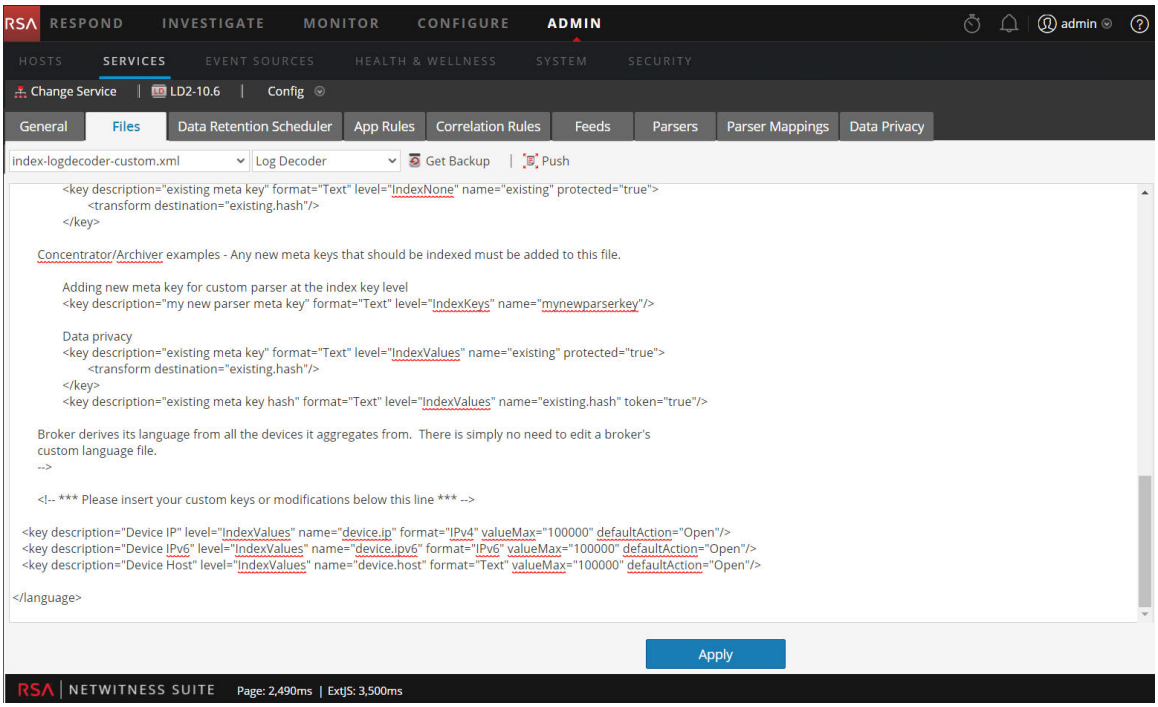
To enable logs preview for a pre-11.0 Log Decoder, follow these steps on the Log Decoder:

1. Go to **ADMIN > Services >** select a **Log Decoder**, then select **> View > Config**.
2. Click the **Files** tab and select **index-logdecoder-custom.xml** from the drop-down menu.
3. Add the following three lines at the end of the file (before the closing language tag):

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
valueMax="100000" defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

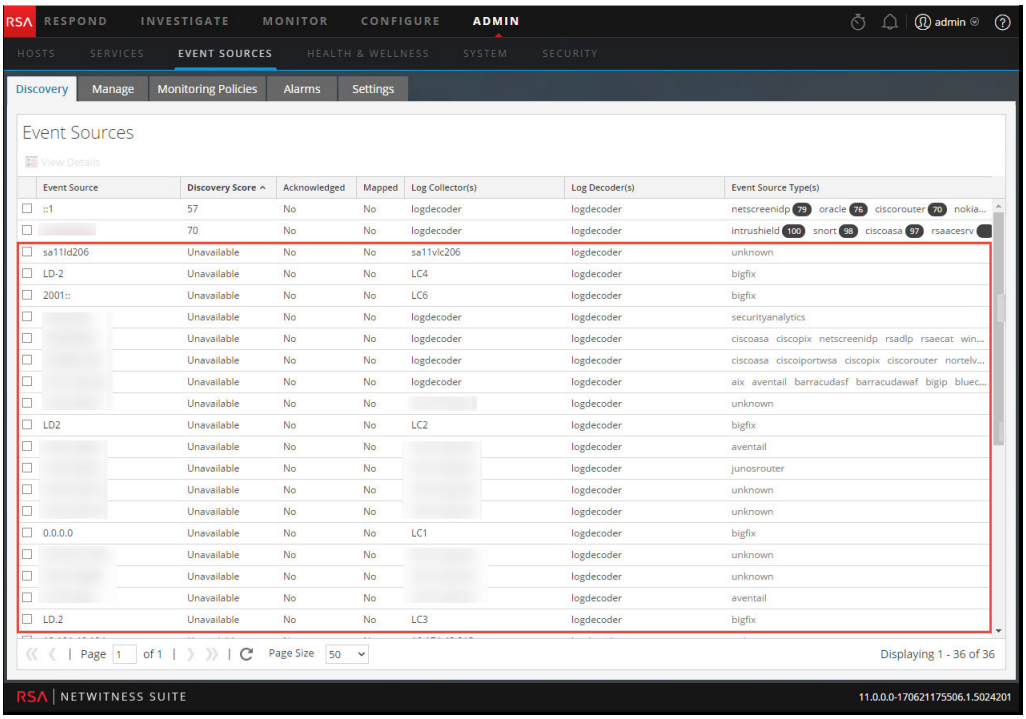
4. Click **Apply**.
5. Restart the Log Decoder service as follows.
   Select Log Decoder service **> Explore > decoder > Properties > reset**

This is an example of the **index-logdecoder-custom.xml** file.



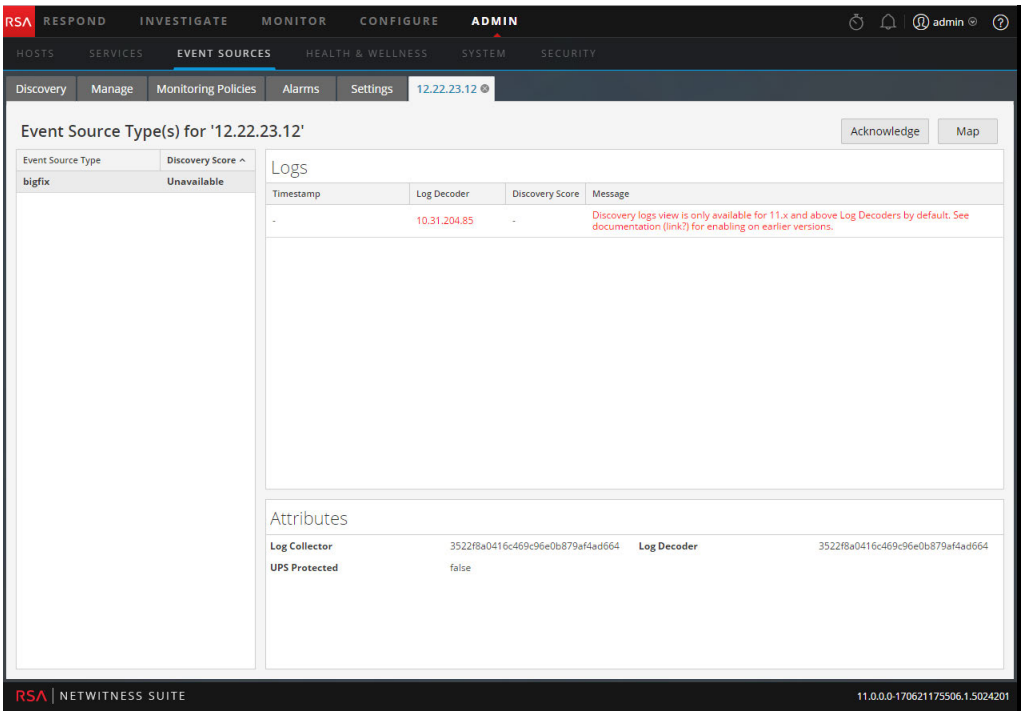
Note: Discovery Scores are only available for 11.x and above Log Decoders. Discovery Scores for pre-11.x Log Decoders are displayed as Unavailable.

The following example shows the Discovery Score as **Unavailable** in the **Details** view for a pre-11.0 Log Decoder.



Note: Device logs are only available for 11.x and above Log Decoders.

The following example shows the message that is displayed in the Logs panel for a pre-11.0 Log Decoder.



Upload a Log File to a Log Decoder

This topic describes the method for importing a log file to a Log Decoder.

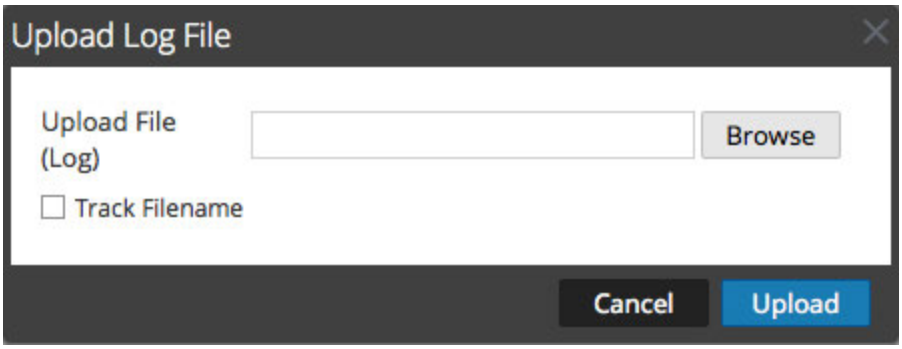
There are occasions when you want to analyze a log file that is not available on the service you are using. You can upload a log file captured on another service to NetWitness Suite. Log filenames are of the type **.log**.

When a log file is uploaded to a Log Decoder, the Log Decoder analyzes and generates meta for each log it contains. These logs are added to the already decoded logs on the Log Decoder and are available for analysis. NetWitness Suite includes a filename tracking option that makes searching for a particular set of logs easier. When the log file is uploaded with file tracking, the Log Decoder adds meta to each log based on the uploaded filename. You can then filter sessions for analysis using that meta.

The option to upload a log file is dimmed when other Log Decoder operations prevent an upload from occurring. For example, when the Log Decoder is capturing logs.

To import a log file to an Log Decoder:

1. Go to **ADMIN > Services**.
2. Select a Log Decoder in the **Service** grid, and select > **View** > **System**.
   The Services System view for the Log Decoder is displayed.
3. In the toolbar, click **Upload Log File**.



4. To choose a log file, click **Browse**.
   A directory view is displayed.
5. Select the log file that you want to upload.
   The filename is displayed in the **Upload File** field.
6. If you want the Log Decoder to add meta to the logs based on the filename, click the checkbox next to **Track Filename**.

7. To upload the file, click **Upload**.
   The selected file is uploaded and a status message indicates that the file is uploaded. The log file is available for analysis.

Upload a Packet Capture File

There are occasions when you want to analyze a packet capture file that is not available on the service you are using. You can upload a file captured on another service to NetWitness Suite. Supported packet capture file types are `pcap` and `pcap.gz`.

When a packet capture file is uploaded to a Decoder, the Decoder creates sessions from the packet capture file packets. These sessions are added to the already decoded sessions on the Decoder and are available for analysis. NetWitness Suite includes a filename tracking option that makes searching for a particular set of sessions easier. When the packet capture file is uploaded with file tracking, the Decoder adds meta to the sessions based on the uploaded filename. You can then filter sessions for analysis using that meta.

The option to upload a packet capture file is dimmed when other Decoder operations prevent an upload from occurring; for example, when the Decoder is capturing packets.

To select and upload a packet capture file:

1. Go to **ADMIN >Services**.

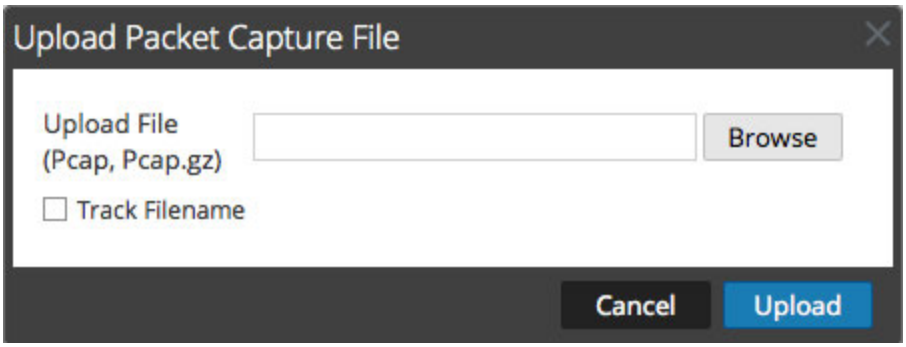
   The Administration Services view is displayed.

2. Select the Decoder name, and > **View** > **System**.

   The Services System view for the Decoder is displayed.

3. In the toolbar, click **Upload Packet Capture File**.

   The **Upload Packet Capture File dialog** is displayed.



4. To choose a capture file, click **Select**.

   A directory view is displayed.

5. Browse the directory and select the packet capture file that you want to upload.

   The filename is displayed in the **Upload File(pcap,pcap.gz)** field.

6. If you want the Decoder to add meta to the sessions based on the filename, click the checkbox next to **Track Filename**.

7. To upload the file, click **Upload**.

   A progress bar shows upload progress.

   Upload time varies depending on the size of the file. When the file upload is complete, a status message is displayed. The file is now available for investigation.

Feed and Parser References

This topic provides more details about the feeds and parsers that the Decoder uses.

- Feed Definitions File
- Flex Parsers
- Geo IP Parser
- Lua Parsers
- Search Parser
- Wireless LAN Configuration

Feed Definitions File

This topic introduces the feed definitions file, which is available for editing in the Services Config view > Files tab.

One of the files available for editing in the Services Config view > Files tab is **`feed-definitions.xml`**, the feed definitions file.

feed-definitions.xml

You can define feeds in the `feed-definitions.xml` file. The Decoder uses an XML schema to define feed messages when it creates a binary .feed file from the feeds defined here.

For details on the feed definition language, refer to the NextGen System Administrator Guide.

Flex Parsers

One of the files available for editing in the Services Config view > Files tab is **NwFlex.xml**, the flex parser.

NwFlex.xml

There are two kinds of Flex parsers:

- **Service identification based solely on port.** These are parsers that use only the source or destination ports to identify the session application type (service). These are the most basic and easiest to define.
- **Service identification based on a found token(s).** These parsers use tokens to identify the service type. This is also an easy way to expand which service types are identified. These are important when identifying non -internet standard applications. These parsers require that the protocol has a definable token that can uniquely identify the service type.

Five common parser operations are:

- Match Port and Identify Immediately
- Match Port and Delay Identification
- Match Token and Identify Immediately
- Match Multiple Tokens
- Match Token and Create Metadata

Detailed language information and samples are provided in this topic. This topic describes the XML schema used to define a FlexParse file. The SML node, attribute, and values referenced in descriptive text are **bold**. The root node of every file must be the **parsers** node. Under that node there can be any number of parser nodes. Each parser node defines a single parser.
A parser node can have an optional **declaration** node and any number of **match** nodes.

Topics

- Arithmetic Functions
- Common Parser Operations
- General Functions
- Logging Functions

- Nodes
- Payload Functions
- Regex
- String Functions

Arithmetic Functions

This topic defines language for the flex parser arithmetic functions.

This topic defines language for the flex parser arithmetic functions. All numbers are 64-bit unsigned values and subject to both underflow and overflow, depending on the operation.

Language Definition

The following table provides language definitions.

Node Name	Attribute Name	Description
and		Performs bitwise AND between two numbers.
	name	Variable to AND result into.
	value	Number to AND into result.
or		Performs bitwise OR between two numbers.
	name	Variable to OR result into.
	value	Number to OR into result.
increment		Performs ADDITION of two numbers.
	name	Variable containing the initial value AND to receive ADDITION results.
	value	Number to ADD to initial value.
decrement		Performs SUBTRACTION of two numbers.
	name	Variable containing initial value AND to receive SUBTRACTION results.
	value	Number to SUBTRACT from initial value.
divide		Performs DIVISION of two numbers.

Node Name	Attribute Name	Description
	name	Variable containing the initial value AND to receive DIVISION results.
	value	Number by which to divide the initial value. Division by zero generates an error and stops any further processing of the current session by this parser.
modulo		Performs MODULO of two numbers.
	name	Variable containing the initial value AND to receive MODULO results.
	value	Number by which to divide the initial value. Division by zero generates an error and stops any further processing of the current session by this parser.
multiply		Performs MULTIPLICATION of two numbers.
	name	Variable containing the initial value AND to receive MULTIPLICATION results.
	value	Number by which to MULTIPLY the initial value.
shiftleft		Performs a binary shift left.
	name	Variable containing the initial value AND to receive shift results.
	value	Number of bits to shift by.
shiftright		Performs a binary shift right.
	name	Variable containing the inital value AND to receive shift results.
	value	Number of bits to shift by.

Common Parser Operations

This topic provides some examples of common parser operations.

This topic includes five common parser operations.

Match Port and Identify Immediately

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
          <parser name="CustApp" desc="Acme Custom App" service="45324">
               <declaration>
                    <port name="port" value="45324" />
               <declaration>
               </match name="port">
                    <identify />
               </match>
          </parser>
</parsers>
```

Match Port and Delay Identification

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MSRPC" desc="Microsoft RPC protocol" service=135">
          <declaration>
               <port name="port" value="135" />
               <number name="state" scope="session" />
               <session name="end" value="end" />
          </declaration>
          <match name="port">
               <assign name="state" value="1" />
          </match>
          <match name="end">
```

```
            <if name="state" equal="1" />
                 <identify />
            </if>
        </match>
    </parser>
</parsers>
```

Match Token and Identify Immediately

```
<?xml version="1.0" encoding="utf-8?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="RDP" desc="Remote Desktop Protocol" service="3389">
          <declaration>
               <token name="signature" value="Cookie: mstshash=" />
          </declaration>
          <match name="signature">
               <identify />
          </match>
     </parser>
</parsers>
```

Match Multiple Tokens

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MyServiceMultiToken" desc="Multiple Tokens"
     service="333">
          <declaration>
               <number name="state" scope="stream" />
               <token name="user" value="USER " />
               <token name="pass" value="PASS " />
               <session name="session" value="end" />
          </declaration>
```

```
          <match name="user">
               <or name="state" value="1" />
          </match>
          <match name="pass">
               <or name="state" value="2" />
          </match>
          <match name="session">
               <if name="state" equal="3">
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Match Token and Create Metadata

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="SHELL" desc="Command Shell Identification">
          <declaration>
               <token name="cmd.exe" value=" (C) Copyright 1985-2001
               Microsoft Corp" options="linestart" />
               <meta name="client" key="client" format="Text" />
          </declaration>
          <match name="cmd.exe"
               <register  name="client" value="MS Command Shell" />
          </match>
     </parser>
</parsers>
```

General Functions

This topic defines language for the flex parser general functions.

General Functions Language Definition

Node Name	Attribute Name	Description
apptype		Gets the currently defined service type for the current session.
	name	A number variable to receive the current service type.
identify		Marks the session with the parser's service type if the service type has not already been identified.
assign		Assigns a value to a variable.
	name	The unique identifier assigned to the item in the declaration section.
	value	Optional. If specified, the action defined in the match is only applied when the declaration matches the given value.
getmeta		Retrieves the value of meta that generated a callback. This function will return empty results (0, zero length string) if called when there was no meta callback.
	name	The variable to receive the value of the meta that generated the callback.OK.
gettoken		Returns the current matched token.
	name	A string variable to receive the current matched token. If there is no current token, the variable is assigned an empty string.
end		This terminates the execution of the current **match** section.

Node Name	Attribute Name	Description
if		Compares two values. If the comparison is true, executes any sub-actions. Comparisons can be **number** or **string** types, as long as both values are the same type.
	name	The unique variable identifier assigned to the item in the **declaration** section.
	equal notequal less lessequal greater greaterequal and or	The operation value to compare. If true, any sub-actions are executed.
register		Adds metadata to the session.
	name	The unique identifier of a meta variable to be created, as defined in the **declaration** section.
	value	The value of the metadata to be created.
while		Compares two values and executes any sub-actions if the comparison is true. Comparisons can be **number** or **string** types, as long as both values are the same type.
	name	The unique variable identifier assigned to the item in the declaration section.

Node Name	Attribute Name	Description
	equal notequal less lessequal greater greaterequal and or	Specifies the operation value to compare. If true, any sub-action is executed. The **and** and **or** attributes signify bitwise operations and can only be applied to **number** variables.
call		Execute the specified **match** element. This can be any match element defined in the same flex parser regardless of how it was declared.
	value	The name of the match element, or a string variable containing the name of a match element. • If the match element name is specified, the parser will not load if the named matched element doesn't exist. • If a string variable is specified, the **call** element will execute any child elements that it may have if the string value resolves to a match element after executing the named match element. • If no **match** element can be found matching the string value, no action is taken.

Logging Functions

This topic defines language for the flex parser logging functions.

Logging functions provide a means for a flex parser to write to the system log. Logging functions can be extremely useful when creating a new flex parser, but should be kept to an absolute minimum when a flex parser is deployed to a production system.

Language Definition

Node Name	Attribute Name	Description
`failure`		Logs a message to the system log with the log level **Failure.**
	`value`	A string to include as the log message.
`warning`		Logs a message to the system log with the log level **Warning.**
	`value`	A string to include as the log message.
`info`		Logs a message to the system log with the log level **Info**.
	`value`	A string to include as the log message.
`debug`		Logs a message to the system log with the log level **Debug.**
	`value`	A string to include as the log message.

Nodes

This topic defines language for the flex parser nodes.

Nodes Language Definition

Node Name	Attribute Name	Description
`parsers`		The root node in each definition file.
	`xmins:xsi`	Defines the namespace to use for the schema inclusion. This attribute is not required; however, language definition is not possible without it. This node must have the following value: http://www.w3.org/2001/XMLSchema-instance
	`xsi:noNamespaceSchemaLocation`	Defines the XSD schema validation file used to validate the language definition. This attribute is not required; however, language definition is not possible without it. This node must have the following value: parsers.xsd
`parser`		The node that defines a single parser definition. This node must be directly under the `parsers` node. There can be more than one per file.

Node Name	Attribute Name	Description
	name	The name that uniquely identifies the parser. This name should be short and succinct. This is used by the system to allow enabling and disabling. It should contain only the letters [a-z] and [A-Z].
	desc	This node provides a friendly description of what the parser does.
	service	This is the unique number assigned to the session when identified.
declaration		The node that delineates the definition. Each of these definitions can have an associated match entry.
token		Specifies a definition for identifying a token somewhere in the session protocol. This defines a match callback when the specified tokens are encountered in a session payload. The read position is set to the byte immediately following the matched token.
	name	This is a unique identifier for the declaration.
	value	This is the exact token value to be identified.

Node Name	Attribute Name	Description
	options	Options specify that the token should start on a new line or at an end of a line (linestart or linestop).
meta-callback		Registers a callback for the flex parser whenever meta of a specific format is created. This can be further qualified to generate callbacks only for sessions that have been identified as a specific apptype (e.g. 80 for http).
	name	Name of the match element to be executed when a callback occurs. (String)
	key	Name of the meta key that generates callbacks. (String)
	format	The data type of the meta key that will generate the meta.
	apptype	The meta callback is only generated if the session being parsed has been identified with the specified apptype. (Unsigned Integer, Optional)
number		Defines a numeric variable that can be referenced elsewhere within the parser definition. All numeric values are 64-bit unsigned values.

Node Name	Attribute Name	Description
	`name`	This is a unique identifier for the declaration.
	`scope` (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are **`global`**, **`constant`**, **`stream`**, and `session` (default).
`string`		Defines a numeric variable that can be referenced elsewhere within the parser definition.
	`name`	This is a unique identifier for the declaration.
	`scope` (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are **`global`**, **`constant`**, **`stream`**, and `session` (default).
port		Defines a **match** callback when a session is encountered using the specified port. The **read** position is set to the first byte of the first stream (client) in the session.
	`name`	This is a unique identifier for the declaration.

Node Name	Attribute Name	Description
	value	This is the port number to identify.
session		Defines a match callback for session begin/end events. These events only occur if a token for the parser is encountered in the session.
	name	This is a unique identifier for the declaration.
	value	Specifies that processing takes place at the beginning of a new session or at the end of a session (begin or end).
stream		Defines a match callback for stream begin/end events. These events only occur if a token for the parser is encountered in the stream.
	name	This is a unique identifier for the declaration
	value	Specifies that processing takes place at the beginning or at the end of a stream (begin or end).
function		Defines a match section that can be used as a generic function. No callbacks are associated with this declaration.
	name	This is a unique identifier for the declaration.

Node Name	Attribute Name	Description
meta		Defines the type of data that the parser will create.
	key	Specifies the key name. The key needs to be 1-16 bytes in size.
	format	Specifies the variant type (for example, **Text**, **IPv4**, **UInt32**). Refer to the SDK documentation for a full list.
pattern		Defines a regular expression variable for use by the regex function
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can be for each side of a two-sided session or only after a new session is detected. Possible values are **global**, **constant**, **stream**, and session (default).
	value (optional)	Specifies a regular expression to assign to the pattern variable. This attribute is only valid when the **scope attribute** is set to constant.

Node Name	Attribute Name	Description
match		The possible entries for taking an action once a match criterion has been found for a declaration. These nodes can be nested to provide deeper logic. There are several categories of execution elements (functions) that can appear as children of a match element: • General • Arithmetic • String • Payload

Payload Functions

This topic defines language for the flex parser payload functions.

These functions operate on a `read` position, set at the beginning of a `match` element.

Language Definition

Node Name	Attribute Name	Description
`find`		Searches the stream payload starting at the read position for a provided string value. If the value is found, the offset from the read position is returned. Any child elements will then execute. If not found, any child elements will not execute.
	`name`	A `number` variable to receive the offset from the `read` position where the match begins.
	`value`	A string to find.
	`length` (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. It is recommended to always use the smallest value possible here in order to reduce the effect on performance.
`install-decoder`		To enable tokens to match on payload data that may be fragmented or otherwise encoded. A scan decoder can be installed to preprocess a section of the payload before it is scanned for tokens. An example would be an HTTP response that uses the chunked transfer encoding with gzip content encoding. By parsing the HTTP header, the necessary type, offset, and length parameters can all be set, after which the HTTP response payload would appear to the token scanning as if neither encoding had been applied. However, this incurs significant overhead.

Node Name	Attribute Name	Description
	`type`	The type of decoder to install. Valid options are: gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	`offset`	Offset from the current read position to begin decoding.
	`length`	The maximum payload length to decode.
`isdecoding`		Tests whether an installed decoder is currently active. If so, any children of this function will execute. This function has no parameters.
`move`		Moves the `read` position forward in the current stream by a specified number of bytes. If there is sufficient data in the stream, the `read` position is updated and any child elements will then execute. If not found, the `read` position remains unchanged and any child elements will not execute.
	`value`	The number of bytes to move the `read` position.
	`direction` (optional)	The direction to move the current read position. Can be `forward` (default) or **`reverse.`**
`packetid`		Returns the id of the packet for the current read position. It is possible for the result to be 0, which indicates that the packet id could not be determined.
	`name`	A number variable to receive the current packet id.
`payload-position`		Returns the current read position. This is a zero based index into the stream payload.
	`name`	A number variable to receive the current read position.

Node Name	Attribute Name	Description
`read`		Reads a specified number of bytes starting at the `read` position into a variable. If there is sufficient data in the stream, the `read` position is updated, the data read assigned, and any child elements will then execute. If not found, the `read` position remains unchanged and any child elements will not execute.
	`name`	The name of a `string` or `number` variable to receive stream data. If a `number` variable is provided, the bytes read are interpreted as a single unsigned numeric value.
	`length`	The number of bytes to read from a stream.
	`endianess` (optional)	The byte ordering to use when reading into a number variable. Can be `big` (default) or `little`. The attribute is invalid when reading into a `string` variable.

Regex

This topic defines language for the flex parser regex node.

Regex searches the stream payload starting at the `read` position for matches to a provided regular expression. If matches are found, the offset from the `read` position and, optionally the matched string, is returned. Any child elements execute. If no matches are found, child elements do not execute.

Language Definition

Attribute Name	Description
`name`	A `number` variable to receive the offset from the `read` position where the match begins.
`value`	A regular expression to find.
`length` (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. It is recommended to always use the smallest value possible here in order to reduce the effect on performance.
`found` (optional)	The name of a `string` variable to receive a matched string.

String Functions

This topic provides language definitions for the flex parser string functions.

String Functions Language Definition

Node Name	Attribute Name	Description
`append`		Attaches a number or string to the end of a `string` variable.
	`name`	The unique identifier of a string variable to which the specified value is to be attached.
	`value`	A number or string to attach.
`find`		Searches a string for a provided string value. If it is found, the position is returned and any child elements will execute. Otherwise, child elements will not execute.
	`name`	A `number` variable to receive the zero-based position, where the provided value string was found in the **in** string.
	`value`	A string to find.
	`in`	A string to search.
	`length` (optional)	A limit to the length of the **in** string to be searched. If a limit is not provided, all of **in** will be searched.
`length`		Assigns the length of a string to a `number` variable.
	`name`	A `number` variable to receive the length of the specified string.

Node Name	Attribute Name	Description
	value	A string value whose length is to be determined.
regex		Searches a string for matches to the provided regular expression. If a match is found, the position and, optionally, the matching string is returned. Any child elements will then execute. If not found, any child elements will not execute. Regular expression operations can adversely affect system performance.
	name	A number variable to receive the zero-based position, where the provided regular expression matched in the in string.
	value	A regular expression to be searched for.
	in	A string to search.
	length (optional)	A limit to the length of the in string to be searched. If a limit is not provided, all of **in** will be searched.
	found (optional)	The name of a string variable to receive the matched string.
substring		At least one of the optional attributes from and length must be specified.
	name	The unique identifier of a string variable to receive the extracted value.
	value	A string value from which to extract a substring.
	from (optional)	The zero-based position from which to begin the substring. If not specified, it defaults to zero.

Node Name	Attribute Name	Description
	`length` (optional)	The number of characters to extract. If not specified, it defaults to the remaining length of the string.
`tolower`		Converts a string to all lowercase letters.
	`name`	The name of a `string` variable to process.
`toupper`		Converts a string to all uppercase letters.
	`name`	The name of a `string` variable to process.
`urldecode`		Decode a string containing url-encoded characters.
	`name`	A string variable to receive the decoded string.
	`value`	A url-encoded string to decode.
`base64decode`		Decodes a base-64 encoded string.
	`name`	A string variable to receive the decoded string.
	`value`	A url-encoded string to decode.
uudecode		Decode a uuencoded string.
	`name`	A string variable to receive the decoded string.
	`value`	A uuencoded string. The header and trailing lines should not be included.
`quotedprintabledecode`		Decode a Quoted-printable encoded string.
	`name`	A string variable to receive the decoded string.
	`value`	A quoted-printable encoded string.

Node Name	Attribute Name	Description
convert-ebcdic		Convert an EBCDIC string to its ASCII equivalent.
	name	A string variable to receive the decoded string.
	value	A url-encoded string to decode.

Geo IP Parser

This topic introduces the Geo IP parser for Decoders.

One of the files available for editing in the Services Config view > Files tab is **GeoPrivate.ipl**, the Geo IP parser.

GeoPrivate.ipl

The Geo IP parser is a fixed parser that takes IP addresses and converts them to geographical locations. The locations are displayed through the Google Earth display.

The geolocation metadata in GeoPrivate.ipl, are added for both **ip.src** and ip.dst. The parser uses two external data files, **GeoCity.dat** and GeoCountry.dat, which are both stored in the application directory. There are up to eight metadata for each IP address as listed in the table below.

Metadata	Description
city.dst	Destination City
city.src	Source City
country.dst	Destination Country
country.src	Source Country
latdec.dst	Destination Decimal Latitude
latdec.src	Source Decimal Latitude
longdec.dst	Destination Decimal Longitude
longdec.src	Source Decimal Longitude

Lua Parsers

One of the files available for editing in the Services Config view > Files tab is **`NwLua.xml`**, the Lua parser.

List of Lua Parsers

There are a number of Lua parsers available from Live. See RSA Content for:

- A complete list of these parsers
- Their interdependencies
- The Flex parsers that are subsumed by each Lua parser.

Five common parser operations are:

- Match Port and Identify Immediately
- Match Port and Delay Identification
- Match Token and Identify Immediately
- Match Multiple Tokens
- Match Token and Create Metadata

Search Parser

This topic explains how to configure a custom parser used on a Decoder to generate metadata by scanning for pre -defined keywords and regular expressions in the Services Config view > Files tab.

One of the files available for editing in the Services Config view > Files tab is **search.ini**, the search parser.

search.ini

The Search Parser is a custom parser used to generate metadata by scanning for pre -defined keywords and regular expressions. The parser searches the payload of a reconstructed session for string matches and can execute a regular expression search. You can configure the parser by editing the search.ini file.

Caution: The search parser can have a significant impact on system performance. It is important that both the search mechanism and the data to which it is applied to be well understood before creating new search definitions and enabling the search parser.

The search definition is used across all protocols. There are three basic search methods:

- Keyword: Search a stream for a specific set of words
- Pattern: Search a stream for a regular expression match
- Keyword + Pattern: Search a stream for a regular expression if it contains any of a given set of keywords.

For a detailed explanation, see Search Parser in the search.ini Search String Syntax.

search.ini Search String Syntax

This topic introduces search methods and syntax for use in Search parser.

The Search parser uses three basic search methods:

- Keyword: Search a stream for a specific set of words.
- Pattern: Search a stream for a regular expression match.
- Keyword+Pattern: Search a stream for a regular expression if it contains any of a given set of key words.

Syntax

```
Maxrecon=<max_size>Maxsearch=<max_ssearch_length>MatchLimit=<max_
matches_per_stream
Search Name
Services=<service_id_list>Keywords=<keyword_
list>|Pattern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

Parameters

Parameters used in this command:

Parameter	Description
`autocheck`	Automatically fixes all problems without prompting
`header Only`	Check/display the header of each file
`chatty`	Displays a hex dump of every object in the file (huge amount of data)
`dump#-#`	Indicates a zero-based object or range of objects in the file to output in hex to the console

Example

Following is an example of the command:

To check all NetWitness database files located in the Collection named Default. If any problems are found, the command will describe the problem and ask if you would like to fix it.

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\
Investigations\Default\*.nw*
```

Wireless LAN Configuration

This topic introduces the wireless LAN configuration file for Decoders, which is in the Services Config view > Files tab.

wlan-config.xml

One of the files available for editing in the Services Config view > Files tab is **`wlan-config.xml`**, the wireless LAN configuration file.

It controls the 802.11 parsers. Its chief purpose is to control decryption of raw 802.11 frames captured by the Decoder. This file is optional. If decryption of 802.11 traffic is not desired, there is no need to create the file.

There are five link-level parsers related to wireless LAN packet capture:

- IEEE 802.11 parser (data frames and beacons only)
- Radiotap w/ 802.11 header
- Absolute Value Systems (AVS) w/ 802.11 header
- Prism II w/ 802.11 header
- CACE's "Per Packet Information" (PPI) w/ 802.11 header

The 802.11 wireless parsers introduced in 9.8 all share a single configuration file. This wlan -config.xml file is used to define any wireless access points the user may have in the network, and its primary purpose is to control decryption. The BSSID of the access point and the SSID that it's authoritative for is added to this file as well as all of the active default keys used by the access point.

Decoder and Log Decoder References

This is a collection of references, which provide information about the user interface for Decoders and Log Decoders in NetWitness Suite, with references to the procedures that describe the work you can do in that part of the user interface. These topics are presented in alphabetical order.

Topics

- Services Config View - Data Retention Scheduler
- Services Config View - Data Privacy Tab
- Services Config View - Feeds Tab
- Services Config View - Files Tab
- Services Config View - General Tab
- Services Config View - Parsers Tab
- Services Config View - Parser Mappings Tab
- Services Config View - Rules Tabs
- Services System View - Decoders

Services Config View - Data Privacy Tab

In the Data Privacy tab (**ADMIN > Services > Select a Decoder or Log Decoder >** **> Config > Data Privacy tab)**, Administrators can configure data privacy parameters for certain Core services. For the Decoder and Log Decoder, you can set the default hash algorithm and salt.

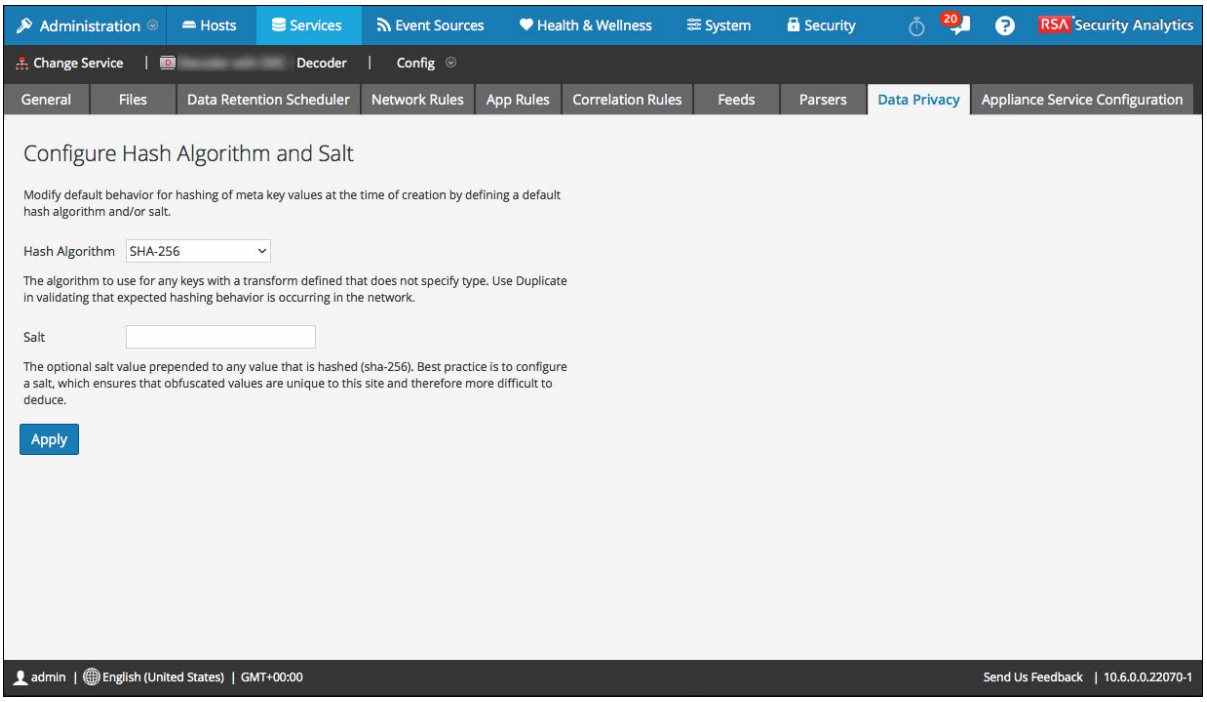
What do you want to do?

User Role	I want to ...	Documentation
Administrator	configure hash algorithm and salt	"Configure the Hash Algorithm and Salt" in the *Data Privacy Management Guide*. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder

Quick Look



The Data Privacy tab has the Configure Hash Algorithm and Salt configuration settings. The following table describes the parameters in this tab.

Parameter	Description
Hash Algorithm	Displays a drop-down list of hash algorithms to use for any keys with a transform that does not specify algorithm type. Possible values are SHA-256 and Duplicate. Duplicate is a special algorithm available for administrators to use when validating that expected hashing behavior is occurring in the network. In versions of NetWitness Suite prior to 10.5, SHA-1 was available as a hash algorithm, but RSA does not recommend use of SHA-1.
Salt	Indicates the optional salt value prepended to any value that is hashed. Best practices for security purposes dictate a salt value that is no less than 100 bits or 16 characters in length. Configuring a value ensures that obfuscated values are unique to this site and therefore more difficult to deduce. For more information on this field, see "Configure Data Obfuscation" in the *Data Privacy Management* guide.

Parameter	Description
Apply	Applies any changes.

Services Config View - Data Retention Scheduler

In the Services Config View Data Retention Scheduler tab, you can set the rollover criteria for removing database records from primary storage using an age-based threshold. You can also schedule the timing to check whether the threshold is reached.

To access the Data Retention Scheduler tab, go to ADMIN > Services > select a Decoder or Log Decoder service and click > View > Config > Data Retention tab.

What do you want to do?

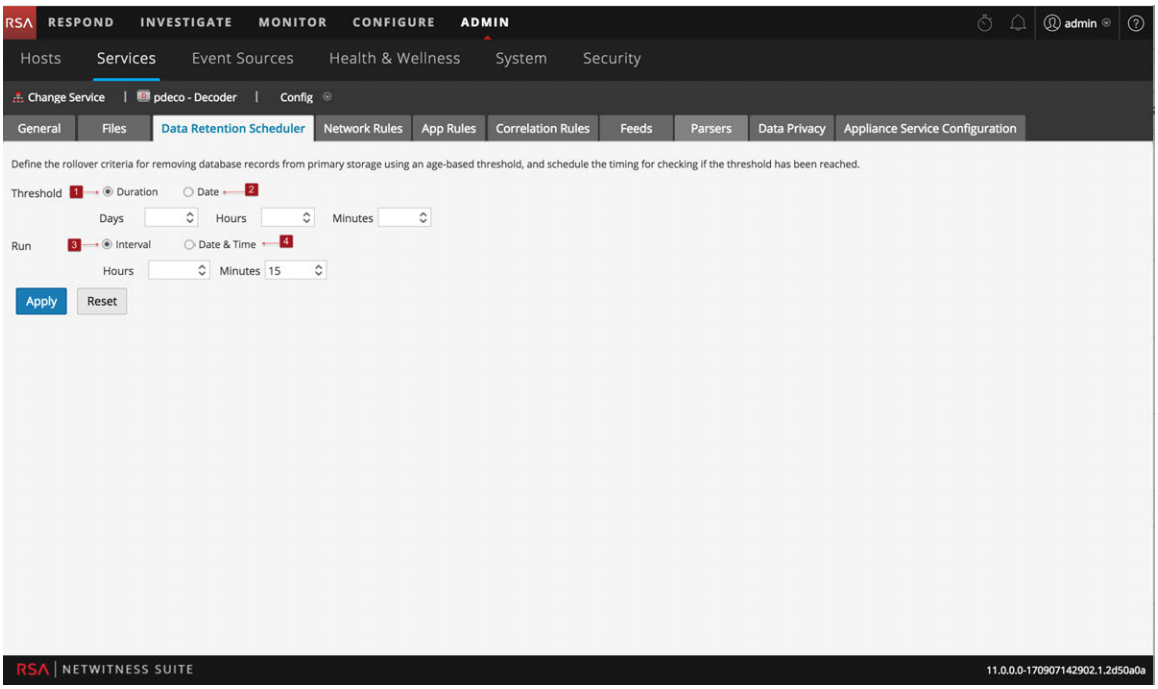
User Role	I want to...	Documentation
Administrator	Schedule the timing to see if the threshold is reached.	Configure Transaction Handling on a Decoder

Related Topics

- Configure Common Settings on a Decoder
- Decoder and Log Decoder Quick Setup

Quick Look

This is an example of the Data Retention Scheduler tab.



1	**Threshold Duration**: Removes database files older than the selected number of days, minutes, or hours.
2	**Threshold Date**: Removes database files older than the selected UTC date (YYYY-MM-DD-HH:MM:SS) that are not compatible with minutes, hours, or days parameters.
3	**Run Interval**: Indicates the number of hours between executions.
4	**Run Date and Time**: Defines which days of the week to execute the scheduler, as well as time of execution in HH:MM:SS format for the local time of the service.

Services Config View - Feeds Tab

Feeds and parsers are Lua programs loaded and compiled when either processing capture files in Investigation or capturing data with Decoders. Most commonly, they are used for static meta extraction and service identification.

Note: Pre-11.0 versions of NetWitness used FLEXPARSE programs in addition to Lua programs; Flexparsers are deprecated in NetWitness Suite 11.0. Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.

NetWitness Suite uses feeds to create metadata based on externally defined meta values. A feed is a list of data that is compared to sessions as they are captured or processed. For each hit, additional metadata is created. This data can identify and classify malicious IPs or incorporate additional information such as department and location based on internal network assignments. Some examples of feeds include threat feeds to identify BOTNets, DHCP mappings, or even active directory information such as physical location or logical department.

Feeds can be added, removed, and updated while a Decoder is running without affecting capture. The Feeds tab (**ADMIN > Services >** select a service and click **> View > Config > Feeds tab**) provides a user interface for managing feeds on Decoders.

What do you want to do?

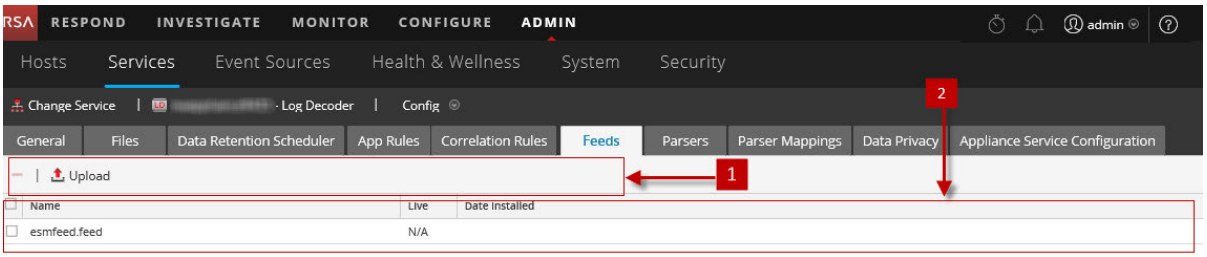
User Role	I want to...	Documentation
Administrator	configure feeds	Configure Feeds and Parsers
Administrator	enable and disable parsers	Enable and Disable Parsers and Log Parsers

Related Topics

- Configure Common Settings on a Decoder
- Decoder and Log Decoder Quick Setup
- Upload Feeds Dialog
- Feed and Parser References

Quick Look

This is an example of the Feeds tab.



1 Feeds Tab Toolbar - Provides options to work with feeds in the grid

2 Feed Grid - Lists all feeds that are currently deployed on the Decoder

Feeds Tab Toolbar

Feature	Description
Upload	Displays the Upload Feeds dialog.
−	Deletes the selected feeds.

Feeds List

The Feeds list provides a listing of all currently deployed feeds for the Decoder.

Column	Description
Name	The name of the feed or the feed file.
Live	Indicates if the feed originated from Live. Possible values are **Yes**, **No**, or **N/A**. • **Yes** = Installed through Live • **No** = Installed through NetWitness Suite • **N/A** = The feed has no attributes file created by NetWitness Suite to track the installation date. The feed may have been installed manually, not through NetWitness Suite or Live Services. Manually installed feeds still function properly.
Date Installed	The date the feed was pushed to the service.

Upload Feeds Dialog

This topic describes the features of the Upload Feeds dialog in the Services Config view > Feeds tab.

The **Upload** option in the Services Config view > Feeds tab displays the Upload Feeds Dialog, in which you can manage the uploading of feeds to a Decoder or Log Decoder.

What do you want to do?

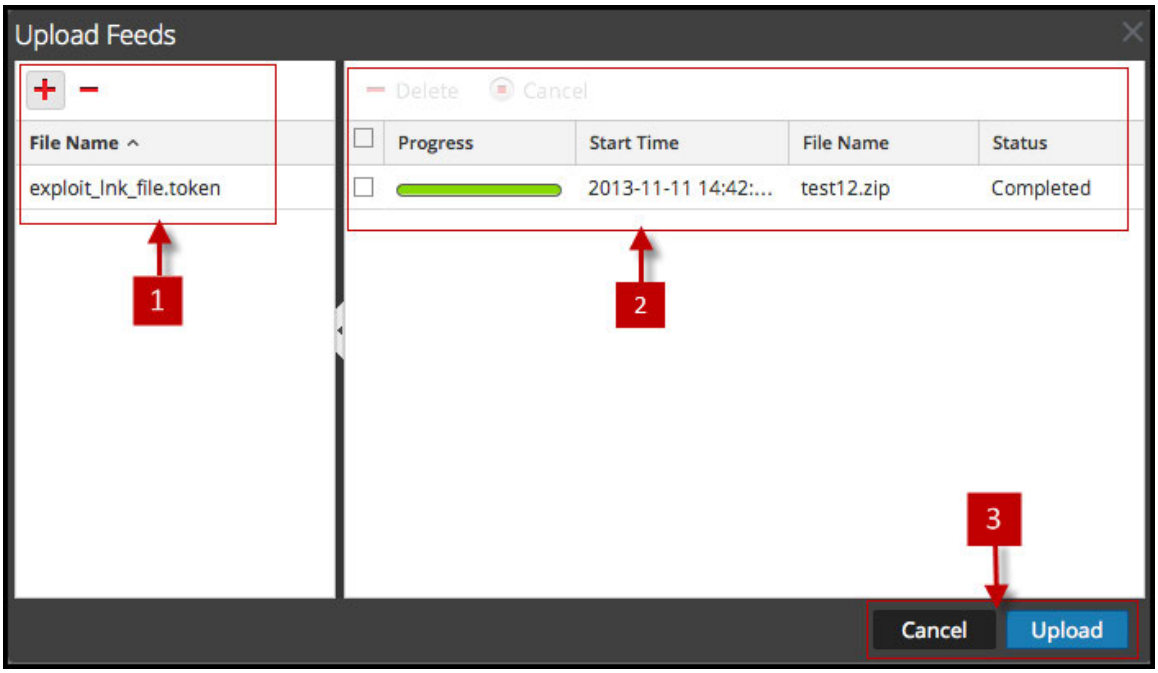
User Role	I want to...	Documentation
Administrator	prepare a list of feeds for upload	Edit, Upload, or Remove a Feed
Administrator	view and delete upload jobs	Edit, Upload, or Remove a Feed

Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- Feed and Parser References

Quick Look

This is an example of the Upload Feeds dialog.



1 File List - Provides place to prepare a list of feeds for uploading

2 Upload Job List - Provides a view of upload jobs

3 Upload Feeds Dialog Buttons

File List

The File List is the place to prepare a list of feeds for uploading. You can add files from a directory structure, and delete files from the grid if you decide that you don't want to upload a particular file. When the list is ready, clicking **Upload** starts the upload process.

Feature	Description
+	Opens a view of the directory structure where you can select files to add to the File list.
−	Deletes the selected files from the File list.
File Name	Lists the feed files you have added from a file system in preparation for uploading to a Decoder. When you click **Upload**, the files listed here are uploaded.

Upload Job List

The Upload Job list provides a view of upload jobs started by clicking **Upload**.

Feature/Column	Description
Delete	Deletes an upload job.
Progress	Displays progress of an upload job.
Start Time	Displays the start time of an upload job.
File Name	Lists filename of the feed being uploaded.
Status	Displays the status of upload job.

Upload Feeds Dialog Buttons

Feature	Description
Cancel	Closes the Upload Feed dialog.
Upload	Starts uploading the feed files listed in the File list. Each feed is listed in a separate row in the Upload Process list.

Services Config View - Files Tab

The Decoder and Log Decoder configuration files are visible and editable in the Services Config view > Files tab. "Edit Core Services Configuration Files" in the *Hosts and Services Getting Started Guide* provides general instructions for editing files. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

Like other Core services, both the Decoder and Log Decoder have an index file, and may also have a crashreporter, netwitness, and scheduler. The Decoder and Log Decoder index files are named **`index-decoder-custom.xml`** and **`index-logdecoder-custom.xml`.**

Note: This file type is available only for Log Decoder with Envision content installed. `Table-map.xml` and `table-map-custom.xml` will now show up but only if `table-map.xml` was found on the file system (for example, it is a log decoder with envision content installed).

What do you want to do?

User Role	I want to...	Documentation
Administrator	obtain log files from pre-11.0 Log Decoder	Obtain Log Files a from Pre-11.0 Log Decoder
Administrator	edit files and parsers	Feed and Parser References

Related Topics

- Configure Common Settings on a Decoder
- Decoder and Log Decoder Quick Setup
- Create Custom Meta Keys Using a Custom Feed

Quick Look

Filename	Description
`GeoPrivate.ipl`	This fixed parser takes the IP addresses and converts them to geographical locations. The locations are displayed through the Google Earth display.

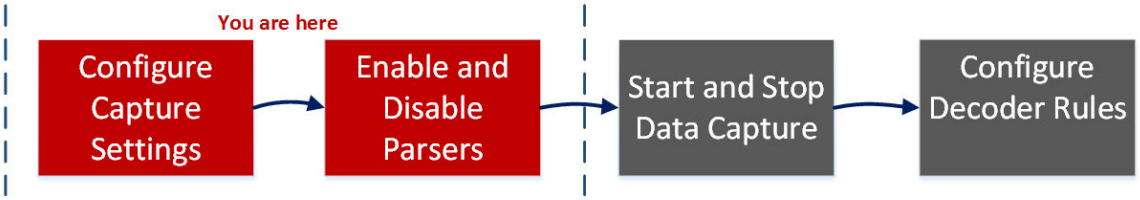
Filename	Description
`feed-definitions.xml`	Used to create custom feeds, this is the XML schema used by the Decoder to define a **feed** message when it creates a **.feed** file.
`traffic_flow_options.lua`	Used to provide directionality information. Update this file with environment-specific internal and external subnets for the Lua parser to create proper directionality in metadata. The parser is described in RSA Content for RSA NetWitness Suite.
`search.ini`	This is the Search Parser configuration file. The Search Parser is a custom parser, used to generate metadata by scanning for pre-defined keywords and regular expressions.
`wlan-config.xml`	This is the wireless LAN configuration file (9/9/2009). This file controls the 802.11 parsers. Its chief purpose is to control decryption of raw 802.11 frames captured by the Decoder.

Services Config View - General Tab

The General tab for a Decoder in the Services Config view provides a way to manage basic service configuration, configure data capture, and select the parsers that are applied to the captured data. To access the General tab, go to **ADMIN** > **Services** > select a Decoder or Log Decoder and click > **View** > **Config** > **General tab**.

Workflow

The following figure depicts common Decoder configuration tasks with the steps you can complete in this view highlighted.



What do you want to do?

User Role	I want to...	Documentation
Administrator	configure capture settings*	Configure Capture Settings
Administrator	manage parsers and log parsers*	Enable and Disable Parsers and Log Parsers
Administrator	start and stop data capture	Start and Stop Data Capture
Administrator	configure rules	Configure Decoder Rules

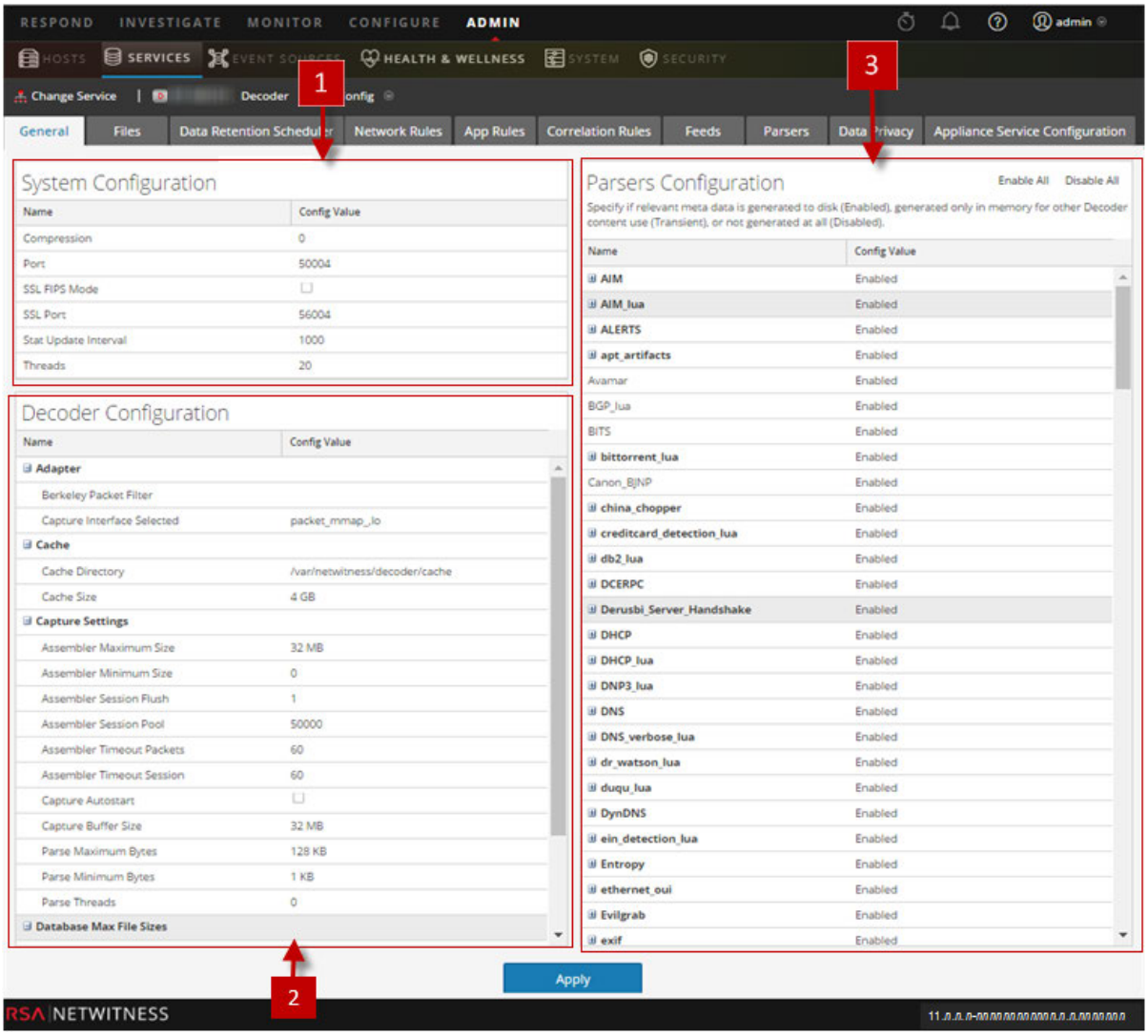
*You can complete these tasks here.

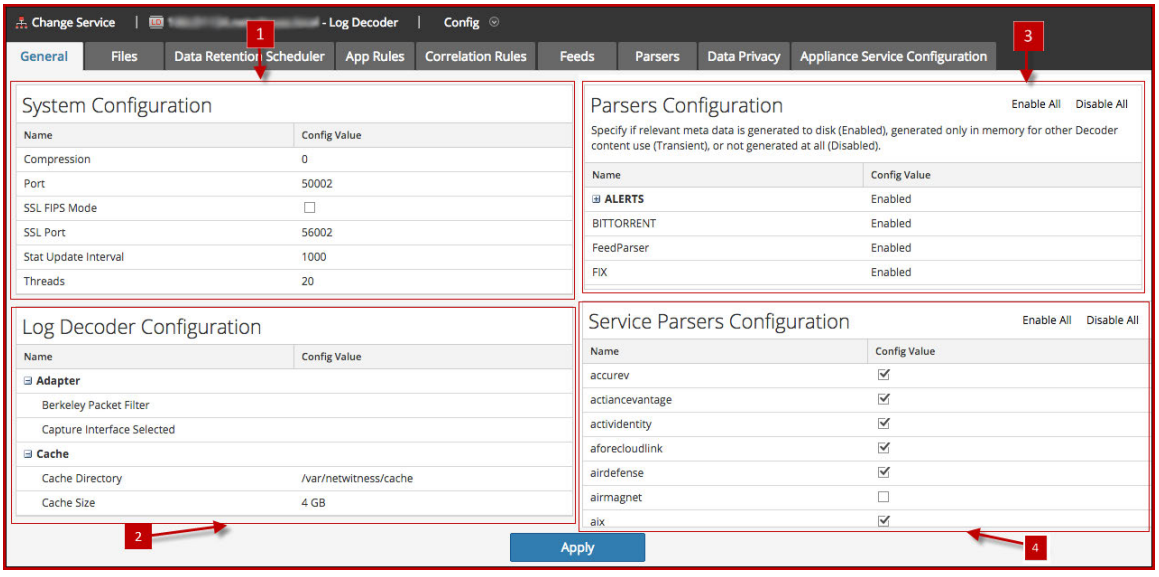
Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- Configure Feeds and Parsers

Quick Look

The first figure is an example of the General tab for a Decoder. The second is the General tab for a Log Decoder.

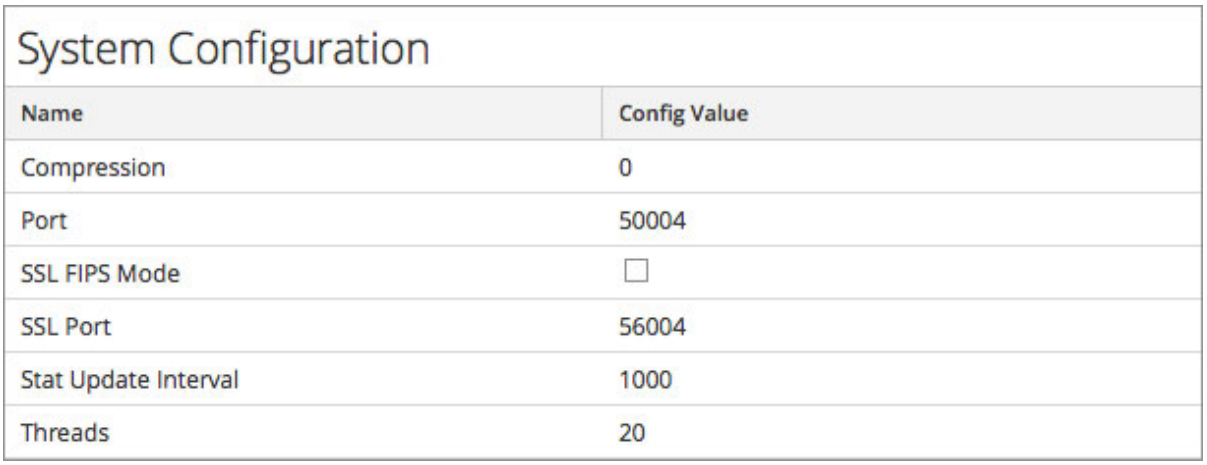

RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Decoder
Config
1
3
General
Files
Data Retention Scheduler
Network Rules
App Rules
Correlation Rules
Feeds
Parsers
Data Privacy
Appliance Service Configuration
System Configuration
Name
Config Value
Compression
0
Port
50004
SSL FIPS Mode
SSL Port
56004
Stat Update Interval
1000
Threads
20
Parsers Configuration
Enable All
Disable All
Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).
AIM
AIM_lua
ALERTS
apt_artifacts
Avamar
BGP_lua
BITS
bittorrent_lua
Canon_BJNP
china_chopper
creditcard_detection_lua
db2_lua
DCERPC
Derusbi_Server_Handshake
DHCP
DHCP_lua
DNP3_lua
DNS
DNS_verbose_lua
dr_watson_lua
duqu_lua
DynDNS
ein_detection_lua
Entropy
ethernet_oui
Evilgrab
exif
Enabled
Decoder Configuration
Adapter
Berkeley Packet Filter
Capture Interface Selected
packet_mmap_lo
Cache
Cache Directory
/var/netwitness/decoder/cache
Cache Size
4 GB
Capture Settings
Assembler Maximum Size
32 MB
Assembler Minimum Size
0
Assembler Session Flush
1
Assembler Session Pool
50000
Assembler Timeout Packets
60
Assembler Timeout Session
60
Capture Autostart
Capture Buffer Size
32 MB
Parse Maximum Bytes
128 KB
Parse Minimum Bytes
1 KB
Parse Threads
0
Database Max File Sizes
2
Apply
RSA NETWITNESS


Change Service
- Log Decoder
Config
1
3
General
Files
Data Retention Scheduler
App Rules
Correlation Rules
Feeds
Parsers
Data Privacy
Appliance Service Configuration
System Configuration
Name
Config Value
Compression
0
Port
50002
SSL FIPS Mode
SSL Port
56002
Stat Update Interval
1000
Threads
20
Parsers Configuration
Enable All
Disable All
Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).
ALERTS
BITTORRENT
FeedParser
FIX
Enabled
Log Decoder Configuration
Adapter
Berkeley Packet Filter
Capture Interface Selected
Cache
Cache Directory
/var/netwitness/cache
Cache Size
4 GB
Service Parsers Configuration
Enable All
Disable All
accurev
actiancevantage
actividentity
aforecloudlink
airdefense
airmagnet
aix
2
Apply
4

1. System Configuration - Manages service configuration for a Decoder.
2. Decoder Configuration or Log Decoder Configuration - Lets you view and edit service configuration parameters for a Decoder or Log Decoder.
3. Parsers Configuration - Lets you select parsers to use on the Decoder.
4. Service Parsers Configuration (Log Decoders only) - Lets you select service parsers to use on the Log Decoder.

System Configuration Section

The System Configuration section manages service configuration for a Decoder. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.



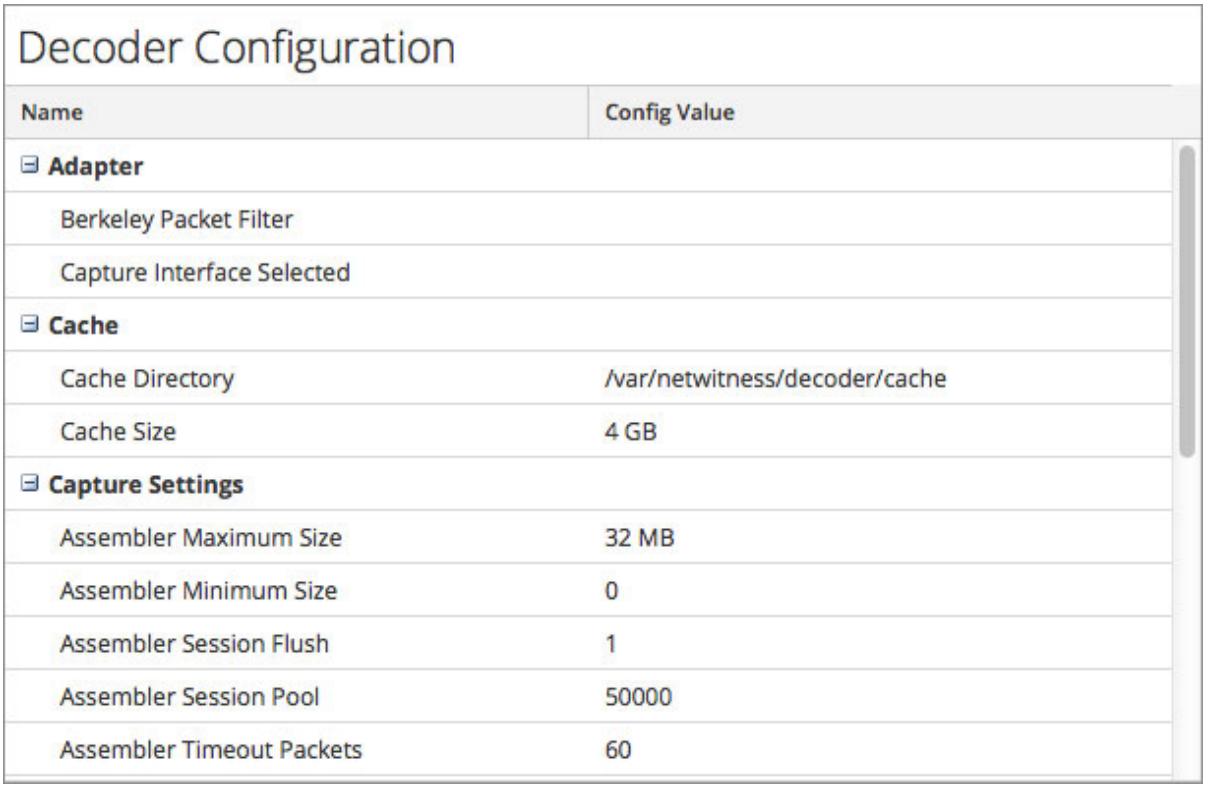
The System Configuration section has these parameters.

Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.
Port	Determines the port used by the service. **Note:** If you change the port number, ensure that you restart the service.
SSL FIPS mode	If enabled, all the data transferred in the network will be encrypted using SSL.
SSL Port	Indicates the port used for encrypting using SSL.

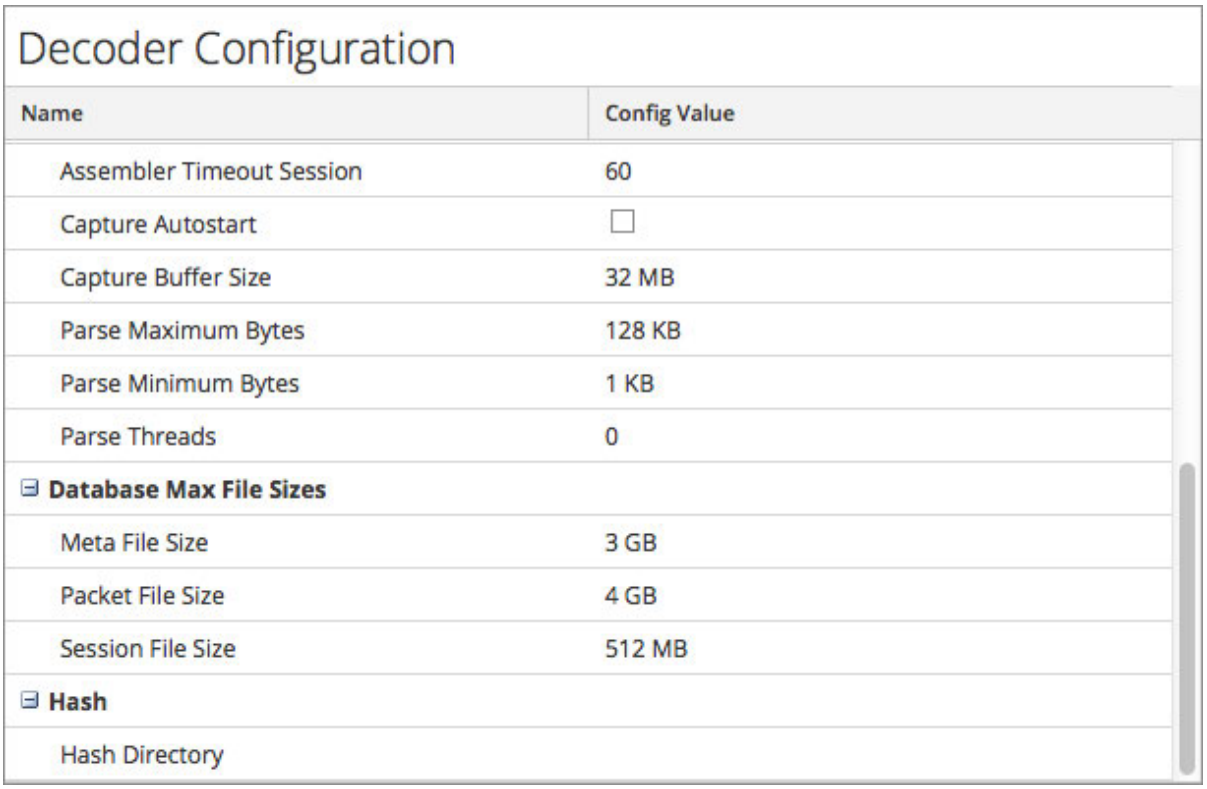
Parameter	Description
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of **0** lets the system decide. A change takes effect on service restart.

Decoder Configuration Section

The Decoder Configuration section provides a way to view and edit service configuration parameters for a Decoder or Log Decoder. When a service is first added, default values are in effect. You can edit these values to manage traffic capture.



Scrolling to the bottom of the section reveals these additional Decoder Configuration parameters.



Adapter Section

Adapter parameters configure the network interface for capture as described in Configure Capture Settings.

Cache Section

Cache parameters configure the cache directory and size for session cache files. The following table describes the cache settings. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

Cache Parameter	Description
Cache Directory	The directory where session cache files are stored. The default value is `/var/netwitness/decoder/cache`. Change takes effect immediately.
Cache Size	The maximum size, in Megabytes (MB), that all files in the cache directory can attain before the oldest files are deleted. Once the threshold is reached, the cache size is reduced by 10%. The default value is **4 GB**. Change takes effect immediately.

Capture Settings Section

The Capture Settings section provides a way to configure operational capture settings. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

Capture Settings Parameter	Description
Assembler Maximum Size	Specifies the maximum size in bytes that a session's packet data size can attain. The default value is **32 MB**. Change takes effect immediately.
Assembler Minimum Size	Specifies the minimum size in bytes that a session must have in order to generate metadata. A value of **0** means every session has metadata generated. The default value is **0.** Change takes effect immediately.
Assembler Session Flush	Specifies whether a session is removed from the assembler when the session's last chain is removed from the assembler. The default value is **1**. • **2** = if the first packet of a session times out of assembler, the session is removed from assembler after parsing is complete. Any subsequent packets for this session create a new session in assembler. • **1** = If the last chain of a session times out of assembler, the session is removed from assembler. Any subsequent packets for this session create a new session in assembler. • **0** = If the last chain of a session times out of assembler, the session is left in assembler until it times out. Any subsequent packets for this session are filtered Change takes effect on service restart.
Assembles Session Pool	Specifies the number of entries in the session pool. The default value is **350000**. Change takes effect on service restart.

Capture Settings Parameter	Description
Assembler Timeout Packets	Specifies the number of seconds before a packet or chain is timed out. T default value is **60**. Change takes effect immediately.
Assembler Timeout Session	Specifies the number of seconds before a session is timed out. Default value is **60**. Change takes effect immediately.
Capture Autostart	Specifies whether capture begins automatically each time Decoder is started. When checked, the value = yes. When unchecked, the value = no. The default value is **no**. Change takes effect immediately.
Capture Buffer Size	The capture memory buffer allocation in Megabytes. Default value is **64 MB**. Change takes effect on service restart.
Parse Maximum Bytes	The maximum number of bytes to scan a stream for additional tokens. When the first token is found, the stream is scanned up to the set number of bytes, but no further. A setting of **0** removes the early termination and the full stream is scanned regardless of size. The default value is **128 KB**. Change takes effect immediately.
Parse Minimum Bytes	The minimum number of bytes to scan a stream for the first token. If no token is found within the set number of bytes, scanning is terminated. A setting of **0** removes the early termination and the full stream is scanned regardless of size. The default value is **1 KB**. Change takes effect immediately.
Parse Threads	The number of parse threads to use for session parsing. A value of **0** means let the server decide. The default value is **0**. Change takes effect on service restart.

Database Max File Sizes Section

The Database Max File Sizes section controls the maximum file size for various databases. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

File Size Parameter	Description
Meta File Size	The maximum size of meta database files in Megabytes. The default value is **10 MB**. Change takes effect on service restart.
Packet File Size	The maximum size of packet database files in Megabytes. The default value is **10 MB**. Change takes effect on service restart.
Session File Size	The maximum size of session database files in Megabytes. The default value is **100 MB**. Change takes effect on service restart.

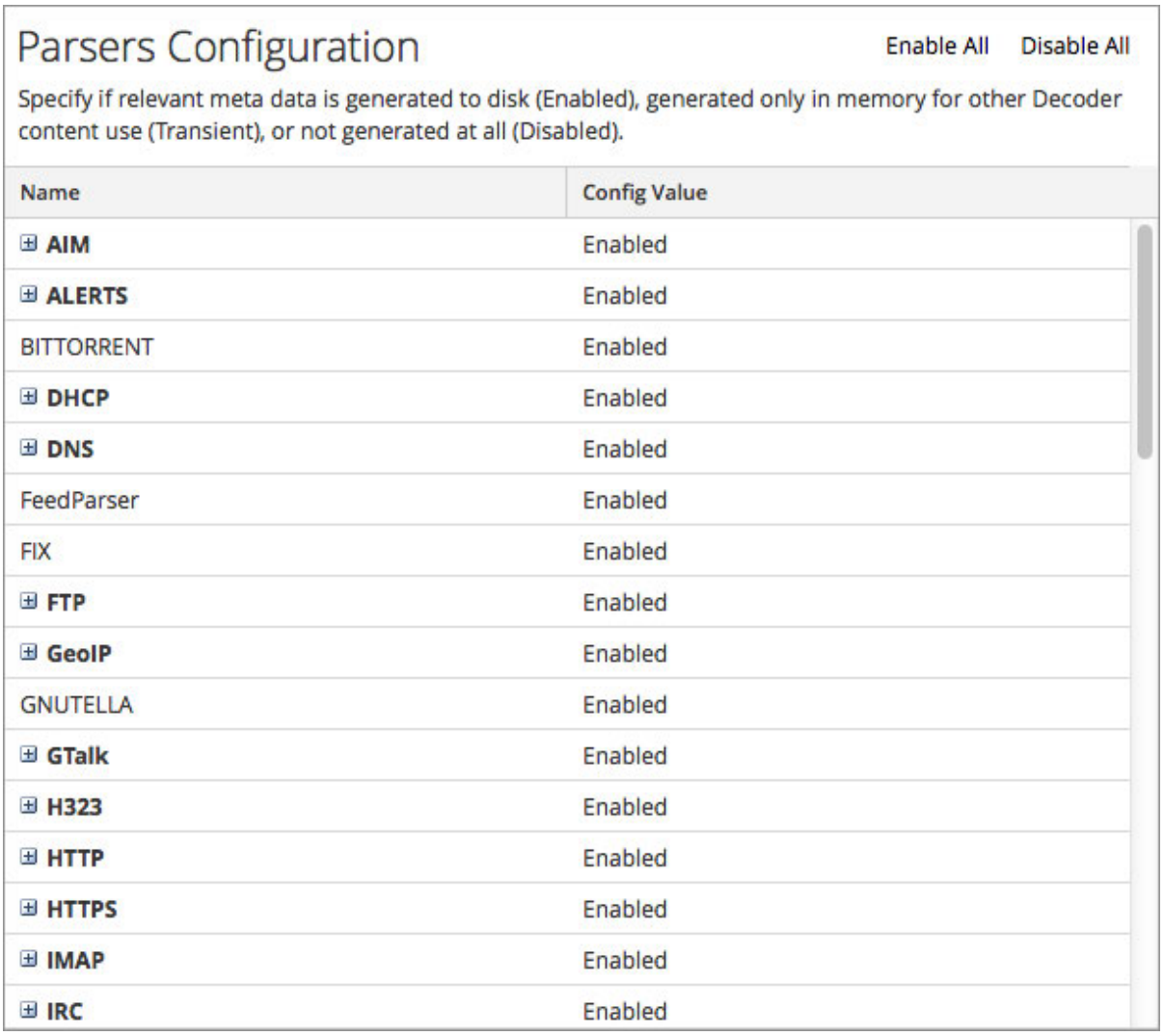
Hash Section

The Hash section settings control data base file hashing options. There is a small performance penalty when hashing.

Hash Parameter	Description
Hash Directory	The server directory where all hash files are written. If empty, each hash file is written to the same directory as the file being hashed. The default value is blank. Change takes effect on service restart.

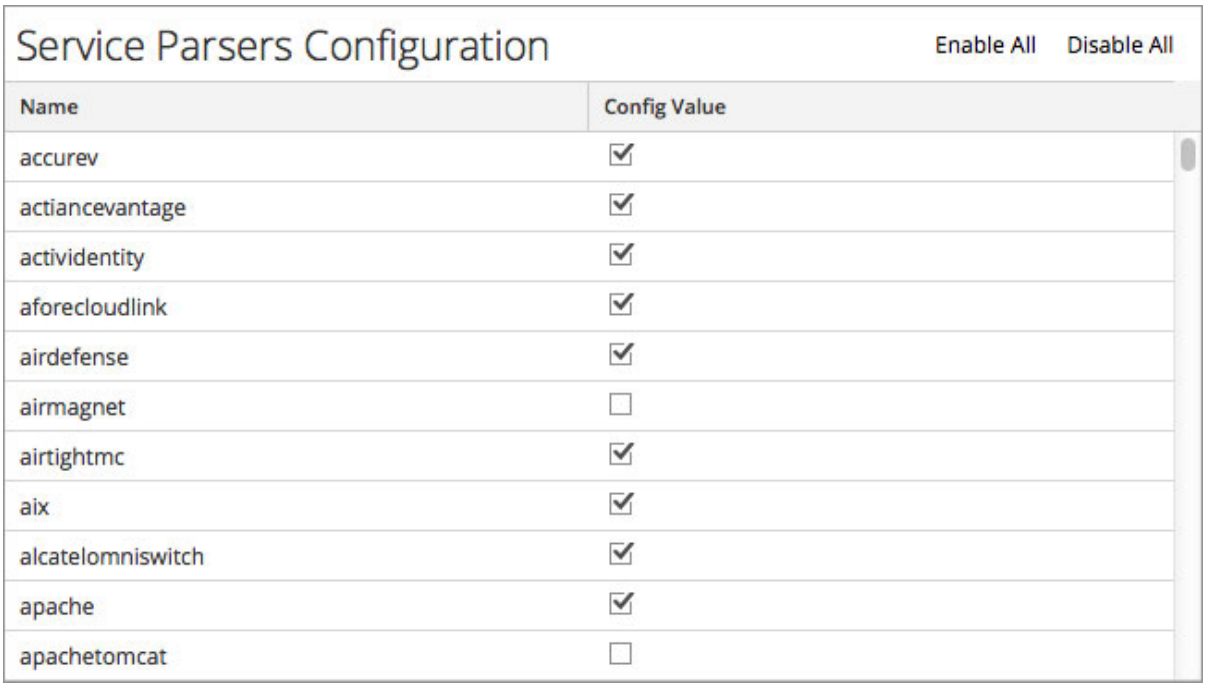
Parsers Configuration Panel

The Parsers Configuration panel provides a way to select parsers to use on the Decoder. Within some parsers, you can also configure the metadata that the parser creates. See Enable and Disable Parsers and Log Parsers for detailed information and procedures.



Service Parsers Configuration Section for Log Decoder

The Service Parsers Configuration section provides a way to select Service parsers to use on the Log Decoder.



Services Config View - Parsers Tab

In the Services Config View > Parsers tab, you can view deployed parsers on a Decoder or Log Decoder, upload parsers, and delete deployed parsers. Parsers can be added and removed while a Decoder or Log Decoder is running without affecting capture.

To access the Parsers tab, go to ADMIN > Services > select a Decoder or Log Decoder service and click > View > Config > Parsers tab.

What do you want to do?

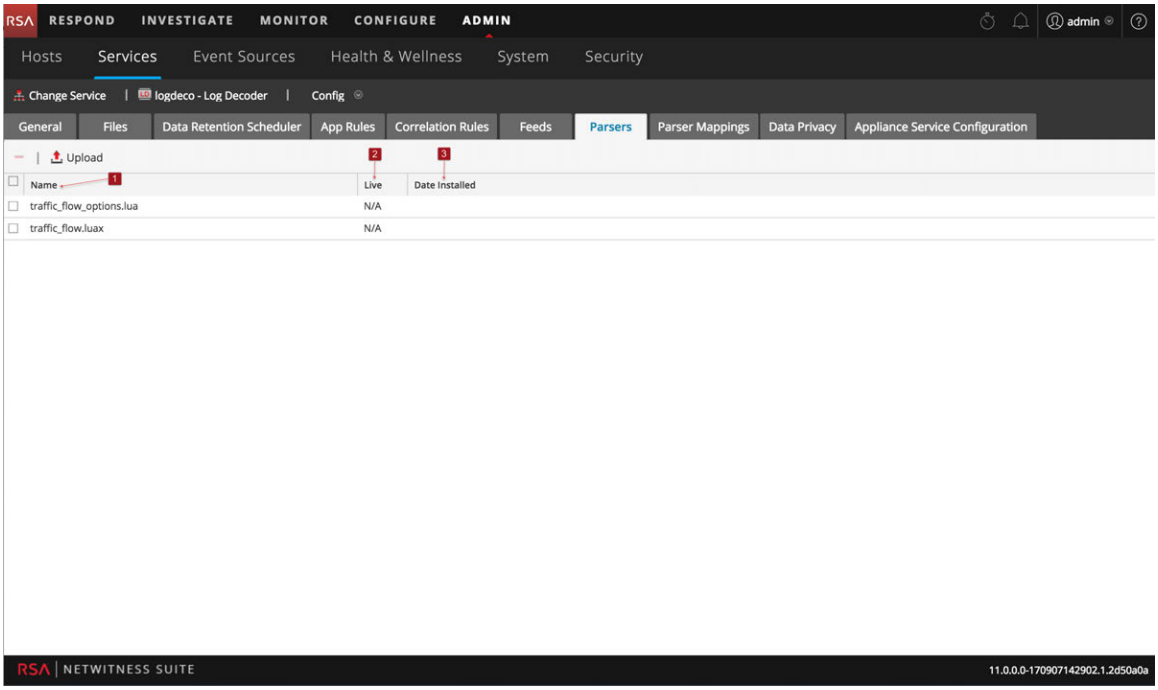
User Role	I want to...	Documentation
Administrator	View deployed parsers.	Enable and Disable Parsers and Log Parsers
Administrator	Upload parsers to a Decoder or Log Decoder.	Enable and Disable Parsers and Log Parsers

Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- Upload and Delete Custom Parsers

Quick Look

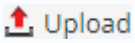
This is an example of the Parsers tab. The Parsers grid lists all parsers that are currently deployed on the Decoder.



1	**Name**: The name of the parser or the parser file.
2	**Live**: Indicates if the parser originated from Live. Possible values are **Yes**, **No**, or **N/A**. • **Yes** = Installed through Live Services. • **No** = Installed through NetWitness. • **N/A** = The parser has no attributes file created by NetWitness to track the installation date. The parser may have been installed manually, not through NetWitness or Live Services.
3	**Date Installed**: The date the parser was pushed to the service.

Parsers Tab Toolbar

The Parsers Tab toolbar has options to work with parsers in the grid.

Feature	Description
	Enables you to upload parsers to a Decoder or Log Decoder.
	Requests confirmation that you want to delete the selected parsers. You can select **No** to cancel the deletion, or select **Yes** to delete the selected parsers.

Services Config View - Parser Mappings Tab

This topic provides a description of the configurable options for a Log Decoder in the Parser Mappings tab.

In the Parser Mappings Administrators can configure log parser mappings for Log Decoder services. To access the Parser Mappings tab, go to ADMIN > Services > select a service and click > View > Config > Parser Mappings tab.

Note: You can also configure log parser mappings for Log Decoder services by navigating to **ADMIN > Services > Event Sources > Discovery**.

This feature is intended to track a subset of Event Sources that is parsing against the wrong parser.

What do you want to do?

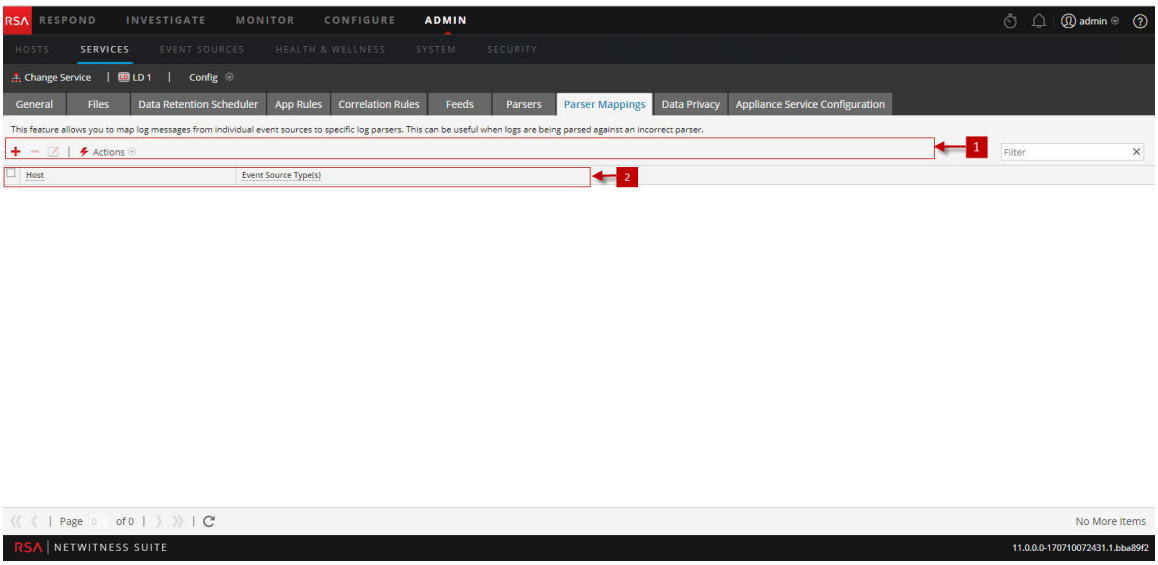
User Role	I want to...	Documentation
Administrator	Manage IPs for Event Source Mapping.	Enable Parser Mappings

Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder

Quick Look

This is an example of the tab.



1 Parser Mappings Toolbar - Provides options to work with parser mappings in the grid

2 Parser Mappings Grid - Lists all parsers that are currently mapped on the Log Decoder

Parser Mappings Toolbar

The Parser Mappings toolbar has options to work with parser mappings in the grid.

Feature	Description
+	Add a parser mapping.
−	Delete the selected parser mapping.
✎	Edit a parser mapping.
↻	Refresh the list of parser mappings.
⚙	Display the Actions menu. • **Import** - Import a parser mapping to a file. • **Export** - Save a parser mapping to a file.

Parser Mappings List

The Parser Mappings list displays all parsers that are currently mapped on the Log Decoder.

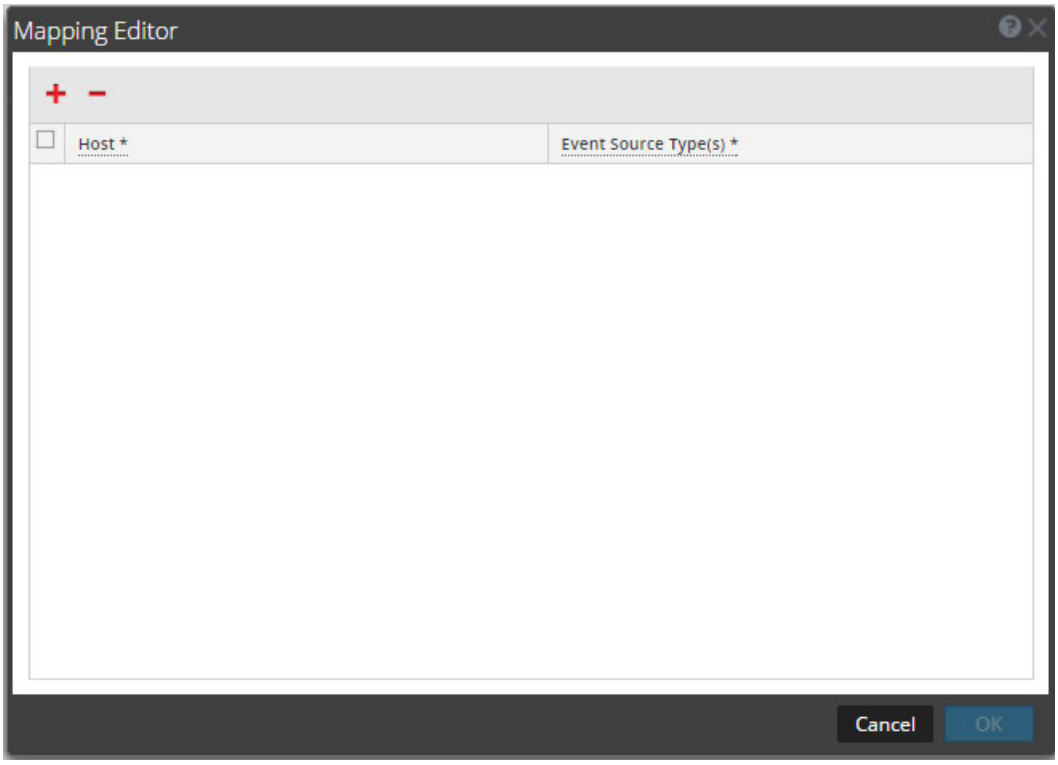
Parameter	Description
Host	Displays the IP address of the host.
Event Source	Displays the Event Sources that are parsing incorrectly.

Parser Mappings Editor Dialog

The Parser Mappings Editor dialog allows you to update an IP to event source mapping.

To access the Parser Mappings Editor dialog, follow these steps:

1. In the NetWitness Suite menu, select **ADMIN > Services**.
2. Select a **Log Decoder**, and in the **Actions** column, select > **View** > **Config**.
   The Services Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Click .
   The Mapping Editor dialog is displayed.



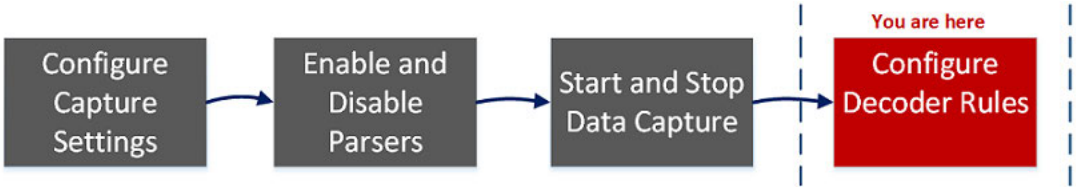
For more information on the Parser Mapping Editor dialog, refer to Enable Parser Mappings.

Services Config View - Rules Tabs

The Rules tabs in the Services Config view (**ADMIN > Services >** select a service and click **> View > Config**) enable you to define and manage capture rules. Each type of rule has a grid with slightly different columns and different parameters in the Rule Editor dialog. Application and correlation rules apply to both Decoders and Log Decoders. Network rules apply only to packet Decoders.

Workflow

The following figure depicts the workflow for common Decoder configuration tasks with the steps you can complete in this view highlighted.



What do you want to do?

User Role	I want to...	Documentation
Administrator	configure capture settings	Configure Capture Settings
Administrator	manage parsers and log parsers	Enable and Disable Parsers and Log Parsers
Administrator	start and stop data capture	Start and Stop Data Capture
Administrator	configure rules*	Configure Decoder Rules
Administrator	import, export, or push a rule*	Configure Decoder Rules
Administrator	enable or disable a rule*	Configure Decoder Rules
Administrator	add, edit, or delete a rule*	Configure Decoder Rules

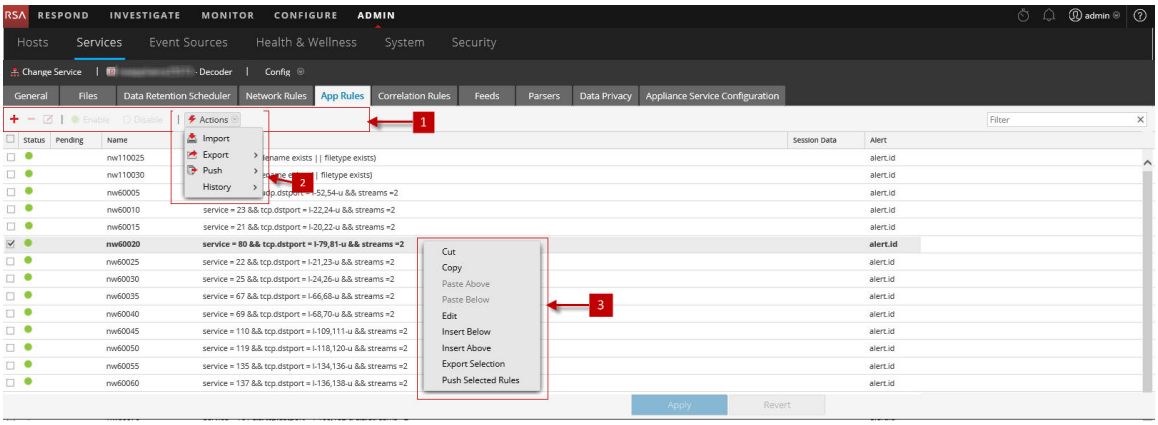
*You can complete these tasks here.

Related Topics

- Configure Common Settings on a Decoder
- Decoder and Log Decoder Quick Setup
- App Rules Tab
- Correlation Rules Tab
- Network Rules Tab

Quick Look

This is an example of the App Rules tab.

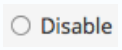
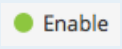


1	Rules Tab Toolbar - Provides options to work with rules in the grid
2	Rules Actions Menu - Provide options to manage sets of rules
3	Rules List Context Actions - Displays the Rules List Context Menu

Rules Tab Toolbar

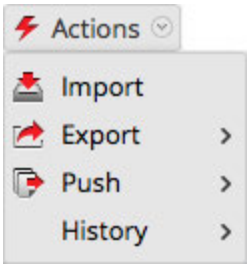
The toolbar is the same for all Config view > Rules tabs.

Feature	Description
Actions	Displays the **Actions** menu.
+	Adds a new rule to a service.
−	Deletes a rule from a service.

Feature	Description
	Allows rule modification.
	Disables a rule (without deleting the rule).
	Enables (reactivates) a rule.
Filter	The input field for a search string. NetWitness Suite filters the rules dynamically as you type a search string. Clicking **x** clears the input field, restoring the unfiltered view.
Apply	Saves the changes made to rules and applies the configured rules to a service. Until you apply changes, it is possible to reload the rules as they were before current modifications.
Revert	Discards unsaved changes to the grid and reverts to the unedited rules.

Rules Actions Menu

The Actions menu has options that help to manage sets of rules.



Option	Description
Import	Imports a set of rules into the user interface so that it can be applied to a service. You can edit the rules before applying.
Export	Saves selected rules or all rules to an .nwr file on the client machine.

Option	Description

Push	Allows rules to be applied to other services (Decoders or Log Decoders) or Decoders belonging to a service group. When pushing, the rules can either be merged (update existing rules and append new ones) or replaced.
	• **Push > All.** Pushes all rules to other services. All rules on the target services are removed and replaced with all of the rules on the source service.
	• **Push > Selection.** Pushes selected rules to other services. You have two options:
	  • **Replace.** Deletes all rules on the target services and replaces them with the selected rules from the source service.
	  • **Merge.** Merges the selected rules with the existing rules on the target services

History	Displays the last ten snapshots of rules applied through NetWitness Suite. You can select and apply (restore) a snapshot to the Decoder at anytime.

Rules List Context Actions

Within a rules grid, right-clicking a row displays the Rules Grid Context Menu.

Option	Description
Cut	Deletes the current rule.
Copy	Copies the current rule.
Paste Above	Pastes the copied rule above the current rule.
Paste Below	Pastes the copied rule below the current rule.
Edit	Edits the current rule.
Insert Below	Inserts imported rules below the current rule.
Insert Above	Inserts imported rules above the current rule.
Export Selection	Exports the selected rules.
Push Selected Rules	Pushes the selected rules to other services.

App Rules Tab

The App Rules tab (**ADMIN > Services >** select a Decoder or Log Decoder and click > **View > Config > App Rules tab**) enables you to manage application rules. NetWitness Suite applies application rules at the session level.

What do you want to do?

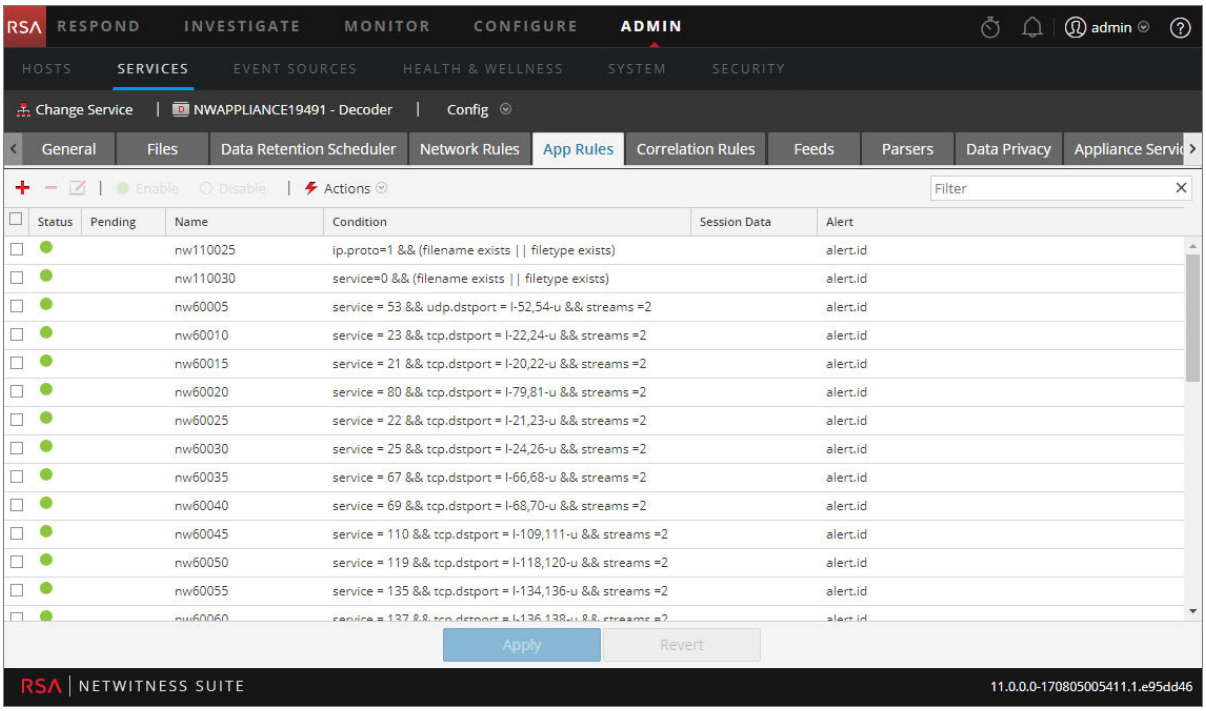
User Role	I want to...	Documentation
Administrator	add or edit application rules	Configure Application Rules

Related Topics

- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- Configure Decoder Rules
- Services Config View - Rules Tabs

Quick Look

The following figure shows an App Rules tab and the table describes the columns..



Column	Description
Pending	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains . Once the rules are applied, the pending indicator is removed.
Name	This is the rule name, a descriptive identifier for the rule.
Condition	This is the definition of the condition that triggers an action when matched.
Session Data	This column displays the Session Data action taken when a packet matches the rule. Possible values are **Filter**, **Keep**, or **Truncate**.
Alert	This column displays the name of the custom alert that the Decoder generates when metadata matches the rule.
Status	This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.

Rule Editor Dialog

The following figure shows the Rule Editor dialog for an application rule.

The Rule Editor dialog provides the fields and options needed to define an application rule.

Field	Description
Rule Name	The descriptive name that identifies the rule.

Field	Description
Condition	The definition of the condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the Intellisense window actions. As you build the rule definition, Intellisense displays syntax errors and warnings. All string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rulesprovides additional details.

The following table describes the Session Data actions and options.

Action	Description
Stop Rule Processing	If checked, further rule evaluation ends if the rule is matched, and the session is saved in accordance with the session action. If not checked, rule evaluation continues until all rules are evaluated.
Keep	The packet payload and associated metadata are saved when they match the rule.
Filter	The packet is not saved when it matches the rule.
Truncate	**Truncate All** – truncates all session payload bytes. The packet payload is not saved when it matches the rule, but packet headers and associated metadata are retained. This is the default truncation option. **Truncate After First <n> Bytes** – truncates the session payload bytes after the specified first <n> bytes, where <n> is an integer. The packet payload is not saved after <n> bytes when it matches the rule, but packet headers and associated metadata are retained. **Truncate SSL/TLS After Handshake** – truncates the payload for all sessions except in the case of an SSL/TLS session, where the SSL exchange is preserved, but the rest of the payload is not saved. This option is for use with SSL parsers.
Alert and **Alert On**	If **Alert** is checked, the packet generates a custom alert when metadata matches the rule. You can select the name of the alert in the **Alert On** field.
Forward	Enables the performance of syslog forwarding when the log matches the rule.

Action	Description
Transient	Prevents the alert metadata that is created from being written to the disk.

The following table describes Rule Editor dialog actions.

Action	Description
Reset	Resets the contents of the dialog to their values before editing; changes are discarded.
Cancel	Cancels any edits and closes the Rule Editor dialog.
OK	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor dialog closes.
Save	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See Fix Rules with Invalid Syntax.

Correlation Rules Tab

The Correlation Rules tab (**ADMIN > Services >** select a service and click > **View > Config > Correlation Rules tab**) enables you to manage correlation rules. Basic correlation rules are applied at the session level and alert the user to specific activities that may be occurring in their environment. NetWitness Suite applies correlation rules over a configurable sliding time window.

What do you want to do?

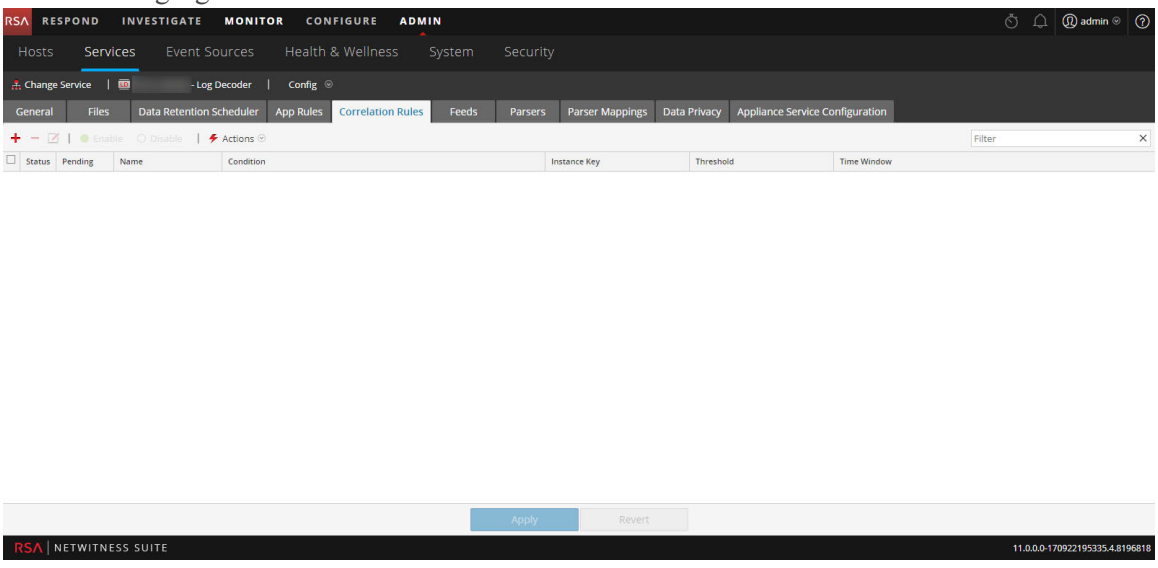
User Role	I want to...	Documentation
Administrator	add or edit a correlation rule	Configure Correlation Rules

Related Topics

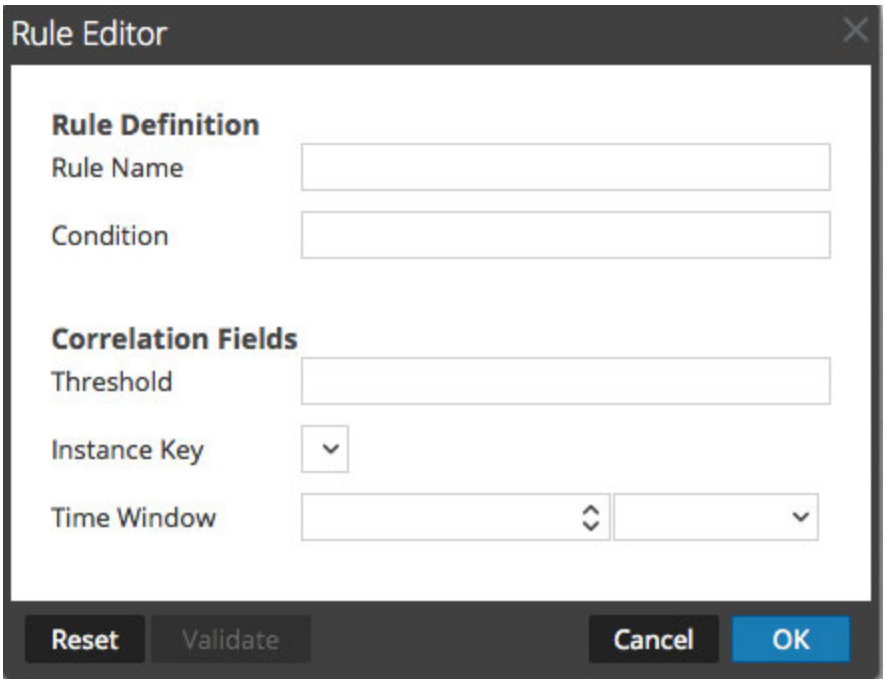
- Configure Common Settings on a Decoder
- Decoder and Log Decoder Quick Setup
- Configure Decoder Rules
- Services Config View - Rules Tabs

Quick Look

The following figure shows the Correlation Rules tab.



The following figure shows the Rule Editor dialog for a correlation rule.



The following table describes the Correlation Rules tab columns.

Column	Description
Pending	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains . Once the rules are applied, the pending indicator is removed.
Name	This is the descriptive name for the rule.
Condition	This is the definition of the condition that triggers an action when matched. In conditions, all string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details.
Instance Key	This is the target indicator to base the event upon. It can be a single primary key, such as ip.src or a compound primary key such as ip.src,ip.dst.

Column	Description
Threshold	This is the minimum number of occurrences required to trigger a correlation session and can include a associated key that identifies the meta type that were are counting to determine if the condition is satisfied. The correlation engine cannot use IPv4 or IPv6 as an associated meta type. Use one of these three arguments: • u_count(associated_key) = the count of unique values of the specified key. A key is required. • sum(associated_key) = the values of the specified key. a key is required. • count() = number of sessions, no associated key used. If included, it is ignored.
Time Window	This is the duration in hours, minutes, or seconds within which the threshold must be reached to trigger a correlation session.
Status	This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.

The **Rule Editor** dialog provides the fields and options needed to define a network rule. The fields correspond exactly to the grid columns.

Action	Description
Reset	Resets the contents of the dialog to their values before editing; changes are discarded.
Cancel	Cancels any edits and closes the Rule Editor Dialog.
OK	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor Dialog closes.
Save	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See Fix Rules with Invalid Syntax.

Network Rules Tab

The Network Rules tab (**ADMIN > Services >** select a Decoder and click **> View > Config > Network Rules tab**) enables you to manage network rules. NetWitness Suite applies network rules at the packet level. Network rules consist of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied to the Decoder. Rules can be applied to multiple layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules apply only to packet Decoders.

What do you want to do?

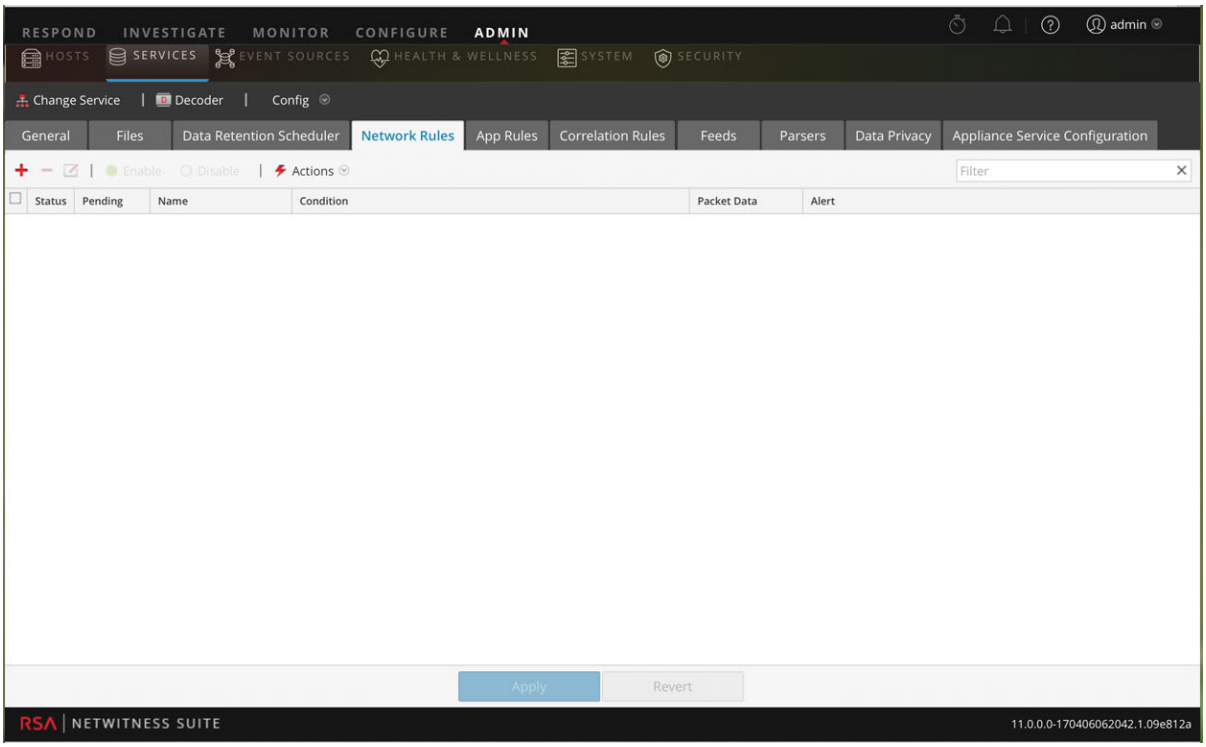
User Role	I want to...	Documentation
Administrator	add, edit, or fix network rules	Configure Network Rules

Related Topics

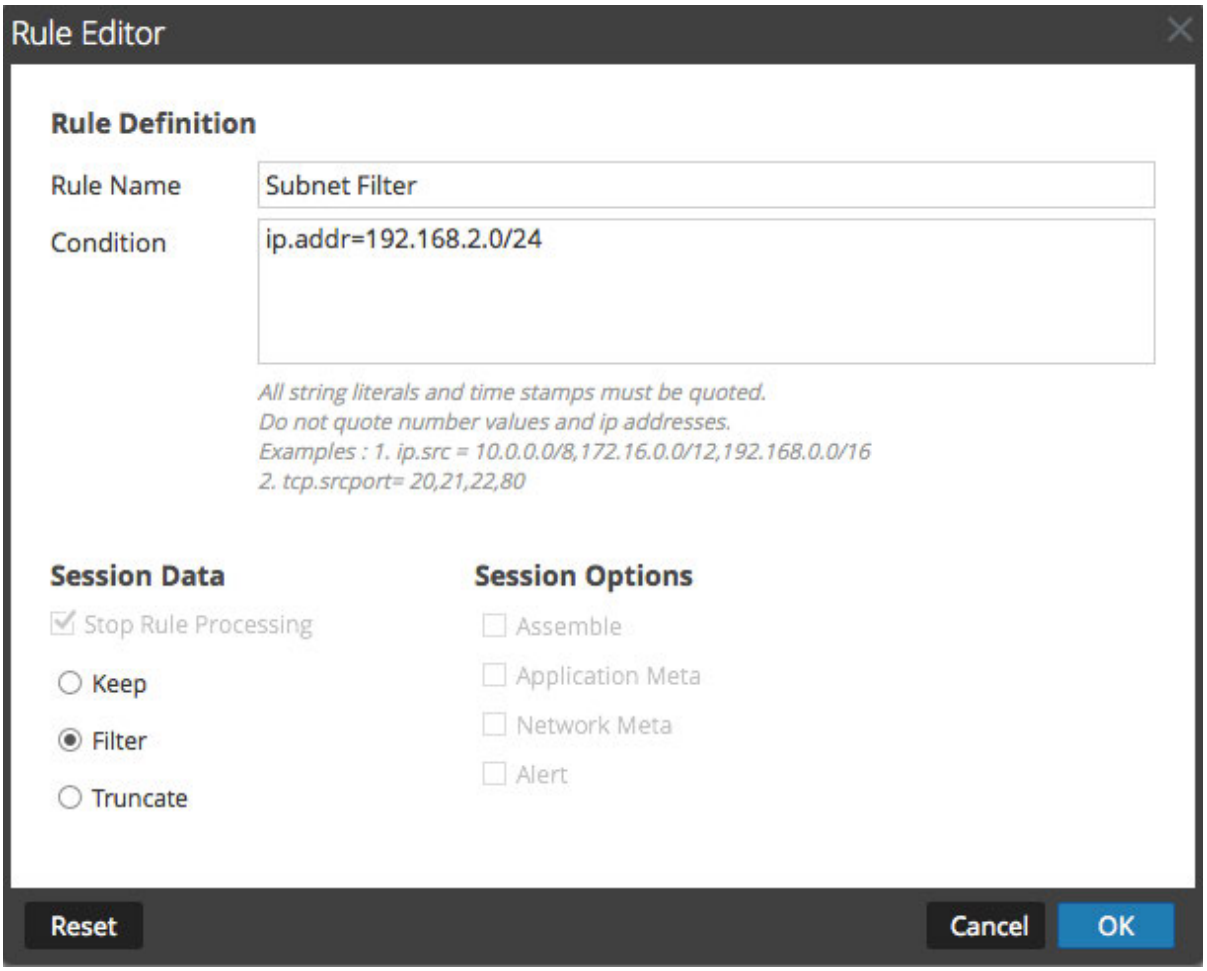
- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- Configure Decoder Rules
- Services Config View - Rules Tabs

Quick Look

The following figure shows the Network Rules tab.



The following figure shows the Rule Editor dialog for a network rule.



The following table describes the columns in the Network Rules grid.

Column	Description
Pending	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains . Once the rules are applied, the pending indicator is removed.
Name	This is the rule name, a descriptive identifier for the rule.
Condition	This is the definition of the condition that triggers an action when matched.
Packet Data	This column displays the Session Data action taken when a packet matches the rule. Possible values are **Filter**, **Keep**, or **Truncate**.

Column	Description
Alert	This column indicates whether the Decoder generates a custom alert when metadata matches the rule. Possible values are **Enabled** or **Disabled**.
Status	This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.

The **Rule Editor** dialog provides the fields and options needed to define a network rule.

The following table describes the Rule Definition fields.

Field	Description
Rule Name	The descriptive name that identifies the rule.
Condition	The definition of the condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the Intellisense window actions. As you build the rule definition, Intellisense displays syntax errors and warnings. In conditions, all string literals and time stamps must be quoted. Do not quote number values and IP addresses. Configure Decoder Rules provides additional details. This section also describes the meta keys that NetWitness Suite supports for use in network rule conditions.

The following table describes the Session Data actions.

Action	Description
Stop Rule Processing	If checked, further rule evaluation ends if the rule is matched, and the session is saved as indicated. If not checked, rule evaluation continues until all rules are evaluated.

Action	Description
Keep	The packet payload and associated meta are saved when they match the rule.
Filter	The packet is not saved when it matches the rule.
Truncate	The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.

The following table describes the session options.

Action	Description
Assemble	If checked, the assembler assembles the packet chain when it matches the rule.
Network Meta	The packet generates network metadata when it matches the rule.
Application Meta	The packet generates application metadata when it matches the rule.
Alert	The packet generates a custom alert when metadata matches the rule.

The following table describes Rule Editor dialog actions.

Action	Description
Reset	Resets the contents of the dialog to their values before editing; changes are discarded.
Cancel	Cancels any edits and closes the Rule Editor dialog.
OK	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor dialog closes.
Save	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See Fix Rules with Invalid Syntax.

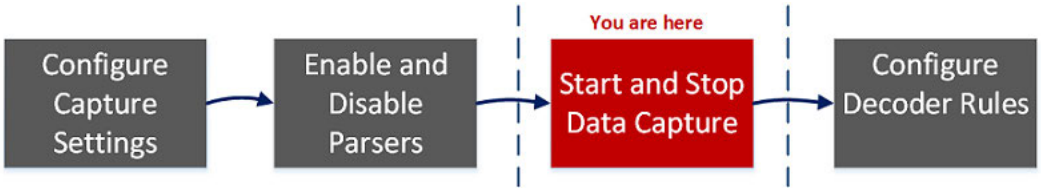
Services System View - Decoders

A Log Decoder is a special type of Decoder, and is configured and managed in a similar way to a Decoder. Therefore, most of the information in this section refers to both types of Decoders. Differences for Log Decoders are noted.

To reach the Services System view, go to **ADMIN > Services >** select a Decoder or Log Decoder > > **View** > **System**.

Workflow

The following figure depicts the workflow for common Decoder configuration tasks with the steps you can complete in this view highlighted.



What do you want to do?

User Role	I want to...	Documentation
Administrator	configure capture settings	Configure Capture Settings
Administrator	manage parsers and log parsers	Enable and Disable Parsers and Log Parsers
Administrator	start and stop data capture*	Start and Stop Data Capture
Administrator	upload packet capture and log files*	Upload a Log File to a Log Decoder Upload a Packet Capture File
Administrator	reset log stats, perform host tasks, shutdown the service, shutdown the appliance service, and reboot the host*	*Hosts and Services Getting Started Guide*

User Role	I want to...	Documentation
Administrator	configure rules	Configure Decoder Rules

*You can complete these tasks here.

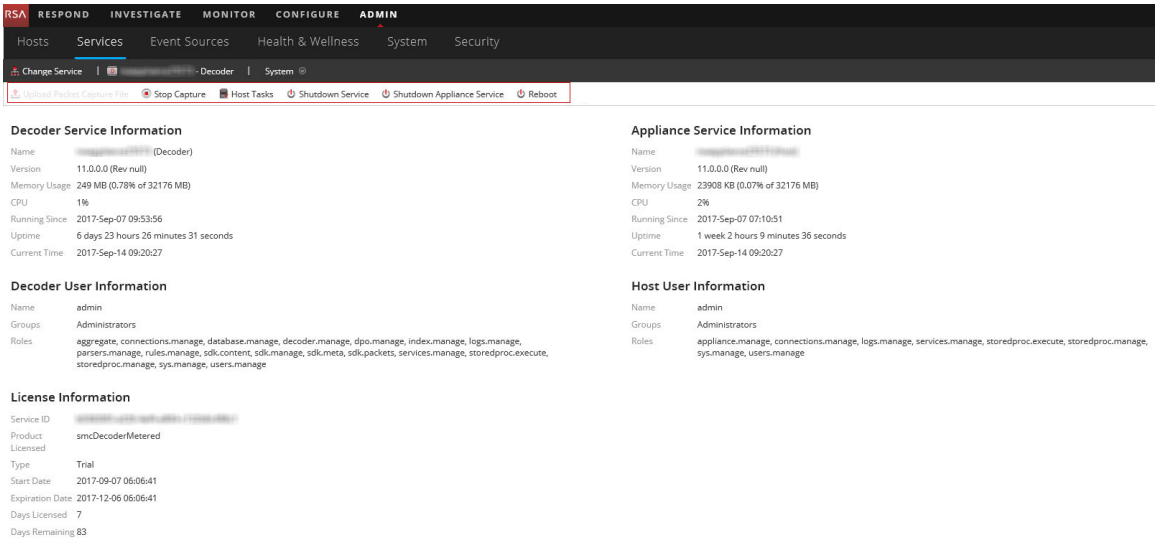
Related Topics

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

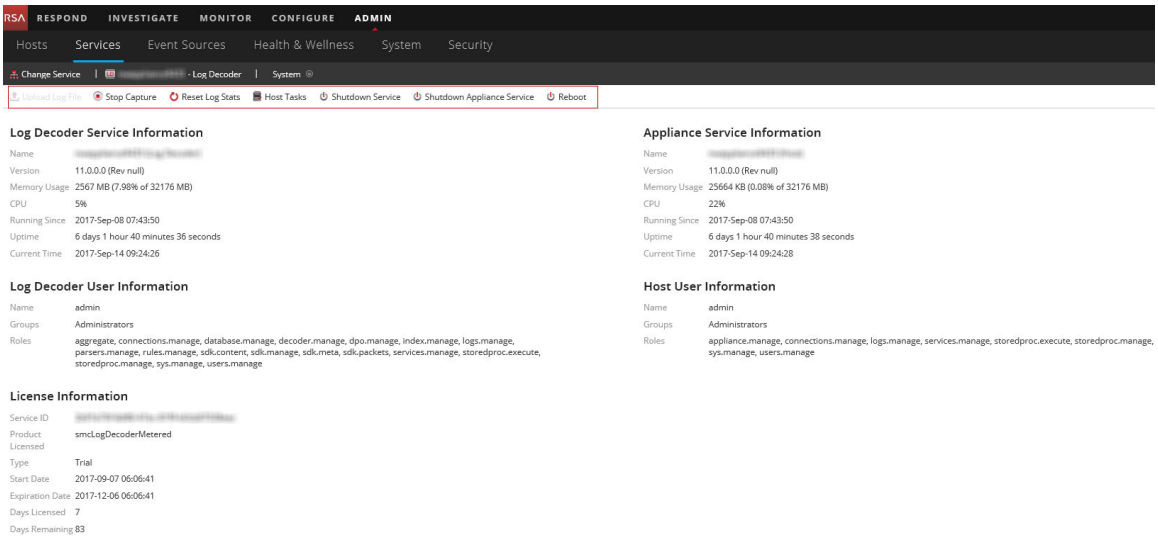
- Decoder and Log Decoder Quick Setup
- Configure Common Settings on a Decoder
- "Services System View" in the *Hosts and Services Getting Started Guide*

Quick Look

This is an example of the Services System view for a Decoder.

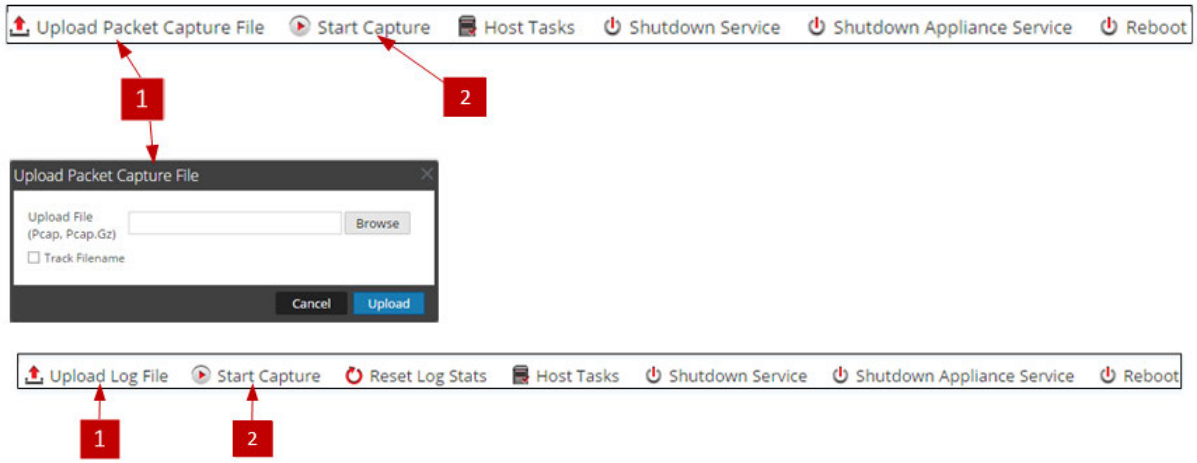


This is an example of the Services System view for a Log Decoder.



Service Info Toolbar

These two toolbars illustrate the options specific to Decoders and Log Decoders.



In addition to the common options in the Services System view toolbar, you can start and stop capture of packets or logs. The upload file options are different for the standard Decoder (packet capture file) and the Log Decoder (log file).

Action	Description
Upload Packet Capture File	Displays a dialog that provides a way to select a packet capture (.pcap) file for upload to the selected Decoder. For more information, see Upload a Packet Capture File. **Note:** This option does not apply to Log Decoders.

Action	Description
Upload Log File	Displays a dialog that provides a way to select a log (.log) file for upload to the selected Log Decoder. For more information, see Upload a Log File to a Log Decoder.
Start/Stop Capture	Starts packet capture on the selected Decoder. When packet capture is in progress, the option in the toolbar changes to Stop Capture, and the option to upload a file is unavailable.

RSA NETWITNESS® SUITE

ESA Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Event Stream Analysis Overview **6**

Configure ESA Correlation Rules **8**

Prerequisites 8

Procedure 8

Result 8

Step 1. Add a Data Source to an ESA Service 9

Prerequisites 9

Procedures 9

Step 2. Configure Advanced Settings for an ESA Service 11

Procedures 11

Configure ESA Analytics **14**

Configure the Whois Lookup Service 14

Prerequisites 15

Configure the Whois Lookup Service 16

Mapping ESA Data Sources to Analytics Modules 17

Module Deployment Example - Two ESAs 17

Module Deployment Example - One ESA 18

Prerequisites 19

Create ESA Analytics Mappings 20

Deploy ESA Analytics Mappings 25

Update a Mapping 25

Undeploy a Mapping 25

Delete a Mapping 26

Change the Warm-up Period and Lag Time 26

Additional ESA Correlation Rules Procedures **29**

Change Memory Threshold for Trial Rules 29

Prerequisites 29

Procedure 30

Configure ESA to Use a Memory Pool 30

Procedure 32

Result 34
Configure ESA to Use Capture Time Ordering 34
Capture Time Order Workflow 35
Prerequisites 36
Procedures 36
Troubleshooting Tips 37
Disable Capture Time Ordering 38
Disable Position Tracking 38
Start, Stop, or Restart ESA Service 39
Start ESA Service 39
Stop ESA Service 39
Restart ESA Service 39
Audit Logs and Verify ESA Component Versions and Status 39
Audit Log Rules 40
Verify ESA Server Version 41
Verify MongoDB Version 41
Verify MongoDB Status 41
References 42
Services Config View Data Sources Tab 43
Workflow 43
What do you want to do? 44
Related Topics 44
Quick Look 44
Services Config View Advanced Tab 47
Workflow 47
What do you want to do? 48
Related Topics 48
Quick Look 48
Whois Lookup Service Configuration 51
What do you want to do? 51
Related Topics 51
Whois Lookup Service Configuration 52
ESA Analytics Mappings 55
Workflow 55

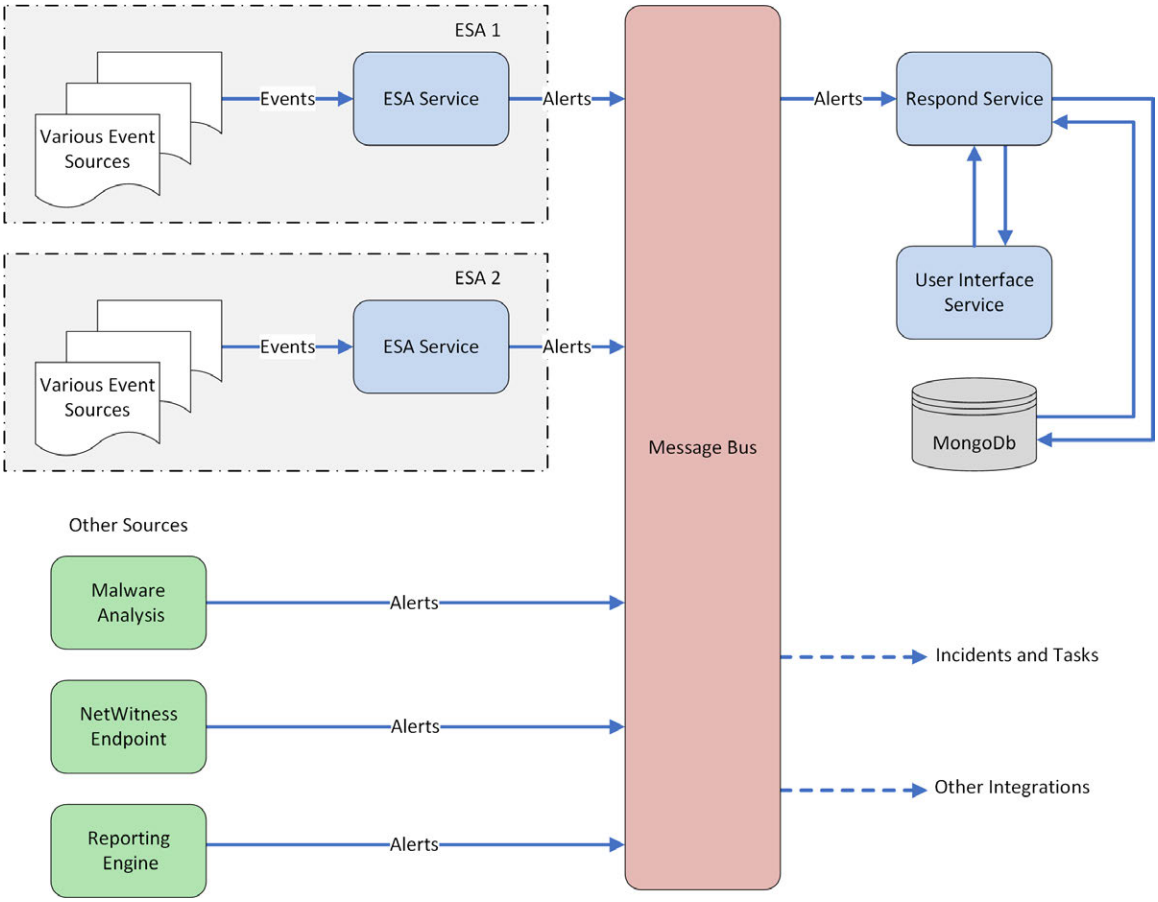
What do you want to do? 56
Related Topics 56
Quick Look 56
Module Settings 61
What do you want to do? 61
Related Topics 61
Module Settings 61

Event Stream Analysis Overview

RSA NetWitness® Suite Event Stream Analysis (ESA) provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators.

ESA's advanced Event Processing Language allows you to express filtering, aggregation, joins, pattern recognition and correlation across multiple disparate event streams. Event Stream Analysis helps to perform powerful incident detection and alerting.

The following diagram shows the high-level data workflow:



There are two ESA services that can run on an ESA host:

- Event Stream Analysis (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

The first service is the Event Stream Analysis service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live. The second service is the ESA Analytics service, which is used for Automated Threat Detection. Because the ESA Analytics service uses preconfigured ESA Analytics modules for Automated Threat Detection, you do not have to create or download rules to use Automated Threat Detection.

ESA Analytics services use query-based aggregation (QBA) to collect filtered events for the ESA Analytics modules from Concentrators. Only the data required by a module is transferred between the Concentrator and the ESA Analytics system. For example, using a Suspicious Domains ESA Analytics module, such as C2 for Packets (http-packet), an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

Configure ESA Correlation Rules

This topic provides high-level tasks to configure RSA NetWitness Suite Event Stream Analysis (ESA) Correlation Rules using the Event Stream Analysis service.

Prerequisites

Make sure that you:

- Install the Event Stream Analysis service in your network environment.
- Install and configure one or more Concentrators in your network environment.

Procedure

Note: You can configure ESA using an SSL port (50030) only. There is no option to configure a Non-SSL port.

To configure Event Stream Analysis:

Tasks	Reference
1. Add a Concentrator as data source to the Event Stream Analysis service.	Refer to Step 1. Add a Data Source to an ESA Service
2. Configure notifications for the Event Stream Analysis service.	Refer to "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide*.
3. Download Event Stream Analysis content using Live.	Refer to "Live Search View" in the *Live Resource Managment Guide*.
4. (Optional) Advanced configuration for Event Stream Analysis service.	Refer to Step 2. Configure Advanced Settings for an ESA Service.

Result

The Event Stream Analysis service is configured and you can now add ESA Rules for event processing and alerting. For information on adding ESA Rules, see "Add Rules to the Rule Library" in the *Alerting with ESA Correlation Rules User Guide*.

Step 1. Add a Data Source to an ESA Service

This topic describes how to add a new or existing data source to the Event Stream Analysis service.

An ESA service ingests data from a Concentrator to detect incidents and alert the user. For ESA to analyze data, you need to configure the sources from which the ESA will read data. Use the procedures in this topic to add data sources for your ESA.

Prerequisites

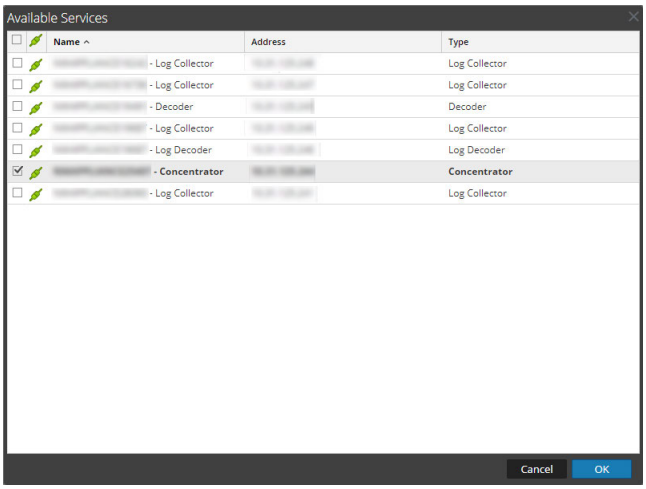
You must have one or more Concentrators configured in NetWitness Suite.

The Event Steam Anaysis service must be installed and running on NetWitness Suite.

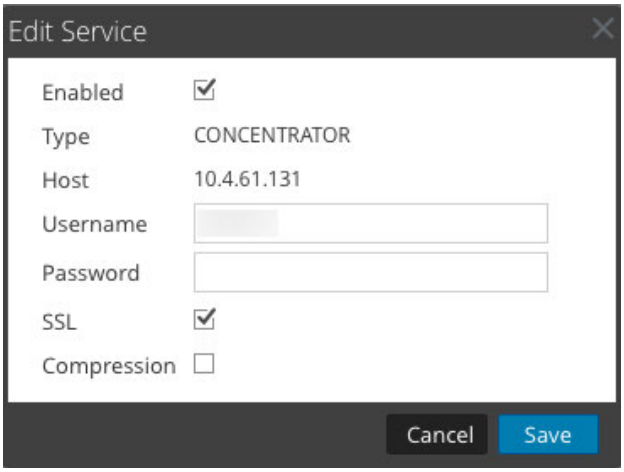
Procedures

Add an Existing Service as Data Source

1. Go to **ADMIN> Services**.
   The Services view is displayed.
2. In Services view, select an ESA service and select > **View** > **Config**.
3. On the **Data Sources** tab, click + .
   The available services are displayed as shown in the following figure.



4. Select a Concentrator service and click **OK**.
   The Edit Service dialog is displayed.



5. Click **Enable** to enable (or disable) the data source (it is enabled by default when adding a new service).
6. Enter a valid **Username** and **Password** for the service.
7. Click to enable or disable the **SSL** or **Compression** options.
8. Click **Save** to save the configuration and close the Edit Service dialog.
9. Click **Apply** to complete the change on the **Data Sources** tab.
   The service is added to the list of services in the **Data Sources** tab.

Note: You can add a Log Decoder as a data source for ESA but RSA recommends you add a Concentrator to take advantage of undivided aggregation as the Decoder may have other processes aggregating from it.

Edit Settings for a Data Source

To edit settings, including the username and password, for a configured data source:

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. In the **Services** view, select a Concentrator service.
3. Click .
   The Edit Service dialog is displayed (see previous figure).
4. Modify the settings as desired, including entering a new username and password. The username field will be prepopulated with the currently configured username. To change the

password, enter a new password in the password field. If you leave the password field blank, the previously configured password will continue to be used.

5. Click **Save** to save the changes and close the Edit Service dialog.
6. Click **Apply** to complete the change on the **Data Sources** tab.

Step 2. Configure Advanced Settings for an ESA Service

This topic provides instructions to configure advanced settings for an Event Stream Analysis service.

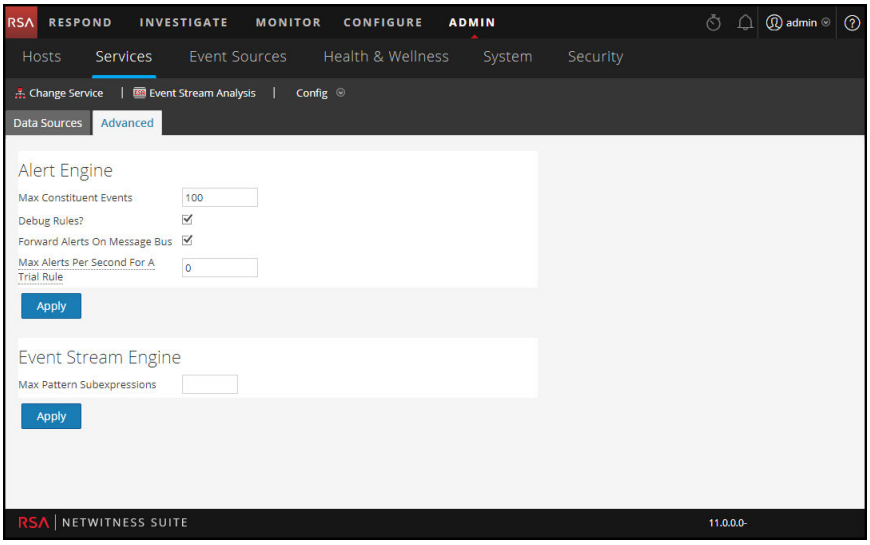
In the Advanced view, you can configure advanced settings to improve performance, to preserve events for rules with multiple events, to buffer events in memory, and to specify the number of events to be stored on the ESA.

Procedures

Configure Advanced Settings

To access the Advanced view and configure advanced settings for an ESA service:

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. In Services view, select an ESA service and > **View** > **Config**.
3. Select the **Advanced** tab.
   The Advanced view is displayed.

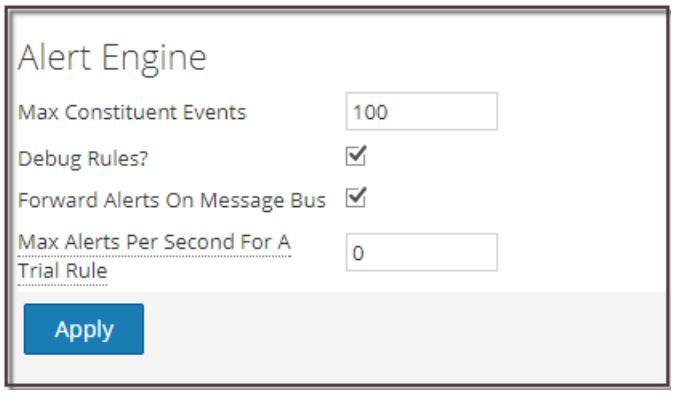


Configure Alert Engine Settings

In the Alert Engine section, you specify values to preserve events for rules that choose multiple events.

Note: After you upgrade to 10.5, the Debug Rules option if enabled previously will be disabled. You will need to enable this option after upgrade.

The following figure shows the Alert Engine section.



To configure Alert Engine settings:

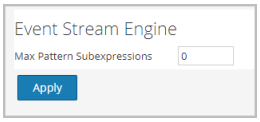
1. In the Alert Engine section, specify a value for **Max Constituent Events**. The default value is 100.
2. Select **Debug Rules?** to enable debugging rules.
3. If you want alerts to be sent to Message Bus and Respond, select the **Forward Alerts On Message Bus** option.
4. To specify the maximum number of alerts to be forwarded to the Message Bus for the trial rule, select **Max Alerts Per Second for a Trial Rule**. The The default value is **10**.
5. Click **Apply** to save the changes and put them into effect immediately.

Note: For more information on the parameters in the Alert Engine section, see Alert Engine Settings in ESA Advanced View.

Configure Event Stream Engine Settings

In the Event Stream Engine section, you specify details to improve performance.

The following figure shows the Event Stream Engine section.



To configure Event Stream Engine settings:

1. In the Event Stream Engine section, specify **Max Pattern Subexpressions**.
2. Click **Apply** to save the changes and put them into effect immediately.

Note: For more information on the parameters in the Event Stream Engine section, see Event Stream Engine Settings in ESA Advanced View.

Configure ESA Analytics

This section provides high-level tasks to configure ESA Analytics services for RSA NetWitness® Suite Automated Threat Detection. The Automated Threat Detection functionality enables you to analyze the data that resides on one or more Concentrators by using preconfigured ESA Analytics modules, such as Suspicious Domains. For example, using a Suspicious Domains module, an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

There are two ESA services that can run on an ESA host:

- Event Stream Analysis (ESA Correlation rules)
- Event Stream Analytics Server (ESA Analytics)

The first service is the Event Stream Analysis service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live. The second service is the ESA Analytics service, which is used for Automated Threat Detection and is configured in this section. Because the ESA Analytics service uses preconfigured ESA Analytics modules for Automated Threat Detection, you do not have to create or download rules to use it.

There are currently two ESA Analytics modules available and they are both for Suspicious Domains:

- C2 for Packets (http-packet)
- C2 for Logs (http-log)

Configure the Whois Lookup Service

The RSA NetWitness Suite Automated Threat Detection functionality enables you to automatically analyze data sources by using preconfigured ESA Analytics modules. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics services process these modules to identify advanced threats.

The Whois Lookup service configuration is required for the Suspicious Domains modules.

Note: (**Important**) RSA strongly recommends that you configure the Whois Lookup service for accuracy in Automated Threat Detection scoring.

Prerequisites

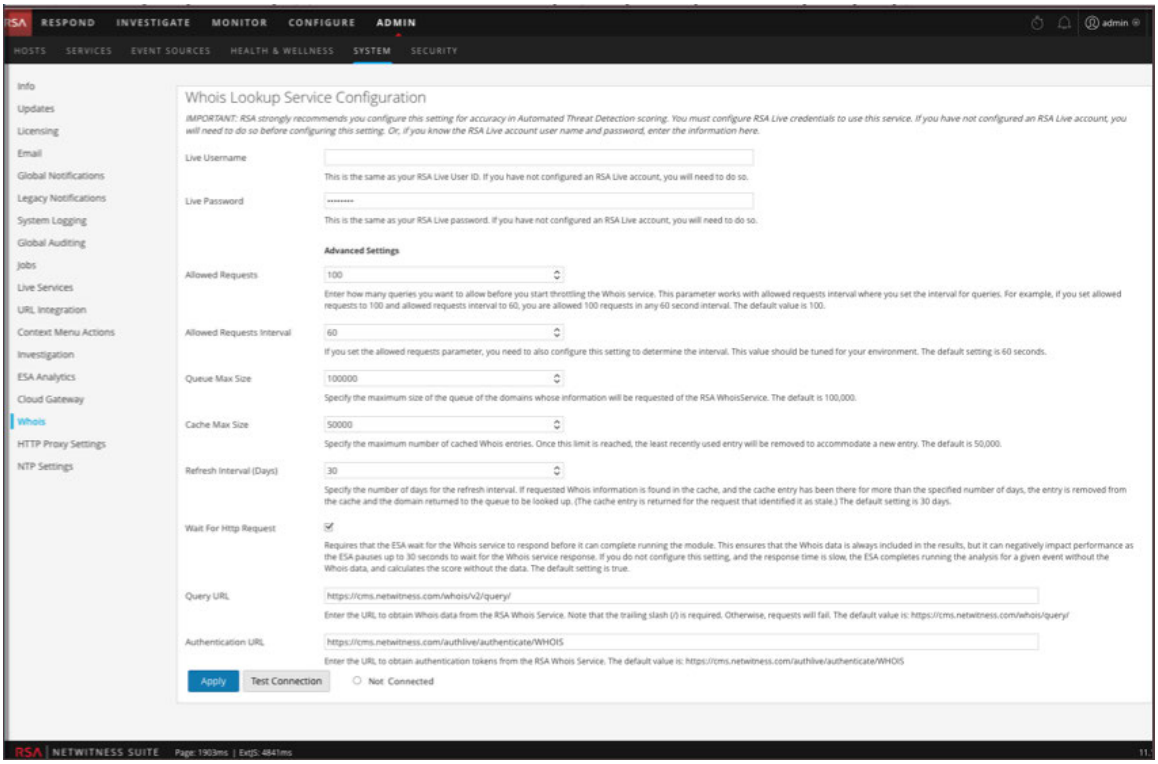
- You must have an RSA Live account to use the Whois Lookup service.
- The ESA Analytics Server service must be available (shows a green circle) in the ADMIN > Services view.

If you configured a Live account in the Live Services panel (ADMIN > System > Live Services), the Whois Lookup Service is automatically configured for you. You only need to check the connection of the Whois Lookup service.

Note: If you do not have an RSA Live account, you can create one at the RSA Live Registration Portal:
https://cms.netwitness.com/registration/
The *Live Services Management Guide* provides additional information.

Configure the Whois Lookup Service

1. Go to **ADMIN > System**.
2. In the options panel, select **Whois**.
3. In the **Whois Lookup Service Configuration** panel, check to see if the Whois Lookup service is connected. At the bottom of the panel, a connected service shows a green circle next to **Connected**: ● Connected



   If it is connected, you are finished with the configuration and you can skip the remaining steps. To adjust the advanced settings, go to step 5.
   If the service is not connected, continue to step 4.
4. In the **Live Username** and **Live Password** fields, enter your RSA Live account credentials to access the RSA Whois server.
5. If necessary, you can adjust the advanced settings. However, RSA recommends that you use the default values. Whois Lookup Service Configuration provides additional details.
6. To test your connection, click **Test Connection**.
   A successful connection shows a green circle next to **Connected**: ● Connected
7. Click **Apply** to save your changes.

Mapping ESA Data Sources to Analytics Modules

This topic tells Administrators how to map specific ESA Analytics modules to multiple data sources and ESA Analytics services, which can make processing more efficient.

You can analyze the data that resides on one or more Concentrators with the RSA NetWitness Suite Automated Threat Detection functionality by selecting a preconfigured ESA Analytics module. The data analyzed by these modules is used to identify advanced threats. To better utilize your network resources and reduce unnecessary data flow, you can map multiple data sources, such as Concentrators, to multiple ESA Analytics services in order to process data more efficiently and take advantage of additional capacity.

An *ESA Analytics module* is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics modules reside within ESA Analytics services.

When you deploy your mapping, the selected ESA Analytics services use query-based aggregation to collect the appropriate filtered events for the selected module from the Concentrators. Query-based aggregation is a predefined query that only transfers data for the selected ESA Analytics module. Only the data required by the module is transferred between the Concentrator and the ESA Analytics system.

There are currently two ESA Analytics modules available for Suspicious Domains: C2 for Packets (http-packet) and C2 for Logs (http-log).

Module Deployment Example - Two ESAs

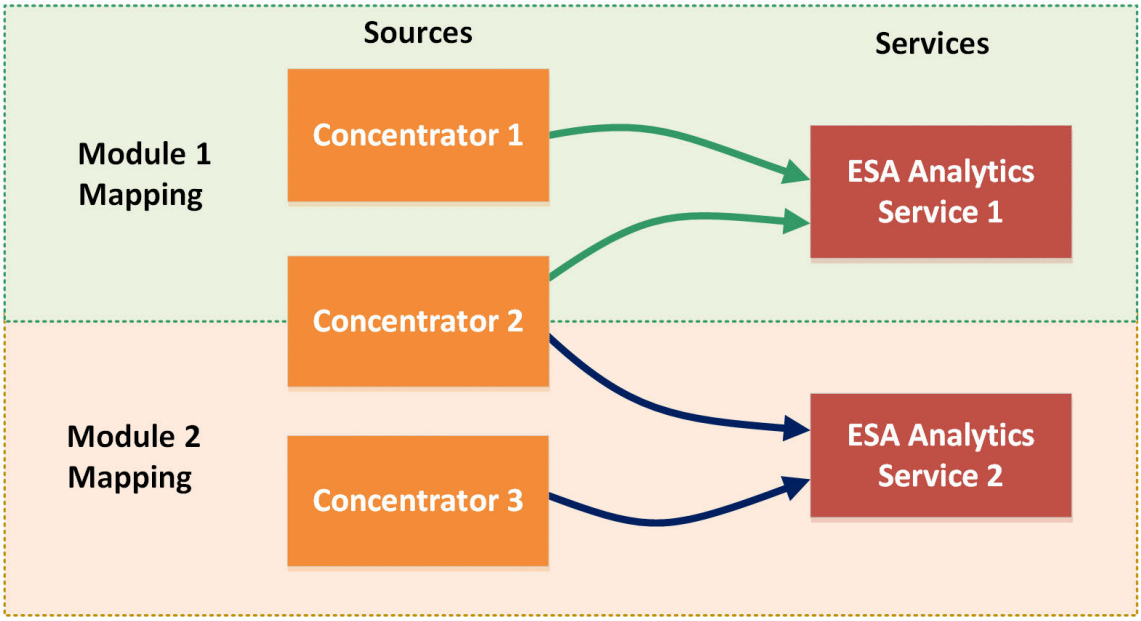
To take advantage of your additional Concentrator capacity, you can map an ESA Analytics module to an ESA Analytics service and deploy it to analyze data from multiple data sources at the same time.

For example, if you have three Concentrators and two ESA Analytics services, you can create and deploy the following mappings:

- Map Module 1 to the Concentrator 1 and 2 sources and the ESA Analytics 1 service. ESA Analytics Service 1 analyzes Module 1 filtered events from Concentrators 1 and 2.
- Map Module 2 to the Concentrator 2 and 3 sources and the ESA Analytics 2 service. ESA Analytics Service 2 processes Module 2 filtered events from Concentrators 2 and 3.

In this example, Module 1 represents an ESA Analytics module, such as C2 for Packets (http-packet) and Module 2 represents another ESA Analytics module, such as C2 for Logs (http-logs) in another location.

Module Deployment Example – Two ESAs



This example shows how both services can process data from the same Concentrator. Notice that ESA Analytics Services 1 and 2 can both process data from Concentrator 2. ESA Analytics Service 1 queries data for Module 1 events and ESA Analytics Service 2 queries different data for Module 2 events.

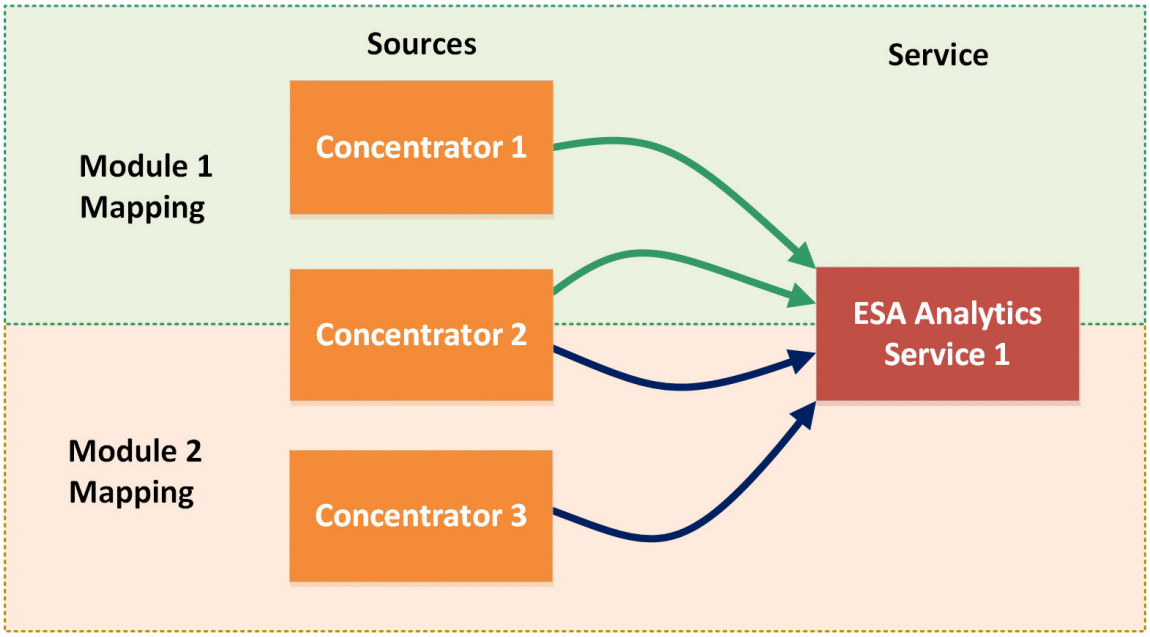
Module Deployment Example - One ESA

In addition to creating module mappings that are processed by different ESA Analytics services, you can map more than one module to the same ESA Analytics service.

For example, if you have three Concentrators and one ESA Analytics service, you can create and deploy the following mappings:

- Map Module 1 to the Concentrator 1 and 2 sources and the ESA Analytics 1 service. ESA Analytics Service 1 analyzes Module 1 filtered events from Concentrators 1 and 2.
- Map Module 2 to the Concentrator 2 and 3 sources and the ESA Analytics 1 service. ESA Analytics Service 1 also processes Module 2 filtered events from Concentrators 2 and 3.

Module Deployment Example – One ESA



This example shows how one service can process data from more than one module. Notice that ESA Analytics Service 1 can process data from Concentrators 1 and 2 for Module 1. It also processes data from Concentrators 2 and 3 for Module 2. ESA Analytics Service 1 queries data for Module 1 events and queries different data for Module 2 events.

Caution: Ensure that all NetWitness Suite host services are in sync with a consistent time source.

Prerequisites

- All NetWitness Suite host services must be in sync with a consistent time source.
- The Concentrator hosts and services must be discovered and available in the NetWitness Suite user interface.
- All module-specific requirements must be followed.
  - For Suspicious Domains:
    - Configure log settings (Suspicious Domains for Logs only)
    - Create a whitelist using the Context Hub service.
    - Configure the Whois Lookup Service.

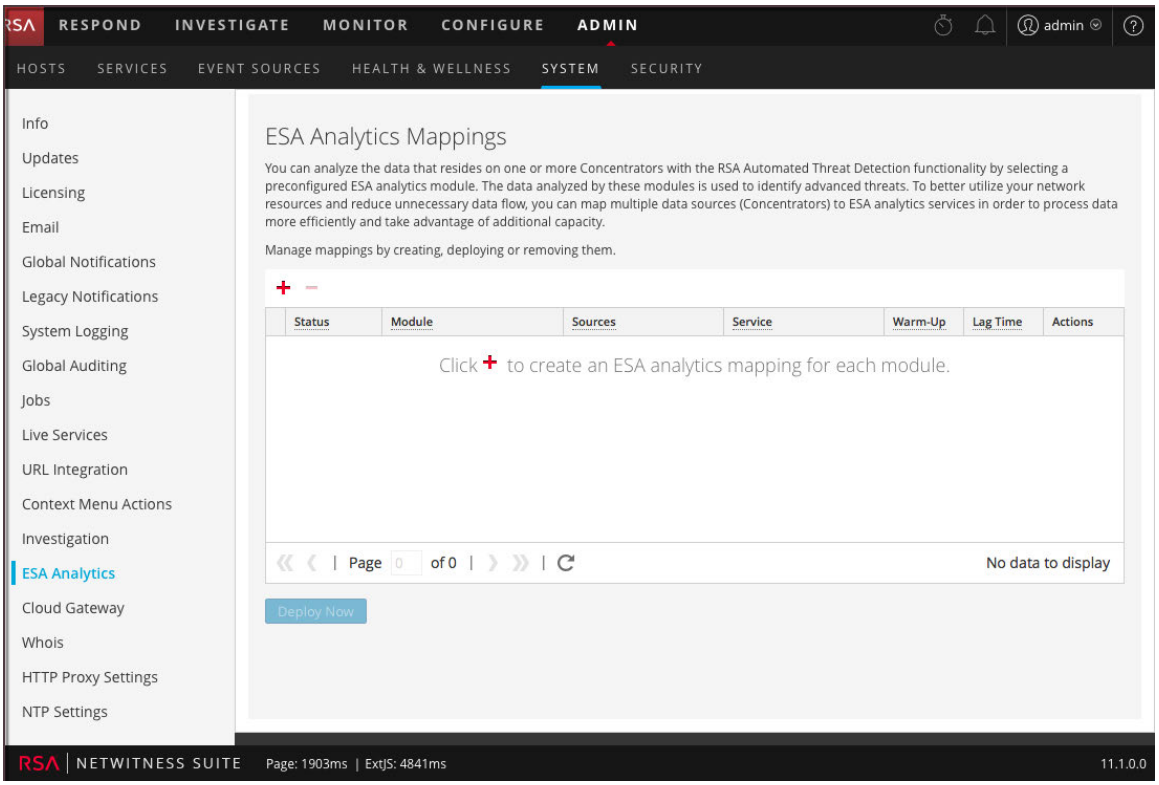
- Verify that the C2 incident rule is enabled and monitor it for activity.
- Verify that the incidents are grouped by Suspected C&C.

For step-by-step procedures, see the *NetWitness Suite Automated Threat Detection Configuration Guide*.

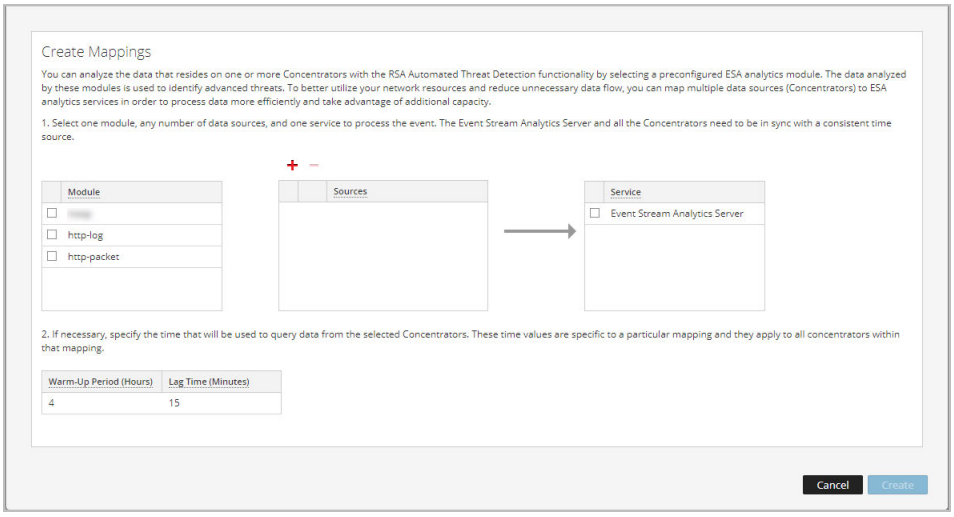
Create ESA Analytics Mappings

The following procedure tells you how to map ESA Analytics modules to sources and services. After creating and reviewing the mappings, you deploy them so that they can start aggregating data.

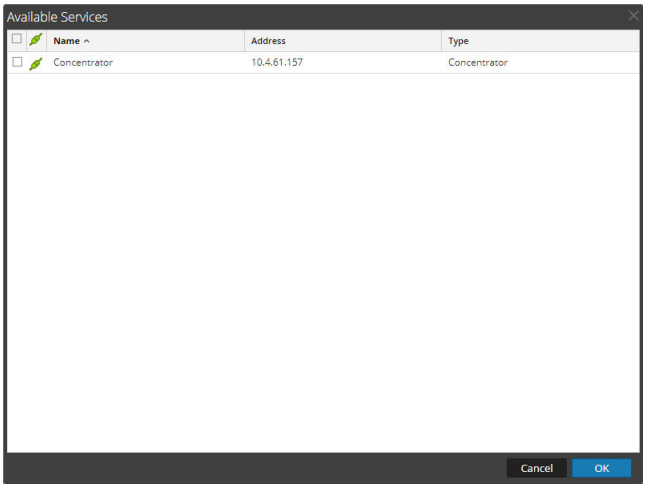
1. Go to **ADMIN** > **System**, and in the options panel, select **ESA Analytics**.
   The **ESA Analytics Mappings** panel is displayed.



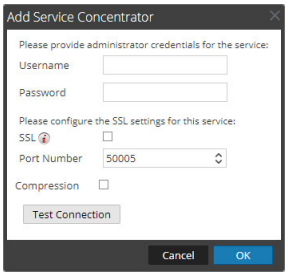
2. Click + to create an ESA Analytics mapping. Create a separate mapping for each module. The **Create Mappings** dialog is displayed.



3. In the **Module** list, select a module.
4. Configure one or more data sources (Concentrators) for your mappings. Do the following for each Concentrator:
   a. Click + .
      The Available Sources dialog shows the data sources that are available from the Admin > Services view.

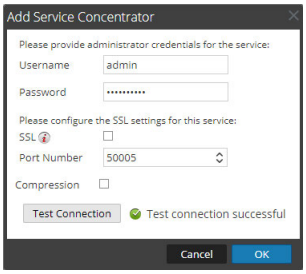


b. In the **Available Sources** dialog, select a Concentrator and click **OK**.
The Add Source dialog is displayed.



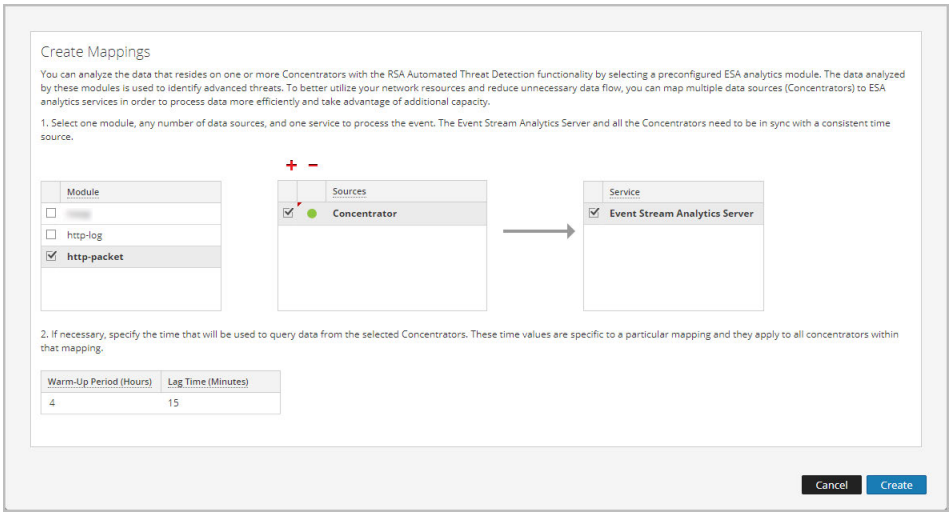
c. In the **Add Source** dialog, type the Administrator username and password for the Concentrator.

d. Click **Test Connection** to make sure that it can communicate with the ESA Analytics service.



e. Click **OK**.
After you configure your data sources and they appear in the Sources list, you can reuse them for additional mappings.

5. In the **Sources** list, select one or more data sources to aggregate the data for the module.



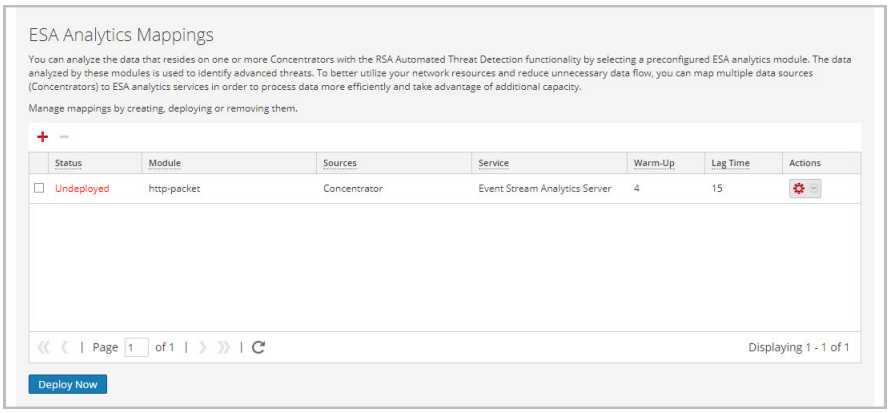
A solid colored green circle indicates a running service and a white circle indicates a stopped service.

6. In the **Service** list, select an ESA Analytics service to process the data for the module.
7. If necessary, specify the time that will be used to query data from the selected Concentrators:

Field	Description
Warm-up Period (Hours)	Specifies a warm-up duration (in hours). A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. For more information about Warm-up Period and Lag time, see Module Settings.

Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. For more information about Warm-up Period and Lag time, see Module Settings.

8. Click **Create**.
   The mappings that you create appear in the list of existing mappings with a status of **Undeployed**.



Important: To start a module so that it starts aggregating data, you need to deploy it.

Deploy ESA Analytics Mappings

After you create your mappings, you need to deploy them in order to start aggregating data for the modules.

1. In the list of mappings, verify that the status of the mappings that you want to deploy show as **Undeployed**.
2. Select one or more mappings with a status of Undeployed and select **Deploy Now**.
   All selected mappings in the Undeployed state start to aggregate data as configured in the mapping. The mapping status changes to **Deployed**.
   You cannot deploy a mapping that has already been deployed.

Update a Mapping

You can only have one mapping per module. If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that module.

You can make the following updates to a deployed mapping without deleting it:

- Undeploy the mapping
- Change the warm-up period and lag time

You can also change the warm-up period and lag time for an undeployed module mapping.

Undeploy a Mapping

If you want to stop aggregating data for a module mapping, but you do not want to delete the mapping, you can undeploy it. This gives you the option of deploying it at a later time. When you undeploy a mapping, the specified ESA Analytics service stops pulling data from the data source for that module.

Caution: Undeploying a mapping with a status of Deployed will affect data aggregation for that module.

To undeploy a mapping:

1. In the ESA Analytics Mappings panel, select the deployed mapping that you want to undeploy.
2. In the **Actions** column, select > **Undeploy**.

   The status changes from Deployed to Undeployed and data aggregation stops.

Delete a Mapping

You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not running, it does not affect data aggregation.

You should undeploy a mapping with a status of Deployed before deleting it. Undeploying and deleting a mapping clears the configuration on the ESA server, reverts the deployment for that mapping, and stops pulling data from the data source for that module.

Caution: Undeploying and deleting a mapping will affect data aggregation for that module.

To delete a mapping:

1. In the ESA Analytics Mappings panel, select the mapping that you want to delete. You can only delete one mapping at a time.
2. Click .

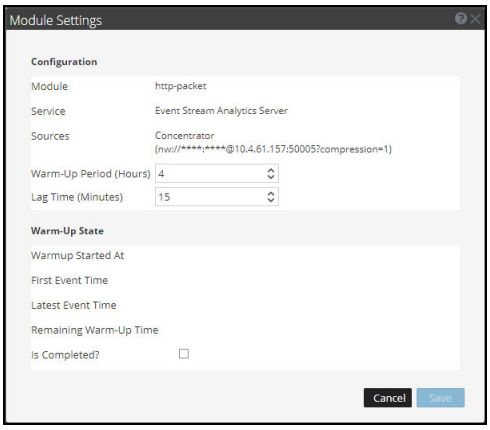
Change the Warm-up Period and Lag Time

You may want to adjust the warm-up period for a specific module mapping. For example, after the warm up period is complete, you can increase the warm-up period setting to allow additional warm-up time. You can even increase the warm-up period when your module mapping is actively warming up.

If necessary, you can change the lag time for the module. The lag time defines the buffer between the current (system) time and the time when the module ingests the data.

1. In the ESA Analytics Mappings panel, select the mapping that you want to change and in the **Actions** column, select > **Edit Module**.

   The Module Settings dialog shows the selected module, ESA Analytics service, and data sources for the mapping. The data sources show the URLs used to communicate with ESA.



2. Review the **Warm-Up State** section to determine the current warm-up state:
   - **Warm Up Started At** - The time when the first event was processed by the ESA Analytics module from the data source.
   - **First Event Time** - The time that the first event occurred. The warm-up time is based on this time.
   - **Latest Event Time** - The time that the latest event occurred.
   - **Remaining Warm Up Time** - The number of hours remaining in the warm-up period.
   - **Is Completed?** - Indicates whether the warm-up period is complete. If it is true, the warm-up period is complete. If it is false, the module is still warming up and you can view the number of hours remaining in the Remaining Warm Up Time field.
3. In the **Configuration** section, you can update the **Warm-Up Period (Hours)** depending on whether or not the warm-up period is complete.
   - **During the warm up period** - You can add hours to the warm-up period or subtract any remaining warm-up time.
   - **The warm-up period is complete** - You can add hours to the warm-up period by adding the difference between the current time and the First Event Time to the hours that you want to add.
     For example, a warm-up period of 10 hours is complete and the First Event Time shows 12:00:00. The current time is 16:00:00 (4 hours later) and you want to add 5 more hours to the warm-up time. To do this, you need to add 9 hours (4+5=9) to the warm-up period of 10, so you would set the new warm-up period to 19 hours.
     You cannot decrease the warm-up period if it is complete, unless you delete the mapping and create a new one.

4. If necessary, you can adjust the **Lag Time (Minutes)** to give the Concentrators in the mapping additional time to finish aggregating all of the data.
5. Click **Save**.
   Changes DO NOT take effect immediately. For the settings to take effect, you need to undeploy and re-deploy the mapping.
6. To undeploy the mapping, in the ESA Analytics Mappings panel, select the mapping that you want to undeploy and > **Undeploy**.
   Data aggregation stops for the selected mapping.
7. To re-deploy the mapping, select the mapping that you want to deploy and > **Deploy**.
   The selected mapping deploys and starts to aggregate data as configured in the mapping.

Additional ESA Correlation Rules Procedures

This topic is a collection of individual procedures, which an Administrator may perform at any time and they are not required to complete the initial setup of ESA Correlation Rules.

Use this section when you are looking for instructions to perform a specific task after the initial setup of ESA.

- Change Memory Threshold for Trial Rules
- Configure ESA to Use a Memory Pool
- Configure ESA to Use Capture Time Ordering
- Start, Stop, or Restart ESA Service
- Audit Logs and Verify ESA Component Versions and Status

Change Memory Threshold for Trial Rules

This procedure is optional and applies only to ESA Correlation Rules.

Administrators can increase or decrease the memory threshold for trial rules. Threshold refers to the ESA memory usage, which includes ESA base memory, trial rules and non-trial rules. When the threshold is exceeded, all deployed trial rules on an ESA service are disabled.

You use trial rules to see if a rule runs efficiently and does not use excessive memory, which can impact performance or force the service to shut down.

By default, the memory threshold is 85, which is the percentage of Java Virtual Memory (JVM).

- The memory threshold is per ESA, not per rule.
- When the memory threshold is exceeded, all trial rules running on the ESA are automatically disabled.
- The ESA configuration has two parameters for trial rules:
  - MemoryThresholdforTrialRules
  - MemoryCheckPeriod, which has a default value of 300 seconds

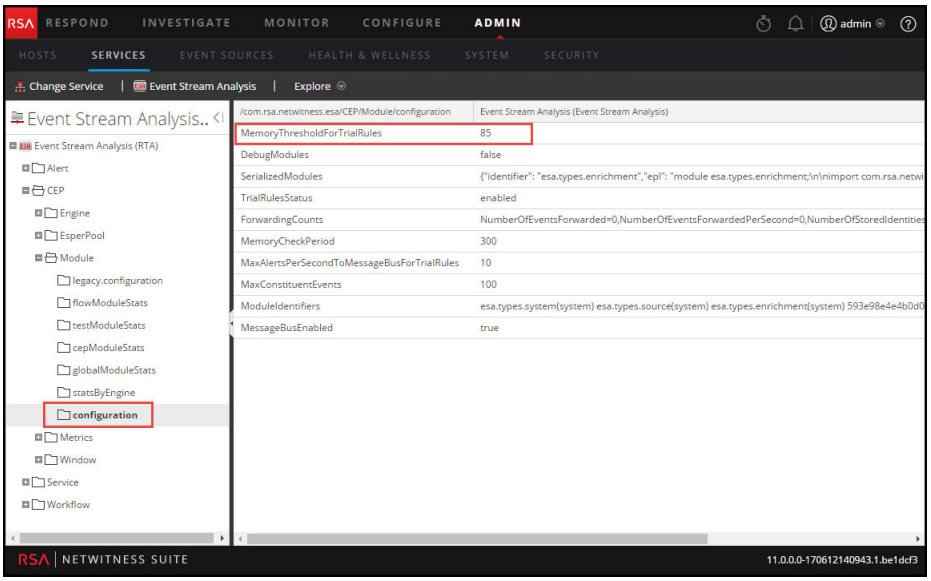
For more information, see "Work with Trial Rules" in the *Alerting with ESA Correlation Rules User Guide*.

Prerequisites

A role with administrative privileges must be assigned to you.

Procedure

1. Log on to NetWitness Suite as admin.
2. Go to **ADMIN** > **Services**.
3. Select the ESA service and select > **View** > **Explore**.
4. On the left, select **CEP > Module** > **configuration**.



5. In the right panel, in **MemoryThresholdForTrialRules** type a percentage of JVM that trial rules on the ESA can not exceed.
   The new memory threshold takes effect immediately.

Configure ESA to Use a Memory Pool

This procedure applies only to ESA Correlation Rules.

Administrators can configure ESA to use a memory pool. A memory pool is a customized implementation of virtual memory for events held by rules in ESA. This helps in scaling the capability of rules by an order of magnitude. When you want to create rules that cover a large time span or which are very complex, you may want to use a memory pool to handle memory more efficiently. When you use a memory pool, instead of holding all of the events in memory, they can be written to disk. This is helpful because when a rule exists that is complex or extends over a long time frame, a large number of events must be held in memor

You can configure memory pool to run in non-batch mode or batch mode:

- **Non-batch mode**. In non-batch mode, events are written to disk as they enter the memory pool. To configure non-batch mode, set the **MapPoolBatchWriteSize** attribute to 1. Non-

batch mode provides a more stable solution because each event is landed and fetched separately without creating memory spikes.

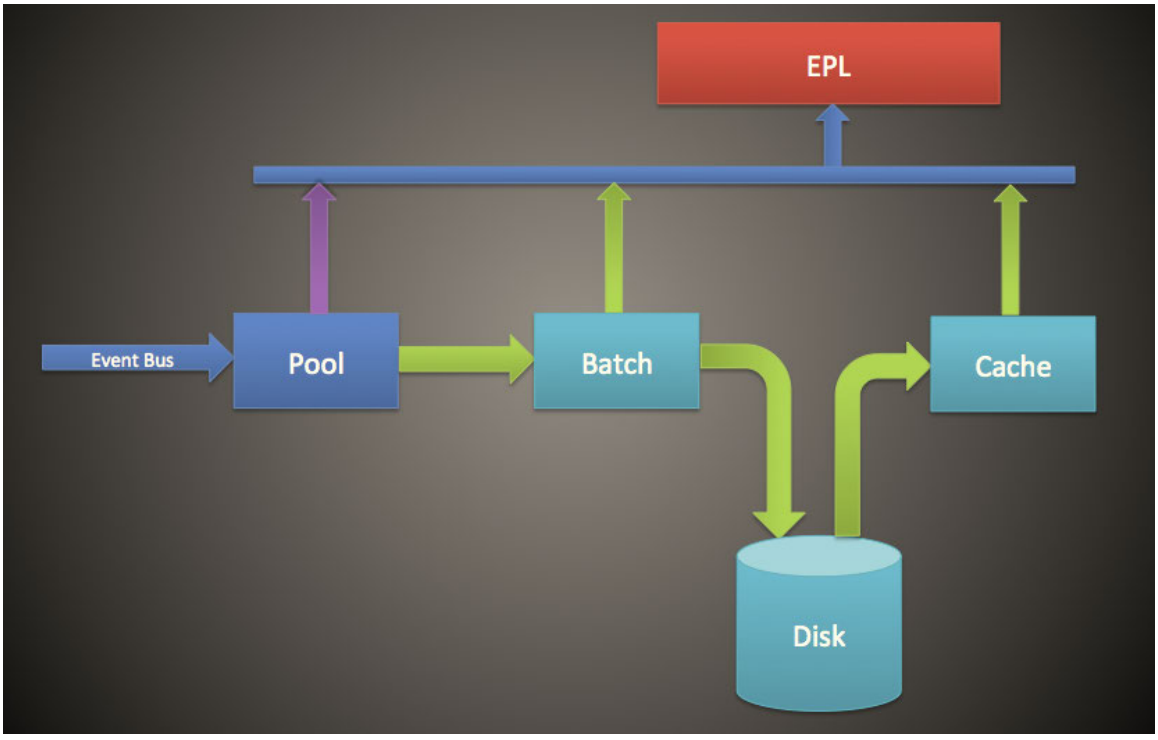
- **Batch mode**. In batch mode, events are grouped into batches and then written to disk. To configure batch mode, set the batch size attribute **MapPoolBatchWriteSize** to a value greater than 1. Batch mode gives better performance since the disk activity for landing events to disk are optimized.

Note: Any changes to these settings will require you to restart the ESA. When ESA restarts, if any events are currently being held by the memory pool, they will be discarded upon restart.

Caution: While this feature can be very helpful in managing memory, it can impact the event processing rate of the ESA. Performance can be affected from 10 to 30 percent, depending on your rules and configuration settings.

Workflow

The following diagram shows the data flow using the memory pool for batch mode.



1. Events are added to the memory pool and references to the events are stored in the memory pool.
2. The events are then batched to be sent to disk (in non-batch mode, this step is skipped).

3. Once the batch has met the threshold, the events are written to disk (in non-batch mode no threshold is required).
4. When the EPL requires an event that was written to disk, the event is sent to the cache and used in the EPL rule.

Procedure

Complete the following steps to configure an ESA memory pool.

1. Go to **ADMIN** > **Services**, select your ESA service, and then > **View** > **Explore**.
2. Select **CEP** > **EsperPool** > **Configuration**.
3. Enter values for the following fields:

Attribute	Description	Configuration
MapPoolPersistenceURI	Location to store the memory pool file.	The default value is **/opt/rsa/esa/pool/esperPool**. RSA recommends you do not modify the default value. If you modify this setting to use a different partition, ensure the partition contains at least 10 times more space than the memory allocated for ESA. **Caution:** If the memory pool is in use while this path is changed, an ESA restart is required. When this occurs, ESA does not discard the stored events so you must manually purge them.
MapPoolEnable	Enable or disable the memory pool.	The default value is **false**. Set the value to **true** to enable the memory pool. Requires a restart when you enable or disable memory pool.

MapPoolFlushIntervalSecs	Time interval to flush events to disk. For example, any event held in Esper longer than 15 minutes gets flushed to disk.	The default value is **15 minutes**. A smaller value ensures that the ESA is more stable when there are EPLs holding a large number of events in memory. A larger value (greater than 30 minutes), ensures that only relevant events required over a longer period of time are flushed to disk. **Note:** Due to Java memory management design, sometimes events not held by EPL may be sent to disk. To help prevent this from occurring, you can set a higher value for MapPoolFlushIntervalSecs.
MapPoolBatchWriteSize	Specify the batch size (and whether to use batch mode). The events are batched into groups and then flushed to disk. To use non-batch mode, set this value to 1. To use batch mode, set this value to greater than 1.	The default batch size is **100,000** events. At the end of flush interval, if the batch capacity is not reached, the batch expires in 30 seconds and all contents of the batch are written to disk as memory pool files. A smaller value for the batch size (for example, 10,000 events) ensures that when events are fetched from disk, they do not pose a risk of bloating the memory, which creates more stability. However, a larger batch size (100,000 events) minimizes the input/output activity when writing events to disk, which can create better performance.
MapPoolMinSize	Minimum size of the memory pool. This value is used for initialization, so it does not typically require editing.	The default value is **10,000** events. A higher value may increase performance. A lower value ensures that the system is more stable.

MapPool Persist Type	This is a view-only parameter that displays the type of optimization used.	The default value is **RMSerialize**.

Note: The effectiveness of this feature depends on your environment. If you write rules that require frequent access of events over a period of time, this feature may degrade performance with no or minimal improvement in scalability.

Memory pool files get deleted when all the events held in the pool file are no longer referenced by an EPL.

Result

For a simple EPL rule, ESA typically improves memory approximately 8 to 9 times.

Configure ESA to Use Capture Time Ordering

This procedure applies only to ESA Correlation Rules.

Administrators can configure the ESA to use capture time ordering when using two or more Concentrators as a source.

By default, ESA uses the ESA time stamp (time at which events are received by the ESA) to correlate events. However, ESA also supports session-ordering based on capture time (the time at which the packet or log event reached the Decoders). This feature is useful if you are correlating events from two or more Concentrators. When you have two or more Concentrators as sources, time ordering ensures that their sessions are correlated together by capture time. This ensures that sessions captured at the same time are correlated together and alerts are consistent with user's expectation even with transmission delays. If any of the sources go offline or are slow to send sessions, ESA will pause to ensure that sessions with same capture timestamps are correlated together.

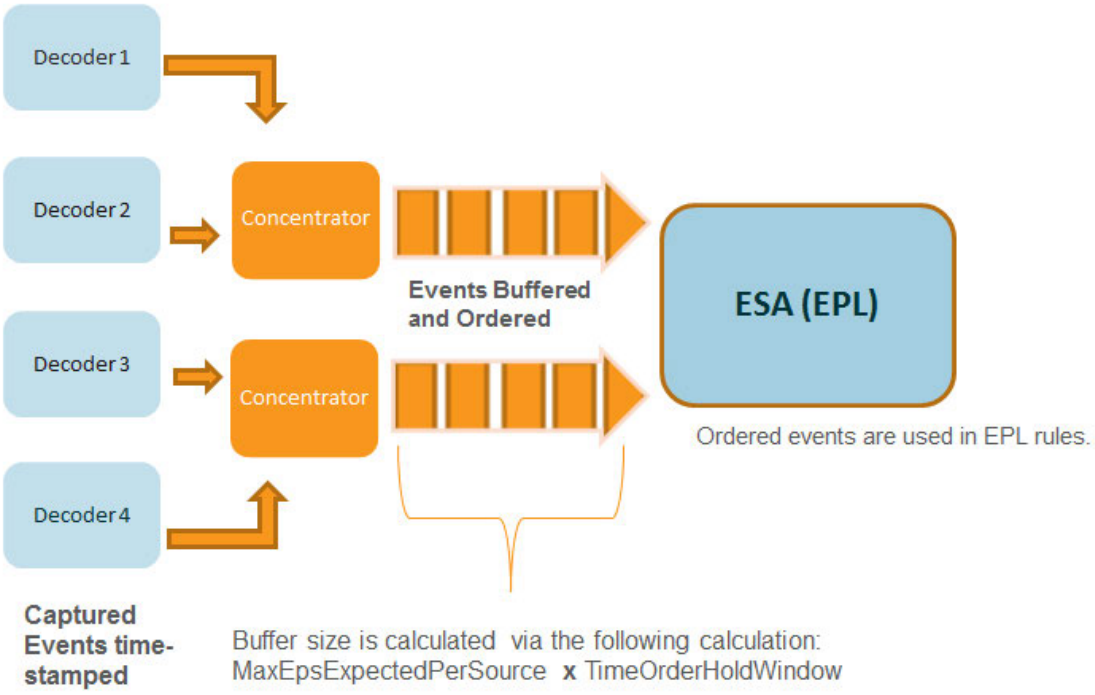
For example, you have two sources with events that occur at 10:00 a.m. Using Capture Time Ordering, these events are held in the buffer until the ESA detects that all events occurring at 10:00 a.m. have been added to the buffer. Once all the events have arrived, events are then processed using EPL rules. This ensures that a rule has all events with the same time-stamp from different sources in order to obtain correct results. If, for example, one Concentrator lags behind another, the ESA pauses until it has all the events time-stamped at 10:00 a.m. from both sources before it runs the EPL rules against the events.

Caution: Although this feature increases accuracy, it impacts performance. The default configuration of the ESA ensures that data is constantly streaming, but because Capture Time Ordering uses a buffer, it takes longer to process events. This is especially true if the ESA must pause for any length of time to wait for the buffer to fill. There are several parameters you can configure (see below) to handle this situation; however, there may still be performance impact.

By default, this feature is disabled.

Capture Time Order Workflow

The following diagram shows the workflow when Capture Time Ordering is enabled.



1. Events are time-stamped as they are captured by the Decoder.
2. After Concentrator processing, events are buffered and ordered. The buffer size is calculated via two parameters MaxEPSExpectedPerSource (the maximum volume of traffic (EPS) you expect **per source** for the ESA to receive) times TimeOrderHoldWindow (the amount of time to allow for events to arrive from all sources).
3. The ordered events are then correctly correlated in EPL rules.

Prerequisites

Two or more Concentrators must be configured as a data source in ESA.

When the **StreamEnabled** parameter is set to true, it is important that all the machines running Core Services should be in NTP Sync.

Procedures

The following procedures tell you how to enable and configure Capture Time Ordering.

Enable Buffering and Capture Time Ordering

Note: After an upgrade or in a high EPS environment, you need to re-add datasources to start seeing the benefits. Or, you must wait until the sessions catch up before you enable Capture Time Ordering.

1. Go to **ADMIN** > **Services**, select your ESA service, and then select > **View** > **Explore**.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the **StreamEnabled** attribute to **true**. StreamEnabled allows ESA to buffer events received from Concentrators.
4. Set the **TimeOrdered** attribute to **true**. This enables the buffered events to be ordered by the time stamp from the Concentrator.

Configure Capture Time Ordering

When you work with Capture Time Ordering, you need to configure several other parameters to ensure performance. The following table shows parameters and their function. Configuring these parameters requires knowledge of your traffic volume and rate.

Note: If you do not know your traffic volume or latency, consult with your Professional Services representative before configuring this feature.

MaxEPSExpectedPerSource	Specify the maximum volume of traffic (EPS, or events per second) you expect for the ESA service to receive from your busiest source (for example, if one source receives 20K EPS, and another receives 25K EPS, set the value at 25K EPS). If you set this rate too low, there is a short-term impact on performance. However, ESA automatically increases the value for `MaxEPSExpectedPerSource` as needed to make progress in Time Ordered mode. The default value is 20K.
TimeOrderHoldWindow	Specify in seconds (whole integers) the amount of time to allow for events to arrive from all sources. Configure this value based on the latency between the sources. The default value is 2 seconds. Decreasing this value can increase the chance of dropped events. Increasing this value can decrease performance because more memory is consumed.
IdleSourceAdvanceAfterSeconds	Specify the interval (in seconds) after which the ESA takes an idle source (no events are coming from the source, but the source is not offline) out of the equation to allow progress on a capture time ordered stream. The default value is 0, meaning that the ESA waits indefinitely for events to arrive.
OfflineSourceAdvanceAfterSeconds	Specify the interval (in seconds) after which the ESA takes an offline source out of the equation to allow progress on a capture time ordered stream. The default value is 0, which means the ESA waits indefinitely. This parameter does not affect the re-connection retries; those which are performed in all cases.

Troubleshooting Tips

Using this feature, it is possible to encounter a situation where events become backlogged. To fix this issue, you can perform one of the following options.

Disable Capture Time Ordering

1. Go to **ADMIN** > **Services**, select your ESA service, and then **> View > Explore**.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the StreamEnabled attribute to false.
4. Set the TimeOrdered attribute to false.

If you disable Capture Time Ordering, you will lose the backlogged data, and events will no longer be ordered by capture time.

Disable Position Tracking

Position tracking allows ESA to track where it stopped processing events if the ESA stops or is shut down. Position tracking is enabled by default with Capture Time Ordering. If you disable position tracking, this allows ESA to skip the backlogged events. For example, if the ESA goes down at 7:00 a.m., and you restart it at 11:00 a.m. with position tracking disabled, the ESA will start processing events that occurred at 10:55 a.m. With position tracking enabled, the ESA will start processing events at the point at which it stopped.

1. Go to **ADMIN** > **Services**, select your ESA service, and then select
   > **View** > **Explore**.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the **PositionTrackingEnabled** attribute to false.

If you disable Position Tracking, you will lose the backlogged data, but going forward, events will be ordered by capture time.

Start, Stop, or Restart ESA Service

This topic provides instructions to start, stop, or restart the Event Stream Analysis service. This procedure applies to ESA Correlation Rules.

Start ESA Service

Before you start:

- Make sure that MongoDB is running.
- If the MongoDB service is not running, use the following command to start the MongoDB service:

  ```
  systemctl start mongod
  ```

To start ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   systemctl start rsa-nw-esa-server
   ```

Stop ESA Service

To stop ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   systemctl stop rsa-nw-esa-server
   ```

Restart ESA Service

To restart ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   systemctl restart rsa-nw-esa-server
   ```

Audit Logs and Verify ESA Component Versions and Status

This topic provides details about audit logging and instructions to verify the versions of the Event Stream Analysis components installed. These procedures apply to ESA Correlation Rules.

Audit Log Rules

Audit logging allows you to view details about rules that are created and edited in NetWitness Suite.

For details on how to access your audit logs, see "Local Audit Log Locations" in the *System Configuration Guide*.

The following sample shows a create, update, and delete log for a given rule.

- **Create log example:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "CREATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true, Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR"`
- **Update log example:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "UPDATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR`
- **Delete log example:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS"category: SYSTEM operation: "DELETE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR "`

Each log contains the following parameters:

- Time stamp: Time the rule was modified. Example: 2016-03-10 14:19:37,951
- DeviceVersion: Version of your ESA device. Example: "10.6.1.0-SNAPSHOT"
- DeviceService: Example: EVENT_STREAM_ANALYSIS
- Category: Example: SYSTEM
- Operation:Example: DELETE/CREATE/UPDATE RULE
- Parameters: Placeholder for the following keys:
- Epl Module Identifier: unique identifier for the rule. Example: 56e1f2adbee8290008241296

- Esper Instance: Esper instance on which rule is deployed. Example: default
- Rule Enabled: Displays if the rule is enabled or not. Example: Rule Enabled: true
- Trial Rule: Displays if the rule is configured as a trial rule or not. Example: Trial Rule: false
- Epl Rule: Displays the rule syntax. Example:

  ```
  @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_
  ESA_ADMINISTRATOR+ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMIN"
  ```

- Identity: Example: “admin"
- userRole: Example: "ROLE_ESA_ADMINISTRATOR"

Note: When a rule is disabled, two logs are generated for the same rule. First a ‘Delete Rule’ [Rule enabled attribute = true] audit log is created, followed by a ‘Create Rule’ [Rule enabled attribute =false] audit log.

Verify ESA Server Version

To verify the ESA Server version:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   rpm -qa | grep rsa-nw-esa-server
   ```

   The ESA server version is displayed.

Verify MongoDB Version

To verify the MongoDB version:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   mongo --version
   ```

   The MongoDB version is displayed.

Verify MongoDB Status

To verify the MongoDB status:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   systemctl status mongod
   ```

3. Run the following command if MongoDB is not running.

   ```
   systemctl start mongod
   ```

References

This section is a collection of references, which describe the user interface for ESA Configuration in NetWitness Suite.

See the following topics for details:

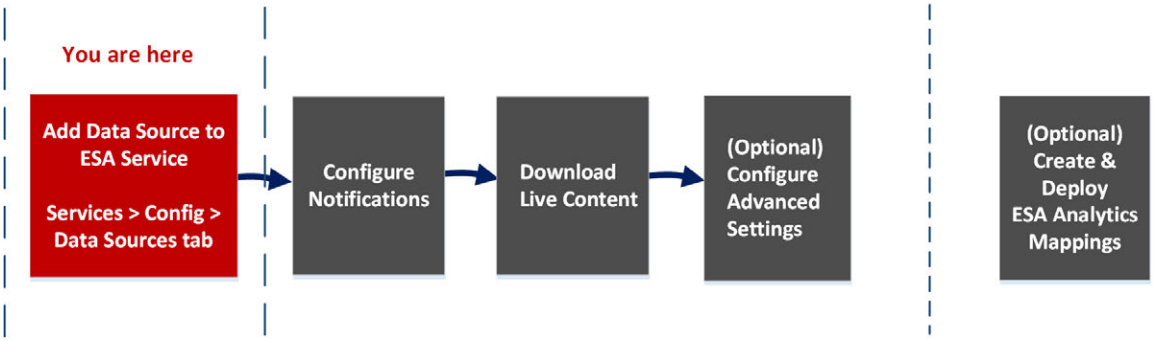
- Services Config View Advanced Tab
- Services Config View Data Sources Tab
- ESA Analytics Mappings
- Module Settings
- Whois Lookup Service Configuration

Services Config View Data Sources Tab

The **Services Config view > Data Sources** tab of an ESA service enables you to configure the sources that ESA uses to analyze data. An ESA service ingests data from Concentrators to detect incidents and alert analysts to potential threats.

Workflow

This workflow shows the overall process for configuring ESA. It also shows where configuring data sources is located in the process.



ESA has two services, the Event Stream Analysis service (ESA Correlation Rules) and the Event Stream Analytics Server service (ESA Analytics). The first four procedures shown pertain to configuring the Event Stream Analysis service:

- Add Data Source to ESA Service
- Configure Notifications
- Download Live Content
- (Optional) Configure Advanced Settings

The last procedure is separate from the others and pertains to creating mappings for the ESA Analytics services to start automatically detecting advanced threats:

- (Optional) Create and Deploy ESA Analytics Mappings

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a Concentrator as a data source to the Event Stream Analysis Service *	See Configure ESA Correlation Rules and Step 1. Add a Data Source to an ESA Service
Administrator	Configure Notifications	See "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide*.
Administrator	Download Live Content	See "Live Search View" in the *Live Resource Management Guide*.
Administrator	Configure Advanced Settings	Step 2. Configure Advanced Settings for an ESA Service

*You can complete these tasks here (that is in the Services Config view Data Sources tab).

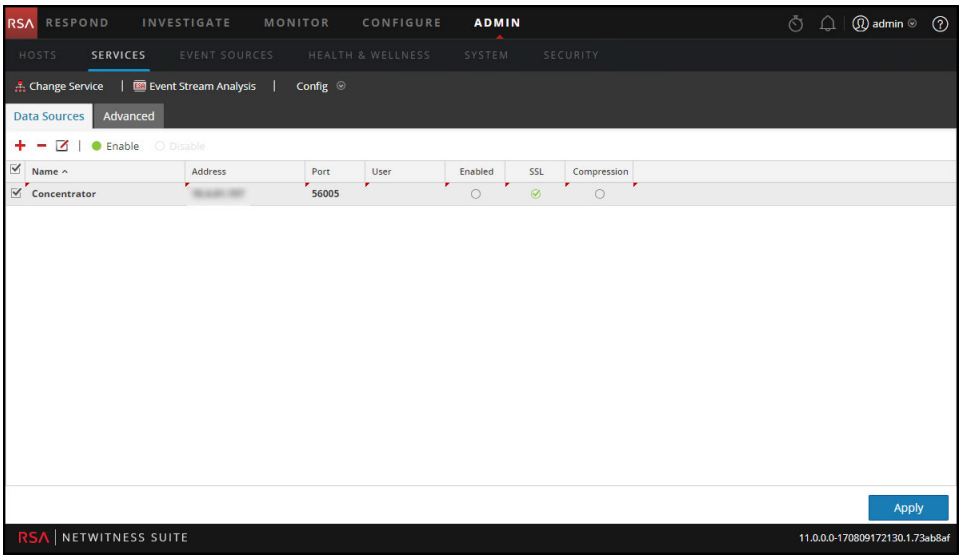
Related Topics

- See "Add or Update a Host" in the *Host and Services Getting Started Guide*

Quick Look

To access the Data Sources tab, go to **ADMIN** > **Services** > (Select an ESA service) > > **View** > **Config**.

The following figure shows the Services Config view Data Sources tab for an ESA service.



Toolbar

The following table describes the options in the toolbar.

Option	Description
+	Adds a new data source to the ESA service.
−	Deletes a data source from the ESA service.
✎	Edits a data source. You must have the username and password credentials for the service in order to make changes.
Enable	Enables the selected data source.
Disable	Disables the selected data source.

Data Sources

The Data Sources list shows all of the data sources added to the ESA service. The following table describes the columns the Data Sources list.

Column	Description
Name	The name of the data source service.

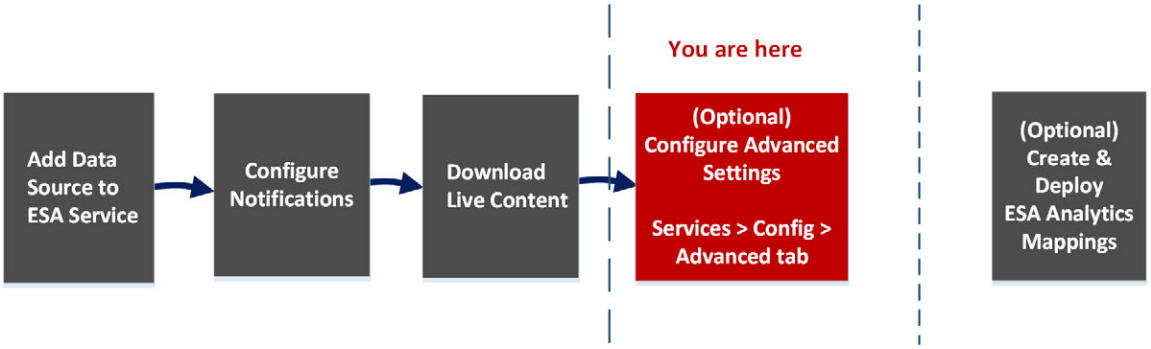
Column	Description
Address	The address of the data source service.
Port	The port used by the data source.
User	The user connected with the data source.
Enabled	Indicates if the data source is enabled.
SSL	Indicates if SSL communication is enabled.
Compression	Indicates if compression is enabled.

Services Config View Advanced Tab

The **Services Config view > Advanced** tab of an ESA service enables you to configure advanced settings. In the Advanced view, you can configure advanced settings to improve performance, to preserve events for rules with multiple events, to buffer events in memory, and to set the number of events to be stored on the ESA.

Workflow

This workflow shows the overall process for configuring ESA. It also shows where configuring advanced settings is located in the process.



ESA has two services, the Event Stream Analysis service (ESA Correlation Rules) and the Event Stream Analytics Server service (ESA Analytics). The first four procedures shown pertain to configuring the Event Stream Analysis service:

- Add Data Source to ESA Service
- Configure Notifications
- Download Live Content
- (Optional) Configure Advanced Settings

The last procedure is separate from the others and pertains to creating mappings for the ESA Analytics services to start automatically detecting advanced threats:

- (Optional) Create and Deploy ESA Analytics Mappings

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a Concentrator as a data source to the Event Stream Analysis Service	See Configure ESA Correlation Rules and Step 1. Add a Data Source to an ESA Service
Administrator	Configure Notifications	See "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide*.
Administrator	Download Live Content	See "Live Search View" in the *Live Resource Management Guide*.
Administrator	Configure Advanced Settings *	Step 2. Configure Advanced Settings for an ESA Service

*You can complete these tasks here (that is in the Services Config view Advanced tab).

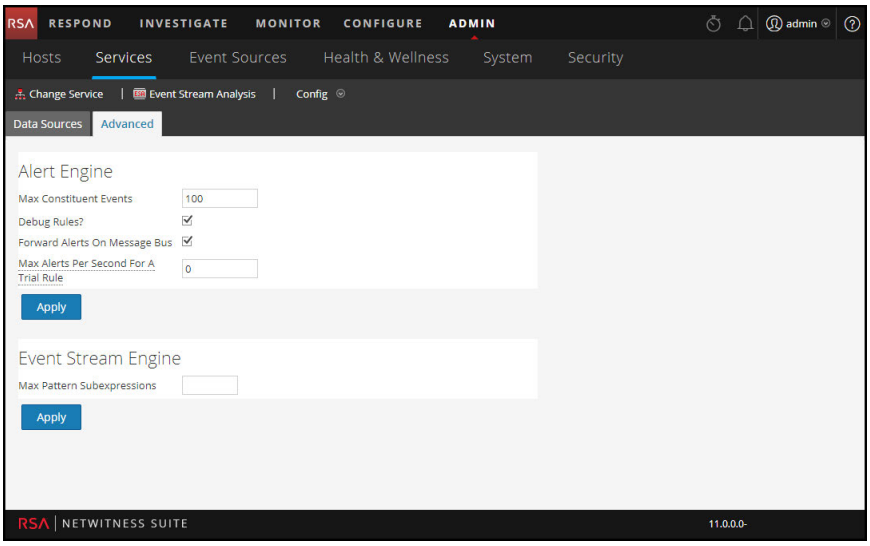
Related Topics

- See "Add or Update a Host" in the *Host and Services Getting Started Guide*

Quick Look

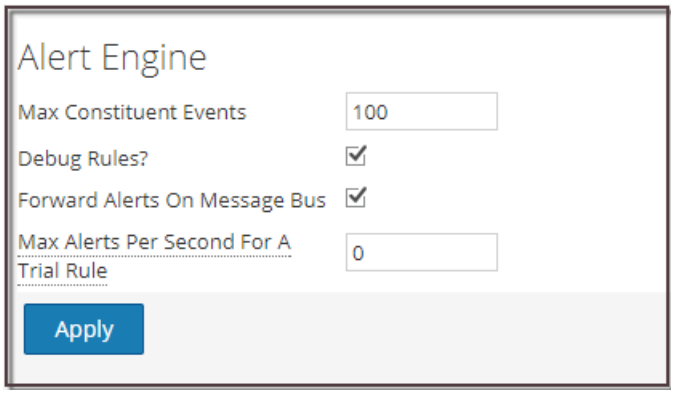
To access the Advanced tab, go to **ADMIN > Services >** (Select an ESA service) > > **View > Config**.

The following figure shows the Services Config view Advanced tab for an ESA service.



Alert Engine Settings

In the Alert Engine section, you specify values to preserve events for rules that choose multiple events. The following figure shows the Alert Engine section.



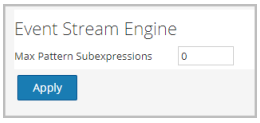
The following table lists the parameters in the Alert Engine section and their descriptions.

Parameter	Description
Max Constituent Events	For rules that choose multiple events, this configuration value decides how many of the associated events are preserved. For example, if a rule fires an alert with 200 associated events and this parameter is set to 100, only the first 100 are preserved by ESA, the rest are dropped. The default value is **100**.
Debug Rules?	Selecting enables debugging rules.

Parameter	Description
Forward Alerts On Message Bus	To forward ESA alerts for NetWitness Respond, you must select this option. The ESA alerts generated will be sent to the Message Bus and subsequently to Respond. This option is selected by default. You may want to ensure that the Respond Server service is running.
Max Alerts Per Second for a Trial Rule	You can specify the maximum number of alerts to be forwarded to the Message Bus for the trial rule. For example, if the value is set to **50**, only 50 alerts will be forwarded to the Message Bus for the trial rule. If the value is set to **0**, then the alerts generated by the trial rule will not be forwarded to the Message Bus. The default value is **10**.

Event Stream Engine Settings

In the Event Stream Engine section, you specify details to improve performance. The following figure shows the Event Stream Engine section.



The following table lists the parameter in the Event Stream Engine section and its description.

Parameter	Description
Max Pattern Subexpressions	Certain rules require ESPER to maintain subexpressions in memory before deciding to fire them or not. These subexpressions consume memory and if left unchecked may cause the service to go down with memory exhaustion. This parameter is a safety measure that keeps such memory hogging rules under check. If a rule exceeds the specified number of subexpressions, its processing is delayed. The default value is **0** which means this setting is disabled. You must set a value if there are service stability issues.

Whois Lookup Service Configuration

In the Whois Lookup Configuration panel (ADMIN > System > Whois), you configure a connection to the Whois Lookup service for your preconfigured ESA Analytics modules used in RSA Automated Threat Detection. The Whois Service enables you to get accurate data about domains that you connect to. In order to ensure effective scoring, it is important that you configure the Whois service settings.

You must have an RSA Live account to use this service.

If you configured a Live account in the Live Services panel (ADMIN > System > Live Services), the Whois Lookup Service is automatically configured for you. You just need to check the connection of the Whois Lookup service.

Note: If you do not have an RSA Live account, you can create one at the RSA Live Registration Portal:
https://cms.netwitness.com/registration/
The *Live Services Management Guide* provides additional information.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure the Whois Lookup service.	Configure the Whois Lookup Service
Administrator	Check the connection of the Whois Lookup service.	Configure the Whois Lookup Service

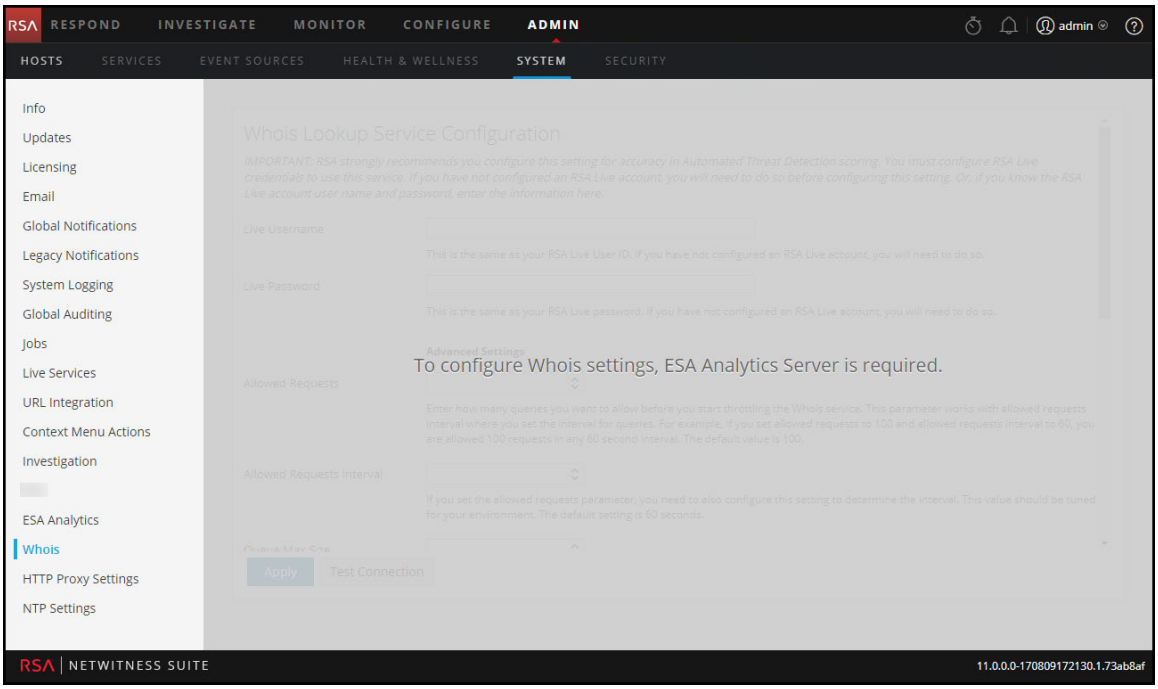
Related Topics

- ESA Analytics Mappings

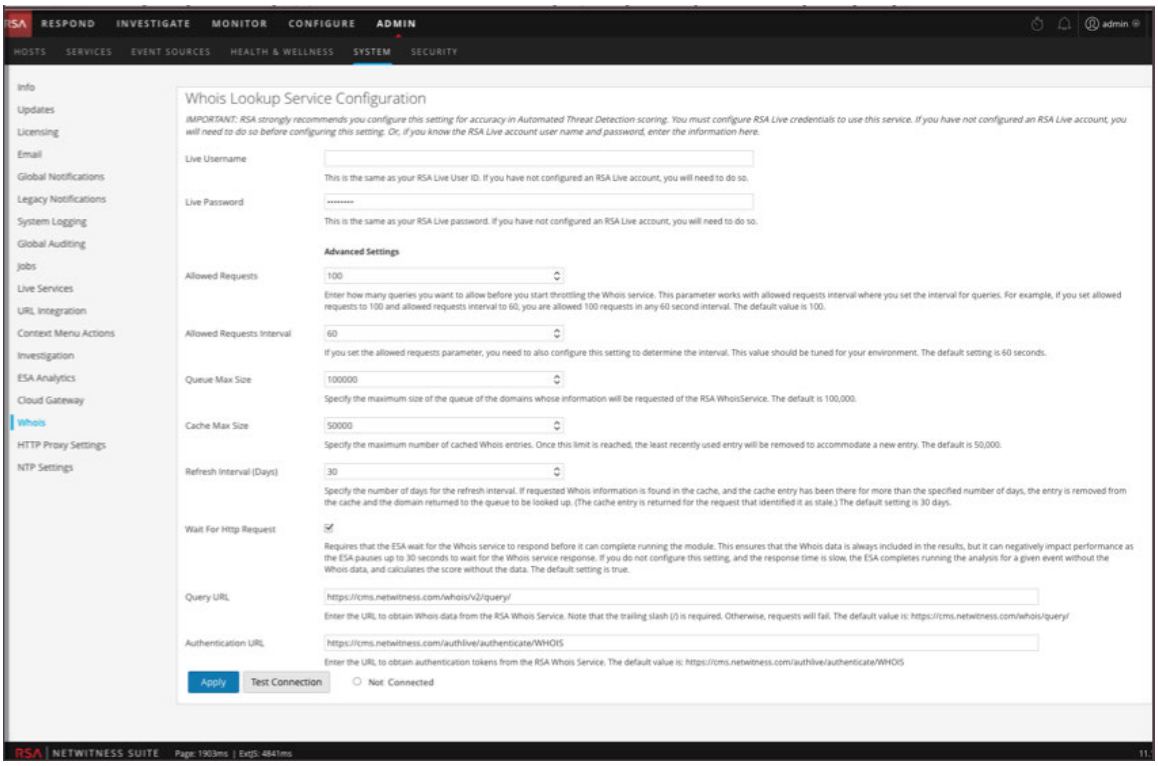
Whois Lookup Service Configuration

To access the Whois Lookup Service Configuration, go to ADMIN > System and in the options panel, select Whois.

The ESA Analytics Server service must be available (shows a green circle) in the ADMIN > Services view. If you do not have an ESA Analytics Server service available, you will see the following panel.



If you have an ESA Analytics Server service available, you will see the following panel.



The following table describes the listed Whois Lookup Service configuration settings.

Parameter	Description
Live Username	**Required only if you did not already configure the Whois Lookup service.** Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live User ID. If you have not configured an RSA Live account, you will need to do so. The default value is "whois."
Live Password	**Required only if you did already configure the Whois Lookup service.** Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live password. If you have not configured an RSA Live account, you will need to do so. The default value is null.
Allowed Requests	(Optional) Enter how many queries you want to allow before you start throttling the Whois service. This parameter works with **Allowed Requests Interval** (in seconds), where you set the interval for queries. For example, if you set **Allowed Requests** to 100 and **Allowed Requests Interval** to 60, you are allowed 100 requests in any 60 second interval. The default value is 100.

Parameter	Description
Allowed Requests Interval	(Optional) If you set the **Allowed Requests** parameter, you need to also configure this setting to determine the interval. This value should be tuned for your environment. The default setting is 60 seconds.
Queue Max Size	(Optional) Specify the maximum size of the queue of the domains whose information will be requested of the RSA WhoisService. The default is 100,000.
Cache Max Size	(Optional) Specify the maximum number of cached Whois entries. Once this limit is reached, the least recently used entry will be removed to accommodate a new entry. The default is 50,000.
Refresh Interval Days	(Optional) Specify the number of days for the refresh interval. If requested Whois information is found in the cache, and the cache entry has been there for more than the specified number of days, the entry is removed from the cache and the domain returned to the queue to be looked up. (The cache entry is returned for the request that identified it as stale.) The default setting is 30 days.
Wait For HTTP Request	(Optional) Requires that the ESA wait for the Whois service to respond before it can complete running the module. This ensures that the Whois data is always included in the results, but it can negatively impact performance as the ESA pauses up to 30 seconds to wait for the Whois service response. If you do not configure this setting, and the response time is slow, the ESA completes running the analysis for a given event without the Whois data, and calculates the score without the data. The default setting is **true**.
Query URL	(Optional) Enter the URL to obtain Whois data from the RSA Whois service. The trailing slash ('/') is required. Otherwise, requests will fail. The default value is: **https://cms.netwitness.com/whois/v2/query/**
Authentication URL	(Optional) Enter the URL to obtain authentication tokens from the RSA Whois service. The default value is: **https://cms.netwitness.com/authlive/authenticate/WHOIS**

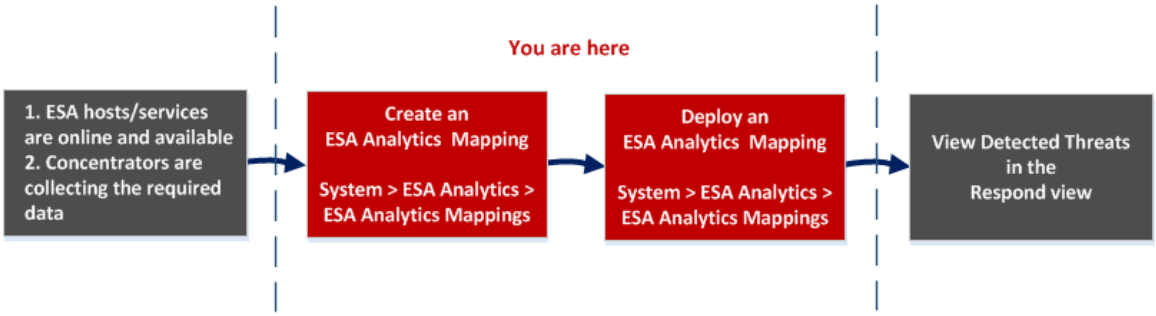
ESA Analytics Mappings

In the ESA Analytics Mappings panel (ADMIN > System > ESA Analytics), you define how the RSA Automated Threat Detection functionality should automatically detect advanced threats. You can analyze the data that resides on one or more Concentrators by selecting a preconfigured ESA Analytics module.

To better utilize your network resources and reduce unnecessary data flow, you can map multiple data sources, such as Concentrators, to available ESA Analytics services in order to process data more efficiently and take advantage of additional capacity.

Workflow

This workflow shows the process for creating and enabling an ESA Analytics mapping to start automatically detecting advanced threats.



Before you create an ESA Analytics mapping, ensure that the ESA hosts and services that you want to use for your mappings are online and available. All of the services need to be in sync with a consistent time source. Also ensure that the Concentrators are collecting the required data. When you create an ESA Analytics mapping, you select an ESA Analytics module to map, such as Suspicious Domains. Then you select the data sources, such as Concentrators, to use for that module along with an ESA Analytics service to process the data. When you are ready to start aggregating data, you deploy the mapping. Analysts can view detected threats for that module in the Respond view.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Verify that the ESA hosts and services are online and available.	ADMIN > HOSTS and ADMIN > SERVICES See *Hosts and Services Getting Started Guide*.
Administrator	Ensure that the Concentrators are collecting the required data.	See *Broker and Concentrator Configuration Guide*
Administrator	Create ESA Analytics mappings*	Mapping ESA Data Sources to Analytics Modules
Administrator	Deploy ESA Analytics mappings*	Mapping ESA Data Sources to Analytics Modules
Administrator, Analyst	View detected threats	See *NetWitness Respond User Guide*.

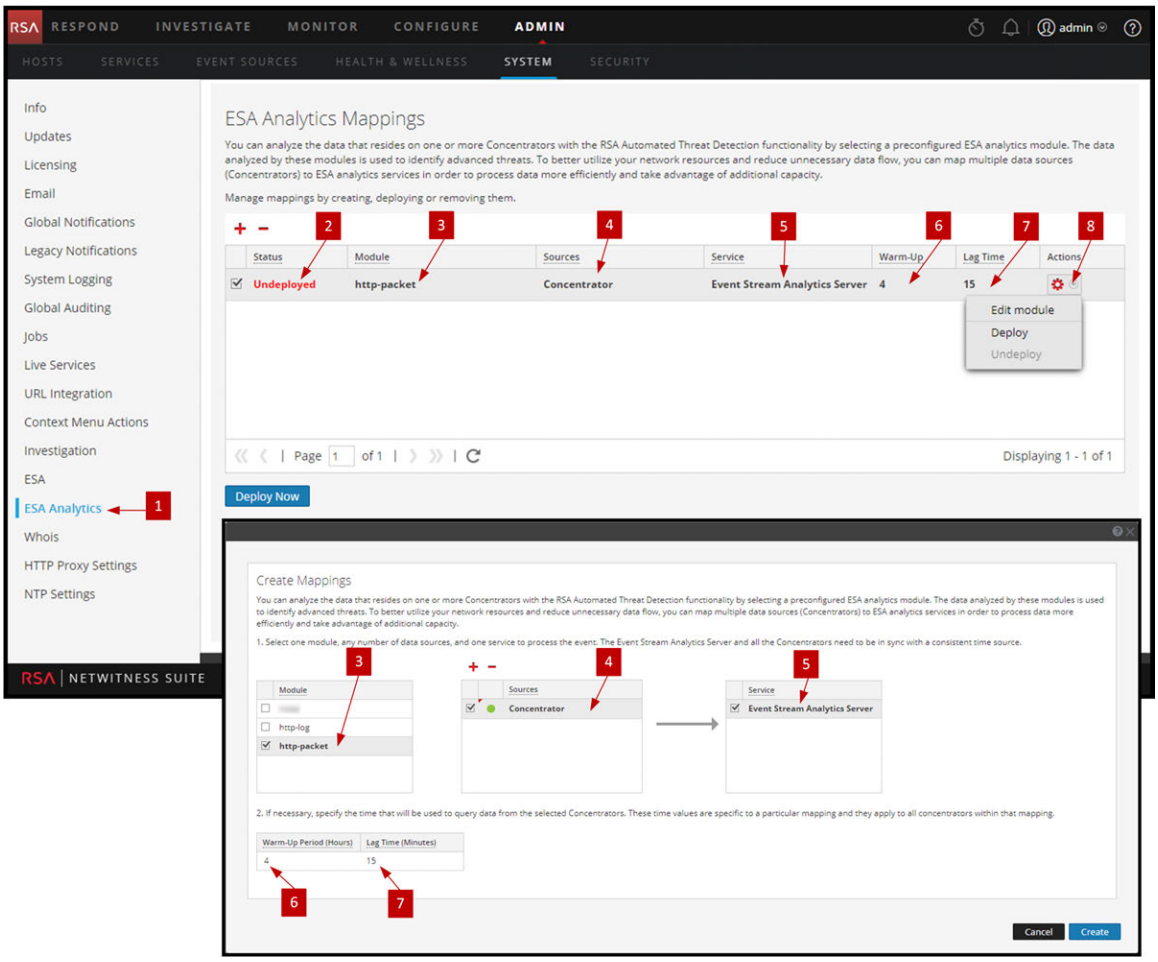
*You can complete these tasks here (that is in the ESA Analytics Mappings panel).

Related Topics

- Configure ESA Analytics
- Update a Mapping
- Undeploy a Mapping
- Delete a Mapping
- Change the Warm-up Period and Lag Time
- Module Settings

Quick Look

The following example illustrates an ESA Analytics mapping. The configuration defines the data sources for the selected module and the ESA Analytics service that will process the events from those data sources.



1	Displays the ESA Analytics Mappings panel.
2	Shows the status of the ESA Analytics mapping.
3	The name of the module that is mapped.
4	Data sources, such as Concentrators, assigned to the mapping.
5	ESA Analytics service that processes the data for the mapping.
6	Warm-up period configuration (in hours) on the data sources for the mapping.
7	Lag configuration (in minutes) on the data sources for the mapping.
8	Actions for changing module settings, deploying module mappings, and undeploying module mappings.

Toolbar

The following table describes the toolbar actions.

Icon / Button	Description
+	Opens the Create Mappings dialog where you can create an ESA Analytics mapping. Create a separate mapping for each module. After creating and reviewing the mappings, you deploy them.
−	Deletes an ESA Analytics Mapping. • You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not deployed and is not running, it does not affect data aggregation. • Deleting a deployed mapping clears the configuration on the ESA server, reverts the deployment for that mapping, and stops pulling data from the data source for that module. You should undeploy a mapping with a status of Deployed before deleting it.
Deploy Now	After you create your mappings, you need to deploy them in order to start aggregating data for the modules. You can select one or more mappings with a status of Undeployed to deploy.

Note: If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that module.

ESA Analytics Mappings

The following table describes the listed ESA Analytics mappings.

Title	Description
☑	To select an individual mapping, select the checkbox next to the mapping.
Status	Shows the status of the mapping. There are two statuses: **Undeployed** - An undeployed mapping maps an ESA Analytics module to sources and an ESA Analytics service. It does not start aggregating data for the module until you deploy the mapping. **Deployed** - A deployed mapping is deployed and running. In a deployed mapping, the selected ESA Analytics service uses query-based aggregation to collect the appropriate filtered events for the selected module from the Concentrators.

Title	Description
Module	Indicates the selected ESA Analytics module. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. The module resides within the ESA Analytics service.
Sources	Sources are the data sources, such as Concentrators, from which ESA will aggregate the data for the specified module.
Service	Indicates the ESA Analytics service that will process the data for the specified module. The selected service needs to be in sync with a consistent time source.
Warm-Up Period (Hours)	Specifies a warm-up duration (in hours). A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. For more information about Warm-up Period and Lag time, see Module Settings.

Title	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. For more information about Warm-up Period and Lag time, see Module Settings.
	Enables you to select additional actions for the selected module mapping: • **Edit Module** - Enables you to configure the warm-up period and lag time for the selected module mapping. • **Deploy** - Deploys the selected module mapping. The specified ESA Analytics service starts pulling data from the data sources for that module. • **Undeploy** - Undeploys the selected module mapping. The specified ESA Analytics service stops pulling data from the data sources for that module. **Caution:** Undeploying a mapping with a status of Deployed will affect data aggregation for that module.

Module Settings

After you create or deploy a module mapping in the ESA Analytics Mappings panel (ADMIN > System > ESA Analytics), you have the option to change some module configurations for that mapping.

What do you want to do?

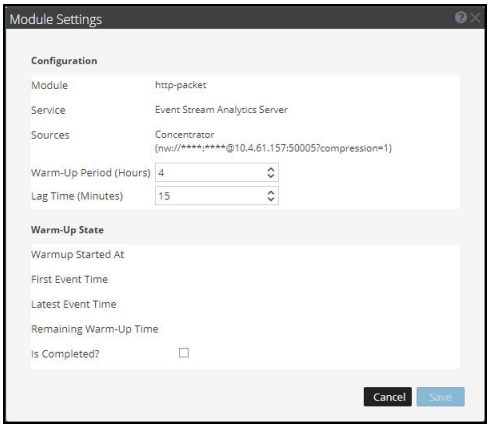
Role	I want to ...	Show me how
Administrator	Change the warm-up period for an undeployed module mapping.	Change the Warm-up Period and Lag Time
Administrator	Change the warm-up period for a module mapping during the warm-up period.	Change the Warm-up Period and Lag Time
Administrator	Change the warm-up period for a module mapping after the warm-up period is complete.	Change the Warm-up Period and Lag Time

Related Topics

- Mapping ESA Data Sources to Analytics Modules
- ESA Analytics Mappings

Module Settings

To access the module settings, in the ESA Analytics Mappings panel, select the mapping that you want to change and in the **Actions** column, select > **Edit Module**. The Module Settings dialog has a Configurations section and a Warm-Up State section.



Configurations

The Configurations section enables you to change the Warm-Up Period and Lag Time configurations.

The following table describes the settings available for an ESA Analytics module mapping.

Field	Description
Module	Shows the name of the mapped module.
Service	Shows the ESA Analytics service that processes the data for the mapping.
Sources	Shows the mapped data sources and the URLs used to communicate with ESA.
Warm-Up Period (Hours)	Specifies a warm-up duration in hours. A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. You can update the Warm-Up Period of a deployed module mapping depending on whether or not the warm-up period is complete: • **During the warm up period** - You can add hours to the warm-up period or subtract any remaining warm-up time. • **The warm-up period is complete** - You can add hours to the warm-up period by adding the difference between the current time and the First Event Time to the hours that you want to add. For example, a warm-up period of 10 hours is complete and the First Event Time shows 12:00:00. The current (system) time is 16:00:00 (4 hours later) and you want to add 5 more hours to the warm-up time. To do this, you need to add 9 hours (4+5=9) to the warm-up period of 10, so you would set the new warm-up period to 19 hours. You cannot decrease the warm-up period if it is complete, unless you delete the mapping and create a new one. The Warm-up Period value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two modules with different warm-up times, the Concentrator uses separate Warm-up Period values for each module mapping.

Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. When you specify a Lag time, the first time the module deploys, data aggregation starts at **Current (System) Time - Lag Time - Warm-Up Time**. For example, if the current time is 2:00 PM, Lag time is 30 minutes, and Warm-up time is 4 hours, when the module deploys for the first time, data collection starts at 9:30 AM (2:00 PM - .5 hour - 4 hours). After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. The Lag time value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two modules with different Lag times, the Concentrator uses separate Lag values for each module mapping. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. To determine the correct Lag Time, add together the following to get an environmental lag time: 1. **Log or Packet Latency** - This is the time it takes for the Log Decoder to receive the logs or the (Packet) Decoder to receive packets. For example, the Log Decoder may get logs every 20 minutes. In this case, you would want to set Lag time to at least 20 minutes, preferably 25 minutes, so that you do not miss events. 2. **Aggregation Latency** - This is the time it takes to get the data from the Log

Field	Description
	Decoder to the Concentrator. 3. **Other Buffer** - Add in any additional time delay specific to your environment.

Warm-Up State

The Warm-Up State section provides information about the warm-up state, which you can use to determine the appropriate adjustments to the warm-up period.

Field	Description
Warmup Started At	The time when the first event was processed by the ESA Analytics module from the data source.
First Event Time	The time that the first event occurred. The warm-up time is based on this time.
Latest Event Time	The time that the latest event occurred.
Remaining Warm-Up Time	The number of hours remaining in the warm-up period.
Is Completed?	Indicates whether the warm-up period is complete. If it is true, the warm-up period is complete. If it is false, the module is still warming up and you can view the number of hours remaining in the Remaining Warm Up Time field.

RSA NETWITNESS® SUITE

Endpoint Insights Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Endpoint Insights Overview 7

Endpoint Server Configuration 9

Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents 11

Configuring Metadata Forwarding 11

Starting Metadata Forwarding to the Log Decoder 13

Stopping Metadata Forwarding to the Log Decoder 13

Removing Metadata Forwarding 13

Configure Scan Schedule 14

Configure Data Retention Policy 16

Manage Inactive Agents 18

Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1 20

Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server (for Option 1) 20

Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2 (for Option 1) 24

Enabling the NetWitness Endpoint 4.4.0.2 Meta Forwarding to the Log Decoder (for Option 2) 24

Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server (for Option 1 and 2) 24

Endpoint References 27

General Tab 28

Workflow 28

What do you want to do? 28

Quick Look 29

Data Retention Scheduler Tab 31

Workflow 31

What do you want to do? 31
Quick Look 32
Scan Schedule Tab 34
Workflow 34
What do you want to do? 34
Quick Look 34
Packager Tab 35
What do you want to do? 36
Troubleshooting 37
Agent Communication Issues 37
Packager Issues 37
Scan Schedule Issues 38
Health and Wellness Issues 38
Meta Data Configuration Issue 41
Installation Issue 41
Finding Inactive Agents Issue 42

NetWitness Endpoint Insights Overview

Note: The information in this guide applies to Version 11.1 and later.

RSA NetWitness Endpoint collects endpoint data from Windows, Mac, or Linux hosts, which can be used to investigate, report, alert, and perform analysis. Analysts can perform instant scans for detailed insights of the host behavior at any point in time. In addition, Endpoint can collect logs from Windows hosts. The NetWitness Endpoint Insights introduces two host types - Endpoint Hybrid and Endpoint Log Hybrid. You can only install one instance of the host type in your deployment. This means, you can deploy either one instance of Endpoint Hybrid or Endpoint Log Hybrid. You cannot change the type once deployed.

Endpoint Hybrid - collects and manages endpoint (host) data. It generates metadata for investigation, analysis, alerting, and reporting. It is configured and managed similar to a Log or Packet Decoder. The Endpoint Hybrid runs an Nginx server (in a reverse proxy mode) that receives data from the Endpoint agent. The following services run on the Endpoint Hybrid:

- Endpoint Server - Manages data received through Nginx, stores it in the Mongo database, and sends metadata to the Log Decoder.
- Log Decoder - Captures data from the Endpoint Server and processes the metadata.
- Concentrator - Aggregates metadata from the Log Decoder and makes it available for all upstream components like Investigate, Reporting Engine, and Event Stream Analysis similar to other NetWitness Decoder and Concentrator setup.

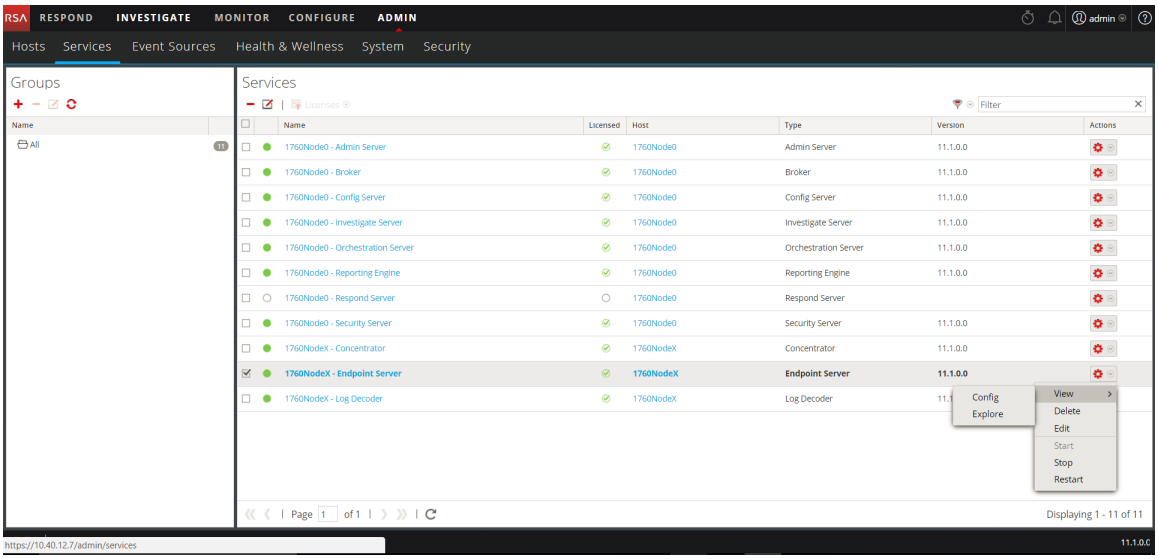
Endpoint Log Hybrid - captures both endpoint and log data. In addition to the services running on the Endpoint Hybrid, a Log Collector service runs on the Endpoint Log Hybrid. It collects logs from Windows hosts, and all other event sources that are supported for the Log collection in the NetWitness Suite.

The *Hosts and Services Getting Started Guide* provides the information you need to understand and install all the NetWitness Suite services.

Basic configuration involves:

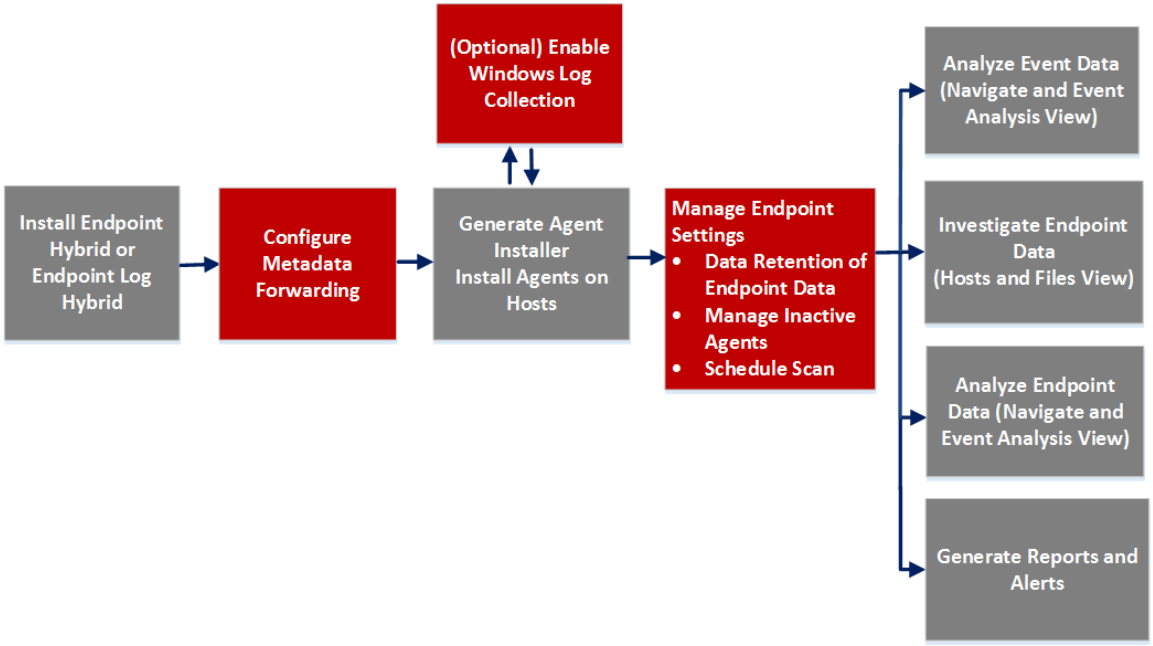
- Installing agents on hosts
- Configuring Endpoint meta forwarding, schedule scan, and retention policies
- Defining health and wellness policies to monitor Endpoint Server.

You can configure the required settings using the options in the NetWitness Suite user interface under Administration Services Config view (**ADMIN > Services > Endpoint Server > Config**).


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Groups
Name
All
11
Services
Filter
Name
Licensed
Host
Type
Version
Actions
1760Node0 - Admin Server
1760Node0
Admin Server
11.1.0.0
1760Node0 - Broker
1760Node0
Broker
11.1.0.0
1760Node0 - Config Server
1760Node0
Config Server
11.1.0.0
1760Node0 - Investigate Server
1760Node0
Investigate Server
11.1.0.0
1760Node0 - Orchestration Server
1760Node0
Orchestration Server
11.1.0.0
1760Node0 - Reporting Engine
1760Node0
Reporting Engine
11.1.0.0
1760Node0 - Respond Server
1760Node0
Respond Server
1760Node0 - Security Server
1760Node0
Security Server
11.1.0.0
1760NodeX - Concentrator
1760NodeX
Concentrator
11.1.0.0
1760NodeX - Endpoint Server
1760NodeX
Endpoint Server
11.1.0.0
1760NodeX - Log Decoder
1760NodeX
Log Decoder
Config
Explore
View
Delete
Edit
Start
Stop
Restart
Page 1 of 1
Displaying 1 - 11 of 11
https://10.40.12.7/admin/services
11.1.0.0

Endpoint Server Configuration

This topic provides the high-level tasks required to configure the Endpoint Server service.



Tasks	Description
Install the Endpoint Hybrid or Endpoint Log Hybrid	See *Physical Host Installation Guide* and *Virtual Host Setup Guide*.
Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents	Similar to Logs and Packets, you can view Endpoint metadata in the Navigate and Event Analysis view. You can also generate reports and alerts for the Endpoint data. By default, the Endpoint Meta option is disabled. The agent must be installed with the Endpoint Meta option enabled to forward metadata.

Tasks	Description
Install Agents on Hosts	The Endpoint agent installer is generated using the Packager tab under **ADMIN > Services > Config > Endpoint Server** from the NetWitness Suite user interface. The Packager is a zip file that contains executables and configuration files for generating agent installer for Linux, Mac, and Windows operating systems. You can install only one version of the agent on a host. If you have a previous version of an agent installed (for example, 4.4), uninstall this agent to install the 11.1 agent. After the agent is installed, it appears on the **Investigate > Hosts** view. By default, the Endpoint data is posted for the first time. To collect subsequent Endpoint data, you have to either schedule a scan or perform ad hoc scan. It retrieves data, such as drivers, processes, DLLs, files (executables), services, autoruns, security information, system configurations, and scripts found on the host. If the agent is configured for Log collection, it collects logs from Windows hosts, and forwards them to a Log Decoder or Remote Log Collector. For more information on Endpoint agent installation, see *Endpoint Insights Agent Installation Guide* .
Investigate Endpoint data	You can investigate the Endpoint data in the **Investigate > Hosts** and **Investigate > Files** views. For more information, see *Investigate User Guide*.
Configure Scan Schedule	Schedule a scan either to run daily or weekly.
Configure Data Retention Policy	Define data retention policies to optimally store and manage the Endpoint data based on the age of the Endpoint data or the storage size. By default, 30 days of agent data is retained.
Manage Inactive Agents	By default, agents (including all the collected Endpoint data) that have not communicated with the Endpoint Server for 90 days will be automatically deleted.

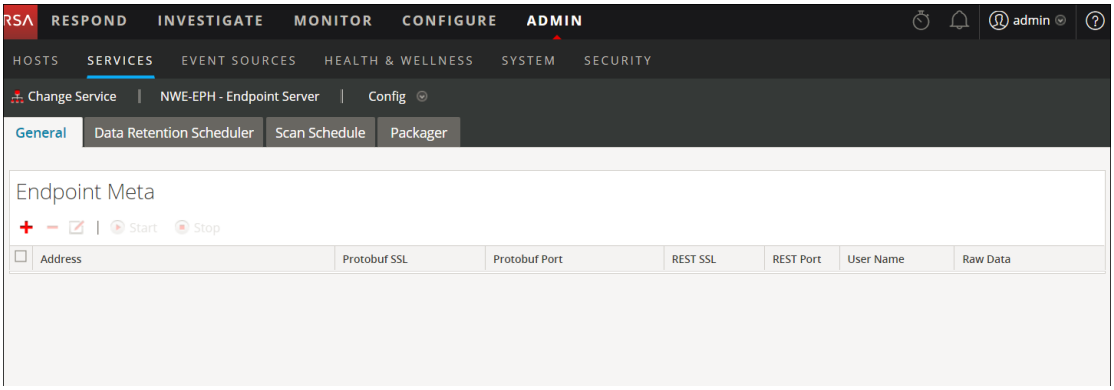
Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents

You can view the Endpoint metadata in the NetWitness Suite Investigate (**Navigate** and **Event Analysis** views) similar to Logs and Packets. You must enable the metadata forwarding to forward the following categories:

Operating System	Categories
Windows	File, Service, DLL, Process, Task, Autorun, and Machine
Linux	File, Loaded Library, Systemd, Process, Cron, Initd, and Machine
Mac	File, Daemon, Process, Task, Dylib, Autorun, and Machine

Configuring Metadata Forwarding

1. Go to **ADMIN** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click and select > **View** > **Config**.
4. Click the **General** tab.

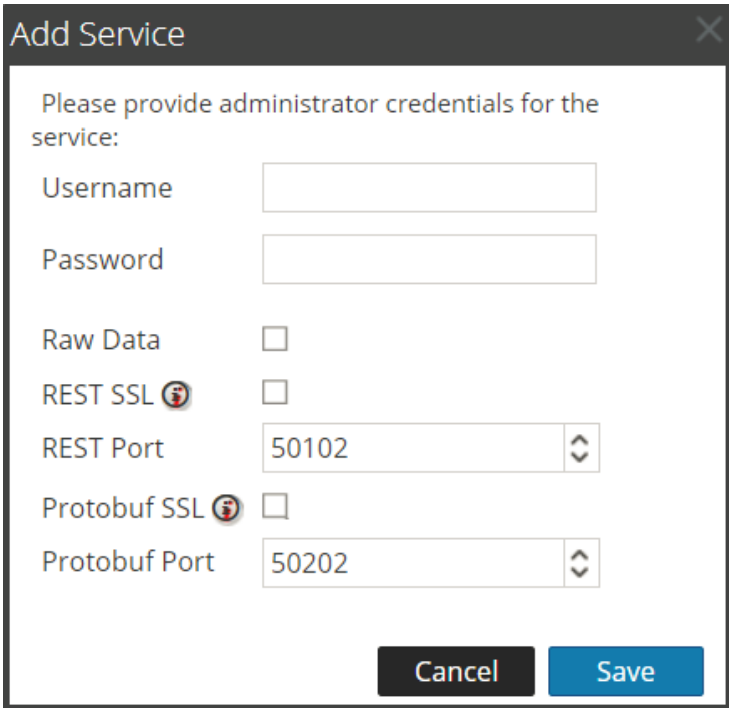


5. Click in the toolbar.

   The Available Services dialog is displayed.

6. Select the Log Decoder service and click **OK**.

   The Add Service dialog is displayed. You can add only one Log Decoder service.



7. Enter the administrator credentials for authentication.
8. (Optional) If you enable Raw Data, a brief summary of the session along with the metadata is sent.
9. (Optional) If you have enabled SSL on the REST port in the Log Decoder, select the **REST SSL** option. By default, the REST port for non-SSL is 50202 and for SSL is 56202.
10. Select the **Protobuf SSL** option to enable SSL on Protobuf. By default, the Protobuf port is 50202.
11. Click **Save**.

After configuring the meta forwarding, make sure to:

- Start the capture on the Log Decoder
- Start the aggregation on the Concentrator
- Add the Log Decoder as a service in the **Concentrator**

Starting Metadata Forwarding to the Log Decoder

1. In the Endpoint Meta config view, select the service.
2. Click

   The Endpoint Server starts forwarding the metadata to the Log Decoder.

Stopping Metadata Forwarding to the Log Decoder

1. In the Endpoint Meta config view, select the service.
2. Click

   The Endpoint Server stops forwarding the metadata to the Log Decoder.

Removing Metadata Forwarding

Note: Make sure you stop the service, before removing the metadata forwarding.

1. In the Endpoint Meta config view, select the service.
2. Click .
3. Click **Apply**.

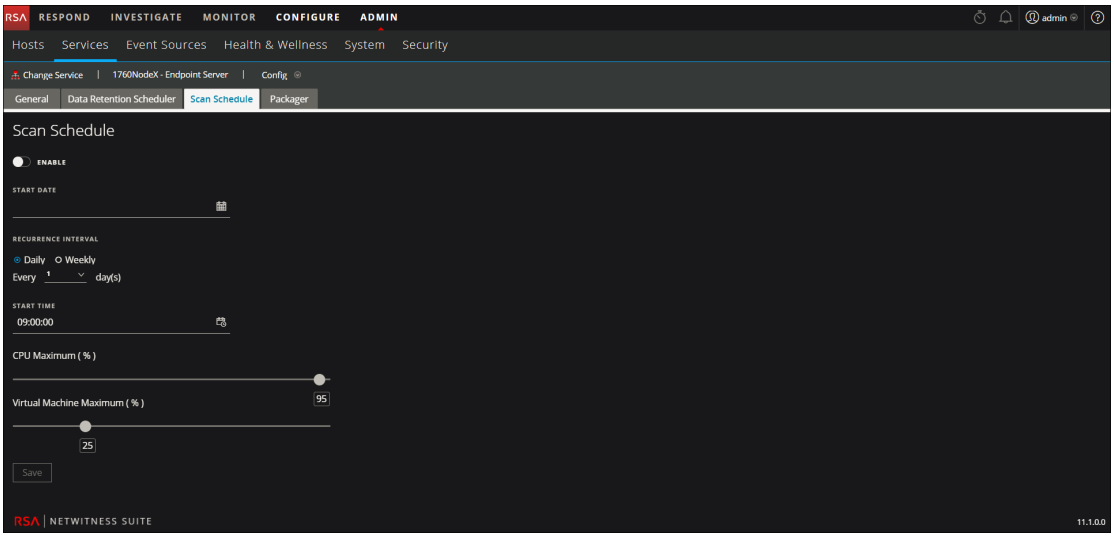
Configure Scan Schedule

You can schedule a scan to run daily or weekly.

Note: Only one schedule can be configured and is applicable to all the agents.

To configure a scan schedule:

1. Go to **Admin** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click and select > **View** > **Config**.
4. Click the **Scan Schedule** tab.



5. Click the **Enable** toggle switch to configure the scan.
6. Select the **Start Date**.
7. Select the recurrence interval - Daily or Weekly.

Note: The values entered are specific to the agent time zone.

8. For a daily scan:
   - Select recurrence interval as **Daily**.
   - Specify the frequency of scan in days.

9. For a weekly scan:
   - Select recurrence interval as **Weekly**.
   - Specify the frequency of scan in weeks.
   - Select the day of the week.
10. Enter the start time of the scan.
11. Set the CPU Maximum value using the slider. This ensures the CPU limit of the NetWitness Endpoint Agent. If the agents are running on the virtual machines, set the Virtual Machine Maximum value using the slider.
12. Click **Save** to save the configuration.

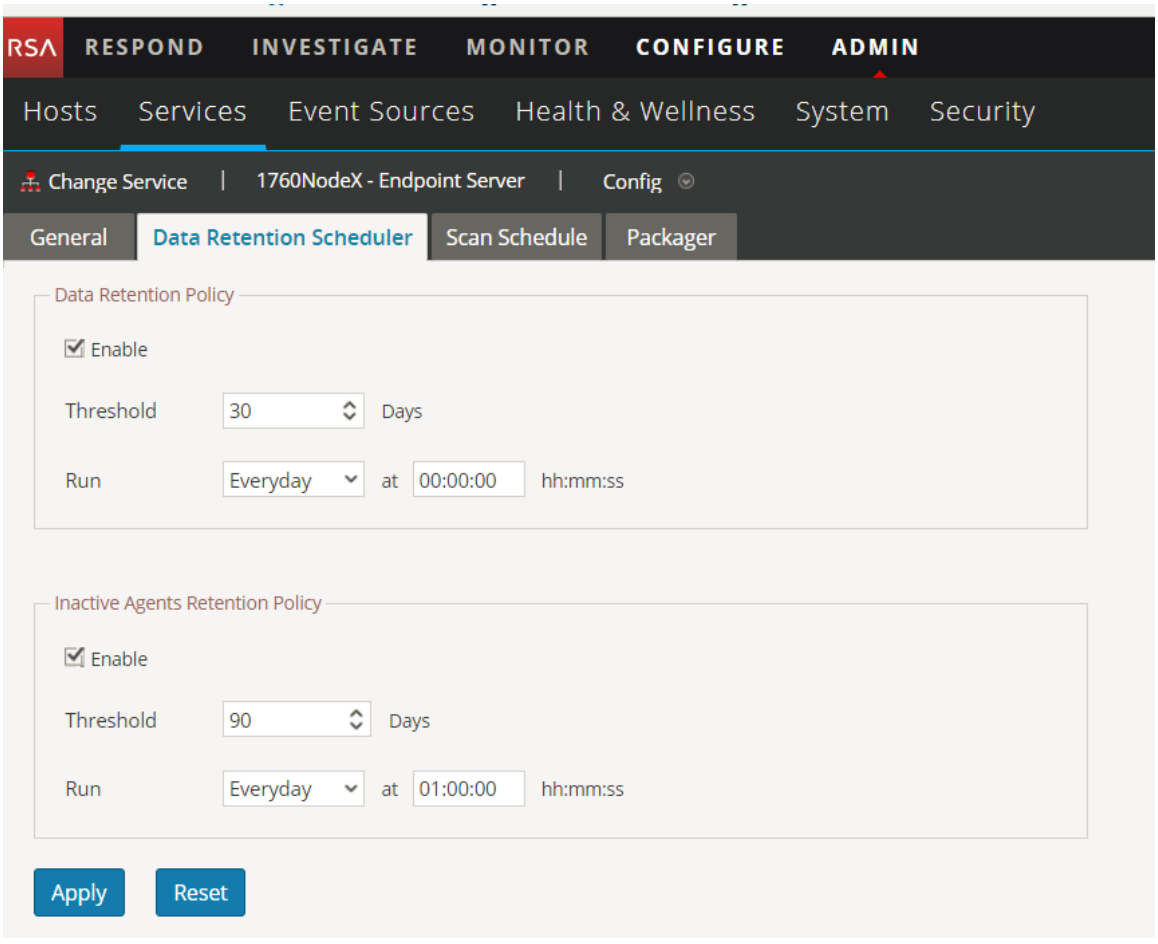
Note: If an agent is not able to perform the scan at the scheduled time because the machine is powered off or agent service is stopped, the next scan is based on the time difference between the current time and the next scheduled scan time.
For example, if a scan is scheduled to run every Wednesday at 6 PM and the agent service has stopped before the scan start time, and if the service is up on Thursday 10 AM, the agent will wait for the system to be fully up and running and immediately run a scan.
But if the service is up on the following Monday at 1 PM, the scan will run on the following Wednesday at 6 PM.

Configure Data Retention Policy

An administrator can configure the retention policies to retain the Endpoint data based on the age or the storage size. By default, days and size-based retention policies are enabled.

To change the configuration for age-based retention:

1. Go to **Admin**> **Services**
2. In the Services view, select the **Endpoint Server** service.
3. Click and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.

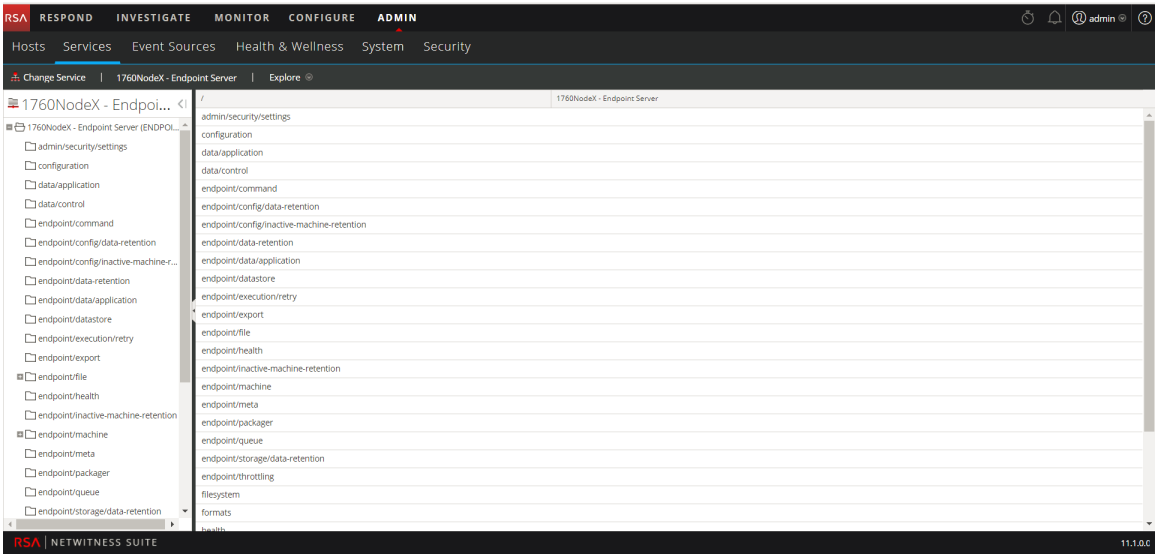


5. In the **Data Retention Policy** panel, by default, the **Threshold** is set to 30 days, and **Run** to Everyday. This means only 30 days of Endpoint data is retained and the older data is deleted from the database.
6. Click **Apply**.

To change the configuration for size-based retention:

By default, for the size-based retention, the `rollover-after` value is set to 80 and `rollover-chunk-size` is set to 10. This means that when the storage size exceeds 80 percent of the space allocated for the disk partition, 10 percent of the older Endpoint data is deleted from the database. However, you can change these values as follows:

1. In the main menu, go to **Admin** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click and select > **View** > **Explore**. The Explore view is displayed:



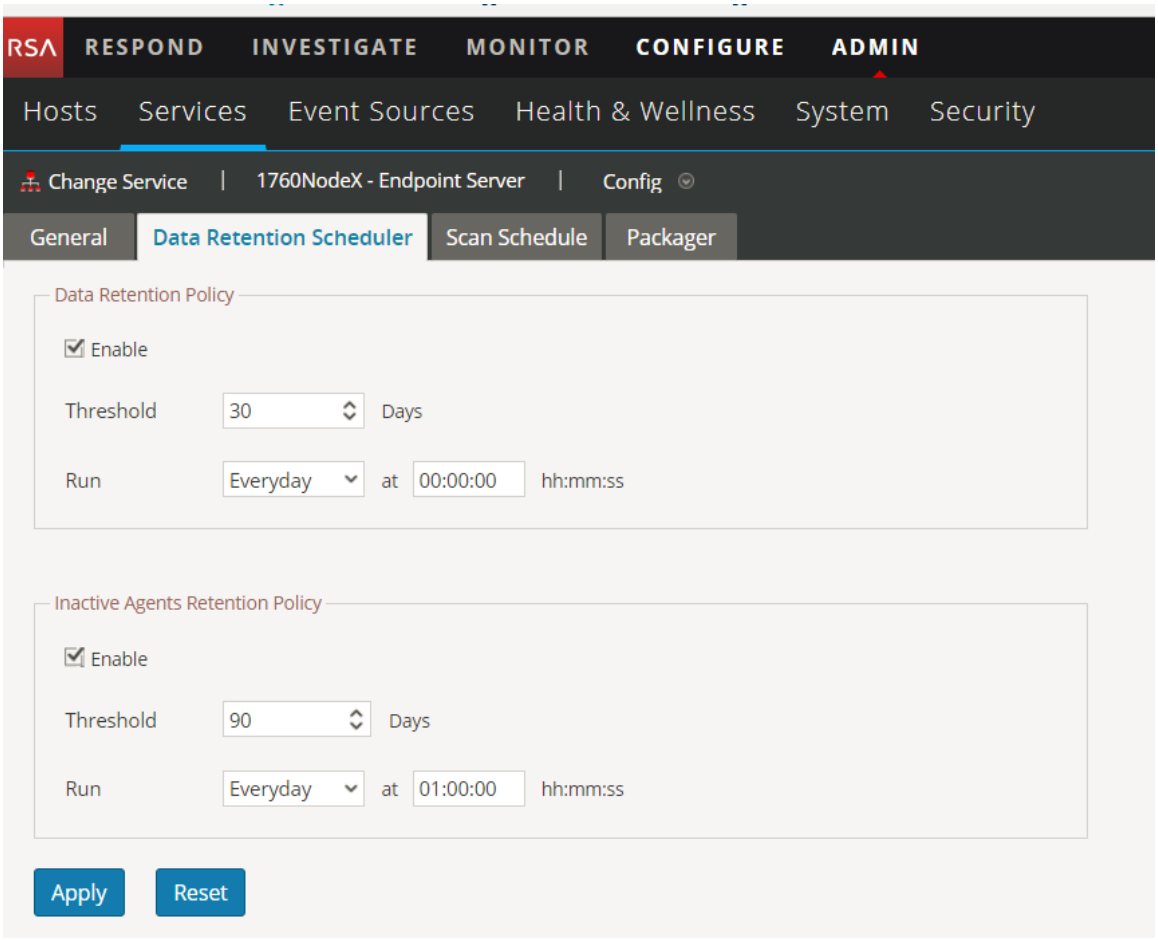
4. In the left panel, select **endpoint/config/data-retention**.
5. Edit the configurations based on your requirements.

Manage Inactive Agents

An administrator can configure the inactive agent retention policy to delete data of agents that are inactive, from the Endpoint Server. On deletion, the Endpoint Server stops collecting data from these agents. By default, this option is enabled.

To configure the inactive agent retention policy:

1. Go to **Admin** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.



5. In the **Inactive Agents Retention Policy** panel, by default, the **Threshold** is set to 90 days and **Run** to Everyday. This means that the data of agents that have not communicated with

the Endpoint server for 90 days is deleted from the database.

6. Click **Apply**.

Note: The Inactive Agents Retention Policy is not applicable for NetWitness Endpoint 4.4.0.2 or later agents.

Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1

You can configure the Endpoint Metadata for the NetWitness Endpoint 4.4.0.2 in one of the following ways:

- **(Option 1) Integrate the NetWitness Endpoint 4.4.0.2 Console Server to an Endpoint Hybrid or Endpoint Log Hybrid** - The NetWitness Endpoint 4.4.0.2 or later agents data will be available in the **Investigate > Hosts** and **Files** view, and you can view the Endpoint metadata in the **Investigate > Navigate** and **Event Analysis** view. For this option, make sure the Endpoint sever is configured for meta forwarding.
- **(Option 2) Integrate the Meta Integrator service in the NetWitness Endpoint 4.4.0.2 directly to a Log Decoder** - You can view the Endpoint metadata in the **Investigate > Navigate** and **Event Analysis** view. The NetWitness Endpoint 4.4 agents data will not be available in the **Investigate > Hosts** and **Files** view.

In addition to the categories mentioned for the NetWitness Endpoint 11.1 agents, the following categories are also forwarded for the NetWitness Endpoint 4.4.0.2 or later agents - File event, Network event, Registry event, and Process event.

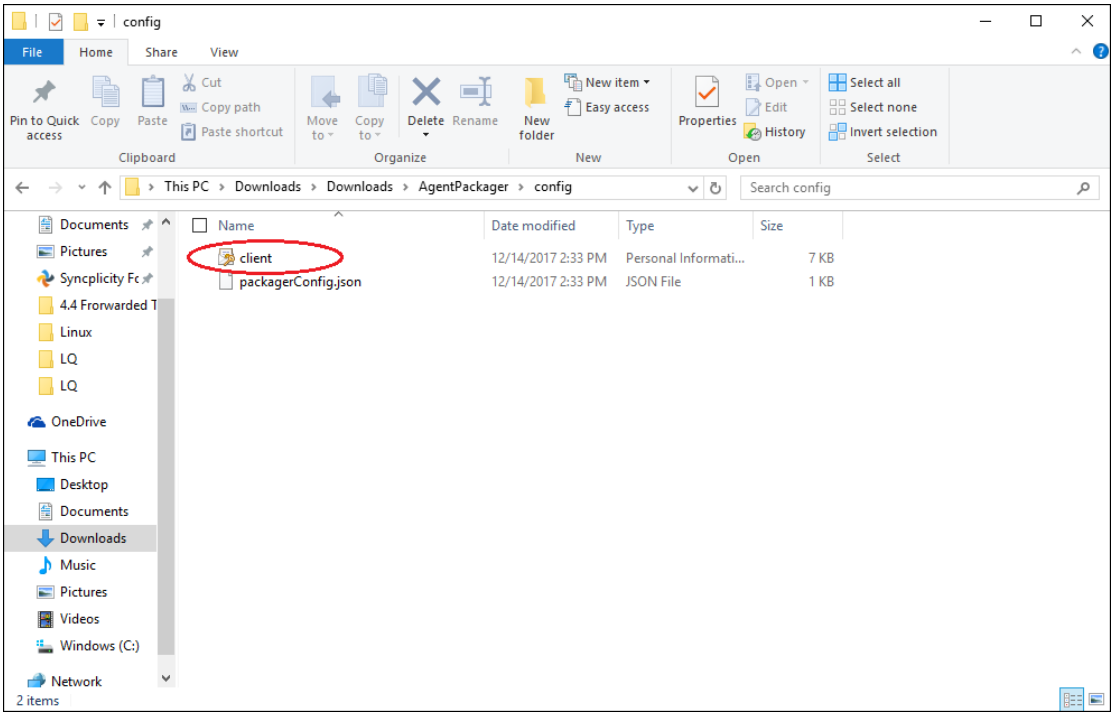
Configuring the NetWitness Endpoint 4.4.0.2 Console Server

Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server (for Option 1)

The NetWitness Endpoint 4.4.0.2 Console Server must use the same client certificate that the NetWitness Endpoint 11.1 agents use to forward the metadata to the Endpoint Server.

1. Download the agent packager. For more information, see *Endpoint Insights Agent Installation Guide*.
2. Extract **AgentPackager.zip** and from the Config folder, obtain the client certificate.

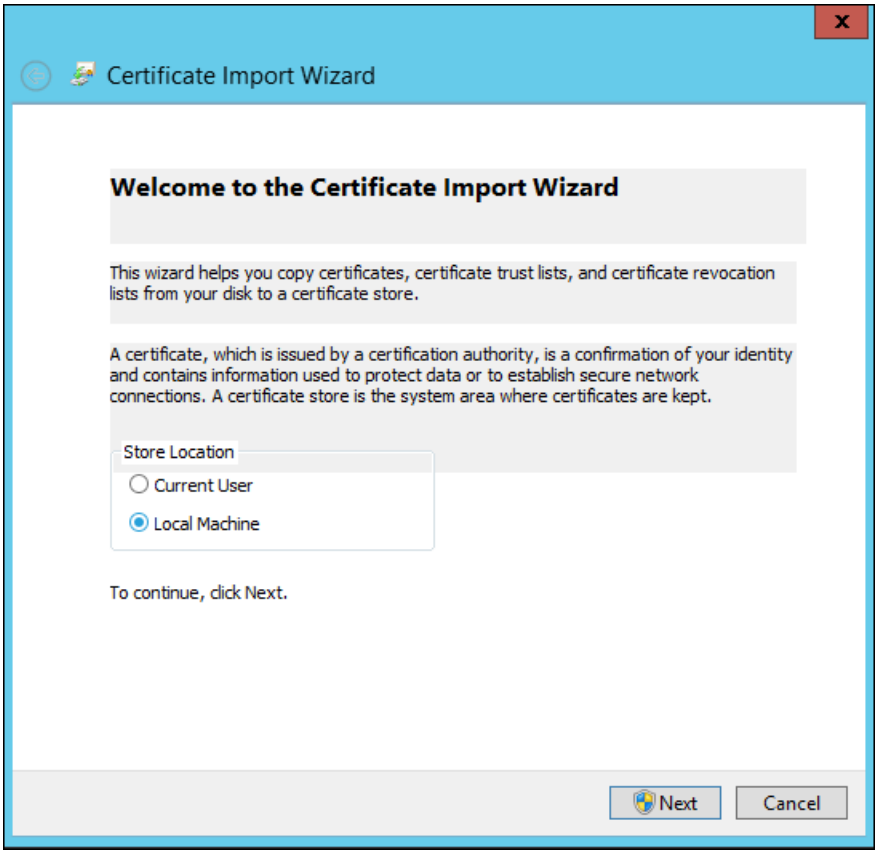
1. Copy the client certificate to the NetWitness Endpoint 4.4 Console Server.



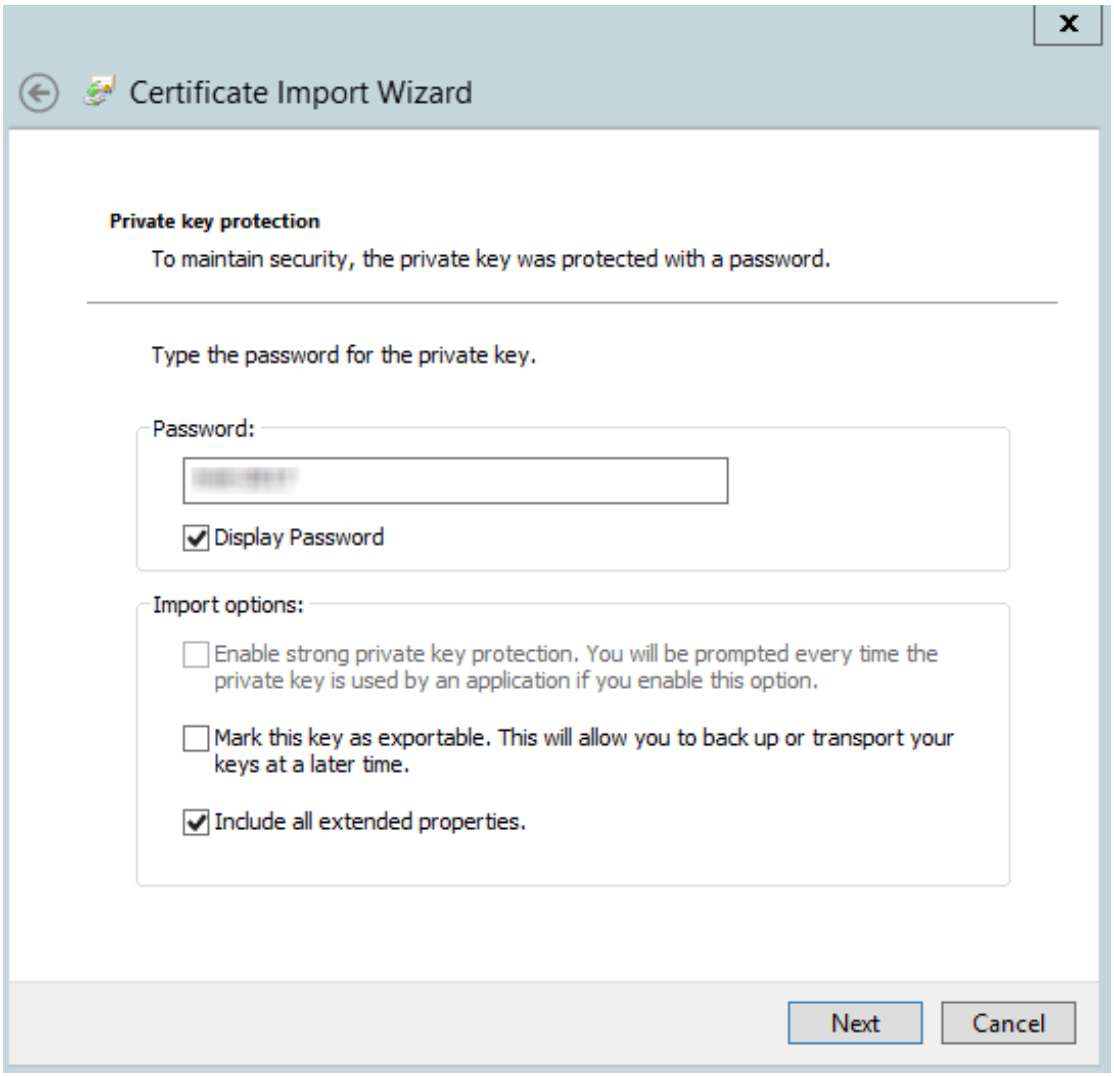
2. Double-click on the **client** file.

   The **Certificate Import Wizard** dialog is displayed.

3. Select the store location as **Local Machine** and click **Next**.

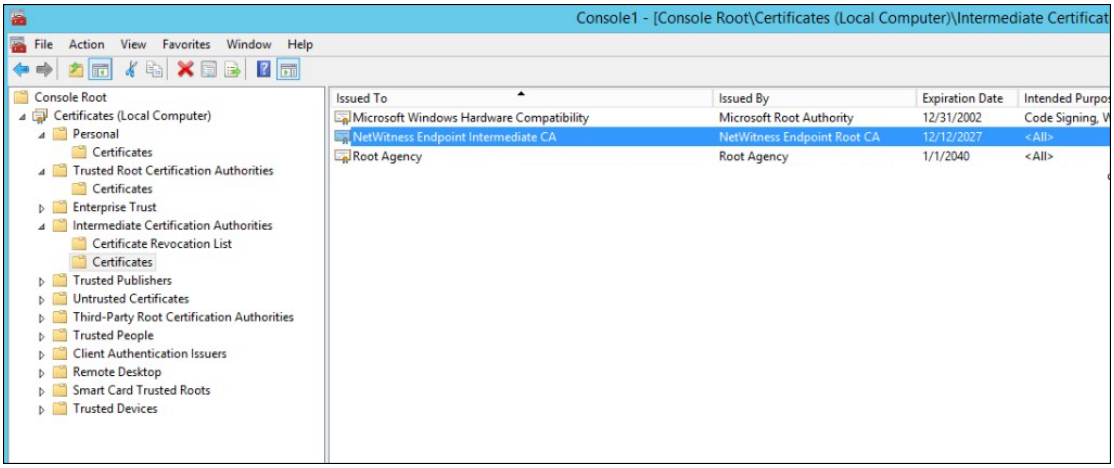


4. Browse the file you want to import and click **Next**.
5. Enter the same password used while generating the agent packager.



6. Click **Next** and **Finish**.

   The certificate is listed under **Personal**, **Intermediate Certificate Authorities** > **Certificate** and **Trusted Root Certification Authorities** in the Console Server.



Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2 (for Option 1)

To enable the metadata forwarding for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

```
ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT HOST> certificate <CERTIFICATE DISPLAY NAME>.
```

For example, `ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://<Ip Address>:443 certificate rsa-nw-endpoint-agent`

Enabling the NetWitness Endpoint 4.4.0.2 Meta Forwarding to the Log Decoder (for Option 2)

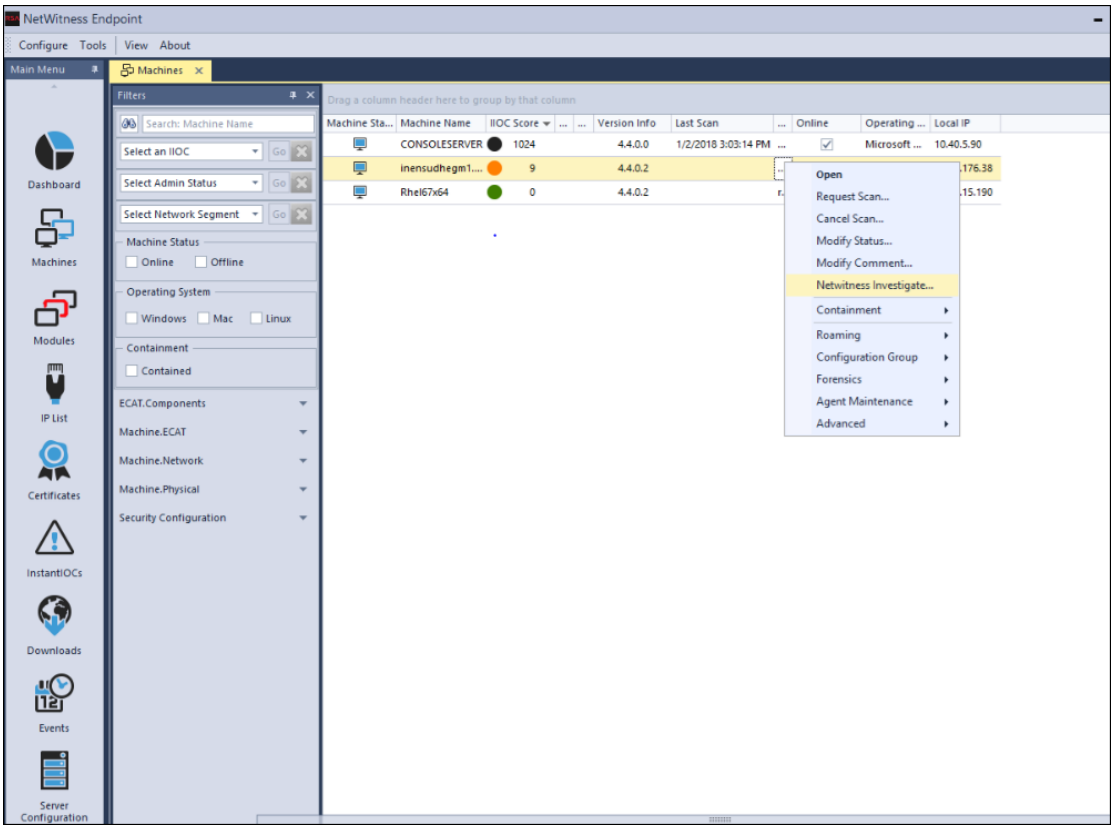
To enable the Metadata Integrator service for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

```
ConsoleServer.exe /nw-investigate enable.
```

Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server (for Option 1 and 2)

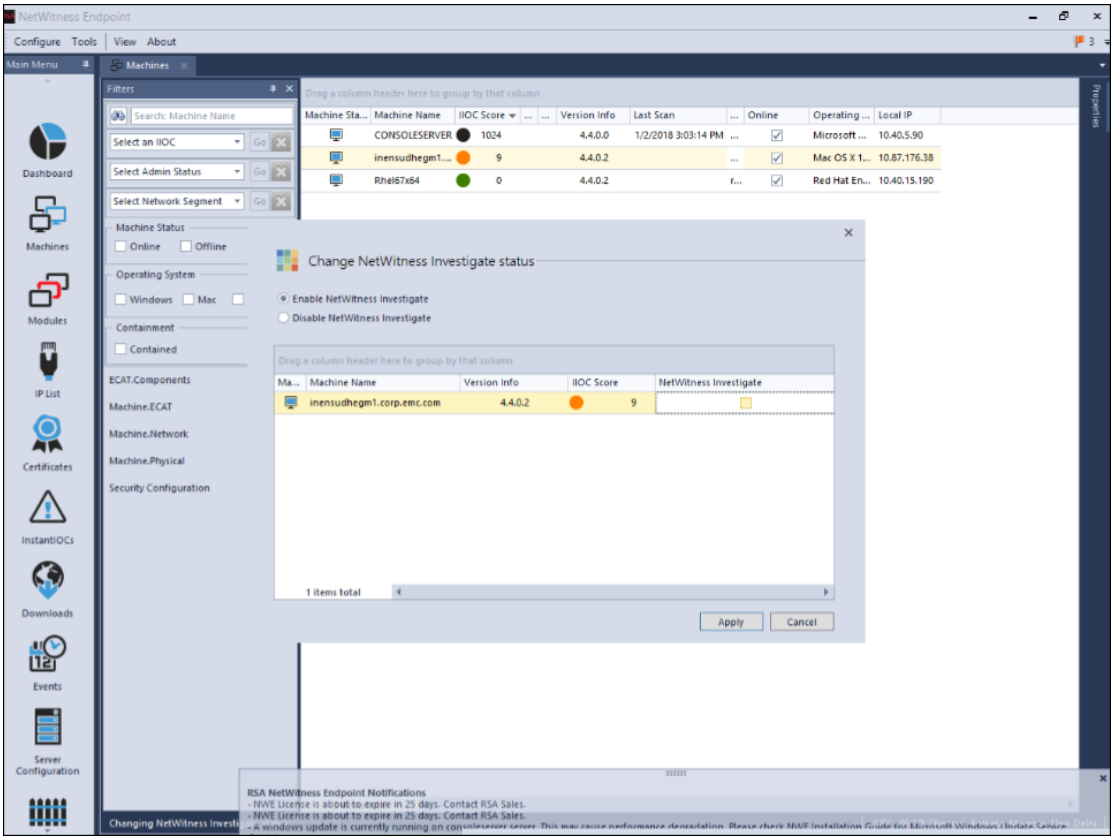
After you enable the Metadata Forwarding using any one of the above options, perform the following to enable the machines to forward metadata.

1. Open the NetWitness Endpoint 4.4.0.2 user interface.
2. Click **Machines** from the left panel. The list of available machines are displayed.



3. Select machines for which you want to forward metadata to the NetWitness Endpoint Server.

4. Right-click and select the **NetWitness Investigate** option.
   The Change NetWitness Investigate Status dialog is displayed.



5. Select the **Enable NetWitness Investigate** option.
6. Click **Apply**.
7. To verify if the **Enable NetWitness Investigate** option is enabled, repeat step 4.

Endpoint References

This section is intended to help you understand the purpose of the Services Config View for the Endpoint Server. For each configuration, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition, it includes workflow and Quick Look sections to highlight important features in the user interface.

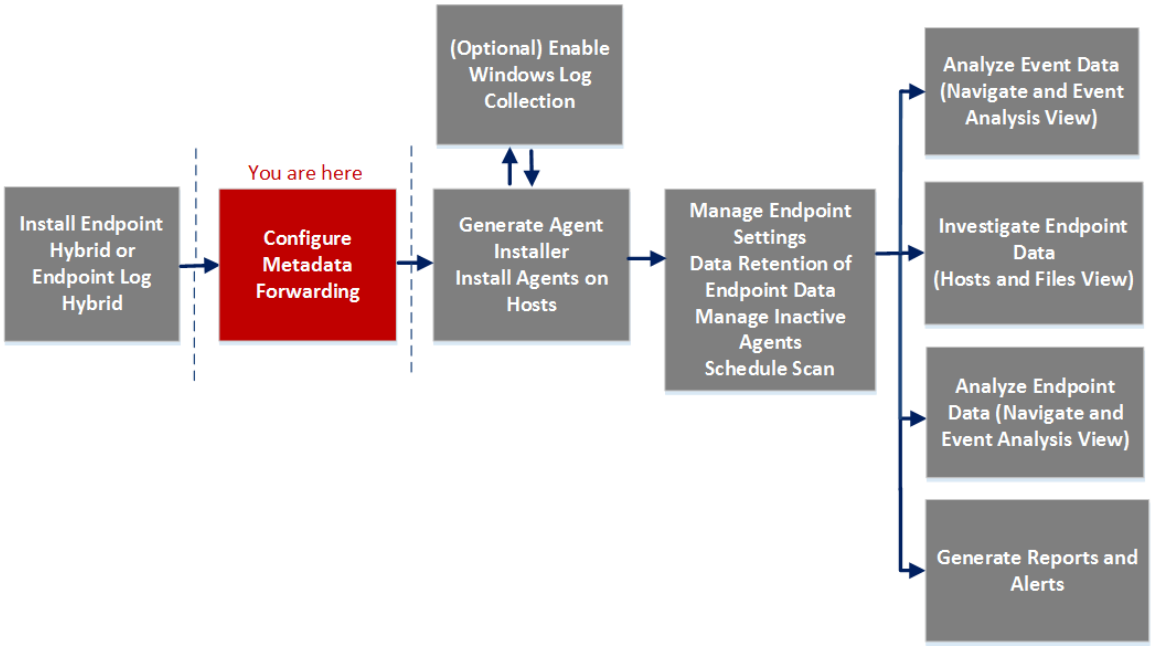
You can view the complete service nodes in tree form in the Services Explore view. For more information, see the "Services Explore View" topic in the *Hosts and Services Getting Started Guide*.

General Tab

In the **General** tab, you can configure the Endpoint metadata forwarding. To access this view:

1. Go to **Admin** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click and select > **View** > **Config**.
4. Click the **General** tab.

Workflow



What do you want to do?

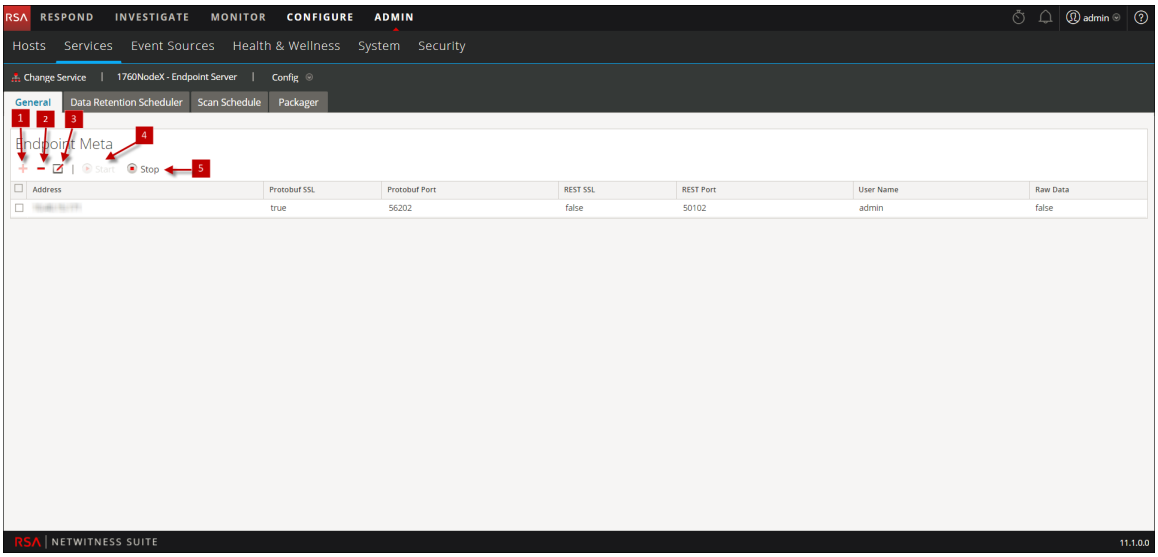
Role	I want to ...	Show me how
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint 11.1 Agents	Configuring Metadata Forwarding

Role	I want to ...	Show me how
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint 4.4.0.2 or later Agents	Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1

*You can perform this task in the current view.

Quick Look

The following figure is an example of the General tab.



1. Click + to view the **Available Services** dialog.
2. Click − to delete the added service.
3. Click to edit the information for the added service.
4. Click Start to start the Endpoint metadata forwarding.
5. Click Stop to stop the Endpoint metadata forwarding.

The following table describes the fields in the General tab.

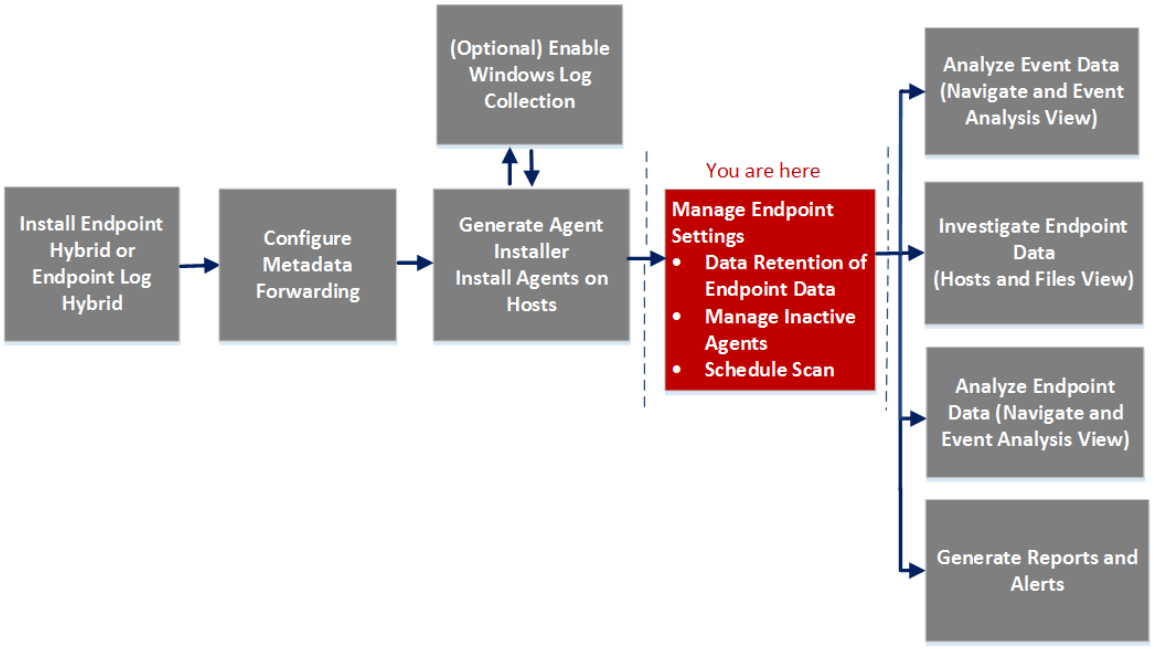
Field	Description
Address	Displays the IP address of the Log Decoder.
Protobuf SSL	Indicates if SSL is enabled on Protobuf. By default, this option is disabled.
Protobuf Port	Displays the port used for Protobuf. By default, the port is 50202.
REST SSL	Indicates if SSL is enabled on the REST port in the Log Decoder. By default, this option is disabled.
REST Port	Displays the port used for REST communication. The default value is 50202 (for non-SSL) and value 56202 (for SSL).
User Name	Displays the user name.
Raw Data	Sends a brief summary of the session along with the metadata if enabled. By default, this option is disabled.

Data Retention Scheduler Tab

In the **Data Retention Scheduler** tab, you can configure data retention and inactive agents policies. To access this view:

1. Go to **Admin** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.

Workflow



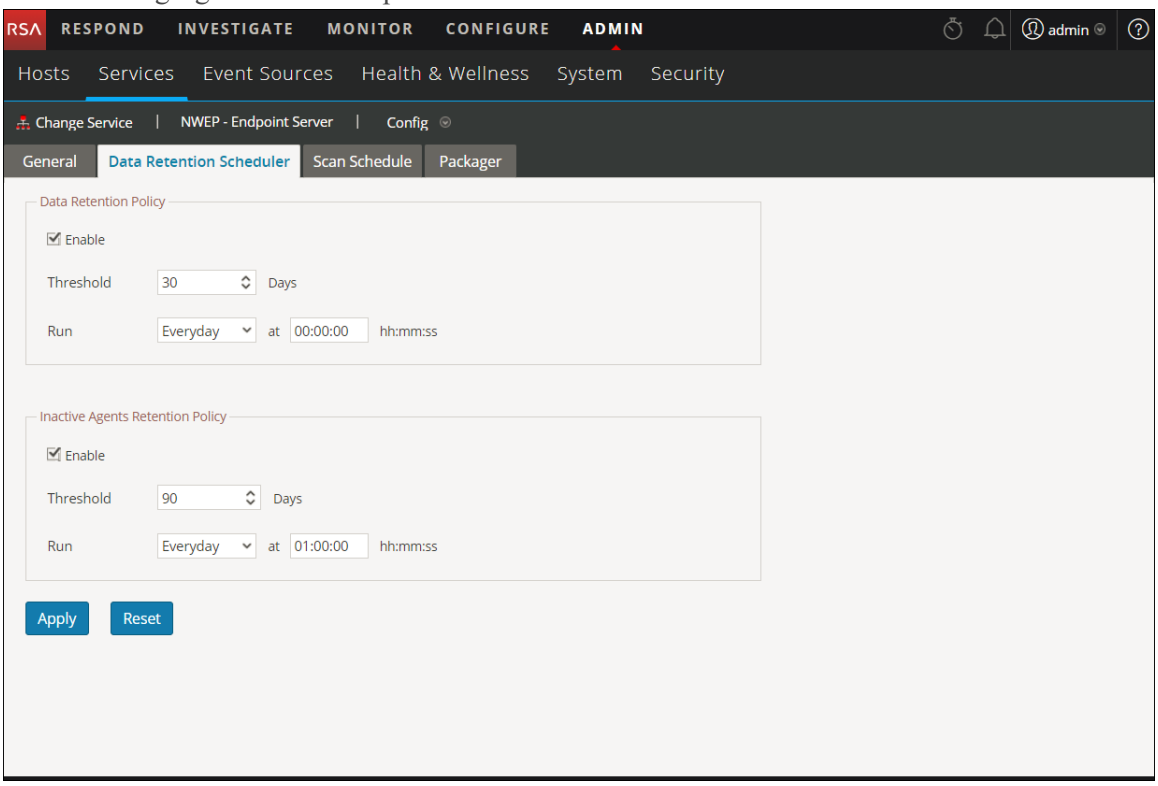
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Data Retention Policy*	Configure Data Retention Policy
Administrator	Configure Inactive Agents Policy*	Manage Inactive Agents

*You can perform this task in the current view.

Quick Look

The following figure is an example of the Data Retention Scheduler tab.



Features

The following table lists the fields for data retention policy.

Field	Description
Enable	Enables the configuration for the data retention policy. By default, this option is enabled.
Threshold	Displays the number of days the Endpoint data is retained in the database. By default, the Threshold is set to 30 days. The data older than 30 days is deleted from the database.

Field	Description
Run	Displays the schedule for running the data retention job. By default, the database check occurs everyday at 00:00:00 AM. You can select the frequency from the drop-down list (Everyday, Weekdays, Weekends, or Custom, where Custom allows you to select one or more specific days of the week) and time to run the job.
Apply	Overwrites any previous schedule for this service and applies the new schedule immediately.
Reset	Resets the schedule to the default settings.

The following table lists the fields for inactive agents retention policy.

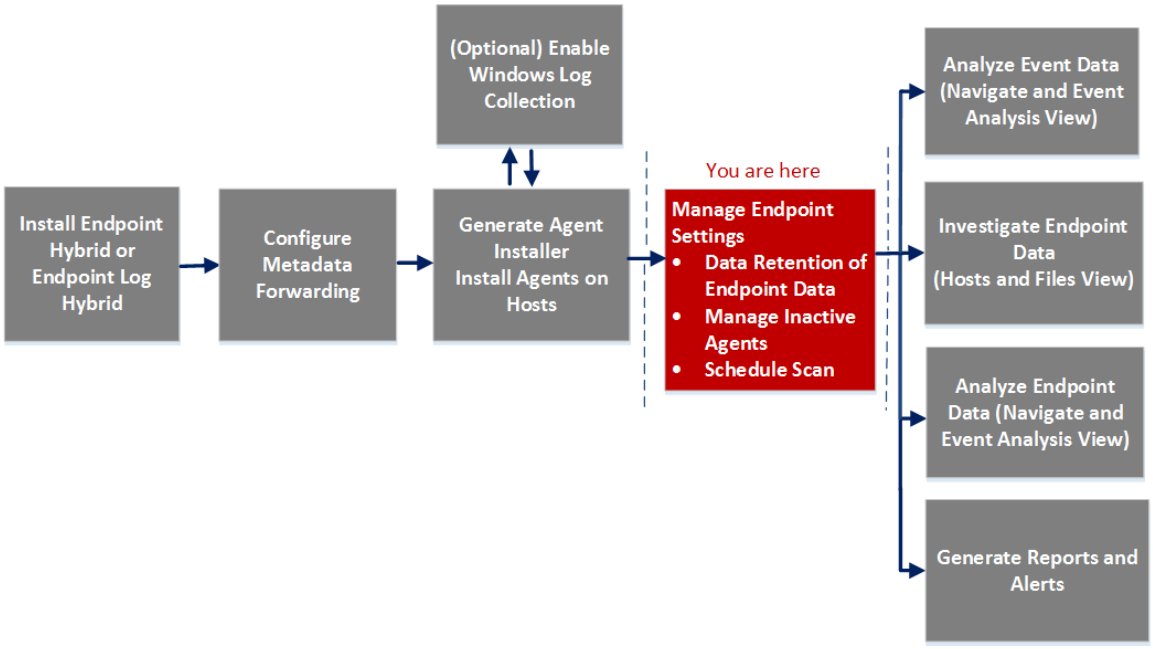
Fields	Description
Enable	Enables the configuration for the inactive agents policy. By default, this option is enabled.
Threshold	Displays the number of days the inactive agents are retained in the Endpoint Server. By default, the threshold value is 90 days.
Run	Displays the schedule for running the inactive agents retention job. By default, the database check occurs everyday at 00:00:00 AM. You can select the frequency from the drop-down list (Everyday, Weekdays, Weekends, or Custom, where Custom allows you to select one or more specific days of the week) and time to run the job.
Apply	Overwrites any previous schedule for this service and applies the new settings immediately.
Reset	Resets the schedule to the default settings.

Scan Schedule Tab

In the **Scan Schedule** tab, you can configure the schedule scan. To access this view:

1. Go to **Admin** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click and select > **View** > **Config**.
4. Click the **Scan Schedule** tab.

Workflow



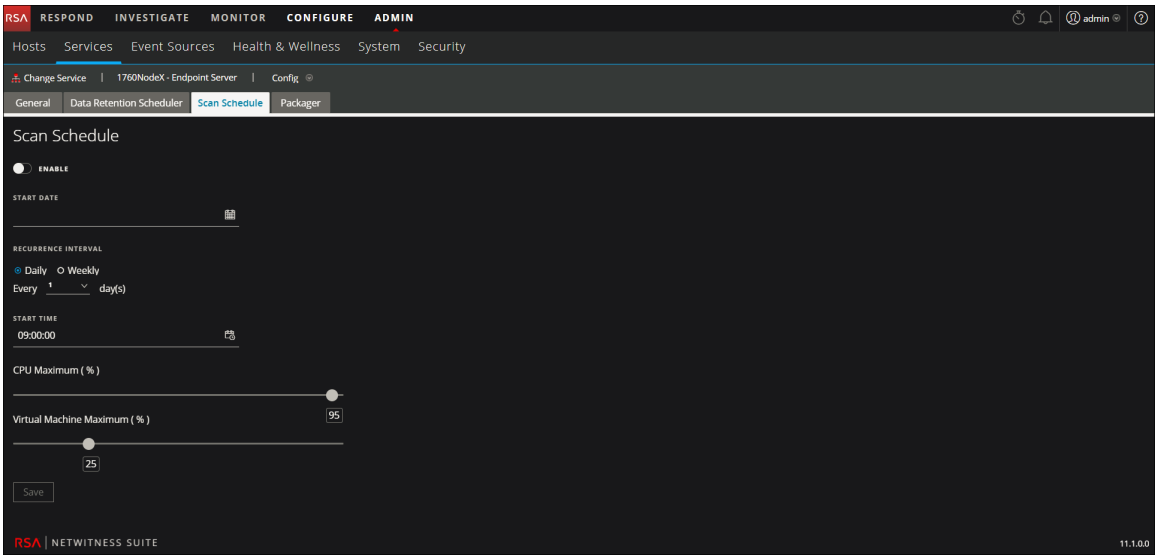
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Scan Schedule*	Configure Scan Schedule

*You can perform this task in the current view.

Quick Look

The following figure is an example of the Scan Schedule tab.



The following table describes the fields in the Scan Schedule tab. The values entered are specific to the agent time zone.

Field	Description
Enable	Select this option to configure the scan. By default, this option is disabled.
Start Date	Specify the date to start the scan.
Recurrence Interval	Select the recurrence interval to Daily or Weekly and set the frequency in days.
Start Time	Specify the time to start the scan.
CPU Max	Set the value using the slider. This ensures the CPU limit of the NetWitness Endpoint Agent.
VM Max	Set the value using the slider. **Note:** Use this option if agents are running on virtual machines. This is applicable only for Windows agents.

Packager Tab

In the **Packager** tab, you can generate an agent packager and agent installer. To access this view:

1. Go to **Admin** > **Services**.

2. In the Services view, select **Endpoint Server**.
3. Click and select > **View** > **Config**.
4. Click the **Packager** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Generate an Agent Packager for Endpoint Data Collection*	*Endpoint Insights Agent Installation Guide*
Administrator	Generating an Agent Packager for Windows Log Collection*	
Administrator	Generate an Agent Installer*	

*You can perform this task in the current view.

For more information on how to generate an agent, see *Endpoint Insights Agent Installation Guide*.

Troubleshooting

This section provides information about possible issues when using the RSA NetWitness Endpoint Insights.

Agent Communication Issues

Issue	Agent is unable to communicate with the Endpoint server.

Explanation	This could be due to one of the following reasons:
	• In the agent packager:
	  • Server IP is incorrect
	  • Port specified is not available for communication with the Endpoint server
	• Endpoint Server or Nginx Server is not running
	• Firewall or IP table rules are blocking the connection between the host and Endpoint Server
	• Agent is inactive or manually deleted from the UI

Resolution	• Check if the Endpoint Server and Nginx Server are reachable • Uninstall the agent, reboot the host, and reinstall the agent • Update Firewall or IP table rules, if required

Issue	Agent takes a long time to scan.
Explanation	Sometimes, the NetWitness Endpoint scan takes a long time to complete. This is because of the CPU usage by other antivirus programs (such as Windows Defender, Mcafee, Norton, and so on) that may be installed on the agent machines.
Resolution	It is recommended to whitelist the NWEAgent.exe file in the antivirus Windows Suite.

Packager Issues

Message	`Failed to load the client certificate.`

Issue	Incorrect certificate password.
Explanation	While generating the agent installer, the certificate password does not match with the one provided while downloading the agent packager from the UI.
Resolution	Specify the correct certificate password.

Message	`An unexpected error has occurred attempting to retrieve this data.`
Issue	When attempting to access the Packager tab, it opens with the message.
Explanation	Endpoint Server might be down or not reachable.
Resolution	Check the status of the Endpoint Server under **Admin > Service**. If the service is not running, start the Endpoint Server.

Scan Schedule Issues

Message	`An unexpected error has occurred attempting to retrieve this data.`
Issue	When attempting to access the Scan Schedule tab, it opens with the message.
Explanation	Endpoint Server might be down or not reachable.
Resolution	Check the status of the Endpoint Server under **Admin > Service**. If the service is not running, start the Endpoint Server.

Health and Wellness Issues

Behavior	Endpoint metadata is not available in the **Investigate > Navigate** or **Event Analysis** view.
Issue	The health check of the Meta-Ld-Buffer shows **Unhealthy** in the Health and Wellness with the following exceptions: dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder

Resolution	Make sure that: • Capture is enabled on the Log Decoder • Metadata is configured properly

Behavior	For the NetWitness Endpoint 4.4.0.2, metadata is not reaching the Endpoint Server.
Issue	The health of the Meta-Ld-Buffer shows **Unhealthy** in the Health and Wellness with the following exceptions: dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder
Explanation	Make sure that: • Certificate is obtained and imported to the NetWitness 4.4.0.2 Console Server • NetWitness Investigate option is enabled in the NetWitness Endpoint UI • Metadata forwarding is configured in the NetWitness 4.4.0.2 Console server

Behavior	The health check of the Data.Application.Connection-Health for Endpoint Server shows **Unhealthy**.
Issue	Either Mongo or Endpoint Server service is down.
Explanation	For error details, check the Endpoint Server logs in /var/log/netwitness/endpoint-server/endpoint-server.log.
Resolution	Restart the Mongo or Endpoint Server service.

Behavior	The health check of the Endpoint.Health.Overall-Health statistic shows **Unhealthy**.
Issue	Either Mongo or Endpoint Server service is down.
Explanation	Check the other Endpoint Server health statistics (such as, Data.Application.Connection-Health, Endpoint.Health.Ld-Buffer-Health) to

	identify which stats shows Unhealthy. If one of them is Unhealthy, the overall health of the Endpoint Server shows Unhealthy.
Resolution	See the resolution for these statistics in the Health and Wellness Issues section.

Issue	Agent rejection count is more than the alarm threshold.
Explanation	The agent rejected count is more than a specific limit and your custom policy is triggered. For example, agent rejected count for the last 5 hours is 10 percent of the deployed agents.
Resolution	Check the overall health of the Endpoint Server and the sizing guidelines.

Issue	Storage size of the Data application statistic has exceeded the alarm threshold.
Explanation	The storage size of the Data application has exceeded the threshold (for example, 75%), and the custom policy is triggered. **Note:** By default, the server automatically deletes the older data when it reaches 80% of the disk space.
Resolution	Check the threshold set in the data retention policy.

Issue	The health check of the Data.Application.Connection-Health shows Unhealthy or Fatal.
Explanation	The Mongo service is down.
Resolution	Check if the Mongo service is running and the Endpoint Server logs for error details.

Issue	The agent request count shows 0 for a alarm threshold.
Explanation	The agent request count shows 0 for the entire day or week. This could be due to one of the following reasons: • In the agent packager: • Server IP is incorrect

	• Port specified is not available for communication with the Endpoint server • Endpoint Server or Nginx Server is not running • Firewall or IP table rules are blocking the connection between the host and Endpoint Server • Agent is inactive or manually deleted from the UI
Resolution	• Check if the Endpoint Server and Nginx Server are reachable • Uninstall the agent, reboot the host, and reinstall the agent • Update Firewall or IP table rules, if required

Meta Data Configuration Issue

Behavior	The console server displays a message.
Issue	The console server displays the following message: *Console Server will Log Processed batch as 1."rsa-nw-endpoint-agent will be used to make SSL connection with Netwitness suite.*
Explanation	When you run a quick scan on the NetWitness Endpoint 4.4 server for an agent or a machine, a message is displayed.
Resolution	Verify the metadata configuration.

Installation Issue

Behavior	NetWitness Suite allows multiple instances of Endpoint Hybrid or Endpoint Log Hybrid to be installed.
Issue	Only one instance of the Endpoint Hybrid or Endpoint Log Hybrid can be used for endpoint data.
Explanation	While the installation of Endpoint Hybrid or Endpoint Log Hybrid is in-progress, you can install another instance and the installation will be successful.
Resolution	You must delete all instances of Endpoint Hybrid or Endpoint Log Hybrid except the one that you want to use for endpoint data.

Finding Inactive Agents Issue

Issue	Agent might be inactive or has not communicated with the Endpoint Server for a long time.
Explanation	A list of inactive agents is available in the Mongo database with the agent ID. Using this information, you can search for further details of the inactive agents.
Resolution	To find inactive agents in your deployment, perform the following: 1. Open the Endpoint Server log file from `/var/log/netwitness/endpoint-server/endpoint-server.log` and search for Agent <ID> does not exist string. 2. Copy the agent ID displayed in the log file. 3. Search for the agent ID in the NGINX access log file (`/var/log/nginx/access.log`) to retrieve the following details of an inactive agent: • IP Address • Date and time that the agent became inactive • Location

RSA NETWITNESS® SUITE

Log Collection Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

About Log Collection **8**

Workflow 8

High-Level Procedures 9

Log Collection Architecture **11**

How You Deploy Log Collection 11

Components of Log Collection 11

Local and Remote Collectors 12

Windows Legacy Remote Collector 13

Setup **15**

Basic Implementation 15

Prerequisites 15

Roles of Local and Remote Collectors 15

Deploying and Configuring Log Collection 15

Adding Local Collector and Remote Collector to NetWitness Suite 17

Configuring Log Collection 17

Data Flow Diagram 17

Provision Local Collectors and Remote Collectors 18

Configure Local and Remote Collectors 20

Local Collectors Tab for a Remote Collector 25

Configure Failover Local Collector 25

Configure Replication 27

Configure Chain of Remote Collectors 30

Throttle Remote Collector to Local Collector Bandwidth 33

Set Up a Lockbox 35

What Is a Lockbox 36

Set Up a Lockbox 36

Start Collection Services 37

Start a Collection Service 37

Enable Automatic Start of Collection Services 38

Verify That Log Collection Is Working 38

Configure Certificates 39
Add a Certificate 39
Certificates Panel 39
Add Cert Dialog 40

Log Collection Basics 41

How Log Collection Works 41
Collection Protocols 41
Basic Procedure 43
Configure Collection in RSA NetWitness Suite 44
Start the Service for your Collection Method 45
Verify that Collection is working for your Event Source 45
Configure Event Filters for a Collector 45
Configure an Event Filter 45
Modify Filter Rules 50
Import, Export, Edit and Test Event Sources in Bulk 52
Import Event Sources in Bulk 52
Export Event Sources in Bulk 55
Edit Event Sources in Bulk 56
Test Event Source Connections in Bulk 57
See Also 58

Configure Collection Protocols and Event Sources 59

Configure AWS (CloudTrail) Event Sources in NetWitness Suite 61
How AWS Collection Works 61
Deployment Scenario 61
Configuration 62
AWS Parameters 63
Configure Azure Event Sources in NetWitness Suite 67
Configuration in NetWitness Suite 67
Azure Parameters 68
Configure Check Point Event Sources in NetWitness Suite 70
How Check Point Collection Works 71
Deployment Scenario 71
Configuration in NetWitness Suite 72
Check Point Parameters 73
Basic Parameters 73

Determine Advanced Parameter Values for Check Point Collection 74
Verify Check Point Collection is Working 76
Configure File Event Sources in NetWitness Suite 77
Configure a File Event Source 77
Stop and Restart File Collection 78
File Collection Parameters 79
Configure Netflow Event Sources in NetWitness Suite 83
Configure a Netflow Event Source 83
Netflow Collection Parameters 85
ODBC 86
Configure ODBC Event Sources in NetWitness Suite 86
Configure a DSN 87
Add an Event Source Type 88
Configure Data Source Names (DSNs) 91
Create Custom Typespec for ODBC Collection 98
Troubleshoot ODBC Collection 103
Configure SDEE Event Sources in NetWitness Suite 104
Configure an SDEE Event Source 104
Configure SNMP Event Sources in NetWitness Suite 107
Configure the SNMP Trap Event Source 107
(Optional) Configure SNMP Users 108
SNMP User Parameters 108
Configure Syslog Event Sources for Remote Collector 109
Configure a Syslog Event Source 109
Syslog Parameters 110
Configure VMware Event Sources in NetWitness Suite 113
Configure a VMware Event Source 113
Configure Windows Event Sources in NetWitness Suite 114
Configure a Windows Event Source 114
Windows Legacy and NetApp Collection Configuration 117
How Legacy Windows and NetApp Collection Works 117
Deployment Scenario 119
Set Up the Windows Legacy Collector 119
Configure Windows Legacy and NetApp Event Sources 120
Troubleshoot Windows Legacy and NetApp Collection 126

Windows Log Collection for Endpoint Agents 130
Add or Update Windows Log Collection Configuration to an existing Endpoint Agent 131
Verify Windows Log Collection 133
Enable log forwarding and Configure Log Decoder 134

Reference 136

AWS Parameters 136
Azure Parameters 142
Check Point Parameters 145
Basic Parameters 146
Determine Advanced Parameter Values for Check Point Collection 147
File Parameters 150
Log Collection Service System View 156
ODBC Event Source Configuration Parameters 158
Access ODBC Configuration Parameters 158
Data Source Name (DSN) Parameters 159
Sources Panel 159
Toolbar 159
Add or Edit DSN Dialog 160
ODBC DSNs Event Source Configuration Parameters 163
Access ODBC Configuration Parameters 163
DSN Panel 164
Add or Edit DSN Dialog 165
Manage DSN Templates Dialog 165
Remote/Local Collectors Configuration Parameters 167
Remote Collectors Tab 168
Local Collector Tab 169
Log Collection Tabs 170
Access Log Collection View 170
Available Tabs 171
Log Collection General Tab 172
Log Collection Event Destinations Tab 176
Log Collection Event Sources Tab 179
Log Collection SettingsTab 183

Troubleshoot Log Collection 185

Log Files 185

Health and Wellness Monitoring 185
Sample Troubleshooting Format 185
Troubleshooting - Windows log Collection using Endpoint Agent 186
Windows Log Configuration File Format Explained 186
Test Log - How to Read 187

About Log Collection

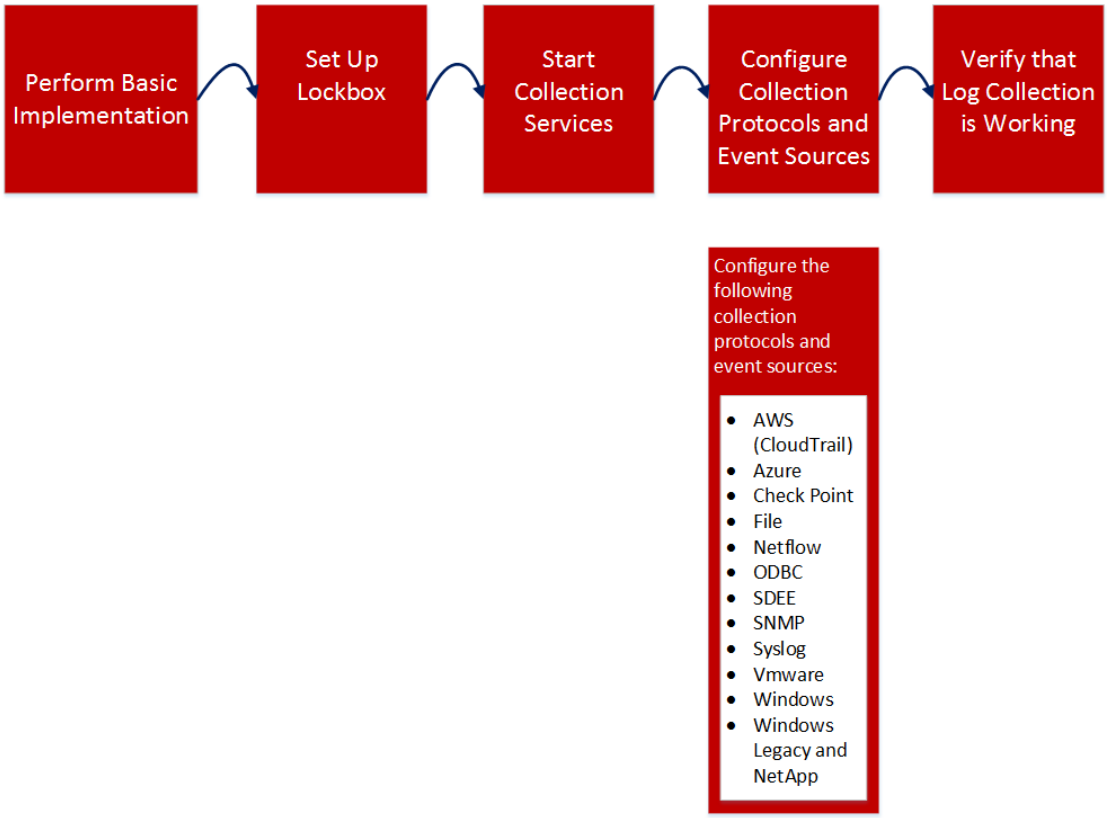
This guide describes the high-level steps and subtasks for setting up and configuring log collection for event sources that include:

- What Log Collection does, how it works from a high level, and provides high-level deployment diagrams.
- How to start collecting events.
- Where to find instructions to set up more complex deployments.
- How to start any collection protocol.
- What the structure of the Log Collection Configuration User Interface is.
- Which tools to use to troubleshoot Log Collection issues and lists global troubleshooting instructions.
- How to fine tune and customize Log Collection in your environment.
- How to configure individual collection protocols. Instructions are in the individual Log Collection sections.

Workflow

This workflow depicts the basic tasks needed to start collecting events through Log

Collection.



High-Level Procedures

At a high level, these are the procedures you must follow for log collection:

I. Add local and remote collectors to RSA NetWitness Suite.

Set up a Log Collector locally on a Log Decoder (that is a Local Collector). You can also set up Log Collectors in as many remote locations (that is Remote Collectors) as you need for your enterprise. For details, see Basic Implementation.

II. Download the latest content from Live. This is a task that you perform periodically, as the content provided on Live is updated regularly.

LIVE is the Content Management System for RSA NetWitness® Suite, from which you download the latest content. The two resource types you use to download Log Collection content are:

- **RSA Log Collector** - content enabling the collection of event source types.
- **RSA Log Device** - the latest supported event source parsers.

You can also subscribe to content on Live. For details, see the *Live Services Management Guide*.

III. Configure Settings: set up the lockbox and Certificates.

For details, see Set Up a Lockbox and Configure Certificates.

IV. Configure Event Sources.

You configure all the event sources on your network to send their log information to RSA NetWitness Suite. Whenever you add new event sources, you need to perform this procedure as well. All event source configuration guides are found in the RSA Supported Event Sources space in RSA Link.

V. Start and stop services for configured protocols. Occasionally, you may be required to stop and restart services, based on new event sources that you add to RSA NetWitness Suite.

VI. Verify that Log Collection is working.

Whenever you set up a new event source or add a new collection protocol, you should verify that the correct logs are being sent to RSA NetWitness Suite.

Log Collection Architecture

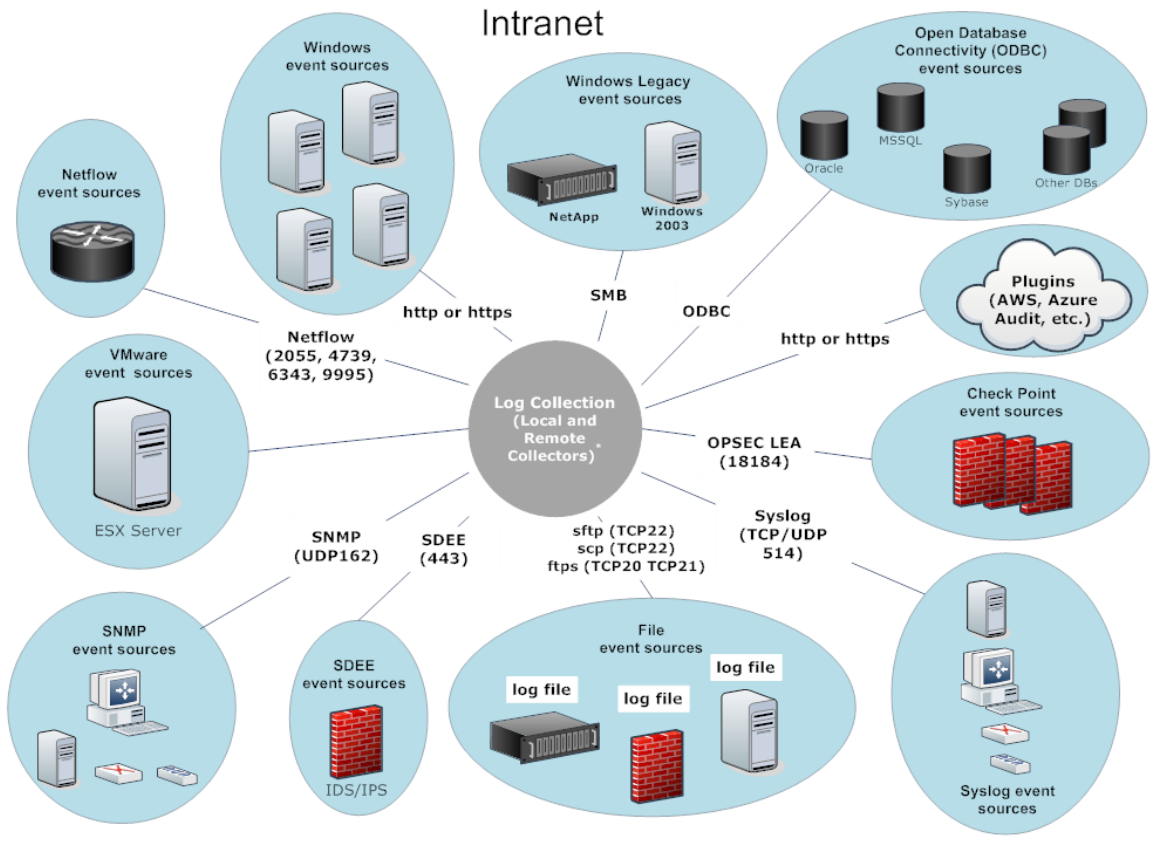
This topic describes how NetWitness Suite performs log collection.

How You Deploy Log Collection

You can deploy Log Collection according to needs and preferences of your enterprise. This includes deploying Log Collection across multiple locations and collect data from varying sets of event sources. You do this by setting up a Local Collector with one or many Remote Collectors.

Components of Log Collection

The following figure shows all the components involved in event collection through the NetWitness Suite Log Collector.



Local and Remote Collectors

The following figure illustrates how the Local and Remote Collectors interact to collect events from all of your locations.

In this scenario, log collection from various protocols like Windows, ODBC, and so on, is performed through both the Remote Collector and Log Collector service. If the log collection is done by the Local Collector, it is forwarded to the Log Decoder service, just like the local deployment scenario. If the log collection is done by a Remote Collector, there are two methods in which these are transferred to the Local Collector:

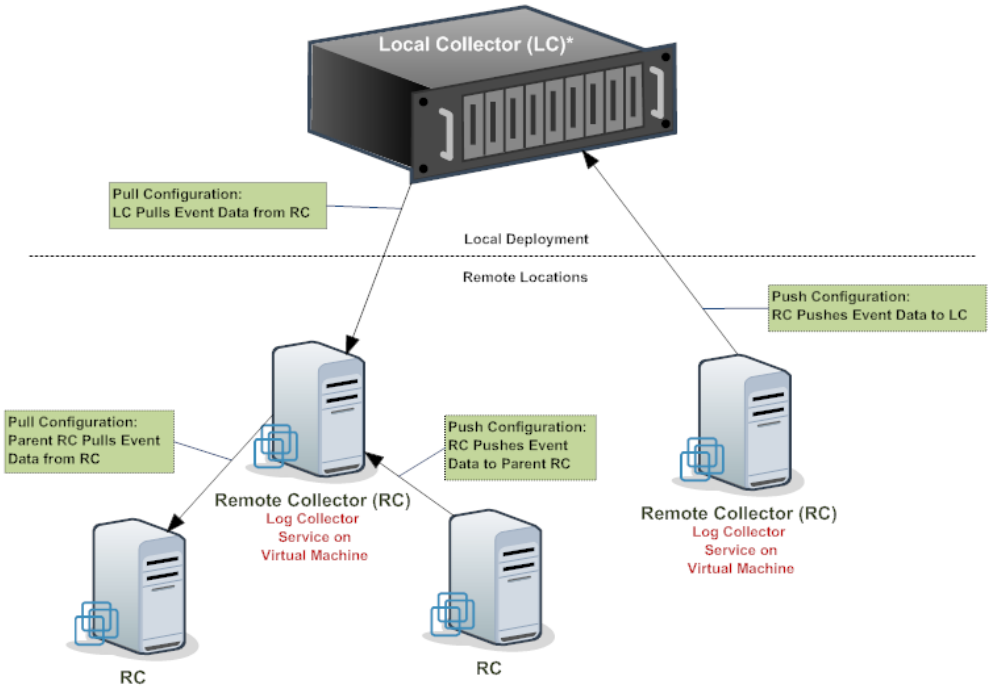
- **Pull Configuration** - From a Local Collector, you select the Remote Collectors from which you want to pull events.
- **Push Configuration** - From a Remote Collector, you select the Local Collector to which you want to push events.

Note: The typical use case is Push. Pull is available if you have a DMZ in your environment. Less secure network segments are not allowed to make connections to more secure network segments. With Pull, the Log Collector (or Virtual Log Collector) in the secure network initiates the connection to the VLC in the less secure network, and the logs are then transferred without breaking the connection rules.

You can configure one or more Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from one or more Remote Collectors.

Additionally, you can set up a chain of Remote Collectors for which you can configure:

- One or more Remote Collectors to push event data to a Remote Collector.
- A Remote Collector to pull event data from one or more Remote Collectors.



* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

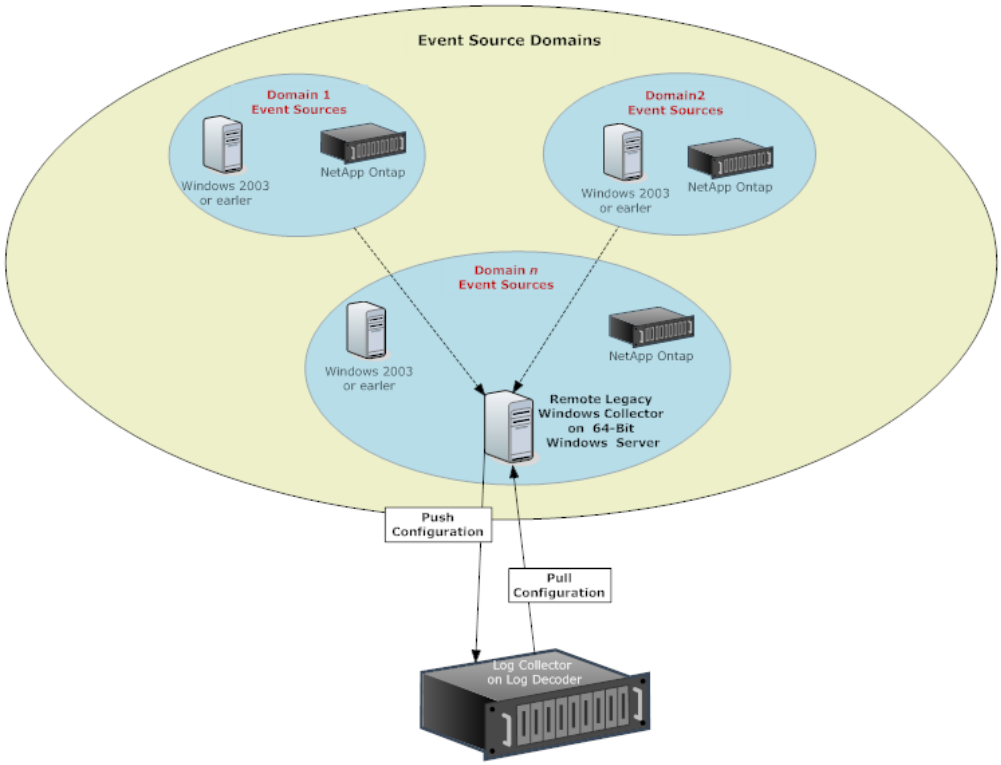
Windows Legacy Remote Collector

The RSA NetWitness® Suite Windows Legacy Collector is a Microsoft Windows based remote log collector (RC) which can be installed on a Windows domain.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

The following figure illustrates the deployment required to collect events from Windows Legacy event sources.


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

Setup

Basic Implementation

This topic tells how to perform the initial setup of Local Collectors and Remote Collectors.

Prerequisites

Verify that the Log Decoder is set up:

- is capturing data.
- has the current content loaded.
- is properly licensed.

Roles of Local and Remote Collectors

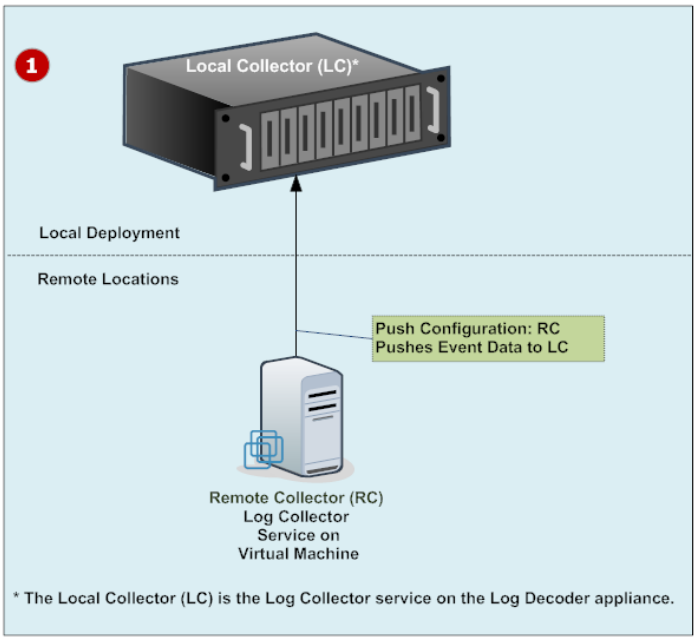
A Local Collector (LC) is a Log Collector service running on a Log Decoder host. In a local deployment scenario, the Log Collector service is deployed on a Log Decoder host, with the Log Decoder service. Log collection from various protocols like Windows, ODBC, and so on, is performed through the Log Collector service, and events are forwarded to the Log Decoder service. The Local Collector sends all collected event data to the Log Decoder service.

You must have at least one Local Collector to collect non-Syslog events.

A Remote Collector (RC), also referred to as a Virtual Log Collector (VLC), is a Log Collector service running on a stand-alone Virtual Machine. Remote Collectors are optional and they must send the events they collect to a Local Collector. Remote Collector deployment is ideal when you have to collect logs from remote locations. Remote Collectors compress and encrypt the logs before sending them to a Local Collector.

Deploying and Configuring Log Collection

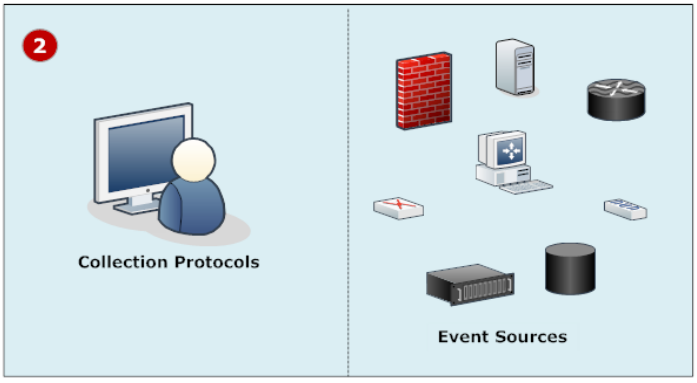
The following figure illustrates the basic tasks you must complete to deploy and configure Log Collection. To deploy Log Collection, you need to set up a Local Collector. You can also deploy one or more Remote Collectors. After you deploy Log Collection, you need to configure the events sources in NetWitness Suite and on the events sources themselves. The following diagram shows the Local Collector with one Remote Collector that pushes events to the Local Collector.



1 Set up Local and Remote Collectors.

The Local Collector is the Log Collector service running on the Log Decoder host.

A Remote Collector is the Log Collector service running on a virtual machine or Windows server in a remote location.



2 Configure event sources:

- Configure collection protocols in NetWitness Suite.
- Configure each event source to communicate with the NetWitness SuiteLog Collector.

Adding Local Collector and Remote Collector to NetWitness Suite

To add a Local Collector and Remote Collector to NetWitness Suite:

1. Go to **ADMIN > Services**.
2. Click + and select **Log Collector** from the menu.

   The **Add Service** dialog box is displayed.
3. Define the details of the **Log Collection** service.
4. Select **Test Connection** to ensure that your Local or Remote Collector is added.

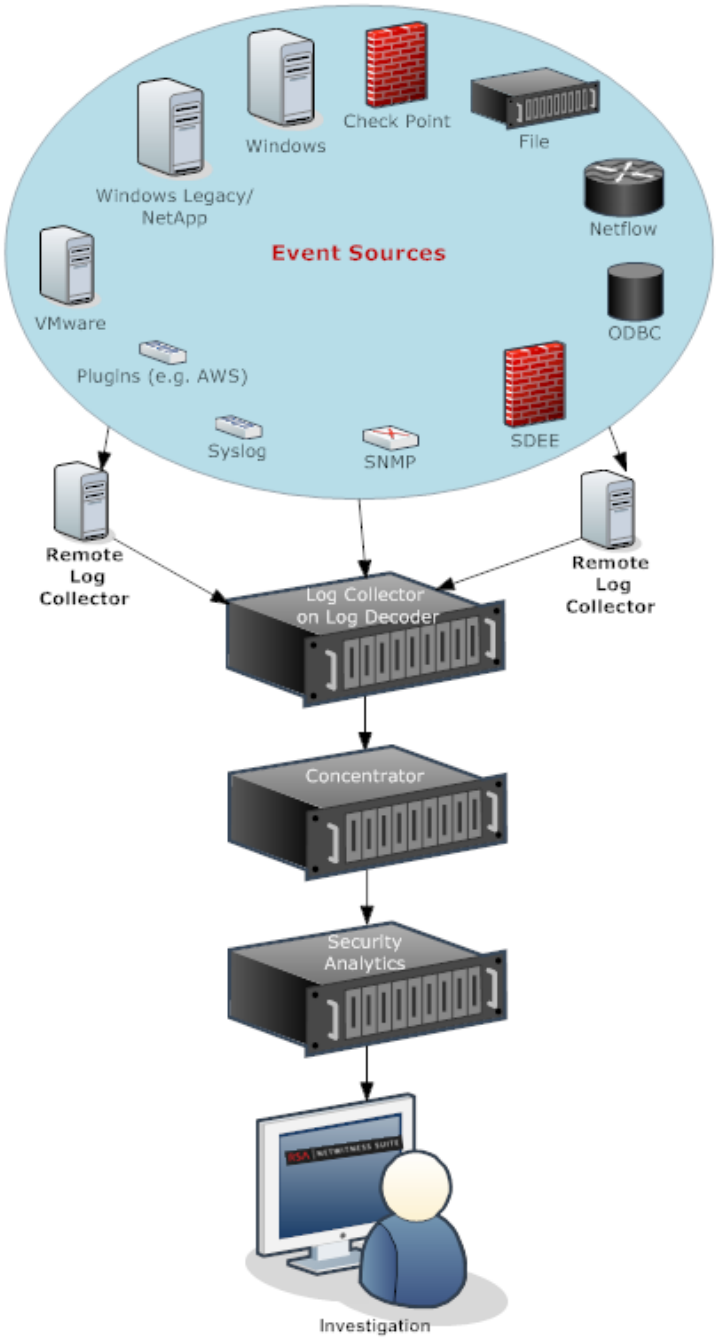
Configuring Log Collection

You choose the Log Collector—that is a Local Collector (LC) or Remote Collector (RC)—for which you want to define parameters in the Services view. The following figure shows how to navigate to the Services view, select a Log Collector service, and display the configuration parameter interface for that service.

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.
3. Click ⚙ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.
4. Define global Log Collection parameters in the **General** tab.
5. For a:
   - Local Collector, NetWitness Suite displays the **Remote Collectors** tab. Select the Remote Collectors from which the Local Collector pulls events in this tab.
   - Remote Collector, NetWitness Suite displays the **Local Collectors**. Select the Local Collectors to which the Remote Collector pushes events in this tab.
6. Edit configuration files as text files in the **Files** tab.
7. Define collection protocol parameters in the **Event Sources** tab.
8. Define the lockbox, encryption keys, and certificates in the Settings tab.
9. Define Appliance Service parameters in the **Appliance Service Configuration** tab.

Data Flow Diagram

You use the log data collected by the Log Collector service to monitor the health of your enterprise and to conduct investigations. The following figure shows you how data flows through NetWitness Suite Log Collection to Investigation.



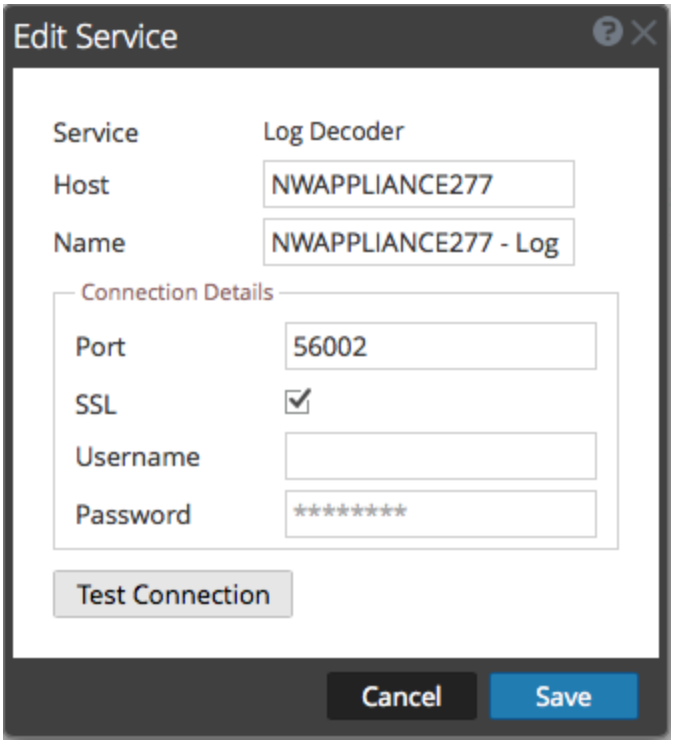
Provision Local Collectors and Remote Collectors

The NetWitness Suite server verifies if an appliance has a Log Decoder service. If there is a Log Decoder service, it becomes a Local Collector. If a Log Decoder service is missing, it becomes a Remote Collector. A local Log Collector has an Event Destination and by default goes to the Local Log Decoder service. A Remote Collector does not have an Event Destination. The NW Server server identifies a Legacy Windows Collector as a Remote Collector.

To edit a Local Collector or Remote Collector :

1. Go to **ADMIN > Services**.
2. In the **Services** view, select in the toolbar.

   The **Edit Service** dialog is displayed.



3. In the **Edit Service** dialog, provide the following information.

Field	Description
Service	Select Log Collector as the service type.
Host	Select a Log Decoder host.
Name	Type name you want to assign to the service.
Port	Default port is 50001 for clear text and 56001 for SSL encrypted.
SSL	Select **SSL** if you want NetWitness Suite to communicate with the host using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates.

Field	Description
(Optional) Username	Type the username of the Local Collector.
(Optional) Password	Type the password of the Local Collector.

4. Click **Test Connection** to determine if NetWitness Suite connects to the service.
5. When the result is successful, click **Save**.

   If the test is unsuccessful, edit the service information and retry.

Configure Local and Remote Collectors

This topic describes how to configure Local and Remote Collectors.

When you deploy Log Collection, you must configure the Log Collectors to collect the log events from various event sources, and to deliver these events reliably and securely to the Log Decoder service, where the events are parsed and stored for subsequent analysis.

You can configure one or more Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from one or more Remote Collectors.

This topic describes how to:

- **Configure Local Collector to Pull Events from Remote Collector**

  If you want a Local Collector to pull events from Remote Collector, you set this up in the Remote Collectors tab of the Local Collector's Configuration view.

- **Configure Remote Collector to Push Events to Local Collectors**

  If you want a Remote Collector to push events to a Local Collector, you set this up in the Local Collector tab of the Remote Collector's Configuration view. In the Push configuration, you can also:

  - **Configure Failover Local Collector for Remote Collector**

    You set up a destination made up of local collectors. When the primary Local Collector is unreachable, the Remote Collector attempts to connect to each Local Collector in this destination until it makes a successful connection.

  - **Configure Replication**

    You set up multiple destination groups so that NetWitness replicates the event data in each group. If the connection to one of the destination groups fails, you can recover the required data because it is replicated in the other destination group.

  - **Configure Log Routing for Specific Protocols**

You set up multiple destinations in a destination group to direct event data to specific locations according to protocol type.

- **Configure Chain of Remote Collectors**

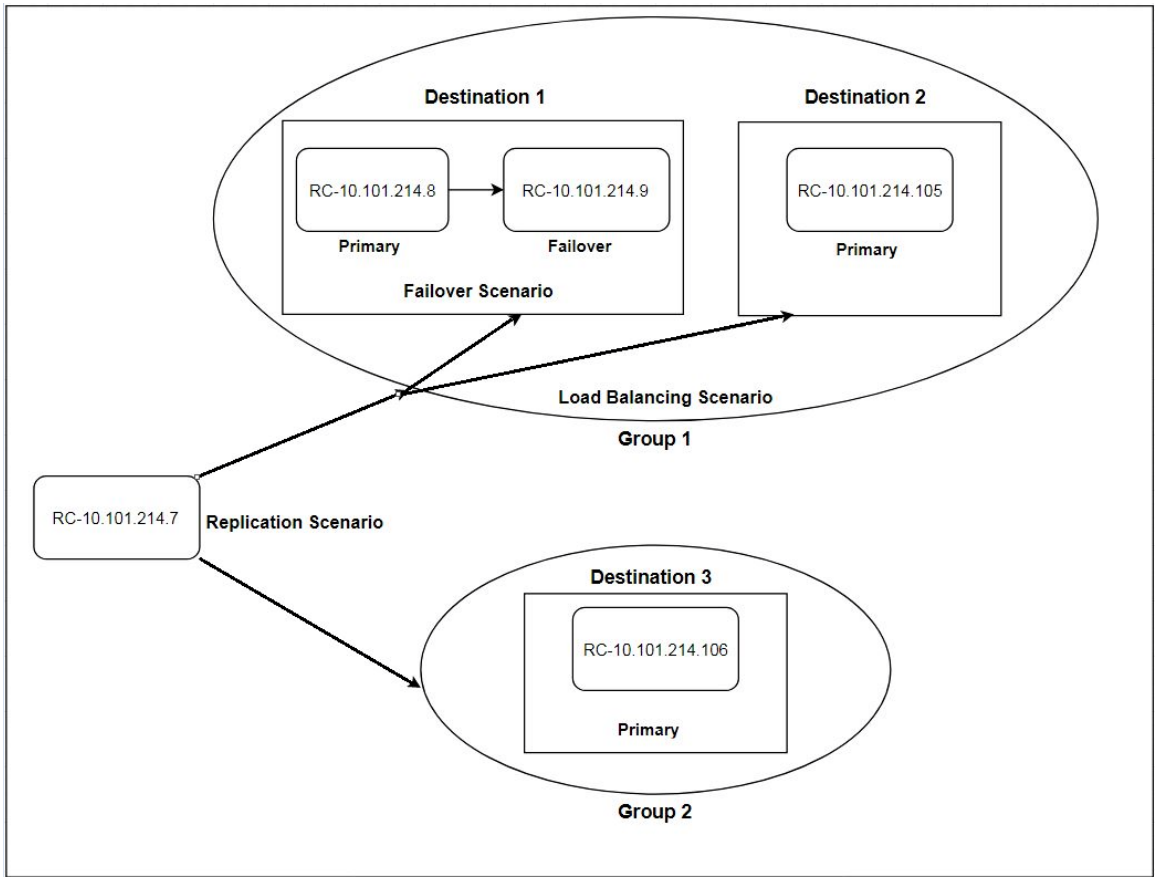
  You can set up a chain of Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from a chain of Remote Collectors.

  - You can configure one or more Remote Collectors to push event data to a Remote Collector.
  - You can configure a Remote Collector to pull event data from one or more Remote Collectors.

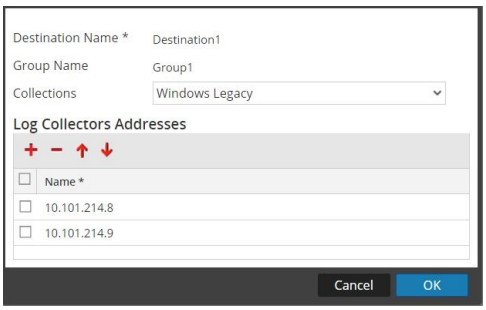
Failover, Replication and Load Balancing

This section describes failover, replication, and load balancing work in how RSA NetWitness Suite.

The following figure illustrates a Remote Collector configured for load balancing, failover and replication.

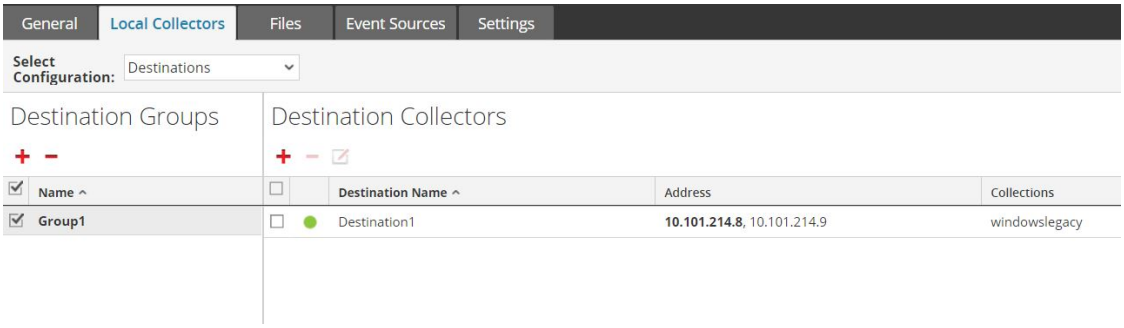


- **Failover** is achieved by setting up multiple collectors in the same Destination. Destination 1 has a primary Collector, and second, failover Collector. This is done in NetWitness Suite by adding multiple Log Collectors to the same Destination.

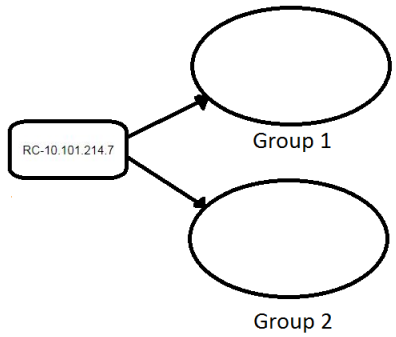


Since 10.101.214.8 is listed first, that becomes the primary collector, and 10.101.214.9 becomes the failover. To make 10.101.214.9 the primary, use the up arrow to change the order.

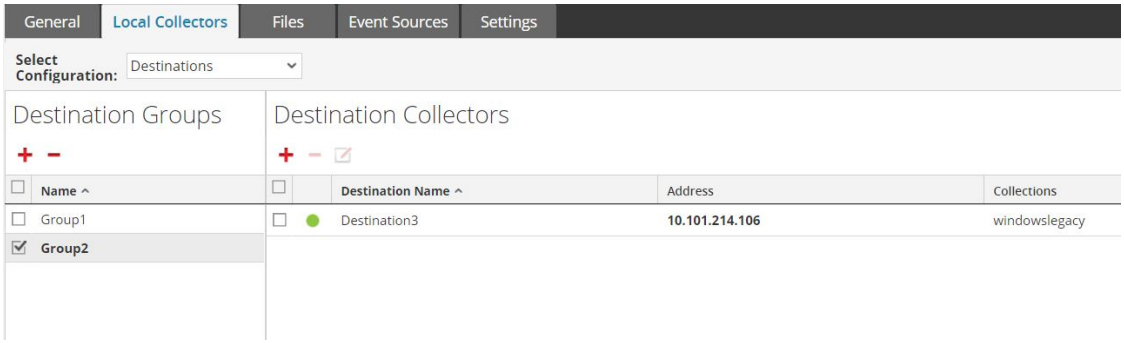
Below, you can see the two collectors both listed for Destination 1. The primary (10.101.214.8) is in bold.



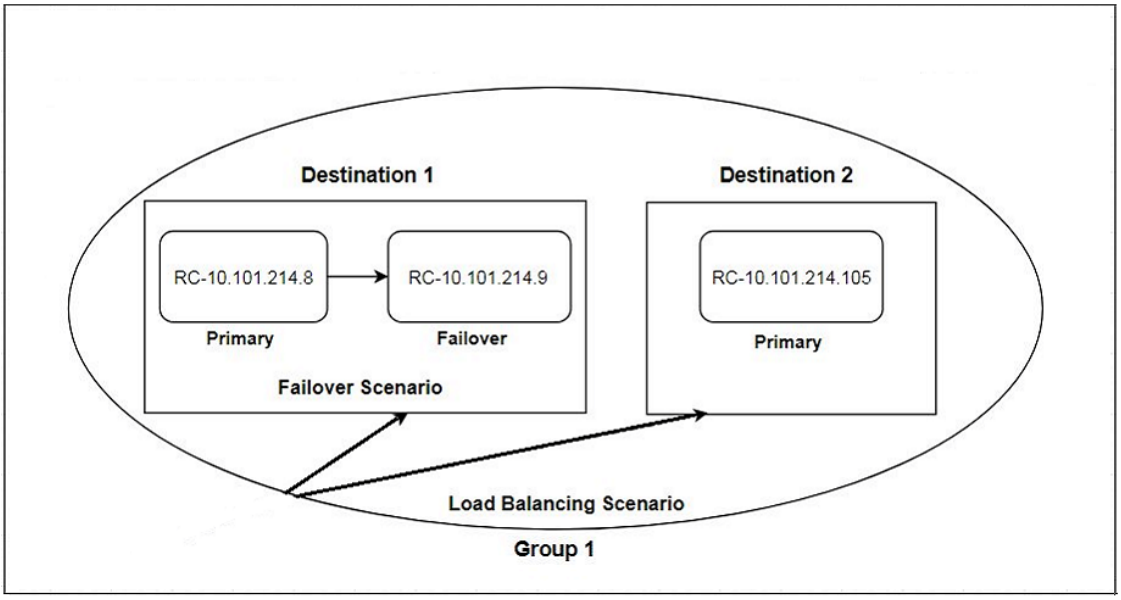
- **Replication** is accomplished by having multiple Destination Groups: each group receive the entire set of message data.



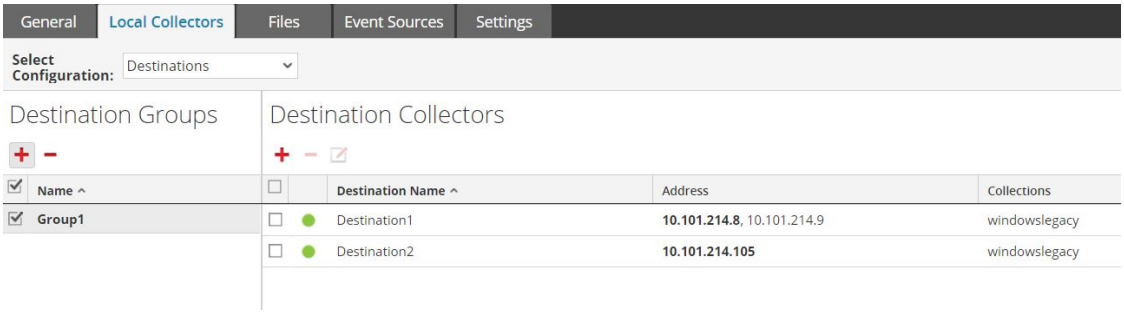
In the following screen, you can see that message data is sent to the collectors in Group 1 *and* Group 2.



- **Load balancing** is achieved by setting up multiple Destinations within a Group.



In the following screen, you can see that Group 1 has two destinations, Destination 1 and Destination 2. The message data is divided up equally among the Destinations in the group.



With two Destinations, each destination receives half the message data. With three Destinations, each would receive 1/3 of the total message data. Keep adding Destinations to further reduce the load on the collectors in each destination.

Note: You can also set up log routing so that event data for specific protocols is sent to specific destinations.

Configure a Local Collector or Remote Collector

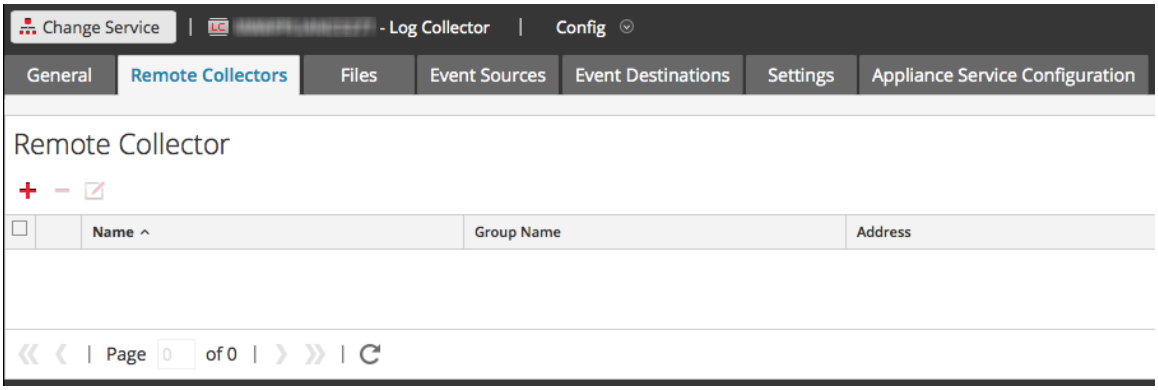
You choose the Log Collector, that is a Local Collector (LC) or Remote Collector (RC), for which you want to define deployment parameters in the Services view. The following procedure shows you how to navigate to the Services view, select a Local or Remote Collector, and display the deployment parameter interface for that service.

To configure a Local Collector or Remote Collector:

1. Go to **ADMIN > Services**.
2. Select a Local or Remote Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Depending on your selection in step 2:
   - If you selected a Local Collector, the **Remote Collectors** tab is displayed. Select the Remote Collectors from which the Local Collector pulls events in this tab.
   - If you selected a Remote Collector, the **Local Collectors** are displayed. Select the Local Collectors to which the Remote Collector pushes events in this tab.

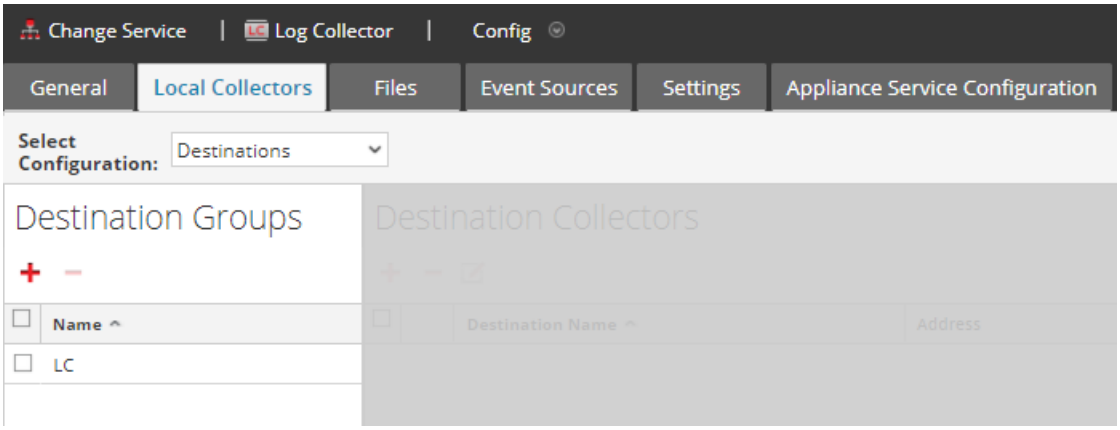
Remote Collectors Tab

The following figure depicts the **Remote Collectors** tab for a Local Collector that is configured to pull events from a Remote Collector. NetWitness Suite displays this tab when you have selected a Local Collector in **Admin > Services**.

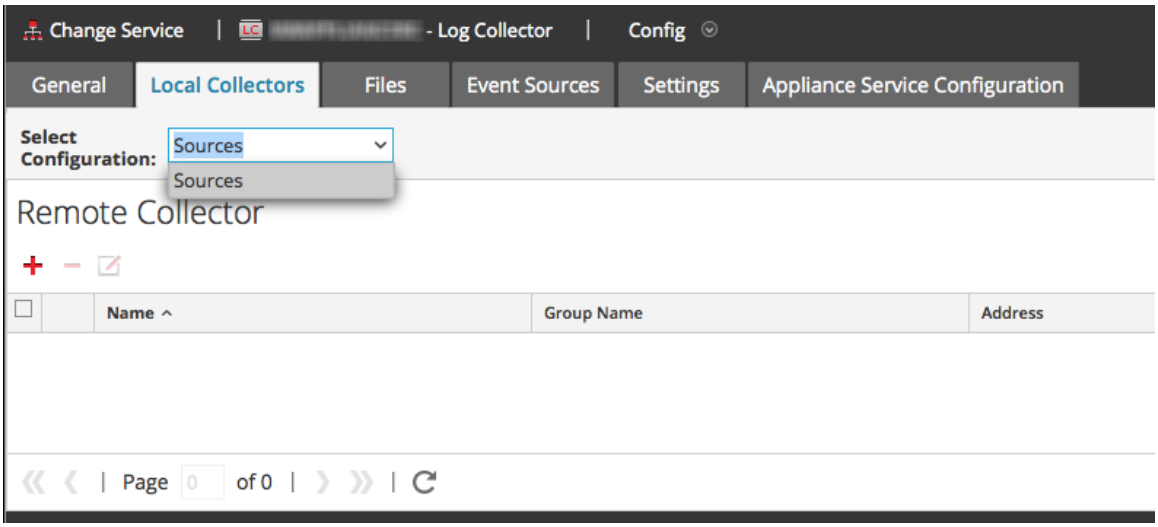


Local Collectors Tab for a Remote Collector

The following figure depicts a **Local Collectors** tab for a Remote Collector that is configured to push events to a Local Collector or another Remote Collector.



The following figure depicts the Local Collectors tab for a Remote Collector that is configured to pull events from a Remote Collector. NetWitness Suite displays this tab when you have selected a Remote Collector in **Admin > Services**.



Parameters

Remote/Local Collectors Configuration Parameters

Configure Failover Local Collector

This topic tells you how to set up a Failover Local or Remote Collector.

Set up a Failover Local Collector

You can set up a Failover Local Collector that RSA NetWitness® Suite will fail over to if your primary Local Collector stops operating for any reason.

1. Go to **ADMIN> Services**.
2. In **Services**, select a Remote Collector service.
3. Click under **Actions** and select **View > Config**.

   The Service Config view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. In the **Destination Groups** panel section, select .

   The Add Remote Destination dialog displays.
6. Set up a Destination Group and select a primary Local Collector (for example, **LC-PRIMARY**).
7. Select the Group (for example, **Primary_Standby_LCs**) in the Destination Groups panel and click .

   The Group you selected is displayed in the Local Collectors panel.
8. Add the Failover Local Collector (for example, **LC-STANDBY**).

   The following examples show the newly added primary and failover Local Collectors showing the primary Local Collector as **Active** and the Failover Local Collector as **Standby**. The active Local Collector is highlighted (for example, **LC-PRIMARY**).
9. (Optional) Add, delete, and change the order of Local Collectors to each Remote Destination.
   a. Click to add a Log Collector as a failover Remote Destination.
   b. When connecting to a Remote Destination, the Remote Collector will attempt to connect to each Local Collector in this list in order, until it makes a successful connection.
   c. Select a Local Collector and use the up ( ) and down ( ) arrow buttons to change the order of connection.
   d. Select one or more Local Collectors and click to remove them from the list.

   The selected Local Collectors are added to the Log Collector section. When the Remote Collector starts collecting data, it pushes data to these Log Collectors.

Set up a Failover Remote Collector

You can set up a Failover Remote Collector that RSA NetWitness® Suite will fail over to if your primary Remote Collector stops operating for any reason.

1. Go to **ADMIN > Services**.
2. In **Services**, select a Remote Collector service.

3. Click under **Actions** and select **View > Config**.

   The Service Config view is displayed with the **Log Collector General** tab open.

4. Select the **Local Collectors** tab.
5. Select **Sources** in **Select Configuration** drop-down menu.
6. Click to display in **Add Source** dialog.
7. Define the failover Remote Collector and click **OK**.

Parameters

Remote/Local Collectors Configuration Parameters

Configure Replication

This topic tells you how to replicate event data sent by a Remote Collector.

You can specify multiple Destination Groups so that the event data is replicated to each group.

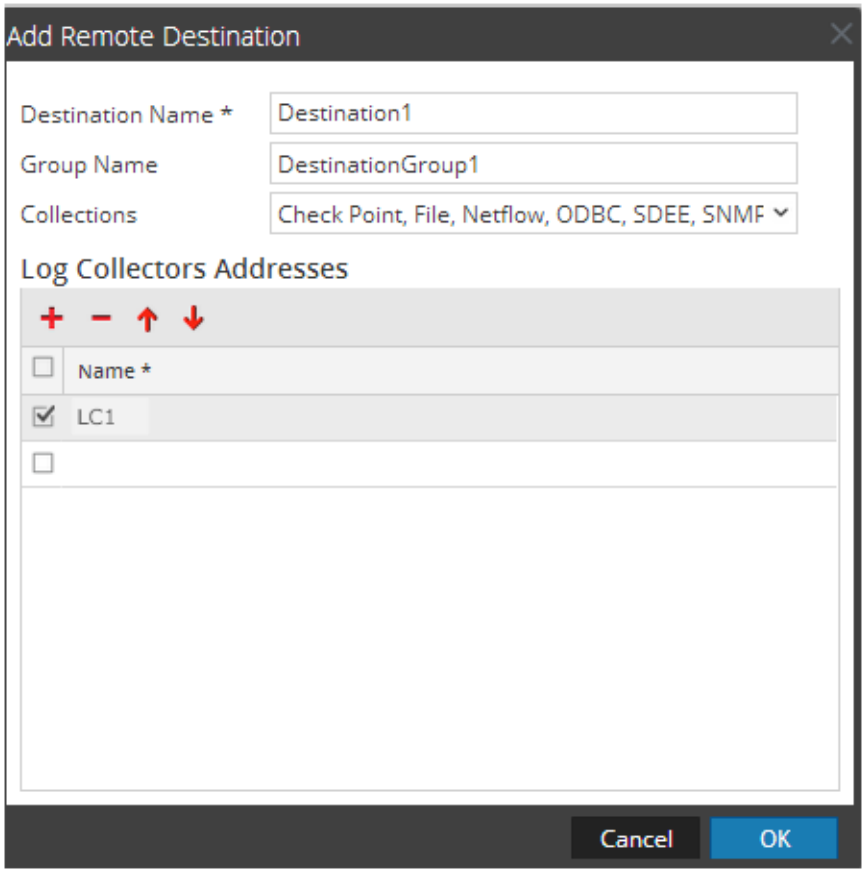
To replicate event data to multiple Local Collectors:

1. Go to **ADMIN > Services.**
2. Select a Remote Log Collection service.
3. Under Actions, select **> View > Config**.

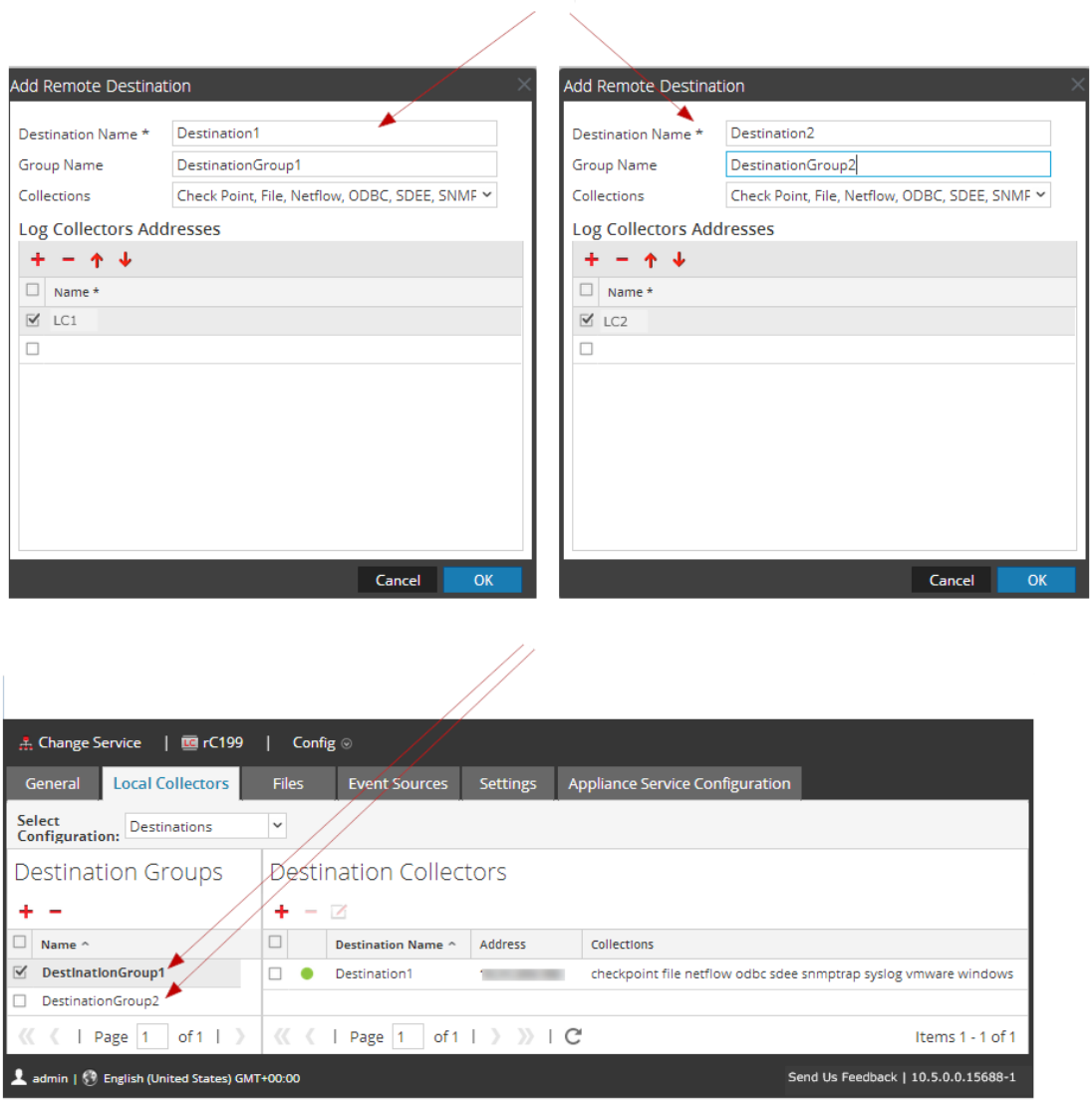
   The Service Config view is displayed with the **Log Collector General** tab open.

4. Select the **Local Collectors** tab.
5. In the **Destination Groups** panel section, click .

   The **Add Remote Destination** dialog is displayed.



6. Set up a separate Destination for each Local Collector and designate the protocols for which you want to push event messages to that Local Collector. The following examples shows the addition of two Destination Local Collectors (**Destination1** and **Destination2**) for the **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog**, and **Windows** collection protocols:



a. Type the **Destination Name**.

b. Type the **Group Name**. If you do not type a Group Name, the Destination Name is taken as the Group Name.

c. Select the collection protocols in the drop-down list.

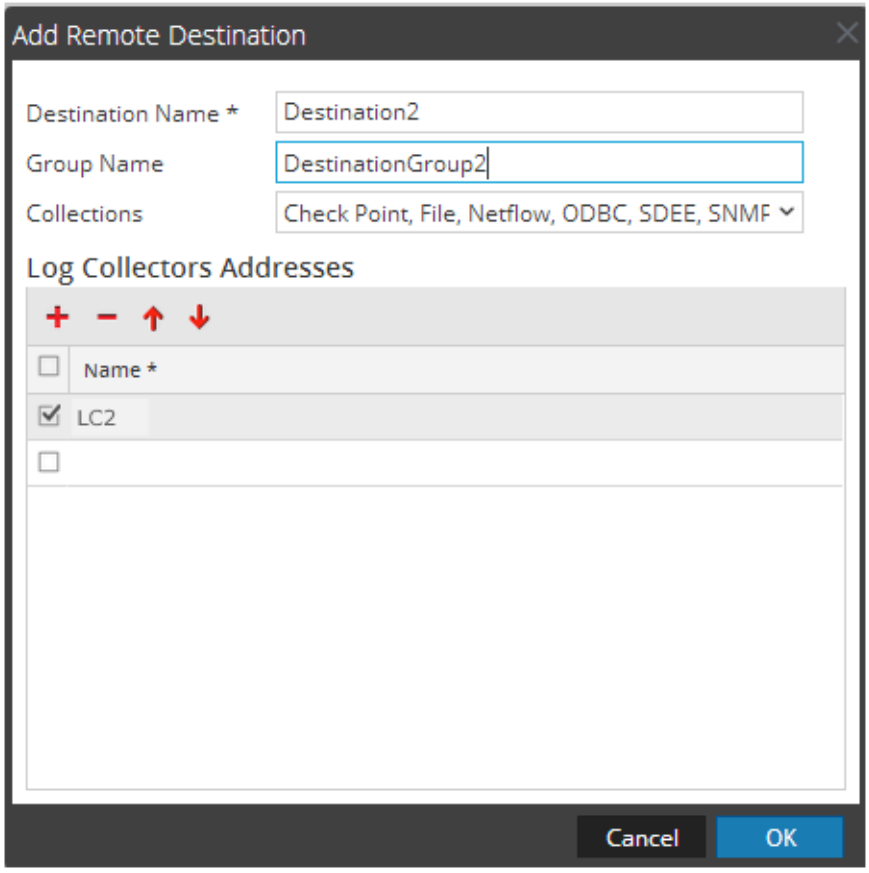
d. Select a Local Collector (for example, **LC1**).

e. Click **OK**.

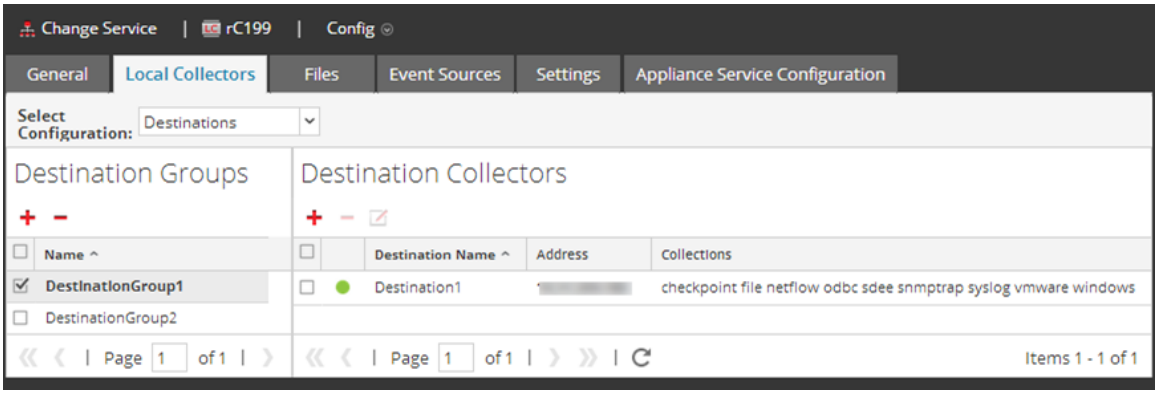
f. Select the new group (for example, **DestinationGroup2**) group in the **Destination Groups** panel and click + in the **Local Collector** panel.

g. In the **Local Collector** panel, click + and complete the **Add Remote Destination**

dialog as illustrated in the following figure.



The **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog**, and **Windows** collection protocols are sent to two Local Collectors (**LC1** and **LC2**). Both Local Collectors are active and collecting event data.



Configure Chain of Remote Collectors

This topic describes how to chain Remote Collectors (also referred to as VLCs).

You can set up a chain of Remote Collectors to push event data to a Remote Collector, or you can configure a Remote Collector to pull event data from a chain of Remote Collectors.

- **Remote Collectors to push data.** Push data from a Remote Collector to other Remote Collectors or Local Collectors.
- **Remote Collector to pull data.** Use a Remote Collector to pull data from one or more Remote Collectors.

Configure Remote Collector to Push Event Data to Remote Collector

You can configure a Remote Collector to push event data to a Remote Collector.

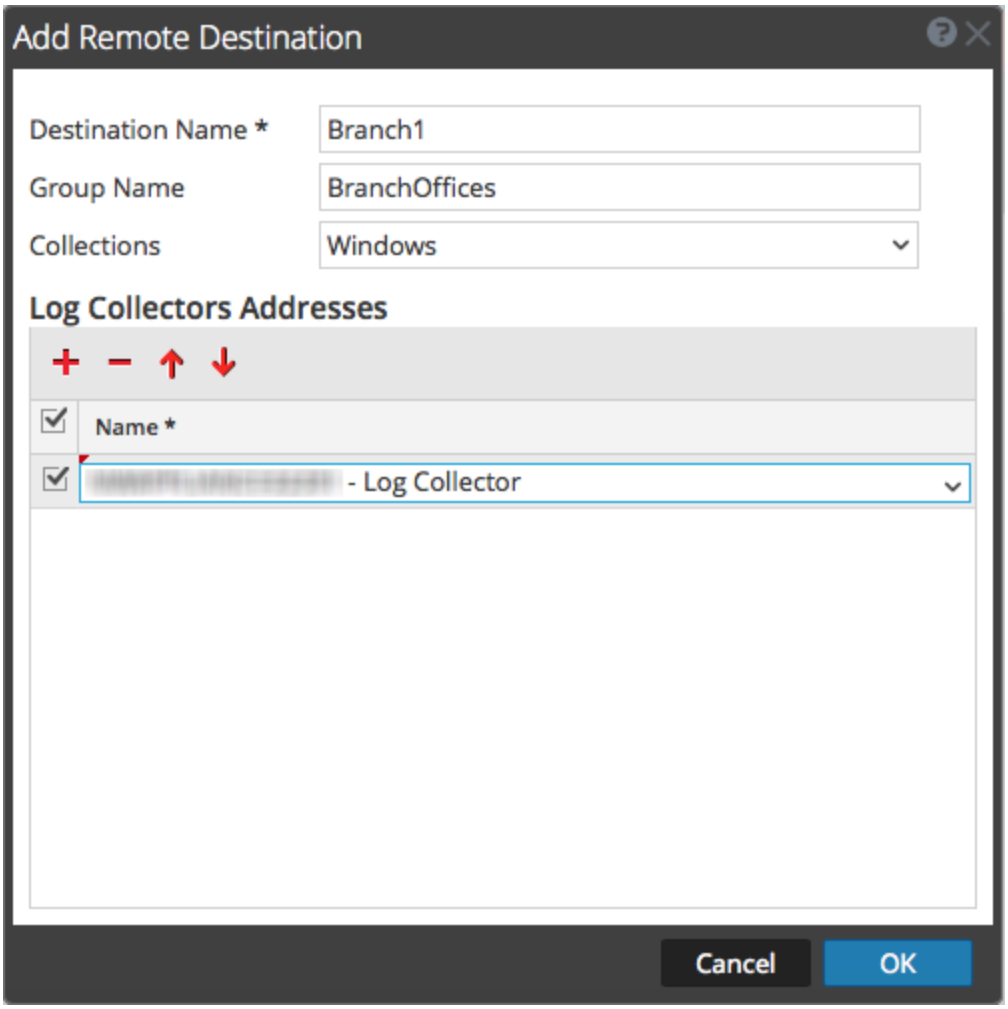
Configure a Remote Collector to Push Events to Specified Remote Collector

1. Go to **ADMIN > Services.**
2. In **Services**, select a **Remote Collector**.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

   The **Log Collector Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. Select **Destinations** in the **Select Configurations** drop-down menu.
6. In the **Destination Groups** panel section, select .

   The **Add Remote Destination** dialog is displayed.
7. Set up a **Destination Group**:
   a. Enter a **Destination Name**.
   b. (Optional) **Enter a Group Name**. If you leave Group Name blank, NetWitness Suite sets it to the value that you specified in Destination Name.
   c. Select one or more collection protocols in the **Collections** drop-down list.

d. Under **Log Collectors Addresses**, click + to select a Remote Collector.



Note: If you do not select a collection protocol, the Remote Collector pushes all collection protocols to the Remote Collectors.

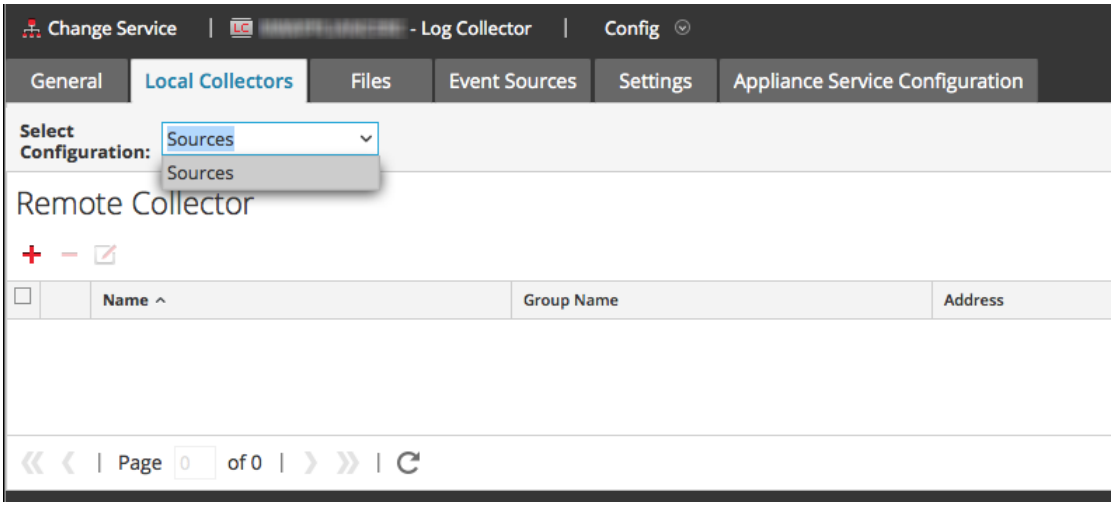
Configure Remote Collector to Pull Event Data from a Remote Collector

Configure the Selected Remote Collector to Pull Events from Specified Remote Collector

1. Go to **ADMIN > Services.**
2. In **Services**, select a **Remote Collector**.
3. Under Actions, select ⚙ **> View > Config** to display the Log Collection configuration parameter tabs.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.

5. Select **Sources** in the **Select Configurations** drop-down menu.



6. In the **Remote Collectors** panel, select +.

   The **Add Source** dialog is displayed.

7. In the **Add Source** dialog:

   a. Select one or more collection protocols.

      If you do not select a collection protocol, the Remote Collector pulls all collection protocols from the Remote Collector.

   b. Click **OK**.

      The Remote Collector is added to the Remote Collector section. When the Log Collector starts collecting data, it pulls event data from this Remote Collector.

Throttle Remote Collector to Local Collector Bandwidth

To improve performance, you can throttle the bandwidth to control the rate that the Remote Collector sends event data to Local Collector or between Message Brokers. To do this, you configure the Linux kernel's filtering and IPTable functionality.

This works for both push and pull Remote Collector configurations. The **set-shovel-transfer-limit.sh** shell script located on the **/opt/netwitness/bin** automates the configuration of the kernel filter and iptables related to this port.

This topic describes how to throttle Remote Collector to Local Collector bandwidth using the **set-shovel-transfer-limit.sh** shell script. It contains the following sections:

- The **set-shovel-transfer-limit.sh** shell script command line help.

> **Note:** The filter value that you need to set depends on the rate at which remote log

collector is sending events to the Local Collector.

- An example that sets the Filter to 4096 kilobits per second.

Command Line Help for Set Shovel Transfer Limit Script

Issue the `-h` command to display help for `set-shovel-transfer-limit.sh` shell script.

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

Usage:

```
code>set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r
rate]
```

where:

- -c = clear existing
- -d = display filter
- -s = set new values
- -i = interface is the name of the network interface. Default value is **eth0**
- -r = rate is the bandwidth rate. Default value is **256kbps**

Bandwidths and rates can be specified in:

- **nolimit**: disables throttling
- **kbit**: Kilobits per second
- **mbit**: Megabits per second
- **kbps**: Kilobytes per second
- **mbps**: Megabytes per second
- **bps**: Bytes per second

Set the Filter to 4096 Kilobits per Second

This example sets the Filter to 4096 kilobits per second.

```
[root@<hostname> bin]#./set-shovel-transfer-limit.sh -s -r
4096kbit
```

```
RATE=4096kbit
 PORTNUMBER=5671
 DEVICE_INTERACE=eth0
```

```
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK
]

Current/new values...

iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source
destination

Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source          destination

Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0     0.0.0.0/0
multiport dports 5671 MARK set 0xa
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0    0.0.0.0/0
multiport sports 5671 MARK set 0xa

Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination

tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000

class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Set Up a Lockbox

This topic tells you how to configure Lockbox Security Settings.

What Is a Lockbox

A lockbox is an encrypted file that you use to store confidential information about an application. The NetWitness Suite Lockbox stores an encryption key for the Log Collector.

The encryption key is used to encrypt all event source passwords and the event broker password.

When you create the Lockbox, you need to define a password for the Lockbox.

TheLog Collector operates the Lockbox in a mode during data collection that does not require you to specify the password (theLog Collector uses the host system fingerprint instead).

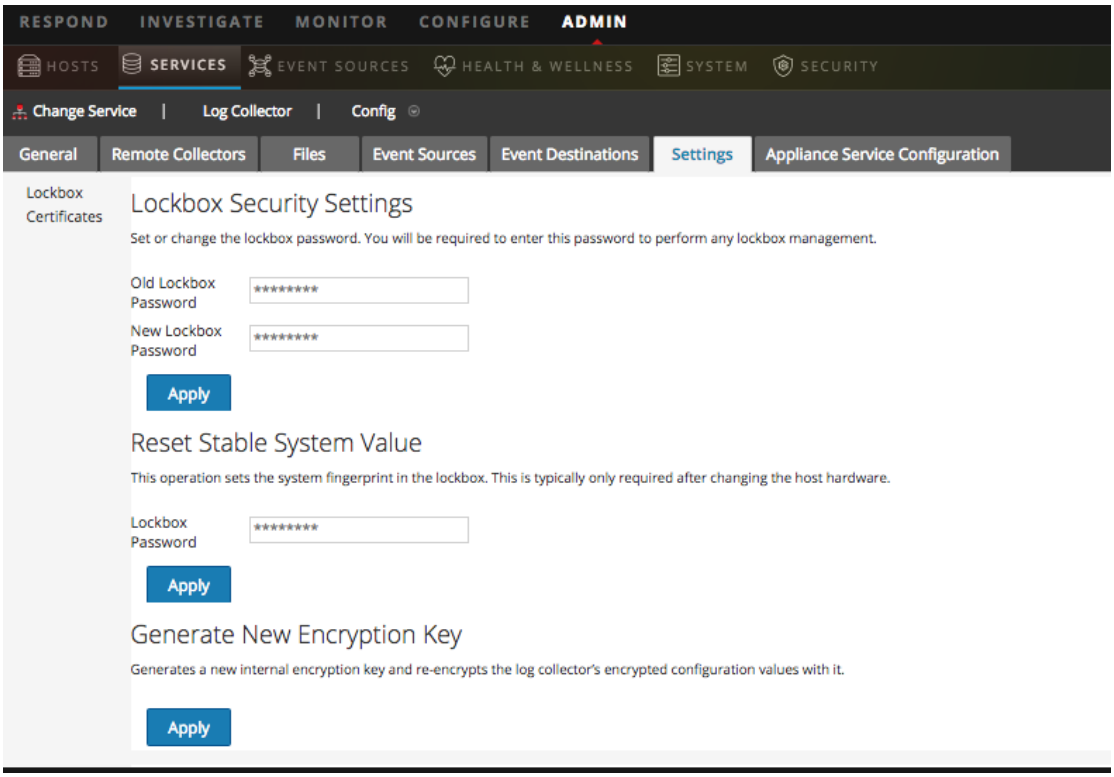
These are the lockbox security settings.

Feature	Description
Old Lockbox Password	When you set up a Lockbox for the first time, this field is blank. NetWitness Suite populates this field after you enter a New Lockbox Password and click Apply.
New Lockbox Password	Initial or new lockbox password. To maximize lockbox security, specify a password that is eight or more characters in length with at least one numeric character, uppercase character, and non-alphanumeric character such as # or !
Apply	Click **Apply** to save the changes to the lockbox password.

Set Up a Lockbox

To set up a lockbox you need to set a password, as follows:

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Settings** tab.



5. In the options panel, select **Lockbox** to configure Lockbox settings.
6. Under **Lockbox Security Settings**, enter a password in the **New Lockbox Password** field and click **Apply**.

Start Collection Services

If a collection service stops, you may need to start it again. You can also enable the automatic start of collection services.

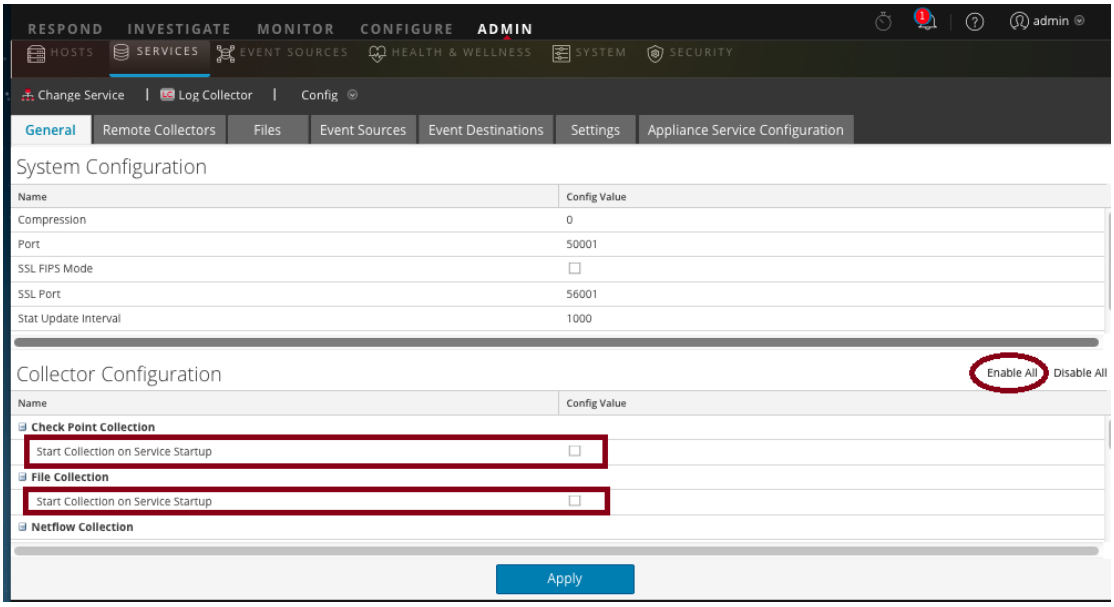
Start a Collection Service

1. Go to **ADMIN > Services**.
2. Select a Log Collector service and click under **Actions**.
3. Click **View** > **System**.
4. Click **Collection** > ***service*** (for example **File**) and click **Start**.

Enable Automatic Start of Collection Services

1. Go to **Admin > Services**.
2. Select a Log Collector service and click under **Actions**.
3. Click **View** > **Config**.

   The General tab is displayed.
4. In the Collector Configuration panel, select **Start Collection on Service Startup** for the individual collection services that you want to start automatically. Alternatively, select **Enable All** to automatically start all collection services.



5. Click **Apply** for your changes to take effect.

Verify That Log Collection Is Working

This topic tells you how to verify that you have set up Log Collection correctly.

The following methods verify that Log Collection is working.

- Verify that there is event activity the Event Source Monitoring tab of the **Administration > Health & Wellness** view.
- Verify that there are parsers in the **device.type** field in the **Details** column in the **Investigation > Events** view for the collection protocol you configured.

Please refer to the topics for each Collection Protocol for steps on how to verify that the protocol is set up correctly.

Configure Certificates

You manage certificates by creating trust stores on the Log Collector. The Log Collector refers to these trust stores to determine whether or not the event sources are trusted.

Add a Certificate

To add a certificate:

1. Go to **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click under **Actions** and select **View > Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Certificates**.
6. Click in the **Certificates** tool bar.

   The **Add Cert** dialog is displayed.
7. Click **Browse** and select a certificate (***.PEM**) from your network.
8. Specify a password (if required).
9. Click **Save**.

Certificates Panel

The following table describe the buttons and columns available in the Certificates panel.

Field	Description
	Opens the Add Cert dialog in which you can add a certificate and password.
	Deletes the selected certificates.
	Selects certificates.
Trust Store Name	Displays the name of the trust store.
Certificate Distinguished Name	For Check Point event source only, displays the distinguished name for the certificate.

Field	Description
Certificate Password Name	For Check Point event source only, displays the password name for the certificate.

Add Cert Dialog

The following table describes the parameters available in the **Add Cert** dialog.

Field	Description
Trust Store Name	Enter a trust store name.
File	Click Browse to select a certificate (*.PEM file) file from your network
Password	Specify the password for this certificate.
Close	Closes the dialog without adding a certificate.
Save	Adds the certificate.

Log Collection Basics

How Log Collection Works

The Log Collector service collects logs from event sources throughout the IT environment in an organization and forwards the logs to other NetWitness Suite components. The logs and the descriptive content are stored as meta data for use in investigations and reports.

Event sources are the assets on the network, such as servers, switches, routers, storage arrays, operating systems, and firewalls. In most cases, your Information Technology (IT) team configures event sources to send their logs to the Log Collector service and the NetWitness Suite administrator configures the Log Collector service to poll event sources and retrieve their logs. As a result, the Log Collector receives all logs in their original form.

Collection Protocols

RSA NetWitness Suite can collect logs from a wide variety of event sources. When you are configuring log collection for a specific event source, you need to know, first and foremost, the protocol that is used to collect the logs.

Collection Protocol	Description
Check Point	Collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs. For details, see Configure Check Point Event Sources in NetWitness Suite.
File	Collects events from log files. Event sources generate log files that are transferred using a secure file transfer method to the Log Collector service. For details, see Configure File Event Sources in NetWitness Suite.
Netflow	Accepts events from Netflow v5 and Netflow v9. For details, see Configure Netflow Event Sources in NetWitness Suite.
ODBC	Collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface. For details, see Configure ODBC Event Sources in NetWitness Suite.

Collection Protocol	Description
Plugins	The Plugins collection is a generic collection framework for collecting events using external scripts written in other languages. RSA currently provides collection for Amazon Web Services (AWS) CloudTrail and Microsoft Azure. • **AWS**: Collects events from Amazon Web Services (AWS) CloudTrail. Specifically CloudTrail records AWS API calls for an account. For details, see Configure AWS (CloudTrail) Event Sources in NetWitness Suite • **Azure**: Collects events from Microsoft Azure. For details, see Configure Azure Event Sources in NetWitness Suite. Customers can use this framework to develop their own collection protocols.
SDEE	Collects Intrusion Detection System (IDS) and Intrusion Prevention Service (IPS) messages. For details, see Configure SDEE Event Sources in NetWitness Suite.
SNMP Trap	Accepts SNMP traps. For details, see Configure SNMP Event Sources in NetWitness Suite.
Syslog	Accepts messages from event sources that issue syslog messages. For details, see Configure Syslog Event Sources for Remote Collector. **Note:** You do not configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors.
VMware	Collects events from a VMware virtual infrastructure. For details, see Configure VMware Event Sources in NetWitness Suite.
Windows	Collects events from Windows machines that support the Microsoft Windows model. Windows 6.0 is an event logging and tracing framework included in the operating system beginning with Microsoft Windows Vista and Windows Server 2008. For details, see Configure Windows Event Sources in NetWitness Suite.

Collection Protocol	Description
Windows Legacy	Collects events from: • Older Windows versions such as Windows 2000 and Window 2003 and collects from Windows event sources that are already configured for enVision collection without having to reconfigure them. • NetApp ONTAP appliance event source so that you can now collect and parse NetApp evt files. • For more information, see.Windows Legacy and NetApp Collection Configuration. **Note:** You install the NetWitness Suite Windows Legacy Collector on a physical or virtual Windows 2008 R2 SP1 64-Bit server using the **SALegacyWindowsCollector-*version-number.exe***.

Basic Procedure

The basic procedure is the same for all of the supported Collection Protocols.

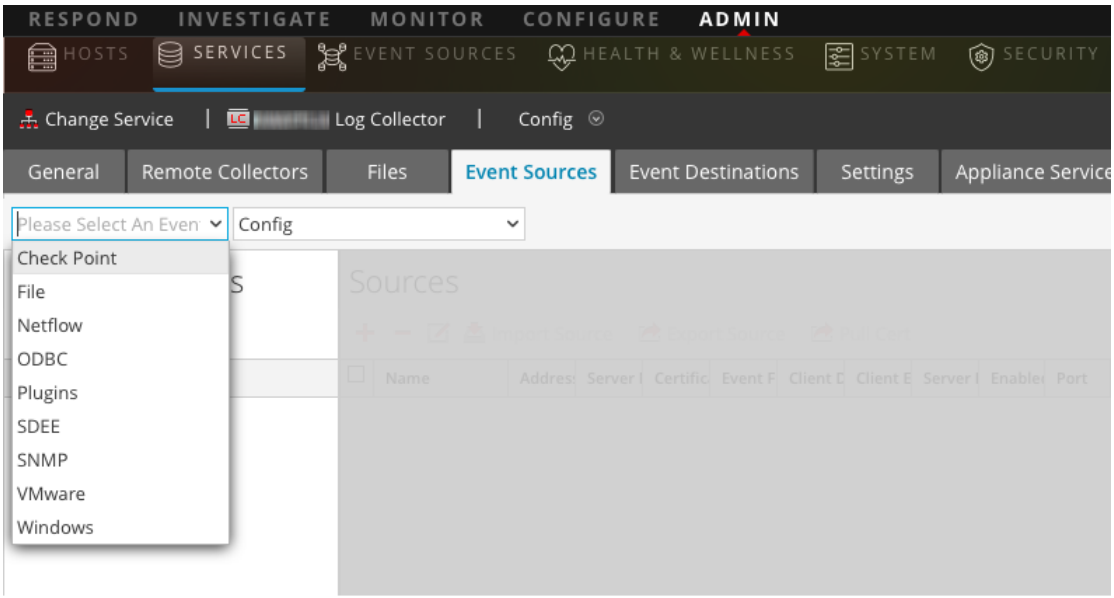
1. **Set up your Event Source for collection.** Each supported event source has a configuration document available in the RSA Supported Event Sources space on RSA Link
   a. Navigate to the RSA Supported Event Sources space on RSA Link.
   b. Find the Instructions for your Event Source.
      The Overview page lists all of the currently supported Event Sources, as well as information about the collection method, device class, and supported versions.
   c. Download the configuration instructions for your event source, and follow them.
2. **Configure collection on RSA NetWitness Suite.** The event source configuration guide contains these instructions. However, this guide also provides these instructions, based on the collection method used by your event source. See Collection Protocols for details.
3. **Start the Service for your Collection Method.** Normally, you only need to do this for the first event source that uses this collection method. For example, the first time you configure an event source that uses File Collection, you may need to start the File Service in NetWitness Suite.
4. **Verify that Collection is working for your Event Source.**

The remainder of this topic discusses steps 2, 3, and 4 in more detail.

Configure Collection in RSA NetWitness Suite

The process to configure event sources is dependent upon the collection method they use. Note, however, that they are very similar. The following procedure is generic: more details for individual collection methods are available in topics that cover the details for each specific collection method.

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. In the **Log Collector Event Sources** tab, select your collection method from the drop-down menu.
6. In the **Event Categories** panel toolbar, click .

   The Available Event Source Types dialog box is displayed.
7. Select an event source type and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.
8. Select the new type in the **Event Categories** panel and click in the Sources toolbar.

   The **Add Source** dialog is displayed.

9. Enter values for the available parameters.

   Refer to the Parameters section of the specific collection method that you are configuring.

10. Click **OK**.

Start the Service for your Collection Method

To start the service for your collection method, do the following:

1. Go to **Admin > Services**.
2. Select a **Log Collector** and select **> View > System**.
3. Click **Collection >** ***protocol*****> Start**

   where ***protocol*** is the protocol that you wish to start, for example **Netflow**.

Verify that Collection is working for your Event Source

You can verify that a collection method is working from the **Admin > Health & Wellness > Event Source Monitoring** tab.

To verify that collection is working for an event source:

1. Go to **ADMIN > Health & Wellness**
2. Click the **Event Source Monitoring** tab.
3. In the grid, find the **Log Decoder**, **Event Source**, and **Event Source Type**.
4. Look for activity in the **Count** column for an event source to verify that collection is accepting events.

Configure Event Filters for a Collector

This topics tells you how to create and maintain Event filters across all collection protocols.

Note: You cannot configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors. See Configure Local and Remote Collectors for additional configuration information.

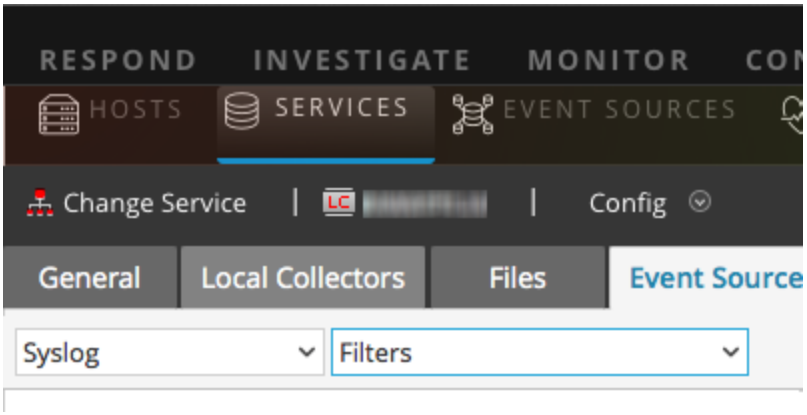
Configure an Event Filter

To configure an event source:

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.

3. Under Actions, select **View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. In the **Event Sources** tab, select any collection method / **Filter** from the drop-down menus.

   The following screen shows **Syslog** selected.

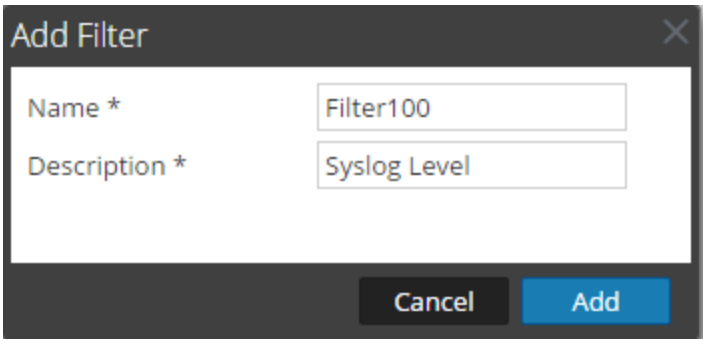


Note: Syslog configuration is only available on Remote Collectors: if you are working with a Local Collector service, **Syslog** is not available from the drop-down menu.

   The **Filters** view displays the filters that are configured for the selected collection method, if any.

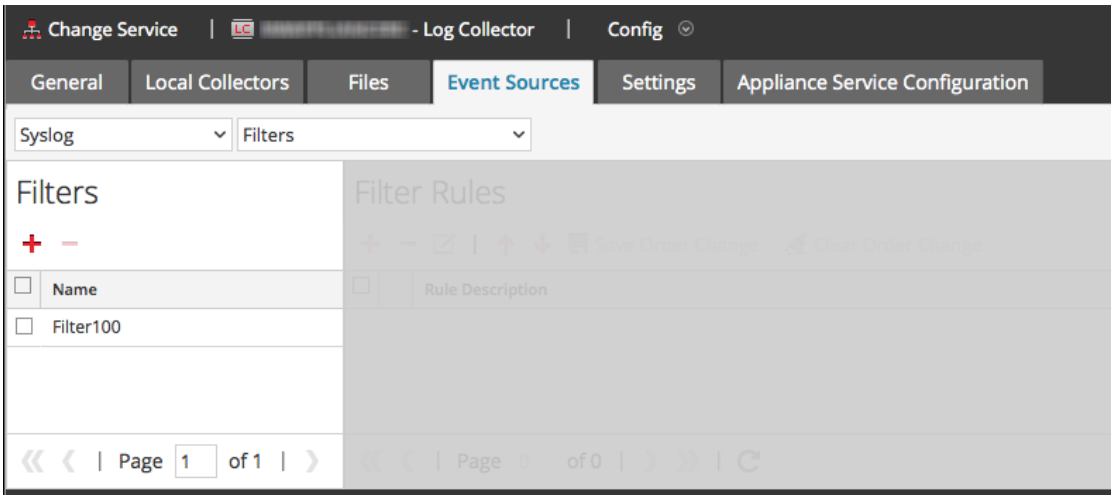
6. In the **Filters** panel toolbar, click +.

   The **Add Filter** dialog displays.



7. Enter a name and description for the new filter and click **Add**.

   The new filter displays in the **Filter** panel.

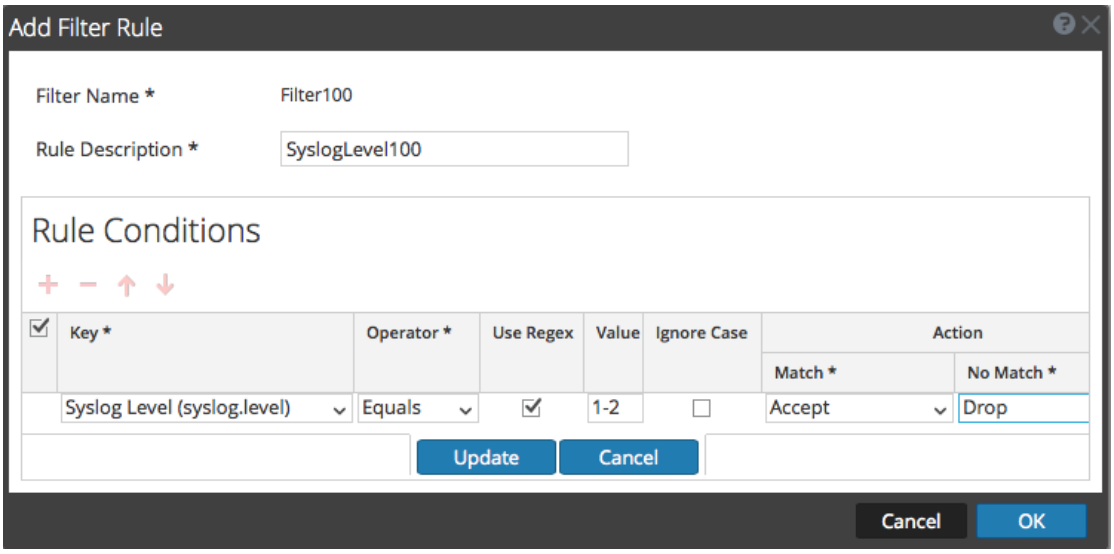


8. Select the new filter in the **Filters** panel and click + in the **Filter Rules** panel toolbar.

   The **Add Filter Rule** dialog is displayed.

9. Click + under **Rule Conditions**.

10. Add the parameters for this rule and click **Update** > **OK**.



NetWitness Suite updates the filter with the rule that you defined.

Note: Rules are processed in order from top down until an Action type aborts the processing, or the final rule is checked. Default behavior is to accept the rule if no matches are found.

The following tables describe the parameters for adding a filter rule.

Event Filter Rule "Key" Parameter

The values for the Key field depend on the Collection method to which the filter applies.

Collection Method	Values for the *Key* Field
Checkpoint, File, Netflow, Plugin, SDEE SNMP and VMware	• All Data Fields • Event Source Type • Event Source Name • Source IP • Raw Event
ODBC	• All Data Fields • Event Source Type • Event Source Name • Source IP • Message ID • Message Level
Syslog	• All Data Fields • Event Source Type • Event Source Name • Source IP • Syslog level • Raw Event

Collection Method	Values for the *Key* Field
Windows	• All Data Fields • Event Source Type • Event Source Name • Source IP • Event ID • Provider • Channel • Computer • UserName • DomainName
Windows Legacy	• All Data Fields • Event Source Type • Event Source Name • Source IP • Event ID

Other Event Filter Rule Parameters

The following table describes all the other available fields for creating an event filter rule.

Field	Description
Operator	Valid values are: • Contains • Equal
Use Regex	Optional. You can select this if you want to use regex.
Value	Value depends on the key value you selected. For example if you choose **Syslog level** for Key, the value will be a number that denotes the syslog level.

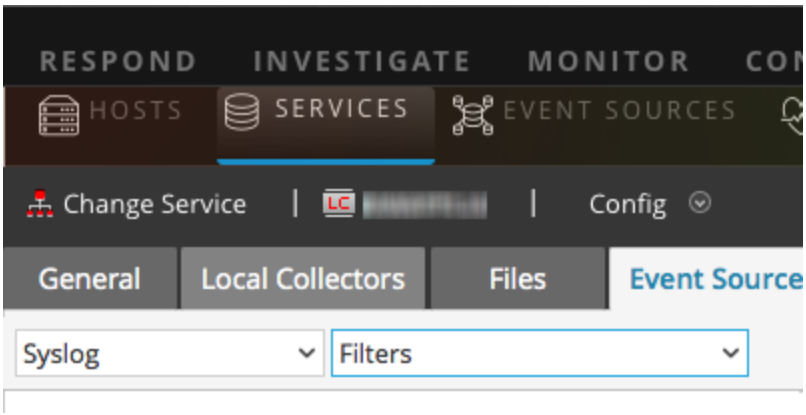
Field	Description
Ignore case	Optional. Select this to ignore the case sensitivity.
Action	If there is a match you can choose an action to accept, drop, next condition or next rule: • **Accept**: events that match the IDs provided will be included in event logs, and will display in the Systems Analytics UI. • **Drop**: events that match the IDs provided will not be included in event logs and will not display in the UI. • **Next condition**: the filter will ignore events with IDs that match, and will move on to the next rule condition. • **Next rule**: the filter will ignore events with IDs that match, and will move on to the next rule. If there is no match, you can choose an action to accept, drop, next condition or next rule.

Modify Filter Rules

To modify an event source:

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.
3. Under Actions, select **View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. In the **Event Sources** tab, select any collection method / **Filter** from the drop-down menus.

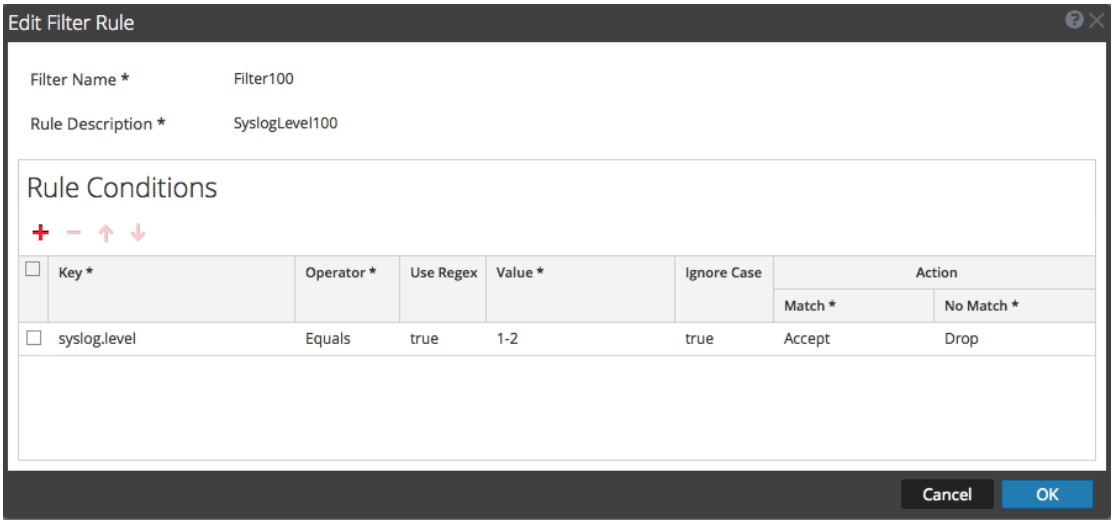
   The following screen shows **Check Point** selected.



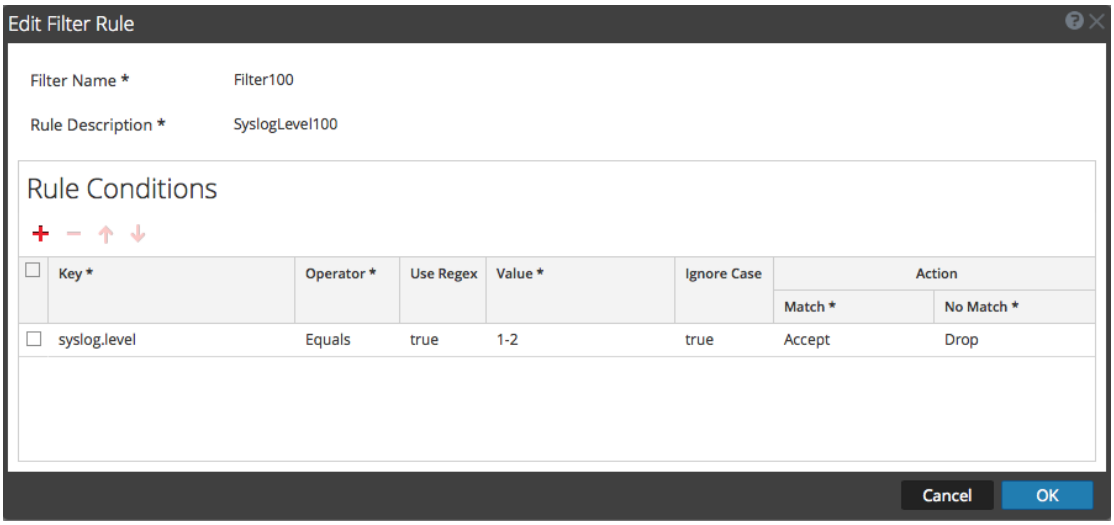
The **Filters** view displays the filters that are configured for the selected collection method, if any.

6. In the **Filter Rules** list, select a rule and click .

   The **Edit Filter Rule** dialog is displayed.



7. Select the rule condition that you want to modify.



8. Modify the condition parameters that require changes and click **Update** > **OK**.

NetWitness Suite applies the condition parameter changes to the selected filter rule.

Import, Export, Edit and Test Event Sources in Bulk

This topic describes how to import, export, edit and test event sources in bulk.

You can use the bulk export option to export the event source details of your current set up and store it. This data can be imported in bulk when you face a problem with your current set up and require the event source data you had.

You can use the bulk edit feature when you have multiple event sources that need a specific modification. You can select all the sources and apply the edit option across them at a time and avoid applying the change one by one.

Import Event Sources in Bulk

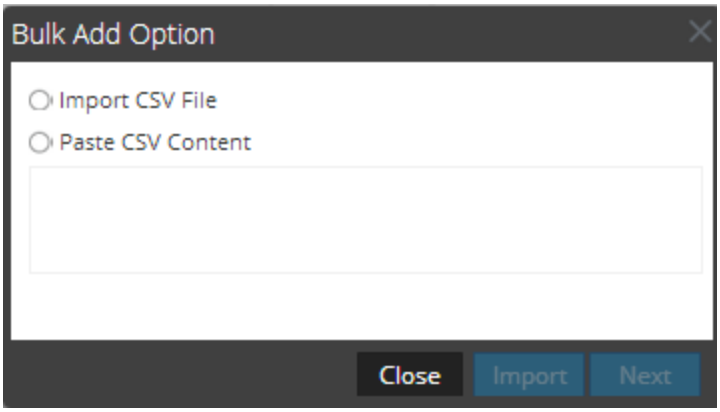
Warning: When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly. This can be avoided by importing the CSV file into the spreadsheet program, and specifying all data fields as text values.

To import multiple event sources at once:

1. Go to **Admin** > **Services**.
2. Select a Log Collection service.
3. Under Actions, select > **View** > **Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.
5. Select **Check Point**, **File**, **Netflow**, **ODBC**, **Plugins**, **SDEE**, **(Syslog for Remote Collectors) only**, **VMware**, **Windows**, or **Windows Legacy** (SNMP does not have an Import function.).
6. In the **Sources** panel toolbar, click **Import Source**.

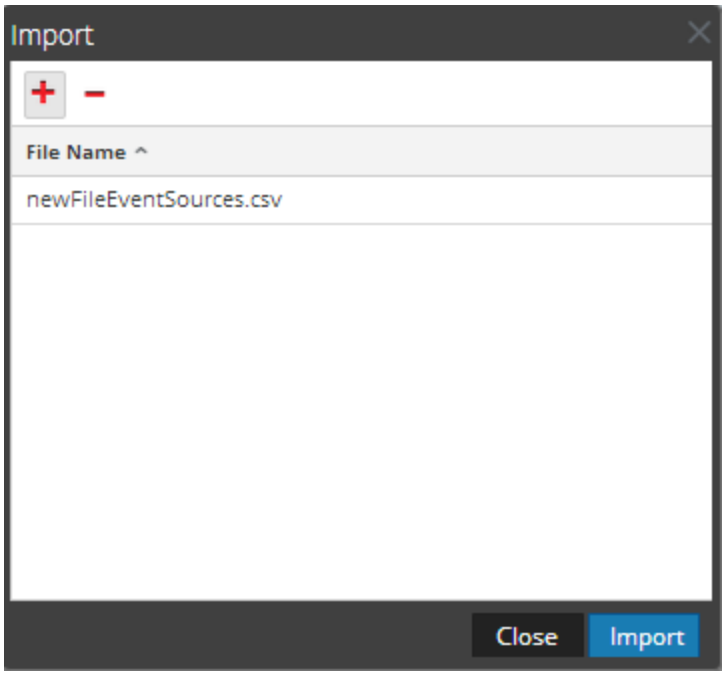
   The **Bulk Add Option** dialog is displayed.



7. Select either **Import CSV File** or **Paste CSV Content**. If you select:
   - Import CSV File:
     a. Click **Next**.

        The **Import dialog** is displayed.

     b. Click **Add** and select a **.csv** file from your network.

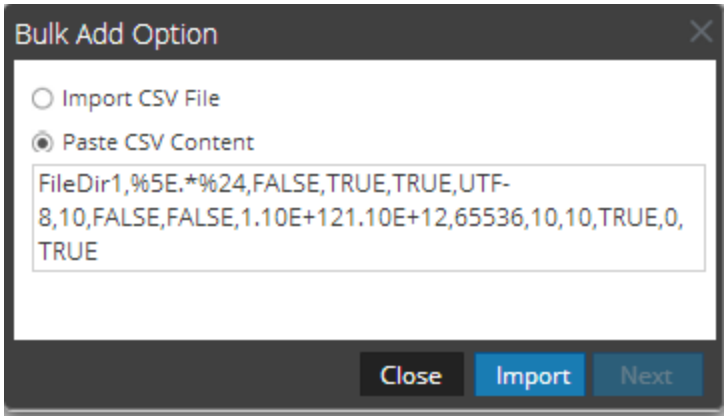


c. Click **Import**.

The event sources are added to the **Event Source** list.

- Paste CSV Content

a. Copy the contents of the **.csv** file and paste them into the dialog.



b. Click **Import**.

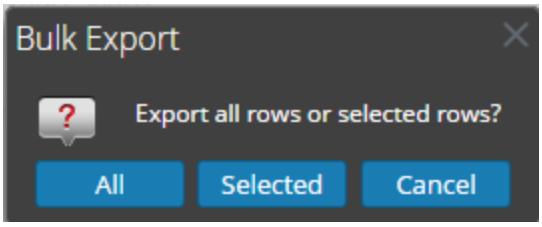
The event sources are added to **Event Source List**.

Export Event Sources in Bulk

Warning: When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly. This can be avoided by importing the CSV file into the spreadsheet program, and specifying all data fields as text values.

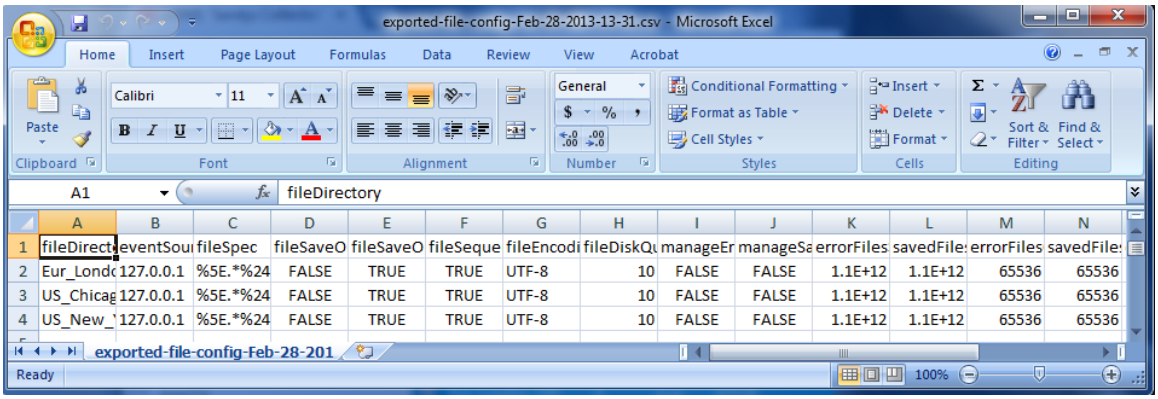
1. Go to **Admin** > **Services**.
2. Select a Log Collection service.
3. Under Actions, select > **View** > **Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. Select **Check Point**, **File**, **Netflow**, **ODBC**, **Plugins**, **SDEE**, **(Syslog for Remote Collectors) only**, **VMware**, **Windows**, or **Windows Legacy** (SNMP does not have an Export function.).
6. In the **Sources** panel, select one or multiple event sources and click **Export Source**.

   The **Bulk Export** dialog is displayed.



7. Based on your selection:
   - **All**, NetWitness Suite exports all event sources to a time-stamped CSV file.
   - **Selected**, NetWitness Suite exports the event source or sources you selected to a time-stamped CSV file.
   - **Cancel**, NetWitness Suite cancels the export.

   The following is an example of a time-stamped CSV file that gets created with the event sources that you selected from the list.

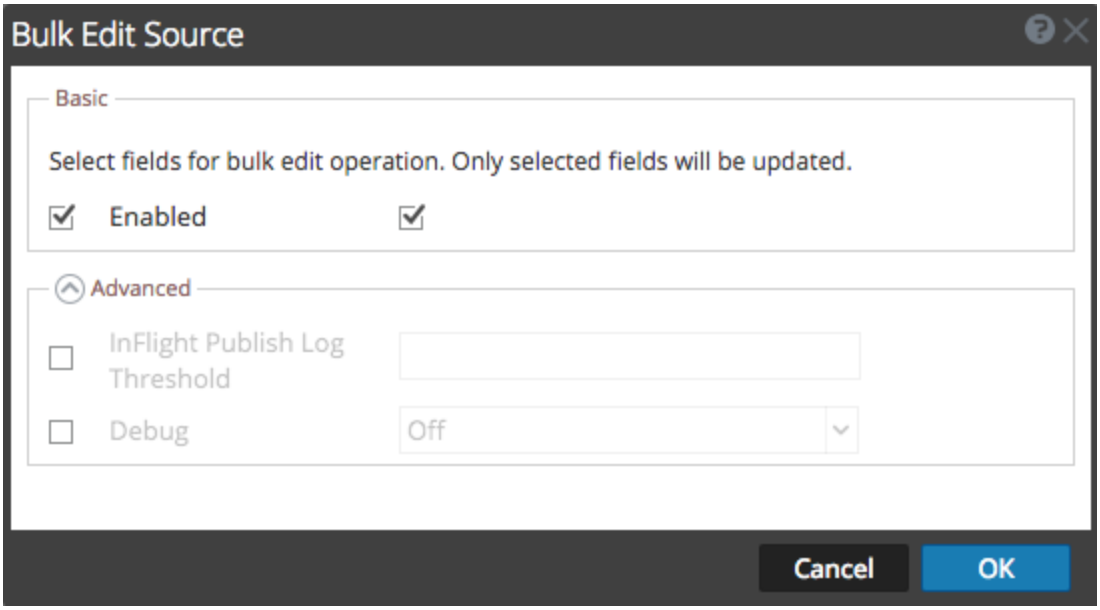


Edit Event Sources in Bulk

To edit multiple event sources at once:

1. On the **Log Collector Event Sources** tab, select **Check Point**, **File**, **Netflow**, **ODBC**, **Plugins**, **SDEE**, **Syslog**, **VMware**, **Windows**, or **Windows Legacy** (SNMP does not have an Edit function.).
2. In the **Sources** panel, select multiple event sources and click (edit icon).

   The appropriate **Bulk Edit** dialog for the selected event source is displayed. The following figure is an example of **Bulk Edit Source** dialog for File event source parameters.



3. Select the checkbox to the left of the fields that you want to modify (for example, **Debug**).
4. Modify the selected parameters (for example, change Debug from **Off** to **On**).
5. Click **OK**.

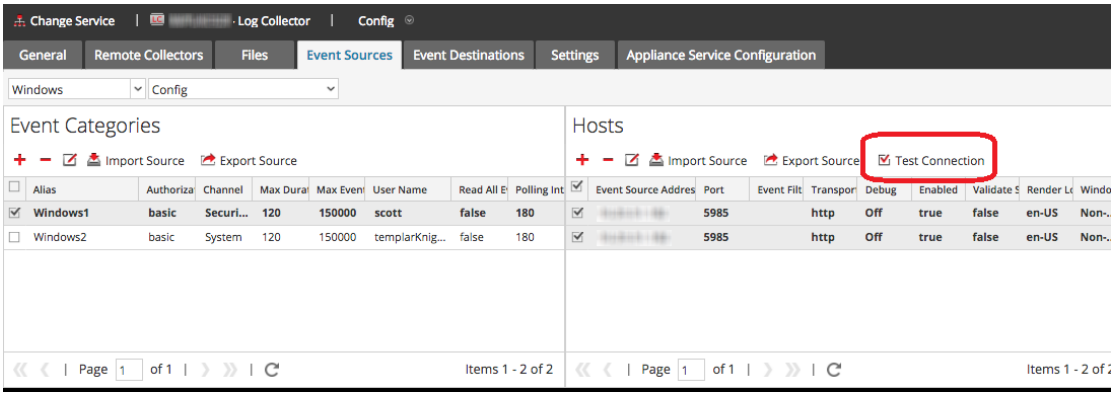
NetWitness Suiteapplies the same parameter value change to all of the selected event sources

Test Event Source Connections in Bulk

To test multiple event source connections at once:

1. Go to **Admin** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Under Actions, select > **View** > **Config** to display the Log Collection configuration parameter tabs.
4. Select the **Event Sources** tab, select **Plugins**, **ODBC**, or **Windows** (the other protocols do not have a bulk test connection function).
5. Select one or more:
   - sources from the **Sources** panel for **Plugins** or **ODBC**
   - hosts from **Hosts** panel for **Windows**

   The **Test Connection** button is enabled.



6. Click Test Connection.

   The **Bulk Test Connections** dialog is displayed showing the current status of the test for each source. The status can be waiting, testing, passed or failed.

   If you choose to close the testing before it is completed, the testing stops and the **Bulk Test Connections** dialog closes.

After the testing is complete, the results are displayed in the **Bulk Test Connections** dialog.

See Also

You can use the **Event Sources** module (Administration > Event Sources) to create groups of event sources, typically imported from a CMDB, and to monitor event sources based on those groups. For details, see the following topics in the *Event Source Management Guide*:

- Import Event Sources
- Export Event Sources
- Bulk Edit Event Source Attributes

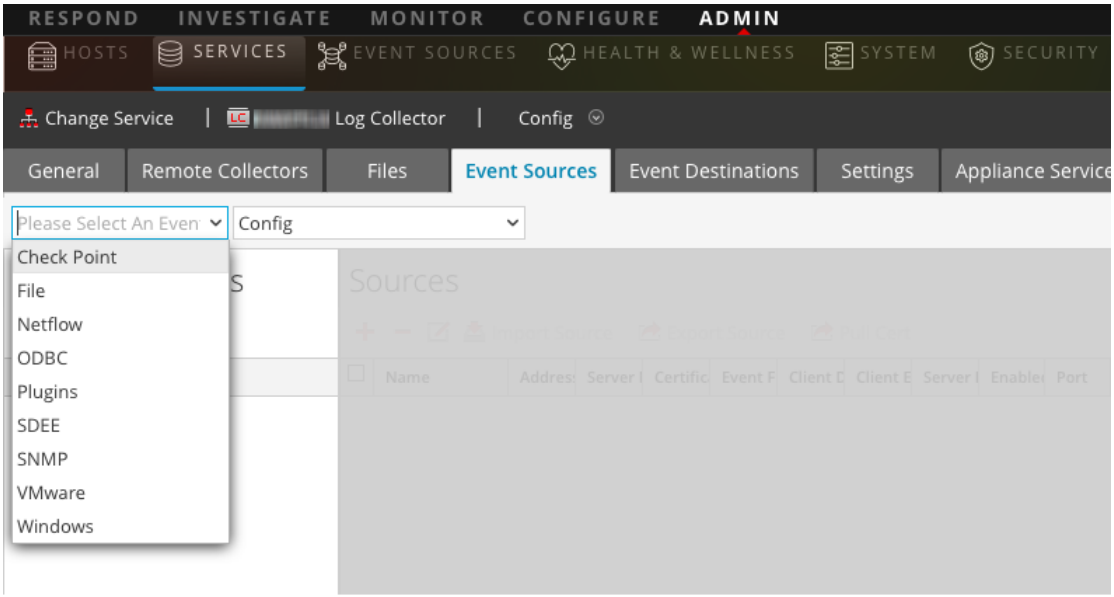
Configure Collection Protocols and Event Sources

This topic tells you how to configure collection protocols and the event sources using those protocols.

You configure the Log Collector to collect event data from your event sources in the Event Sources tab of the Log Collection parameter view.

To configure a collection protocol:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. Select a collection protocol (for example, **File**) and select **Config**.
6. Click + and select an event source.
7. Select the newly added category and click +.
8. Specify the parameters for the event source. For details, see the individual collection protocol topics.

The following guides provide detailed instructions on how to configure the collection protocols and their associated event sources in NetWitness Suite. Each guide includes an index to configuration instructions for the event sources supported for that collection protocol.

To configure individual collection protocols, see the following topics:

- Configure AWS (CloudTrail) Event Sources in NetWitness Suite
- Configure Azure Event Sources in NetWitness Suite
- Configure Check Point Event Sources in NetWitness Suite
- Configure File Event Sources in NetWitness Suite
- Configure Netflow Event Sources in NetWitness Suite
- Configure ODBC Event Sources in NetWitness Suite
  - Configure Data Source Names (DSNs)
  - Create Custom Typespec for ODBC Collection
  - ODBC Event Source Configuration Parameters
  - ODBC DSNs Event Source Configuration Parameters
- Configure SDEE Event Sources in NetWitness Suite
- Configure SNMP Event Sources in NetWitness Suite
- Configure Syslog Event Sources for Remote Collector
- Configure VMware Event Sources in NetWitness Suite
- Configure Windows Event Sources in NetWitness Suite
- Windows Legacy and NetApp Collection Configuration
  - Set Up the Windows Legacy Collector
  - Configure Windows Legacy and NetApp Event Sources
  - Troubleshoot Windows Legacy and NetApp Collection

Configure AWS (CloudTrail) Event Sources in NetWitness Suite

This topic tells you how to configure the AWS collection protocol, which collects events from Amazon Web Services (AWS) CloudTrail.

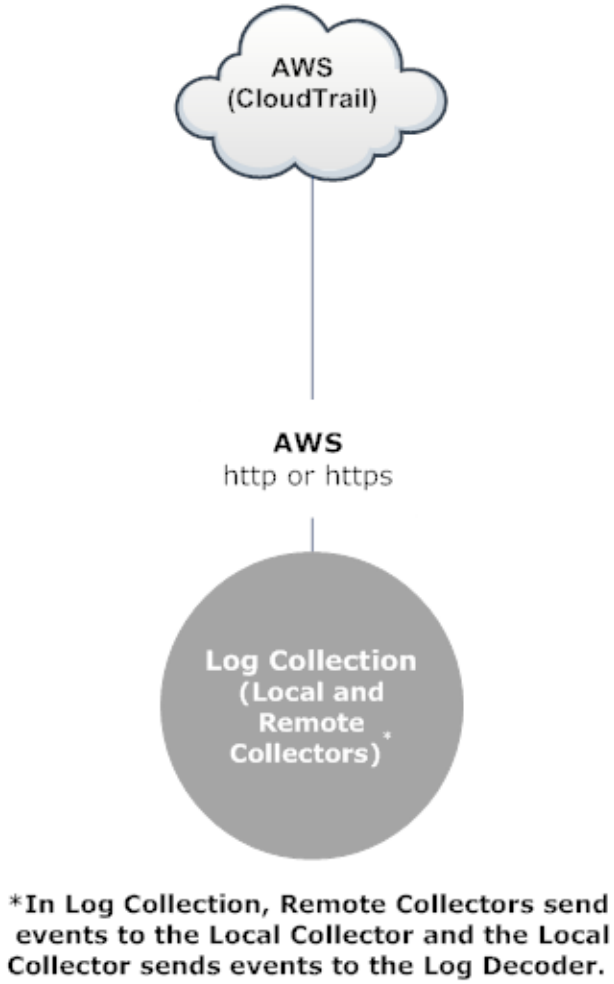
Note: The AWS plugin is meant only for collecting from AWS CloudTrail logs, and not for collecting from arbitrary logs in S3 buckets (under arbitrary directories). The AWS CloudTrail logs are sent in JSON format, as detailed in the AWS documentation here: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html.

How AWS Collection Works

The Log Collector service collects events from Amazon Web Services (AWS) CloudTrail. CloudTrail records AWS API calls for an account. The events contain the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. The AWS API call history provided by CloudTrail events enables security analysis, resource change tracking, and compliance auditing. CloudTrail uses Amazon S3 for log file storage and delivery. NetWitness Suite copies the log files from the cloud (S3 bucket), and sends the events contained in the files to the Log Collector.

Deployment Scenario

The following figure illustrates how you deploy the AWS Collection Protocol in NetWitness Suite.

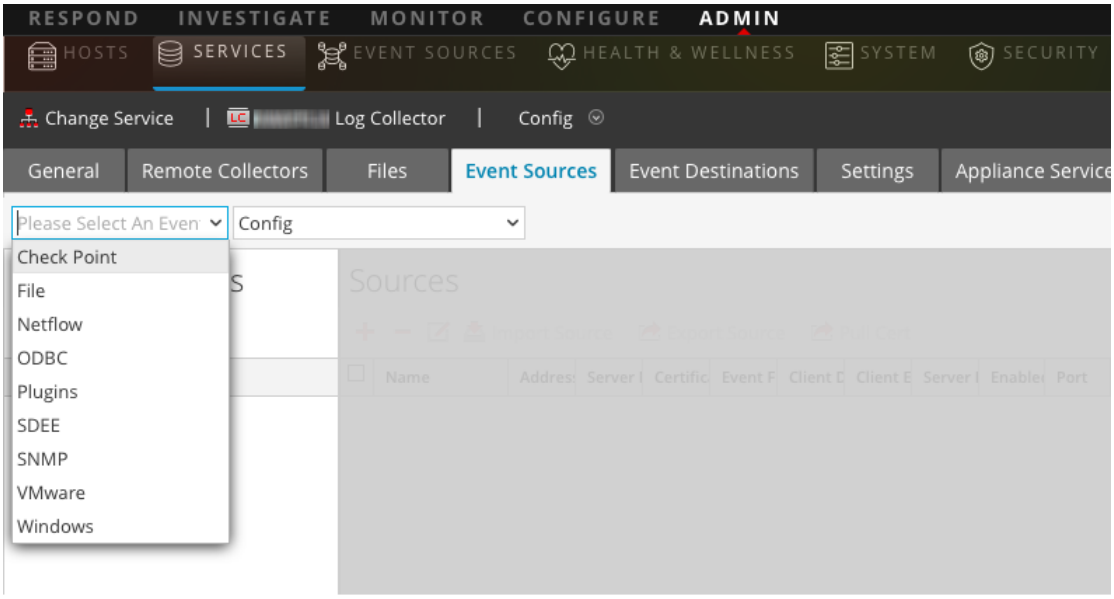


Configuration

To configure an AWS (CloudTrail) Event Source:

1. Go to **ADMIN > Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.
7. Select **cloudtrail**) and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.
8. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.
9. Define parameter values. For details, see AWS Parameters below.
10. Click **Test Connection**.

    The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

    Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the NetWitness Suite displays an error message.
11. If the test is successful, click **OK**.

    The new event source is displayed in the **Sources** panel.

AWS Parameters

The following table describes the available configuration parameter for AWS collection.

Parameter	Description
Parameter	**Description**
	Basic
Name *	Name of the event source.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Account Id *	Account Identification code of the S3 Bucket
S3 Bucket Name *	Name of the AWS (CloudTrail) S3 bucket. Amazon S3 bucket names are globally unique, regardless of the AWS (CloudTrail) region in which you create the bucket. You specify the name at the time you create the bucket. Bucket names should comply with DNS naming conventions. The rules for DNS-compliant bucket names are: • Bucket names must be at least three and no more than 63 characters long. • Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period “.”. Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number. • Bucket names must not be formatted as an IP address (for example, 192.168.5.4). The following examples are **valid** bucket names: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** The following examples are **invalid** bucket names: • **.myawsbucket** - Do not start a Bucket Name with a period ".". • **myawsbucket.** - Do not end a Bucket Name with a period ".". • **my..examplebucket** - Only use one period between labels.

Parameter	Description
Access Key *	Key used to access the S3 bucket. Access Keys are used to make seure REST or Query protocol requests to any AWS service API. Please refer to Manage User Credentials on the Amazon Web Services support site for more information on Access Keys.
Secret Key *	Secret key used to access the S3 bucket.
Region *	Region of the S3 bucket. **us-east-1** is the default value.
Region Endpoint	Specifies the AWS CloudTrail hostname. For example, for an AWS public cloud for us-east region, the Region Endpoint would be s3.amazonaws.com. More information can be found at http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. This parameter is necessary to collect CloudTrail logs from AWS Government or Private clouds.
Use Proxy	Enable **Use Proxy** to set proxy for AWS server. By default, it is disabled.
Proxy Server	Enter the proxy name you want to connect to access the AWS server.
Proxy Port	Enter the port number that connects to the proxy server to access the AWS server.
Proxy User	Enter the user name to authenticate with the proxy server.
Proxy Password	Enter the password to authenticate with proxy port.
Start Date *	Starts AWS (CloudTrail) collection from the specified number of days in the past, measured from the current timestamp. The default value is 0, which starts from today. The range is 0–89 days.
Log File Prefix	Prefix of the files to be processed. **Note:** If you set a prefix when you set up your CloudTrail service, make sure to enter the same prefix in this parameter.
Advanced	

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Command Args	Arguments added to the script.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 60. For example, if you specify 60, the collector schedules a polling of the event source every 60 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 60 seconds for the polling to start because the threads are busy.
SSL Enabled	Select the check box to communicate using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The check box is selected by default.

Parameter	Description
Test Connection	Validates the configuration parameters specified in this dialog are correct. For example, this test validates that: • NetWitness can connect with the S3 Bucket in AWS using the credentials specified in this dialog. • NetWitness can download a log file from the bucket (test connection would fail if there were no log files for the entire bucket, but this would be extremely unlikely).
Cancel	Closes the dialog without adding the AWS (CloudTrail).
OK	Adds the current parameter values as a new AWS (CloudTrail).

Configure Azure Event Sources in NetWitness Suite

This topic tells you how to configure the Azure collection protocol. Microsoft Azure is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

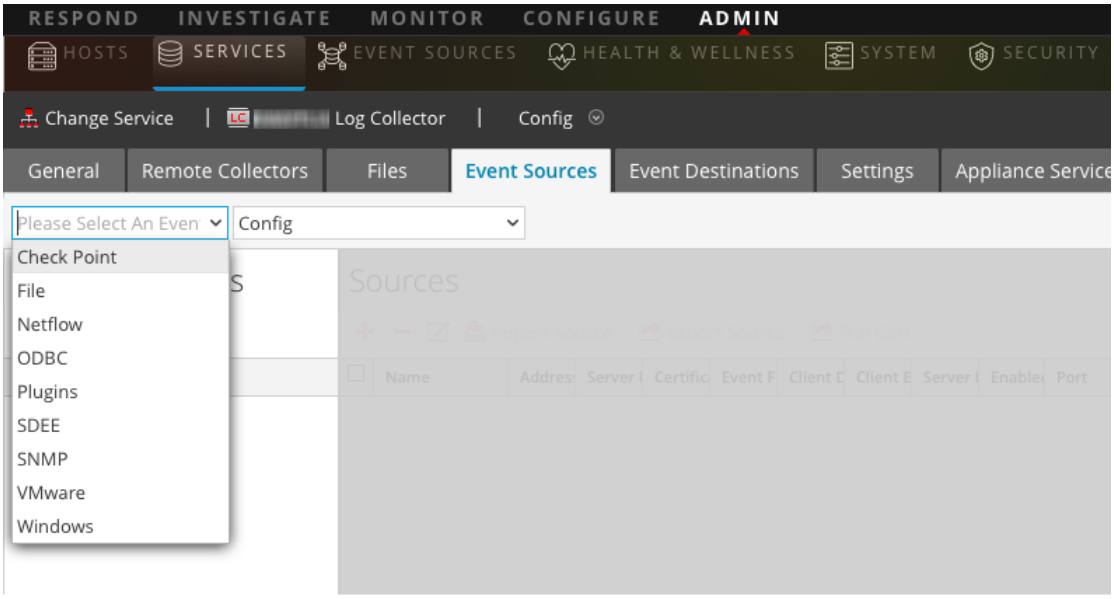
Configuration in NetWitness Suite

For complete details about configuring Azure as an event source, see the Azure Event Source Configuration Guide, available on RSA Link.

To configure an Azure Event Source:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click + .

   The **Available Event Source Types** dialog is displayed.
7. Select **azureaudit**) and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.
8. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.
9. Define parameter values. For details, see Azure Parameters below.
10. Click **Test Connection**.

    The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

    Log Collectortakes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the NetWitness Suite displays an error message.
11. If the test is successful, click **OK**.

    The new event source is displayed in the **Sources** panel.

Azure Parameters

This section describes the Azure event source configuration parameters.

Note: Items that are followed by an asterisk (*) are required.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Client ID *	The Client ID is found the Azure Application Configure tab. Scroll down until you see it.
Client Secret *	When you are configuring the event source, the client secret is displayed when you are creating a key, and you select a duration of validation. Make sure to save this, because you will only be able to see it once, and it cannot be retrieved later.
API Resource Base URL *	Enter `https://management.azure.com/`. Be sure to include the trailing slash (/).
Federation Metadata Endpoint *	In your Azure application, click the **View Endpoints** button (near the bottom of the pane). There are a lot of links that all begin with the same string. Compare the URLs and find the common string that begins most of them. This common string is the endpoint that you need to enter here.
Subscription ID *	You can find this in the Microsoft Azure dashboard: click on Subscriptions at the bottom of the list on the left.
Tenant Domain *	Go to the active directory and click on the directory. In the URL, the tenant domain is the string directly following **manage.windowsazure.com/**. The tenant domain is the string up to and including the **.com**.
Resource Group Names *	In Azure, select Resource groups from the left navigation pane, then select your group.
Start Date *	Choose the date from which to start collecting. Default's to the current date.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click next to **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. **Caution:** Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Configure Check Point Event Sources in NetWitness Suite

This topic tells you how to configure the Check Point collection protocol, which collects events from Check Point event sources.

This protocol collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs.

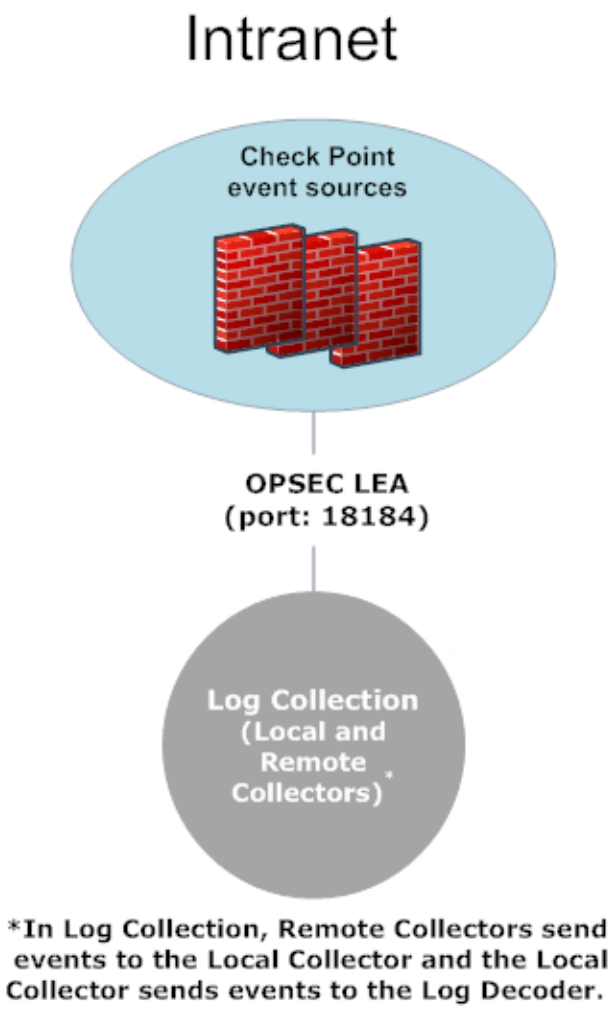
How Check Point Collection Works

The Log Collector service collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs.

Note: OPSEC LEA (Log Export API) supports extraction of logs from Check Point event sources configured with a SHA-256 or SHA-1 certificate.

Deployment Scenario

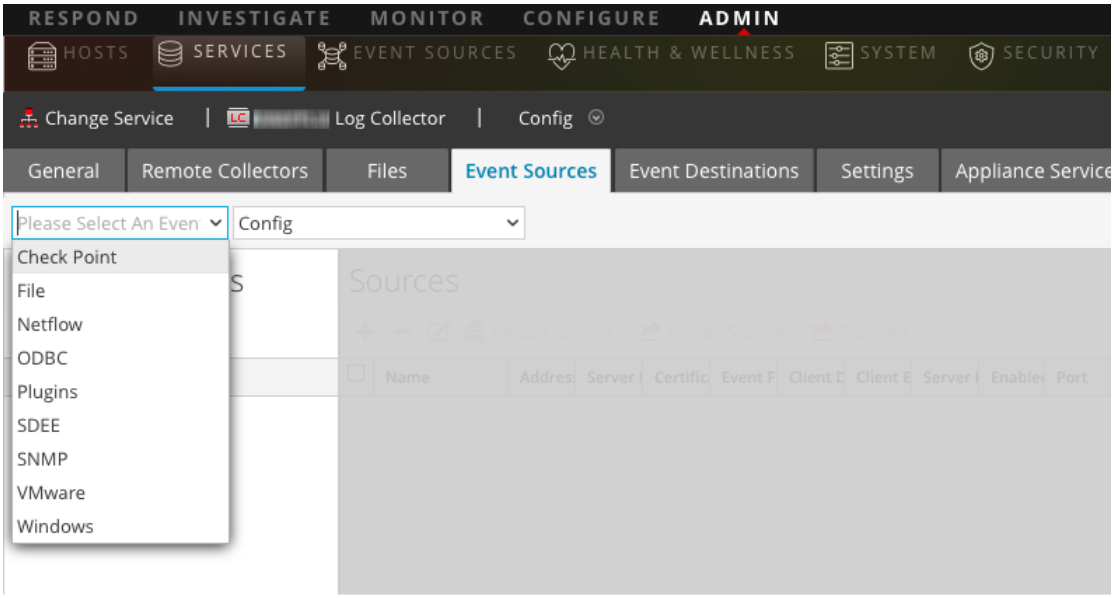
The following figure illustrates how you deploy the Check Point Collection Protocol in NetWitness Suite.



Configuration in NetWitness Suite

To configure a Check Point Event Source:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **Check Point/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click .

   The **Available Event Source Types** dialog is displayed.
7. Select a check point event source type and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.
8. Select the new type in the **Event Categories** panel and click in the **Sources** toolbar.

   The **Add Source** dialog is displayed.
9. Define parameter values. For details, see Check Point Parameters below.
10. Click **Test Connection**.

    The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

Log Collectortakes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the NetWitness Suite displays an error message.

11. If the test is successful, click **OK**.

    The new event source is displayed in the **Sources** panel.

Check Point Parameters

This section describes the Check Point event source configuration parameters.

Basic Parameters

Parameter	Description
Name*	Name of the event source.
Address*	IP Address of the Check Point server.
Server Name*	Name of the Check Point server.
Certificate Name	Certificate name for secure connections to use when the transport mode is https. If set, the certificate must exist in the certificate trust store that you created using the Settings tab. Select a certificate from the drop-down list. The file naming convention for Check Point event source certificates is **checkpoint_*name-of-event-source***.
Client Distinguished	Enter the Client Distinguished Name from the Check Point server.
Client Entity Name	Enter the Client Entity Name from the Check Point server.
Server Distinguished	Enter the Server Distinguished Name from the Check Point server.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Pull Certificate	Select the checkbox to pull a certificate for first time. Pulling a certificate makes it available from the trust store.

Parameter	Description
Certificate Server Address	IP Address of the server on which the certificate resides. Defaults to the event source address.
Password	Only active when you select the Pull Certificate checkbox for first time. Password required to pull the certificate. The password is the activation key created when adding an OPSEC application to Check Point on the Check Point server.

Determine Advanced Parameter Values for Check Point Collection

You use less system resources when you configure a Check Point event source connection to stay open for a specific time and specific event volume (transient connection). RSA NetWitness Suite defaults to the following connection parameters that establish a transient connection:

- Polling Interval = **180** (3 minutes)
- Max Duration Poll = **120** (2 minutes)
- Max Events Poll = **5000** (5000 events per polling interval)
- Max Idle Time Poll = **0**

For very active Check Point event sources, it is a good practice to set up a connection that stays open until you stop collection (persistent connection). This ensures that Check Point collection maintains the pace of the events generated by these active event sources. The persistent connection avoids restart and connection delays and prevents Check Point collection from lagging behind event generation.

To establish a persistent connection for a Check Point event source, set the following parameters to the following values:

- Polling Interval = **-1**
- Max Duration Poll = **0**
- Max Events Poll = **0**
- Max Idle Time Poll = **0**

Parameter	Description
Port	Port on the Check Point server that Log Collector connects to. Default value is 18184.

Parameter	Description
Collect Log Type	Type of logs that you want to collect: Valid values are: • **Audit** - collects audit events. • **Security** - collects security events. If you want to collect both audit and security events, you must create a duplicate event source. For example, first you would create an event source with Audit selected pulling a certificate into the trust store for this event source. Next you would create another event source with the same values except that you would select Security for the Collect Log Type and you would select the same certificate in Certificate Name that you pulled when you set up the first set of parameters for this event source and you would make sure that Pull Certificate was not selected.
Collect Logs From	When you set up a Check Point event source, NetWitness collects events from the current log file. Valid values are: • **Now** - Start collecting logs now (at this point in time in the current log file). • **Start of Log** - Collect logs from the beginning of the current log file. If you choose "Start of Log" for this parameter value, you may collect a very large amount of data depending on how long the current log file has been collecting events. Note that this option is effective only for the first collection session.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).

Parameter	Description
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.> **300** is the default value.
Forwarder	Enables or disables the Check Point server as a forwarder. By default it is disabled.
Log Type (Name Value Pair)	Logs from the event source in Name Value format. By default it is disabled.
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables and disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).

Verify Check Point Collection is Working

The following procedure illustrates how you can verify that Check Point collection is working from the **Administration > Health & Wellness > Event Source Monitoring** tab.

1. Access the **Event Source Monitoring tab** from the **Administration > Health & Wellness** view.
2. Find **checkpointfw1** in the **Event Source Type** column.
3. Look for activity in the **Count** column to verify that Check Point collection is accepting events.

The following procedure illustrates how you can verify that Check Point collection is working from the **Investigation > Events** view.

1. Access the **Investigation > Events** view.
2. Select the Log Decoder (for example, **LD1**) collecting Check Point events in the **Investigate a Device** dialog.
3. Look for a Check Point event source parser (for example, **checkpointfw1**) in the **device.type** field in the **Details** column to verify that Check Point collection is accepting events.

Note: If the logs from the VSX Checkpoint firewall server are collected by the Log Collector checkpoint service, to translate the VSX IP in the logs to **ip.orig** meta, you must add the VSX hostname and the VSX IP address to the `/etc/hosts` file in the Log Collector.

Configure File Event Sources in NetWitness Suite

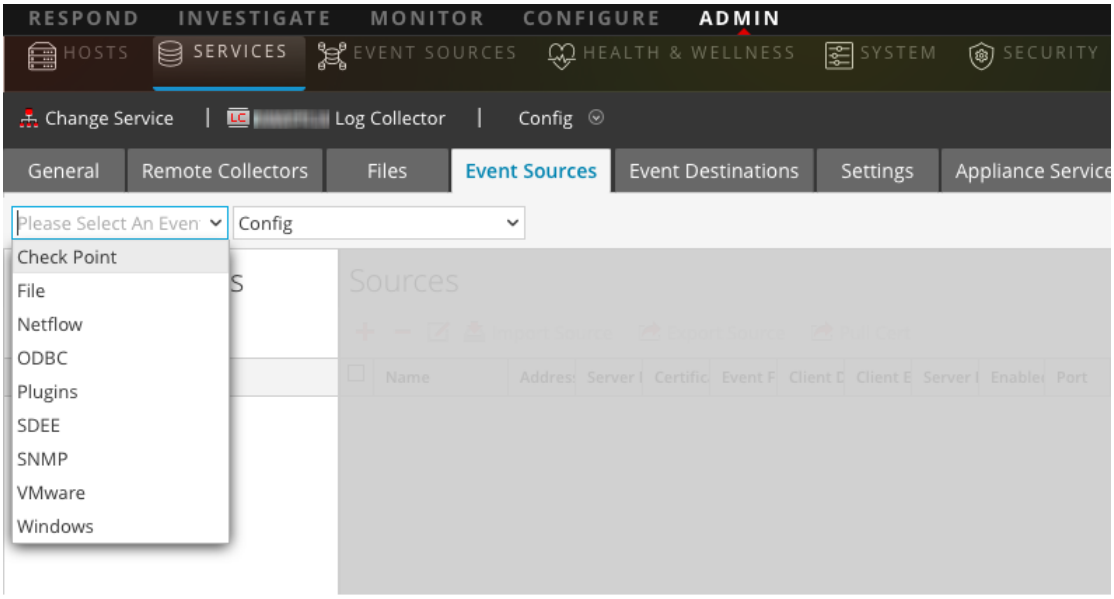
This topic tells you how to configure the File collection protocol.

Configure a File Event Source

To configure a File Event Source:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **File/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.
7. Select a file event source type and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.
8. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.
9. Add a **File Directory** name and modify any other parameters that require changes. For details, see File Collection Parameters below.
10. To get the public key and enter it into the dialog box, do the following:
    a. Select and copy the public key from the Event Source by running: **cat ~/.ssh/id_rsa.pub**
    b. Paste the public key in the **Eventsource SSH Key** field.
11. Click **OK**.

You need to restart file collection for your changes to take effect.

Stop and Restart File Collection

After you add a new event source that uses file collection, you must stop and restart the NetWitness Suite File Collection service. This is necessary to add the key to the new event source.

File Collection Parameters

The following table provides descriptions of the File Collection source parameters.

Name	Description
	Basic
File Directory*	Collection directory (for example, **Eur_London100**) into which the File event source places its files. Valid value is a character string that is conforms to the following regular expression: **[_a-zA-Z][_a-zA-Z0-9]*** This means that the file directory must start with a letter followed by numbers, letters, and underscores. Do not modify this parameter after you start collecting event data. After you create the collection, the Log Collector creates the work, save, and error sub-directories under the collection directory.
Address*	IP address of the event source. Valid value is an **IPv4 address**, **IPv6 address**, or a **hostname** including a fully-qualified domain name.
File Spec	Regular expression. For example, **^.*$** = process everything.
File Encoding	Internationalization file encoding. Enter the File Encoding method, the following strings are examples of valid methods: • UTF-8 (default) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
	Advanced

Name	Description
Ignore Encoding Conversion Errors	Select the check box to ignore encoding conversion errors and ignore invalid data. The check box is selected by default. **Caution:** This may cause parsing and transformation errors.
File Disk Quota	Determines when to stop saving files regardless of the **Save On Error** and **Save On Success** parameter settings. For example, a value of 10 indicates that when there is less than 10% available disk left, the Log Collector stops saving files to reserve enough space for your estimated normal collection processing. **Caution:** Available disk refers to a partition where the base collection directory is mounted. If the Log Decoder server has a 10TB disk size and 2TB is allocated to base collection directory, then setting this value to 10 causes log collection to stop when less than 0.2TB (10% of 2TB) of space is left. It does not mean 10% of 10TB. Valid value is a number in the **0** to **100** range. **10** is the default.
Sequential Processing	Sequential processing flag: • Select the check box (default) to process event source files in collection order. • Do not select the checkbox to process event source files in parallel.
Save On Error	Save on error flag. Check the checkbox to retain the **eventsource collection** file when the Log Collector it encounters an error. The check box is selected by default.
Save On Success	Save **eventsource collection** file after processing flag. Check the checkbox to save the eventsource collection file after processing it. The check box is not selected by default.

Name	Description
Eventsource SSH Key	SSH public key used to upload files for this event source. Please refer to the *Generate Key Pair on Event Source and Import Public Key to Log Collector* section in the Install and Update the SFTP Agent Guide for instructions on generating keys. **Note:** If File collection is stopped, NetWitness Suite does not update the authorized_keys file with the SSH public key that you add or modify in this parameter. You must restart File collection to update the public key. You can add or modify the value of the public key in this parameter in multiple File event sources without File collection running, but NetWitness Suite will not update the **authorized_keys** file until File collection is restarted.
Manage Error Files	By default, the Log Collectoruses the **File Disk Quota** parameter to ensure that the disk does not fill up with error files. If you set this parameter to **true**, you can specify one of these: • Maximum space allotted to error files in the **Error Files Size** parameter. • Maximum number of error files allowed in **Error Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached. Select the check box to manage error files. The check box is not selected by default.
Error Files Size	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Specifies to what extent NetWitness Suite saves error files. The value that you specify is the maximum total size of all the files in the error directory. Valid value is a number in **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Error Files Count	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Maximum number of error files allowed in the error directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.

Name	Description
Error Files Reduction %	Percent amount by size or count of the error files that the Log Collectorservice removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.
Manage Saved Files	Select the check box to manage saved files. The check box is not selected by default. By default, the Log Collector uses the **File Disk Quota** parameter to ensure that the disk does not fill up with saved files. If check this check box, you can specify one of these: • Maximum space allotted to saved files in the **Saved Files Size** parameter. • Maximum number of saved files allowed in **Saved Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached.
Saved Files Size	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum total size of all the files in the save directory. Valid value is a number in the **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved Files Count	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum number of saved files in the save directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved File Reduction %	Percent amount by size or count of the saved files that the Log Collector service removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

Configure Netflow Event Sources in NetWitness Suite

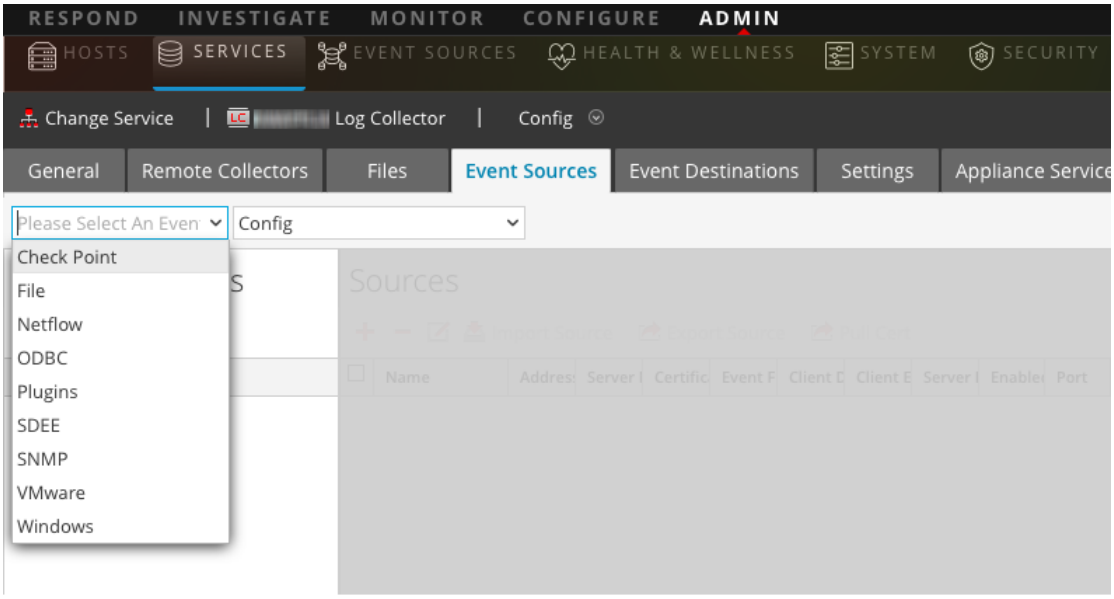
This topic tells you how to configure the Netflow collection protocol.

Configure a Netflow Event Source

To configure a Netflow Event Source:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.

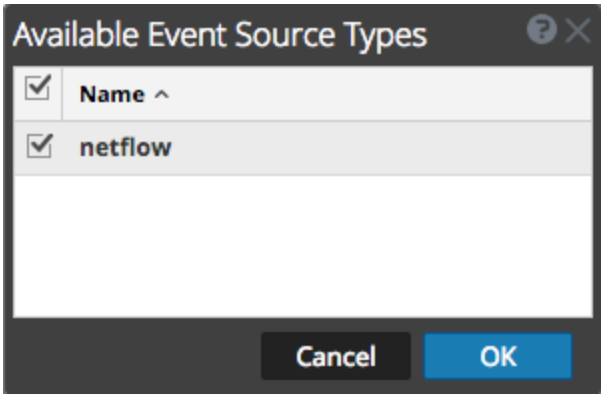


5. In the **Event Sources** tab, select **Netflow/Config** from the drop-down menu.

6. In the **Event Categories** panel toolbar, click + .

   The **Available Event Source Types** dialog is displayed.

7. Select the **netflow** event source type and click **OK**.



   The newly added event source type is displayed in the **Event Categories** panel.

8. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.

9. Enter a port number in the **Port** field, and ensure the Enabled box is checked.

   Note: NetWitness Suite opens the 2055, 4739, 6343, and 9995 ports on the firewall by default. You can open other ports for Netflow if required.

For details of other parameters, see Netflow Collection Parameters below.

10. Click **OK**.

The new event source is displayed in the list.

Netflow Collection Parameters

The following table provides descriptions of the Netflow Collection source parameters.

Name	Description
	Basic
Port	Specify the port number configured for the Netflow event source. NetWitness Suite opens the 2055, 4739, 6343, and 9995 ports for Netflow by default. You can open other ports for Netflow if required.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
	Advanced
InFlight Publish Log Threshold	Establishes a threshold that, when reached, NetWitness Suite generates a log message to help you resolve event flow issues. The Threshold is the size of the netflow event messages currently flowing from the event source to NetWitness Suite . Valid values are: • **0 (default)** - disables the log message. • **100-100000000** - generates a log message when this Log Collector has processed the specified number of netflow events. For example, if you set this value to 100, NetWitness Suite generates a log message when 100 netflow events of the specific netflow version (v5 or v9) have been processed.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector . Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

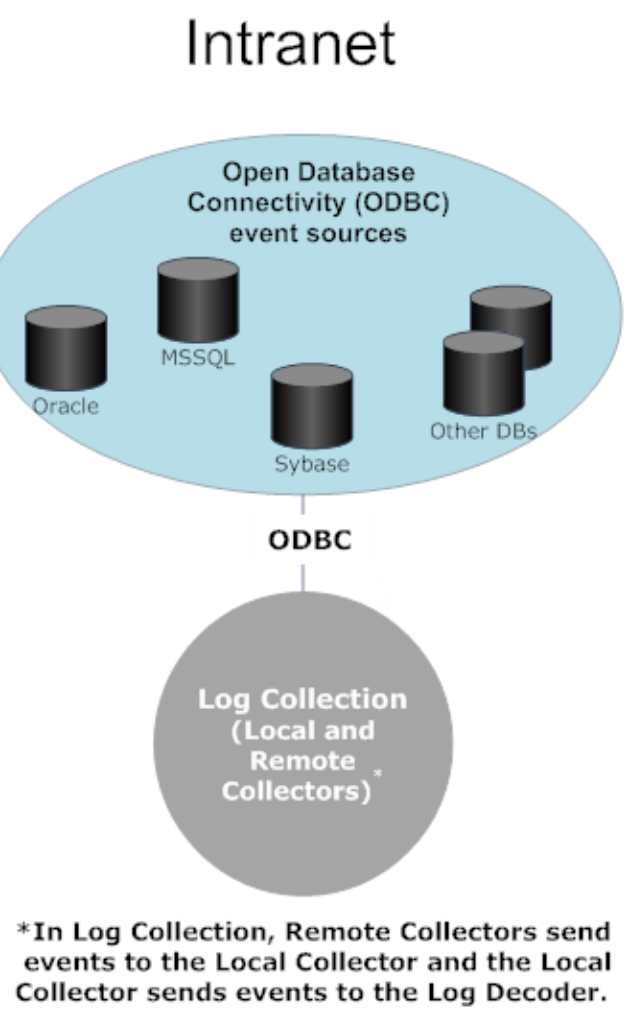
ODBC

Configure ODBC Event Sources in NetWitness Suite

This topic tells you how to configure ODBC collection protocol which collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface.

Deployment Scenario

The following figure illustrates how you deploy the ODBC Collection Protocol in NetWitness Suite.



Configure an ODBC Event Source

To configure an ODBC event source, you need to configure an event source type, and also choose a DSN template.

Configure a DSN

The following procedure describes how to add a DSN from an existing DSN template. For other procedures related to DSNs, see Configure Data Source Names (DSNs).

Configure a DSN (Data Source Name):

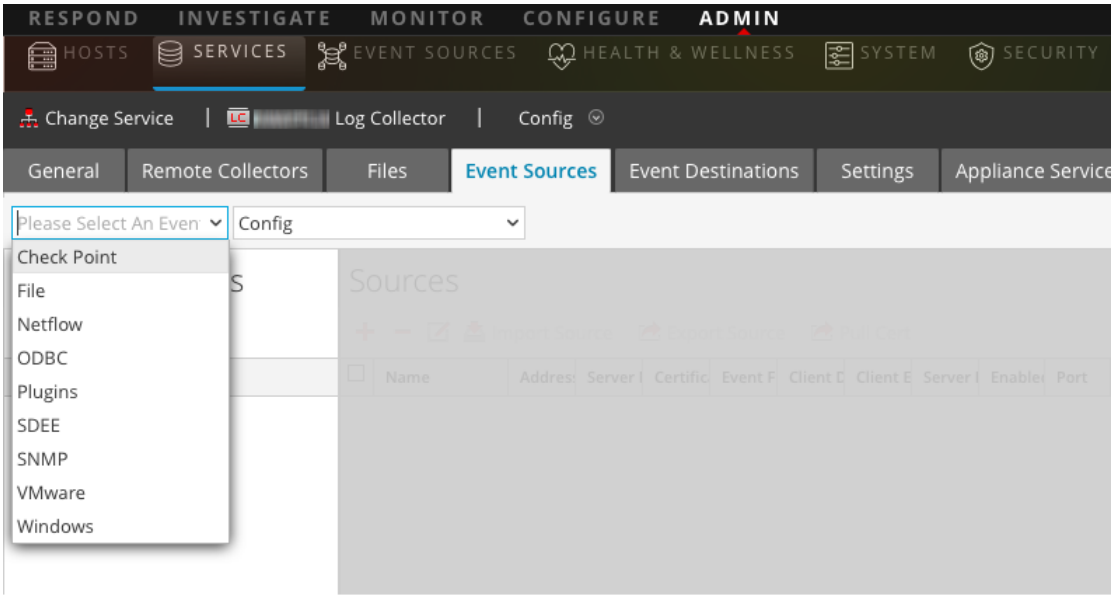
1. Go to **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.

5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click + to open the **Add DSN** dialog.
7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.) If required, click Manage Templates to add or delete DSN templates.
8. Fill in the parameters and click **Save**.

Add an Event Source Type

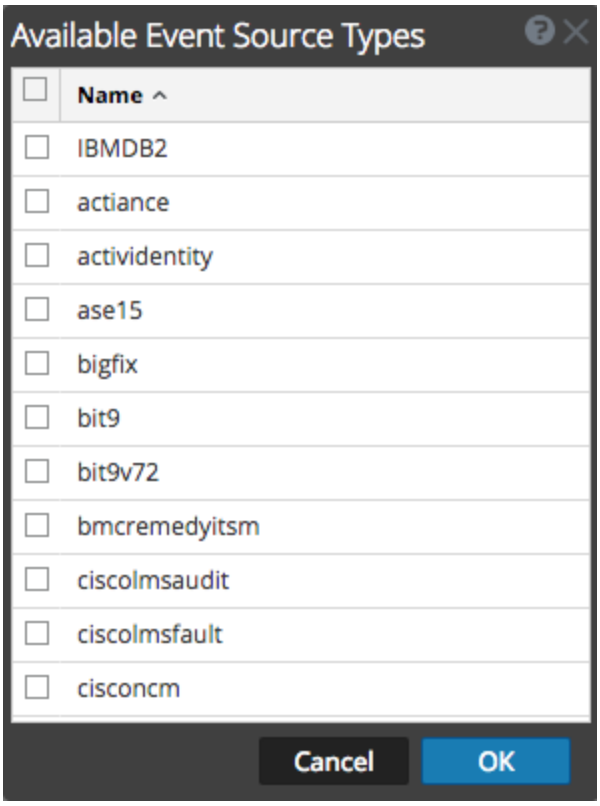
To configure an ODBC Event Source Type:

1. Go to **ADMIN> Services**.
2. Select a Log Collection service.
3. Under Actions, select > **View** > **Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **ODBC/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.

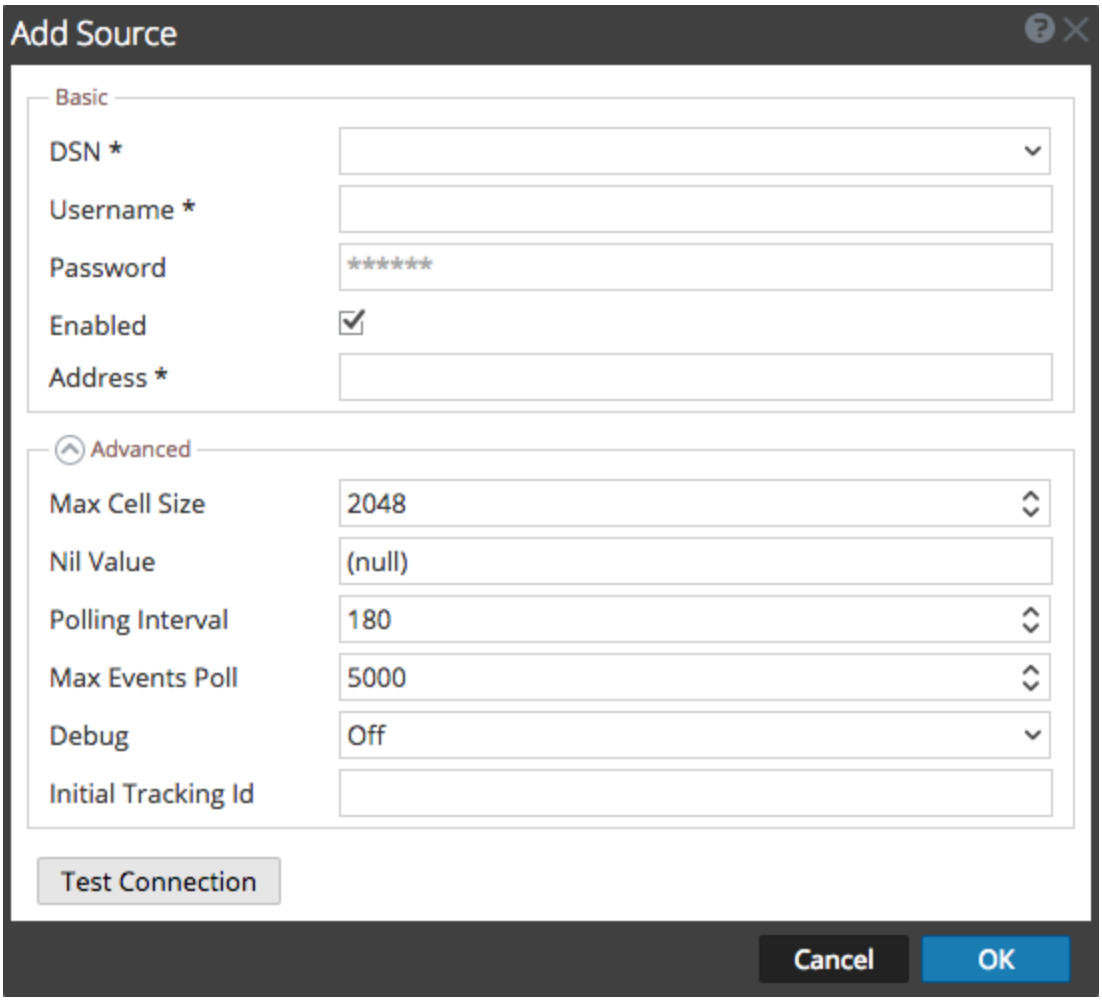


7. Select an event source category (for example **mssql** and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

8. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.



9. Select a DSN from the drop down list, specify or modify the other parameters as required, and click **OK**.
10. Click **Test Connection**.

    The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the DSN information and retry.

    Note: Log Collectortakes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the NetWitness Suite server displays an error message.

11. If the test is successful, click **OK**.

The newly defined DSN is displayed in the **Sources** panel.

ODBC Collection Parameters

The following table provides descriptions of the ODBC Collection source parameters.

Configure Data Source Names (DSNs)

This topic tells you how to create and maintain DSNs for ODBC Collection.

Context

Open Database Connectivity (ODBC) event sources require Data Source Names (DSNs) so you need to define DSNs with their associate value pairs for ODBC event source configuration.

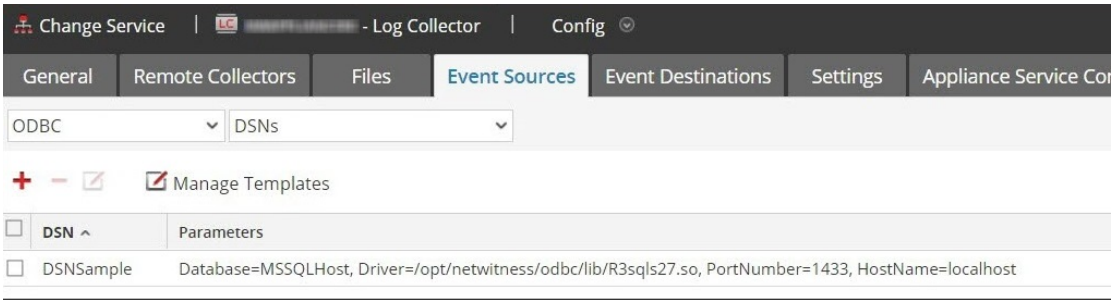
Navigate to the DSN Panel

To add or edit DSNs or DSN templates, first navigate to the appropriate screen.

To navigate to the DSN templates panel:

1. Go to **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.

   The **DSNs** panel is displayed with the DSNs that are added, if any.



From this screen, you can perform the following actions:

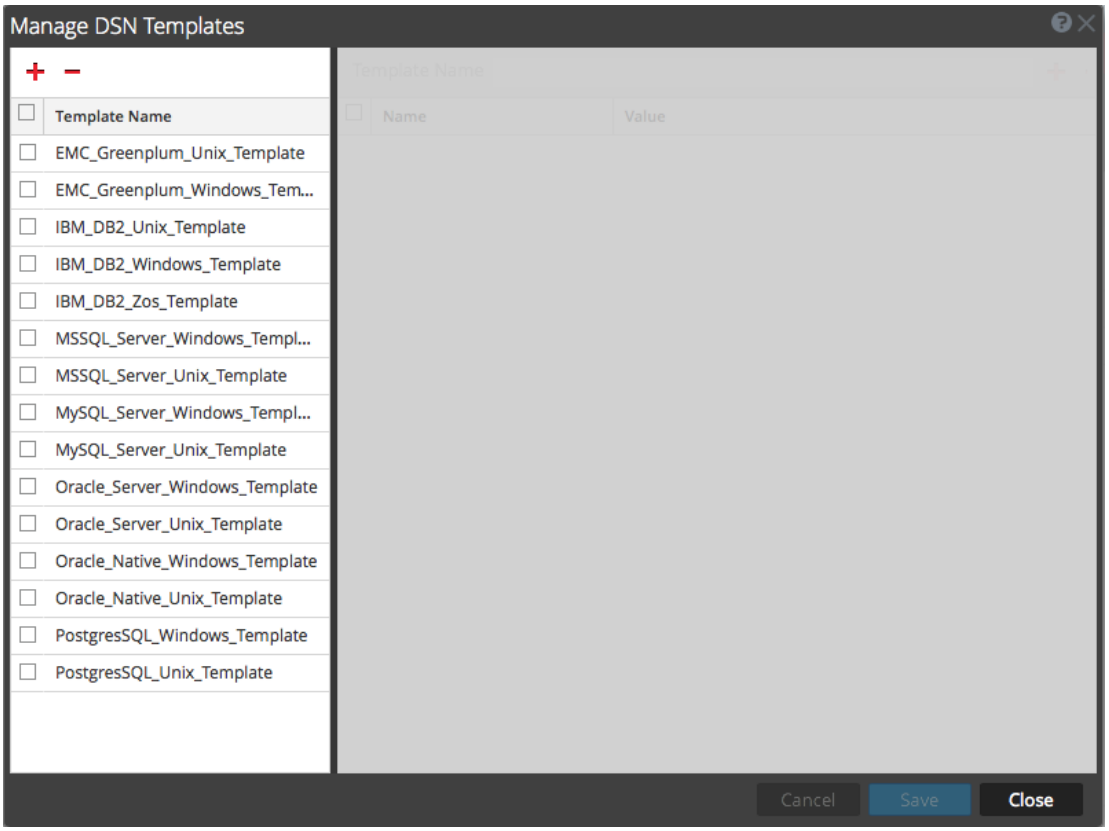
- Add a new DSN template
- Add a DSN from an existing template
- Add a DSN by editing an existing DSN template
- Remove a DSN or DSN template

Add a New DSN Template

If none of the predefined DSN templates fit your needs, use this procedure to add a DSN template.

1. From the DSNs panel, click .

   The **Manage DSN Templates** dialog is displayed.



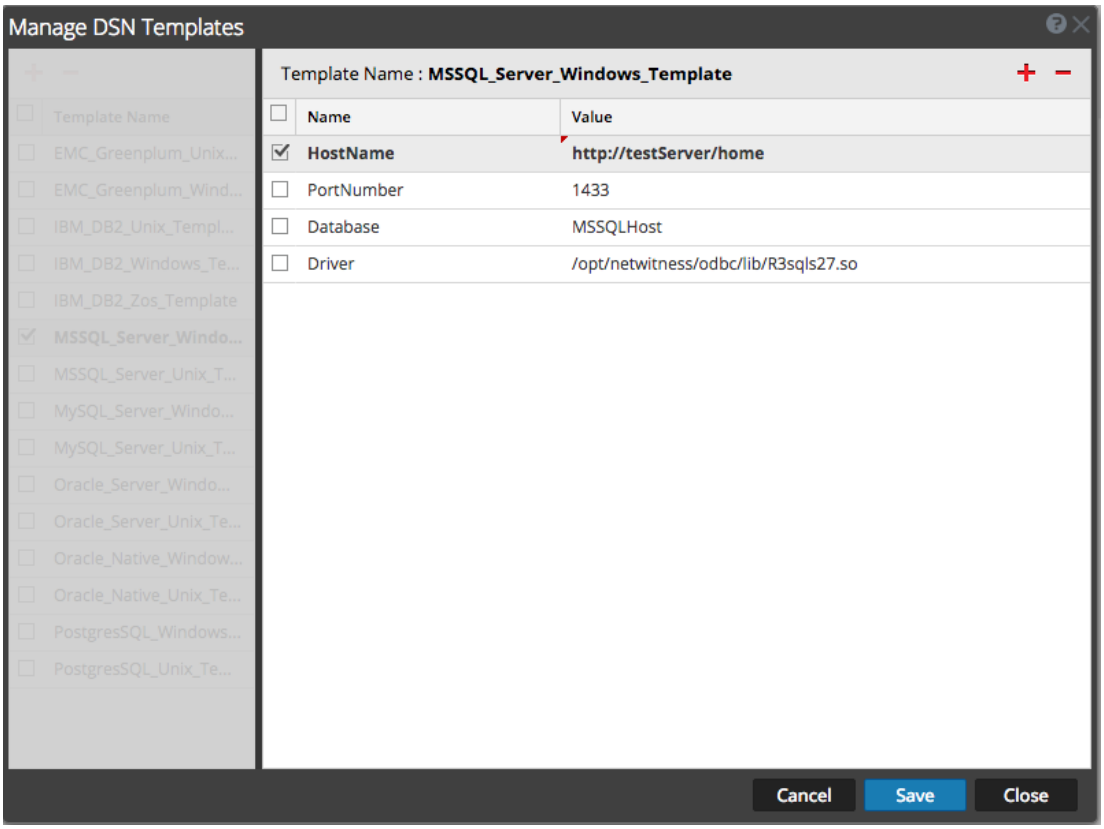
Note: RSA provides default templates on the left side panel that you can use while adding a new DSN.

2. Click +.

   The right panel is activated.

3. Specify a template name and click + on the right panel to add parameters.

4. Specify the parameters. Click **Save**.



The new DSN template is added in the **Manage DSN Templates** list.

Add a DSN from an existing template

You can select an existing template, and fill in the parameters for your needs.

1. From the DSNs panel, click + to open the Add DSN dialog box.

   The **Add DSN** dialog is displayed with existing DSNs, if any

2. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)

3. Fill in the parameters and click **Save**.

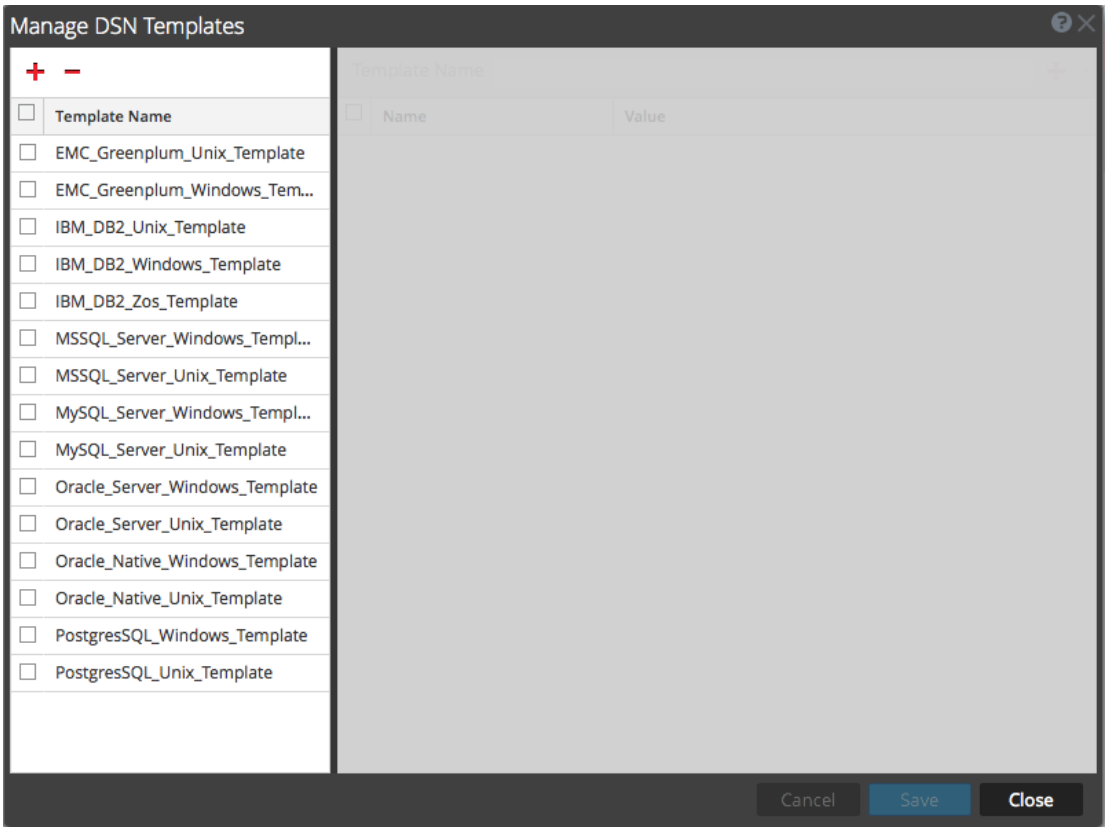
Your DSN is added to the list of DSNs.

Add a New DSN by editing an existing DSN template

You can add a DSN by updating an existing DSN template to fit your needs.

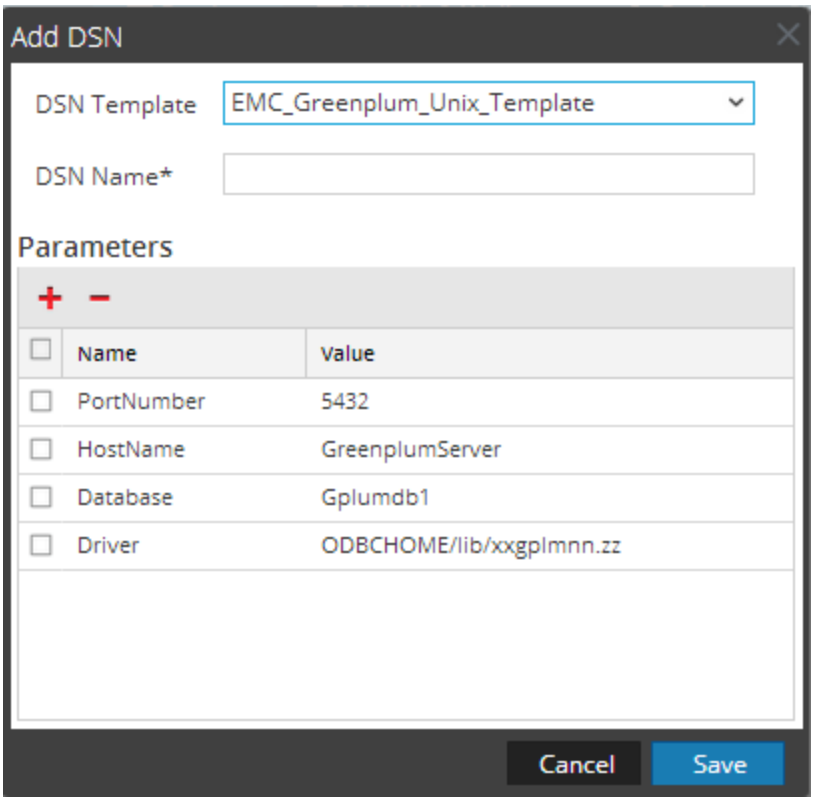
1. From the DSNs panel, click Manage Templates.

   The **Manage DSN Templates** dialog is displayed.



2. Select the existing template that you want to modify.

   The right panel is activated, and the default parameters for the selected template are displayed.



3. Specify a name in the **DSN Name** field.
4. Add, delete or edit the default parameters.
5. Once you have the set of required parameters, click **Save**, then **Close**.
6. Choose the DSN Template that you updated from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

Your DSN is added to the list of DSNs.

Remove a DSN or DSN template

If you no longer use a DSN or a DSN template, you can remove it from the system.

To remove an existing DSN:

1. From the DSNs panel, select an existing DSN.
2. Click —.

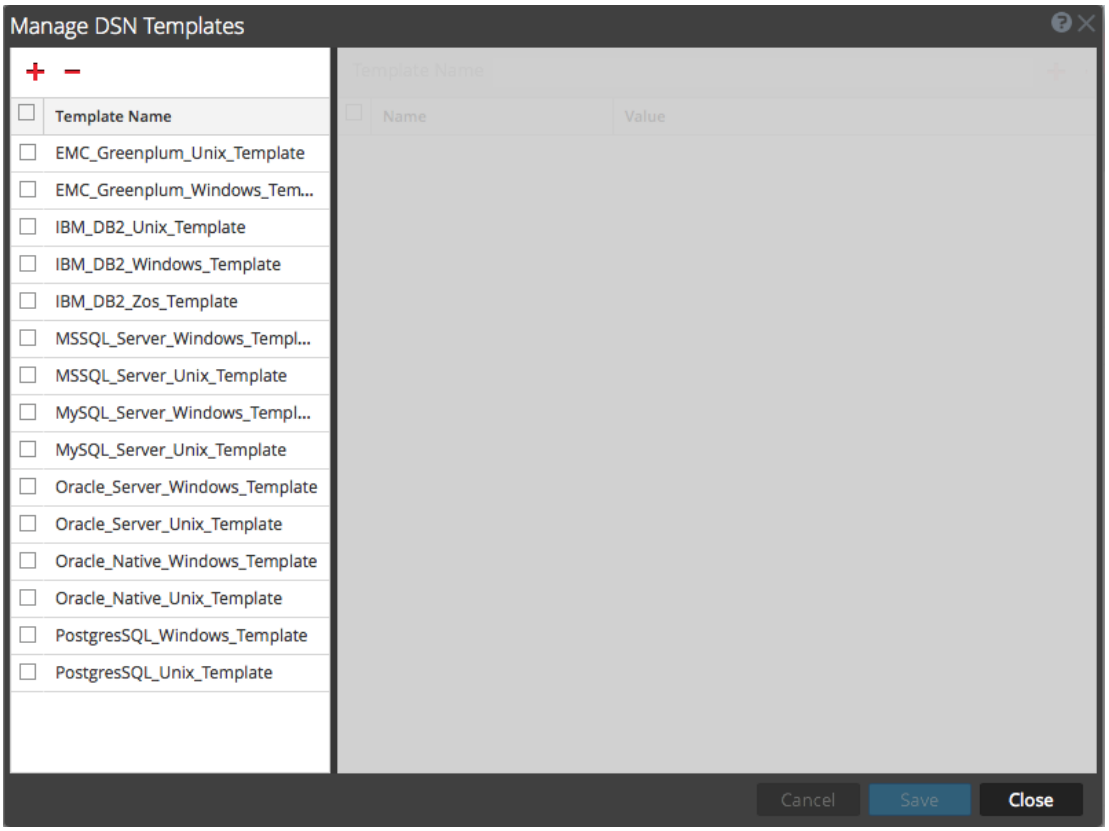
   A Warning message appears, asking whether you are sure you want to delete the DSN.
3. To delete the DSN, click **Yes**. Alternatively, to cancel the deletion, click **No**.

If you confirmed the deletion, the selected DSN is removed from the system.

To remove an existing DSN Template:

1. From the DSNs panel, click Manage Templates.

   The **Manage DSN Templates** dialog is displayed.



2. From the DSNs panel, select an existing DSN Template.
3. Click −.

   A Confirmation message appears, asking whether you are sure you want to delete the DSN Template.

4. To delete the DSN Template, click **Yes**. Alternatively, to cancel the deletion, click **No**.

If you confirmed the deletion, the selected DSN Template is removed from the system.

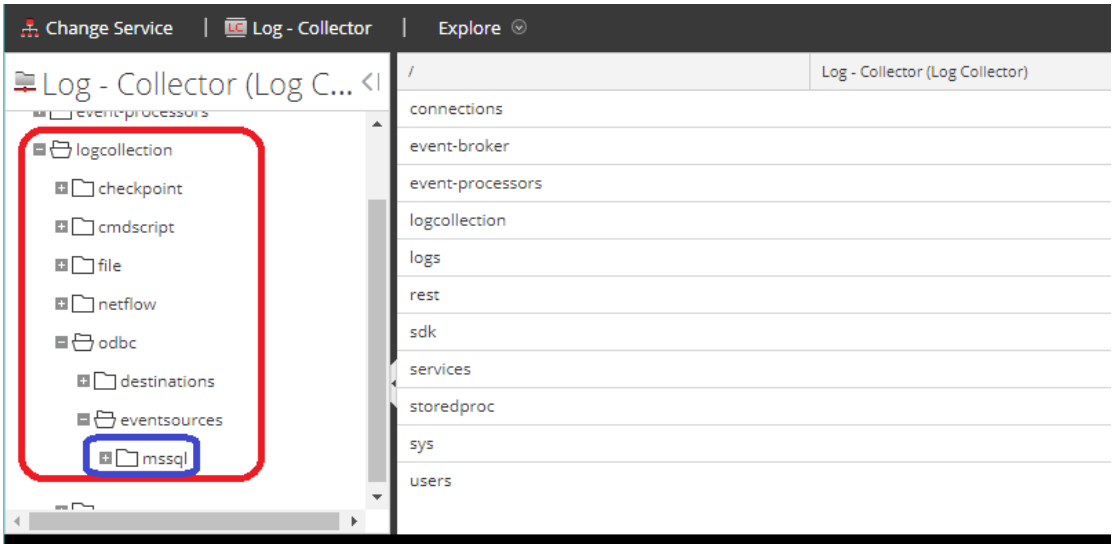
Configure device.ip meta for ODBC Data Source

For any ODBC event source, you can choose to have the ODBC collector populate the **device.ip** meta value with either the event source IP address or the actual source IP on which logs are being collected.

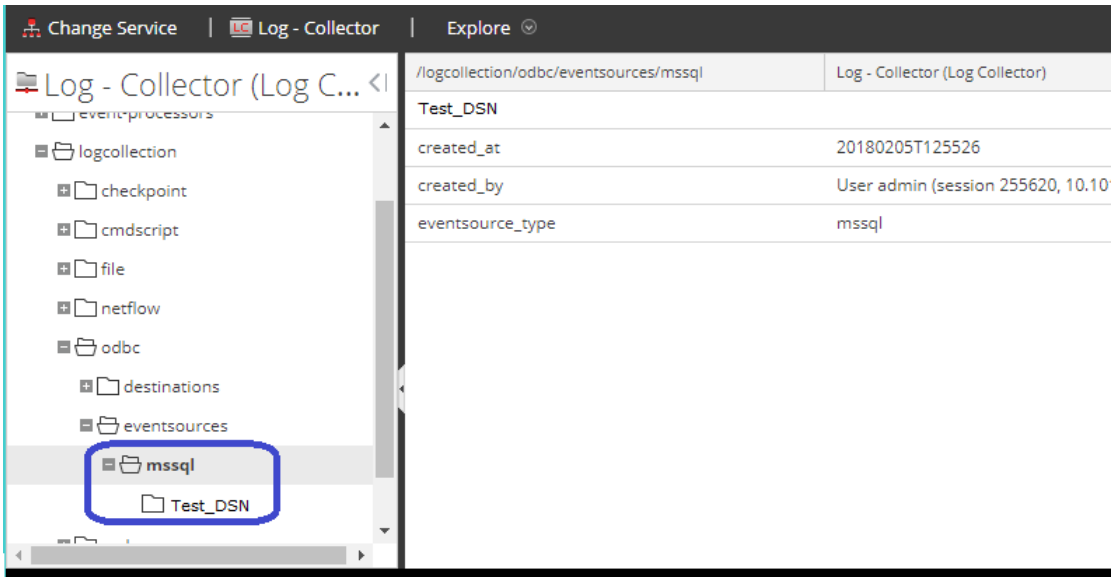
To view or set this parameter:

1. Go to **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click under **Actions** and select **View > Explore**.
4. Navigate to **logcollection > odbc > eventsources**.

   There are entries for each ODBC event source that you have configured in NetWitness. For example, for this installation, the only ODBC event source currently configured is MS SQL:

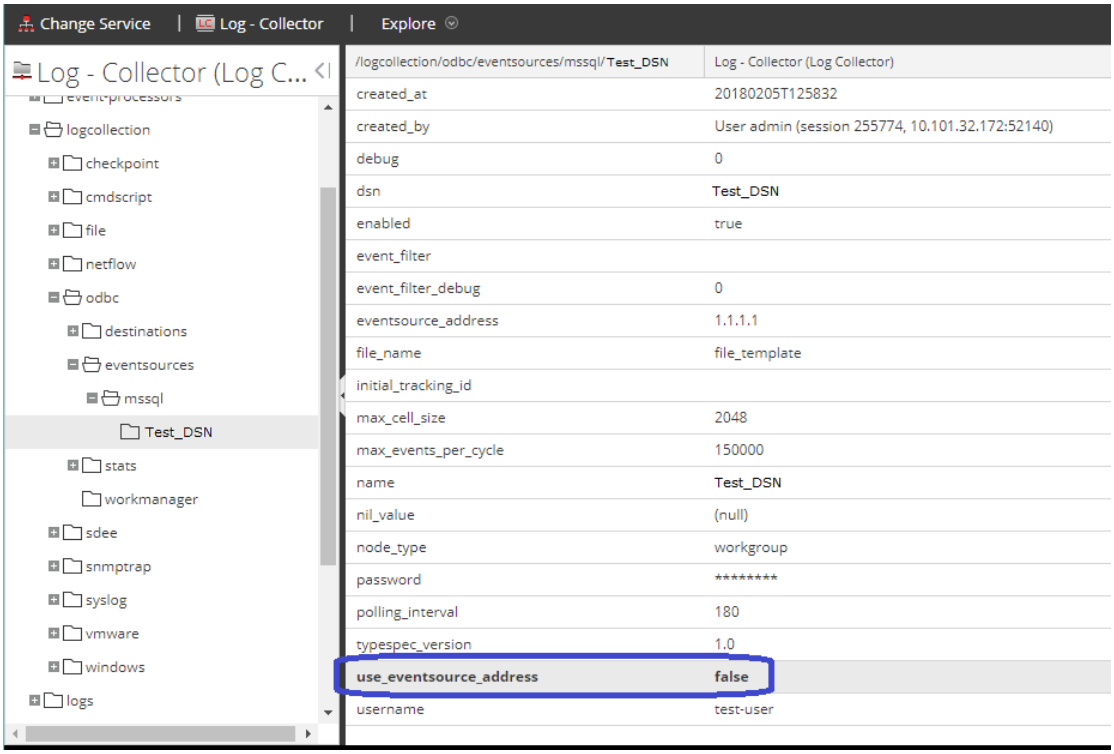


5. Click + next to an event source to expand it and see its DSN entry.



6. Click the DSN entry (in this example **Test_DSN**) to show the parameters.

7. The **use_eventsource_address** parameter is listed.



- **False**: actual source IP address is used. This is the default value.
- **True**: event source IP address is used.

8. Click on the value (in this case **False**), and type in the new value.

> **Note:** If you type anything other than **true** or **false** (case does not matter), you receive an error saying that the value you entered cannot be set.

Any changes you make take effect immediately.

Create Custom Typespec for ODBC Collection

This topic tells you how to create a custom typespec for the Log Collector. The topic includes:

- Create Custom typespec procedure
- ODBC Collection typespec syntax
- Sample ODBC Collection typespec files

Create Custom Typespec

To create a custom typespec file:

1. Open an SFTP client (for example, WinSCP) and connect to a Log Collector or remote Log Collector.
2. Navigate to **/etc/netwitness/ng/logcollection/content/collection/odbc**, and copy an existing file, for example **bit9.xml**.
3. Modify the file according to your requirements. See ODBC Collection Typespec Syntax for details.
4. Rename and save the file to the same directory.
5. Restart the Log Collector.

Note: You will not be able to see new Event Source type in NetWitness Suite until you restart the Log Collector.

ODBC Collection Typespec Syntax

The following table describes the typespec parameters.

Parameter	Description
name	The display name of your ODBC event source (for example, **activeidentity**). NetWitness Suite displays this name in the **Sources** panel of the **View > Config > Events Sources** tab. Valid value is an alphanumeric string. You cannot use - (dashes), _ (underscores), or spaces. The name must be unique across all typespec files in the folder.
type	Event source type: **odbc**. Do not modify this line.
prettyName	User-defined name for the event source. You can use the same value as name (for example, apache) or use a more descriptive name.
version	Version of this typespec file. Default value is 1.0.
author	Person who created the typespec file. Replace author-name with your name.
description	Formal description of the event source. Replace formal-description with your description of the event source.
<device> Section	

Parameter	Description
parser	This optional parameter contains the name of the log parser. This value forces the Log Decoder to use the specified log parser when parsing logs from this event source. **Note:** Please leave the field blank when unsure of the log parser to be used.
name	Name your ODBC event source (for example, **ActivIdentity ActivCard AAA Server**).
maxVersion	The version number of the event source (for example, **6.4.1**).
description	Description of the event source.
	<collection> Section
odbc	The syntax under `<odbc>` is used for event collection and processing. You can provide multiple queries for the same event source type by adding `<query>` tags.
query	This section contains the details of the query used to collect information from the event source.
tag	The prefix tag you want to add to events during transformation (for example **ActivIdentity**).
outputDelimiter	Specify the delimiter to use to separate fields. Specify any of the following values: • || (piping) • ^ (caret) • **,** (comma) • **:** (colon) • **0x20** (to represent a space)
interval	Specify the number of seconds between events. Default value is **60**.

Parameter	Description
dataQuery	Specify the query to fetch data from the ODBC eventsource database for SQL-syntax. For example: SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate
maxTrackingQuery	The query used on the initial pull of events to identify the starting point within the data set to begin pulling logs from. After the initial pull, this query is no longer used, unless the **maxTracking** value has been reset or altered. For example: SELECT MAX(Event_Id) from ExEvents
trackingColumn	The tracking column value used when the ODBC collector pulls a new set of events.

Sample ODBC Collection Typespec Files

The following sample is the typespec file for the IBM ISS SiteProtector event source.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>siteprotector4_x</name>
   <type>odbc</type>
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
```

```
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

The following sample is the typespec file for the Bit9 Security Platform event source.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Bit9 Events</description>

   <device>
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
            SELECT
```

```
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from
ExEvents</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

Troubleshoot ODBC Collection

You can troubleshoot problems and monitor ODBC collection by reviewing the ODBC collector log informational, warning, and error messages to during execution of collection.

Each ODBC log messages includes the:

- Timestamp
- Category: `debug`, `info`, `warning`, or `failure`
- collection method = `OdbcCollection`
- ODBC event source type (GOTS-name) = Generic ODBC Type Specification name that you configured for the event source.
- collection function completed or attempted (for example, `[processing]`)

- ODBC event source name (DSN-name) = Data Source Name that you configured for the event source.
- description (for example, how many events the Log Collector collected)
- tracking ID = the Log Collector position in the target database table.

The following example illustrates the message you would receive upon successful collection of an ODBC event:

2014-July-25 17:21:25 info (OdbcCollection) : [event-source] [processing] [event-source] Published 100 ODBC events: last tracking id: 2014-July-25 13:22:00.280

The following example illustrates a message you may receive upon unsuccessful collection of an ODBC event:

Log Message	timestamp failure (OdbcCollection: [event-source] [processing][event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver][event-source-type]Invalid object name 'object-name'.
Possible Cause	ODBC collection failed while accessing the ODBC Driver or the target database.
Solutions	Validate the DSN value pairs for the events source.

Configure SDEE Event Sources in NetWitness Suite

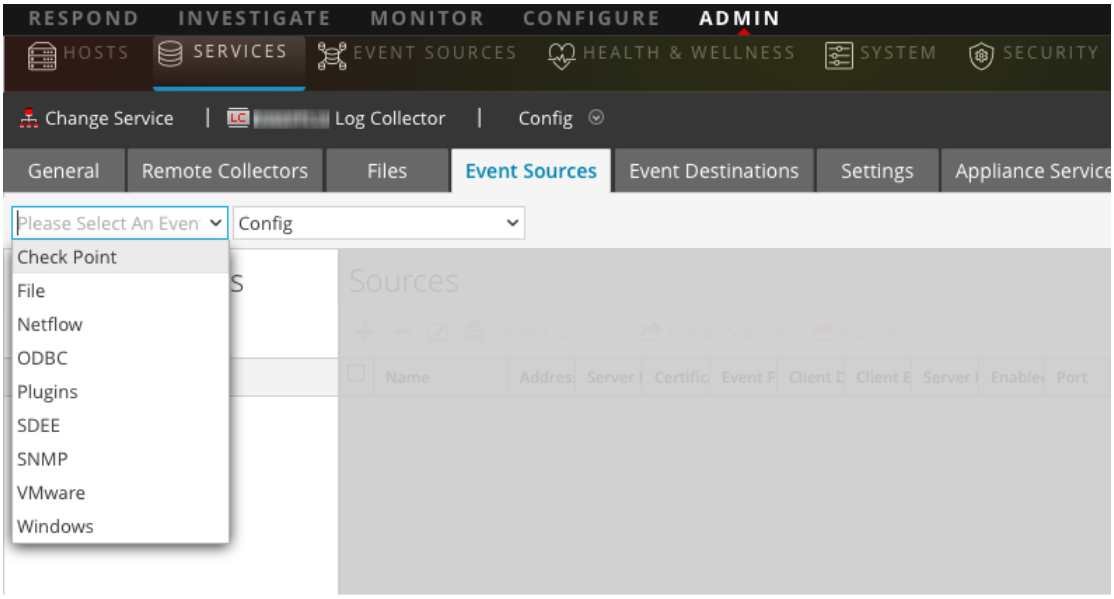
This topic tells you how to configure the SDEE collection protocol.

Configure an SDEE Event Source

To add an SDEE Event Source:

1. Go to **ADMIN> Services**.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.

4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **SDEE/Config** from the drop-down menu.

   The Event Categories panel displays the SDEE event sources that are configured, if any.

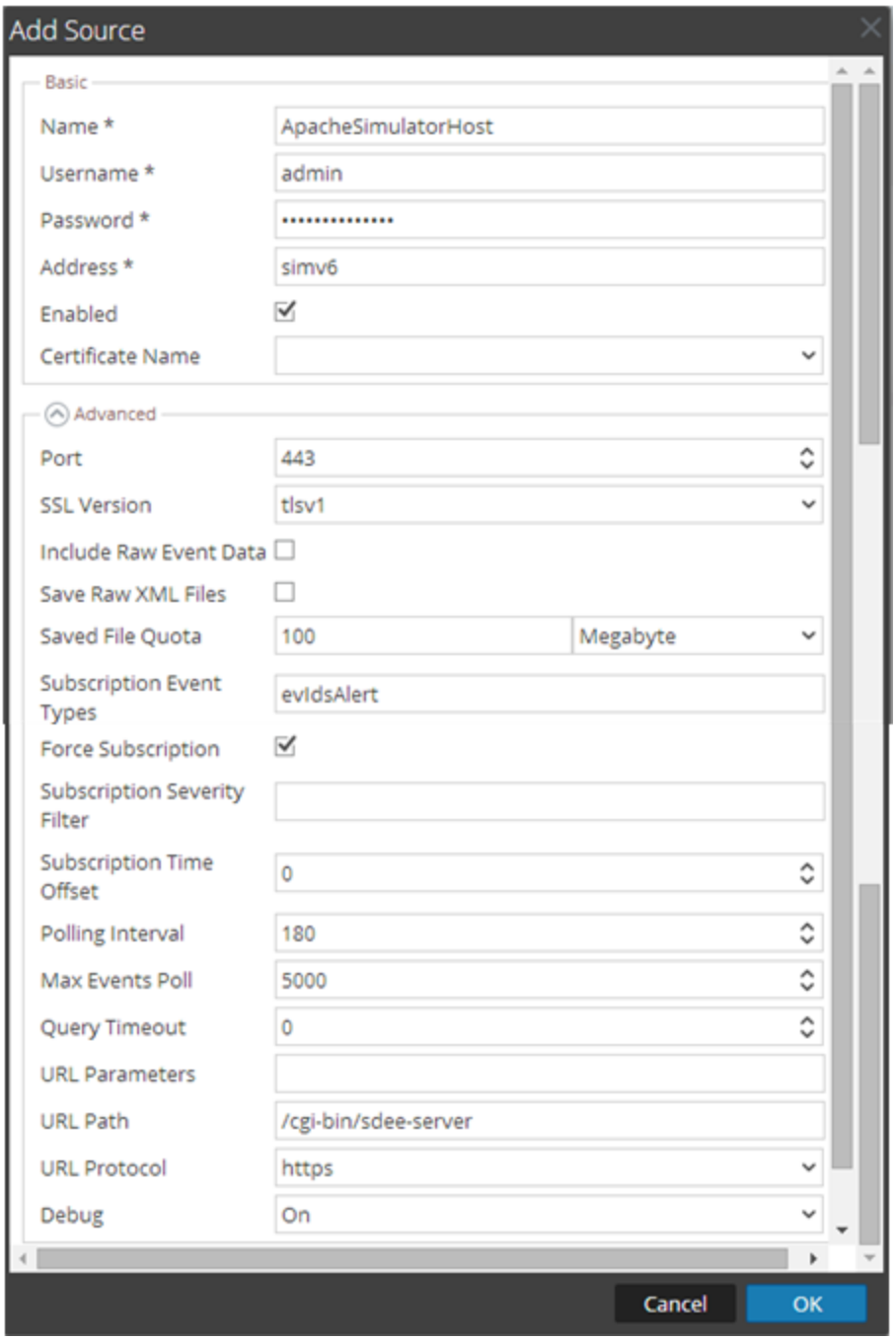
6. In the **Event Categories** panel toolbar, click + .

   The **Available Event Source Types** dialog is displayed.

7. Select an event source type and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

8. Select the new type in the Event Categories panel and click + in the Sources panel toolbar. The Add Source dialog is displayed.



9. Add a Name, Username, Address, and Password, and modify any other parameters that require changes, and click **OK**.

Configure SNMP Event Sources in NetWitness Suite

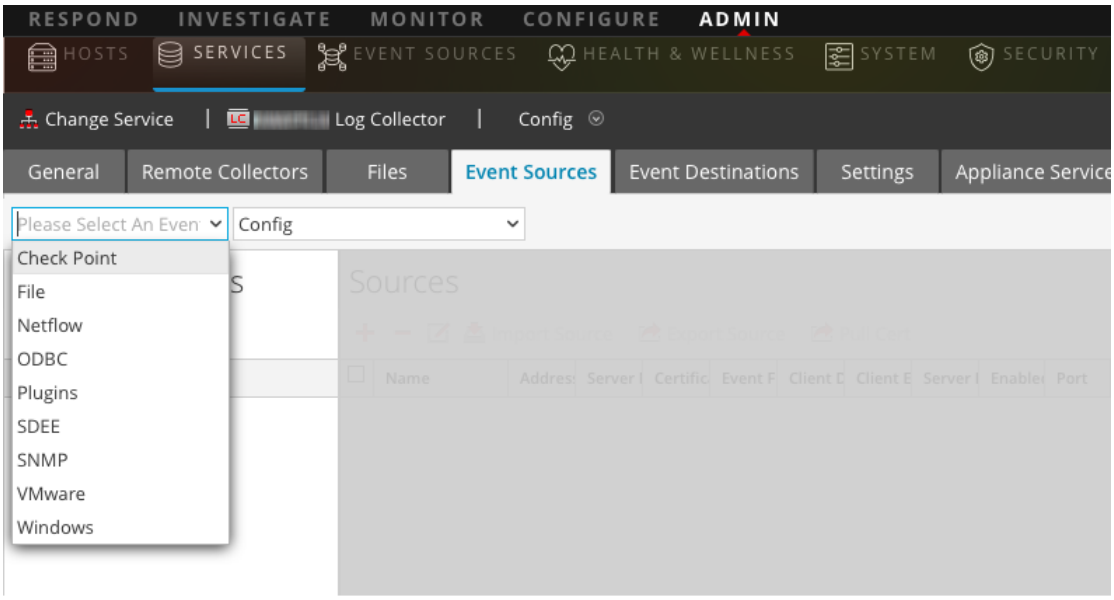
This topic tells you how to configure the SNMP collection protocol.

Configure the SNMP Trap Event Source

To add the SNMP Event Source:

Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. In the **Event Sources** tab, select **SNMP/Config** from the drop-down menu.
6. In the **Event Categories** panel toolbar, click .

   The **Available Event Source Types** dialog is displayed.
7. Select the **snmptrap** event source type and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.
8. Select **snmptrap** in the Event Categories panel.

9. Select **snmptrap** in the Sources panel and then click the Edit icon, , to edit the parameters.
10. Update any of the parameters that you need to change and click **OK**.

(Optional) Configure SNMP Users

If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. Go to **Admin** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

   The SNMP v3 User panel is displayed with the existing users, if any.
5. Click to open the **Add SNMP User** dialog.
6. Fill in the dialog with the necessary parameters. The available parameters are described below.

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	User name (or more accurately in SNMP terminology, security name). NetWitness Suite uses this parameter and the **Engine ID** parameter to create a user entry in the SNMP engine of the collection service. The **Username** and **Engine ID** combination must be unique (for example, **logcollector**).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.

Parameter	Description
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: • **None** (default) - only security level of **noAuthNoPriv** can be used for traps sent to this service • **SHA** - Secure Hash Algorithm • **MD5** - Message Digest Algorithm **DO NOT USE: do not select MD5, as it conflicts with the Log Collector running in FIPS mode.**
Authentication Passphrase	Optional if you do not have the **Authentication Type** set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: • **None** (default) • **AES** - Advanced Encryption Standard • **DES** - Data Encryption Standard **DO NOT USE: do not select DES, as it conflicts with the Log Collector running in FIPS mode.**
Privacy Passphrase	Optional if you do not have the **Privacy Type** set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

Configure Syslog Event Sources for Remote Collector

This topic tells you how to configure Syslog event sources for the Log Collector.

You do not configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors.

Configure a Syslog Event Source

Syslog listeners for UDP on port 514, TCP on port 514 and SSL on port 6514 are created by default. You should not change the SSL settings on the TCP and SSL listeners. If you need SSL certificate verification, create a new event source type to listen on a different port. Please note that **iptables** needs to be configured to open that port.

To configure the Remote Log Collector for Syslog collection:

1. Go to **ADMIN > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **> View > Config**.
3. Select the **Event Sources** tab.
4. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.

   Note: For RSA NetWitness Suite, some Syslog event sources are available by default. In this case, you can proceed to step 6.

5. In the Event Categories panel toolbar, click .

   The Available Event Source Types dialog is displayed.
6. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
7. Select the new type in the Event Categories panel and click in the Sources panel toolbar.

   The Add Source dialog is displayed.
8. Enter the port number, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in RSA NetWitness Suite.

Syslog Parameters

The following tables describe the available basic and advanced parameters for Syslog configuration.

Basic Parameters

Name	Description
Port*	Default port is **514**.

Name	Description
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
SSL Receiver	**Note:** This parameter applies to RSA NetWitness® Suite version 11.1 and newer. It is available only for the **syslog-tcp** Event Category. If you select the check box, the event source accepts SSL/TLS connections only. Also, if you change this setting, you must stop and restart Syslog collection for the change to become effective.

Advanced Parameters

Name	Description
Inflight Publish Log Threshold	Establishes a threshold that, when reached, NetWitness generates a log message to help you resolve event flow issues. The Threshold is the size of the syslog event messages currently flowing from the event source to NetWitness. Valid values are: • **0** (default) - disables the log message • **100-100000000** - generates log message when the syslog event messages currently flowing from the event source to NetWitness are within the 100 to 100000000 byte range.
Maximum Receivers	Maximum number of receiver resources used to process collected syslog events. The default value is **2**.
Event Filter	Select a filter. Please refer to Configure Event Filters for a Collector for instructions on how to define filters.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
SSL Verify Mode	**Note:** This parameter applies to RSA NetWitness® Suite version 11.1 and newer. It is available only for the **syslog-tcp** Event Category. This setting is relevant only if the **SSL Receiver** setting is selected. If you change the SSL Verify Mode, you must stop and restart Syslog collection for the change to become effective. Available options: • **verify-none**: (default) The server does not verify the client's certificate, if any. A client can connect without presenting a certificate. • **verify-peer**: The server verifies the client's certificate, if any. A client can connect without presenting a certificate. **Note:** If verification fails, a warning is logged but the messages will still be accepted. • **verify-peer-fail-if-no-cert**: The client must present a certificate and the server will verify it. **Note:** If you use this mode, the client's CA certificate ***must*** be uploaded to the Log Collector's truststore using the REST API at `http://LC-ip-address:50101/sys/caupload`

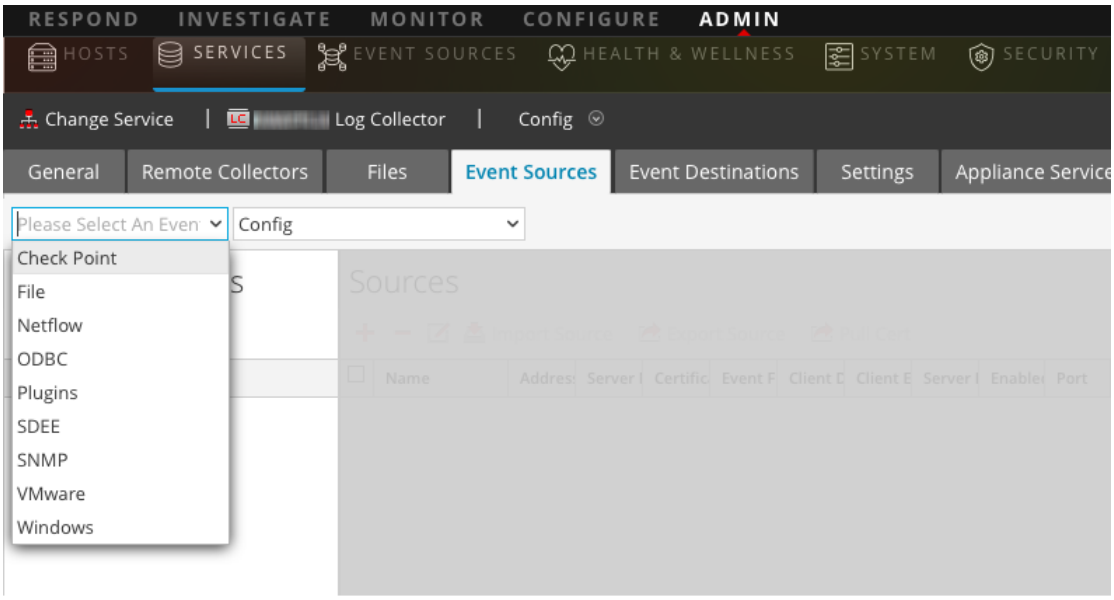
Configure VMware Event Sources in NetWitness Suite

This topic tells you how to configure the VMware collection protocol.

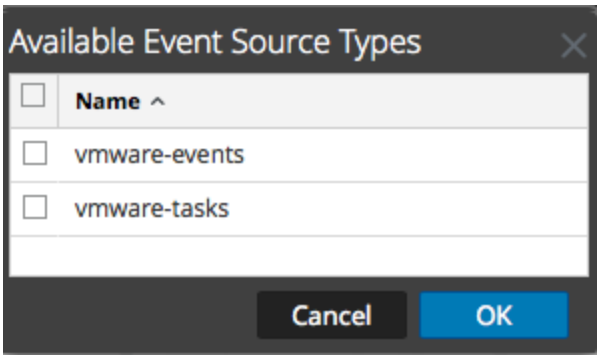
Configure a VMware Event Source

To add a VMware Event Source:

1. Go to **ADMIN> Services**.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. In the Log Collector **Event Sources** tab, select **VMware/Config** from the drop-down menu. The Event Categories panel displays the VMware event sources that are configured, if any.
6. Click to open the **Available Event Source Types** dialog.



7. Select **vmware-events** or **vmware-tasks** from the Available Event Source Types dialog and click **OK**.

   The VMware available event source types are as follows:

   - **vmware-events:** Setup vmware-events to collect events from vCenter Servers and ESX/ESXi servers.
   - **vmware-tasks:** (Optional) Setup vmware-tasks to collect tasks from vCenter Servers.

8. Select the new type in the Event Categories panel, and click + in the Sources toolbar.
9. Add a Name, Username and Password, and modify any other parameters that require changes.

   Caution: If you need to enter the domain name as part of the Username, you must use a double-backslash as a separator. For example, if the domain|username is corp\smithj, you must specify **corp\\smithj**.

10. Click **OK** to save your changes.

Configure Windows Event Sources in NetWitness Suite

This topic tells you how to configure the Windows collection protocol.

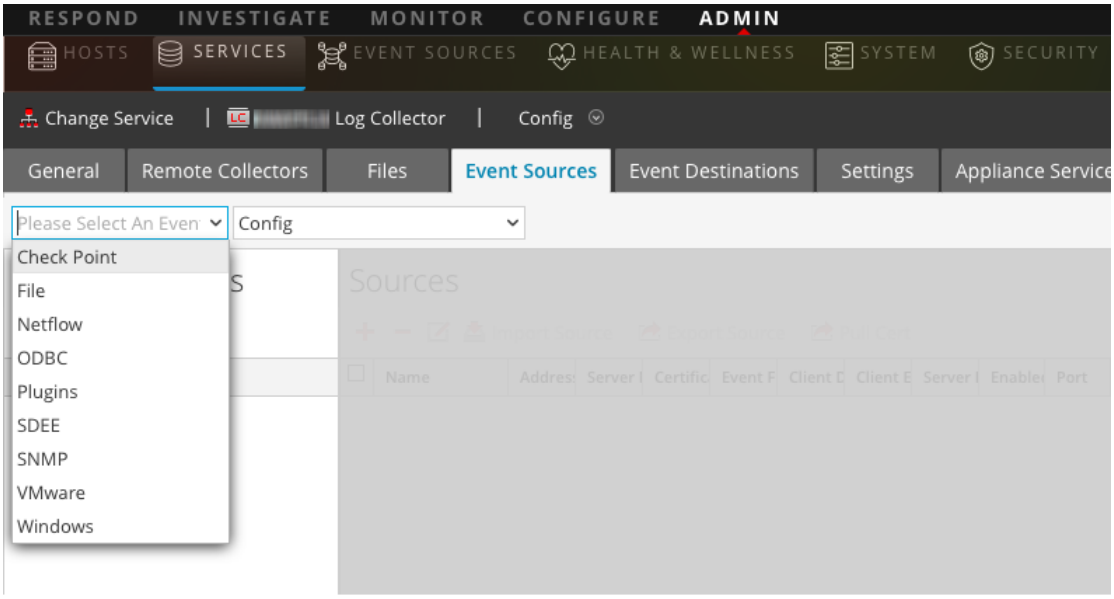
Configure a Windows Event Source

In RSA NetWitness Suite, you need to configure the Kerberos Realm, and then add the Windows Event Source type.

To configure the Kerberos Realm for Windows collection:

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.

3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.



5. Select **Windows/Kerberos Realm** from the drop-down menu.
6. In the Kerberos Realm Configuration panel toolbar, click to add a new realm.

   The Add Kerberos Domain dialog is displayed.
7. Fill in the parameters, using the guidelines below.

Parameter	Details
Kerberos Realm Name	Enter the realm name, in all caps. For example, DSNETWORKING.COM. Note that the Mappings parameter is automatically filled with variations on the realm name.
KDC Host Name	Enter the name of the Domain Controller. ***Do not*** use a fully qualified name here: just the host name for the DC. **Note:** Make sure that the log collector is configured as a DNS client for the corporate DNS server. Otherwise, the Log Collector will not know how to find the Kerberos Realm.
Admin Server	(Optional) The name of the Kerberos Administration Server in FQDN format.

8. Click **Save** to add the Kerberos domain.

To add a Windows Event Source:

1. Go to **ADMIN > Services**.
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. In the Log Collector **Event Sources** tab, select **Windows/Config** from the drop-down menu.

   The Event Categories panel displays the VMware event sources that are configured, if any.

Next, continue from the current screen to add a Windows Event Category and type.

To configure the Windows Event Type:

1. Select **Windows/Config** from the drop-down menu.
2. In the Event Categories panel toolbar, click to add a source.

   The Add Source dialog is displayed.
3. Fill in the parameters, using the guidelines below.

Parameter	Details
Alias	Enter a descriptive name.
Authorization Method	Choose **Negotiate**.
Channel	For most event sources that use Windows collection, you want to collect from the **Security**, **System**, and **Application** channels.
User Name	Enter the account name for the Windows user account that you set up earlier for communicating with NetWitness. Note that you need to enter the full account name, which includes the domain. For example, **rsalog@DSNETWORKING.COM**.
Password	Enter the correct password for the user account.
Max Events Per Cycle	(Optional). RSA recommends that you set this value to 0, which collects everything.
Polling Interval	(Optional). For most users, a value of **60** should work well.

4. Click **OK** to add the source.

   The newly added Windows event source is displayed in the Event Categories panel.

5. Select the new event source in the Event Categories panel.

   The **Hosts** panel is activated.

6. Click + in the Hosts panel toolbar.

7. Fill in the parameters, using the guidelines below.

Parameter	Details
Event Source Address	Enter the IP address for the Windows host.
Port	Accept the default value, **5985**.
Transport Mode	Enter **http**.
Enabled	Ensure the box is checked.

8. Click **Test Connection**.

   Note: You should be able to successfully test the connection, even if the Windows service is not running.

For more information on any of the previous steps, see the following Help topics in the NetWitness Suite User Guide:

- Configure Windows Collection: https://community.rsa.com/docs/DOC-43410
- Microsoft WinRM Configuration Guide: https://community.rsa.com/docs/DOC-58163
- Test and Troubleshoot Microsoft WinRM Guide: https://community.rsa.com/docs/DOC-58164

Windows Legacy and NetApp Collection Configuration

This **Windows Legacy** protocol collects events from Windows Legacy (Windows 2003 or earlier event sources) and CIFS Auditing events from NetApp ONTAP event sources.

You must deploy Log Collection, that is set up a Local Collector and Windows Legacy Remote Collector, before you can configure the Windows Legacy collection protocol.

How Legacy Windows and NetApp Collection Works

You use the Windows Legacy collection protocol to configure NetWitness Suiteto collection events from:

- Legacy Microsoft Windows event sources (Window 2003 and earlier event sources)
- NetApp event sources

Window 2003 and Earlier Event Sources

Legacy Windows event sources are older Windows versions (such as Windows 2000 and Window 2003). The Windows Legacy collection protocol collects from Windows event sources that are already configured for enVision collection without having to reconfigure them. You set up these event sources under the windows event source type.

NetApp Event Sources

NetApp appliances running Data ONTAP support a native auditing framework that is similar to Windows Servers. When configured, this auditing framework generates and saves audit events in Windows.evt file format. The Windows Legacy collection protocol supports collection of events from such NetApp.evt files. You set up these event sources under the netapp_evt event source type.

The NetApp Data ONTAP appliance is configured to generate CIFS Auditing events and save them periodically as.evt files in a format that includes the timestamp in the filename. Refer to the Network Appliance Data ONTAP Event Source Configuration Guide on RSA Link for details. The collection protocol saves the timestamp of the last processed.evt filename to keep track of collection status.

Net App Specific Parameters

Most of the parameters that you maintain in Add/Edit Source dialog apply to both Windows Legacy and Net App events sources.

The following two parameters are unique to NetApp event sources.

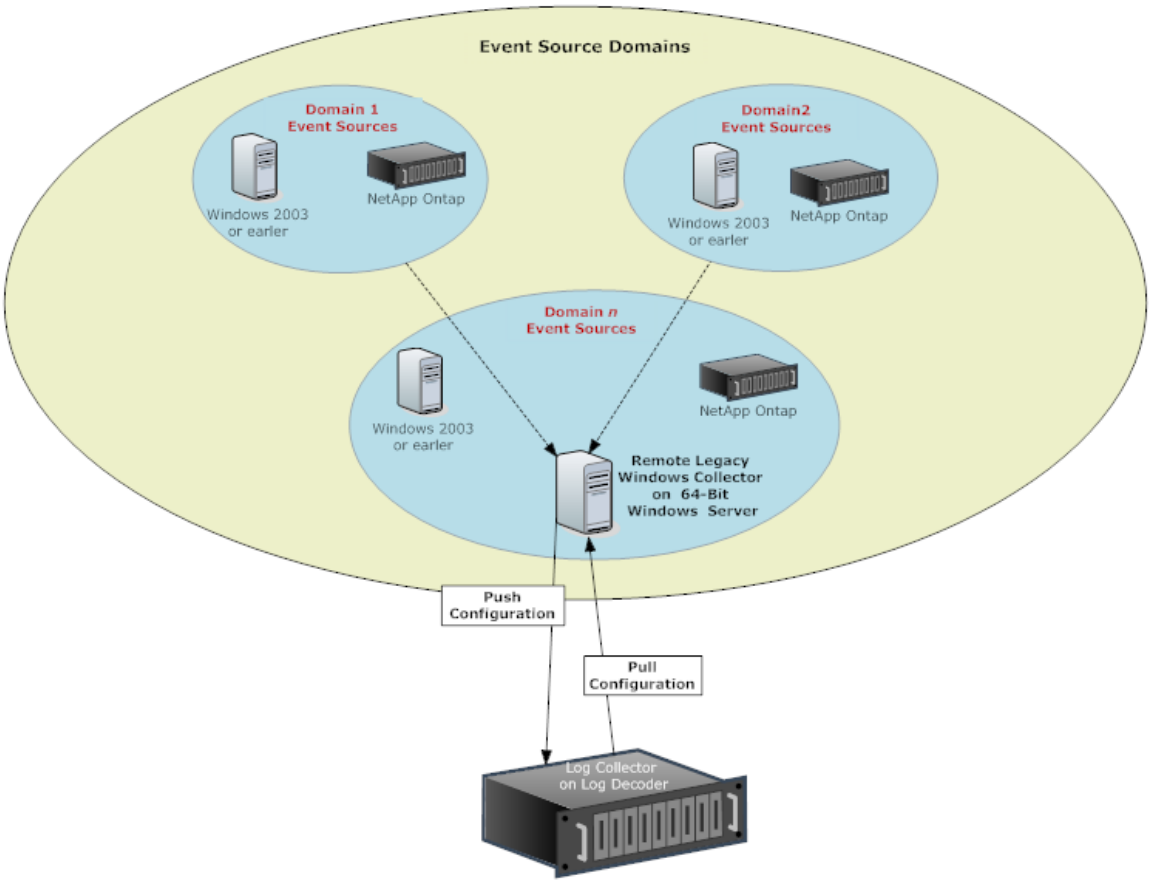
- **Event Directory Path** - The NetApp appliance generates event data and saves it in.evt files in a shareable directory on the NetApp appliance. NetWitness Suite requires you to specify this directory path in the Event Directory Path parameter
- **Event File Prefix** - Similar to the Event Directory Path, NetWitness Suite requires you to specify the prefix (for example, adtlog.) of the event data.evt files so that NetWitness Suite can process this data.

In each polling cycle, NetWitness Suite browses the configured NetApp shared path for the **.evt** files that you identified with the Event Directory Path and Event File Prefix parameters. NetWitness Suite:

- Sorts Files matching the event-file-prefix.YYMMDDhhmmss.evt format in ascending order.
- Uses the timestamp of the last file processed to determine the files that still need processing. If NetWitness Suite finds a partially processed file, it skips the events already processed.

Deployment Scenario

The Windows Legacy collection protocol collects event data from Windows 2003 or earlier, and NetApp ONTAP appliance, event sources. The Windows Legacy Remote Collector is the SA Legacy Windows Collector installed on physical or virtual Windows 2008 64-bit server in your event source domain.



Set Up the Windows Legacy Collector

This topic tells you where to find the executable and instructions required to install or upgrade the Windows Legacy collector in your Windows Legacy domain or domains.

You install the NetWitness Suite Windows Legacy collector on a physical or virtual Windows 2008 R2 SP1 64-Bit server using the **NWLegacyWindowsCollector-11.*version-number.exe***. You download the **NWLegacyWindowsCollector-11.*version-number.exe*** from RSA Link. Please refer to the *NetWitness 11.x Windows Legacy Collection Upgrade & Installation Instructions* for the details on how to install or upgrade Windows Legacy collection.

Note: The Microsoft Management Console (MMC) should be closed during the installation process.

Configure Windows Legacy and NetApp Event Sources

This topic tells you how to configure Windows Legacy event sources in NetWitness Suite.

The Windows Legacy collection protocol collects event data from Windows 2003 or earlier event sources, and from NetApp event sources.

Prerequisites

Before you configure a Windows Legacy event source, make sure that you have:

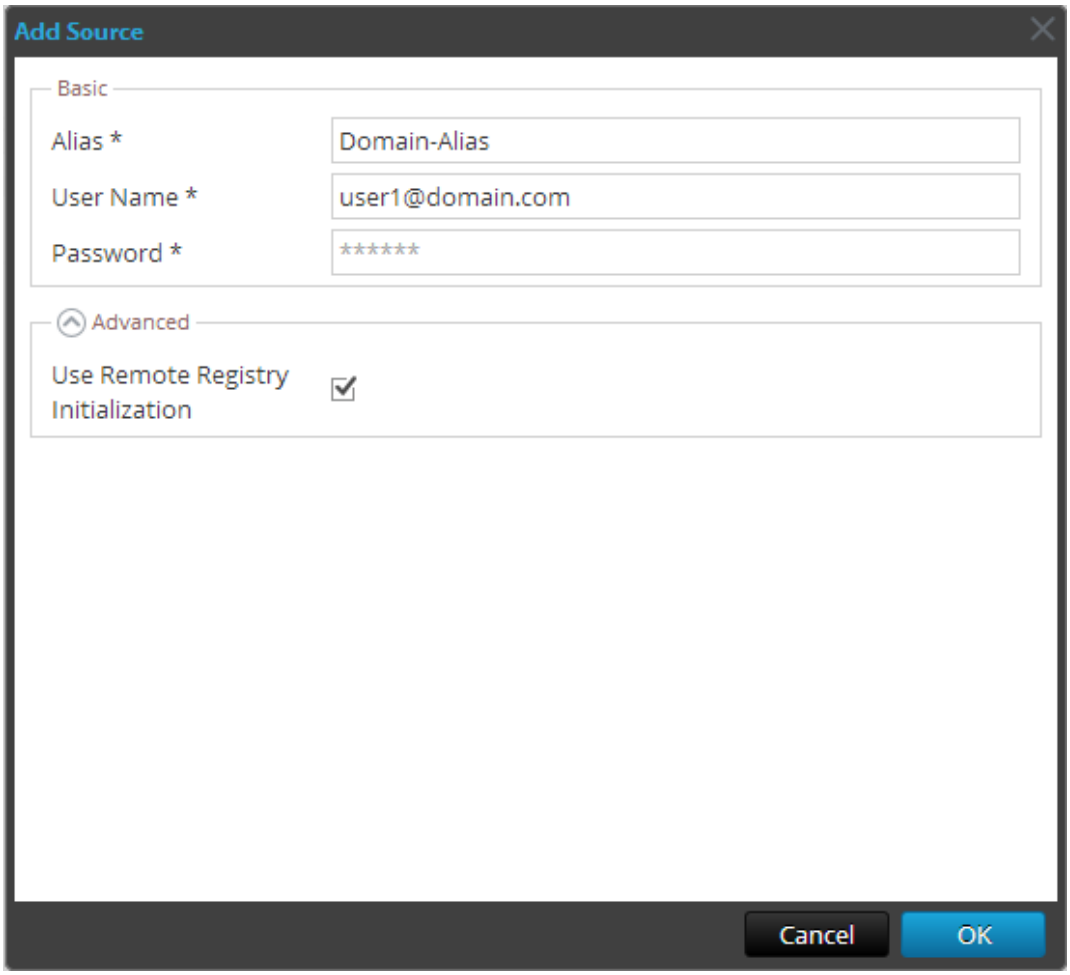
1. Installed the NetWitness Suite Windows Legacy Remote Collector on a physical or virtual Windows 2008 64-bit server.
2. Added this Windows Legacy Remote Collector to NetWitness Suite.

Add a Windows Legacy Event Source

1. Access the Services view by selecting **Admin > Services** from the NetWitness Suite menu.
2. In the **Services** grid, select a **Windows Legacy Log Decoder** service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. In the **Event Sources** tab, select one of the following options from the drop-down menu.
    - Windows Legacy/Windows.
    - Windows Legacy/NetApp.
6. Configure the alias:
    a. Click in the **Event Categories** panel toolbar.

    The **Add Source** dialog is displayed.

    b. Specify values for the parameters and click **OK**.



Note: By default, **Remote Registry Initialization** is selected. For details, see Remote Registry Access below.

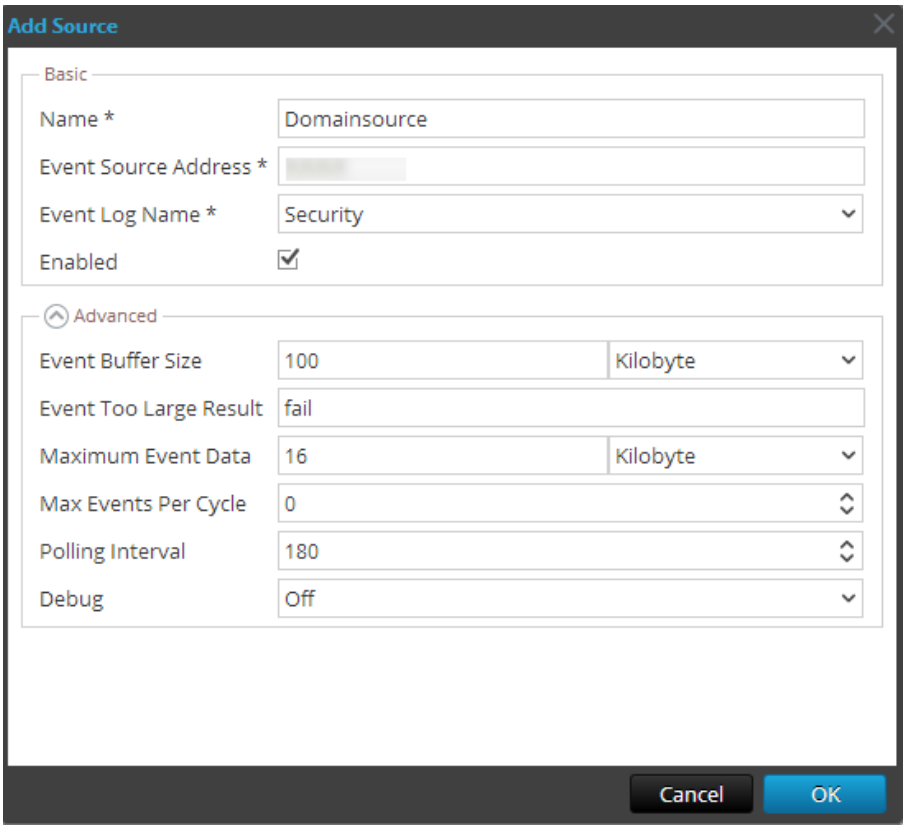
The newly added windows event source type is displayed in the **Event Categories** panel.

7. Add the event source:

   a. Select the new alias in the **Event Categories** panel and click + in the **Source** panel toolbar.

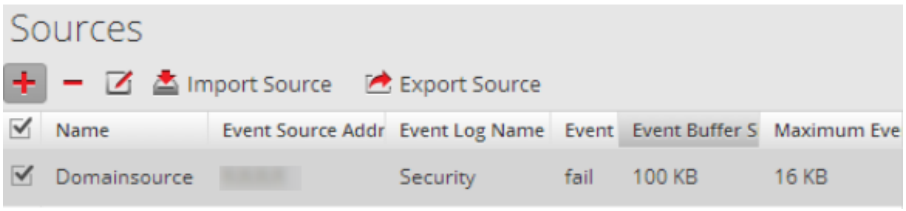
      The **Add Source** dialog is displayed.

   b. Specify values for the event source parameters and click **OK**.



For details, see Windows Legacy Configuration Parameters below.

The newly added Windows event source is displayed in the **Event Categories** panel.



Remote Registry Access

Windows Legacy Collector performs an initial verification of the event source before collecting data. By default, Windows Legacy Collector uses Windows Management Instrumentation (WMI) method to perform this initial verification. If you enable Remote registry access method, Windows Legacy Collector performs a remote registry query to verify the event source.

Configure Push or Pull between Log Collector and Windows Legacy Collector

You can configure the Windows Legacy Collector to push event data to a Local Collector, or you can configure a Local Collector to pull event data from the Windows Legacy Collector.

To configure a Local Collector or the Windows Legacy Collector:

1. Go to **ADMIN > Services**.
2. Select a Local Collector or the Windows Legacy Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Depending on your selection in step 2:
   - If you selected a Local Collector, the **Remote Collectors** tab is displayed. Select the Windows Legacy Collector from which the Local Collector pulls events in this tab.
   - If you selected a Windows Legacy Collector, the **Local Collectors** are displayed. Select the Local Collectors to which the Windows Legacy Collector pushes events in this tab.

Windows Legacy Configuration Parameters

The following table describes the parameters for a Windows Legacy event source.

Feature	Description
	Basic
Name*	The name of the event source. Valid value is a name in the **[_a-zA-Z] [_a-zA-Z0-9]*** range. You can use a dash "-" as part of the name.
Event Source Address*	IP address of the event source. Valid value is an IPv4 address, IPv6 address, or a hostname including a fully qualified domain name. NetWitness Suite defaults to **127.0.0.1**. Log Collector converts the hostname to lower-case letters to prevent duplicate entries.

Feature	Description
Event Log Name	The name of the event log from which to collect event data (for example, **System**, **Application**, or **Security**). The following are examples of some of these channels: • **System** - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system. • **Application** - all user-level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application-specific channel for it. • **Security** - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority.
Enabled	Select this checkbox to collect from this event source. If you do not check this checkbox, the Log Collector does not collect events from this event source.

Event Directory Path	NetApp **.evt or.evtx** files directory path. This must be the UNC path.
	The NetApp generates event data and saves it in.evt or.evtx files in a shareable directory on the NetApp appliance.
	• In each polling cycle, Log Collector browses the configured NetApp shared path for the.evt files that you identified with the **Event Directory Path** and **Event File Prefix parameters**. Log Collector :
	  ◦ sorts files that match the **event-file-prefix.YYMMDDhhmmss.evt** format in ascending order.
	  ◦ uses the timestamp of the last file processed to determine the files that still need processing. If Log Collector finds a partially processed file, it skips the events already processed.
	• In each polling cycle, Log Collector browses the configured NetApp shared path for the **.evtx** files that you identified with the **Event Directory Path** and **Event File Prefix parameters**. Log Collector :
	  ◦ sorts files that match the **event-file-prefix.YYMMDDhhmmssms.evtx** format in ascending order.
	  ◦ uses the timestamp of the last file processed to determine the files that still need processing. If Log Collector finds a partially processed file, it skips the events already processed.

Feature	Description
Event File Prefix	Prefix of the **.evt** files (for example, **adtlog**.) saved in the **Event Directory Path**.
	Advanced
Event Buffer Size	Maximum size of the data the Log Collector pulls from the event source for each request. Valid value is a number in **0** to **511** Kilobytes range. You specify this value in **Kilobytes**.
Event Too Large Result	Tells Log Collector what to do if an event is too large for the event buffer.
Maximum Event Data	Maximum size of event data to include in the output. Valid value is a number in **0** to **511Kilobytes** range. You specify this value in **Kilobytes** or **Megabytes**. • 1 Kilobyte - 100 Megabytes • 0 = do not include event data in the output.
Max Events Per Cycle	The maximum number of events per polling cycle (how many events collected per polling cycle).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.

Feature	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). Limit the number of event sources for which you use Verbose debugging to minimize performance impact.
Cancel	Closes the dialog without adding the Windows Legacy event source.
OK	Adds the current parameter values as a new event source

Troubleshoot Windows Legacy and NetApp Collection

This topic highlights possible problems that you may encounter with Windows Legacy Collection (LWC) and suggested solutions to these problems.

Note: In general, you receive more robust log messages by disabling SSL.

Protocol Restart Problems

Problem	Possible Causes	Solutions
You restart the Legacy Windows collection protocol, but NetWitness Suite is not receiving events.	The logcollector service is stopped.	Restart the **logcollector** service. 1. Log on to the **Windows Legacy Remote Collector**. 2. Go to **Start > Administrative Tools > Task Scheduler** and click on **Task Scheduler Library**. 3. In the right panel, look for the **restartnwlogcollector** task and make sure that it is running. 4. If this is not the case, right-click **restartnwlogcollector** and select **Run**.

Installation Problems

If you see any of the following messages in the **MessageBroker.log**, you may have issues.

Log Messages	Any message that contains "rabbitmq"
Possible Cause	RabbitMQ service may not be running. Port **5671** may not be opened.
Solutions	Make sure that the RabbitMQ service is running. Make sure that port **5671** is open.
Log Messages	Error: Adding logcollector user account. Error: Adding administrator tag to logcollector account. Error: Adding Adding logcollection vhost. Error: Setting permissions to logcollector account in all vhosts.

Possible Cause	**rabbitmq-server** was not running when installer tried to create users and vhosts.
Solutions	Make sure that the **RabbitMQ** service is running and run below commands manually. rabbitmqctl -q add_user logcollector netwitness rabbitmqctl -q set_user_tags logcollector administrator rabbitmqctl -q add_vhost logcollection rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*" rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"

Windows Legacy Federation Script Issues

If you see any of the following messages in the federation script log, you may have issues.

Problem	Possible Symptoms	Solutions
Federation script started, b ut the LWC service went down.	NetWitness Suite log shows connection failure exceptions with Windows Legacy Collector.	This issue is fixed automatically after restarting the Windows Legacy service.

Problem	Possible Symptoms	Solutions

LWC is running, but RabbitMQ service is down or restarting.	Federation log file at Windows Legacy side displays an error message about RabbitMQ service being down.
	The log file to look at is: **C:\NetWitness\ng\logcollector**
	The following error message is logged in case RabbitMQ is not running:
	`"Unable to connect to node logcollector@localhost: nodedown"`
	The following diagnostics messages are displayed:
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost:`
	`* connected to epmd (port 4369) on localhost`
	`* epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084']`
	`* suggestion: start the node`
		Run the **federation.bat** script manually at LWC.
		To run the **federate.bat** script manually, perform the following steps:
		1. Go to folder C**:\Program Files\NwLogCollector** where the Windows Legacy instance is installed.
		2. Locate the file **federate.bat i**n this folder. Select the file and right click.
		3. Select **Run as Administrator**.
		4. To monitor the log file, navigate to **C:\NetWitness\ng\logcollector\federate.log** while the **federate.bat** script is being executed.
		Note: Make sure the log file does not show any errors while the script is being executed.

RabbitMQ service is down on the NetWitness Suite side.	NetWitness Suite User Interface pages do not work.	Restart RabbitMQ service.

Problem	Possible Symptoms	Solutions
Customer receives a Health and Wellness notification, or the following Health and Wellness Alarm is displayed: "Communication failure between Master NetWitness Suite Host and a Remote Host" with LWC Host as the Remote IP.	**Federate.bat** script failed to run successfully.	If the **Federate.bat** script did not run correctly, run it manually as described previously.

Windows Log Collection for Endpoint Agents

In 11.1, Windows Log collection can be achieved using the RSA® NetWitness® Endpoint Insights Agent. When the agent is enabled for log collection, a log configuration file is included with the Agent Packager to enable collection and forwarding of windows logs in addition to the Endpoint data. The generated configuration file contains information of the channels from which logs are to be collected from and the destination (Log Decoder or a Remote Log Collector) to forward the defined windows events. The generated Agent packager is able to collect both Endpoint and Windows log data from hosts. The Endpoint Agent packager is extracted locally on a Windows machine to create the agent installer file. The installer file is then deployed through a third party software distribution tool to all endpoints in your network.

There are three scenarios for Windows log collection, these are:

1. **Generate Agent with Log Collection**: If the **Enable Windows Log Collection** option is enabled and you click **Generate Agent** after filling the details. The generated AgentPackager.zip contains the log collection file. For more information, see the "Generating an Agent Packager with Windows Log Collection" in the *Endpoint Insights Agent Installation Guide* .

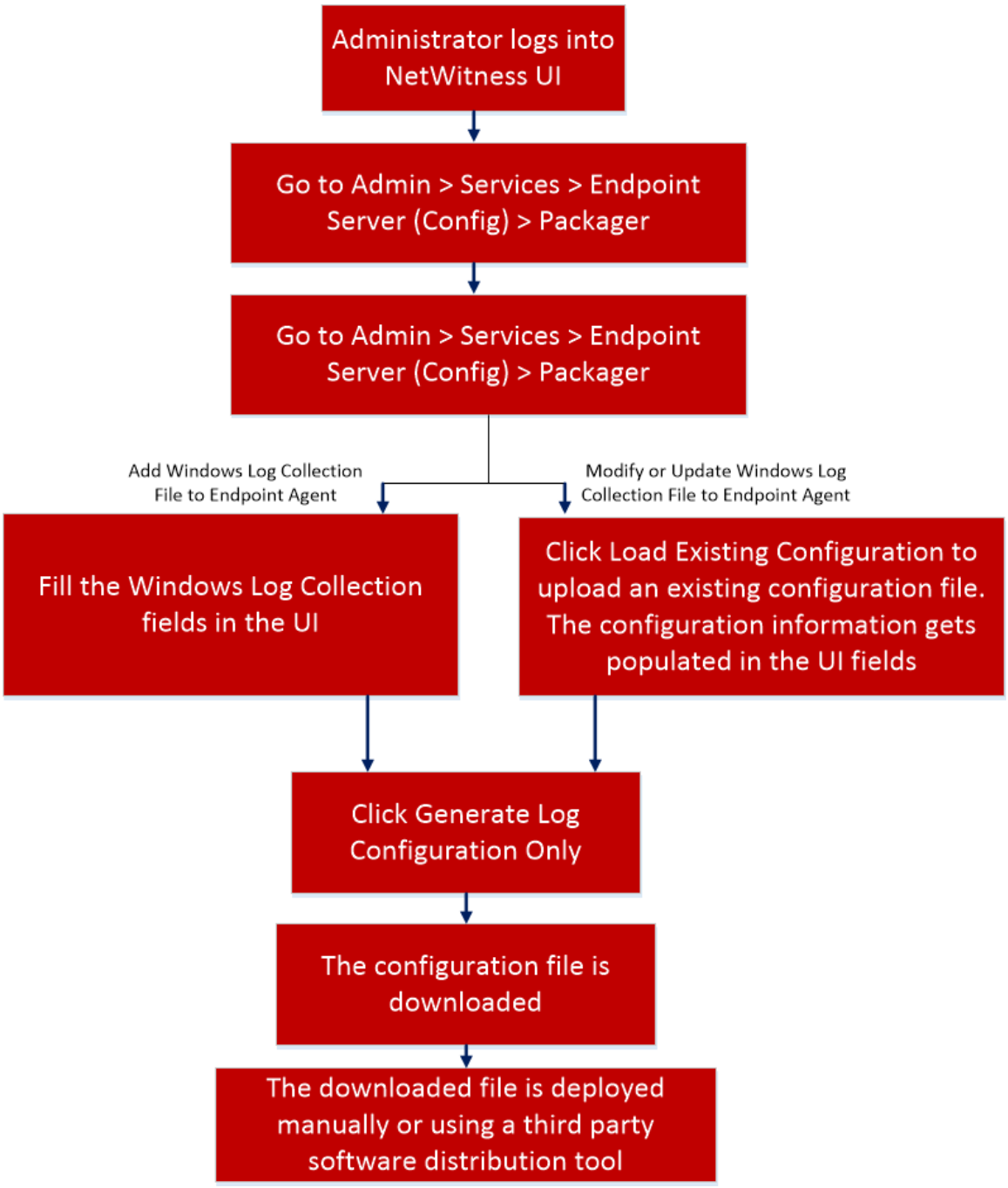
2. **Generate Agent file only Without Log Collection**: If the **Enable Windows Log Collection** is disabled and you click **Generate Agent** then only the Zip file gets created without the log collection file. For more information, see the "Generate an Endpoint Agent Packager" in the *Endpoint Insights Agent Installation Guide* .
3. If you click on **Generate Log Configuration Only** then only the log configuration gets created. This can be used to update the log configuration file in an existing Endpoint agent deployment for log collection or to add the log configuration to an Endpoint agent deployment. For more information, see "Add or Update Windows Log Collection Configuration to an existing Endpoint Agent".

Add or Update Windows Log Collection Configuration to an existing Endpoint Agent

You can add a Windows Log Collection Configuration file to an Endpoint Agent and also modify an existing log collection configuration file. If a change is required in the log collection configuration for endpoint agents, the agents do not require to be installed again. The log configuration file (`nwelcfg file`) can be generated from the Packager User Interface and modified.

Workflow

This workflow shows the procedure to add of update a Windows Log Collection Configuration file.



Following are some example reasons that would require a change in the configuration:

1. The destination to which the windows are to be forwarded needs to be changed for better load management in the destination side.
2. The endpoint is moved to a new group defined by a third party endpoint management system which needs a change in the destination or list of event ids to be forwarded.
3. There are requirements to change the list of event ids consumed at the destination side.

A new configuration file can be generated either by entering the new values in the Packager screen or by loading an existing configuration file.

Note: The endpoint agent is built to read the `nwelcfg` file with the latest timestamp under the config folder. So, please ensure the third party endpoint management tool updates the timestamp of the file to the current time of endpoint while pushing the configuration file.

Follow these steps to add or update a Windows log collection configuration file to an existing Endpoint Agent:

1. In the Packager UI, perform one of the following:
   a. To add the Windows Log Collection Configuration: Fill the required information mentioned in the "Generating an Agent Packager with Windows Log Collection" in the *Endpoint Insights Agent Installation Guide* .
   b. To update the Windows Log Collection Configuration: Click **Load Existing Configuration** and edit the intended fields mentioned in the "Generating an Agent Packager with Windows Log Collection" in the *Endpoint Insights Agent Installation Guide* .
2. Click **Generate Log Configuration Only** to generate the `nwelcfg`file.
3. Copy the downloaded `nwelcfg` file to the Endpoint Agent from where the logs are to be forwarded. The configuration file should be copied to %ProgramData%\NWEAgent folder. To deploy the configuration file to multiple agents, use the third party software distribution tool.

The agent is designed to pick the log configuration file holding the latest timestamp. If there is a time zone difference, please make sure the configuration file is updated to the agent's timestamp after copying. This can be achieved by running the command on the agent: `copy /b <filename.nwelcfg> +,,` from the folder %programdata%\NWEAgent\ where the nwelcfg file is there.

Verify Windows Log Collection

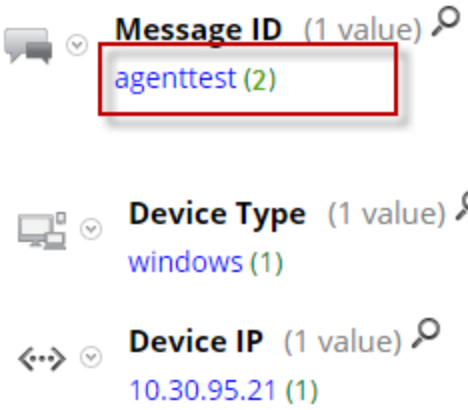
To verify the windows log collection is successfully deployed on an Endpoint Agent, follow these steps:

1. Go to **ADMIN** > **Health & Wellness** > **Event Source Monitoring**.
2. In the Time Frame field, select **Last 5 minutes** or **Last 10 Minutes** depending on when the Agents were installed.
3. Click **Apply**.

4. In the list displayed, the IP address of the Agent should be displayed in the Event Source column with Event Source Type as windows. This confirms the Agent was installed successfully.

To verify a windows log collection has been updated successfully, follow these steps:

1. Go to **INVESTIGATE** > **Navigate**. Wait for 2-3 minutes until this config file is picked by the Endpoint agent.
2. Select the **Concentrator** from **Investigate**.
3. Change the timeline to **last 5 minutes** or as applicable.
4. Click **Load Values**.
5. Search for message ID meta key.
6. There should be an agent.test value. An increase in the number of events signifies that the updation is done successfully.



Enable log forwarding and Configure Log Decoder

If you want to enable log forwarding feature and configure the log decoder in endpoint hybrid as a destination in the Packager UI. Then you have to add the ports, TCP/UDP 514 in the iptables file on Endpoint Hybrid.

Follow these steps to add the ports:

1. For TCP, you have to add the "514" port to the existing list of ports in the `/etc/sysconfig/iptables` file on Endpoint Hybrid: `A INPUT -p tcp -m tcp -m multiport --dports 514, 6514,50002,50102,50202,56002,56202 -m comment --comment "nwlogdecoderPorts" -m conntrack --ctstate NEW -j ACCEPT -`

2. For UDP, you have to add the below content in the `/etc/sysconfig/iptables` file in Endpoint Hybrid: `-A INPUT -p udp -m udp -m multiport --dports 514 -m comment --comment "nwlogcollectorUdpPorts" -m conntrack --ctstate NEW -j ACCEPT`
3. Restart iptables service for the above new configurations to take effect: `service iptables restart`.

Related Topics

Troubleshooting - Windows log Collection using Endpoint Agent

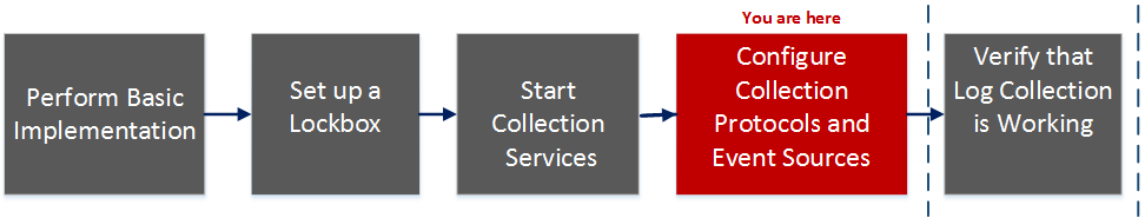
Reference

AWS Parameters

This topic provides an overview of the AWS collection configuration parameters for deploying a remote log collection service (VLC) in an Amazon Web Services (AWS) environment.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Configure AWS (CloudTrail) Event Sources in NetWitness Suite

The following table describes the available configuration parameter for AWS collection.

Parameter	Description
Parameter	**Description**
	Basic
Name *	Name of the event source.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Account Id *	Account Identification code of the S3 Bucket

Parameter	Description
S3 Bucket Name *	Name of the AWS (CloudTrail) S3 bucket. Amazon S3 bucket names are globally unique, regardless of the AWS (CloudTrail) region in which you create the bucket. You specify the name at the time you create the bucket. Bucket names should comply with DNS naming conventions. The rules for DNS-compliant bucket names are: • Bucket names must be at least three and no more than 63 characters long. • Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period “.”. Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number. • Bucket names must not be formatted as an IP address (for example, 192.168.5.4). The following examples are **valid** bucket names: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** The following examples are **invalid** bucket names: • **.myawsbucket** - Do not start a Bucket Name with a period ".". • **myawsbucket.** - Do not end a Bucket Name with a period ".". • **my..examplebucket** - Only use one period between labels.
Access Key *	Key used to access the S3 bucket. Access Keys are used to make seure REST or Query protocol requests to any AWS service API. Please refer to Manage User Credentials on the Amazon Web Services support site for more information on Access Keys.
Secret Key *	Secret key used to access the S3 bucket.
Region *	Region of the S3 bucket. **us-east-1** is the default value.

Parameter	Description
Region Endpoint	Specifies the AWS CloudTrail hostname. For example, for an AWS public cloud for us-east region, the Region Endpoint would be s3.amazonaws.com. More information can be found at http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. This parameter is necessary to collect CloudTrail logs from AWS Government or Private clouds.
Use Proxy	Enable **Use Proxy** to set proxy for AWS server. By default, it is disabled.
Proxy Server	Enter the proxy name you want to connect to access the AWS server.
Proxy Port	Enter the port number that connects to the proxy server to access the AWS server.
Proxy User	Enter the user name to authenticate with the proxy server.
Proxy Password	Enter the password to authenticate with proxy port.
Start Date *	Starts AWS (CloudTrail) collection from the specified number of days in the past, measured from the current timestamp. The default value is 0, which starts from today. The range is 0–89 days.
Log File Prefix	Prefix of the files to be processed. **Note:** If you set a prefix when you set up your CloudTrail service, make sure to enter the same prefix in this parameter.
Advanced	

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Command Args	Arguments added to the script.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 60. For example, if you specify 60, the collector schedules a polling of the event source every 60 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 60 seconds for the polling to start because the threads are busy.
SSL Enabled	Select the check box to communicate using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The check box is selected by default.

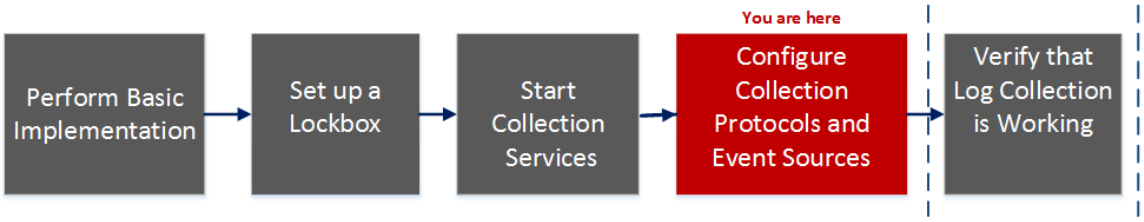
Parameter	Description
Test Connection	Validates the configuration parameters specified in this dialog are correct. For example, this test validates that: • NetWitness can connect with the S3 Bucket in AWS using the credentials specified in this dialog. • NetWitness can download a log file from the bucket (test connection would fail if there were no log files for the entire bucket, but this would be extremely unlikely).
Cancel	Closes the dialog without adding the AWS (CloudTrail).
OK	Adds the current parameter values as a new AWS (CloudTrail).

Azure Parameters

Microsoft Azure is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Configure Azure Event Sources in NetWitness Suite

Azure Event Source Configuration Parameters

This topic describes the Azure event source configuration parameters.

Note: Items that are followed by an asterisk (*) are required.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Client ID *	The Client ID is found the Azure Application Configure tab. Scroll down until you see it.
Client Secret *	When you are configuring the event source, the client secret is displayed when you are creating a key, and you select a duration of validation. Make sure to save this, because you will only be able to see it once, and it cannot be retrieved later.
API Resource Base URL *	Enter `https://management.azure.com/`. Be sure to include the trailing slash (/).
Federation Metadata Endpoint *	In your Azure application, click the **View Endpoints** button (near the bottom of the pane). There are a lot of links that all begin with the same string. Compare the URLs and find the common string that begins most of them. This common string is the endpoint that you need to enter here.
Subscription ID *	You can find this in the Microsoft Azure dashboard: click on Subscriptions at the bottom of the list on the left.
Tenant Domain *	Go to the active directory and click on the directory. In the URL, the tenant domain is the string directly following **manage.windowsazure.com/**. The tenant domain is the string up to and including the **.com**.
Resource Group Names *	In Azure, select Resource groups from the left navigation pane, then select your group.
Start Date *	Choose the date from which to start collecting. Default's to the current date.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click next to **Advanced** to view and edit the advanced parameters, if necessary.

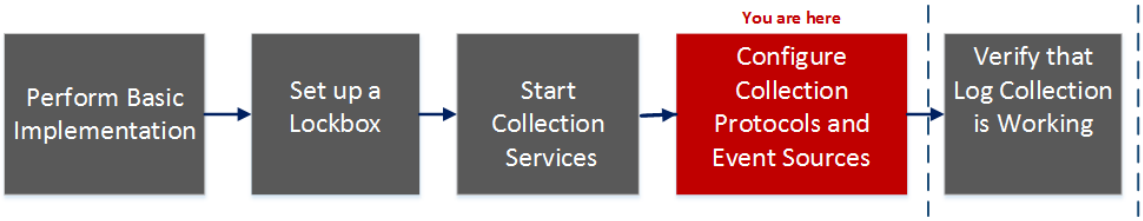
Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. **Caution:** Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Check Point Parameters

The Check Point Collection protocol collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Configure Check Point Event Sources in NetWitness Suite

Check Point Collection Configuration Parameters

Basic Parameters

Parameter	Description
Name*	Name of the event source.
Address*	IP Address of the Check Point server.
Server Name*	Name of the Check Point server.
Certificate Name	Certificate name for secure connections to use when the transport mode is https. If set, the certificate must exist in the certificate trust store that you created using the Settings tab. Select a certificate from the drop-down list. The file naming convention for Check Point event source certificates is **checkpoint_*name-of-event-source***.
Client Distinguished	Enter the Client Distinguished Name from the Check Point server.
Client Entity Name	Enter the Client Entity Name from the Check Point server.
Server Distinguished	Enter the Server Distinguished Name from the Check Point server.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Pull Certificate	Select the checkbox to pull a certificate for first time. Pulling a certificate makes it available from the trust store.
Certificate Server Address	IP Address of the server on which the certificate resides. Defaults to the event source address.
Password	Only active when you select the Pull Certificate checkbox for first time. Password required to pull the certificate. The password is the activation key created when adding an OPSEC application to Check Point on the Check Point server.

Determine Advanced Parameter Values for Check Point Collection

You use less system resources when you configure a Check Point event source connection to stay open for a specific time and specific event volume (transient connection). RSA NetWitness Suite defaults to the following connection parameters that establish a transient connection:

- Polling Interval = **180** (3 minutes)
- Max Duration Poll = **120** (2 minutes)
- Max Events Poll = **5000** (5000 events per polling interval)
- Max Idle Time Poll = **0**

For very active Check Point event sources, it is a good practice to set up a connection that stays open until you stop collection (persistent connection). This ensures that Check Point collection maintains the pace of the events generated by these active event sources. The persistent connection avoids restart and connection delays and prevents Check Point collection from lagging behind event generation.

To establish a persistent connection for a Check Point event source, set the following parameters to the following values:

- Polling Interval = **-1**
- Max Duration Poll = **0**
- Max Events Poll = **0**
- Max Idle Time Poll = **0**

Parameter	Description
Port	Port on the Check Point server that Log Collector connects to. Default value is 18184.

Parameter	Description
Collect Log Type	Type of logs that you want to collect: Valid values are: • **Audit** - collects audit events. • **Security** - collects security events. If you want to collect both audit and security events, you must create a duplicate event source. For example, first you would create an event source with Audit selected pulling a certificate into the trust store for this event source. Next you would create another event source with the same values except that you would select Security for the Collect Log Type and you would select the same certificate in Certificate Name that you pulled when you set up the first set of parameters for this event source and you would make sure that Pull Certificate was not selected.
Collect Logs From	When you set up a Check Point event source, NetWitness collects events from the current log file. Valid values are: • **Now** - Start collecting logs now (at this point in time in the current log file). • **Start of Log** - Collect logs from the beginning of the current log file. If you choose "Start of Log" for this parameter value, you may collect a very large amount of data depending on how long the current log file has been collecting events. Note that this option is effective only for the first collection session.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).

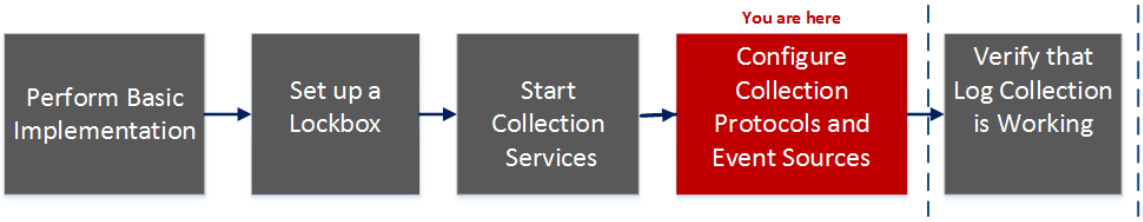
Parameter	Description
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.> **300** is the default value.
Forwarder	Enables or disables the Check Point server as a forwarder. By default it is disabled.
Log Type (Name Value Pair)	Logs from the event source in Name Value format. By default it is disabled.
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables and disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).

File Parameters

This topic describes the File Collection configuration parameters.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Configure File Event Sources in NetWitness Suite

File Collection Event Source Parameters

The following table provides descriptions of the File Collection source parameters.

Name	Description
	Basic
File Directory*	Collection directory (for example, **Eur_London100**) into which the File event source places its files. Valid value is a character string that is conforms to the following regular expression: **[_a-zA-Z][_a-zA-Z0-9]*** This means that the file directory must start with a letter followed by numbers, letters, and underscores. Do not modify this parameter after you start collecting event data. After you create the collection, the Log Collector creates the work, save, and error sub-directories under the collection directory.
Address*	IP address of the event source. Valid value is an **IPv4 address**, **IPv6 address**, or a **hostname** including a fully-qualified domain name.
File Spec	Regular expression. For example, **^.*$** = process everything.
File Encoding	Internationalization file encoding. Enter the File Encoding method, the following strings are examples of valid methods: • UTF-8 (default) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
	Advanced

Name	Description
Ignore Encoding Conversion Errors	Select the check box to ignore encoding conversion errors and ignore invalid data. The check box is selected by default. **Caution:** This may cause parsing and transformation errors.
File Disk Quota	Determines when to stop saving files regardless of the **Save On Error** and **Save On Success** parameter settings. For example, a value of 10 indicates that when there is less than 10% available disk left, the Log Collector stops saving files to reserve enough space for your estimated normal collection processing. **Caution:** Available disk refers to a partition where the base collection directory is mounted. If the Log Decoder server has a 10TB disk size and 2TB is allocated to base collection directory, then setting this value to 10 causes log collection to stop when less than 0.2TB (10% of 2TB) of space is left. It does not mean 10% of 10TB. Valid value is a number in the **0** to **100** range. **10** is the default.
Sequential Processing	Sequential processing flag: • Select the check box (default) to process event source files in collection order. • Do not select the checkbox to process event source files in parallel.
Save On Error	Save on error flag. Check the checkbox to retain the **eventsource collection** file when the Log Collector it encounters an error. The check box is selected by default.
Save On Success	Save **eventsource collection** file after processing flag. Check the checkbox to save the eventsource collection file after processing it. The check box is not selected by default.

Name	Description
Eventsource SSH Key	SSH public key used to upload files for this event source. Please refer to the *Generate Key Pair on Event Source and Import Public Key to Log Collector* section in the Install and Update the SFTP Agent Guide for instructions on generating keys. **Note:** If File collection is stopped, NetWitness Suite does not update the authorized_keys file with the SSH public key that you add or modify in this parameter. You must restart File collection to update the public key. You can add or modify the value of the public key in this parameter in multiple File event sources without File collection running, but NetWitness Suite will not update the **authorized_keys** file until File collection is restarted.
Manage Error Files	By default, the Log Collectoruses the **File Disk Quota** parameter to ensure that the disk does not fill up with error files. If you set this parameter to **true**, you can specify one of these: • Maximum space allotted to error files in the **Error Files Size** parameter. • Maximum number of error files allowed in **Error Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached. Select the check box to manage error files. The check box is not selected by default.
Error Files Size	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Specifies to what extent NetWitness Suite saves error files. The value that you specify is the maximum total size of all the files in the error directory. Valid value is a number in **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Error Files Count	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Maximum number of error files allowed in the error directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.

Name	Description
Error Files Reduction %	Percent amount by size or count of the error files that the Log Collectorservice removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.
Manage Saved Files	Select the check box to manage saved files. The check box is not selected by default. By default, the Log Collector uses the **File Disk Quota** parameter to ensure that the disk does not fill up with saved files. If check this check box, you can specify one of these: • Maximum space allotted to saved files in the **Saved Files Size** parameter. • Maximum number of saved files allowed in **Saved Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached.
Saved Files Size	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum total size of all the files in the save directory. Valid value is a number in the **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved Files Count	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum number of saved files in the save directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved File Reduction %	Percent amount by size or count of the saved files that the Log Collector service removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

Log Collection Service System View

A Log Collector is a service that runs on a Log Decoder host (referred to as a Local Collector) or sends events from a Remote Collector to a Local Collector, and is configured and managed in a similar way to a Log Decoder.

To access the Log Collection Service System view, go to ADMIN > Services and select a Log Collector service, then select View > System.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.

What do you want to do?

Role	I want to ...	Documentation
Administrator	Perform basic Log Collection implementation	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings	Set Up a Lockbox
Administrator	*Start Log Collection Services.	Start Collection Services
Administrator	Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

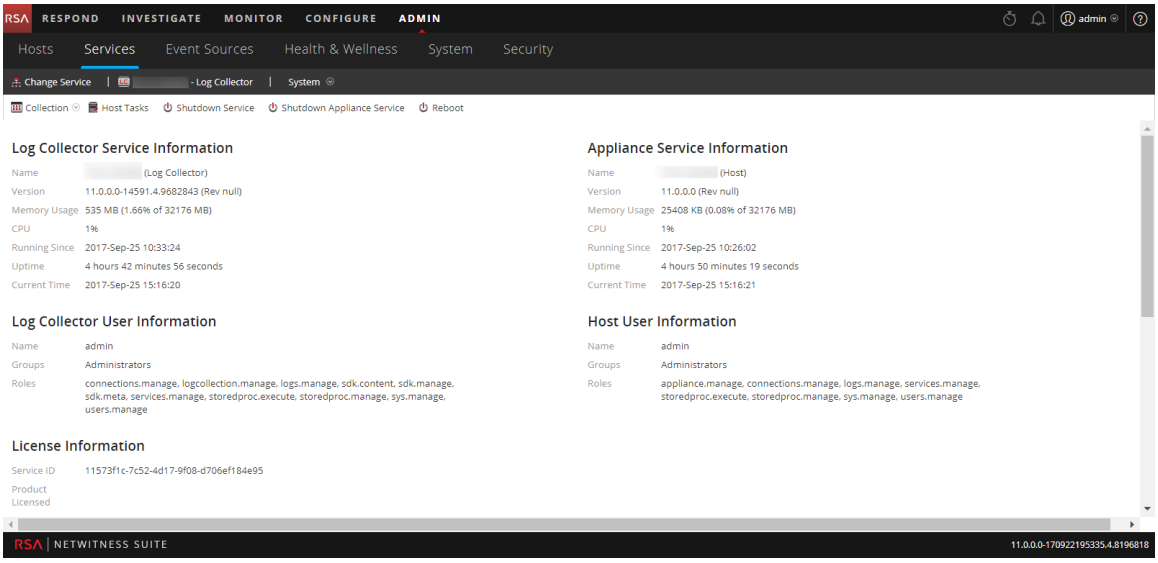
*You can perform this task here.

Related Topics

Basic Implementation

Quick Look

From the Log Collector Service Information Toolbar, you can manage event data using the Collection icon to start event data from a stopped protocol or stop collecting data from a started protocol. From the Host Tasks icon, you can select tasks that you want to run. You can also shutdown your service and reboot your service from the Service Information Toolbar.



ODBC Event Source Configuration Parameters

This topic tells you how to configure ODBC collection protocol which collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface.

Access ODBC Configuration Parameters

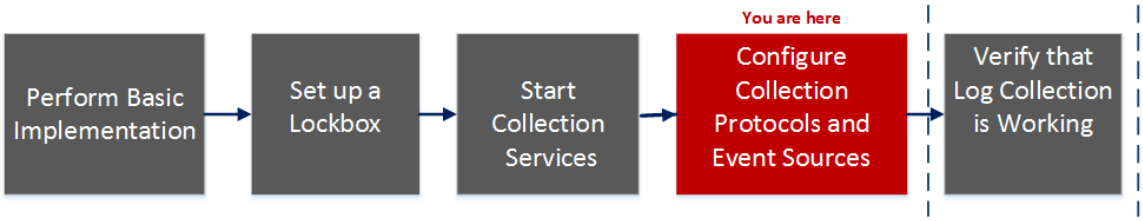
To access the ODBC Event Source Configuration Parameters:

1. Go to **Administration > Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **View > Config** to display the Log Collection configuration parameter tabs.

   The **Service Config** view is displayed with the Log Collector **General** tab open.
4. Click the **Event Sources** tab, and select **ODBC/Config** from the drop-down menu.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services

Role	I want to...	Documentation
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Configure ODBC Event Sources in NetWitness Suite
- Configure Data Source Names (DSNs)
- Troubleshoot ODBC Collection
- Create Custom Typespec for ODBC Collection

Data Source Name (DSN) Parameters

Use the Sources panel to review, add, modify, and delete Data Source Name (DSN) parameters.

Sources Panel

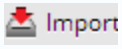
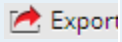
An ODBC DSN tells the Log Collector how to reach an ODBC endpoint. You refer to an ODBC DSN when you configure a data source name with information such as which ODBC driver to use or the host name and port of the ODBC endpoint.

An ODBC DSN is a sequence of name-value pairs. For information about the valid names for a given ODBC data source type, such as Sybase, Microsoft SQL Server, or Oracle, please download the *DataDirect Connect Series for ODBC User's Guide and DataDirect Connect Series for ODBC User's Guide* in the Progress DataDirect Document Library.

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
+	Opens the Add DSN dialog in which you add an event source for the event source type you selected in the Event Categories panel.
−	Deletes the selected event sources.

Option	Description
	Opens the Edit DSN dialog in which you modify the configuration parameters for the selected event source. When you select multiple event sources, this option opens the Bulk Edit Source dialog in which you can edit the parameters values for the selected file directories. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
	Opens the Bulk Add Option dialog in which you can import DSN parameters in bulk from a comma-separated values (CSV) file. The Bulk Add Option dialog has the following two options. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
	Creates a **.csv** file that contains the parameters for the selected DSNs. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
	Validates the configuration parameters for the selected ODBC database. Refer to the *Log Collection Configuration Guide*for detailed steps on how to test event source connections in bulk.

Add or Edit DSN Dialog

In this dialog, you add or modify an event source for the selected event source.

Name	Description
	Basic
DSN*	The data source name (DSN) that defines the database from which to collect events. Select an existing DSN from the drop-down list. For details, see ODBC DSNs Event Source Configuration Parameters.
Username*	User name that the data source name uses to connect to the database. You must specify a user name when you create the event source.
Password	Password that the data source name uses to connect to the database. **Caution:** The password is encrypted internally and is displayed in its encrypted form.

Name	Description
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Address*	For ODBC, this field is not used. The Log Collector uses the address in the **ODBC.ini** file.
	Advanced
Max Cell Size	Maximum size in bytes of the data that the Log Collector can pull from one cell in the database. The default value is **2048**.
Nil Value	Character string that the Log Collector displays when NIL is returned for a cell in the database. Default value: **“”** (null).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Name	Description
Initial Tracking Id	Initial identification code that the Log Collector assigns to this event source if collection is not started. If there is no value for this parameter, the Log Collector starts at the end of the table and only pulls rows after the end of the table as they are added. The default value is **“”** (null).
Filename	For Microsoft SQL Server Event Sources only, the location of the trace files directory (for example, **C:\MyTraceFiles**). Please refer to the RSA Microsoft SQL Server Event Source Configuration Guide, located on RSA Secure Care Online (SCOL) for detailed information on how to create this directory with the correct permissions.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.
Cancel	Closes the dialog without adding or modifying DSN parameters.
OK	Adds or modifies the parameters for the DSN.

ODBC DSNs Event Source Configuration Parameters

Open Database Connectivity (ODBC) event sources require Data Source Names (DSNs) so you need to define DSNs with their associate value pairs for ODBC event source configuration.

Access ODBC Configuration Parameters

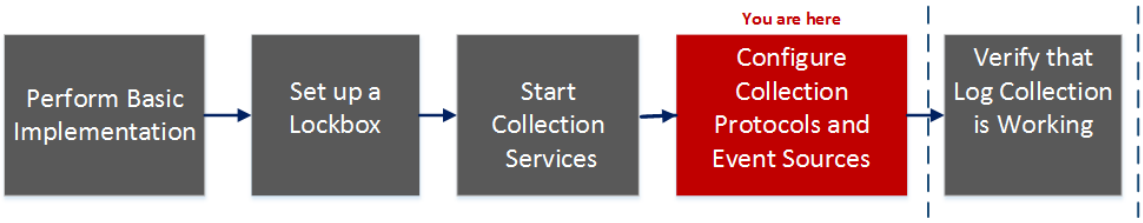
To access the ODBC Event Source Configuration Parameters:

1. Access the Services view by selecting **Admin > Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **View > Config** to display the Log Collection configuration parameter tabs.

   The **Service Config** view is displayed with the Log Collector **General** tab open.
4. Click the **Event Sources** tab, and select **ODBC/DSNs** from the drop-down menu.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services

Role	I want to...	Documentation
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

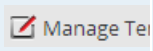
- Configure ODBC Event Sources in NetWitness Suite
- Configure Data Source Names (DSNs)

ODBC DSN Configuration Parameters

This topic describes the Data Source Names DSNs configuration parameters.

DSN Panel

In the DSNs panel, you can add, delete, or edit DSNs and the DSN name-value pairs for ODBC Event sources.

Feature	Description
	Displays the Add DSN dialog in which you define a DSN and its parameters.
	Deletes the selected DSNs.
	Displays the Edit DSN dialog in which you edit the name-value pairs for the selected DSN.
	Displays the Manage DSN Templates dialog in which you can add or delete DSN name-value pair templates.
	Selects DSNs.
DSN	Name of the DSN that you added.
Parameters	**<name-value for="" p="" pairs="" the=""> </name-value>**

Add or Edit DSN Dialog

In this dialog, you add or modify a file directory for the selected event source.

Feature	Description
DSN Template	Select a predefined DSN value name-value pairs template for the DSN.
DSN Name*	Add the name of the DSN. You cannot edit a DSN name after you add it. This value must correspond with a DSN entry in the ODBC.ini file. Valid value is a character string that is restricted to the following characters: [_a-zA-Z][_a-zA-Z0-9]* This means that the file directory must start with a letter followed by numbers, letters, and underscores (for example, **oracle_executive_compensation**).
Parameters	Adds a row in which you can define a parameter name-value pair. Deletes the selected parameter name-value pair. Selects parameter name-value pairs. Name - Enter or modify the parameter name. Value - Enter or modify the value associated with the parameter name.
Cancel	Closes the dialog without adding the DSN and its name-value pairs or saving modifications to the name-value pairs.
Save	Adds the DSN and its name-value pairs or saves modifications to the name-value pairs.

Manage DSN Templates Dialog

In this dialog, you can add or delete DSN name-value pair templates.

Feature	Description
	Template Selection Panel
	Opens the Add Template panel in which you can add a DSN name-value pair template.

Feature	Description
	Deletes the selected template.
	Selects a template for deletion or modification.
	Add Template Panel
	Adds a value pair row.
	Deletes a value pair row.
	Selects a value pair row.
Name	Enter the parameter name.
Value	Enter the value associated with the parameter name.
Cancel	Cancels any changes you made in the dialog.
Save	Adds the DSN and its name-value pairs or saves modifications to the name-value pairs.
Close	Closes the dialog without adding the DSN and its name-value pairs or saving modifications to the name-value pairs.

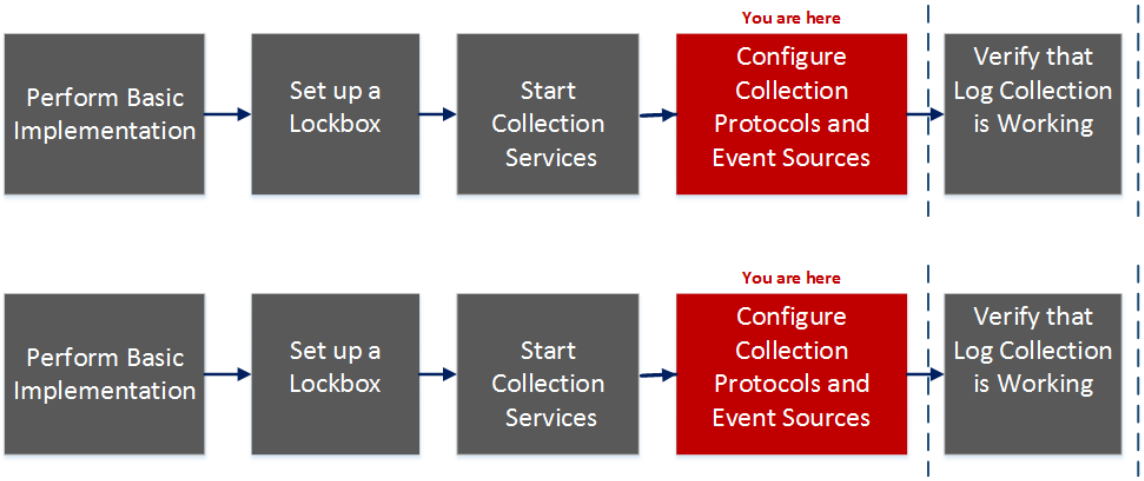
Remote/Local Collectors Configuration Parameters

When you deploy Log Collection, you must configure the Log Collectors to collect the log events from various event sources, and to deliver these events reliably and securely to the Log Decoder host, where the events are parsed and stored for subsequent analysis.

This topic introduces features of the Services Config view > Remote Collectors/Local Collectors tab.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources

Role	I want to...	Documentation
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

- Provision Local Collectors and Remote Collectors
- Configure Local and Remote Collectors

Services Config View

The Services Config view is the view on which you maintain all the Log Collection parameters. The tab in which you maintain the deployment parameters referred to in this guide is the **Remote/Local** Collectors tab:

- If you are configuring a Local Collector , NetWitness Suite displays the **Remote Collectors** tab so that you can configure the Local Collector to pull events from Remote Collectors.
- If you are configuring a Remote Collector , NetWitness Suite displays the **Local Collectors** tab so that you can configure the Remote Collector to push events to a Local Collector .

Remote Collectors Tab

On a Local Collector, the Remote Collectors panel provides a way to add or delete Remote Collectors from which the Local Collector pulls events.

Column	Description
	Displays the **Add Source** dialog in which you select the Remote Collectors from which you want the Local Collector to pull events.
	Deletes the Remote Collector from the Local Collector Remote Collectors panel.
	Displays the **Edit Source** dialog for the selected Remote Collector .
	Selects Remote Collectors.

Column	Description
Name	Names of the Remote Collectors from which the Local Collector currently pulls events.
Address	IP Addresses of the Remote Collectors from which the Local Collector currently pulls events.
Collections	Choose which collection protocols that the Remote Collector pushes to a Local Collector. You can select any combination of protocols. If you do not select a protocol, NetWitness Suite selects all protocols.

Local Collector Tab

On a Remote Collector , the Local Collector panel provides a way to add or delete the Local Collectors to which you want to the Remote Collector to push events.

Select the **Destination** or **Source** in the **Select Configuration** drop-down menu.

- **Destination** displays the **Add Remote Destination** dialog.
- Source displays the **Add Source** dialog.

The following table describes the Add Source dialog.

Column	Description
	Displays the **Add Source** dialog in which you select the Remote Collectors from which you want the Local Collector to pull events.
	Deletes the Remote Collector from theLocal Collector Remote Collectors panel.
	Displays the **Edit Source** dialog for the selected Remote Collector .
	Selects Remote Collectors.
Name	Names of the Remote Collectors from which the Local Collector currently pulls events.
Address	IP Addresses of the Remote Collectors from which the Local Collector currently pulls events.

The following table describes the Local Collectors Panel.

Column	Description
	Displays the **Add Remote Destination** dialog for the Group that you selected. You add destination Local Collectors for this group to which you want the Remote Collector to push events.
	Deletes the destination Log Collector from the group.
	Displays the **Edit Remote Destination** dialog for the selected destination Local Collector .
	Selects a destination Local Collector .
Destination Name	Displays the name of the destination Local Collector .
Address	Displays the IP address of the destination Local Collector .
Collections	Choose which collection protocols that the Local Collector pulls from a Remote Collector. You can select any combination of protocols. If you do not select a protocol, NetWitness Suite selects all protocols.

Log Collection Tabs

This topic describes the tabs available in the Log Collection view.

Access Log Collection View

1. Go to **ADMIN > Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Under Actions, select **View > Config** to display the Log Collection configuration parameter tabs.

   The **Service Config** view is displayed with the Log Collector **General** tab open.
4. Select any of the available tabs to view or update the corresponding parameters.

Available Tabs

Use the Admin > Services view to maintain Log Collection parameters. It has the following tabs:

- **General**: contains high-level parameters that govern the operation of the Log Collector service and each collection protocol. See Log Collection General Tab for details.
- **Remote Collectors**: use this tab to set up remote collectors. See Configure Local and Remote Collectors for details.
- **Files**: provides an interface for editing Log Collector configuration files.
- **Event Sources**: use this tab to configure collection for your event sources. See Log Collection Event Sources Tab for details.
- **Event Destinations**: Use the Event Destinations tab of the Log Collection service Config view to configure the destination of event data collected by the Log Collector. See Log Collection Event Destinations Tab for details.
- **Settings**: contains parameters for Lockbox security setup, and certificate management.
- **Appliance Service Configuration**: contains configuration parameters for the RSA NetWitness Suite Core Appliance service.

Please refer to the **Files** tab and the **Appliance Service Configuration** tab in the *Host and Services Configuration Guide* for information on the configuration parameters on these tabs.

Log Collection General Tab

This topic introduces features of the service Config view > General tab that relate specifically to Log Collector .

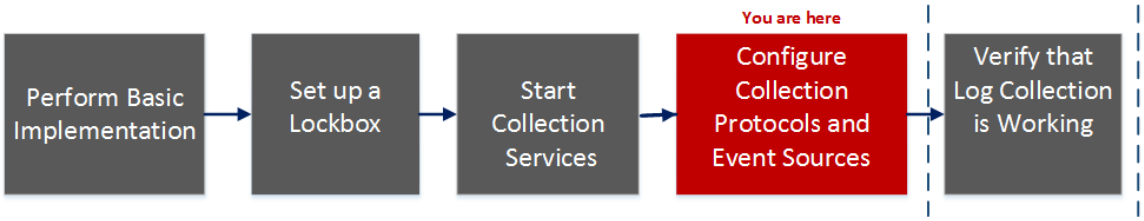
To access the Log Collection General tab:

1. Go to **ADMIN> Services** from the NetWitness Suite menu.
2. Select a Log Collection service.
3. Click under Actions and select **View > Config**.

   The **Service Config** view is displayed with the Log Collector **General** tab open.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	*Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

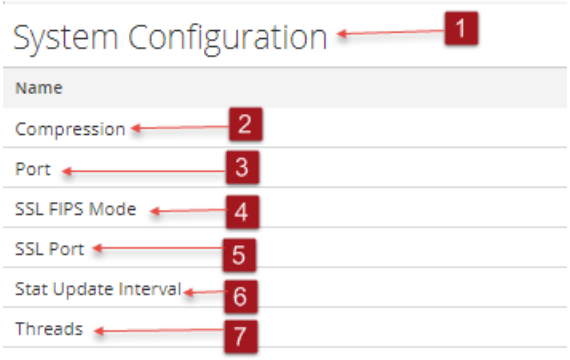
- Configure AWS (CloudTrail) Event Sources in NetWitness Suite
- Configure Check Point Event Sources in NetWitness Suite
- Configure File Event Sources in NetWitness Suite
- Configure Netflow Event Sources in NetWitness Suite
- Configure ODBC Event Sources in NetWitness Suite
- Configure SDEE Event Sources in NetWitness Suite
- Configure SNMP Event Sources in NetWitness Suite
- Configure Syslog Event Sources for Remote Collector
- Configure VMware Event Sources in NetWitness Suite
- Configure Windows Event Sources in NetWitness Suite
- Windows Legacy and NetApp Collection Configuration

Quick Look

The RSA NetWitness Suite administrator must configure event sources to send logs to the collectors. When event sources are configured they poll event sources, retrieve logs, and send the event data to NetWitness Suite).

System Configuration Panel

The System Configuration panel manages service configuration for a NetWitness Suite service. When a service is first added, default values are in effect. You can edit these values to tune performance. Refer to the **General** tab for a description of these parameters.

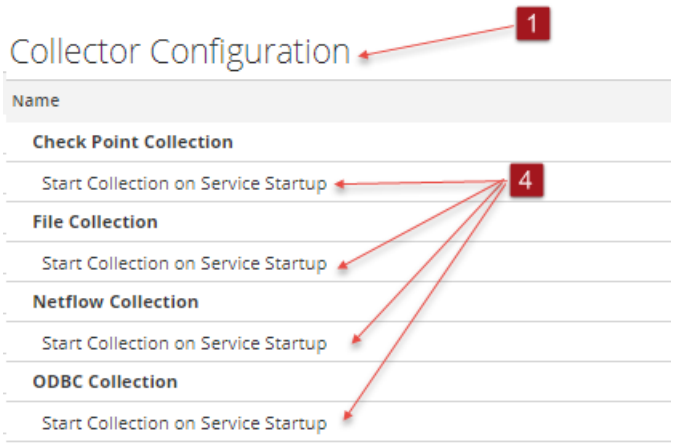


1	System Configuration Panel manages service configuration for a NetWitness Suite service.

2	Compression: The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.
3	Port: The port on which the service listens. The ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
4	SSL FIPS Mode: When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
5	SSL Port: The NetWitness Suite Core SSL port on which the service listens. The ports are: • 56001 for Log Collectors • 56002 for Log Decoders • 56003 for Brokers • 56004 for Decoders • 56005 for Concentrators • 56007 for other services
6	Stat Update Interval: The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
7	Threads: The number of threads in the thread pool to handle incoming requests. A setting of 0 lets the system decide. The default value is 15. A change takes effect on service restart.

Collector Configuration Panel

The Collector Configuration panel provides a way to enable automatic start of log collection by event source type.



1	Collector Configuration Panel provides a way to enable automatic start of log collection by event source type.
2	Enable All enables the automatic collection for all event types. **Enable All** = start receiving events and collecting logs for all event types when the Log Collector service starts.
3	Disable all disables the automatic collection for all event types. **Disable All** = (default) do not receive event data for all event types until you explicitly start collection.
4	Start Collection on Service Startup enables automatic start, per event source type, of log collection when the Log Collector service starts. Valid values are: • Selected = start collecting logs when the Log Collector service starts. • Not selected = (default) do not collect event data until you explicitly start collection.
5	**Apply**: Click **Apply** to save the changes to the parameter values.

Log Collection Event Destinations Tab

Use the Event Destinations tab of the Log Collection service Config view to configure the destination of event data collected by the Log Collector :

- Log Decoders
- Identity Feed

Prerequisites

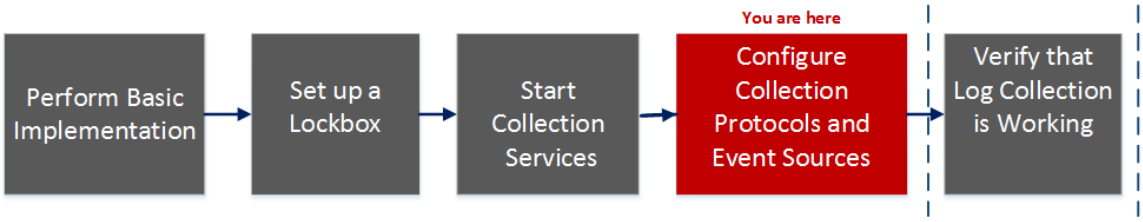
You must implement the following configuration to create an identity feed.

- A Log Collector service with an Identity Feed Event Processor
- A Log Collector service with Windows Collection configured and enabled

Note: See the "Create an Identity Feed" topic in the *Live Resource Management Guide* for more information on how to create and investigate on an identity feed.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources

Role	I want to...	Documentation
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

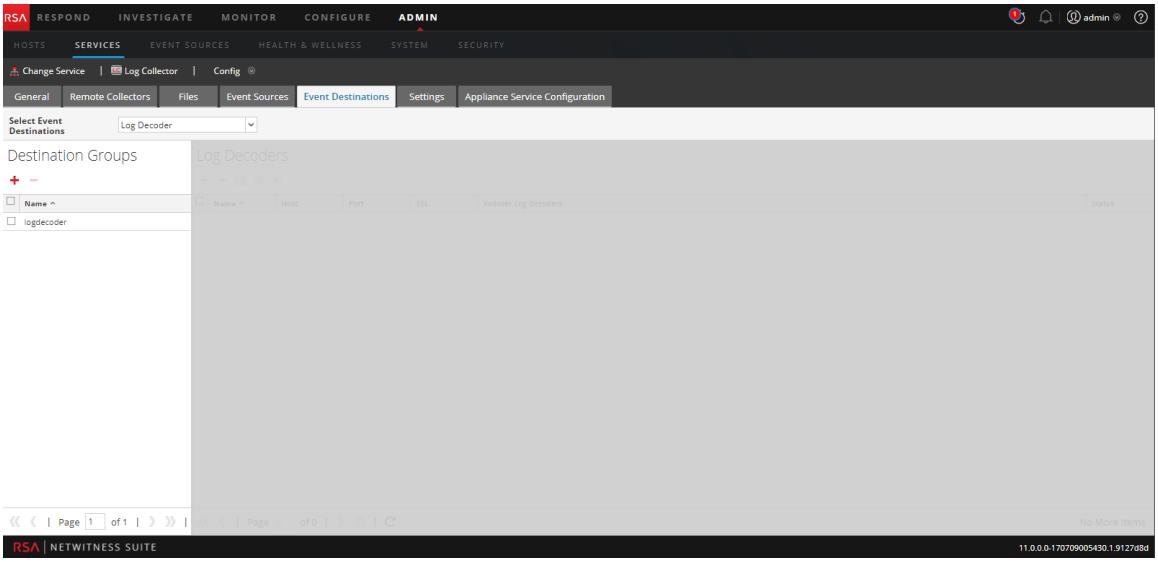
*You can perform this task here.

Related Topics

- See the **Create an Identity Feed** topic in the *Live Resource Management Guide*.

Quick Look

The Event Destinations tab of the Log Collection service Config view allows you to configure the destination of event data collected by the Log Collector .

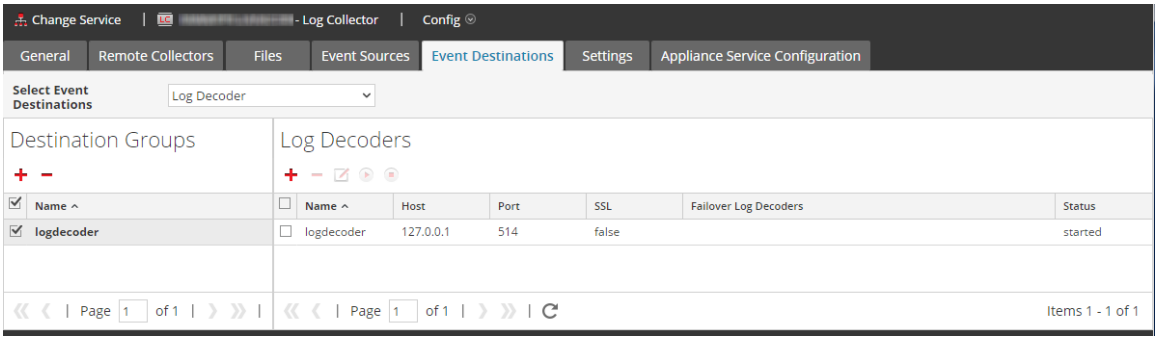


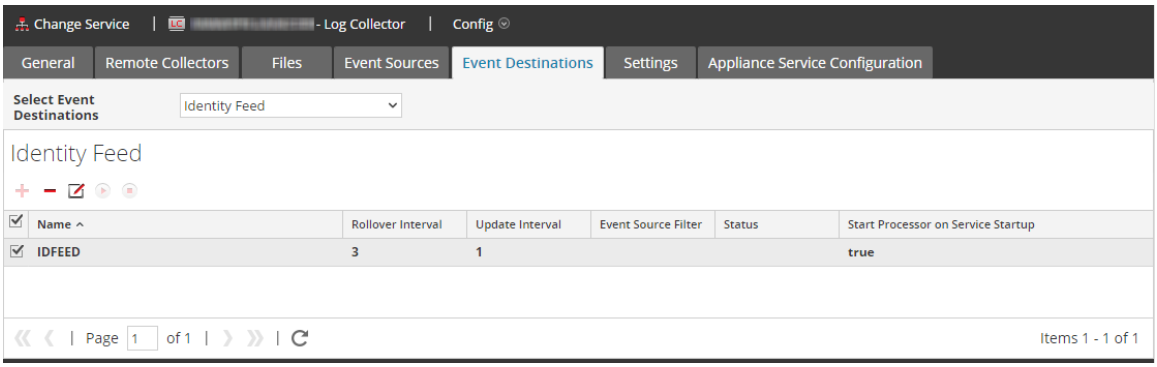
The required permission to access this view is Manage Services.

1. Go to **ADMIN> Services** .
2. Select a Log Collection service.
3. Under Actions, select **> View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Destinations** tab.
5. In the **Select Event Destinations** drop-down menu:
   - Select **Log Decoder** to configure Log Decoder destinations for event data collected by the Log Collector .

Note: You must select a Log Decoder service from the Add Log Decoder Destination dialog, but the remainder of the configuration is done automatically.

- Select **Identity Feed** to configure an identity feed destination for event data collected by the Log CollectorLog Collector .





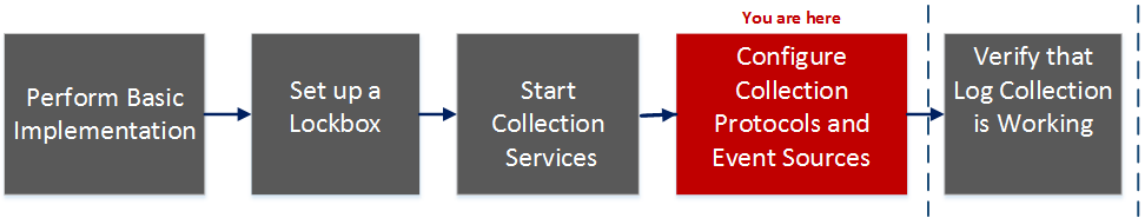
Log Collection Event Sources Tab

Use the Event Sources tab to configure the AWS (CloudTrail), Check Point, File, ODBC, SDEE, SNMP, Syslog, SNMP, VMware, Windows, and Windows Legacy event sources.

To access the Event Sources tab, go to ADMIN > Services > select Log Collection service > View > Config > Event Sources) .

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	*Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

*You can perform this task here.

Related Topics

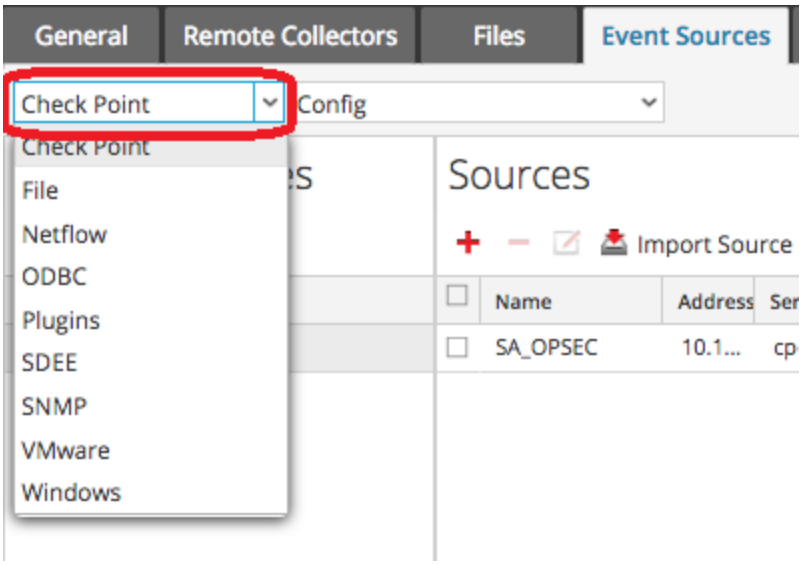
- Configure AWS (CloudTrail) Event Sources in NetWitness Suite
- Configure Check Point Event Sources in NetWitness Suite

- Configure File Event Sources in NetWitness Suite
- Configure ODBC Event Sources in NetWitness Suite
- Configure SDEE Event Sources in NetWitness Suite
- Configure SNMP Event Sources in NetWitness Suite
- Configure Syslog Event Sources for Remote Collector
- Configure VMware Event Sources in NetWitness Suite
- Configure Windows Event Sources in NetWitness Suite
- Windows Legacy and NetApp Collection Configuration

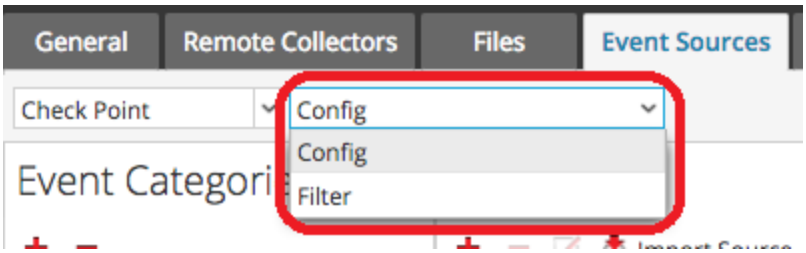
Quick Look

The Config view has two drop-down menus:

- The left-most menu lists all of the available collection protocols.



- The right-most menu has two choices: **Config** and **Filter**.



The Config view in the Event sources tab has two panels: Event Categories and Sources.

Note: For details on the Filter menu item, see Configure Event Filters for a Collector.

Event Source Types Menu

The Log Collector Event Sources tab has a two-box, drop-down menu in which you select the collection protocol and any supporting parameters for that protocol.

In the left box, you select one of the following protocols: Check Point, File, ODBC, Plugins, SDEE, SNMP, SNMP, VMware, Windows, and Windows Legacy.

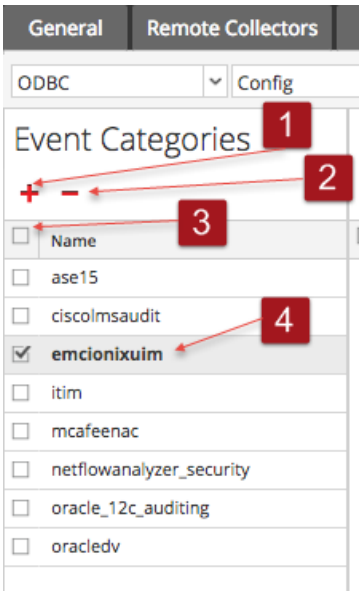
In the right box, you select:

- Config to configure the generic event source parameters for the type you selected in the left drop-down. All generic Config panels have a toolbar with these options:
  - Add, Edit, and Delete
  - Import (also Import Source, Import DSN)
  - Export (also Export Source, Export DSN)
- For ODBC, SNMP, and Windows only:
  - For ODBC, DSNs to configure
  - For SNMP, SNMP v3 User Manager
  - For Windows, Kerberos Realm Configuration

Selecting an option displays a configuration panel where you configure the collection parameters for the event source. The configuration panels are slightly different for different event sources and are described separately.

Event Categories Panel

Once you select a collection protocol, the Event Categories panel is populated with all of the event sources that you have configured for that collection protocol. For example, the following image shows ODBC event sources that have been configured:



The Event Categories panel provides a way to add or delete event source types.

1	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
2	Deletes the selected event source types from the Event Categories panel.
3	Selects event source types.
4	Displays the name of the event source types that you have added.

Sources Panel

The Sources panel lists the values of the parameters for the selected event source type. For details, see the individual collection protocol topics.

Log Collection SettingsTab

Use the Settings tab to:

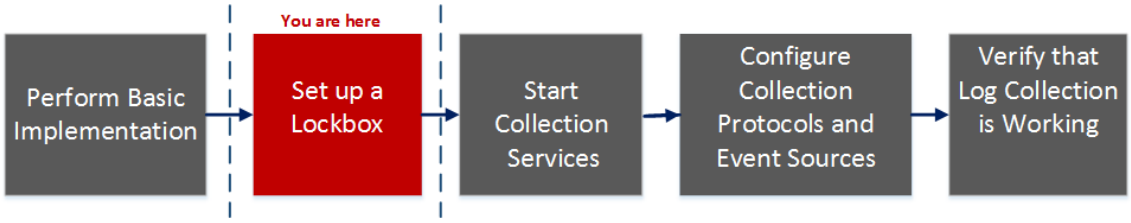
- Set up a lockbox
- Reset Stable System value
- Manage certificates

Caution: If the host name on which the Log Collector is installed is changed after installation, the Log Collector will fail to collect events from event sources. You must reset stable system values if the hostname changes.

To access the Log Collection Settings Tab, go to ADMIN > Services. In the Services grid, select a Log Collector Service. Click Actions menu cropped under Actions and select View > Config.

Workflow

This workflow illustrates the basic tasks needed to start collecting events through Log Collection.



What do you want to do?

Role	I want to...	Documentation
Administrator	Perform basic Log Collection implementation.	Basic Implementation
Administrator	*Set up a lockbox to maintain lockbox settings.	Set Up a Lockbox
Administrator	Start Log Collection services.	Start Collection Services
Administrator	Configure Log Collection protocols and event sources.	Configure Collection Protocols and Event Sources

Role	I want to...	Documentation
Administrator	Verify that Log Collection is working.	Verify That Log Collection Is Working

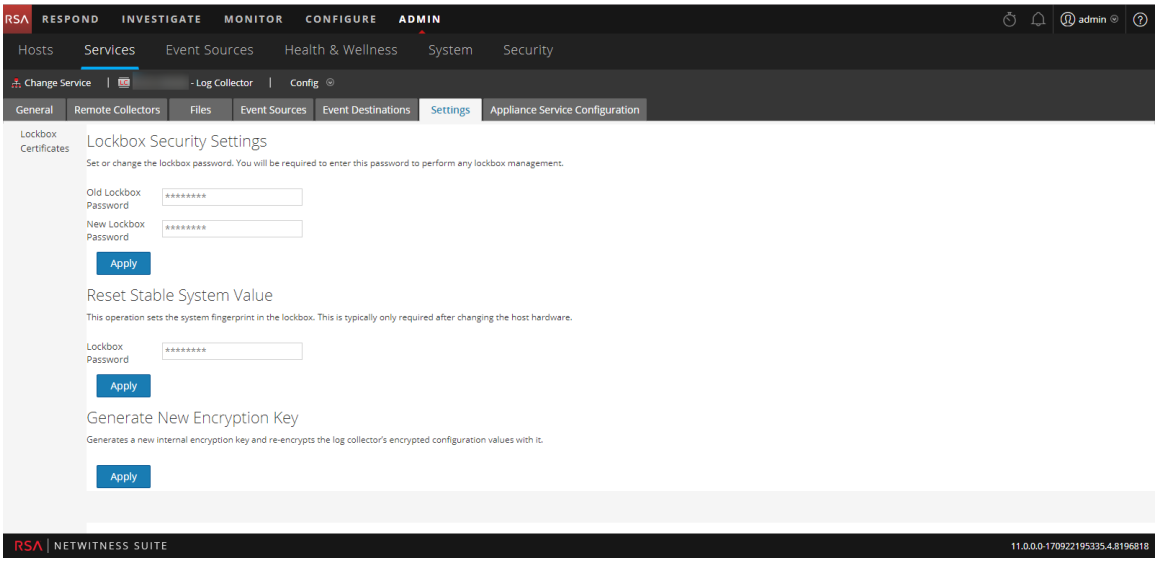
*You can perform this task here.

Related Topics

- See the "Create an Identity Feed topic" in the *Live Resource Management Guide*.

Quick Look

This is an example of the Settings tab.



Troubleshoot Log Collection

This topic describes the format and content of Log Collection Troubleshooting. NetWitness Suite informs you of Log Collector problems or potential problems in the following two ways.

- Log files.
- Health and Wellness Monitoring views.

Log Files

If you have an issue with a particular event source collection protocol, you can review debug logs to investigate this issue. Each event source has a Debug parameter that you can enable (set parameter to On or Verbose) to capture these logs.

Caution: Only enable debugging if you have a problem with this event source and you need to investigate this problem. If you have Debug enabled all the time it will adversely affect the performance of the Log Collector.

Health and Wellness Monitoring

Health and Wellness monitoring makes you aware of potential hardware and software problems in a timely manner so that you can avoid to outages. RSA recommends that you monitor the Log Collector statistical fields to make sure that the service is operating efficiently and is not at or near the maximum values you have configured. You can monitor the following statistics (Stats) described in the **Admin > Health & Wellness** view.

Sample Troubleshooting Format

RSA NetWitness Suite returns the following types of error messages in the log files for.

Log Messages	timestamp failure (LogCollection) Message-Broker Statistics:... timestamp failure (AMQPClientBaseLogCollection):... timestamp failure (MessageBrokerLogReceiver):...
Possible Cause	The Log Collector cannot reach the Message Broker because the Message Broker: • stopped running. • has erroneous connection settings.

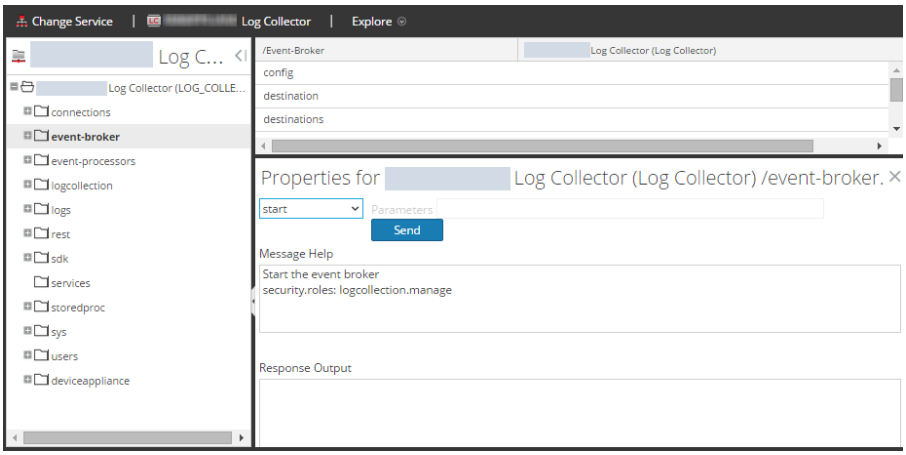
Solutions

1. <use the="the" systemctl="systemctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>

   prompt$ systemctl status rabbitmq-server

   rabbitmq start/running, process 10916

2. Start the RabbitMQ Message Broker on event-broker node in the Explore view:



Troubleshooting - Windows log Collection using Endpoint Agent

The following topics helps troubleshoot issues you can come across while using windows log collection file on Endpoint Insights Agent.

Windows Log Configuration File Format Explained

The log configuration file comprises of information helpful for analyzing event logs. The generated config file comprises of the following:

Note: The contents of the generated configuration file should not be tampered. If any changes are made, the agent does not read the information from the file.

```
#### Warning: Do not modify this system generated file.
{
  "enabled" : true,
  "configName" : "FE",
  "servers" : [ "tcp://[redacted]" ],
  "filter" : "<QueryList><Query Id='0'> <Select
  Path='ForwardedEvents'>*</Select> </Query></QueryList>",
  "testLogOnLoad" : true
}

q5yrOSY6qkdediE9XUI361926LOF2ZyU7JU2sklntgMWeV3KWFekwqJqhZ8XmPr6vbeOTK6wiYb
uW6zDL0WB/PPo+x5bErzvjoALA7zwAu61HVk4R4sYP4MRgGCsuiikC2pMB667P5bFg0+sUESsxZ
eFN91cjFPUjIIujuUdd0uMhnyur4tt+4F/WGJsBl57pTow2D8NRHvb9hKBjE1lo7/nZ0WpSO0Fq
yHx90NuS42d0OhjrC3oDyucwdAjqKkxm7VtsAJQwwxZTlwUbmDRPoiIyTG7egERVDDyqGcu2Ii+
fkijkFhuxTta8kWIeleQiBts1BAk+JZNfDSNYdYqUg==
```

Config name: Name of the configuration file.

Servers: Array of server URLs, describing both their address and protocol to use when forwarding the logs. The agent will attempt to contact them in order.

Filter: Windows Event viewer compatible XML which describes the channels to watch and any event ID exclusion. A standard XML filter to collect from channel Application and System, with one event ID excluded from both would look like this.

```
<QueryList>
    <Query Id="0" Path="Application">
        <Select Path="Application">*</Select>
        <Select Path="System">*</Select>
        <Suppress Path="Application">*[System[(EventID=3366)]]</Suppress>
        <Suppress Path="System">*[System[(EventID=3366)]]</Suppress>
    </Query>
</QueryList>
```

Enabled: Allows to disable collection but still send a test log if that is enabled.

TestLogOnLoad: Will send a log message when a configuration is loaded, even if event forwarding is not enabled. This helps Analysts test a configuration before enabling collection. This message is not logged locally in the Windows Event log.

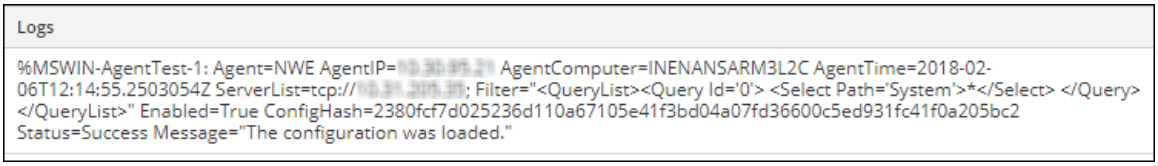
Test Log - How to Read

Test log message is sent whenever an Endpoint Agent with windows log collection file is installed for the first time on an Endpoint Agent or when the log configuration file is updated. On a successful install or updation of windows log collection - There are 3 sections displayed in the test log file.

1	Test log message type, Agent's IP address, Agent's Hostname and time of generation of the test log
2	Configuration provided during the creation of the agent
3	Status and the message associated with it

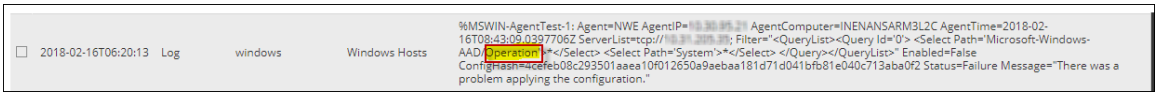
There are three scenarios.

1. Successful deployment of a log collection configuration - Test Log message type will be -1 and status will be displayed as success.



2. Whenever the log collection configuration file is tampered with - The Agent Test message will be displayed as -2 and a message displaying the configuration file has been tampered with is displayed. In case, you want to reapply the changes, regenerate the log collection file.

3. When the custom channel name is wrong - Status Failure message is displayed. Regenerate the log collection with the correct channel.



RSA NETWITNESS® SUITE

Malware Analysis Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

How Malware Analysis Works **1**

Functional Description 1

Analysis Method 3

NetWitness Server Access to the Malware Analysis Service 3

Scoring Method 4

Deployment 4

Scoring Modules **5**

Network 5

Static Analysis 6

Community 6

Sandbox 6

Roles and Permissions for Analysts **7**

Required Roles and Permissions 7

Malware Analysis Configuration **9**

Basic Configuration Checklist 9

Configure Malware Analysis Operating Environment 11

Network Connections 12

Add Malware Analysis Host and Service 13

Prerequisite 13

Procedure 13

Configure General Malware Analysis Settings 18

View the Basic Settings 19

Configure Continuous Polling 19

Configure Manual File Upload Settings 22

Configure the Data Repository 23

Calibrate Scoring Modules 23

Configure Static Analysis Scoring 24

Configure Community Analysis Scoring 25

Configure Sandbox Analysis Scoring 26

Configure Indicators of Compromise 28

Filter Displayed IOCs by Module 29
Filter Displayed Modules to Show Only Modified Modules 30
Enable and Disable IOCs for a Scoring Module 30
Adjust the Score Weight for an IOC 31
Set the High Confidence Flag for an IOC 32
Reset IOCs to Default Settings 33
Configure Installed Antivirus Vendors 33
Identify Installed AV Software 34
Enable Community Analysis 35
(Optional) Configure Auditing on Malware Analysis Host 37
Configure the Auditing Threshold 38
Configure Incident Management Alerting 38
Configure SNMP Auditing 39
Configure File Auditing Settings 39
Configure Syslog Auditing Settings 40
(Optional) Configure Hash Filter 41
View the Hash List 41
Add a File Hash to the Hash Filter 41
Mark a Hash as Trusted or Untrusted 42
Delete a Hash from the Hash Filter 42
Search for a File Hash 42
Import a Hash List Using the Watched Folder 42
(Optional) Configure Malware Analysis Proxy Settings 45
Configure the Web Proxy 46
(Optional) Register for a ThreatGrid API Key 47

Additional Procedures for Configuring Malware Analysis 49

Create Custom Alert in CEF Format 49
The CEF Template 49
Understand a Syslog Auditing File Entry 50
Edit the Configuration File 55
Example 55
Enable Custom YARA Content 69
Prerequisites 69
Install Libraries and Applications Required to Build YARA on a CentOs-Based Appliance 69
Set Up Yara 70

Malware Analysis References **72**
Services Config View - Auditing Tab 73
Packet Reconstruction Details 75
Text Reconstruction Details 75
File Reconstruction Details 76
Detailed Description 77
Services Config View - AV Tab 79
Services Config View - General Tab 80
Continuous Scan Configuration Section 80
Repository Configuration Section 84
Miscellaneous Configuration Section (10.3 SP2 and Later) 85
Modules Configuration Section 85
ThreatGrid Sandbox Settings 89
Services Config View - Hash Tab 90
Services Config View - Indicators of Compromise Tab 92
Services Config View - Integration Tab 94
Services Config View - IOC Summary Tab 96
Service Config View - Proxy Tab 98
Services Config View - ThreatGRID Tab 99

How Malware Analysis Works

NetWitness Suite Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows portable executable (PE), PDF, and MS Office) to assess the likelihood that a file is malicious.

Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- Network Session Analysis (network)
- Static File Analysis (static)
- Dynamic File Analysis (sandbox)
- Security Community Analysis (community)

Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

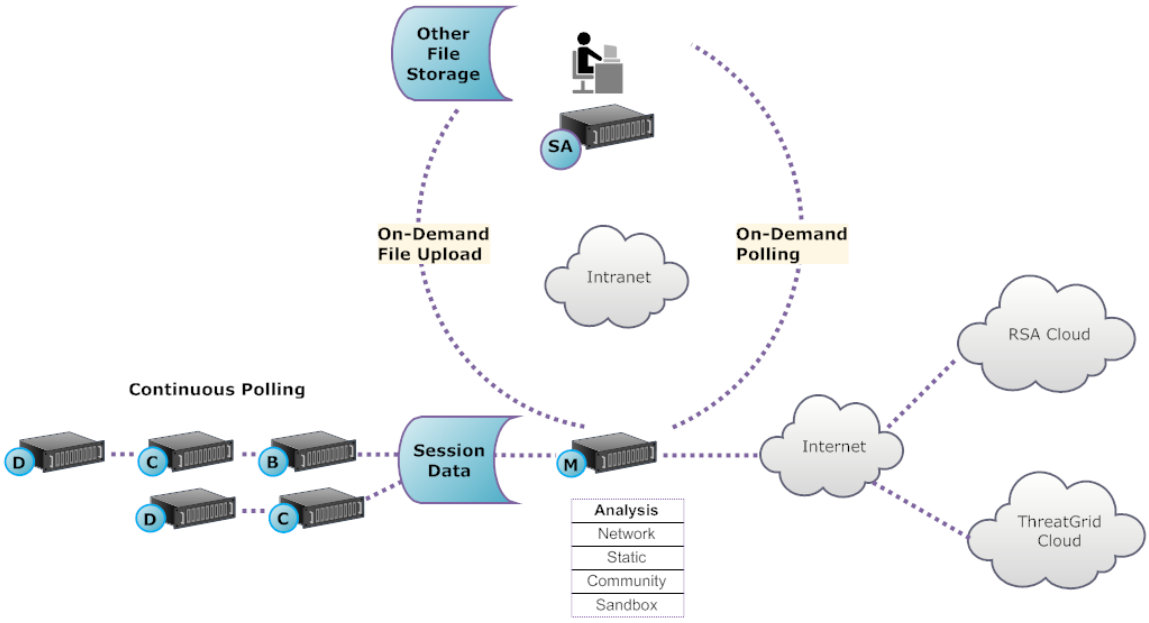
In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language, which allows malware researchers to identify and classify malware samples. This allows IOC authors to add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live. These YARA-based IOCs in RSA Live will automatically be downloaded and activated on the subscribed host, to supplement the existing analysis that is performed in each analyzed file.

Malware Analysis also has features that support alerts for Incident Management.

Functional Description

This figure depicts the functional relationship between the Core services (the Decoder, Concentrator, and Broker), the Malware Analysis service, and the NetWitness Server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



The Malware Analysis service analyzes file objects using any combination of the following methods:

- **Continuous automatic polling of a Concentrator or Broker** to extract sessions identified by a parser as potentially carrying malware content.
- **On-demand polling of a Concentrator or Broker** to extract sessions identified by a malware analyst as potentially carrying malware content.
- **On-demand upload of files** from a user-specified folder.

When automatic polling of a Concentrator or Broker is enabled, the Malware Analysis service continuously extracts and prioritizes executable content, PDF documents, and Microsoft Office documents on your network, directly from data captured and analyzed by your Core service. Because the Malware Analysis service connects to a Concentrator or Broker to extract only those executable files that are flagged as possible malware, the process is both rapid and efficient. This process is continuous and does not require monitoring.

When on-demand polling of a Concentrator or Broker is chosen, the malware analyst uses Investigation to drill into captured data and choose sessions to be analyzed. The Malware Analysis service uses this information to automatically poll the Concentrator or Broker and to download the specified sessions for analysis.

On-demand upload of files provides a method for the analyst to review files captured external to the Core infrastructure. The malware chooses a folder location and identify one or more files to be uploaded and analyzed by Malware Analysis. These files are analyzed using the same methodology as files automatically extracted from network sessions.

Analysis Method

For the Network analysis, the Malware Analysis service looks for characteristics that seem to deviate from the norm, much as an analyst does. By looking at hundreds to thousands of characteristics and combining the results into a weighted scoring system, legitimate sessions that coincidentally have a few abnormal traits are dismissed, while the actual bad ones are highlighted. A user can learn patterns that indicate anomalous activity in the sessions as indicators that warrant further investigation, Indicators of Compromise.

The Malware Analysis service can perform Static analysis against suspicious objects it finds on the network and determine whether those objects contain malicious code. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. For Sandbox analysis, the services can also push data into major security, information and event management (SIEM) hosts (the ThreatGrid Cloud).

Malware Analysis has a unique method for analysis that is partnered with industry leaders and experts, so their technologies can enrich the Malware Analysis scoring system.

NetWitness Server Access to the Malware Analysis Service

The NetWitness Server is configured to connect to the Malware Analysis service and import tagged data for deeper analysis in Investigation. Access is based on three subscription levels.

- Free subscription: All NetWitness Suite customers have a free subscription, with a free trial key for ThreatGrid analysis. The Malware Analysis service is rate-limited to 100 file samples per day. The number of samples (within the set of files from above) submitted to the ThreatGrid Cloud for sandbox analysis is limited to 5 per day. If one network session had 100 files in it, customers would hit the rate limit after processing the one network session. If 100 files were manually uploaded, that would cause the rate limit to be reached.
- Standard subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 1000 per day.
- Enterprise subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 5000 per day.

Scoring Method

By default, the Indicators of Compromise (IOC) are tuned to reflect industry best practices. During analysis, the IOCs that trigger cause the score to move upward or downward to indicate the likelihood that the sample is malicious. The tuning of IOCs is exposed in NetWitness Suite so that the malware analyst can choose to override the assigned score or to disable an IOC from being evaluated. The analyst has the flexibility to either use the default tuning, or to completely customize the tuning to specific needs.

YARA-based IOCs are interleaved with the built-in IOCs within each built-in category and are not distinguished from native IOCs. When viewing IOCs in the Service Configuration view, administrators can select YARA from the Module selection list to see a list of YARA rules.

After a session is imported into NetWitness Suite, all of the viewing and analysis capabilities in Investigation are available to further analyze Indicators of Compromise. When viewed in Investigation, YARA IOCs are distinguished from the built-in native IOCs by the tag `Yara rule`.

Deployment

The Malware Analysis service is deployed as a separate RSA Malware Analysis host. The dedicated Malware Analysis host has an onboard Broker which connects to the Core infrastructure (either another Broker or a Concentrator). Prior to this connection, a collection of parsers and feeds must be added to the Decoders that are connected to the Concentrators and Brokers from which the Malware Analysis service pulls data. This allows suspicious data files to be marked for extraction. These files are `malware analysis` tagged content available through the RSA Live content management system.

Scoring Modules

RSA NetWitness Suite Malware Analysis analyzes and scores sessions and the embedded files within these sessions by scoring four categories: Network, Static Analysis, Community, and Sandbox. Each category comprises many individual rules and checks that are used to calculate a score between 1-100. The higher the score, the more likely the session is to be malicious and worthy of more in-depth follow-on investigation.

Malware Analysis can facilitate a historical investigation into events leading up to a network alarm or incident. If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections. You can also modify behavior for each scoring category based on the scoring category or the file type (Windows PE, PDF, and Microsoft Office).

Once you become familiar with data navigation methods, you can explore the data more completely through:

- Searching for specific types of information
- Reviewing specific content in detail.

Category scores for Network, Static Analysis, Community, and Sandbox are maintained and reported independently. When events are viewed based on the independent scores, as long as one category detects malware, it is evident in the Analysis section.

Network

The first category examines each core network session to determine if the delivery of the malware candidates was suspicious. For example, benign software being downloaded from a well-known safe site, using proper ports and protocols, is considered less suspicious than downloading software known to be malicious from a known dubious download site. Sample factors used in the scoring of this criteria set may include sessions that:

- Contain threat feed information
- Connect to well-known bad sites
- Connect to high-risk domains/countries (for example, .cc domain)
- Use well-known protocols on non-standard ports
- Contain obfuscated JavaScript

Static Analysis

The second category analyzes each file in the session for signs of obfuscation in order to predict the likelihood of the file behaving maliciously if allowed to run. For example, software that links to networking libraries is more likely to perform suspicious network activity. Sample factors used in the scoring of this criteria set may include:

- Files found to be XOR encoded
- Files found embedded within non-EXE formats (for example, PE file found embedded in a GIF format)
- Files linking to higher risk import libraries
- Files highly deviating from the PE Format

Community

The third category scores the session and files based on the collective knowledge of the security community. For example, files whose fingerprint/hash is already known to be good or bad by respected anti-virus (AV) vendors is scored accordingly. Files are also scored based on knowledge that a file was delivered from a site known to be good or bad by the security community.

Community scoring also indicates whether the AV on your network flagged the files as malicious. It does not indicate that the resident AV product acted to protect your system.

Sandbox

The fourth category examines the behavior of the software by actually running it in a sandbox environment. By running the software to watch its behavior, a score can be calculated by identifying well-known malicious activity. For example, software that configures itself to autostart on each reboot and make IRC connections would score higher than a file with no known bad behavior.

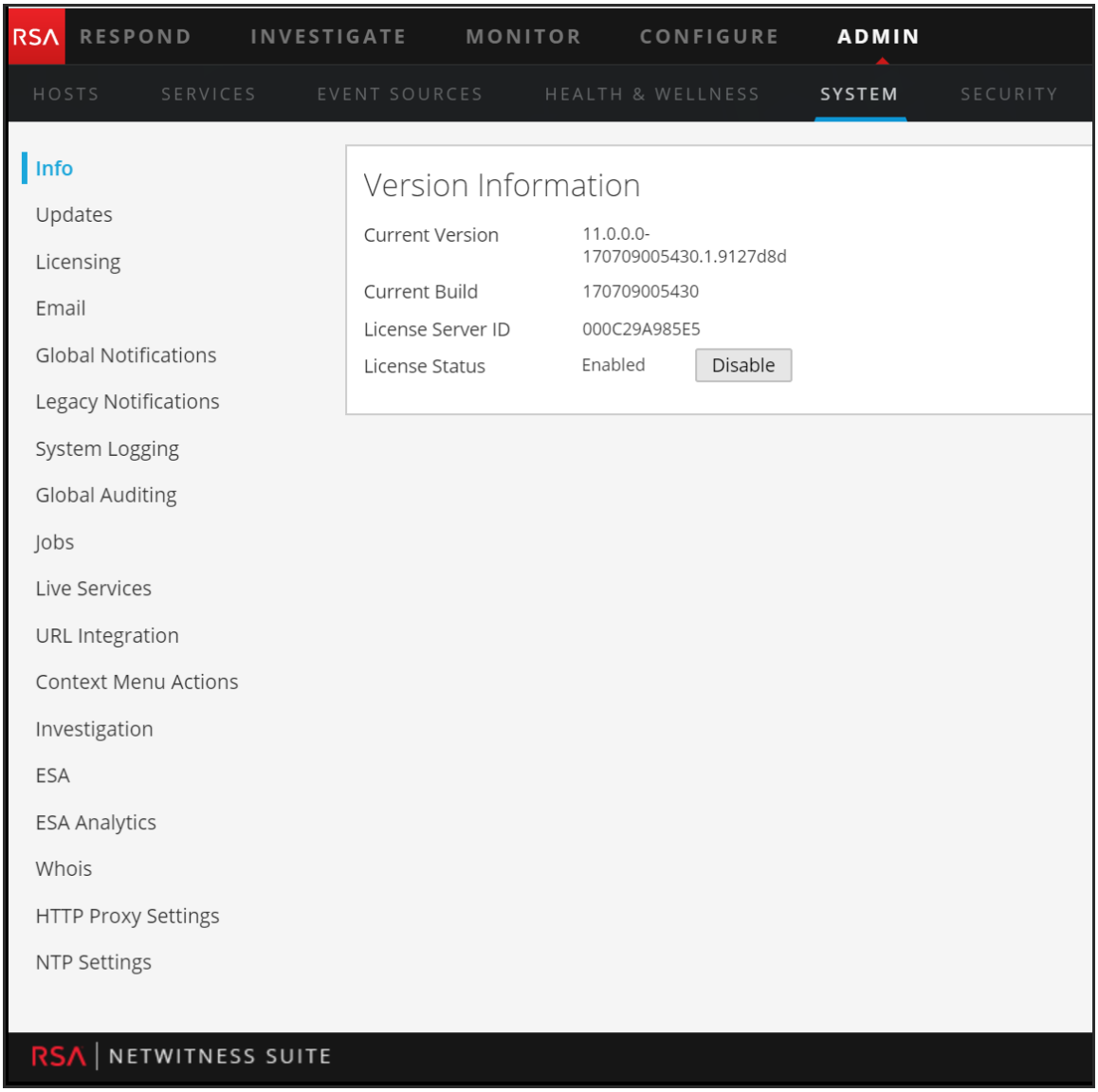
Roles and Permissions for Analysts

This topic identifies the user roles and permissions required for a user to conduct malware analysis in NetWitness Suite. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

Required Roles and Permissions

RSA NetWitness Suite manages security by providing access to views and functions using both system permissions and permissions on individual services.

On the system level, the user needs to be assigned a system role, in the Administration > System view, that provides access to specific views and functions.



The default `Malware_Analysts` role in NetWitness Suite 11.1 is assigned all of the permissions listed below. If necessary, an Administrator can create a custom role with some combination of the following permissions:

- Access Investigation Module (required)
- Investigation - Navigate Events
- Investigation - Navigate Values
- Access Incident Module
- View and Manage Incidents
- View Malware Events (to view events)
- File Download (to download files from the Malware Analysis service)
- Initiate Malware Scan (to initiate a one-time service scan or one-time file upload)
- Dashlet permissions for convenience: Dashlet - Investigate Top Values Dashlet, Dashlet - Investigate Service List Dashlet, Dashlet - Investigate Jobs Dashlet, Dashlet - Investage Shortcuts Dashlet.

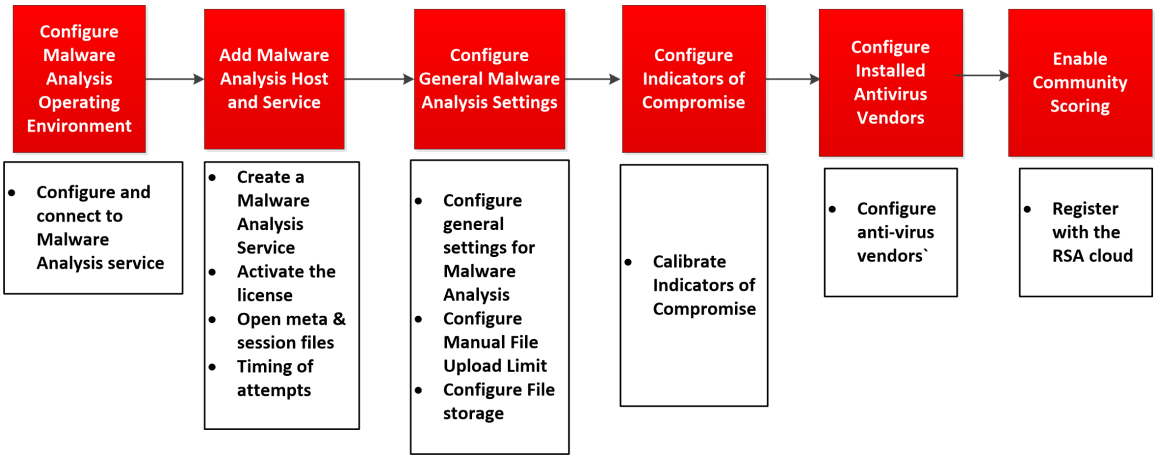
A use case for creating a custom role would be a Junior Malware Analyst role, with limited permissions that do not include the File Download permission.

On specific services, a malware analyst needs to be a member of the **Analysts** group, or to a group that has the two default permissions assigned to the Analyst group: **sdk.meta** and **sdk.content**. Users who have these permissions can use specific applications, run queries, and view content for purpose of analysis on the service.

Malware Analysis Configuration

Malware Analysis can operate as a service on a Decoder or as a service on a dedicated appliance. This guide includes instructions for setting up the operating environment and then configuring the Malware Analysis service. After this configuration is complete, analysts can conduct malware analysis.

These are the required configuration steps for Malware Analysis, and also for editing the configuration. Perform the steps in the section in the sequence they are given.



Basic Configuration Checklist

The following checklist provides the sequence for tasks that are required to configure Malware Analysis that has been added to NetWitness Suite in accordance with the *Hosts and Services Guide*.

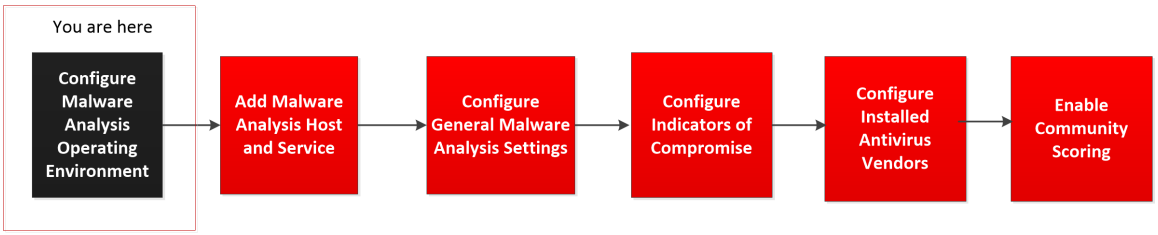
Step	High-Level Task
Step 1 - Configure Malware Analysis Operating Environment	Configure Malware Analysis Operating Environment This topic describes the procedures for configuring the environment to connect to the Malware Analysis service.

Step	High-Level Task
Step 2 - Add Malware Analysis Host and Service	Add Malware Analysis Host and Service **Note:** To complete this step you must have the NetWitness Suite License Server setup as described in the Licensing Guide. In NetWitness Suite, create a Malware Analysis service and activate the license. The default REST port is 60007. Sites that are using the free version of Malware Analysis must configure the service IP address as localhost or loopback.
Step 3 - Configure General Malware Analysis Settings	Configure General Malware Analysis Settings • Enable continuous polling. • Configure manual file upload limit. • Configure the file storage repository and database. • Calibrate the Static, Network, Community, and Sandbox scoring modules.
Step 4 - Configure Indicators of Compromise	Configure Indicators of Compromise Calibrate Indicators of Compromise that are applied for each scoring module (Static, Network, Community, Sandbox) and for YARA-based IOCs.
Step 5 - Configure Installed Antivirus Vendors	Configure Installed Antivirus Vendors
Step 6 - Enable Community Scoring	Enable Community Analysis Register with the RSA cloud and test connections to enable Community scoring.
Step 7 - Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host Configure auditing thresholds and enable Syslog, SNMP, and file auditing.

Step	High-Level Task
Step 8 - Configure Hash Filter	(Optional) Configure Hash Filter Configure hash filtering to fine tune Malware Analysis event analysis based on known good or bad file hashes.
Step 9 - Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings (Optional) Configure Malware Analysis to communicate with the RSA Cloud through a web proxy instead of directly.
Step 10 - Register for a ThreatGrid API key	(Optional) Register for a ThreatGrid API Key

Configure Malware Analysis Operating Environment

You can configure the NetWitness Suite operating environment to connect to a NetWitness Suite Malware Analysis service.



Malware Analysis operates as a service on a dedicated Malware Analysis appliance. If your site is using a dedicated appliance, do one of the following:

- If your site is adding a new dedicated NetWitness Suite Malware Analysis appliance, install the physical appliance in your network and configure the operating environment.
- If your site is upgrading a dedicated Spectrum appliance to a dedicated NetWitness Suite Malware Analysis appliance, re-image the Spectrum appliance as a Malware Analysis appliance.

Malware Analysis is dependent on the Core infrastructure to operate. The following steps are necessary before Malware Analysis can successfully analyze data.

1. Configure the onboard Broker on the Malware Analysis appliance to connect another Broker or Concentrator in the existing Core infrastructure.

Note: If no Core infrastructure exists, only manually uploaded files can be analyzed.

2. Use NetWitness Suite Live to find all Live resources with the `malware analysis` tag and deploy these resources to each Decoder service that will be capturing traffic for Malware Analysis to analyze. NetWitness Suite uses this proprietary set of parsers and feeds to find events that are likely to be malware.
3. Configure communications ports. Malware Analysis requires a number of different communications ports to be open, including TCP/443 for HTTPS. These are described below in Network Connections.
4. Configure the NextGen source to which Malware Analysis will connect. This is the Broker or the Concentrator.
   Malware Analysis is now ready to begin analyzing network traffic.

Network Connections

The inbound and outbound network connections must be configured for the Malware Analysis appliance to properly communicate with services, RSA sources for software updates, and other critical information.

Your network firewall must be configured to allow the Malware Analysis access to the internet. Proxy servers may be used to facilitate these connections, if necessary.

Inbound Connections

TCP/22 - Secure Shell access to the Malware Analysis server to review log files and troubleshoot. Access can be limited to IP addresses that will be managing Malware Analysis.

- TCP/443 - HTTPS web-based connection to access the Malware Analysis user interface.
- TCP/50008 - JMX port for performance troubleshooting, using an application such as JVisualVM. This is optional and access can be limited to IP addresses that will be managing Malware Analysis.

Outbound Connections

- TCP/443 - HTTPS connections to SSL-based web servers. Some features include Malware Analysis sending files or documents to servers for analysis, which require a secure connection. Use of a web proxy server is supported.
- (TCP/443 - SSL connection from Malware Analysis to the RSA Cloud. Use of a SOCKS proxy server is supported. Customer infrastructure changes may be required to ensure that 443 is open to cloud.netwitness.com.)

- TCP/50103 - REST API port used to communicate with a Broker. (NetWitness Suite 10.3.x and earlier)
- TCP/50105 - REST API port used to communicate with a Concentrator. (NetWitness Suite 10.3.x and earlier)
- TCP/50003 TCP/56003 - Ports used to communicate with a Broker. (NetWitness Suite 10.4 and later)
- TCP/50005 TCP/56005 - Ports used to communicate with a Concentrator. (NetWitness Suite 10.4 and later)
- ICMP - JMS connection from NetWitness Suite to the Malware Analysis service to verify if the hostname and ip address entered is valid for a successful test connection.

Add Malware Analysis Host and Service

You can add a Malware Analysis host and service to NetWitness Suite. Your NetWitness Suite environment determines how you add a host. Refer to the basic instructions for adding a host (Add or Update a Host) in the Host and Services Getting Started Guide. Use the procedure in this section only if you need to add a Malware Analysis host manually.

Note: To complete this step you must have the NetWitness Suite License Server setup as described in the Licensing Guide.

- Add Malware Analysis host if there is a physical or virtual Malware Analysis appliance.

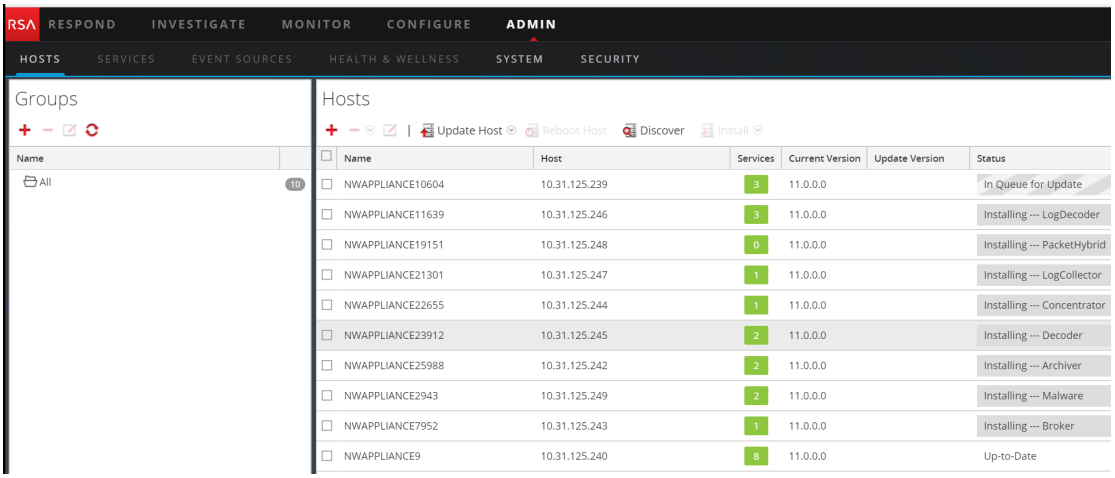
Prerequisite

To add a host and service in NetWitness Suite, the operations setup must be complete and an instance of NetWitness Suite must be installed and running.

Procedure

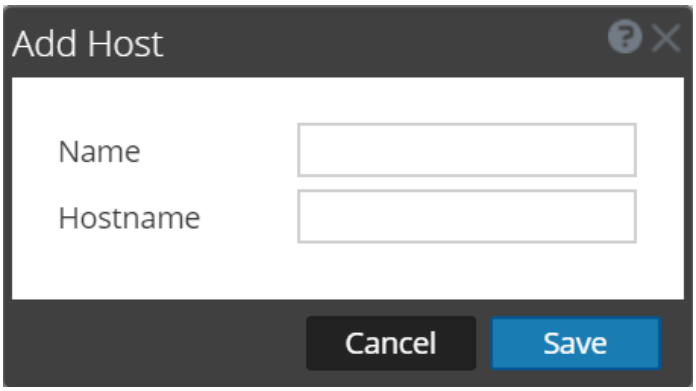
To manually add a Malware Analysis host to NetWitness Suite:

1. Log in to NetWitness Suite.
2. In the main menu, select **Administration > Hosts**. The Administration > Hosts view is displayed.

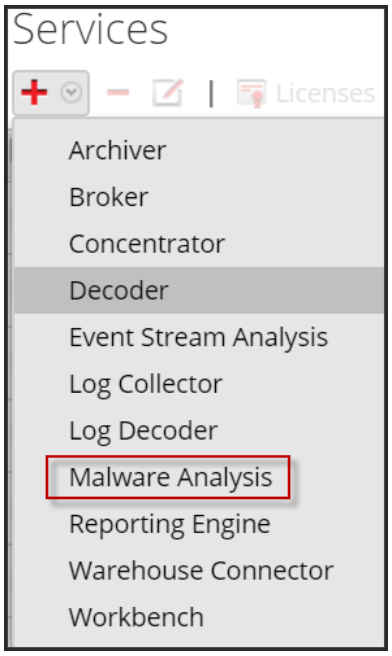


3. In the Hosts panel toolbar, click .

   The Add Host dialog is displayed.



4. In the **Name** field, enter a name for the Malware Analysis host. In the **Hostname** field, enter the host name, the virtual IP address, or IP address on the Malware Analysis. Click **Save.**
5. In the toolbar, select **Services**.
6. In the **Services** panel toolbar, click and select **Malware Analysis** in the resulting drop-down list of available services.



The Add Service dialog is displayed with the service type Malware Analysis

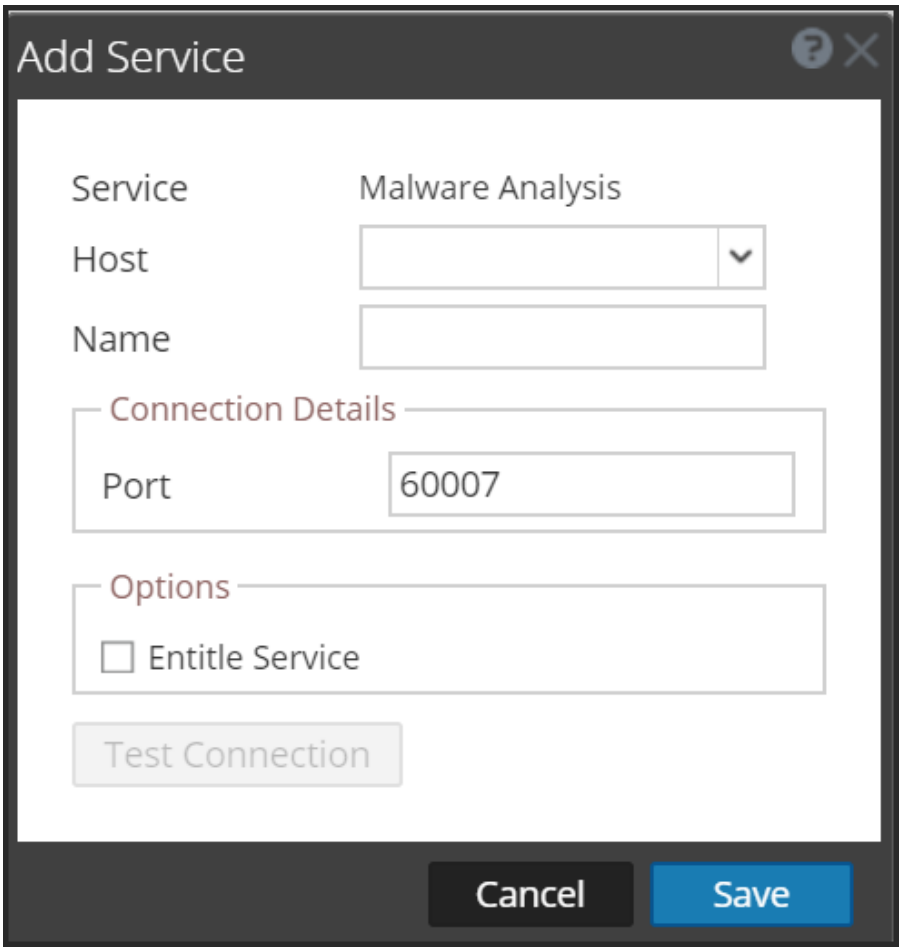
7. Enter the following information:

   In the **Name** field, enter a name for the Malware Analysis service.

   In the **Host** field, enter the host name, the virtual IP address, or IP address on the Malware Analysis.

   In the **Port** field, enter **60007**.

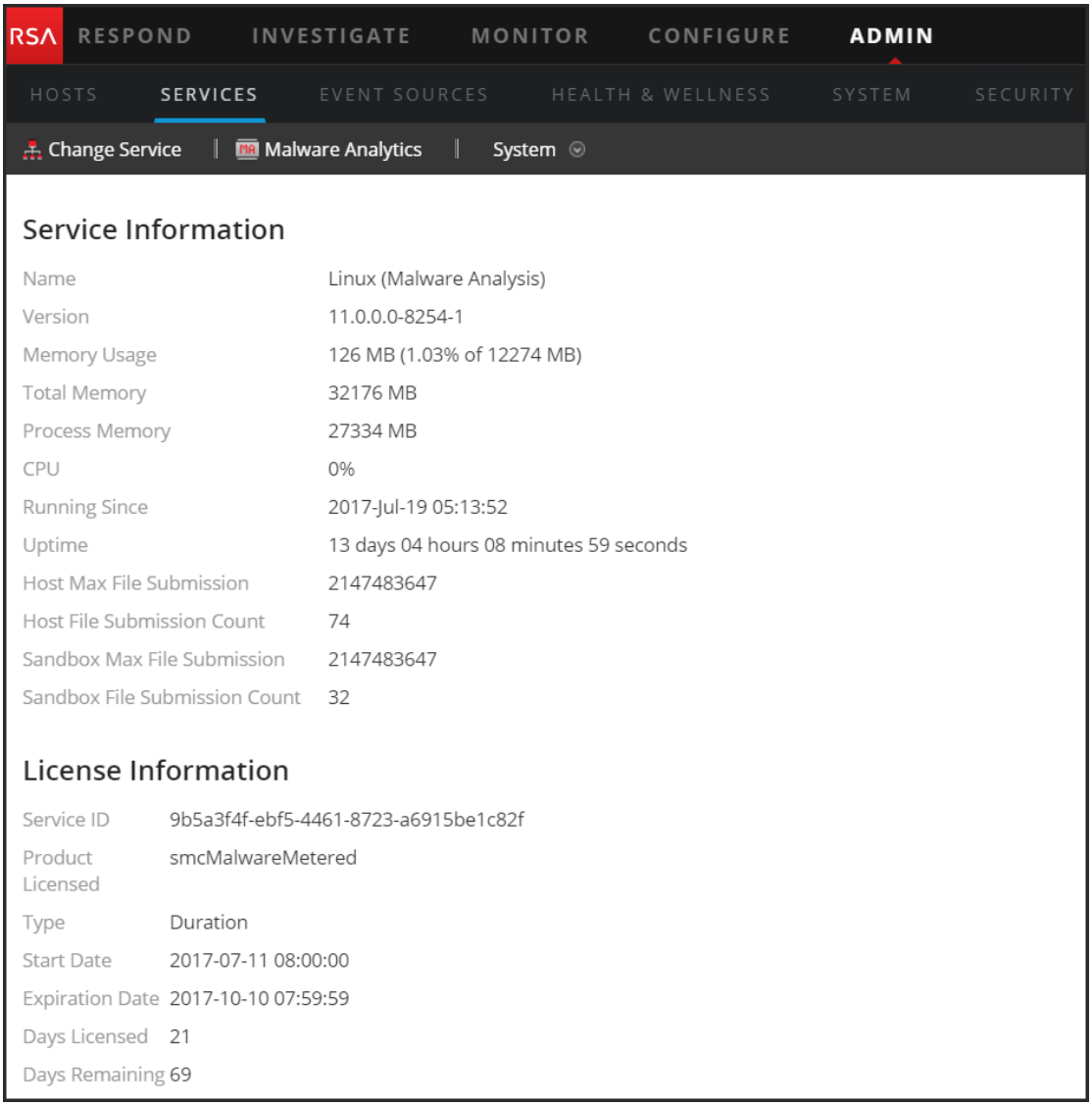
   (Optional) Under **Options**, select **Entitle Service**.



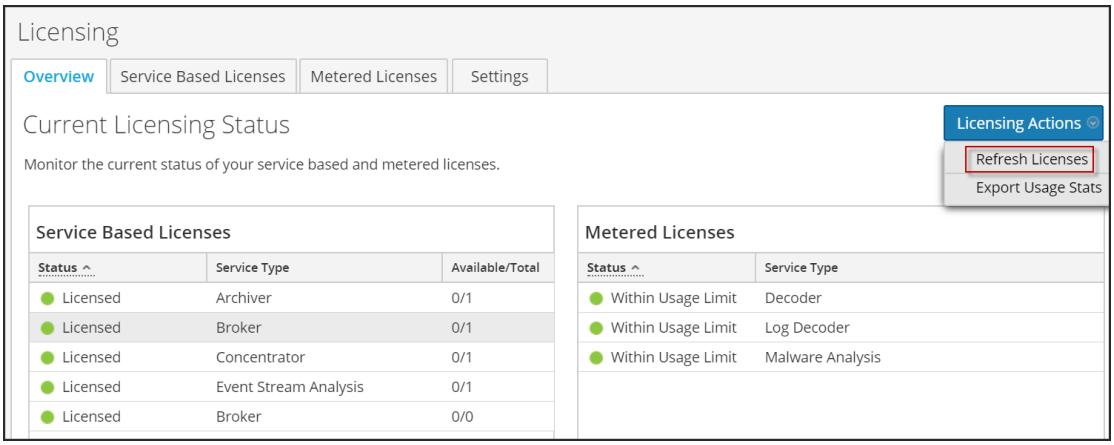
8. Click **Test Connection**.

   While adding the service, NetWitness Suite sends ICMP packets to the service to verify if the hostname and ip address entered is valid for a successful test connection. The result of the test is displayed in the Add Service dialog. If the test is unsuccessful, edit the service information and retry.

9. When the result is successful, click **save**. The Add Service dialog closes and the Malware Analysis service is available to NetWitness Suite.(Optional) Verify the status of the Malware Analysis service. In the Administration Services view, select the Malware Analysis service and select **View > System**. Below is a sample of the information available for a Malware Analysis service.

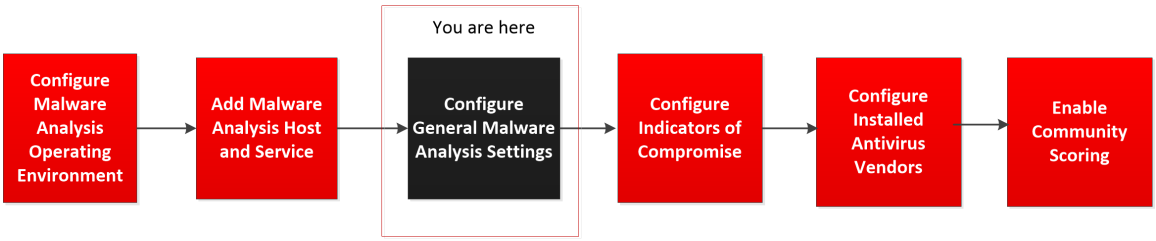


If the service is not licensed, navigate to the Administration > System > Licensing panel, and select **Refresh Licenses** in the **Licensing Actions** menu.



Configure General Malware Analysis Settings

You can configure several basic settings required to enable and calibrate the consumption of sessions, manual file upload, and the different scoring modules that Malware Analysis uses to analyze data.



You can also set up file sharing with the data repository. Malware Analysis has three modes of consuming sessions and files. Any combination of the three choices may be used to initiate analysis in Malware Analysis. The choices are:

- **Continuous Polling of the Core service:** You can enable and configure continuous polling of the Core service. When enabled and configured, Malware Analysis continuously polls the Core service for sessions tagged for analysis. By default, continuous polling is disabled. You can enable Denial of Service (DOS) attack prevention for use during continuous polling. You can test the connection to the Malware Analysis service that is being continuously polled using an option in the Integration tab.

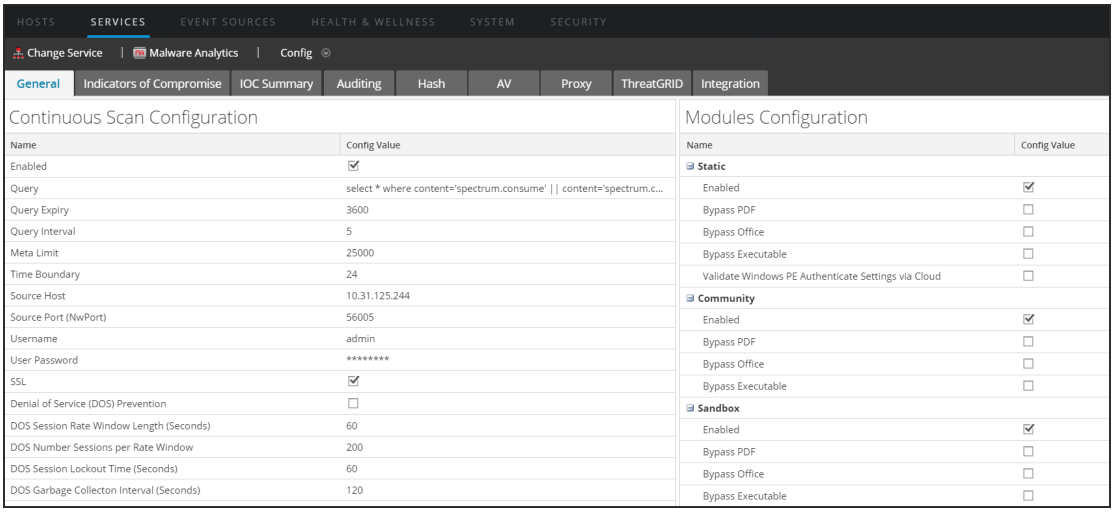
> **Note:** When adding a Core service as a service for continuous polling on 10.3.5 and earlier Malware Analysis, use the REST port; for example, add a Concentrator to 10.3.5 Malware Analysis with REST port (50105) instead of the native NexGen port (50005).

- **On-Demand Analysis of the Core service:** You can analyze sessions based on Investigations initiated directly in NetWitness Suite. This method allows manually controlled consumption of Core sessions and allows tighter control over how files in those sessions are processed (for example, send to sandbox for processing). Document types can bypass the default restrictions and be sent to community or sandbox processing regardless of the configured setting.
- **Manual File Upload:** You can manually upload one or more files for analysis by navigating to a visible folder on your computer and selecting files to be uploaded. The maximum size for the uploaded files is configurable.

View the Basic Settings

To view the basic settings:

1. In the **main menu**, select **Administration > Services**.
2. In the **Services** grid, select a Malware Analysis service and click **> View > Config**.
   The Service Config for the service is displayed with the **General** tab open.



Configure Continuous Polling

Malware Analysis is rate limited so that 1,000 files per day may be submitted to ThreatGrid's Cloud for sandbox processing. To optimize your use of the sandbox, Malware Analysis configuration allows you to choose which of several methods of consumption Malware Analysis uses; you can enable or disable continuous polling.

An important consideration when configuring continuous polling is the Denial of Service (DOS) Prevention parameters. By default this feature is disabled because you need to carefully consider the settings for your environment before enabling the feature.

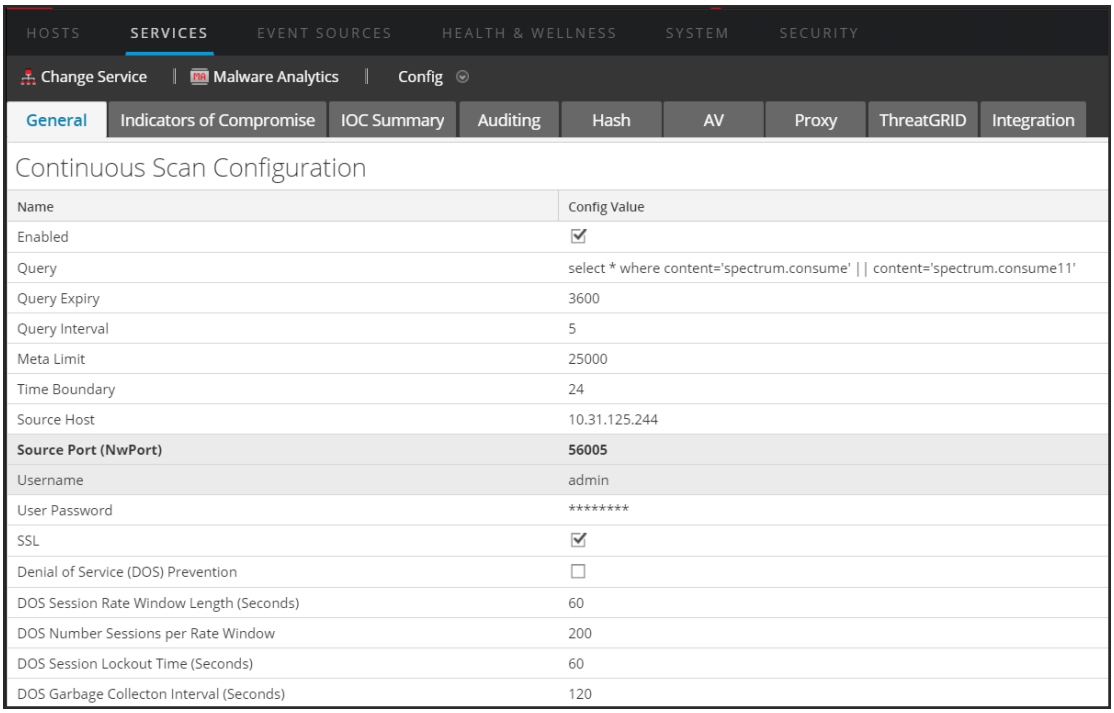
When DOS Prevention is disabled, Malware Analysis analyzes the queued sessions in first-in first-out order. A DOS attack may rapidly fill the queue so that Malware Analysis is busy handling those sessions, while a malware attack is occurring in a later session. The later session with the actual attack may not reach the beginning of the queue and undergo analysis until after the attack has begun.

When DOS Prevention is enabled, Malware Analysis treats too many sessions from a single IP address as a DOS attack. If an IP address exceeds the Number of Sessions per Rate Window, Malware Analysis begins to disregard sessions from that address until the Session Lockout time is reached. Then Malware Analysis resumes analysis of the sessions from that IP address. The disregarded sessions from the IP address are not analyzed at all, so a malware attack may slip through during the Session Lockout period.

Using the DOS Garbage Collection Interval setting, Malware Analysis clears in-memory storage of an IP source after a specified number of seconds. IP addresses with little activity during this interval are cleared from memory. If an IP address is active at intervals that exceed the DOS Garbage Collection Interval, Malware Analysis may not identify it as a DOS attack.

To configure Malware Analysis for continuous polling, in the Continuous Scan Configuration section:

1. Under **Admin**, click **Services**.
2. In the **General** tab, under **Continuous Scan Configuration** you can configure continuous polling.



3. To enable continuous polling, click **Enabled**.
4. (Optional) If you want to change the default values for querying, enter new values for the **Query Expiry**, **Query Interval**, **Meta Limit**, and **Time Boundary**.
5. To configure the Malware Analysis appliance that Malware Analysis queries to retrieve data for analysis, specify the **Source Host** and **Source Port (NwPort)**.
6. (Optional) If you want to change the default logon credentials for the Malware Analysis appliance, specify the **Username** and **User Password**.
7. If you want to use SSL for communication between the Malware Analysis appliance and the Core service, enable **SSL**.
8. (Optional) If you want to configure Denial of Service (DOS) prevention:
   a. Enable the **Denial of Service (DOS) Prevention** parameter.
   b. Set up the DOS prevention session limitations:
      - Specify the number of seconds of the time window during which Malware Analysis counts sessions for a single IP address (**DOS Session Rate Window Length**). The window is called a Rate Window and a counter is set when the first session is received from that IP source. The default value is 60 seconds.
      - Specify the number of sessions allowed per Rate Window in the **DOS Number Session per Rate Window**. The default value is 200 sessions. When the number of

sessions is reached within the Rate Window; Malware Analysis begins disregarding sessions from the IP address and the disregarded sessions from that IP are not analyzed at all. Malware Analysis continues to disregard sessions until the lockout time is reached.

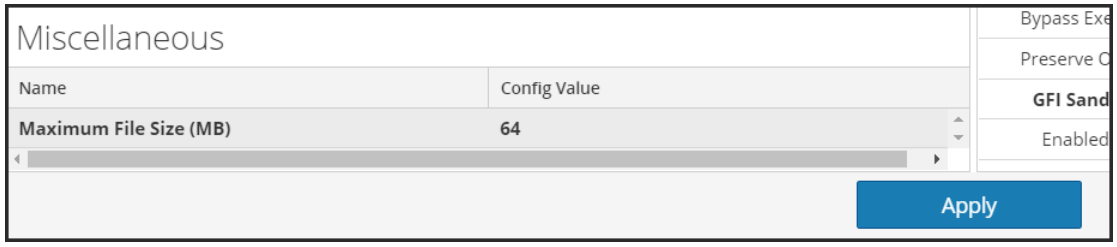
- Specify the length of lockout time (during which sessions from the IP address are disregarded and not analyzed) in the **DOS Session Lockout Time (Seconds)**. The default value is 60 seconds. When the lockout duration has elapsed, Malware Analysis resumes analysis of sessions from that IP address.
- Specify the interval of inactivity for an IP address before NetWitness Suite removes the in-memory object for the IP source in **DOS Garbage Collection Interval (Seconds)**. The default value is 120 seconds.

9. Click **Apply** to apply the changes.
   The applied changes become immediately effective as Malware Analysis receives new packets.
10. Test the connection of the Malware Analysis service to the Core service selected in the **Integration** tab by clicking the **Test Connection** button in the **Continuous Scan Connect Test** section.

Configure Manual File Upload Settings

To configure the maximum file size for manual file upload:

1. In the Miscellaneous section, type the maximum file size in Megabytes allowed for files uploaded manually for Malware Analysis scanning.



2. Click **Apply**.
   The changes become immediately effective.

Configure the Data Repository

Malware Analysis can store a finite number of files on the appliance. The data repository configuration has a file system retention period of 60 days. This setting determines how long files are retained in the Malware Analysis appliance. When old files are deleted, they cannot be recovered. Every day, Malware Analysis deletes files that exceed the file system retention period to ensure that there is no wasted disk space.

The File System Retention Period is the only setting that governs when files are deleted. Files are not deleted based on the amount of disk space being used. If the setting needs to be changed, the administrator must configure the retention period based on the anticipated space usage during the number of retention days specified.

The visible data repository parameters in the NetWitness Suite user interface are:

- The location of the repository is **/var/lib/netwitness/malware-analytics-server/spectrum**. Do not edit this value.
- The file sharing protocol, which allows access through one of the File Sharing Protocols to copy files from the Malware Analysis service.
- The file retention period in number of days.

To configure file sharing, in the Data Repository section:

1. Click on the the File Sharing Protocol to select FTP or SAMBA.
2. Select the number of days that files are maintained in the repository before deletion.
3. Click **Apply.**

The changes become immediately effective.

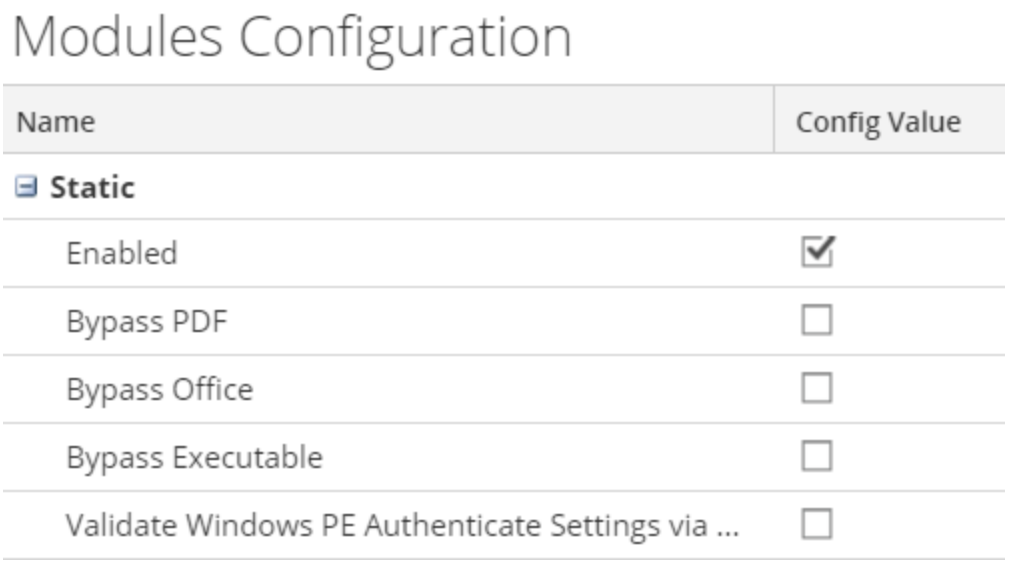
Calibrate Scoring Modules

The Modules configuration section helps configure the following components of Malware Analysis to:

- Completely disable any or all of three scoring modules (Static, Community, and Sandbox). Before disabling or enabling any scoring module, ensure that you understand what each scoring module detects.
- Malware Analysis tags sessions containing Microsoft Office, Windows PE, and PDF files for consumption by the Malware Analysis service. You can configure Malware Analysis to ignore Windows PE, Microsoft Office, and PDF documents entirely. If this is the case, a better option is to adjust your Core settings to ignore these files so they are not tagged for Malware Analysis consumption.

A sample application for using scoring module calibration is this: when setting up rule groups or analyzing system performance, you can test various scenarios in which PDF documents are not analyzed, but Microsoft Office and Windows PE documents are. You can test the scenario in each of the three scoring modules. If you see a measurable improvement in system performance, you can apply this knowledge on a broader scale.

Configure Static Analysis Scoring



To configure Static analysis scoring, in the **Modules Configuration** section:

1. By default the Static module is enabled. To enable or disable Static analysis entirely, click the **Enabled** checkbox.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select any of the checkboxes **Bypass PDF**, **Bypass Office**, and **Bypass Executable**.
3. To configure your preference for Authenticode validation of digitally signed Windows PE files, click the **Validate Windows PE Authenticate Settings via Cloud** checkbox. If you want to prevent Windows PE files that are digitally signed from being transmitted to the RSA Cloud for validation, remove the check.
   When disabled, ALL static analysis is performed locally (skipping Authenticode validation). Regardless of this setting, PDF and MS Office documents are not subject to Authenticode validation and are not transmitted over the network during static analysis.
4. Click **Apply.**The changes become immediately effective as Malware Analysis receives new packets.

Configure Community Analysis Scoring

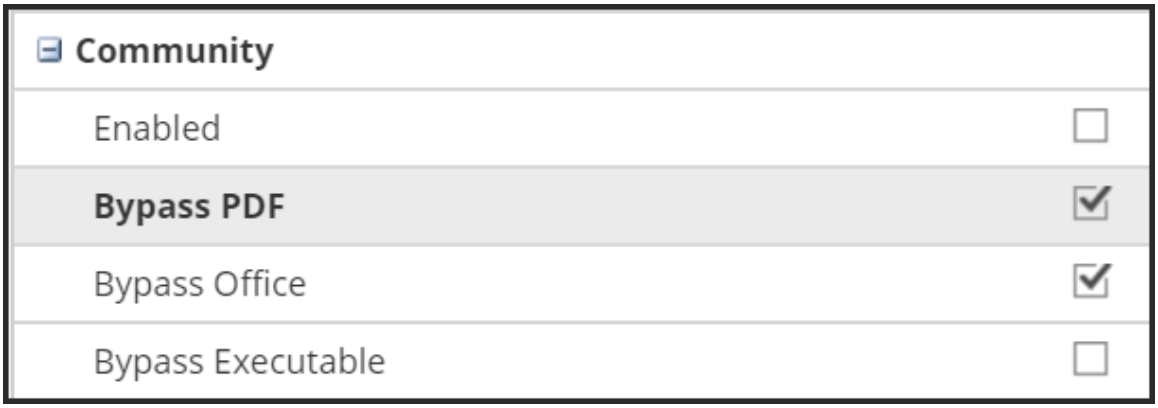
Once the Community module is enabled, the security community analyzes all documents not prevented from processing. This is achieved by sending network session and file attributes to the RSA Cloud for processing. The RSA Cloud then may make external connection to security community partners as needed to process the information.

The file content is never sent to the community for analysis. Instead, the MD5/SHA-1 hash of the file is sent for Anti-Virus detection and Blacklisting. Similarly, session Meta is harvested and analyzed as part of this process. Meta elements such as URL and Domain Name are examined and transmitted to the RSA Cloud to identify known bad URLs/Domains.

You can enable Community analysis and limit which document types are processed. There is no risk for the file content (except for a hash) being sent outside of your network.

Note: To gain access to the RSA Cloud where processing occurs, you must register your Malware Analysis service with RSA customer service. There are two methods: register the service using the options in the Integration tab or contact RSA Customer Care.

To configure Community analysis scoring, in the Modules Configuration section:



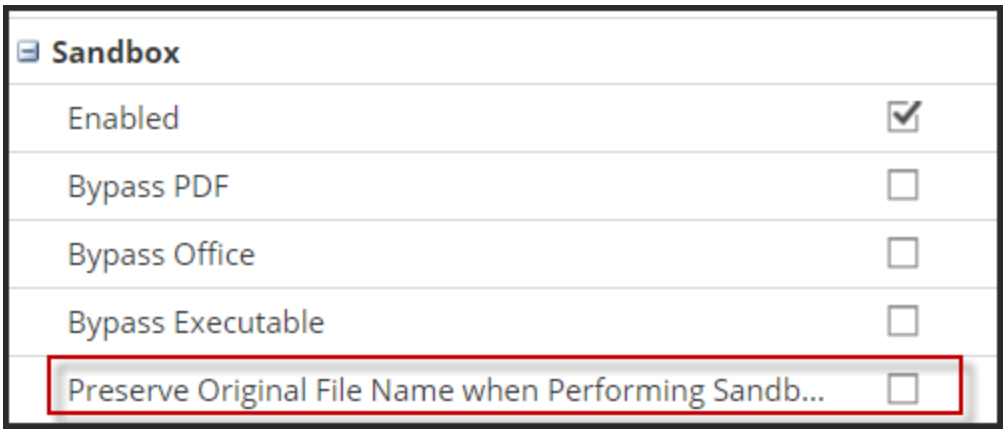
1. To enable or disable Community analysis entirely, click the **Enabled** checkbox. The default value is **Disabled**.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select the specific checkboxes - **bypasspdf**, **bypass office, bypass executable.**
3. Click **Apply** to save the changes and put them into effect immediately as Malware Analysis receives new packets.

Configure Sandbox Analysis Scoring

By default, the sandbox module is disabled and MS Office and PDF files are prevented from being processed. The intent is to set to the most restrictive settings to force the user to specify whether or not potentially sensitive information is sent outside of the network for processing. If a document type is not prevented from being processed, the entire file (not just the hash) is sent to the destination sandbox server.

In addition, you can choose to preserve the original file name when performing sandbox analysis.

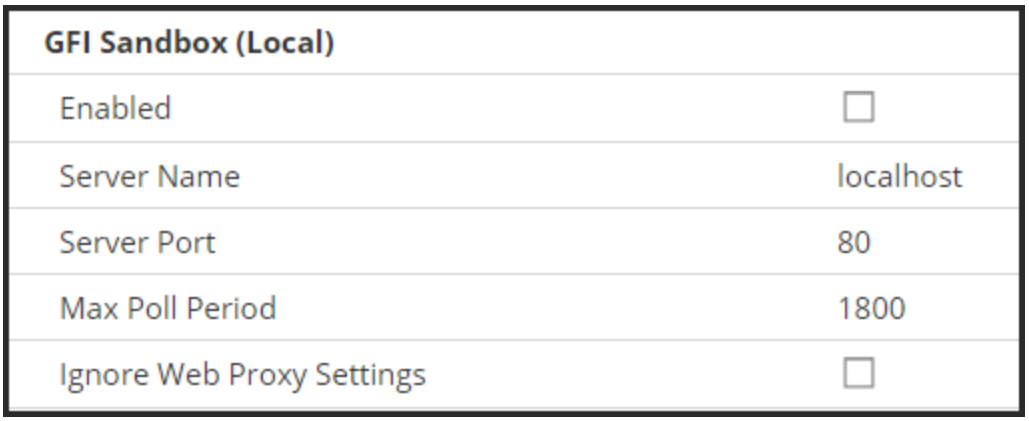
Note: If you do not specify the **Preserve Original File Name when Performing sandbox Analysis** parameter, NetWitness Suite hashes the files.



When you enable the sandbox module, you must specify whether or not the sandbox processing is performed using a local GFI sandbox, a local ThreatGrid sandbox, or a cloud version of the ThreatGrid sandbox. The cloud version of the ThreatGrid sandbox is provided directly by ThreatGrid and requires an activation key to be obtained from ThreatGrid and configured in the ThreatGRID tab.

GFI Sandbox Settings

To use a locally installed GFI sandbox, you must enable GFI and supply the Server Name and Server Port of the GFI sandbox Server. The Max Poll Period and Polling Interval determine how long to wait for a submitted sample to finish processing and how often to check the status (in seconds). The Ignore Web Proxy Settings option allows you to indicate that you want Malware Analysis to bypass a web proxy when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.



ThreatGrid Sandbox Settings

Note: Before enabling ThreatGrid scoring, a ThreatGrid-supplied Service Key must be configured so that ThreatGrid can recognize that samples submitted from this site are legitimate. Use NetWitness Suite to register for a ThreatGrid API key, then you can enable and configure a locally installed ThreatGrid sandbox or the ThreatGrid Cloud sandbox. Refer to the following detailed task: Register for a ThreatGrid API Key.

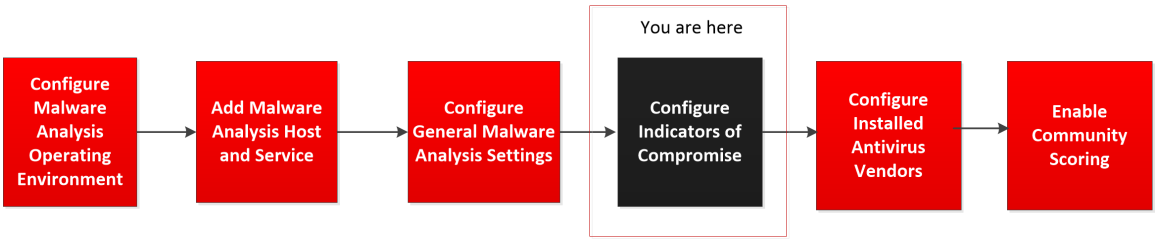
The Ignore Web Proxy Settings allows you to indicate that you want Malware Analysis to bypass a web proxy when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.

To configure sandbox scoring, in the Modules Configuration section:

1. To enable or disable sandbox analysis entirely, click the **Enabled** checkbox. The default value is **Disabled**.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select any of the three checkboxes **Bypass PDF**, **Bypass Office, Bypass Executable.**
3. Configure the active sandbox vendor. You have three options:
   a. To use a locally installed instance of the GFI sandbox, provide the Server Name and Server Port of the GFI sandbox Server, the Max Poll Period and Polling Interval, and optionally, select the Ignore Web Proxy checkbox.
   b. To use a locally installed instance of ThreatGrid, enable ThreatGrid scoring, provide the ThreatGrid Service Key and optionally, select the Ignore Web Proxy checkbox.
   c. To use the ThreatGrid Cloud, you must first register for a ThreatGrid API key. Then enable ThreatGrid scoring, provide the ThreatGrid Service Key, enter the URL for the ThreatGrid server (https://panacea.threatgrid.com), and optionally, select the Ignore Web Proxy checkbox.
4. Click **Apply**.
   The changes become immediately effective.

Configure Indicators of Compromise

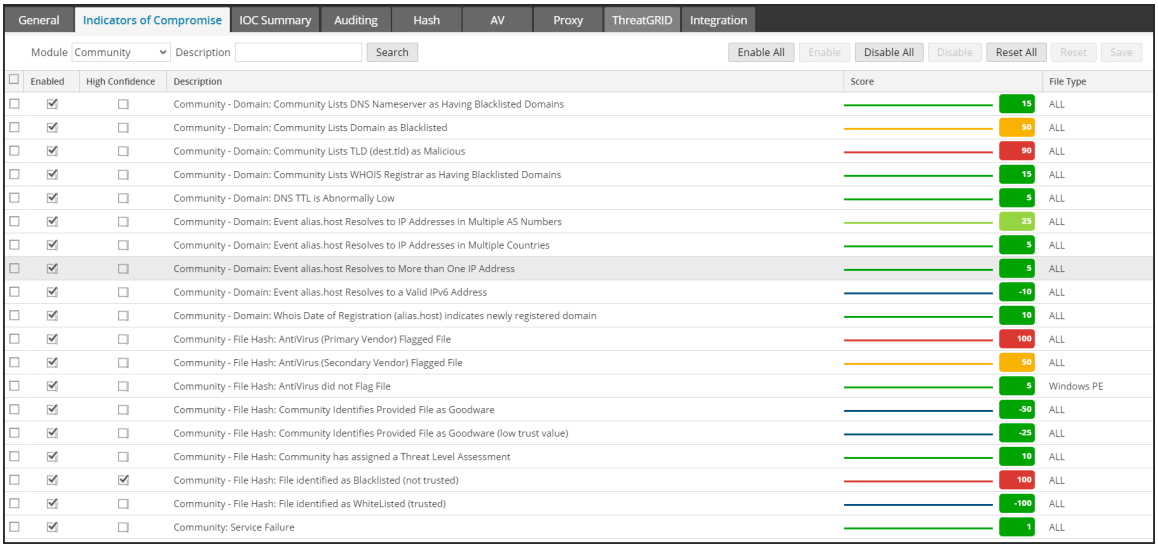
The Indicators of Compromise (IOC) for the Malware Analysis scoring modules are configured since, each Malware Analysis scoring module -- Network, Static, Community, sandbox, and YARA -- has a default set of Indicators of Compromise (IOCs) that it uses to evaluate the file and session data in order to assess the likelihood of malware being present.



Each IOC is assigned a numeric score weighting between -100 (good) and 100 (bad). When an IOC triggers, the numeric score weighting is factored into the total score for the session or file being analyzed. The individual score weightings for all matched IOCs are aggregated to produce the resulting score for each session or file. The aggregated score is adjusted to ensure that it does not exceed the valid score range (-100 through 100).

Note: The score weighting assigned to an IOC is not always the explicit score value that is aggregated (it is not a simple addition of score weights for each IOC that triggers). Instead, the IOC's score is a weighting or indicator of importance that is factored into calculating an overall score.

The Indicators of Compromise (IOC) configuration settings for Malware Analysis are in the Service Config view > Indicators of Compromise tab. Below is an example of the tab.



Using the **Community - File Hash: AntiVirus (Primary Vendor) Flagged File** IOC as an example, the IOC's score weighting could be set to 100. However, Malware Analysis dilutes this value based on the percentage of primary AV vendors that agree if the sample is malicious. The closer to 100% of the vendors who agree that the sample is malicious, the closer to the full 100 points are used in aggregating a score. As the percentage drops closer to 0%, the proportion of the full 100 points used in the aggregated score drops.

IOCs use logic implemented natively in Malware Analysis. You cannot adjust the logic. Instead, you can only adjust the IOC to increase or decrease its impact on scoring, to indicate a confidence setting, or to turn the IOC on or off. The typical scenario is to adjust a limited set of IOC score weighting values downward for IOCs that are inflating the final score and causing false positive analysis results. An extreme version of tuning would be to disable the IOCs entirely if they consistently contribute to false positive results. Additionally, the flexibility exists to allow you to disable all IOCs and to choose a select few to leave enabled. For example, all IOCs can be disabled with the exception of a select few IOCs that detect AntiVirus matches. Using Malware Analysis in this extremely limited configuration, you can reduce results in Malware Analysis such that only known A/V matches generate results.

You can configure this functionality in several ways:

- Disable IOCs so that they are not evaluated as part of the scoring module to which they are assigned.
- Adjust the score weight for an IOC such that its impact on the aggregated score is increased or decreased.
- Mark IOCs that you expect to be strong indicators of malware and display a high-confidence (HC) flag on sessions that triggered these IOCs in the Malware Analysis results.
- Customize score and confidence settings uniquely to the file type being analyzed. Each IOC is pre-assigned a file type to which it is applied. Possible values are **ALL**, **PDF**, **MS Office**, and **Windows PE**. The IOC with the most applicable file type is used during file-based analysis. For example, if a PDF is analyzed, an IOC with a file type set to **PDF** will be chosen rather than the same IOC with a file type set to **ALL.** If no file-type specific match is found, the IOC with a file type set to **ALL** is selected.
- Search for rules to display in the grid based on a match to the rule description.

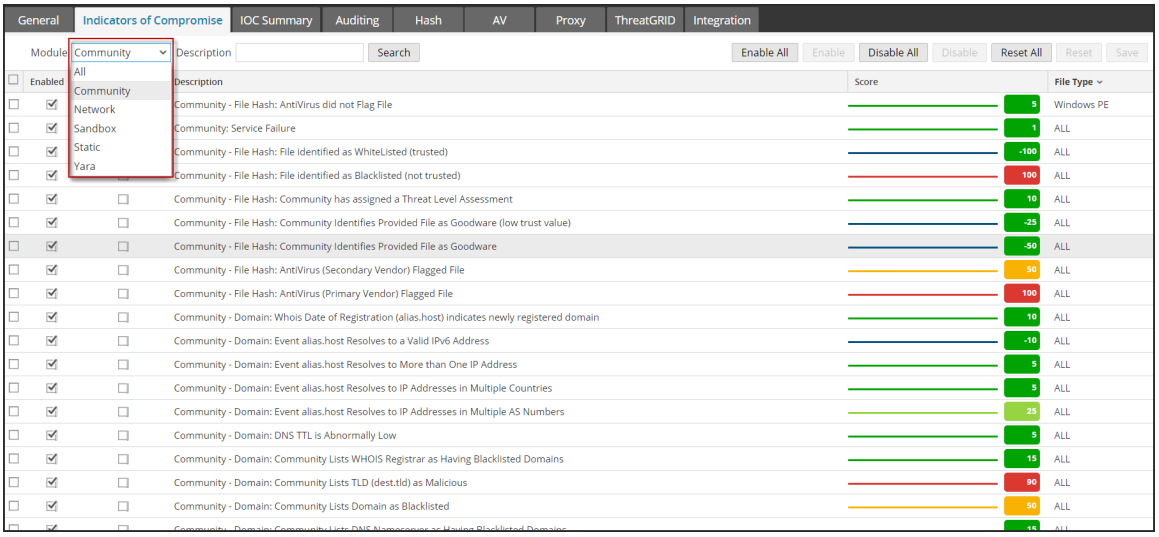
Filter Displayed IOCs by Module

You can filter the displayed IOCs by scoring module: one of the four built-in modules or YARA. YARA-based IOCs are interleaved with the native IOCs with each category. Although the YARA IOCs are not identified as such in the other views, you can select YARA from the Module selection list to see a list of YARA rules.

To view the IOCs for one or the four scoring modules or for YARA:

1. In the **main menu**, select **Admin > Services.**
2. Select a Malware Analysis service.
3. In the row, select **> View > Config**.
4. Click the **Indicators of Compromise** tab.
5. In the **Module** selection list, select All, NextGen, Static, Community, sandbox, or Yara.

   The configured rules and settings for the module are displayed.



Filter Displayed Modules to Show Only Modified Modules

The **Indicators of Compromise** tab visually identifies IOCs that are locally modified. When an IOC has been modified, for example, the score weight has been changed, and the name is displayed in red and includes a modification indicator appended to the IOC name. The modification indicator is ++ and can be used as a filtering mechanism when searching for IOCs. To limit the display to locally modified IOCs:

1. In the **Description** field, enter ++.
2. Click **Search**.

   The view is filtered to show only modified IOCs.

Enable and Disable IOCs for a Scoring Module

When an IOC is disabled, it no longer impacts the aggregate score for the scoring module to which it belongs. If the IOC has multiple instances (differentiated only by file type), disabling a more file-type specific IOC results in use of the more file-type agnostic version of the IOC in scoring.

For example, if the same IOC exists as file type **ALL** and file type **Windows PE**, disabling the **Windows PE** instance of the IOC causes the **ALL** version to be used in scoring. In order to disable the IOC entirely for **Windows PE**, while leaving the IOC enabled for other file types, set the score weighting of the **Windows PE** instance of the IOC to a value of zero as described below. This leaves the IOC enabled for Windows PE files (although it has a zero weighting and is suppressed from being displayed in analysis results), while not affecting the other file types. The remaining file types will continue to use the **ALL** instance of the IOC.

To enable or disable an IOC so that it no longer factors into a scoring module:

1. In the **main menu**, select **Admin > Services.**
2. Select a Malware Analysis service, and in the row select > **View > Config**.
3. Click the **Indicators of Compromise** tab.
4. In the **Module** selection list, select a scoring module: All, Community, Network, sandbox, Static, or Yara.
   The configured rules and settings for the module are displayed.
5. Do one of the following:
   a. Click the **Enabled** checkbox in the column next to a rule that you want to enable.
   b. Select one or more rules, and click **Enable** or **Disable** in the toolbar.
   c. To toggle between Enabled and Disabled for all rules displayed on the page, click the **Enabled** checkbox in the column title.
   d. To enable or disable all rules for the scoring module, click **Enable All** or **Disable All** in the toolbar.
6. To save the changes to the page, click **Save** in the toolbar.

> **Note:** Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

Adjust the Score Weight for an IOC

Adjusting the score weight for an IOC increases or decreases the IOC's overall impact on the aggregate score for the module in which it is configured. To raise or lower the overall impact of the IOC, reduce the current value to a new setting.

- Values ranging from -100 to -1 indicate that the session or file being analyzed is not likely to be malware (-100 being the least likelihood).
- Values ranging from 1 to 100 indicate a likelihood that the file or session being analyzed is malware (100 being the highest likelihood).
- Setting the value to zero leaves the IOC enabled, but causes the IOC to no longer impact the aggregate score and suppresses the IOC from being displayed in analysis results. Setting the value to zero is a method of disabling a file-type specific instance of an IOC while leaving

the original file-type agnostic instance of the rule intact for scoring of the remaining file types.

To adjust the score weight:

1. In the **main menu**, select **Admin > Services.**
2. Select a Malware Analysis service.
3. In the **Toolbar**, select **View > Config**.
4. Click the **Indicators of Compromise** tab.
5. In the **Module** selection list, select a scoring module: All, Network, Static, Community, sandbox or Yara.
   The configured rules and settings for the module are displayed.
6. Do one of the following:
   a. Drag the score slider left or right to decrease or increase the score weight.
   b. Click directly on the displayed score weight and enter a new score weight.
7. To save the changes to the page, click **Save** in the toolbar.

   Note: Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

Set the High Confidence Flag for an IOC

The High Confidence setting is used as a method of flagging specific IOCs as high confidence indicators that malware is present. As an example, the **Community - File Hash: AntiVirus (Primary Vendor) Flagged File** IOC has a low probability of being a false positive, combined with a high probability of being an accurate measurement of malware being present. By flagging this IOC (and others) as High Confidence, you can use a filter in the Malware Analysis results to limit display to only those sessions that include one or more high confidence rules. By doing so, the display is limited to a smaller subset of results whose accuracy is accorded a higher degree of confidence. Displaying results not limited to high confidence IOCs still allows you to review results that are more grey in nature. This provides for results that are less prone to false negative results. Choosing to filter or to not filter results based on confidence level has a valid use case in the NetWitness Suite workflow.
To set the High Confidence flag:

1. In the **Indicators of Compromise** tab, select a scoring module from the **Module** selection list: All, Network, Static, Community, sandbox, or Yara.
   The configured rules and settings for the module are displayed.
2. Click the **High Confidence** checkbox in the column next to a rule that you want to flag or unflag as highly likely to indicate the presence of malware in a session when matched.
3. To save the changes to the page, click **Save** in the toolbar.

Note: Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

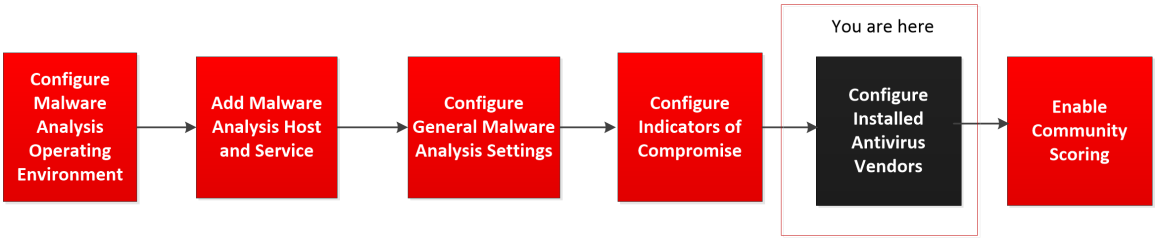
Reset IOCs to Default Settings

1. In the **Indicators of Compromise** tab, select a scoring module from the Module selection list: All, Network, Static, Community, sandbox, or Yara.
   The configured rules and settings for the module are displayed.
2. If you want to reset all rules on the current page to their default settings, click **Reset** in the toolbar.
3. If you want to reset all rules for the selected scoring module to default settings, click **Reset All** in the toolbar.
4. To save changes to the page, click **Save** in the toolbar.

Configure Installed Antivirus Vendors

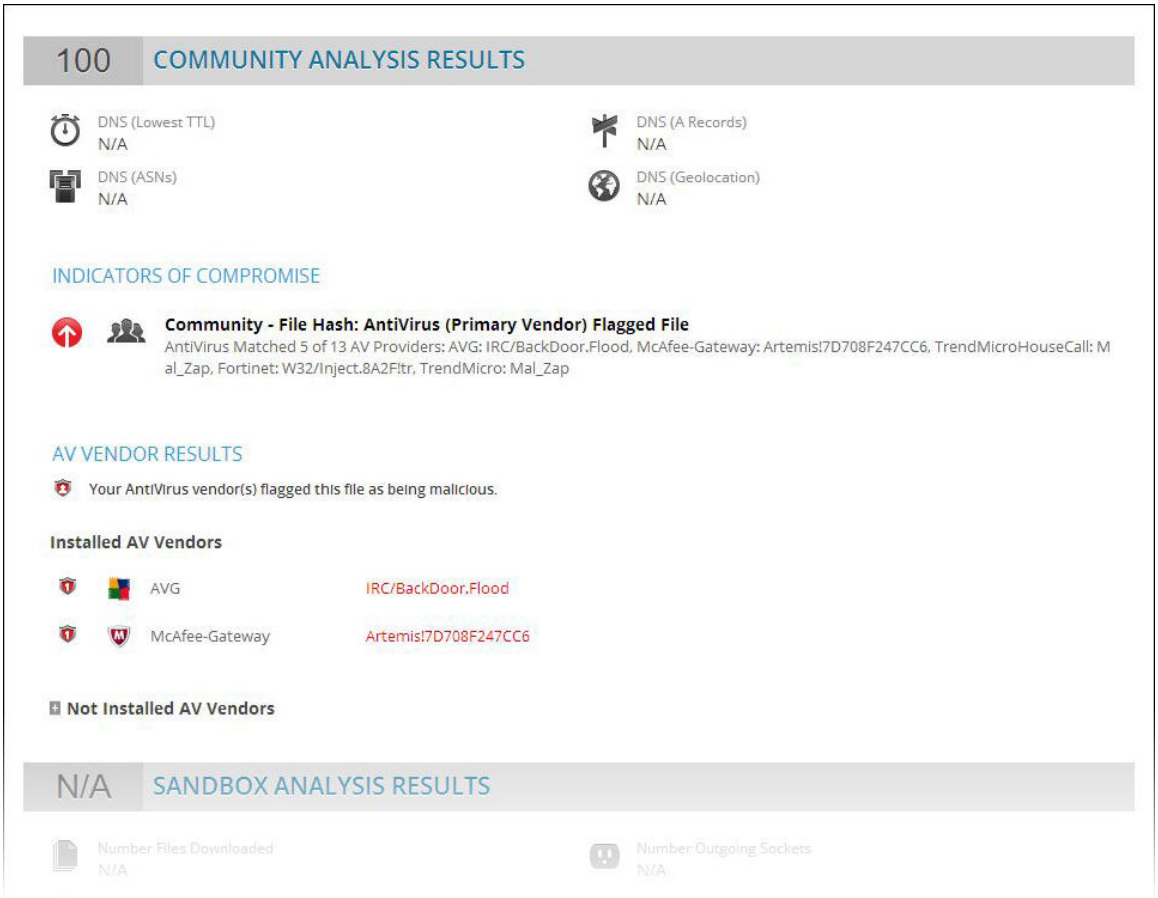
You can compare file analysis results from your installed antivirus (AV) vendors versus community results from the Malware Analysis knowledge base. While a file is being analyzed by community analysis, Malware Analysis checks an antivirus knowledge base to determine if the sample is already known to be malicious. If the file is known to be malicious, NetWitness Suite flags the file to indicate whether a primary antivirus vendor or a secondary antivirus vendor identified the sample. NetWitness Suite classifies vendors as primary and secondary to indicate the level of reputation the vendors have in the industry, and Indicators of Compromise factor the reputation into scoring. For example, detection made solely by secondary antivirus vendors may score less than detection by primary vendors.

Note: When choosing AV vendor software to install on your network, it is highly recommended that you include at least one from NetWitness Suite Primary Vendors list.



You can identify the antivirus vendors installed on your network to NetWitness Suite. NetWitness Suite compares the antivirus results during community analysis against the results from the installed vendors selected in the AV tab. If a match is detected, the file being analyzed is flagged to indicate that your locally installed primary or secondary antivirus software detected the sample.

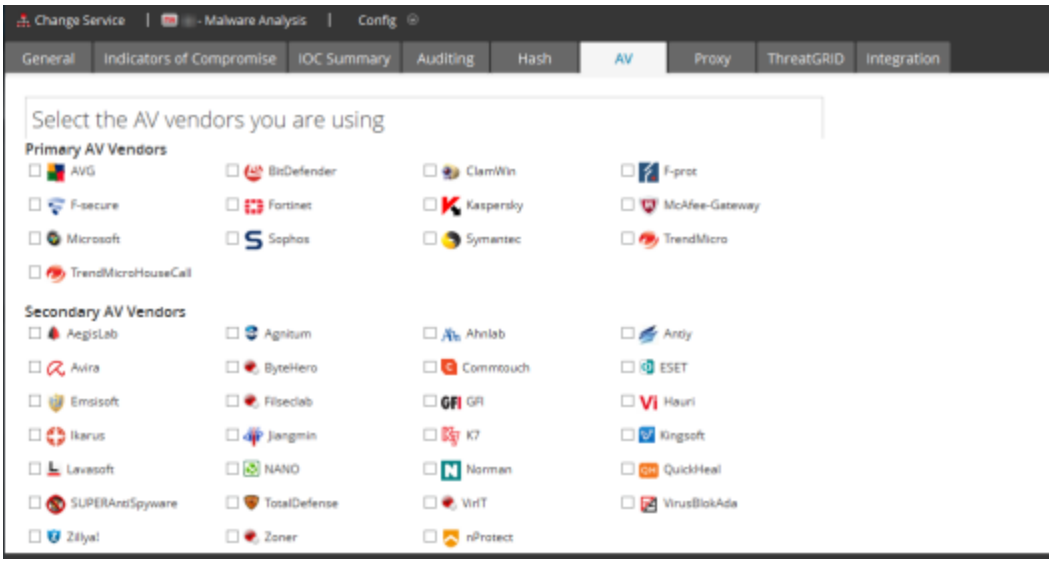
The example below shows the community analysis results for a file that had a score of 100. Under **Indicators of Compromise**, you can see that the file was flagged by the listed AV vendors in the Community. Under **AV Vendor Results**, NetWitness Suite indicates whether the AV vendors installed in your environment flagged the file as malicious. If your installed AV vendors detected the virus, the name of the malware is displayed. If your installed AV vendors did not detected the virus, **--Not detected--** is displayed next the AV vendor name. Under **Not Installed Vendors**, you can click + to expand the section and see if other vendors not installed on your system detected the virus.



Identify Installed AV Software

To identify Antivirus software installed on your network:

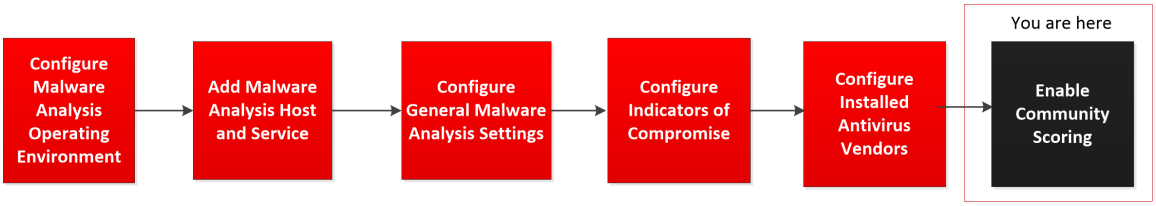
1. In the **main menu**, select **ADMIN > Services.**
2. Select a Malware Analysis service, and in the row select > **View** > **Config**.
3. In the **Service Config View**, select the **AV** tab.



4. Select the checkbox next to each antivirus vendor (primary and other) whose software is installed on your network.
5. To save the changes, click **Apply**.
   The Community Analysis results will indicate whether your software flagged an event.
6. (Optional) If you want to reset the list of installed AV software to the default value (none), click **Reset**.
   All selections are removed.
7. To save changes, click **Apply**.

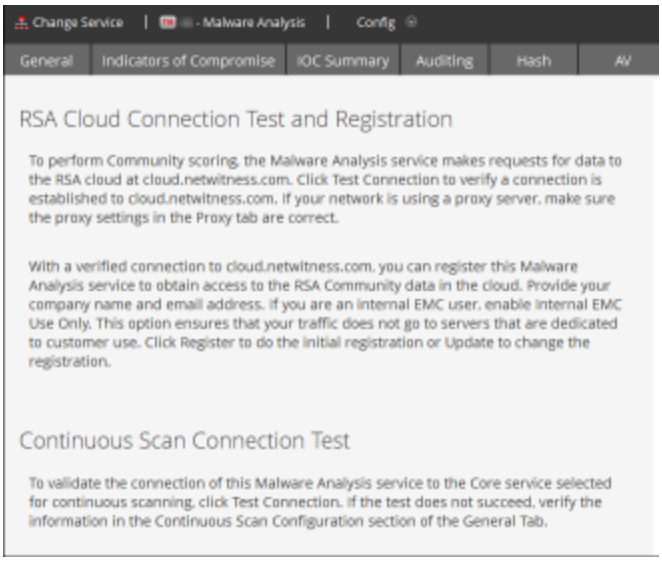
Enable Community Analysis

An Administrator can enable community analysis. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. To enable Community analysis, you must register with the RSA cloud and test connection to the cloud, then to test the connection between the RSA cloud and the service you have configured for continuous scanning.



A complete description of analysis methods is provided in How Malware Analysis Works.

1. In the **main menu**, select **ADMIN > Services.**
2. Select a Malware Analysis service, and in the row select **> View > Config**.
3. In the **Service Config View**, select the **Integration** tab.



4. Scroll down to the Continuous Scan Connection Test, and click **RSA Cloud Connection Test and Registration**.

   NetWitness Suitetests communications with the site at `https://cloud.netwitness.com`. If your company uses a proxy for outbound traffic, please check your Proxy settings. A valid connection is required in order to register with the RSA Community Service.

5. Enter your company name and contact email. Click **Register**.

   If all required fields are complete, your registration is completed. The label on the button used to register changes to Update.

6. To verify that the Malware Analysis Service can connect to the Core service selected for continuous scanning, click **Continuous Scan Connection Test**.

   NetWitness Suiteinitiates a check based on the Source Host, Source Port, Username, and User Password specified in the General tab. When the test executes successfully, analysts are able to see Community Scoring in Malware Analysis.

(Optional) Configure Auditing on Malware Analysis Host

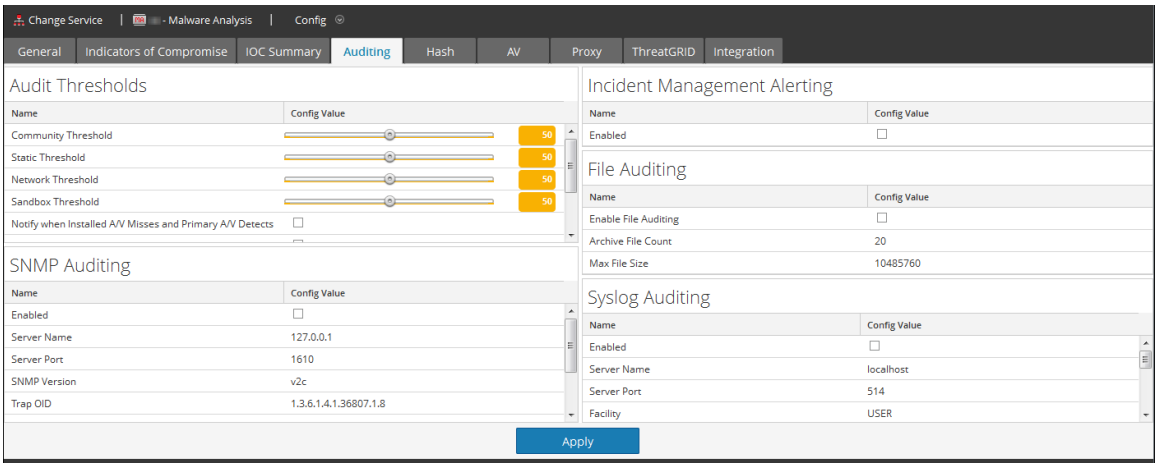
This topic introduces the configurable features of the Malware Analysis auditing log and the procedures for configuring the features. Malware Analysis is capable of generating auditing alerts based on configured score module thresholds. Once the analysis score for a file in an analysis session meets or exceeds the configured threshold(s), an auditing alert is generated. Thresholding allows sessions and files that score high enough to be likely malware candidates to automatically generate an alert.

Alerts can be configured to be formatted as SNMP, Syslog or File entries. Supporting various audit formats provides a method for external systems to ingest auditing events based on their capability of parsing the supported formats.

In addition to auditing analysis sessions, the following events will trigger an audit alert:

- User login successes and failures
- Changes to system configuration settings
- Server restart
- Server version upgrade and install

The Auditing configuration settings for Malware Analysis are in the Service Config view > Auditing tab.



Configure the Auditing Threshold

The sole purpose of the thresholds is to specify the criteria that must be reached prior to an alert being generated for an analyzed session/file. If auditing is enabled, each scored file/session is examined to determine if the score in each score module meets or exceeds the configured auditing threshold. If so, an alert is generated using the configured audit alert format (e.g., SNMP, Syslog or File). For example, by configuring SNMP and setting the Community Threshold to 90, all sessions/files that score 90 or higher in the Community Score module generate an SNMP trap. If all of the thresholds are set to 90, then an alert is not generated unless a session or file scores 90 or higher in the Network, Static, Community and sandbox score modules.

To configure the auditing threshold:

1. In the **main menu**, select **ADMIN > Services**.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, click the **Auditing** tab.
4. In the **Auditing Thresholds** section:
   a. Set the threshold for the **Community**, **Static**, **Network**, and **Sandbox** by doing one of the following for each scoring module:
      - In the slider, click and drag the handle in either direction.
      - In the value field, type a number between 0 and 100, inclusive.
   b. (Optional for 10.3 SP2) Select one or more triggers to record a message and deliver it through all enabled auditing methods.
   c. Click **Apply**.
      - The threshold setting becomes effective immediately for all enabled auditing methods: SNMP, File, and Syslog.
      - The recorded messages are sent through all enabled auditing methods: SNMP, File, and Syslog.

Configure Incident Management Alerting

When enabled, Incident Management can audit Malware Analysis alerts to feed into the Incident Management workflow.

1. In the **main menu**, select **ADMIN > Services**.
2. Select a Malware Analysis service, and select select **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.

4. In the **Incident Management Alerting** section, select the Enabled checkbox and click Apply.
   Alerting becomes effective immediately.

Configure SNMP Auditing

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing services on IP networks. When SNMP auditing is enabled, Malware Analysis can send an audit event as an SNMP trap to a configured SNMP trap host. In addition to the score and event ID, the alert includes all session meta as well as generated meta data. This is useful for users who want to feed event data to third-party systems.

To configure SNMP auditing:

1. In the main menu, select **ADMIN > Services**.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **SNMP Auditing** section, click the checkbox to enable SNMP auditing.
5. Configure the SNMP server name and port.
6. Configure the SNMP version and trap OID for sending traps.
7. Configure the Malware Analysis community, and retry and timeout parameters when sending traps.
8. Click **Apply**.
   The SNMP auditing settings become effective immediately.

Configure File Auditing Settings

When file auditing is enabled, the audit log file is kept in the Malware Analysis Home Directory. The default location for this log file is:

`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`.

As each log reaches the maximum file size, it is archived and a new log is created. The size of these audit logs and their number are both configurable.

Caution: Avoid setting the max file size and archive file count too high, because it may have an adverse effect on the available disk space on the Malware Analysis appliance.

To configure the file auditing settings:

1. In the **main menu** , select **ADMIN > Services**.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **File Auditing** section, click the checkbox to enable file auditing.
5. (Optional) Set the Archive File Count and Max File Size.
6. Click **Apply**.
   The file auditing settings become effective immediately.

Configure Syslog Auditing Settings

When enabled, Syslog provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

In addition to the score and event ID, the syslog includes all session meta as well as generated meta data. This is useful for users who want to feed event data to third-party systems.

To configure the syslog auditing settings:

1. In the **main menu**, select **ADMIN > Services**.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **Syslog Auditing** section, click the checkbox to enable syslog auditing.
5. Configure the host where the target syslog process is running and the port on the host where the syslog process is listening.
6. Configure the facility, encoding, format, max length, and timestamp for outgoing syslog messages.

   Note: (Optional) Configure Identity String to prepend to syslog alerts.
   For CEF format, please refer to Create Custom Alert in CEF Format for additional considerations.

7. Click **Apply**.

   The syslog auditing settings become effective immediately.

(Optional) Configure Hash Filter

This topic introduces hash filters as a method of marking files in Malware Analysis that are known to be good or known to be bad. Hash filtering allows you to maintain a list of known good or known bad file hashes. In the Hash tab, you can fine tune Malware Analysis event analysis based on file hashes. When a file hash is marked as Good, Malware Analysis does not analyze the file the next time it is seen. When a file hash is marked as Bad, Malware Analysis automatically raises the file's community score by a large number of points. Malware Analysis still analyzes the file, just in case new information becomes available.

Note: If an event contains a single file and that file's hash is marked as Good, Malware Analysis filters the entire event and you do not see it in Malware Analysis results.

To add hash filters to the hash list, you can use either of these manual methods:

1. Context menu add in the Event Detail view: Right-click on a file, and a context menu allows marking of the hash for the selected file as Good (Normal) or Bad (Malicious).
2. Hash tab toolbar: Click on the Add button in the Hash tab to add a file hash, file size, and optionally, mark the hash as trusted.

There is also an automated method to add hash filters to Malware Analysis by importing a hash list in bulk from the watched folder. Hashes imported through the watched folder do not appear in the hash list. With bulk importing and the watched directory (/var/netwitness/malware-analytics-server/spectrum/hashWatch) on the Malware Analysis server set up, copy a hash list into the watched folder to be automatically imported into the system. Hashes imported using the bulk import method overwrite hashes that were previously imported through the watched folder.

View the Hash List

To view the Hash List:

1. In the **main menu**, select **ADMIN > Services**.
2. In the Services view, select a Malware Analysis service, and select **> View > Config**.
3. Select the **Hash** tab.

   The hash list is displayed in the Hash tab. Only file hashes that have been added using one of the methods are displayed.

Add a File Hash to the Hash Filter

To add a file hash to the hash filter:

1. In the **Hash** tab, in the toolbar, click **Add**.

   The Add Hash dialog is displayed.
2. If the hash is trusted, select **Trusted**.

3. Enter the MD5 hash and the file size in bytes.
4. Click **Save**.

   The file hash is added to the hashes and used to perform hash filtering in Malware Analysis.

Mark a Hash as Trusted or Untrusted

To mark a file hash as trusted or untrusted:

1. In the **Hash** tab, to toggle between trusted and untrusted, click in the **Trusted** column for the hash.
2. In the toolbar, click **Save Edit**.

Delete a Hash from the Hash Filter

To delete a hash from the hash filter:

1. In the **Hash** tab, select one or more hashes that you want to remove from the hash filter.
2. In the toolbar, click **Delete**.

   A dialog requests confirmation and offers an opportunity to cancel.
3. To confirm the deletion, click **Yes**.

   The file hash is deleted from the grid and no longer used to perform hash filtering in Malware Analysis.

Search for a File Hash

In the Hash tab, you can search for a file hash that is displayed in the grid. In the MD5 field, type the file hash for which you are searching, and click **Search**. The list of files that contain the hash is displayed in the grid.

Import a Hash List Using the Watched Folder

To import a hash list from the watched directory, the hash list must be in the specified format and must be sorted on md5. You can drop a file formatted as described below into a folder (/var/netwitness/malware-analytics-server/spectrum/hashWatch) on the Malware Analysis appliance, and it is automatically imported into the local hash database. This is the only way to import file hashes into. An additional use case is to allow a system administrator to expose the watched directory to some process that would push a file to this directory. This is a bulk import method designed to handle a high volume of hash imports.

This is a csv-formatted file with no spaces between the data in each row. The assumption with the data in the hash list is that there are no duplicates. Duplicates are ignored during processing. If duplicate hashes are encountered, the log file will display the following message to indicate the number of duplicate hashes contained in the file:

2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing - /var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /var/lib/rsa>malware/hashWatch/test.csv

Below is an example of a hash list in the default file format.

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

A NetWitness Suite configuration file (**/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml**) specifies the format and options in the hash list import process. Below is a listing of the configuration file.

```
<config>
 <enabled>true</enabled>
 <distributedCacheEnabled>true</distributedCacheEnabled>

<watchDirectory>/
/var/lib/rsamalware/hashWatch</watchDirectory>

<processedDirectory>/
var/lib/rsamalware/hashWatch/processed</processedDirectory>
```

```
<erroredDirectory>/
var/lib/rsamalware/hashWatch/error</erroredDirectory>
 <md5Col>0</md5Col>
 <fileSizeCol>-1</fileSizeCol>
 <isTrustedCol>1</isTrustedCol>
 <isTrust>false</isTrust>
 <ignoreFirstLine>false</ignoreFirstLine>
 <frequencyInMinutes>1</frequencyInMinutes>
 <isGzipCompressed>false</isGzipCompressed>
 </config>
```

Line	Description
<md5Col>0</md5Col>	The location of the md5 hash in each entry. The default value is position **0**, or the first position.
<fileSizeCol>1</fileSizeCol>	The location of the hash size in each entry. The default value is position **1**, or the second position. If the hash size is not included in the csv file, the value must be **-1**.
<isTrustedCol>2</isTrustedCol>	The location of the Trusted Column in each entry. The default value is position **2**. If the Trusted parameter is not included in the csv file, the value must be **-1**.
<isTrust>false</isTrust>	The default assumption for **Trusted** in each entry is **false**.
<ignoreFirstLine>false</ignoreFirstLine>	The presence or absence of a header in the hash. The default value is **false**. If the hash has a header, the value must be set to **true**.
<frequencyInMinutes>1</frequencyInMinutes>	The interval between checks by NetWitness Suite in the watched directory. The default value is **1** minute.
<isGzipCompressed>false</isGzipCompressed>	The hash is compressed using Gzip. The default value is **false**. If the hash is Gzip compressed, the value must be set to **true** here.

When the hash list has been imported, the system log has entries similar to this:

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processed -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

If there is a problem loading the file, the system log has entries similar to this:

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 ... Verbose log
 2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Error Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

To import a hash list using the watched folder method:

1. Copy the hash lists that you want to import into the **/var/netwitness/malware-analytics-sever/spectrum/hashWatch** directory.
   Malware Analysis automatically watches this folder and processes files placed there.
   Malware Analysis adds every hash found in the hash lists to the hash filter.
   If there are processing errors, they are logged in **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error**
   Processed files are cataloged in **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed**
   Processed files are not removed from the hashWatch directory.
2. After importing hashes in bulk, the System Administrator can use a cronjob to clean up old processed files.

(Optional) Configure Malware Analysis Proxy Settings

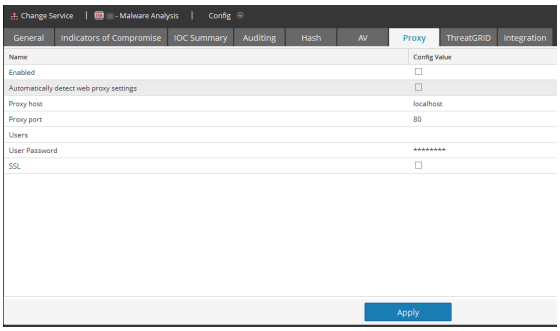
This topic describes the configuration of a web proxy for communicating with the RSA Cloud service and local ThreatGrid or GFI service. The settings in the Service Configuration view > Proxy tab set up communication by web proxy, which Malware Analysis can use to communicate with RSA Cloud for community analysis and sandbox analysis. Once the proxy is configured:

- Malware Analysis communicates via web proxy with the RSA Cloud for community analysis.
- Malware Analysis communicates via web proxy with the configured ThreatGrid or GFI sandbox service. Using a web proxy may negatively affect performance. ThreatGrid and GFI configuration sections in the General tab have an option to ignore the web proxy and communicate directly with the sandbox to improve performance.

Configure the Web Proxy

To configure the web proxy for Malware Analysis:

1. Navigate to the **ADMIN > Services** view.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, select the **Proxy** tab.



4. To enable the proxy, select the **Enabled** checkbox.
5. (Optional) To automatically detect proxy settings for the NetWitness Server, select the checkbox.

   The proxy host and proxy port fields are autofilled.
6. If you want to use a different proxy, enter the **Proxy Host** and **Proxy Port**.
7. Enter the username and password used to log on to the proxy host.
8. (Optional) Select **SSL**, if the proxy host communicates over SSL.
9. Click **Apply**.

   The settings are saved and become effective immediately.

Note: Malware Analysis does not support NTML web proxy authentication.

(Optional) Register for a ThreatGrid API Key

This topic provides the procedure for obtaining a trial ThreatGrid API key for use in the ThreatGrid Cloud sandbox. Before enabling ThreatGrid as the sandbox service in the sandbox module, a ThreatGrid-supplied Service Key must be configured so that ThreatGrid can recognize that samples submitted from this site are legitimate.

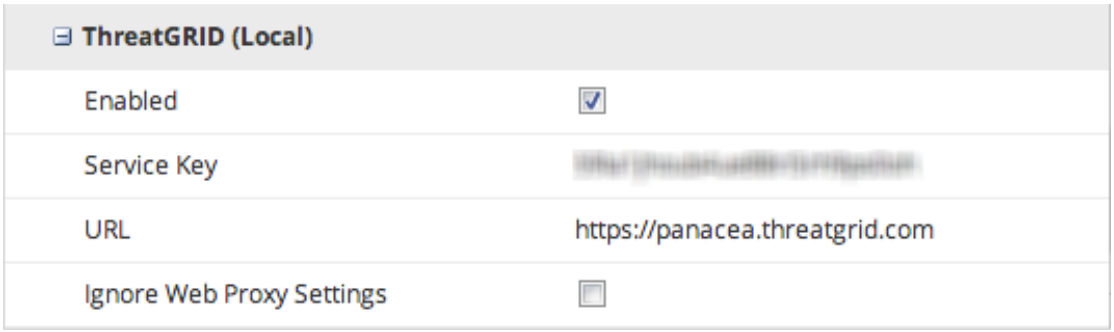
If you do not have a ThreatGrid-supplied Service Key, you can obtain a key using this tab. The key is provided on a trial basis.

When you fill in your user information and click **Register**, a key is displayed in this tab, and automatically added to the ThreatGrid configuration in the **General** tab. In a few minutes, you will receive an email from ThreatGrid containing a link to their page where you can log on. After you agree to the license terms on the ThreatGrid page, you can submit files for analysis, and ThreatGrid will recognize files that Malware Analysis submits for sandbox analysis.

To obtain a Trial ThreatGrid API key:

1. In NetWitness Suite, go to **ADMIN > Services**.
2. Select a Malware Analysis service, and select **> View > Config**.
3. In the **Services Config** view, select the **ThreatGrid** tab.
4. Enter your full name, job title, organization name, and email address.
5. In the User Id and Password field, create a user ID and password for logging on to ThreatGrid.
6. Click **Register**.

   Your registration is sent to ThreatGrid and an API key is displayed below the Register button. The key is automatically filled in the **General** tab.
7. Select the **General** tab to confirm that the ThreatGRID configuration now includes the API key.



8. When you receive an email from ThreatGrid with a link where you can log on, log on and accept the terms of the agreement.

Your trial of ThreatGrid begins and Malware Analysis can send five files per day to the ThreatGrid Cloud for sandbox analysis.

Additional Procedures for Configuring Malware Analysis

This topic provides procedures that an Administrator may perform to accomplish an objective that is not part of basic Malware Analysis setup. After Malware Analysis is configured, administrators may want to fine-tune the service and implement advanced customization; an example of this is implementing custom YARA content.

- Create Custom Alert in CEF Format
- Enable Custom YARA Content

Create Custom Alert in CEF Format

This topic provides instructions for creating custom alerts in Common Event Format (CEF) to send to a service that ingests events as CEF. This is an advanced configuration task, which requires sufficient knowledge to manually edit the configuration file: `/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`. Before editing the file, you must stop the Malware Analysis service in the operating system. The CEF Alert becomes active when you restart the Malware Analysis service.

The CEF Template

To send events to a service ingesting events as CEF, NetWitness Suite runs them through a configuration file that serves as a CEF template before feeding the events to a correlation technology. You can tune the configuration file, which specifies the sequence and mapping of syslog fields in each alert.

The following example syslog message shows the CEF fields in the extensions section of the alert (following the last '|' in the alert). Each field can be configured to indicate the sequence (described in the Example section below). Fields can be excluded entirely from the alert via a configuration setting.

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0
nextgen=25.0 community=100.0 sandbox=25.0 file.name=myFile.exe
file.size=1234556 file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563
event.type=MANUAL_UPLOAD event.id=0 country.dst.code=--
country.dst=Unavailable ip.src=0:0:0:0:0:0:0:1
ip.dst=0:0:0:0:0:0:0:1 event.uuid=f7a6155a-31de-4fa6-ba16-
41fb9a8e5f26 ...
```

Understand a Syslog Auditing File Entry

The description of the file structure is based on the following sample.

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125

CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected
suspicious
 network event ID 857 session ID 73|2|

static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307

com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2
referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/
risk.info=http client server version mismatch
```

First Line

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

Log Information	Description
Feb 6 10:02:28	The timestamp for the entry.
10.10.10.125	The source IP address for the event.
SpectrumServer125	The source hostname for the event.

Audit Common Event Format (CEF) Header

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
network event ID 857 session ID 73|2|
```

The audit CEF header is a pipe-separated listing of the following fields:

Log Information	Description
0	The ArcSight Common Event Format (CEF) version used for the audit syslog.
NetWitness	The service that created the syslog message.
Spectrum	Malware Analysis is the logger for the event.
1.2.1.130	Malware Analysis version.
event ID 857	Unique network event id for this event.
session ID 73	Core unique session id for the session that included this event.
2	Severity, an integer between 1 and 6 indicates the level of severity for the message. • 1 = INFORMATION_LEVEL • 2 = WARNING_LEVEL • 3 = ERROR_LEVEL • 4 = SUCCESS_LEVEL • 5 = FAILURE_LEVEL • 6 = AUDIT_FAILURE_LEVEL

Audit CEF Extension

```
static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc  file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
```

```
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-
fc12-149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server
version mismatch
```

Analysis Scores

The first entry in the audit CEF extension provides the four Malware Analysis scores for the event: Static, Network, Community, and Sandbox.

Log Information	Sample Value
static	100.0
network	29.0
community	8.0 A score of 0.0 can be a community score for the event or can indicate that no community services were enabled.
sandbox	N/R N/R means not run. This indicates that the GFI sandbox was not enabled.

File Information

The next three entries provide file information: file name, size, and hash.

Log Information	Sample Value
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

Event Meta Data Retrieved by NextGen

The record continues with the Core meta data for the event. The meta data in the message depends on the event. The amount of data in the message is truncated to the maximum length in bytes configured in the Syslog Settings. The default value is 1024.

Log Information	Sample Value
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149
client	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Private
time	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
action	get
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	rtf
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6
tcp.flags	27
ip.src	10.25.50.61

Log Information	Sample Value
tcp.dstport	80
threat.category	spectrum
eth.dst	00:0C:29:F8:50:2D
lifetime	0
alert.id	nw32535
sessionid	73
medium	1
size	117864
content	spectrum.consume11
extension	doc
directory	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
service	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
server	Apache/2.2.13 (Fedora)
streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	http client server version mismatch

Edit the Configuration File

1. Stop the Malware Analysis service.
2. Edit the configuration file as described in the Example.
3. Start the Malware Analysis service.
   The Malware Analysis service begins processing alerts through the configuration file and sending CEF alerts to designated services.

Example

The configuration file can be used to dictate which fields appear in the resulting alert as well as the label associated with each field and the order in which the data fields appear. The configuration file is composed of one or more XML `MalwareCefExtension` blocks as shown in the example below. The ordering of these blocks in the configuration file implies the order of the data fields in the CEF alert.

In the example below, the CEF alert would include two data fields, `ip.src` followed by `ip.dst`. The `customKey` is used to indicate the labeling of the data field in the alert. This allows the user to choose a custom label in order to force the alerting format to better match the expectations of the alert consumer. In other words, the format can be tuned to prevent unwanted changes to an existing alert parser. Lastly, the `isDisplay` setting determines if the field is included in the alert output. This allows the user to turn off data fields without having to physically delete the `MalwareCefExtension` block from the configuration.

```
<config>
<malwareExtensionList>
<com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>ip.src</customKey>
  <malwareKey>ip.src</malwareKey>
  <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>ip.dst</customKey>
  <malwareKey>ip.dst</malwareKey>
  <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
</malwareExtensionList>
</config>
```

At the end of the configuration file are three additional settings that can be used to further tune the alert format. They are as follows:

Setting	Description
includesUnknownMeta	This true or false setting indicates if unknown data elements are included in the resulting alert. Any NextGen session meta can be considered for inclusion into a CEF alert. Because additional session meta can be introduced via authoring new NextGen parsers, meta that is not contained in the default configuration may be encountered. You can set includesUnknownMeta to true to include the unknown meta in the alert and label it using the NextGen meta key name. To force a custom key for the unknown meta, you must edit this file and add a new MalwareCefExtension to the dictionary. To omit unknown meta from the alert, set includesUnknownMeta to false.
displayNulls	This true or false setting indicates if values that are set to null are included in the alert. If displayNulls is set to false, the null value fields are omitted even if their MalwareCefExtension isDisplay property is turned on. This allows dynamic formatting of alerts to exclude null fields.
valueIfNull	This true or false setting allows you to specify a string placeholder (n/a by default) to be used as the value for any null valued fields. If displayNulls is set to true, then null valued fields are included in the alerts. Their value is set to the value specified in valueIfNull.

The following represents the default CEF configuration file. The default configuration file includes all default NextGen session meta.

```
<config>
 <malwareExtensionList>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>static</customKey>
  <malwareKey>static</malwareKey>
  <isDisplay>true</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>nextgen</customKey>
<malwareKey>nextgen</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>community</customKey>
<malwareKey>community</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sandbox</customKey>
<malwareKey>sandbox</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.name</customKey>
<malwareKey>file.name</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.size</customKey>
<malwareKey>file.size</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
```

<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>

<malwareKey>country.dst.code</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>

<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcpport</customKey>
<malwareKey>tcp.srcpport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
<malwareKey>agency.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>

<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
<malwareKey>threat.category</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>lifetime</customKey>
<malwareKey>lifetime</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
<malwareKey>latdec.src</malwareKey>
<isDisplay>false</isDisplay>

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>size</customKey>
<malwareKey>size</malwareKey>
```

<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>

<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>

<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
<isDisplay>false</isDisplay>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filename</customKey>
<malwareKey>filename</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
<malwareKey>streams</malwareKey>
<isDisplay>false</isDisplay>

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
```

<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referer</customKey>
<malwareKey>referer</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>

```
  <malwareKey>risk.warning</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>attachment</customKey>
  <malwareKey>attachment</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>whois.registrar</customKey>
  <malwareKey>whois.registrar</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>whois.registrant</customKey>
  <malwareKey>whois.registrant</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>whois.date.creation</customKey>
  <malwareKey>whois.date.creation</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
  <com.netwitness.malware.core.cef.MalwareCefExtension>
  <customKey>whois.server</customKey>
  <malwareKey>whois.server</malwareKey>
  <isDisplay>false</isDisplay>
  </com.netwitness.malware.core.cef.MalwareCefExtension>
 </malwareExtensionList>
 <includesUnknownMeta>false</includesUnknownMeta>
 <displayNulls>false</displayNulls>
 <valueIfNull>n/a</valueIfNull>
</config>
```

Enable Custom YARA Content

This topic provides instructions for enabling custom YARA content on the NetWitness Suite host on which the Malware Analysis service is installed. In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language that allows malware researchers to identify and classify malware samples. RSA makes built-in YARA-based Indicators of Compromise (IOCs) available in RSA Live; these are automatically downloaded and activated on subscribed appliances.

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the appliance to consume. This section provides instructions for the Administrator who configures appliances to enable the creation of custom YARA content.

Prerequisites

This is an advanced configuration task, which requires sufficient privilege and knowledge to set up a GNU Compiler Collection (GCC) and C++ Python development library to build YARA. In addition, you must be thoroughly familiar with the standard YARA documentation. The following components are required:

- The Perl-Compatible Regular Expression (PCRE) library: pcre-8.33.tar.bz2
- The yara 1.7 (rev:167) stand-alone YARA command line: yara-1.7.tar
- The YARA extension for Python: yara-python-1.7.tar.gz
- YARA rules documentation: YARA User's Manual 1.6.pdf

The components are available for download here: https://code.google.com/p/yara-project/downloads/list

Note: As of writing, YARA 2.0 is available but not supported for Malware Analysis 10.5.

Install Libraries and Applications Required to Build YARA on a CentOs-Based Appliance

As a prerequisite to building YARA on a host that is running CentOS, you must install `make`, the GNU Compiler Collection, and C++ `Python` Development Library on the appliance. To install the applications and libraries required to build YARA:

1. To ensure the standard YUM repo and no other repo files are in the /etc/yum.repos.d folder, enter the following command:

   `ls -al /etc/yum.repos.d`

   The results should be similar to the following:

   ```
   -rw-r-r-. 1 root root 1926 Jun 26  2012 CentOS-Base.repo
   -rw-r-r-. 1 root root  637 Jun 26  2012 CentOS-Debuginfo.repo
   ```

```
-rw-r-r-. 1 root root  626 Jun 26  2012 CentOS-Media.repo
-rw-r-r-. 1 root root 2593 Jun 26  2012 CentOS-Vault.repo
```

2. To install `make` on the appliance, enter the following commands:

   a. **`yum search make`**
   The following message is returned: `make.x86_64 : A GNU tool which simplifies the build process for user`

   b. **`yum install make.x86_64`**

3. To install and test GCC on the host, enter the following commands:

   a. **`yum search gcc`**
   The following messages are displayed:
   `gcc-c+.x86_64 : C+ support for GCC`
   `gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)`

   b. Enter the following commands:
   `yum install gcc.x86_64`
   `yum install gcc-c++.x86_64`

   c. To test the gcc commands, enter the following commands:
   `gcc -v`
   `cc -v`

4. To install the C++ Python development library on the appliance, enter the following commands:

   a. **`yum search python dev`**
   The following message is returned:
   `python-devel.x86_64 : The libraries and header files needed for Python development`

   b. **`yum install python-devel.x86_64`**

Set Up Yara

To create a GCC and C++ Python development library in which you can build YARA on the NetWitness Suite host that is running Malware Analysis:

1. Do one of the following:

   a. If the host on which you are installing is running Mac OS, install xCode for Mac OS.

   b. If the host on which you are installing is running CentOS, install make, GCC and C++ Python development library using the YUM command line.

2. To Install the PCRE library on the host, open a terminal window and enter the following commands:

```
tar -xvf pcre-8.33.tar.bz2
cd pcre-8.33
./configure
make
sudo make install
```

3. To install the stand-alone YARA command line, enter the following commands:

```
tar -xvf yara-1.7.tar
cd yara-1.7
./configure
make
sudo make install
```

4. To test the stand-alone YARA command line:

   a. Enter the following command:

   ```
   yara
   ```

   b. If the command succeeds, continue with Step 7. If the command fails and returns the `yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory` error, enter the following command to check the `/etc/ld.so.conf` file or `LD_LIBRARY_PATH` environment variable.

   ```
   ldconfig -v
   ```

5. To install the YARA extension for Python, enter the following commands:

```
tar -xvf yara-python-1.7.tar.gz
cd yara-python-1.7
python setup.py build
sudo python setup.py install
```

6. To test the YARA extension:

   a. Enter the following command: **`python`**

   b. At the Python prompt (>>>), enter the following commands:

   ```
   import yara
   exit()
   ```

When this configuration is complete, analysts can create custom YARA IOCs for consumption on a Malware Analysis host as described in "Implement Custom YARA Content" in the *Investigation and Malware Analysis Guide*

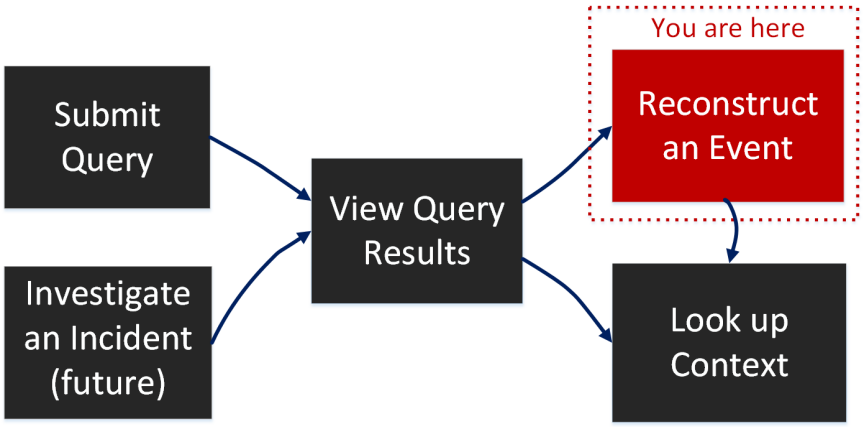
Malware Analysis References

- Services Config View - Auditing Tab
- Services Config View - AV Tab
- Services Config View - General Tab
- Services Config View - Hash Tab
- Services Config View - Indicators of Compromise Tab
- Services Config View - Integration Tab
- Services Config View - IOC Summary Tab
- Service Config View - Proxy Tab
- Services Config View - ThreatGRID Tab

Services Config View - Auditing Tab

In the Events view and the New Events view - Reconstruction panel (**Investigate > Events panel > click an event),** you can safely view a reconstruction of an event of interest that you found in the Navigate view or the Events panel.

Workflow



What do you want to do?

User Role	I want to ...	Documentation
Threat Hunter	submit query	Conducting an Investigation
Threat Hunter	view query results	Analyze Events in the Event Analysis View
Threat Hunter	reconstruct an event*	Reconstruct an Event
Threat Hunter	export files from an event	Reconstruct an Event
Threat Hunter	Look up additional context of an event	Looking up Contextual Information

Related Topics

- How NetWitness Investigate Works
- Conducting an Investigation
- Analyze Events in the Event Analysis View
- Navigate View
- Event Analysis View - Text Analysis Panel

Quick Look

The Investigate Reconstruction panel displays a reconstruction of a single event in Packet View, File View, and Text View. When you click an event in the Events panel, the adjacent Reconstruction panel shows the packet reconstruction of the event. You can use the options in the Event Reconstruction toolbar to change the reconstruction type and direction (request or response), to hide or display the header panel, and to expand, contract, and close the Event Reconstruction panel. Depending on the reconstruction type selected and the contents of the payload, additional options are available. For example, you can display the payload only in the Text View, download files in the Files View, and download PCAP files in the Packet View.

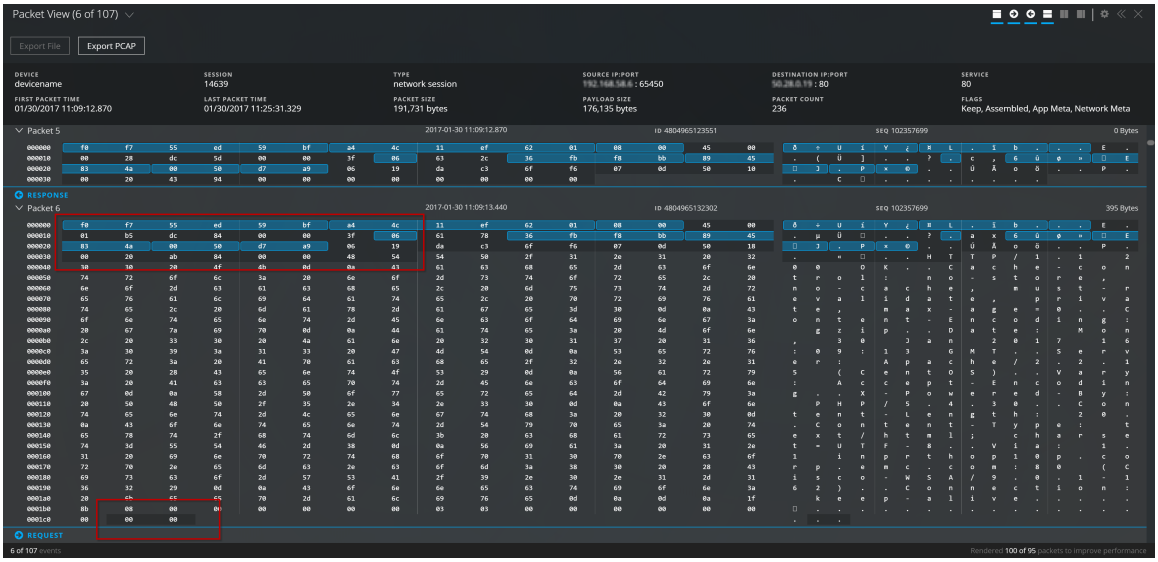
Below is an example of a packet Reconstruction.

1	Tabs or drop-down menu to select the reconstruction type: packet view, file view, text view. The currently selected type is displayed in the label.
2	Click to hide or show the header panel.
3	Click these icons to display the Request, Response, or both.
4	Click this icon to show or hide the Event Meta panel, which provides a detailed listing of meta data associated with the event..
5	An option to expand or contract the Reconstruction panel horizontally in the Navigate view.
6	An option to close the Reconstruction panel.
7	The header displays summary information for the event being reconstructed.
8	Lists each packet in the event. For each packet, you can see the packet number, the direction (Request or Response), and the packet contents in binary format on the left, hexadecimal format in the middle, and text format on the right.

Packet Reconstruction Details

In the packet reconstruction, Investigate provides the packet number, the direction of the packet (Request or Response), the packet start time, and then the contents of the packet.

All packets begin with a header, and some packets have a footer. In the Packet View, the header and footer have a darker background so that you can distinguish them from the payload of the packet. The darker background for the header and footer appears in both the hexadecimal and text format.



The contents of the packet are provided in hexadecimal, and text format. The meta data is highlighted in blue; when you hover over the meta data, the meta key/meta value information is displayed as a screen tip.

Additional options in the Packet View include the ability to Download the PCAP for the event, and display payloads only. When Payload only is displayed, you can use the Shade Bytes option to help distinguish patterns in the data.

Text Reconstruction Details

In the Text reconstruction, network events and log events are presented differently. For network events, Investigate provides the direction of the packet (Request or Response) and contents of each packet in text format.

For log events, (filter on Medium = Log), there is no request or response; only the raw log is displayed in the Text reconstruction.

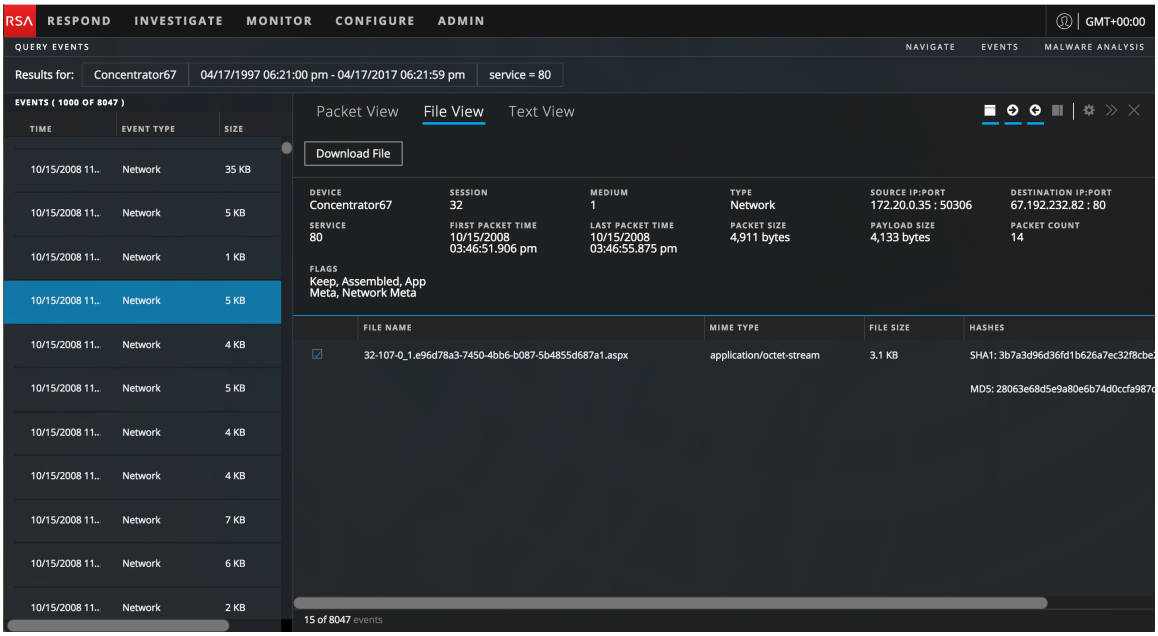
A subset of the reconstruction options is available in the Text View. You can:

- Hide and show the header.
- For Network events, select display of Requests only, Responses only, or both.
- For Network events, export the session as a PCAP file.
- For Log events, export the raw log.
- Switch between a compressed and decompressed view of payloads. When the session is decompressed, the compressed parts of the text become readable.
- Select text for decoding and encoding.

Note: This feature is not available for the File view, non-http network sessions, and log data.

File Reconstruction Details

In the File reconstruction, Investigate presents a list of files associated with the selected network event.



You can select one file, one or more files, or all files to export to your local file system. When files are selected, the Export Files button becomes active and reflects the number of files selected. Clicking the button exports the selected files as a zip archive, which ensures that any potentially malicious files will not be opened by the default application and executed. The exported archive is named using the following convention:

```
<service-ID or host name>_SID<nnnnnnnn>_FC<n>.zip
```

where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved
- `SID<nnnnnnnn>` is the session ID number
- `FC<nnnnnnnn>` is the file count or number of files in the archive.

To prevent an archive from being unzipped automatically when downloaded, NetWitness Suite exports the archive with password protection. To open an archive, enter the following password: **netwitness**.

Caution: Caution is advised when unzipping and opening files that are associated with a default application; for example, an Excel spreadsheet may automatically open in Excel before you have a chance to verify it is safe.

Detailed Description

Feature	Description
Reconstruction type menu	In this menu, you can select the type of reconstruction: **Packet** or **File**. When you first open a reconstruction, NetWitness Suite chooses the best reconstruction by default.
Download options	Options for exporting a log, a PCAP, or files for deeper analysis and to share with others.
	Controls the display of a header above the packet list; you can click this icon to hide the header or display it. Hiding the header allows more space for the packet list, reducing the amount of scrolling required to view more packets. The header provides information about the reconstructed event: the name of the service that collected the packet, session or event number, type of event (network), source IP:port, destination IP:port, sevice type, first packet time in the event, last packet time in the event, event size, payload size in bytes, packet count, and the flags applied to the event (keep, assembled, App meta, network meta).
	Two controls turn the display of Request and Response on and off (see Reconstruct an Event).
	Displays the meta details for the event in another panel.

Feature	Description
	(Future) Settings menu.
	Sizing controls for the Reconstruction panel (see Reconstruct an Event).
	Closes the Reconstruction panel. The view now shows only the Events panel and the Events panel.

Services Config View - AV Tab

This topic introduces the features and functions of the AV tab in the Service Config view for a Malware Analysis service. The AV tab provides a way to identify the anti-virus software vendors whose software is in use on your network. NetWitness Suite can include the results from these vendors in the detailed results view of an event that has been analyzed using Malware Analysis.

This is an example of the AV tab.

Features

The AV tab lists anti-virus vendors whose software may be installed in your network. There are two categories for vendors: Primary, which are the most trusted, and Secondary, which are less known. Each vendor name has a checkbox and an icon. Checking a vendor name indicates that you have installed the selected AV software from that vendor in your environment.

This table describes the options in the AV tab.

Feature	Description
Vendor Checkbox	Choose one or more AntiVirus vendors from the supplied list to indicate which products have been installed in the local organization.
Apply	Saves changes made in the AV tab.
Reset	Resets the AV list to the default state, which has no vendors selected.

Services Config View - General Tab

This topic introduces the configuration settings in the Service Config view > General tab for Malware Analysis, which has parameters specific to the Malware Analysis service. In this tab, you configure:

- The processing parameters for Core services that are capturing data.
- The repository for captured data.
- The static, community, and sandbox scoring categories used to analyze data.

The following task provides detailed procedures: Configure General Malware Analysis Settings.

This is an example of the General tab.

This tab has four sections: Continuous Scan Configuration, Repository Configuration, Miscellaneous, and Modules Configuration.

Continuous Scan Configuration Section

This table describes the features of the Continuous Scan Configuration section.

Parameter	Description
Enabled	Completely disable or enable continuous polling of the Core service. By default this is not selected (**disabled**).
Query	While the Decoder is analyzing network traffic, it creates a meta field called content with a value of **spectrum.consume** in sessions that are likely to contain malware. By default, Malware Analysis only performs analysis on events that have this particular meta value. By changing this query, Malware Analysis can be configured to analyze different types of events. Making this query too broad may force Malware Analysis to analyze too many events, causing it to fall behind or perform poorly. The default query is **select * where content='spectrum.consume'**

Parameter	Description
Query Expiry	When Malware Analysis queries the Core service for meta, it gets a result back within a few seconds. If there is a problem, such as a network connectivity issue, Malware Analysis abandons the query after this configured amount of time. The default value is **3600 seconds**.
Query Interval	How often, in minutes, to query for new session meta and files.
Meta Limit	Each time Malware Analysis queries the Core service, it pulls an amount of meta, up to this meta limit. Using this setting, in conjunction with the query interval, you can tune the performance of Malware Analysis in the Core infrastructure. The default value is **25000**.
Time Boundary	Malware Analysis analyzes sessions that occurred after the Time Boundary. This setting is most important when installing a new Malware Analysis appliance, because it determines how far back in time to begin analysis. Setting the boundary too many hours in the past may cause Malware Analysis to analyze too many past events, causing a large delay before you see any traffic happening in real time. The default value is **24 hours**.
Source Host	Hostname of the Malware Analysis appliance. This is the IP address, or the hostname, of the service that Malware Analysis queries to retrieve its data for analysis. Do not use localhost as the source host. Depending on the model of the appliance and the configuration of the NetWitness Suite infrastructure, this source host can vary.
Source Port	Malware Analysis communicates with the NetWitness Suite infrastructure using the REST service listening on this port. This port number is specific to the type of the Core service that is being used as the Source host. This corresponds to the outbound connections for your Core service.

Parameter	Description
Username	Username. The default value is **admin**. Malware Analysis must authenticate to the Source host each time it queries for data. In most cases, the account used by Malware Analysis is the same account used to access the Core service through NetWitness Suite. However, it is recommended to create a new account on the Core service dedicated to Malware Analysis.
User Password	User password. The default value is **netwitness**.
SSL	Use SSL when communicating with Core. If Malware Analysis is using an SSL connection to communicate with a Core service, check this option. The default value is unchecked.
Denial of Service (DOS) Prevention	The Denial of Service Prevention feature provides safeguards against malware that intentionally generates high volumes of network connections between two endpoints containing Windows PE content. Generating a high volume of connections artificially inflates the amount of traffic that security services monitoring the network must consume and analyze resulting in a denial of service. This feature helps identify these sessions so that you can have the analysis processing disregard them. The default value is unchecked.

Parameter	Description
DOS Session Rate Window Length (Seconds)	Malware Analysis uses this parameter with the **DOS Number Sessions per Rate Window** and **DOS Session Lockout Time (Seconds)** parameters to identify a Denial of Service Attack and determine how long to disregard sessions from a single IP address. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP address during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic from the IP address is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **60** seconds
DOS Number Sessions per Rate Window	Malware Analysis uses this parameter with the **DOS Session Rate Window Length (Seconds)** and **DOS Session Lockout Time (Seconds)** parameters to identify a Denial of Service Attack and determine how long to disregard sessions from the IP address. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP source during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **200** sessions

Parameter	Description
DOS Session Lockout Time (Seconds)	Malware Analysis uses this parameter with the **DOS Session Rate Window Length (Seconds)** and **DOS Number Sessions per Rate Window** parameters to identify a Denial of Service Attack and determine how long to disregard such an attack. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP address during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **60** seconds
DOS Garbage Collection Interval (Seconds)	Performs garbage collection on the internal memory structure used to track Denial of Service attempts. If memory usage is abnormally high, you can decrease this setting to free unused memory more often. If CPU usage is abnormally high, you can increase this setting to eliminate processing overhead (at the expense of memory usage). The default value is: **120** seconds

Repository Configuration Section

Malware Analysis stores all of the files that are analyzed for future use. These files can be downloaded through the user interface or accessed via one of the file sharing protocols.

This table describes the features of the Repository Configuration section.

Parameter	Description
Directory Path	All files are stored in the following directory on the Malware Analysis appliance: **/var/lib/netwitness/spectrum**

Parameter	Description
File Sharing Protocol	Possible values for the file sharing protocol are FTP, SAMBA, and None. You can enable FTP access and SAMBA file sharing to allow a user access to the stored files on the Malware Analysis from a remote location. No credentials are required to access these files. The port required for FTP access is TCP/21. The default file sharing protocol is **None**.
Retention (in days)	Malware Analysis maintains files stored in the repository for a specified number of days. You can set the number of days that files are retained before being deleted. The default value is **60** days.

Miscellaneous Configuration Section (10.3 SP2 and Later)

This table describes the features of the Miscellaneous Configuration section.

Parameter	Description
Maximum File Size	Limits the size of each file that you can scan for manually. This parameter applies to the feature described in "Upload Files for Malware Scanning" in the Investigation and Malware Analysis Configuration Guide. The default value is **64 MB**. If the file size limit is exceeded, prevents you from scanning the file.

Modules Configuration Section

The Modules Configuration section allows configuration of the static, community, and sandbox scoring categories.

Static Analysis Configuration

The static module is the only scoring category that is enabled by default. This table describes the parameters for configuring static analysis.

Feature	Description
Enabled	Completely disable or enable static analysis. By default this is selected (**enabled**).
Bypass PDF	Disable analysis of PDF documents. By default this is not selected; all PDF files undergo static analysis.
Bypass Office	Disable analysis of Office documents. By default this is not selected; all MS Office files undergo static analysis.
Bypass Executable	Disable analysis of Windows PE documents. By default this is not selected; all Windows PE files undergo static analysis.
Validate Windows PE Authenticate Settings via Cloud	Specify whether or not Windows PE files are sent to the RSA-Netwitness Cloud for Authenticode validation. The default value is selected. • When selected, any Windows PE file that is digitally signed is transmitted over the network (in its entirety) to the RSA-Netwitness Cloud for validation. If the intent is to prevent Windows PE files from leaving the customer network, you should disable this option. • When not selected, ALL static analysis is performed locally (skipping Authenticode validation). Regardless of this setting, PDF and M/S Office documents are not subject to Authenticode validation and are not transmitted over the network during static analysis.

Community Analysis Configuration

By default, the community module is disabled and the options are selected to prevent PDFs and MS Office documents from being processed. The intent is to default the settings to the most restrictive choices so that no sensitive documents leave the network unless the user chooses. This table describes the parameters for configuring Community analysis.

Feature	Description
Enabled	Completely disable or enable static analysis. By default this is not selected (**disabled**).

Feature	Description
Bypass PDF	Disable analysis of PDF documents. By default this is selected; PDF files are not processed.
Bypass Office	Disable analysis of Office documents. By default this is selected; Microsoft Office documents are not processed.
Bypass Executable	Disable analysis of Windows PE documents. By default this is selected; Windows PE documents are not processed

Sandbox Analysis Configuration

By default, the sandbox module is disabled and MS Office and PDF files are prevented from being processed. The intent is to set the most restrictive settings to force the user to specifically choose whether or not potentially sensitive information is sent outside of the network for processing. If the document type is not prevented from being processed, the file is sent to the destination sandbox server in its entirety (not limited to a hash of the file contents).

This table describes the parameters for configuring Sandbox analysis.

Feature	Description
Enabled	Completely disable or enable sandbox analysis. By default this is not selected **(disabled)**.
Bypass PDF	Disable analysis of PDF documents. By default this is selected; PDF files are not processed. When not selected, all PDF files are submitted in their entirety to the Sandbox for analysis.
Bypass Office	Disable analysis of Office documents. By default this is selected; Microsoft Office documents are not processed. When not selected, all MS Office files are submitted in their entirety to the Sandbox for analysis.

Feature	Description
Bypass Executable	Disable analysis of Windows PE documents. By default this is selected; Windows PE documents are not processed. When not selected, all Windows PE documents are submitted in their entirety to the Sandbox for analysis.
Preserve Original File Name when Performing Sandbox Analysis	In 10.3 SP2 and later, enable the ability to hash for filenames when they are sent to a local sandbox. By default this is not selected. **Note:** If you do not select this parameter, NetWitness Suite hashes the files.

GFI Sandbox Settings

In the GFI Sandbox section, you can enable sandbox processing by GFI and configure the locally installed GFI sandbox. The table describes the parameters for configuring the GFI sandbox.

Feature	Description
Enabled	When enabled, sandbox processing is performed by a local copy of GFI. The default value is **disabled**. If you enable GFI, you need to configure the remaining parameters.
Server Name	The GFI Sandbox server name. No default value.
Server Port	The GFI Sandbox server port. Default value is **80**.
Max Poll Period	Determines how long to wait for a submitted sample to finish processing. Default value is **600 seconds**.
Ignore Web Proxy Settings	Tells Malware Analysis to bypass the web proxy, if a web proxy is configured, when making this connection. If no web proxy has been configured in Malware Analysis, the setting is ignored.

ThreatGrid Sandbox Settings

In the ThreatGrid Sandbox section, you can enable sandbox processing by ThreatGrid and choose whether to use the locally installed ThreatGrid or the ThreatGrid Cloud for sandbox analysis.

- If you have a local copy of ThreatGrid, configure sandbox processing to use the local copy.
- If no local instance of ThreatGrid has been purchased and installed, configure the ThreatGrid Cloud.

The table describes the parameters for configuring the ThreatGrid sandbox.

Note: Before enabling this service, you must configure a ThreatGrid-supplied Service Key. The service key allows ThreatGrid to recognize that samples submitted from this site are legitimate.

Feature	Description
Enabled	When enabled, sandbox processing is performed by ThreatGrid, either a local copy or the ThreatGrid Cloud. The default value is **disabled**.
Service Key	Before enabling the sandbox module, a ThreatGrid-supplied Service Key must be configured. The service key allows ThreatGrid to recognize that samples submitted from this site are legitimate.
URL	The URL for the ThreatGrid server to be used (if you are not using a locally installed ThreatGrid). The ThreatGrid Cloud is reachable via https://panacea.threatgrid.com
Ignore Web Proxy Settings	Tells Malware Analysis to bypass the web proxy, if a web proxy is configured, when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.

Services Config View - Hash Tab

This topic introduces the features and functions available in the Service Config view > Hash tab for Malware Analysis.

In this tab, you can manage hash filtering in Malware Analysis. The hash grid is initially empty; the grid lists filters that have been added to Malware Analysis. In this view, you can add a hash filter, delete a hash filter, mark a hash filter as trusted or untrusted, and save changes.

This is an example of the Hash tab.

This is an example of the Add Hash dialog.

Features

The **Hash** tab consists of a toolbar and a pageable hash grid.

This table describes the Hash tab toolbar.

Feature	Description
MD5 Search	Enter an MD5 hash for which you want to search the results in the grid. The search function is case-insensitive.
Add	Displays the Add Hash dialog in which you can add a new hash to the hash grid, specify whether the hash is trusted or not, and provide the hash file size.
Save Edit	Saves any additions or edits to hashes in the grid.
Delete	Deletes selected hashes from the grid.

This table describes the Hash grid columns.

Feature	Description
Select Checkbox	Click to select a row. Click in the column header to select a header.
Trusted	Marks a hash as trusted or untrusted.
MD5	Identifies the MD5 hash.

Feature	Description
File Size	Identifies the hash file size in kilobytes.

Services Config View - Indicators of Compromise Tab

This topic introduces the features and functions available in the Service Config view > Indicators of Compromise tab, which applies to the Malware Analysis service. This tab provides a way to configure the way each of the four scoring modules uses the available rules to score data.

This is an example of the Indicators of Compromise tab.

Features

The Indicators of Compromise tab consists of a toolbar and pageable grid.

This table describes the features of the grid.

Feature	Description
Module selection list	Selects the scoring module for which you want to view the Indicators of Compromise: All, Network, Static, Community, Sandbox, or Yara.
Search field	Type text for which you are searching in the Description field.
Search option	Filters the grid to display only Descriptions that match the Description search term.
Enable All option	Click to enable all rules for the scoring module, as opposed to enabling all rules on the page using the checkbox.
Enable option	Click to enable selected rules.
Disable All option	Click to disable all rules for the scoring module, as opposed to disabling all rules on the page using the checkbox.

Feature	Description
Disable option	Click to disable selected rules.
Reset All option	Click to reset all rows on the page to their default values.
Reset option	Click to reset selected rows to their default values.
Save option	Click to save changes you made on this page. If you leave the page without saving, the changes are lost. The description of each row with unsaved changes has a red corner.

This table describes the features of the toolbar.

Column	Description
Selection checkbox	Checkboxes for selecting individual rows or all rows on the page.
Enabled checkbox	If the indicator of compromise is enabled, Malware Analysis uses the rule for scoring session data.
High Confidence checkbox	If checked, Malware Analysis treats the rule as one very likely to indicate the presence of malware, and an event that triggers that rule is marked in the results grid.
Description	Describes the Indicator of Compromise.
Score	Specifies the score that you want to factor in to the total score for any event that triggers the rule. The default score is displayed and you can raise or lower the score by dragging the slider or typing a number in the score box.
File Type	Displays the file types to which the rule applies. Possible values are **ALL**, **PDF**, **MS Office**, and **Windows PE**.

Services Config View - Integration Tab

This topic introduces the features and functions of the Integration tab in the Administration Services Config view for Malware analysis. This tab provides a way to test connections and enable Community scoring by registering the Malware Analysis service. An administrator can test the connection to cloud.netwitness.com and to a core service that was configured for continuous scan.

The following figure is an example of the Integration tab.

Features

This tab has two sections: RSA Cloud Connection Test and Registration and Continuous Scan Connection Test. The following table describes the features.

Feature	Description
RSA Cloud Connection Test and Registration button	Clicking this button tests for an active connection to cloud.netwitness.com. NetWitness Suite tests communications with the site and checks Proxy settings. A valid connection is required in order to register with the RSA Community Service.
Company Name	This is the name of your company. This is a required field.
Contact Email	This is the contact email. This is a required field.
Internal EMC Use Only Check box	This is an optional field. EMC customers, salespersons, or demo users should check this option to ensure that their requests do not use bandwidth on the production server. When the box is checked the following warning is displayed: `Checking this box may cause a less robust performance because the production server isn't being used.`
Register button	Clicking the Register button completes registration if all required fields are filled in. The Register button becomes the Update button after registration is complete.

Feature	Description
Update button	The Update button is displayed after registration is complete.
Continuous Scan Connection Test button	Clicking this button initiates a check to verify that the Malware Analysis service can connect to the Core service selected for continuous scanning (the Source Host, Source Port, Username, and User Password as specified in the General tab).

Services Config View - IOC Summary Tab

This topic introduces the features and functions available in the Service Config view > IOC Summary tab. This tab provides a way to view summary information for any IOC. A grid for each scoring module lists the configured IOCs along with statistics associated with that IOC of a specific range of time. The statistics include:

- The number of events for a network session or the number of files for a static, community, or sandbox event that were flagged with the IOC.
- The current score configured for the IOC in the Indicators of Compromise tab.
- The scores returned by each of the scoring modules.

When you select an event, you can show the Malware Events view or Malware Files view for the IOC. You can also open the selected IOC in the Indicators of Compromise tab to edit the Current Score.

This is an example of the IOC Summary tab for the Network scoring module.

Features

The IOC Summary consists of four tabs, one for each scoring module: Network, Static, Community, and Sandbox. Each tab has the same form and same information with a toolbar and pageable grid.

This table describes the features of each tab.

Feature	Description
Time Range	Selects the time range for the IOC Summary. Possible values are: Last 5 Minutes, Last 15 Minutes, Last 30 Minutes, Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 5 Days, Early Morning, Morning, Afternoon, Evening, All Day, Yesterday, This Week, Last Week, or Custom.
Description column	Lists the descriptions for the IOCs.

Feature	Description
Count column	Lists the number of occurrences of the IOCs. In the Network tab, the count is the number of events in which the IOC was found. In the other tabs, the count is the number of files in which the IOC was found.
Current Score column	Lists the current score for the IOCs as configured in the Indicators of Compromise tab.
Static, Network, Community, and Sandbox columns	List the scores that each of the scoring modules gave the IOCs.
Actions drop-down	The Actions drop-down menu has two options: Show Events/Files and Edit. Show Events opens the IOC in the Investigation Events view or Files view. This view can also be opened by double-clicking on the IOC. Edit opens the IOC in the Indicators of Compromise tab to edit the Current Score.

Service Config View - Proxy Tab

This topic introduces the parameters configured in the Proxy tab in the Service Config view for a Malware Analysis service. This tab configures Malware Analysis communication via web proxy with the RSA Cloud for community analysis and with the sandbox service for sandbox analysis to preserve anonymity. If you are using a local sandbox service, communications via web proxy are unnecessary and may slow performance. When configuring the sandbox module in the **General** tab, you can choose to bypass the configured web proxy.

This is an example of the Proxy tab.

Features

This table describes the features in the Proxy tab.

Feature	Description
Enabled	Select the checkbox to enable communication via web proxy with the RSA Cloud for community analysis and with the sandbox service for sandbox analysis to preserve anonymity.
Automatically detect web proxy settings	Select the checkbox to use settings configured in the System settings.
Proxy host	Enter the hostname for the proxy host.
Proxy port	Enter the port used for communication on the proxy host
Users	Enter the username used to log on to the proxy host.
User Password	Enter the user password used to log on to the proxy host.
SSL	(Optional) Select the checkbox to enable communication using SSL.
Apply button	Click the **Apply** button to submit chosen settings.

Services Config View - ThreatGRID Tab

This topic introduces the parameters required to obtain a trial ThreatGrid API key in the Malware Analysis **ThreatGRID** tab, which provides a method of obtaining a trial ThreatGrid API key for use in the ThreatGrid Cloud sandbox. Before enabling ThreatGrid as the sandbox service in the Sandbox module, a ThreatGrid-supplied Service Key must be configured so that ThreatGrid can recognize that samples submitted from this site are legitimate.

If you do not have a ThreatGrid-supplied Service Key, you can obtain a key using this tab. The key is provided on a trial basis.

This is an example of the ThreatGRID tab.

Features

This table describes the features of the **ThreatGRID** tab.

Feature	Description
Full Name	Your first and last name.
Title	Your job title.
Organization Name	The name of your organization.
Email	Your email address.
User Id	Your user ID for ThreatGrid access.
Password	Your password for ThreatGrid access.
Register button	Click the **Register** button to submit the request.

RSA NETWITNESS® SUITE

NetWitness Respond Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

About this Document **5**

NetWitness Respond Configuration Overview 5

Configuring NetWitness Respond **7**

Step 1. Configure Alert Sources to Display Alerts in Respond View 8

Prerequisites 8

Configure Reporting Engine to Display Alerts Triggered by Reporting Engine in Respond View 8

Configure Malware Analytics to View Alerts Triggered by Malware Analytics in Respond view 8

Configure NetWitness Endpoint to View Alerts Triggered by NetWitness Endpoint in Respond View 9

Configure NetWitness Endpoint to Display NetWitness Endpoint Alerts 9

Step 2. Assign Respond View Permissions 12

Respond-server 13

Incidents 14

Integration-server 15

Respond Role Permission Examples 16

Step 3. Enable and Create Incident Rules for Alerts 17

Enable an Incident Rule 17

Create an Incident Rule 19

Verify the Order of your Incident Rules 22

Clone an Incident Rule 22

Edit an Incident Rule 22

Additional Procedures for Respond Configuration **24**

Set Up and Verify Default Incident Rules 25

Set up the User Behavior Incident Rule 25

Set up or Verify a Default Incident Rule 32

Configure Respond Email Notification Settings 42

Set a Retention Period for Alerts and Incidents 44

Prerequisites 44

Procedure 44

Result 45
Obfuscate Private Data 46
Prerequisites 46
Procedure 46
Manage Incidents in NetWitness SecOps Manager 48
Prerequisites 48
Procedure 48
Set Counter for Matched Alerts and Incidents 50
Configure a Database for the Respond Server Service 52
Prerequisites 52
Procedure 52
NetWitness Respond Configuration Reference 55
Configure View 55
Incident Rules List View 56
What do you want to do? 56
Related Topics 56
Incident Rules List View 56
Incident Rule Details View 59
What do you want to do? 59
Related Topics 59
Incident Rule Details View 59
Group By Meta Key Mappings 64
Respond Notification Settings View 66
What do you want to do? 66
Related Topics 66
Respond Notification Settings 66
Aggregation Rules Tab 69
What do you want to do? 69
Related Topics 69
Aggregation Rules 69
New Rule Tab 72
What do you want to do? 72
Related Topics 72
New Rule 72

About this Document

This guide provides an overview of NetWitness Respond, detailed instructions on how to configure NetWitness Respond in your network, additional procedures that are used at other times, and reference materials that describe the user interface for configuring NetWitness Respond in your network.

Topics

- NetWitness Respond Configuration Overview
- Configuring NetWitness Respond
- Additional Procedures for Respond Configuration
- NetWitness Respond Configuration Reference

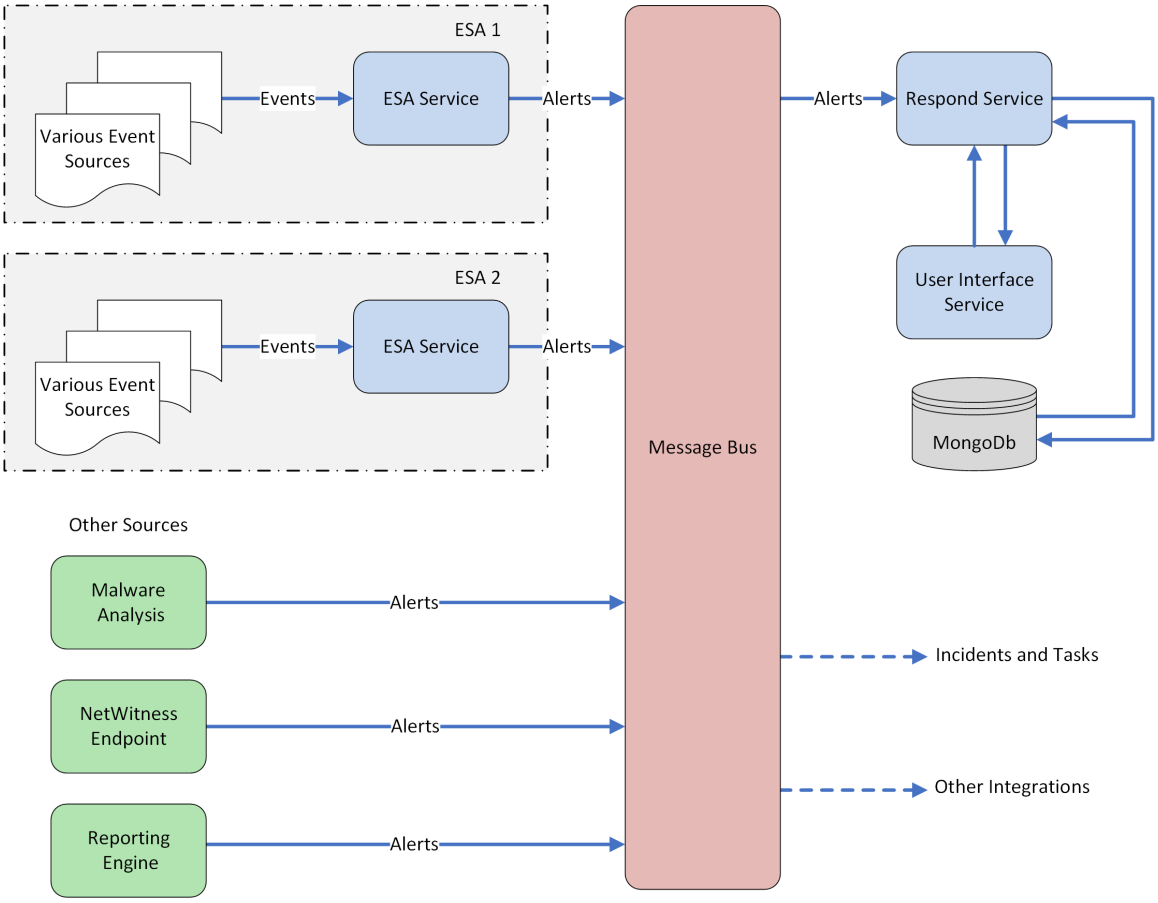
NetWitness Respond Configuration Overview

RSA NetWitness® Suite NetWitness Respond consumes Alert data from various sources via the Message Bus and displays these alerts on the NetWitness Suite user interface. The Respond Server service allows you to group the alerts logically and start a NetWitness Respond workflow to investigate and remediate the security issues raised.

The Respond Server service consumes alerts from the message bus and normalizes the data to a common format (while retaining the original data) to enable simpler rule processing. It periodically runs rules to aggregate multiple alerts into an incident and set some attributes of the Incident (for example, severity, category, and so on). The incidents are persisted into MongoDb by the Respond Server service. Incidents are also posted onto the message bus for consumption by other systems (for example, Archer integration).

Note: NetWitness Respond requires an ESA primary server that contains the MongoDb. Alerts, Incidents, and Task records are persisted into this MongoDb by the Respond Server.

The following diagram illustrates the high level flow of alerts.



You have to configure various sources from which the alerts are collected and aggregated by the Respond Server service.

Configuring NetWitness Respond

This topic provides the high-level tasks required to configure the Respond Server service. The administrator needs to complete the steps in the sequence provided.

Topics

- Step 1. Configure Alert Sources to Display Alerts in Respond View
- Step 2. Assign Respond View Permissions
- Step 3. Enable and Create Incident Rules for Alerts

Step 1. Configure Alert Sources to Display Alerts in Respond View

This procedure is required so that alerts from the alert sources are displayed in NetWitness Respond. You have an option to enable or disable the alerts being populated in the Respond view. By default this option is disabled in the Reporting Engine, Malware Analytics, and NetWitness Endpoint and enabled only in Event Stream Analysis. So when you install the Respond Server service you need to enable this option in the Reporting Engine, Malware Analytics, and NetWitness Endpoint to populate the corresponding alerts in the Respond view.

Prerequisites

Ensure that:

- The Respond Server service is installed and running on NetWitness Suite.
- A database is configured for the Respond Server service.
- NetWitness Endpoint is installed and running.

Configure Reporting Engine to Display Alerts Triggered by Reporting Engine in Respond View

The Reporting Engine alerts are by default disabled from being displayed in Respond view. To display and view the Reporting Engine alerts, you have to enable the NetWitness Respond alerts in the Services Config view > General tab for the Reporting Engine.

1. Go to **ADMIN > Services,** select a Reporting Engine service, and then select **> View > Config**.
   The Services Config view is displayed with the Reporting Engine General tab open.
2. Select **System Configuration**.
3. Select the checkbox for **Forward Alerts to Respond**.
   The Reporting Engine now forwards the alerts to NetWitness Respond.

For details on parameters in the General tab, see the "Reporting Engine General Tab" topic in the *Reporting Engine Configuration Guide*.

Configure Malware Analytics to View Alerts Triggered by Malware Analytics in Respond view

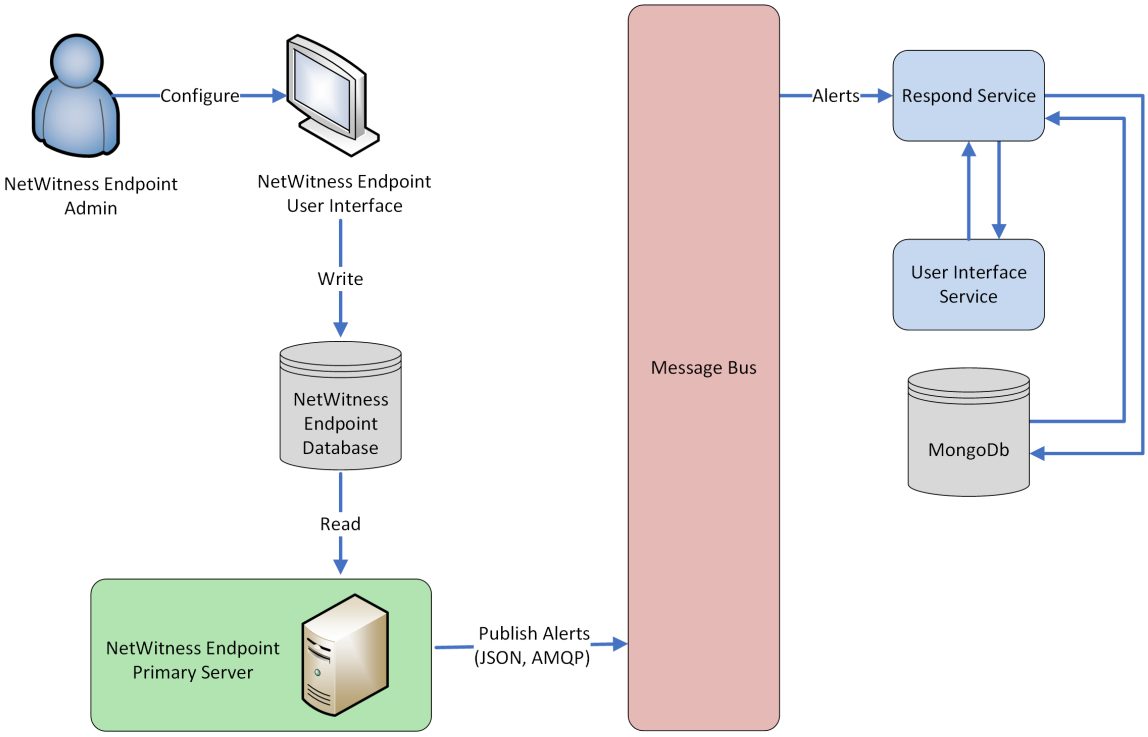
Viewing NetWitness Respond alerts is a function of auditing in Malware Analysis. The procedure of enabling NetWitness Respond alerts is described in the "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Analysis Configuration Guide*.

Configure NetWitness Endpoint to View Alerts Triggered by NetWitness Endpoint in Respond View

This procedure is required to integrate NetWitness Endpoint with NetWitness Suite so that the NetWitness Endpoint alerts are picked up by the NetWitness Respond component of NetWitness Suite and displayed in the **RESPOND > Alerts** view.

Note: RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, or later for NetWitness Respond integration. For more detailed information, see the "RSA NetWitness Suite Integration" topic in the *NetWitness Endpoint User Guide*.

The diagram below represents the flow of NetWitness Endpoint alerts to the NetWitness Suite Respond Server service and its display in the **RESPOND > Alerts** view.

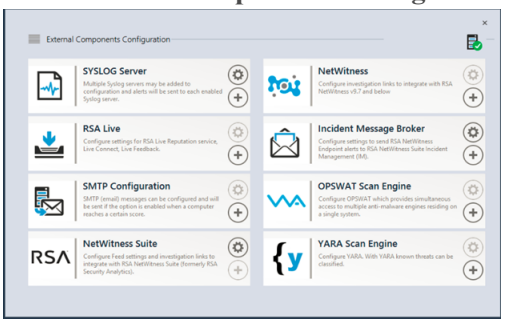


Configure NetWitness Endpoint to Display NetWitness Endpoint Alerts

To configure NetWitness Endpoint to display NetWitness Endpoint alerts in the NetWitness Suite user interface:

1. In the NetWitness Endpoint user interface, click **Configure > Monitoring and External Components**.

The **External Components Configuration** dialog is displayed.



2. From the components listed, select **Incident Message Broker** and click + to add a new IM broker.
3. Enter the following fields:
   a. **Instance Name**: Enter a unique name to identify the IM broker.
   b. **Server Hostname/IP address**: Enter the Host DNS or IP address of the IM broker (NetWitness Server).
   c. **Port number**: The default port is 5671.
4. Click **Save**.
5. Navigate to the **ConsoleServer.exe.Config** file in **C:\Program Files\RSA\ECAT\Server**.
6. Modify the virtual host configurations in the file as follows:
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite 11.0, the virtual host is "/rsa/system". For version 10.6.x and below, the virtual host is "/rsa/sa".
7. Restart the API Server and Console Server.
8. To set up SSL for Respond Alerts, perform the following steps on the NetWitness Endpoint primary console server to set the SSL communications:
   a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key).
   b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You MUST set the CN name to ecat.)

      ```
      makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
      sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NWECA" -is MY -ir
      LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
      cy end -sy 12 client.cer
      ```

> **Note:** In the above code sample, if you upgraded to Endpoint version 4.3 from a previous version and did not generate new certificates, you should substitute "EcatCA" for "NWECA".

c. Make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the IMBrokerClientCertificateThumbprint section of the ConsoleServer.Exe.Config file as shown.

```
<add key="IMBrokerClientCertificateThumbprint"
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```

9. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:
`/etc/pki/nw/trust/import`

10. Issue the following command to initiate the necessary Chef run:
`orchestration-cli-client --update-admin-node`
This appends all of those certificates into the truststore.

11. Restart the RabbitMQ server:
`systemctl restart rabbitmq-server`
The NetWitness Endpoint account should automatically be available on RabbitMQ.

12. Import the **/etc/pki/nw/ca/nwca-cert.pem** and **/etc/pki/nw/ca/ssca-cert.pem** files from the NetWitness Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Step 2. Assign Respond View Permissions

Add users with the required permissions to investigate incidents and alerts in NetWitness Respond. Users with access to the Respond view need both Incidents and Respond-server permissions. Users with access to configure Respond notification settings need additional Integration-server permissions.

The following pre-configured roles have permissions in the Respond view:

- **Analysts**: The Security Operations Center (SOC) Analysts have access to Alerting, NetWitness Respond, Investigation, and Reporting, but not system configurations.
- **Malware Analysts**: Malware Analysts have access to investigations and malware events.
- **Operators**: Operators have access to configurations, but not Investigation, ESA, Alerting, Reporting and NetWitness Respond.
- **SOC_Managers**: The SOC Managers have the same access as Analysts plus additional permissions to handle incidents and configure NetWitness Respond.
- **Data_Privacy_Officers**: Data Privacy Officers (DPOs) are like Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system. See *Data Privacy Management* for additional information.
- **Respond_Administrator**: The Respond Administrator has full access to NetWitness Respond.
- **Administrators**: the Administrator has full system access to NetWitness Suite and has all permissions by default.

The NetWitness Respond default permissions are shown in the following tables. You need to assign user permissions from both the **Incidents** and **Respond-server** tabs, which are the Permissions tab names in the ADMIN > Security view Add or Edit Roles dialogs. You may want to add additional user permissions for Alerting, Context Hub, Investigate, Investigate-server, and Reports.

Caution: It is very important that you assign equivalent user permissions from BOTH the Respond-server tab AND the Incidents tab.

Users who configure Respond notification settings also need permissions in the Integration-server tab.

Respond-server

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
respond-server.alert.delete			Yes*	Yes*		
respond-server.alert.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.alert.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.alertrule.manage		Yes	Yes*	Yes*		
respond-server.alertrule.read		Yes	Yes*	Yes*		
respond-server.configuration.manage			Yes*	Yes*		
respond-server.health.read			Yes*	Yes*		
respond-server.incident.delete			Yes*	Yes*		
respond-server.incident.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.incident.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.journal.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.journal.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.logs.manage			Yes*	Yes*		
respond-server.metrics.read			Yes*	Yes*		
respond-server.notification.manage (Available in 11.1 and later)		Yes	Yes*	Yes*		

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
respond-server.notification.read (Available in 11.1 and later)		Yes	Yes*	Yes*		
respond-server.process.manage			Yes*	Yes*		
respond-server.remediation.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.remediation.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.security.manage			Yes*	Yes*		
respond-server.security.read			Yes*	Yes*		

* Data Privacy Officers and Respond Administrators have the **respond-server.*** permission, which gives them all of the Respond-server permissions.

Incidents

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
Access Incident Module	Yes	Yes	Yes	Yes		Yes
Configure Incident Management Integration		Yes	Yes	Yes		
Delete Alerts and Incidents			Yes	Yes		
Manage Alert Handling Rules		Yes	Yes	Yes		
View and Manage Incidents	Yes	Yes	Yes	Yes		Yes

The Respond Administrator has all of the Respond-server and Incidents permissions.

Integration-server

(The Integration-server permissions are available in NetWitness Suite version 11.1 and later.) Users who configure Respond Notifications also need Integration-server permissions. The following table lists the Respond Notification setting permissions in the Integration-server tab assigned to each role.

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
integration-server.notification.read		Yes	Yes	Yes		
integration-server.notification.manage		Yes	Yes	Yes		

Respond Notification Settings Permissions

(The Respond notification setting permissions are available in NetWitness Suite version 11.1 and later.)

Note: If you are updating from NetWitness Suite version 11.0 to 11.1, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. For all upgrades to 11.1, you will need to add additional permissions to custom roles.

The following permissions are required for Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (CONFIGURE > Respond Notifications).

Incidents tab:

- Configure Incident Management Integration

Respond-server tab:

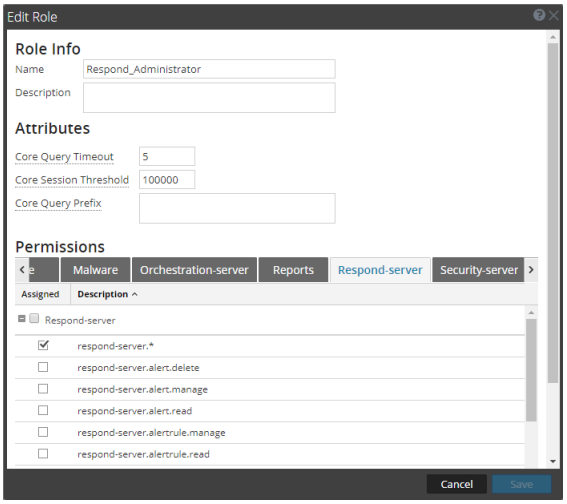
- respond-server.notification.manage
- respond-server.notification.read

Integration-server tab:

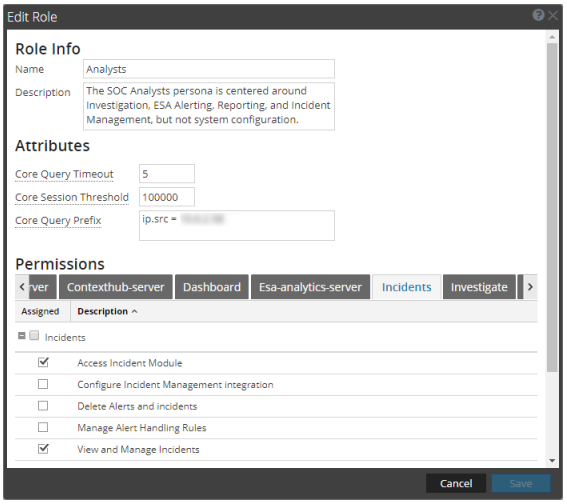
- integration-server.notification.read
- integration-server.notification.manage

Respond Role Permission Examples

The following figure shows Respond-server permissions for the default Respond Administrator role. The Respond Administrator role contains all of the NetWitness Respond permissions.



The following figure shows the Incidents permissions for the default Analysts role:



For more information, see "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management* guide.

Step 3. Enable and Create Incident Rules for Alerts

NetWitness Respond incident rules contain various criteria to automate the process of creating incidents from alerts. Alerts that meet the rule criteria are grouped together to form an incident. Analysts use these incidents to locate indicators of compromise. Instead of creating an incident for a particular set of alerts and adding the alerts to that incident manually, you can save time by using incident rules to create incidents from alerts for you.

NetWitness Suite provides predefined incident rules that you can use and you can also create your own rules based on your business requirements.

To create incidents automatically, you need to enable at least one incident rule.

When you have two or more incident rules enabled, the order of the rules becomes very important. The highest priority rules are at the top of the Incident Rules List. The highest priority rule has the number 1 in the Order field. The next highest priority rule is number 2 in the Order field, and so on. Alerts can only be part of one incident. If an alert matches more than one rule in the Incident Rule list, it is only evaluated using the highest priority rule that it matches.

NetWitness Suite has 12 predefined incident rules that you can use. To set up your incident rules, you can do any of the following:

- Enable predefined incident rules
- Add new rules
- Clone rules
- Edit \existing rules

The User Behavior default incident rule is available in NetWtitness Suite 11.1 and later. It captures network user behavior and uses deployed RSA Live ESA Rules to create incidents from alerts. You can select and deploy the RSA Live ESA Rules that you want to monitor. For more information, see Deploy the RSA Live ESA Rules.

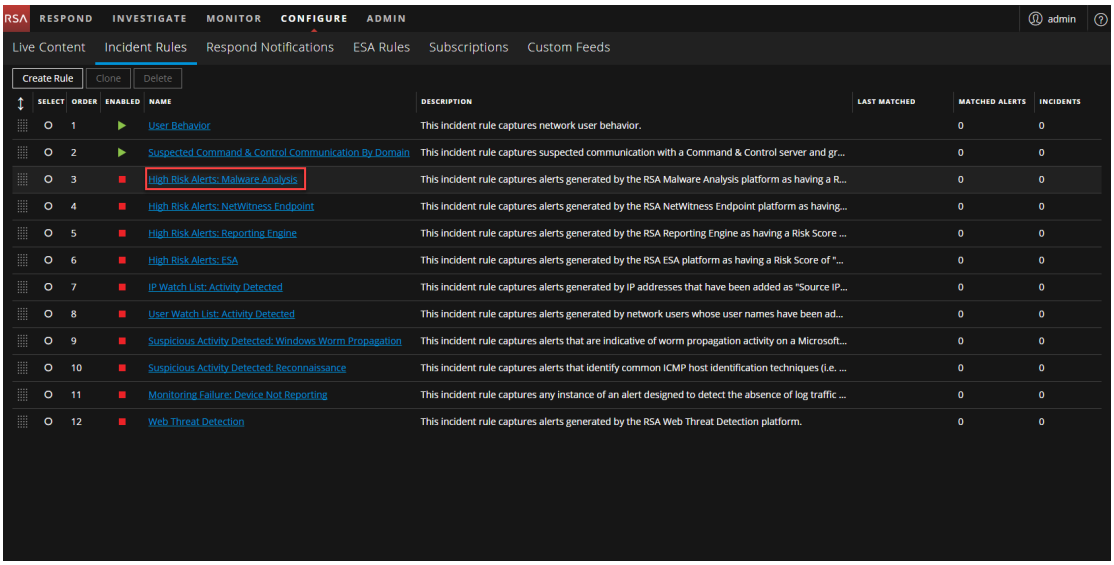
Some predefined (default) incident rules changed slightly in 11.1. To verify your existing default incident rules with the 11.1 default incident rules, see Set Up and Verify Default Incident Rules.

Enable an Incident Rule

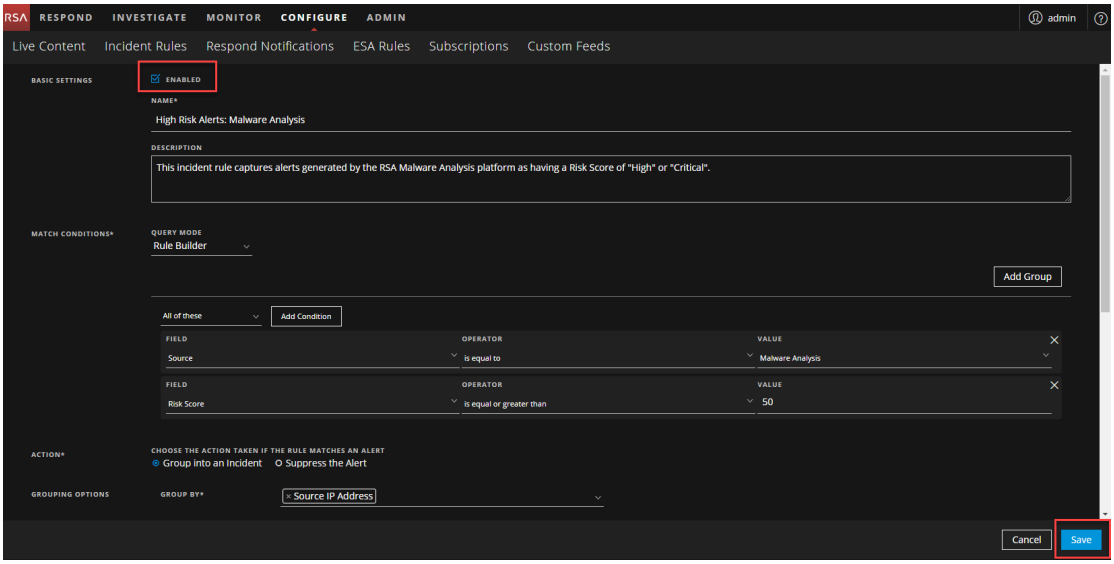
To create incidents automatically, you need to enable at least one incident rule. Predefined (default) incident rules or rules that you create must be enabled before they start creating incidents.

1. Go to **CONFIGURE > Incident Rules**.

   The Incident Rules List view is displayed. The example below shows the 12 default incident rules.

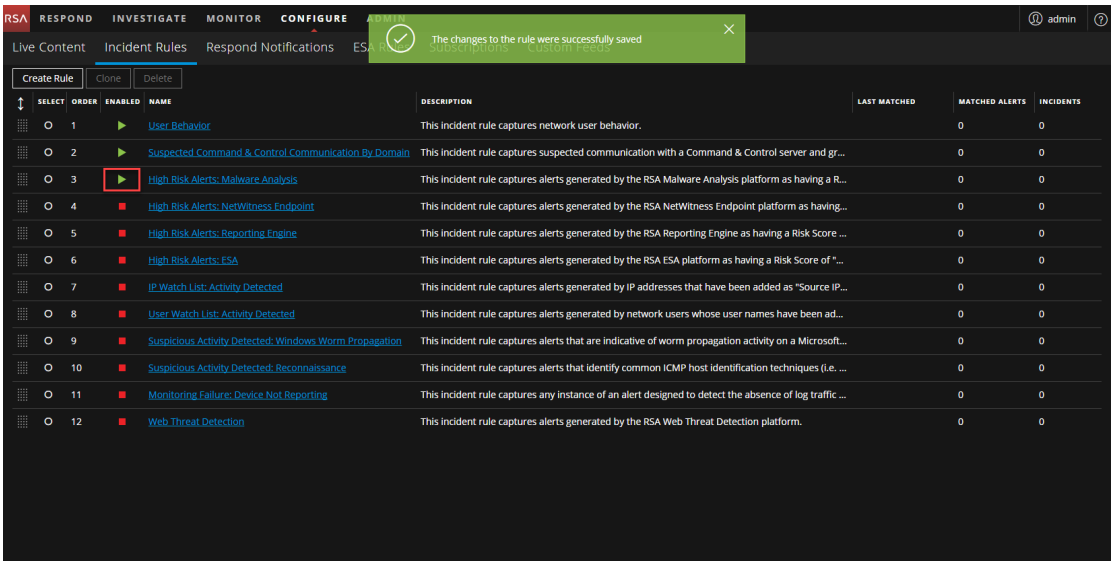


2. Click the link in the **Name** column for the rule that you want to enable.
   The Incident Rule Details view is displayed for the selected rule.



3. Adjust the parameters and conditions of your rule as required. For details about various parameters that can be set as criteria for an incident rule, see Incident Rule Details View.
4. In the Basic Settings section, select **Enabled**.

5. Click **Save** to enable the rule.
   Notice that the Enabled column changes from a red square ■ (Disabled) to green triangle ▶ (Enabled).

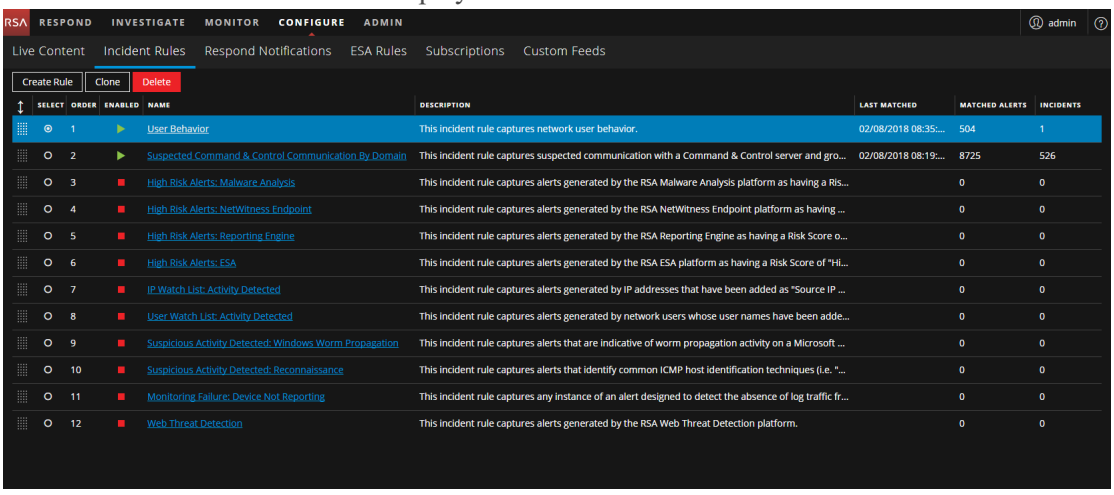


6. Verify the order of your incident rules.

Create an Incident Rule

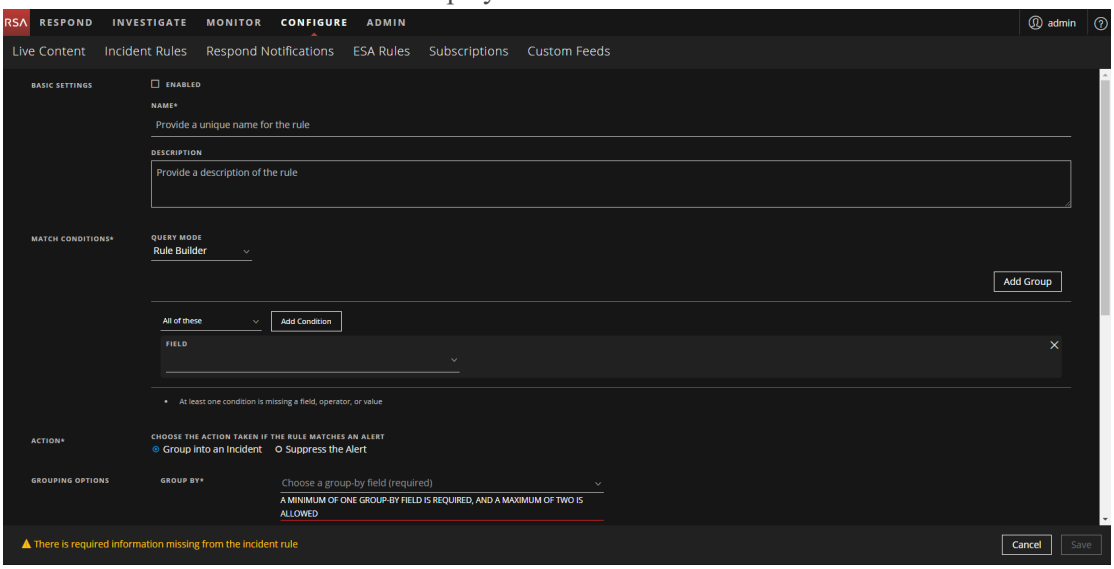
1. Go to **CONFIGURE > Incident Rules**.

   The Incident Rules List view is displayed.



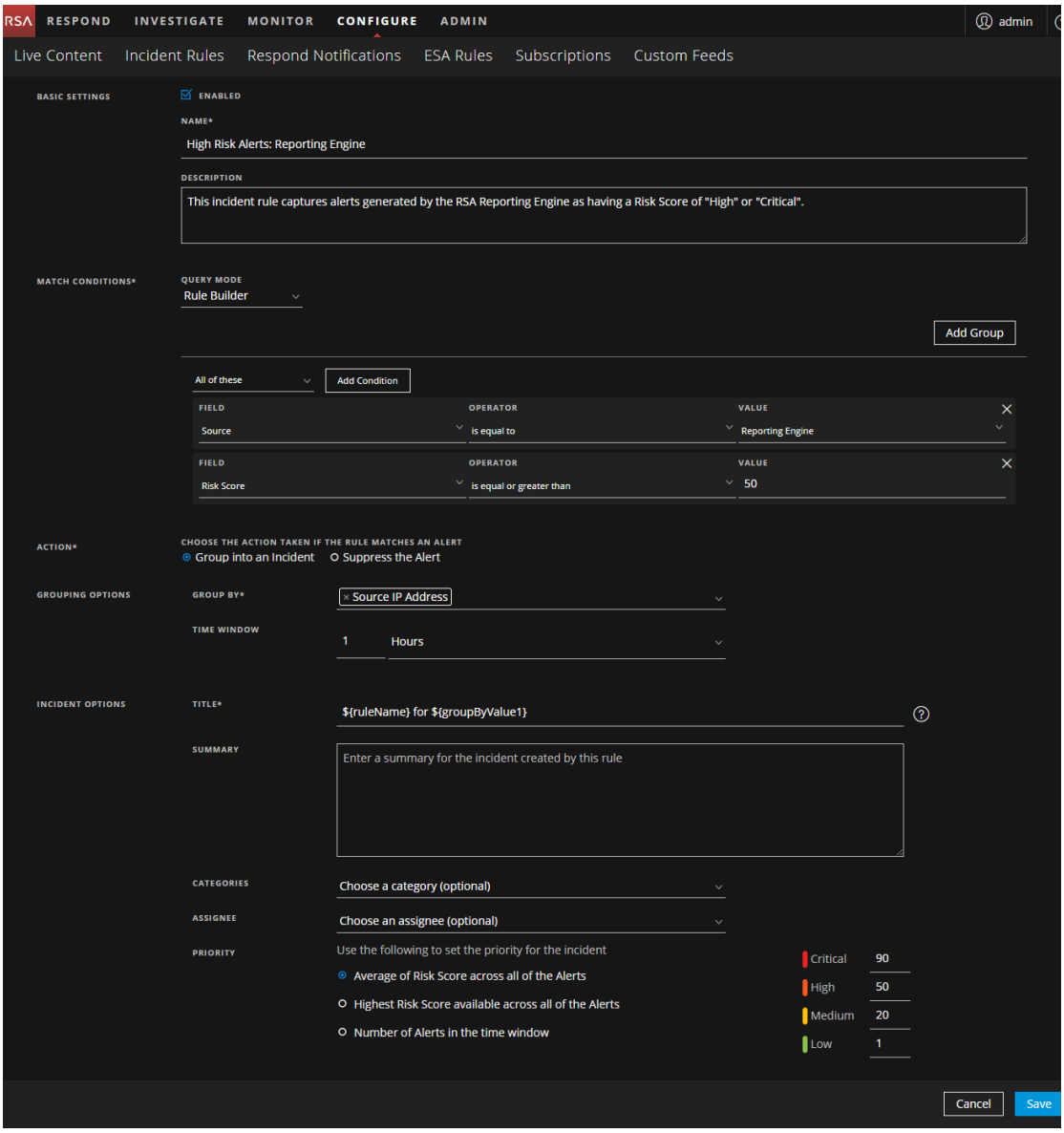
2. To add a new rule, click **Create Rule**.

The Incident Rule Details view is displayed.



3. Enter the parameters and conditions of your rule. All rules need to have at least one condition. For details about various parameters that can be set as criteria for an incident rule, see Incident Rule Details View.

   The following figure shows a rule example.



4. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
5. Click **Save**.

   The rule appears in the Incidents Rules list. If you selected Enabled, the rule will be enabled and it starts creating incidents depending on the incoming alerts that are matched as per the criteria selected.
6. Verify the order of your incident rules.

Verify the Order of your Incident Rules

To change the order of the rules, use the drag pads ( ) in front of the rules to move them up and down in the list.
The rule order determines which rule takes effect if the criteria for multiple rules match the same alert. If two rules match an alert, only the rule with the highest priority is evaluated.

Clone an Incident Rule

It is often easier to duplicate an existing rule that is similar to a rule that you want to create and adjust it accordingly.

1. Go to **CONFIGURE > Incident Rules**.
   The Incident Rules List view is displayed.
2. Select the rule that you would like to copy and click **Clone**.
3. Adjust the parameters and conditions of your rule as required. All rules need to have at least one condition.
4. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
5. Click **Save** to update the rule.
6. Verify the order of your incident rules.

Edit an Incident Rule

1. Go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.
   The Incident Rule Details view is displayed.
2. Adjust the parameters and conditions of your rule as required. All rules need to have at least one condition.
3. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save** to update the rule.
5. Verify the order of your incident rules.

See Also:

- For details about various parameters that can be set as criteria for an incident rule, see Incident Rule Details View.

- For details on the parameter and field descriptions in the Incident Rules List view, see Incident Rules List View.

Additional Procedures for Respond Configuration

Use this section when you are looking for instructions to perform a specific task after the initial setup of NetWitness Respond.

- Set Up and Verify Default Incident Rules
- Configure Respond Email Notification Settings
- Set a Retention Period for Alerts and Incidents
- Obfuscate Private Data
- Manage Incidents in NetWitness SecOps Manager
- Set Counter for Matched Alerts and Incidents
- Configure a Database for the Respond Server Service

Set Up and Verify Default Incident Rules

The User Behavior incident rule, which captures network user behavior, was introduced in NetWitness Suite 11.1. This rule uses deployed RSA Live ESA Rules to create incidents from alerts. You can select and deploy the RSA Live ESA Rules that you want to monitor.
The following default incident rules changed slightly in 11.1 and now have **Source IP Address** as the Group By value:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

To verify your existing default incident rules with the 11.1 default incident rules, look at the default incident rule tables following these procedures.

Set up the User Behavior Incident Rule

In order to use the default User Behavior incident rule, you need to deploy the RSA Live ESA Rules that you want to monitor from those listed in the User Behavior incident rule conditions. Complete the following procedures to start aggregating alerts for the User Behavior default incident rule:

- Deploy the RSA Live ESA Rules
- Adjust and enable the User Behavior default rule (or create it if you do not have it)

Deploy the RSA Live ESA Rules

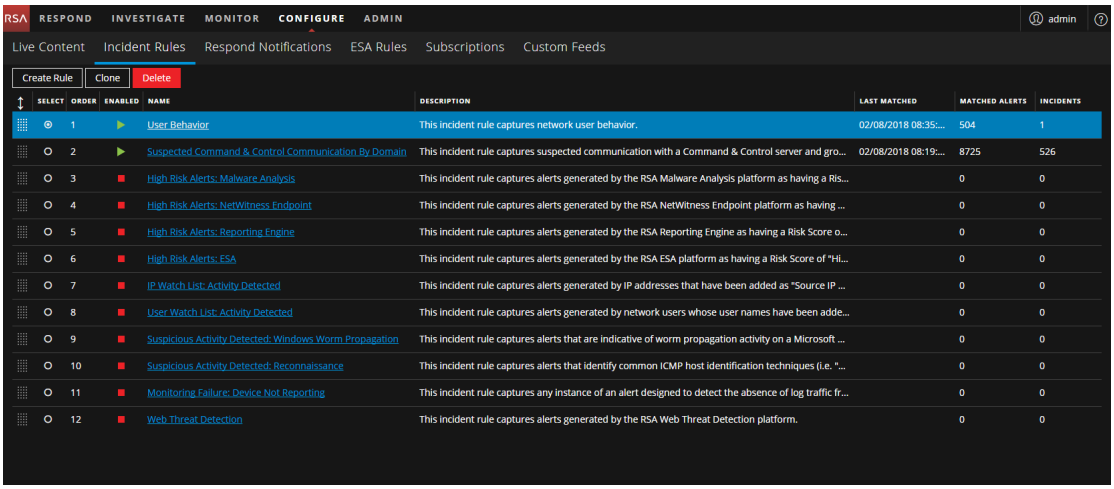
1. Go to **CONFIGURE > Live Content**.
2. In the **Resource Types** field, select **Event Steam Analysis Rule** and click **Search**.
3. In the **Matching Resources** list, select the ESA Rules from the following **User Behavior** table that you are interested in monitoring and deploy them (click **Deploy**).
4. Go to **CONFIGURE > ESA Rules > Rules** tab, and in the Rule Library **Filter** drop-down list, select **RSA Live ESA Rule**.
5. To add a new Deployment, in the drop-down list near **DEPLOYMENTS**, click **Add**.
   a. In the ESA Service section, add and then select your ESA service.
   b. In the ESA Rules section, click + and in the Deploy ESA Rules dialog, select the ESA Rules that you selected from the **User Behavior** table, and then click **Save**.
   The selected ESA rules are listed with a status of **Added**.
6. Select the ESA rules that you added from the previous step, and click **Deploy Now**.
   The status of the selected ESA rules changes to **Deployed**.
7. Go to **CONFIGURE > ESA Rules > Services** tab.
   In the **Deployed Rule Stats** for your ESA service, the rules that you added should have a status of enabled, which is indicated by a green circle in the Enable column.

Adjust and Enable the User Behavior Default Rule (or Create it if you do not have it)

If you have the User Behavior default rule, you can adjust it for your environment and enable it. If you do not have the User Behavior default rule, you can create it manually.

(Optional) To create the User Behavior default rule:

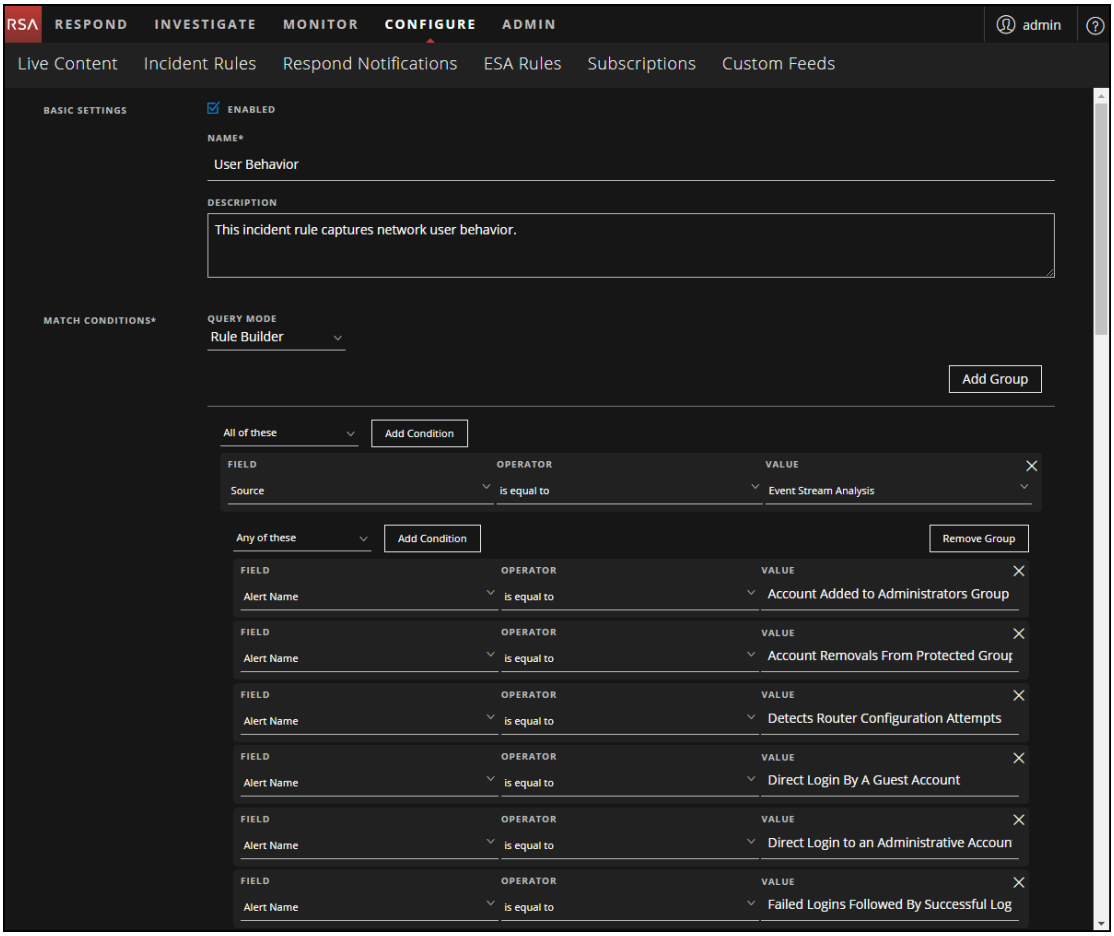
1. Go to **CONFIGURE > Incident Rules.**
   The Incident Rules List view is displayed.



2. Click **Create Rule** and in the Incident Rule Details view, create the User Behavior default incident rule using the values in the User Behavior table following this procedure. Values not listed in the table should be set for your business requirements. For details about various parameters that can be set as criteria for an incident rule, see Incident Rule Details View.

   The following figure shows a portion of the User Behavior default rule details. Notice that

there are two groups in this rule.



3. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save**.
   The rule appears in the Incidents Rules list. If you selected Enabled, the rule will be enabled and it starts creating incidents depending on the incoming alerts that are matched as per the rule criteria.
5. Verify the order of your incident rules. For more information, see Verify the Order of your Incident Rules .

User Behavior

The following table shows the values for the User Behavior default incident rule.

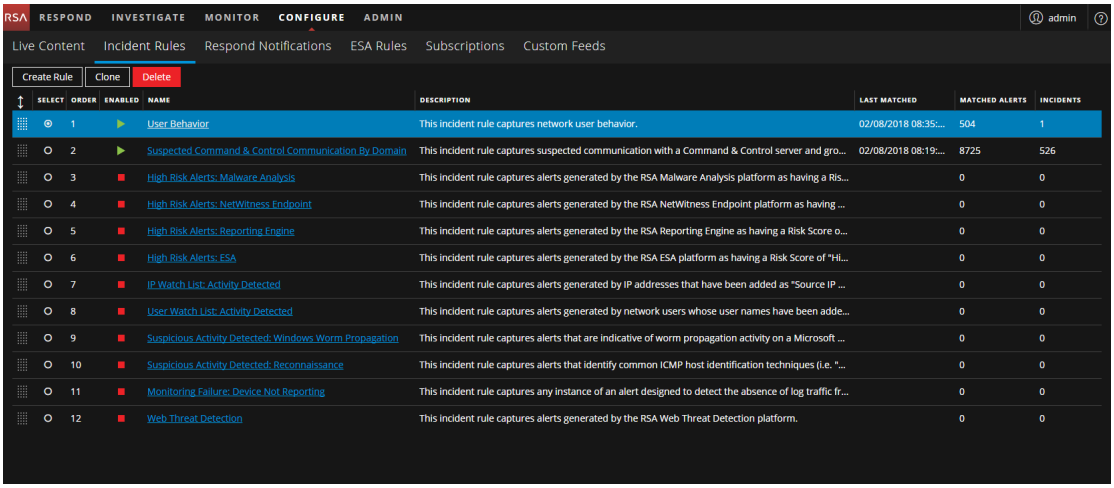
Field	Condition Field	Condition Operator	Value
Name			User Behavior
Description			This incident rule captures network user behavior.
1st Group:			All of these
Condition:	Source	is equal to	Event Stream Analysis
2nd Group:			Any of these
Conditions:	Alert Name	is equal to	Account Added to Administrators Group and Removed
	Alert Name	is equal to	Account Removals From Protected Groups on Domain Controller
	Alert Name	is equal to	Detects Router Configuration Attempts
	Alert Name	is equal to	Direct Login By A Guest Account
	Alert Name	is equal to	Direct Login to an Administrative Account
	Alert Name	is equal to	Failed Logins Followed By Successful Login Password Change
	Alert Name	is equal to	Insider Threat Mass Audit Clearing
	Alert Name	is equal to	Internal Data Posting to 3rd Party Sites

Field	Condition Field	Condition Operator	Value
	Alert Name	is equal to	kbrtgt Account Modified on Domain controller
	Alert Name	is equal to	Lateral Movement Suspected Windows
	Alert Name	is equal to	Logins across Multiple Servers
	Alert Name	is equal to	Logins by Same User to Multiple Servers
	Alert Name	is equal to	Malicious Account Creation Followed by Failed Authorization
	Alert Name	is equal to	Multiple Account Lockouts From Same or Different Users
	Alert Name	is equal to	Multiple Failed Logins Followed By a Successful Login
	Alert Name	is equal to	Multiple Failed Logins from Same User Originating from Different Countries
	Alert Name	is equal to	Multiple Failed Privilege Escalations by Same User
	Alert Name	is equal to	Multiple Intrusion Scan Events from Same User to Unique Destinations
	Alert Name	is equal to	Multiple Login Failures by Administrators to Domain Controller
	Alert Name	is equal to	Multiple Login Failures by Guest to Domain Controller

Field	Condition Field	Condition Operator	Value
	Alert Name	is equal to	Multiple Failed Logons from Same Source IP with Unique Usernames
	Alert Name	is equal to	Multiple Successful Logins from Multiple Diff Src to Diff Dest
	Alert Name	is equal to	Multiple Successful Logins from Multiple Diff Src to Same Dest
	Alert Name	is equal to	Privilege Escalation Detected
	Alert Name	is equal to	Privilege Escalation Detected in Unix
	Alert Name	is equal to	Privilege User Account Password Change
	Alert Name	is equal to	Failed Logins Outside Business Hours
	Alert Name	is equal to	DNS Tunneling
	Alert Name	is equal to	User Login Baseline
Group By			Destination User Account
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

Set up or Verify a Default Incident Rule

1. Go to **CONFIGURE > Incident Rules.**
   The Incident Rules List view is displayed.



2. Click the link in the **Name** field of a default incident rule to view the Incident Rule Details view. Set up or verify the default incident rule using the values in the default incident rules tables in this topic. Values not listed in the tables should be set for your business requirements. For details about various parameters that can be set as criteria for an incident rule, see Incident Rule Details View.
3. When you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save**.
5. Verify the order of your incident rules. For more information, see Verify the Order of your Incident Rules .

Suspected Command & Control Communication By Domain

The following table shows the values for the Command & Control Communication By Domain default incident rule.

Field	Condition Field	Condition Operator	Value
Name			Command & Control Communication By Domain
Description			This incident rule captures suspected communication with a Command & Control server and groups results by domain.

Field	Condition Field	Condition Operator	Value
Group:			All of these
Conditions:	Source	is equal to	Event Stream Analysis
	Alert Rule Id	is equal to	Suspected C&C
Group By			Domain for Suspected C& C
Time Window			7 Days
Title			Suspected C&C with ${groupByValue1}
Summary			NetWitness Suite detected communications with ${groupByValue1} that may be command and control malware. 1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.). 2. Review the domain registration for suspect information (Registrant country, registrar, no registration data found, etc). 3. If the domain is suspect, go to the Investigation module to locate other activity to or from it.

High Risk Alerts: Malware Analysis

The following table shows the values for the High Risk Alerts: Malware Analysis default incident rule.

Field	Condition Field	Condition Operator	Value
Name			High Risk Alerts: Malware Analysis
Description			This incident rule captures alerts generated by the RSA Malware Analysis platform as having a Risk Score of "High" or "Critical".

Field	Condition Field	Condition Operator	Value
Group:			All of these
Conditions:	Source	is equal to	Malware Analysis
	Risk Score	is equal or greater than	50
Group By			Source IP Address
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

High Risk Alerts: NetWitness Endpoint

The following table shows the values for the High Risk Alerts: NetWitness Endpoint default incident rule.

Field	Condition Field	Condition Operator	Value
Name			High Risk Alerts: NetWitness Endpoint
Description			This incident rule captures alerts generated by the RSA NetWitness Endpoint platform as having a Risk Score of "High" or "Critical".
Group:			All of these
Conditions:	Source	is equal to	NetWitness Endpoint
	Risk Score	is equal or greater than	50
Group By			Source IP Address
Time Window			1 Hour

Field	Condition Field	Condition Operator	Value
Title			${ruleName} for ${groupByValue1}

High Risk Alerts: Reporting Engine

The following table shows the values for the High Risk Alerts: Reporting Engine default incident rule.

Field	Condition Field	Condition Operator	Value
Name			High Risk Alerts: Reporting Engine
Description			This incident rule captures alerts generated by the RSA Reporting Engine as having a Risk Score of "High" or "Critical".
Group:			All of these
Conditions:	Source	is equal to	Reporting Engine
	Risk Score	is equal or greater than	50
Group By			Source IP Address
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

High Risk Alerts: ESA

The following table shows the values for the High Risk Alerts: ESA default incident rule.

Field	Condition Field	Condition Operator	Value
Name			High Risk Alerts: ESA

Field	Condition Field	Condition Operator	Value
Description			This incident rule captures alerts generated by the RSA ESA platform as having a Risk Score of "High" or "Critical".
Group:			All of these
Conditions:	Source	is equal to	Event Stream Analysis
	Risk Score	is equal or greater than	50
Group By			Source IP Address
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

IP Watch List: Activity Detected

The following table shows the values for the IP Watch List: Activity Detected default incident rule.

Field	Condition Field	Condition Operator	Value
Name			IP Watch List: Activity Detected
Description			This incident rule captures alerts generated by IP addresses that have been added as "Source IP Address" *and* "Destination IP Address" conditions of the rule. To add additional IP addresses to the watch list, simply add a new Source and Destination IP Address conditional pair.
Group:			Any of these
Conditions:	Source IP Address	is equal to	1.1.1.1

Field	Condition Field	Condition Operator	Value
	Destination IP Address	is equal to	1.1.1.1
	Source IP Address	is equal to	2.2.2.2
	Destination IP Address	is equal to	2.2.2.2
Group By			Source IP Address
Time Window			4 Hours
Title			${ruleName}

User Watch List: Activity Detected

The following table shows the values for the User Watch List: Activity Detected default incident rule.

Field	Condition Field	Condition Operator	Value
Name			User Watch List: Activity Detected
Description			This incident rule captures alerts generated by network users whose user names have been added as a "Source UserName" condition. To add more than one Username to the watch list, simply add an additional Source Username condition.
Group:			Any of these
Conditions:	Source Username	is equal to	jsmith
	Source Username	is equal to	jdoe

Field	Condition Field	Condition Operator	Value
Group By			Source Username
Time Window			4 Hours
Title			${ruleName}

Suspicious Activity Detected: Windows Worm Propagation

The following table shows the values for the Suspicious Activity Detected: Windows Worm Propagation default incident rule.

Field	Condition Field	Condition Operator	Value
Name			Suspicious Activity Detected: Windows Worm Propagation
Description			This incident rule captures alerts that are indicative of worm propagation activity on a Microsoft network
1st Group:			All of these
Condition:	Source	is equal to	Event Stream Analysis
2nd Group:			Any of these
Conditions:	Alert Name	is equal to	Windows Worm Activity Detected Logs
	Alert Name	is equal to	Windows Worm Activity Detected Logs
Group By			Source IP Address
Time Window			1 Hour
Title			${ruleName}

Suspicious Activity Detected: Reconnaissance

The following table shows the values for the Suspicious Activity Detected: Reconnaissance default incident rule.

Field	Condition Field	Condition Operator	Value
Name			Suspicious Activity Detected: Reconnaissance
Description			This incident rule captures alerts that identify common ICMP host identification techniques (i.e. "ping") accompanied by connection attempts to multiple service ports on a host
1st Group:			All of these
Condition:	Source	is equal to	Event Stream Analysis
2nd Group:			Any of these
Conditions:	Alert Name	is equal to	Port Scan Horizontal Packet
	Alert Name	is equal to	Port Scan Vertical Packet
	Alert Name	is equal to	Port Scan Horizontal Log
	Alert Name	is equal to	Port Scan Vertical Log
Group By			Source IP Address
Time Window			4 Hours
Title			${ruleName}

Monitoring Failure: Device Not Reporting

The following table shows the values for the Monitoring Failure: Device Not Reporting default incident rule.

Field	Condition Field	Condition Operator	Value
Name			Monitoring Failure: Device Not Reporting
Description			This incident rule captures any instance of an alert designed to detect the absence of log traffic from a previously reporting device
Group:			All of these
Conditions:	Source	is equal to	Event Stream Analysis
	Alert Name	is equal to	No logs traffic from device in given time frame
Group By			Source IP Address
Time Window			2 Hours
Title			${ruleName}

Web Threat Detection

The following table shows the values for the Web Threat Detection default incident rule.

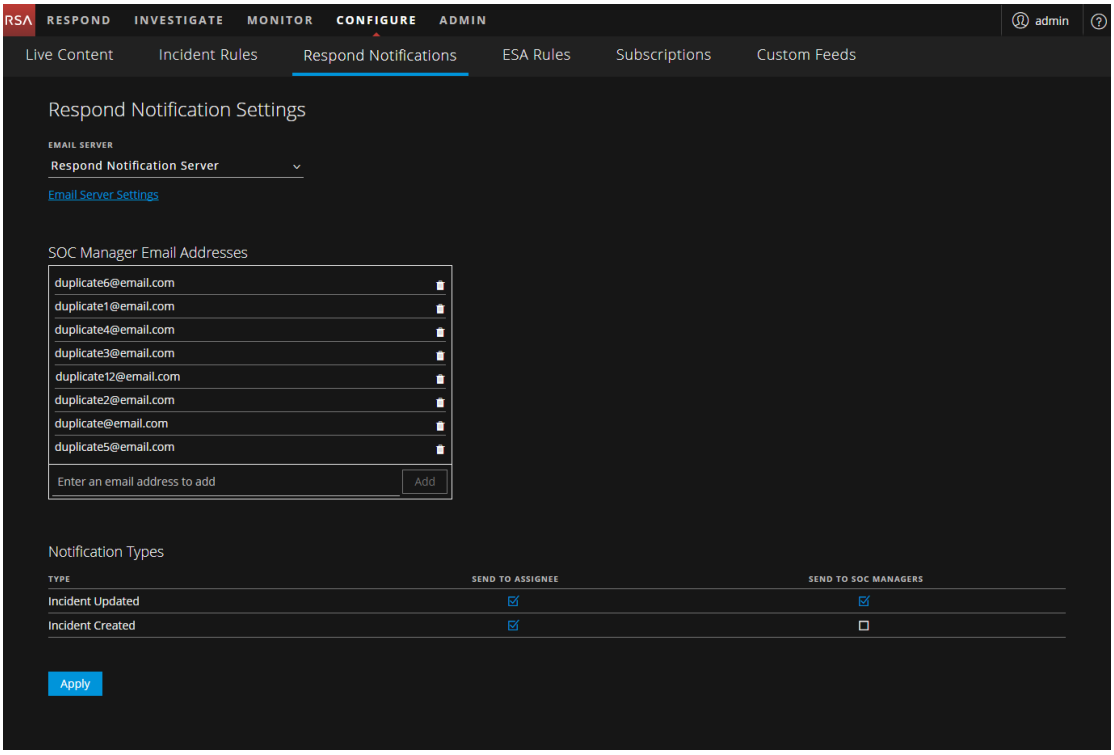
Field	Condition Field	Condition Operator	Value
Name			Web Threat Detection
Description			This incident rule captures alerts generated by the RSA Web Threat Detection platform.
Group:			All of these
Condition:	Source	is equal to	Web Threat Detection
Group By			Alert Rule Id

Field	Condition Field	Condition Operator	Value
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

Configure Respond Email Notification Settings

NetWitness Respond notification settings enable email notifications to be sent to SOC Managers and the Analyst assigned to an incident when an incident is created or updated.

1. Go to **CONFIGURE > Respond Notifications**.
   The Respond Notifications Settings view is displayed.



2. In the **Email Server** section, select the email server from the drop-down list that will send out email notifications when the notification settings are enabled.
   If there is no email server configured, you will not see an email server listed in the drop-down list. You have to configure an email server before you can continue with this procedure. To configure an email server, click the **Email Server Settings** link. For more information, click the help icon or refer to the *System Configuration Guide*.

3. In the **SOC Manager Email Addresses** section, add the email addresses of the SOC Managers that you want to receive email notifications. To add an SOC Manager email address to the list, type it in the field that shows **Enter an email address to add** and click **Add**. To remove an SOC Manager email address from the list, click next to the email address to be removed.

4. In the **Notification Types** section, select who should receive an email notification when an incident is created and when an incident is updated.
   - **Send to Assignee**: An email is sent to the Analyst assigned to the incident.
   - **Send to SOC Manager**: An email is sent to all of the addresses listed in the **SOC Manager Email Addresses** list.
5. Click **Apply**. Changes take effect immediately.

Note: If user email address information is updated in the ADMIN > Security > Users tab, it can take up to two minutes for the new email changes to take effect. Any incident creation or incident update email notifications sent during this time will go to the old email address.

Migration Considerations

Notification Settings do not migrate from NetWitness Suite version 10.6.x to 11.1. The Incident Management Notification Settings in 10.6.x are different from the Respond notification settings available in 11.1. You will need to manually update the Respond Notification Settings in version 11.1.

Notification Servers from 10.6.x will not display in the Email Server drop-down list. The email servers settings must be added to the Global Notification Servers (ADMIN > System > Global Notifications > Server tab).

Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

Set a Retention Period for Alerts and Incidents

Sometimes data privacy officers want to retain data for a certain period of time and then delete it. A shorter retention period frees up disk space sooner. In some cases, the retention period must be short. For example, laws in Europe state that sensitive data cannot be retained for more than 30 days. After 30 days, the data must be obfuscated or deleted.

Setting a retention period for data is an optional procedure. The time that NetWitness Respond receives alerts and creates an incident determine when retention begins. Retention periods range from 30 to 365 days. If you set a retention period, one day after the period ends data is permanently deleted.

Retention is based on the time that NetWitness Respond receives the alerts and the incident creation time.

Caution: Data deleted after the retention period cannot be recovered.

When the retention period expires, the following data is **permanently deleted**:

- Alerts
- Incidents
- Tasks
- Journal entries

Logs track retention and manual deletion so you can see what has been deleted. You can view Respond Server logs in the following locations:

- **Respond Server Service log**: /var/log/netwitness/respond-server/respond-server.log
- **Respond Server Audit log**: /var/log/netwitness/respond-server/respond-server.audit.log

The data retention period that you set here does not apply to Archer or other third-party SOC tools. Alerts and incidents from other systems must be deleted separately.

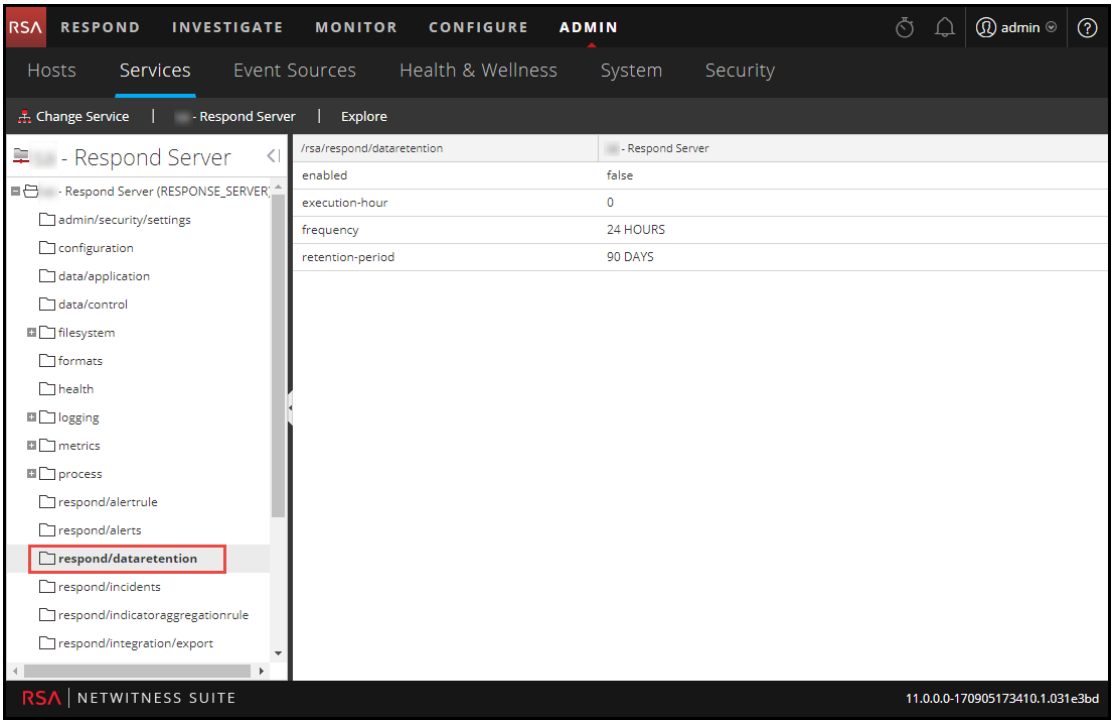
Prerequisites

The Administrator role must be assigned to you.

Procedure

1. Go to **ADMIN > Services** , select the Respond Server service, and then select > **View > Explore**.

2. In the Explore view node list, select **respond/dataretention**.



3. In the **enabled** field, select **true** to delete incidents and alerts older than the retention period. The scheduler runs every 24 hours at 23:00.
   You will see a notice that the configuration was successfully updated.
4. In the **retention-period** field, type the number of days to retain incidents and alerts. For example, type 30 DAYS, 60 DAYS, 90 DAYS, 120 DAYS, 365 DAYS, or any number of days.
   You will see a notice that the configuration was successfully updated.

Result

Within 24 hours after the retention period ends, the scheduler permanently deletes all alerts and incidents older than the specified period from NetWitness Respond. Journal entries and tasks associated with the deleted incidents are also deleted.

Obfuscate Private Data

The Data Privacy Officer (DPO) role can identify meta keys that contain sensitive data and should display obfuscated data. This topic explains how the administrator maps those meta keys to display a hashed value instead of the actual value.

The following caveats apply to hashed meta values:

- NetWitness Suite supports two storage methods for hashed meta values, HEX (default) and string.
- When a meta key is configured to display a hashed value, all security roles see only the hashed value in the Incidents module.
- You use hashed values the same way you use actual values. For example, when you use a hashed value in rule criteria the results are the same as if you used the actual value.

This topic explains how to obfuscate private data in NetWitness Respond. Refer to the "Data Privacy Management Overview" topic in the *Data Privacy Management Guide* for additional information about data privacy.

Mapping File to Obfuscate Meta Keys

In NetWitness Respond, the mapping file for data obfuscation is data_privacy_map.js. In it you type an obfuscated meta key name and map it to the actual meta key name.

The following example shows the mappings to obfuscate data for two meta keys, ip.src and user.dst:

```
'ip.src.hash' : 'ip.src',
 'user.dst.hash' : 'user.dst'
```

You determine the naming convention for obfuscated meta key names. For example, ip.src.hash could be ip.src.private or ip.src.bin. You must choose one naming convention and use it consistently on all hosts.

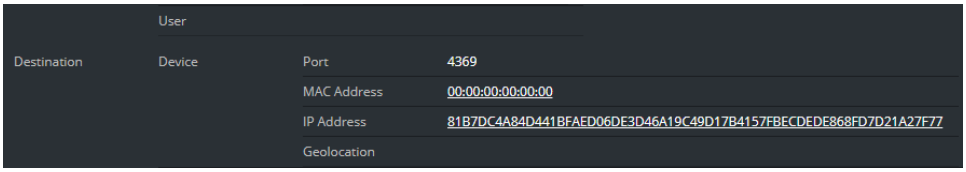
Prerequisites

- DPO role must specify which meta keys require data obfuscation.
- Administrator role must map meta keys for data obfuscation.

Procedure

1. Open the data privacy mapping file:
   /var/lib/netwitness/respond-server/scripts/data_privacy_map.js

2. In the `obfuscated_attribute_map` variable , type the name of a meta key to hold obfuscated data. Then map it to the meta key that does not contain obfuscated data according to this format:
   `'ip.src.hash' : 'ip.src'`
3. Repeat step 2 for every meta key that should display a hashed value.
4. Use the same naming convention as in step 2 and use it consistently on all hosts.
5. Save the file.
   All mapped meta keys will display hashed values instead of actual values.
   In the following figure, a hashed value displays for the destination IP address in the Event Details:



   New alerts will display obfuscated data.

Note: Existing alerts still display sensitive data. This procedure is not retroactive.

Manage Incidents in NetWitness SecOps Manager

If you want to manage incidents in RSA NetWitness® SecOps Manager instead of NetWitness Respond, you have to configure system integration settings in the Respond Server service Explore view. After you configure the system integration settings, all incidents are managed in NetWitness SecOps Manager. Incidents created before the integration will not be managed in NetWitness SecOps Manager.

Caution: If you are managing incidents in NetWitness SecOps Manager instead of NetWitness Respond, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Do not create incidents from the Respond Alerts List view or from Investigate.

For more detailed integration information, see the *RSA Archer Integration Guide*.

Prerequisites

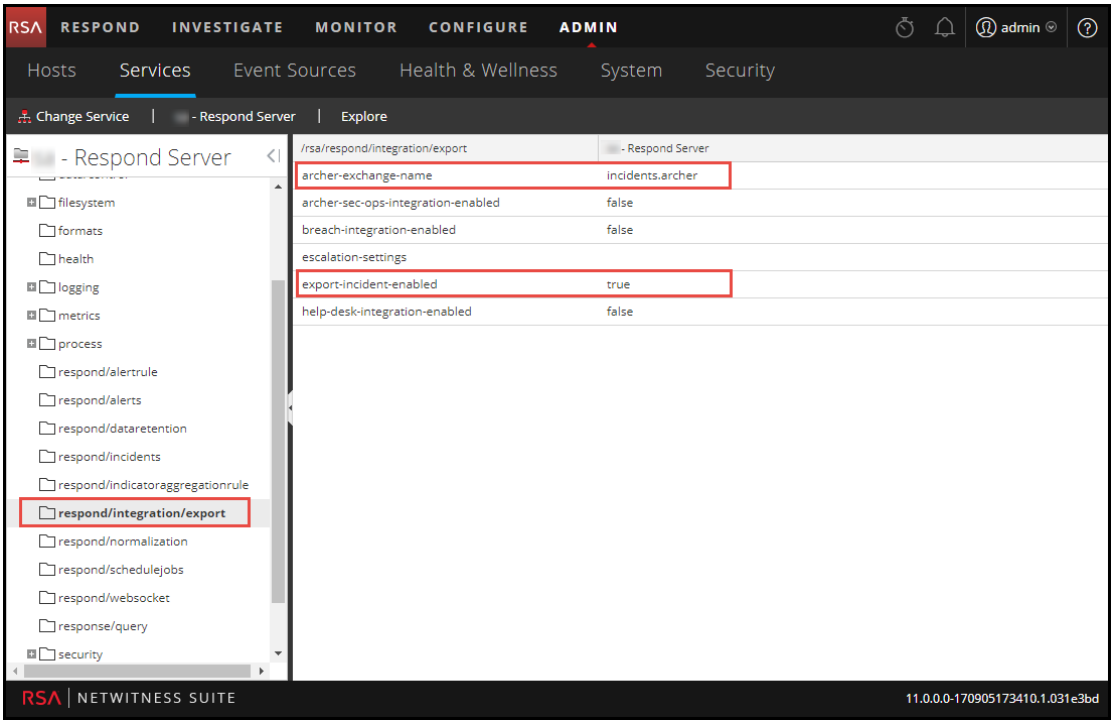
- NetWitness SecOps Manager 1.3.1.2 (NetWitness Suite11.0 will only work with NetWitness SecOps Manager 1.3.1.2.)

Procedure

Follow this procedure to configure Respond Server service settings to manage incidents in NetWitness SecOps Manager.

1. Go to **ADMIN > Services**, select the Respond Server service, and then select > **Config > Explore**.

2. In the Explore view node list, select **respond/integration/export**.

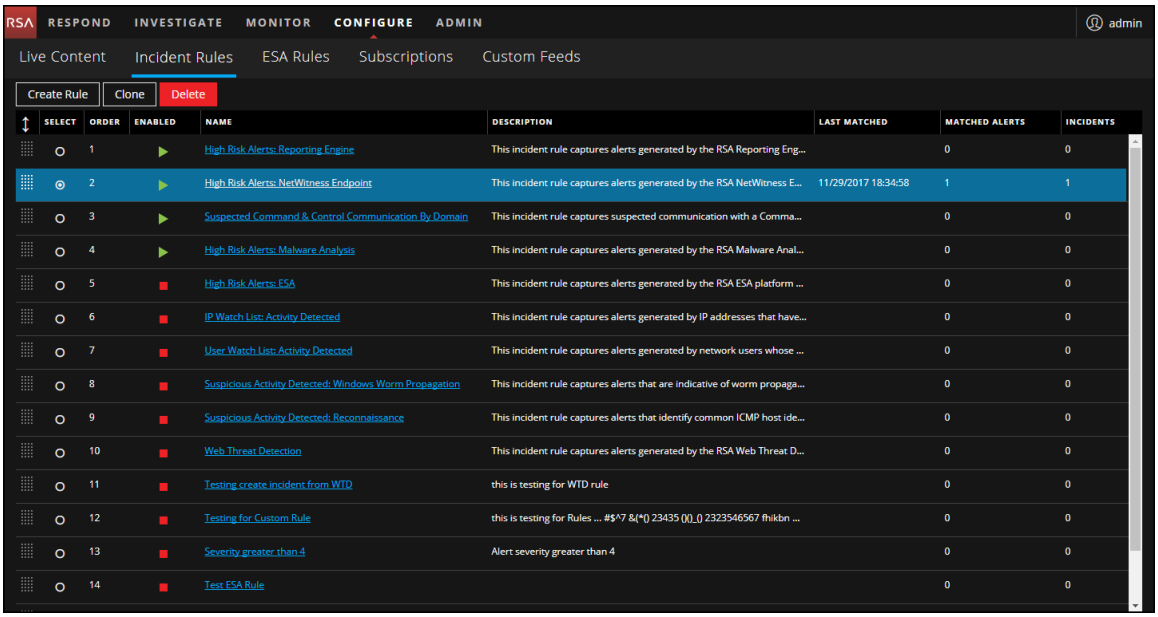


3. In the **archer-exchange-name** field, type the NetWitness SecOps Manager exchange name.
   You will see a notice that the configuration was successfully updated.

4. In the **archer-sec-ops-integration-enabled** field, select **true**.
   You will see a notice that the configuration was successfully updated.
   Incidents will be managed exclusively in NetWitness SecOps Manager.

Set Counter for Matched Alerts and Incidents

This procedure is optional. Administrators can use it to change when the count for matched alerts is reset to 0. The Incident List view displays these counts in columns on the right.



These columns provide the following information for a rule:

- **Last Matched** column shows the time when the rule last matched alerts.
- **Matched Alerts** column displays the number of matched alerts for the rule.
- **Incidents column** displays the number of incidents created by the rule.

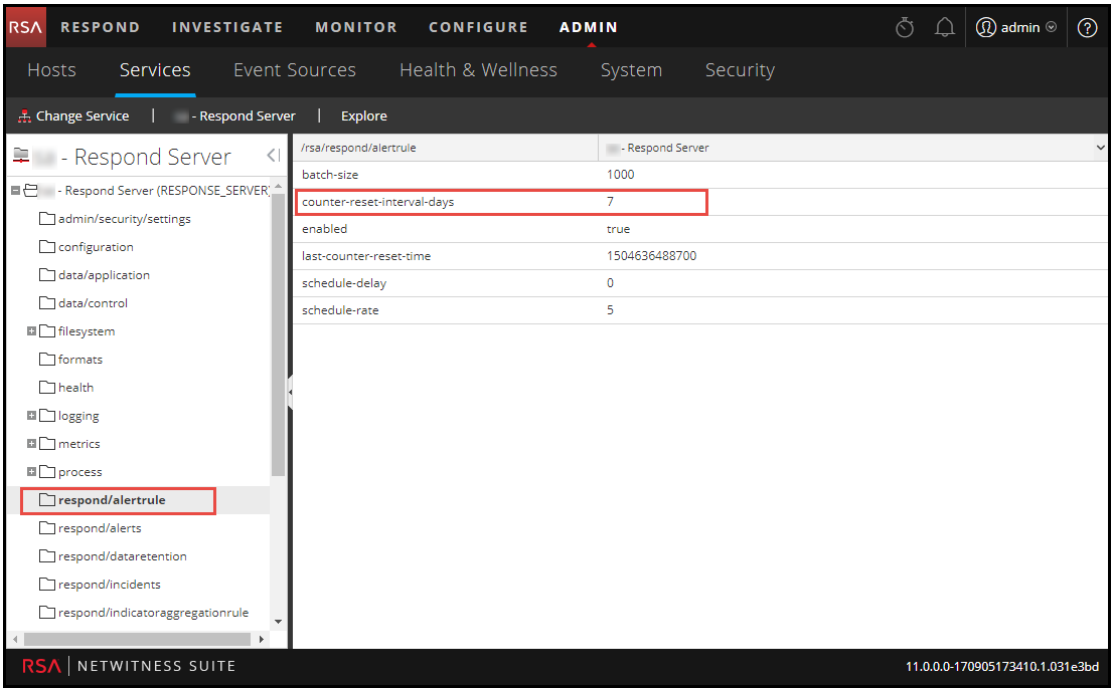
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.

Note: When the counter resets to zero, only the numbers in the three columns change to zero. No alerts or incidents get deleted.

To set a counter for matched alerts and incidents:

1. Go to **ADMIN > Services**, select the Respond Server service and then select **> View > Explore**.

2. In the Explore view node list, select **respond/alertrule**.



3. In the right panel, type the number of days in the **counter-reset-interval-days** field.
4. Restart the Respond Server service for the new setting to take effect. To do this, go to **ADMIN > Services**, select the Respond Server service, and then select > **Restart**.

Configure a Database for the Respond Server Service

This procedure is required only if you need to change the database configuration for Respond Server after the deployment of the NetWitness or ESA Primary hosts and their corresponding services. You have to select the ESA Primary server to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks. You also have to select the NetWitness Server to act as the database host for NetWitness Respond control data, such as incident rules and categories.

Prerequisites

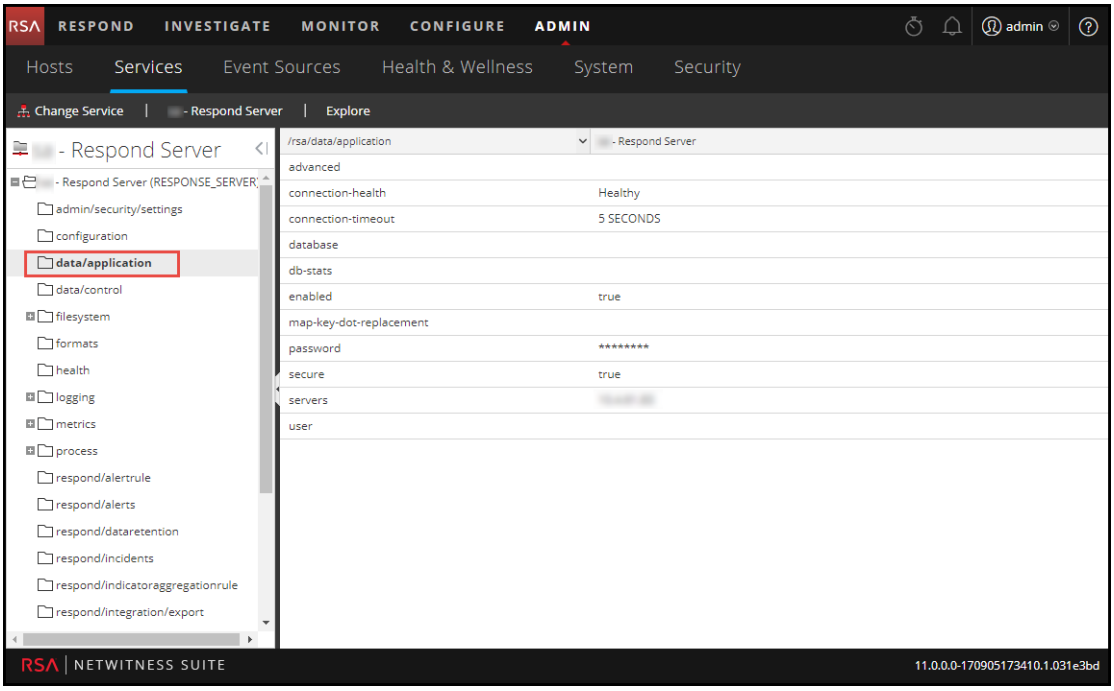
Ensure that:

- You have installed a host on which you want to run the Respond Server service. Refer to "Step 1: Deploy a Host" in the *Hosts and Services Getting Started Guide* for the procedure to add a host.
- The Respond Server service is installed and running on NetWitness Suite.
- An ESA host is installed and configured.

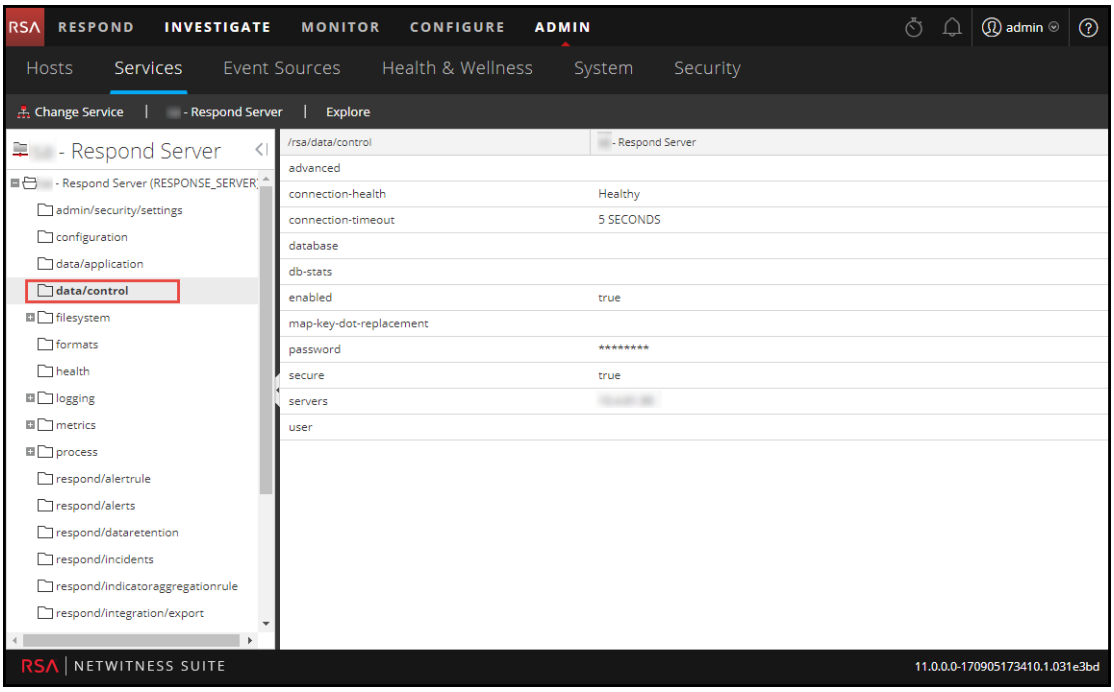
Procedure

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. In the Services panel, select the **Respond Server** service and then select **> View > Explore**.

3. In the Explore view node list, select **data/application**.



4. Provide the following information:
   - **database**: The database name. The default value is respond-server.
   - **password**: The password used for the deployment of the ESA primary server (password for deploy_admin user).
   - **servers**: The hostname or IP address of the **ESA primary server** to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks.
   - **user**: Enter **deploy_admin**.
5. In the Explore view node list, select **data/control**.



6. Provide the following information:
   - **database**: The database name. The default value is respond-server.
   - **password**: The password used for the deployment of the NetWitness Server (password for deploy_admin user).
   - **servers**: The hostname or IP address of the **NetWitness Server** to act as the database host for NetWitness Respond control data, such as incident rules and categories.
   - **user**: Enter **deploy_admin**.
7. Restart the Respond Server service. To do this, go to **ADMIN > Services**, select the Respond Server service, and then select > **Restart**.

Note: Restarting the Respond Server service is important for the database configuration to be complete.

NetWitness Respond Configuration Reference

This section contains reference information for configuring NetWitness Respond.

Configure View

The Configure view enables you to configure NetWitness Respond functionality.

You can configure incident rules to automate the Respond workflow for automatically creating incidents. You can also configure notification settings to send emails when incidents are created or updated.

Topics

- Incident Rules List View
- Incident Rule Details View
- Respond Notification Settings View
- Aggregation Rules Tab
- New Rule Tab

Incident Rules List View

The Incident Rules List View enables you to create and manage incident rules for automating the incident creation process. NetWitness Suite provides preconfigured rules. You can add to and adjust these rules for your own environment.

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

What do you want to do?

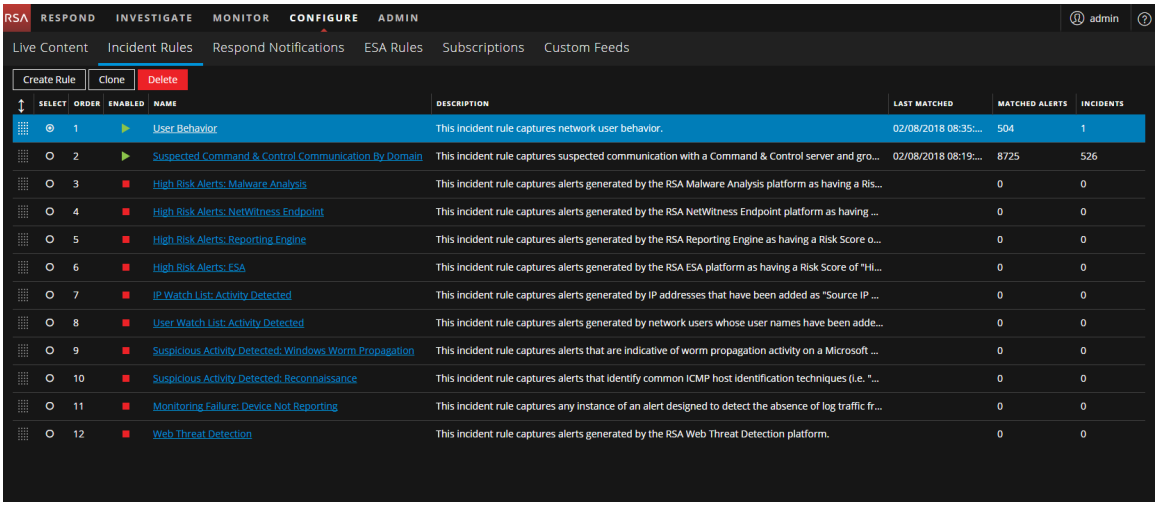
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create or edit an incident rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my incident rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

- Incident Rule Details View

Incident Rules List View

To access the Incident Rules List view, go to **CONFIGURE > Incident Rules**.



The Incident Rules List view consists of a list and series of buttons.

Incident Rules List

The following table describes the columns in the Incident Rules list.

Column	Description
	Enables you to change the priority order of the rules. Use the drag pad ( ) in front of a rule to move it up and down in the list.
Select	Enables you to select a rule in order to take an action, such as Clone or Delete.
Order	Shows the order in which the rule is placed. The rule order determines which rule takes effect if the criteria for multiple rules match the same alert. If two rules match an alert, only the rule with the highest priority is evaluated.
Enabled	Shows whether the rule is enabled or not. The specifies that the rule is enabled. The specifies that the rule is not enabled.
Name	Displays the name of the rule with a hyperlink. If you click the link, it opens the Rule Details view, where you can edit the rule.
Description	Displays the description of the rule.
Last Matched	Displays the time when an alert was successfully matched with the rule. This value is reset once a week.
Matched Alerts	Displays the number of matched alerts. This value is reset once a week. To change the setting, see Set Counter for Matched Alerts and Incidents.
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the Set Counter for Matched Alerts and Incidents.

Incident Rules Actions

The following table shows the operations that can be performed on the Incident Rules list.

Action	Description
Create Rule button	Allows you to add a new rule.
Delete button	Allows you to delete a rule.
Clone button	Allows you to duplicate a rule.
Name hyperlink	Allows you to edit a rule.

Incident Rule Details View

The Incident Rule Details view enables you to create and edit incident rules for creating incidents from alerts. This topic describes the information required when creating or editing a new rule.

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

What do you want to do?

Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Enable, create, or edit an incident rule.	Step 3. Enable and Create Incident Rules for Alerts
Analyst, Content Expert, SOC Manager	Set up and use the User Behavior default rule. Set up or verify the preconfigured (default) incident rules.	Set Up and Verify Default Incident Rules
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my incident rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

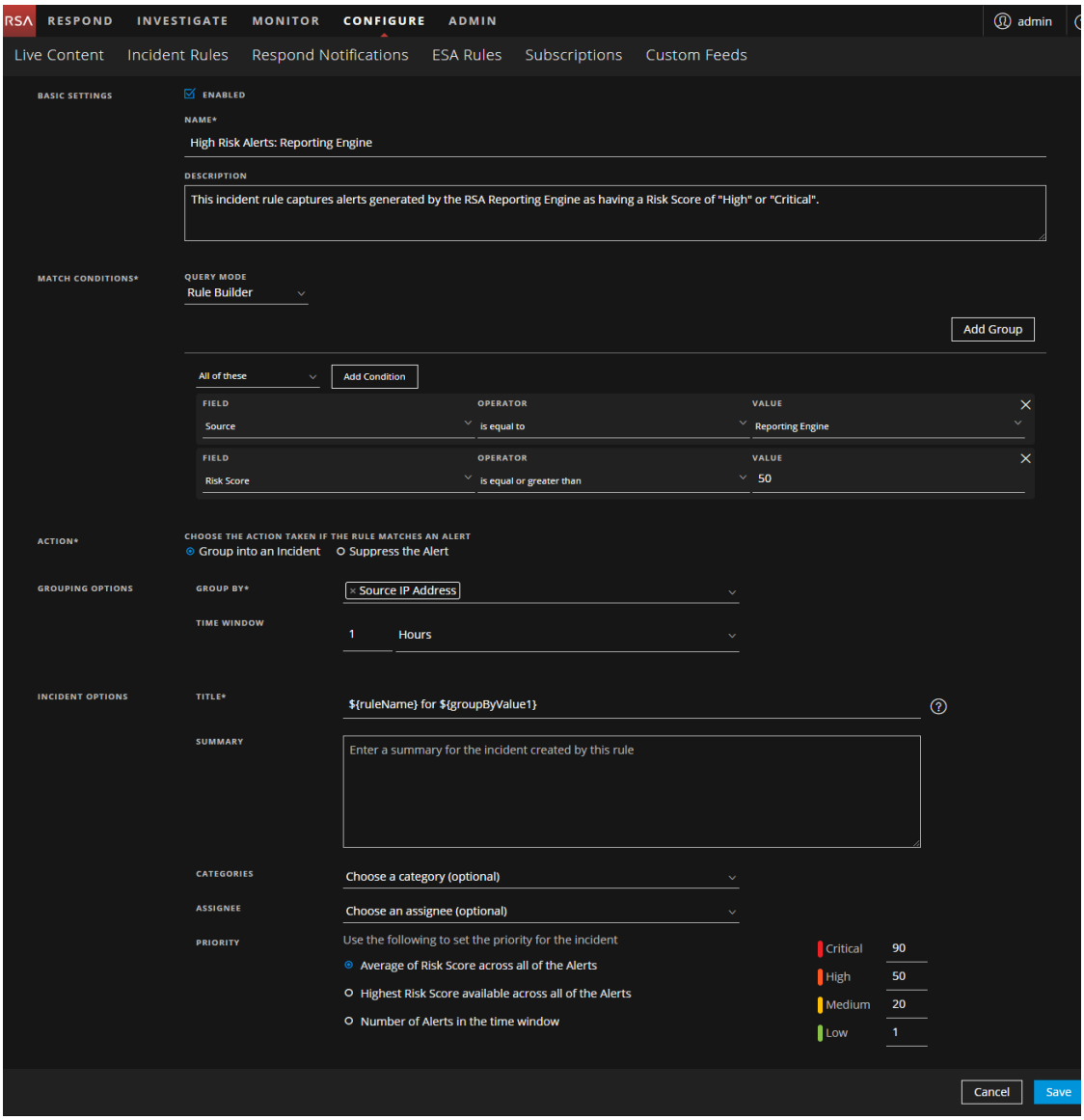
- Incident Rules List View

Incident Rule Details View

To access the Incident Rule Details view, do one of the following:

- To create a rule, go to **CONFIGURE > Incident Rules** and click **Create Rule**.
- To edit a rule, go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.

  The Incident Rule Details view is displayed. The following figure shows the Incident Rule Details view in Rule Builder query mode.



In the Match Conditions section, if you select Advanced query mode, a field to enter advanced queries is available as shown in the following figure.

The following table describes the options available when creating or editing incident rules.

Section	Field	Description
BASIC SETTINGS	ENABLED	Select to enable the rule.
	NAME*	Name of the rule. This is a required field.
	DESCRIPTION	A description of the rule to indicate which alerts get aggregated.
MATCH CONDITIONS*	QUERY MODE	**Rule Builder**: Select the Rule Builder option if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions. In the Match Conditions, you can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. For example, if you set the match condition to All of these, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. • Add a Condition to be matched by clicking the **Add Condition** button. • Add a Group of Conditions by clicking the **Add Group** button and add conditions by clicking the **Add Condition** button. You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents. **Advanced**: Select the Advanced query option if you want to use the advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected. For example, you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/

Section	Field	Description
ACTION*	CHOOSE THE ACTION TAKEN IF THE RULE MATCHES THE ALERT	**Group into an Incident**: If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert**: If enabled, the alerts that match the criteria are suppressed.
GROUPING OPTIONS	GROUP BY*	The criteria to group the alerts as per the specified alert fields. You can use a maximum of two fields to group the alerts. You cannot group alerts with fields that do not have values. Grouping on an alert field means that all matching alerts containing the same meta key value for that field are grouped together in the same incident. (See the following **Group By Meta Key Mappings** table.)
	TIME WINDOW	The time range specified to group alerts. For example, if the time window is set to 1 hour, all alerts that match the criteria set in the Group By field and that arrive within an hour of each other are grouped into an incident.

Section	Field	Description
INCIDENT OPTIONS	TITLE*	Title of the incident. You can provide placeholders based on the attributes you grouped. Placeholders are optional. If you do not use placeholders, all Incidents created by the rule will have the same title. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from NetWitness Endpoint would be named **Alerts for NetWitness Endpoint**.
	SUMMARY	(Optional) Summary of the incident created by this rule.
	CATEGORIES	(Optional) Category of the incident created. An incident can be classified using more than one category.
	ASSIGNEE	(Optional) Name of the user assigned to the incident.
	PRIORITY	**Average of Risk Score across all of the Alerts**: Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts**: Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window**: Takes the count of the number of alerts in the time window selected to set the priority of the incident created. **Critical, High, Medium, and Low**: Specify the incident priority threshold of the matched incidents. The defaults are: • Critical: 90 • High: 50 • Medium: 20 • Low: 1 For example, with the Critical priority set to 90, incidents with a risk score of 90 or higher will be assigned a Critical priority for this rule.

Group By Meta Key Mappings

The following table shows the mapped meta keys for the available Group By field selections. For example, if you select the Group By field value **Destination Host**, it uses the mapped meta key `alert.groupby_host_dst`. All alerts with the same meta key value for `alert.groupby_host_dst` are grouped together in the same incident.

Group By Field Value	Mapped Meta Key
Alert Name	alert.name
Alert Rule Id	alert.signature_id
Alert Type	alert.groupby_type
Date Created	alert.timestamp
Destination Country	alert.groupby_destination_country
Destination Domain	alert.groupby_domain_dst
Destination Host	alert.groupby_host_dst
Destination IP Address	alert.groupby_destination_ip
Destination Port	alert.groupby_destination_port
Destination User Account	alert.groupby_user_dst
Detector IP Address	alert.groupby_detector_ip
Domain	alert.groupby_domain
Domain for Suspected C&C	alert.groupby_c2domain
File Analysis	alert.groupby_analysis_file
Filename	alert.groupby_filename
File MD5 Hash	alert.groupby_data_hash
Risk Score	alert.risk_score

Group By Field Value	Mapped Meta Key
Service Analysis	alert.groupby_analysis_service
Session Analysis	alert.groupby_analysis_session
Severity	alert.severity
Source	alert.source
Source Country	alert.groupby_source_country
Source Domain	alert.groupby_domain_src
Source Host	alert.groupby_host_src
Source IP Address	alert.groupby_source_ip
Source User Account	alert.groupby_user_src
Source Username	alert.groupby_source_username
User Account	alert.groupby_username

Respond Notification Settings View

The Respond Notification Settings view enables you to send email notifications when incidents are created or updated to SOC Managers and the Analysts assigned to the incidents.

Note: The information in this topic applies to RSA NetWitness® Suite Version 11.1 and later.

What do you want to do?

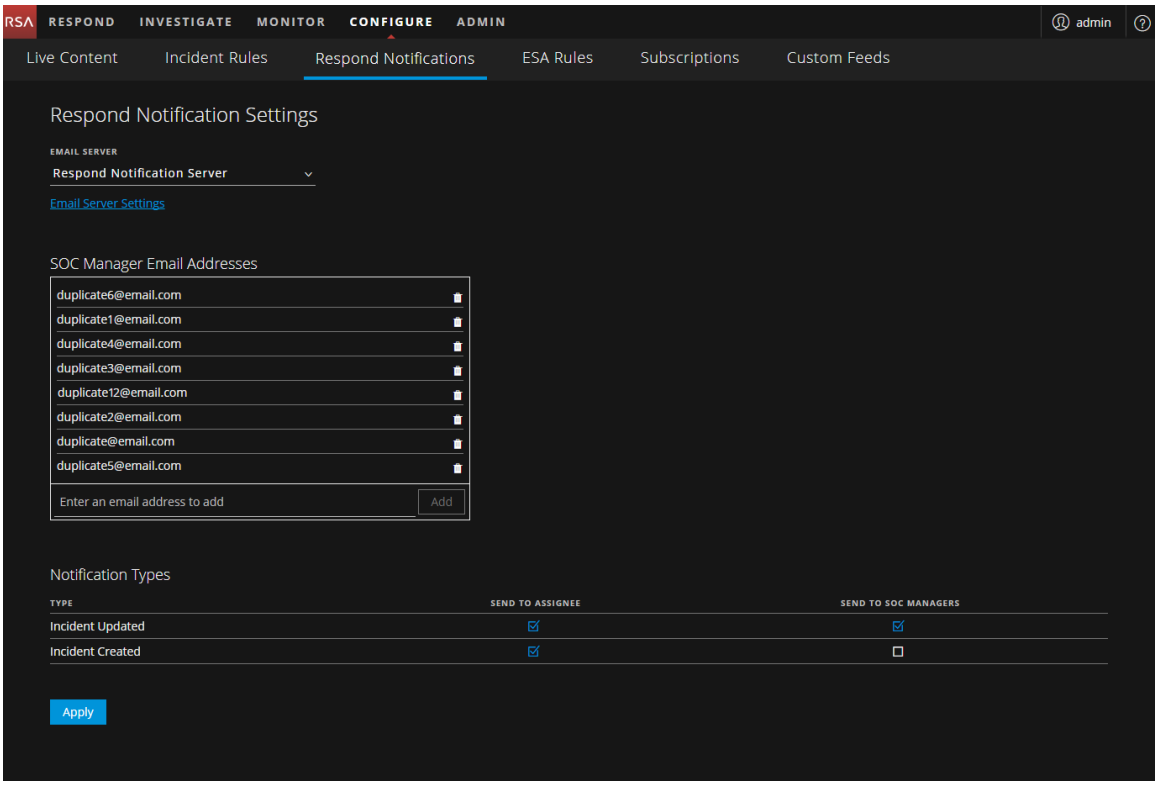
Role	I want to ...	Show me how
Administrator	Configure an email server.	Refer to the *System Configuration Guide*. Click the **Email Server Settings** link or go to ADMIN > SYSTEM > Global Notifications.
Incident Responders, Analysts, Content Experts, SOC Manager	Configure email notifications for when an incident is created or updated.	Configure Respond Email Notification Settings

Related Topics

- Incident Rules List View

Respond Notification Settings

To access the Respond notification settings, go to **CONFIGURE > Respond Notifications**. The Respond Notification Settings view is displayed.



The following table lists the Respond notification settings.

Setting	Description
Email Server	Shows the Email server that will send the email notifications.
Email Server Settings	If the Email server that you would like to use for notifications is not listed in the Email Server drop-down list, you can configure the email server settings. Click the **Email Server Settings** link to go to ADMIN > SYSTEM > Global Notifications. For instructions, refer to the *System Configuration Guide*.
SOC Manager Email Addresses	Lists the SOC Manager email addresses that will receive email notifications when you select **Send to SOC Manager** in the Notification Types section. You can add and remove email addresses as needed.

Setting	Description
Notification Types - Incident Created	Shows who should receive an email notification when an incident is created. • **Send to Assignee**: When an incident is created, an email is sent to the Analyst assigned to the incident. • **Send to SOC Manager**: When an incident is created, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.
Notification Types - Incident Updated	Shows who should receive an email notification when an incident is created. • **Send to Assignee**: When an incident is updated, an email is sent to the Analyst assigned to the incident. • **Send to SOC Manager**: When an incident is updated, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.
Apply	Changes to these settings take effect immediately.

Note: If user email address information is updated in the ADMIN > Security > Users tab, it can take up to two minutes for the new email changes to take effect. Any incident creation or incident update email notifications sent during this time will go to the old email address.

Aggregation Rules Tab

The Aggregation Rules tab enables you to create and manage aggregation rules for automating the incident creation process. NetWitness Suite provides 11 preconfigured rules. You can add to and adjust these rules for your own environment.

Note: This topic applies to NetWitness Suite version 11.0 and earlier.

What do you want to do?

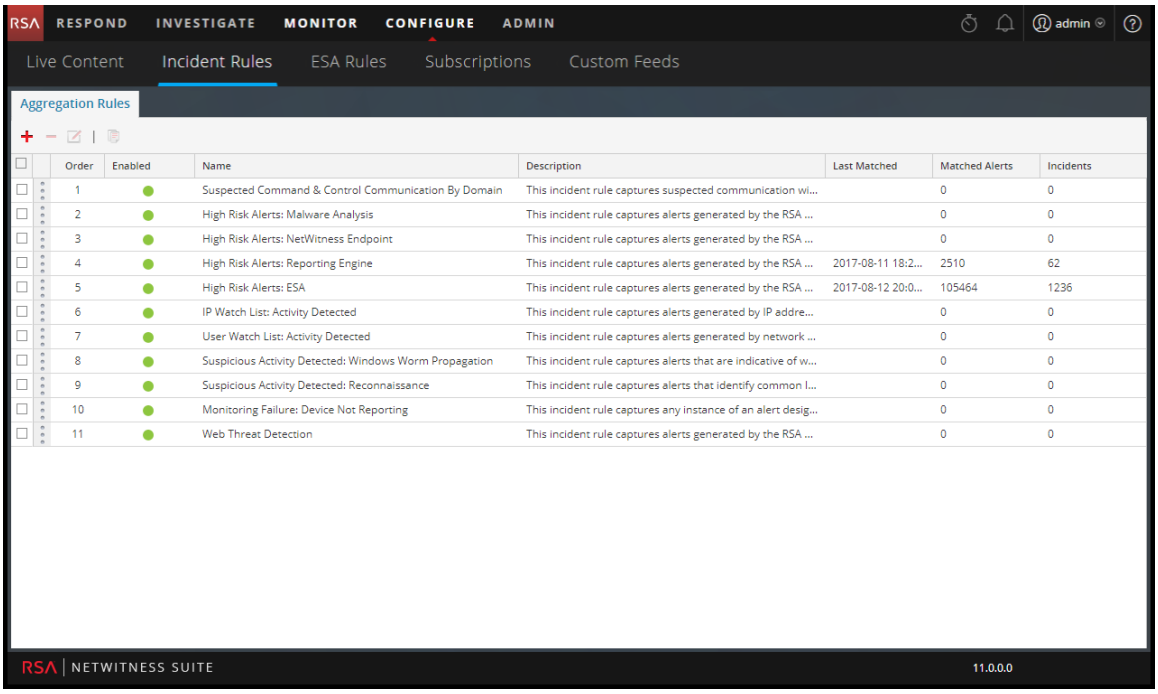
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

- New Rule Tab

Aggregation Rules

To access the Aggregation Rules tab, go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.



The Aggregation Rules tab consists of a list and toolbar.

Aggregation Rules List

The following table describes the columns in the Aggregation Rules list.

Column	Description
Select	Enables you to select a rule in order to take an action, such as Clone or Delete.
Order	Shows the order in which the rule is placed. The rule order determines which rule takes effect if the criteria for multiple rules match the same alert. If two rules match an alert, only the rule with the highest priority is evaluated.
Name	Displays the name of the rule.
Enabled	Shows whether the rule is enabled or not. The ● specifies the rule is enabled.
Description	Displays the description of the rule.
Last Matched	Displays the time when an alert was successfully matched with the rule. This value is reset once a week.

Column	Description
Matched Alerts	Displays the number of matched alerts. This value is reset once a week. To change the setting, see Set Counter for Matched Alerts and Incidents.
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the Set Counter for Matched Alerts and Incidents.

Aggregation Rules Toolbar

The following table shows the operations that can be performed in the Aggregation Rules tab.

Option	Description
	Allows you to add a new rule.
	Allows you to edit a rule.
	Allows you to delete a rule.
	Allows you to duplicate a rule.

New Rule Tab

The New Rules tab enables you to create custom aggregation rules for automating the incident creation process. This topic describes the information required when creating a new rule.

Note: This topic applies to NetWitness Suite version 11.0 and earlier.

What do you want to do?

Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

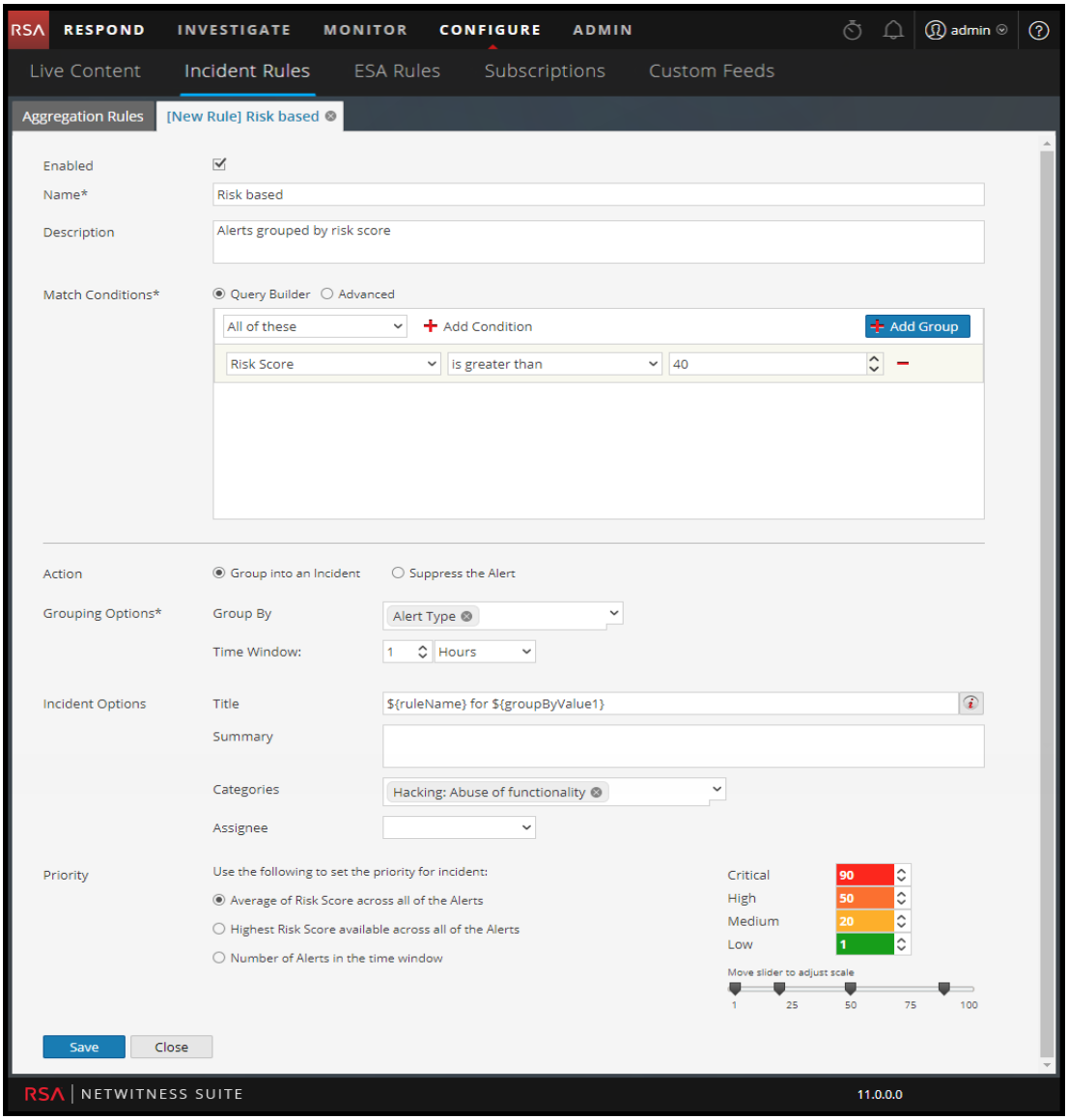
- Aggregation Rules Tab

New Rule

To access the New Rule tab view:

1. Go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.
2. Click +.

The **New Rule** tab is displayed.



The following table describes the options available when creating customized aggregation rules.

Field	Description
Enabled	Select to enable the rule.
Name*	Name of the rule. This is a required field.
Description	A description for the rule to give an idea about what alerts get aggregated.

Field	Description
Match Conditions*	**Query Builder** - Select if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions. Match Conditions - You can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. **For example**, if you set the match condition to All of these, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. • Add a Condition to be matched by clicking + **Add Condition**. • Add a Group of Conditions by clicking + **Add Group** and adding conditions by clicking + **Add Condition**. You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.
	Advanced - Select if you want to add an advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected. **For example:** you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/
Action	**Group into an Incident** - If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert** - If enabled, the alerts that match the criteria are suppressed.
Grouping Options*	**Group By:** The criteria to group the alerts as per the specified category. You can use a maximum of two attributes to group the alerts. You can group the alerts with one or two attributes. You can no longer group alerts with attributes that do not have values (empty attributes). Grouping on an attribute means that all matching Alerts containing the same value for that attribute are grouped together in the same incident. **Time Window:** The time range specified to group alerts. For example if the time window is set to 1 hour, all alerts that match the criteria set in Group By field and that arrive within an hour of each other are grouped into an incident.

Field	Description
Incident Options	**Title -** (Optional) Title of the incident. You can provide placeholders based on the attributes you grouped. Placeholders are optional. If you do not use placeholders, all Incidents created by the rule will have the same title. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from NetWitness Endpoint would be named **Alerts for NetWitness Endpoint**.
	Summary - (Optional) Summary of the incident.
	Category - (Optional) Category of the incident created. An incident can be classified using more than one category.
	Assignee - (Optional) Name of the assignee to whom the incident is assigned to.
Priority	**Average of Risk Score across all of the Alerts** - Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts** - Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window** - Takes the count of the number of alerts in the time window selected to set the priority of the incident created. **Critical, High, Medium, and Low** - Specify the incident priority threshold of the matched incidents. The defaults are: • Critical: 90 • High: 50 • Medium: 20 • Low: 1 For example, with the Critical priority set to 90, incidents with a risk score of 90 or higher will be assigned a Critical priority for this rule. You can change these defaults by manually changing the priorities or by moving the slider under **Move slider to adjust scale**.

RSA NETWITNESS® SUITE

Reporting Engine Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

How Reporting Engine Works **5**

Workflow 5

Configure the Reporting Engine **7**

Configure the Data Sources **8**

Configure a NWDB Data Source 8

Configure a Warehouse Data Source 9

Enable Jobs 13

Enable Kerberos Authentication 18

Set a Data Source as the Default Source 21

(Optional) Add Workbench as Data Source 22

(Optional) Add Archiver as Data Source 25

(Optional) Integrate Endpoint Information Into Reports 27

(Optional) Add Collection as Data Source to Reporting Engine 28

Configure Data Privacy for the Reporting Engine **31**

Add a NWDB Data Source with Different Service Accounts 32

Configure Data Source Permissions **35**

Configure Reporting Engine Settings **38**

Enable LDAP Authentication 38

Add Additional Space for Large Reports 39

Accessing Reporting Engine Log Files 40

Configuring Task Scheduler for a Reporting Engine 40

Specify the Pools and Queues 41

Define Reports, Charts, and Alerts **43**

Define Reports, Charts, and Alerts **44**

How to define Reports 44

How to define Charts 44

How to define Alerts 44

Configure Reporting Engine General Settings 46

Access the General Tab 46

References 47

General Tab 48

System Configuration 50

Logging Configuration 54

Warehouse Analytics Output Configuration 55

Warehouse Analytics Model Configuration 56

Warehouse Kerberos Configuration 57

Sources Tab 59

Output Actions Tab 64

NetWitness Suite Configuration 67

SMTP 68

SNMP 70

Syslog 71

SFTP 74

URL 75

Network Share 77

Manage Logos Tab 79

How Reporting Engine Works

Netwitness Reporting Engine is a service on the Netwitness Admin Server and facilitates the data extraction from different data sources to generate reports for compliance and analysis. Reporting Engine stores the definitions of the charts, rules, reports and alerts that are used to generate reports, charts and alerts.

Reporting Engine configuration includes configuring the data sources, definitions of outputs or notifications and parameters to improve the performance of data extraction and report, chart, and alert generation.

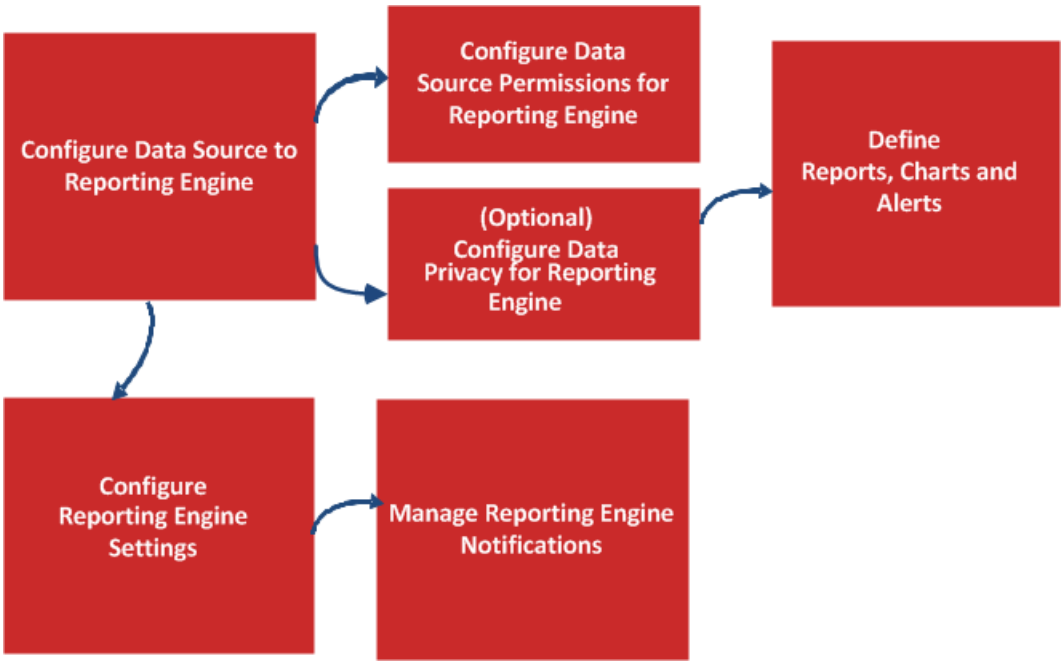
When you install the NetWitness Suite, Reporting Engine is automatically installed as a service. This enables the Reports, Charts, and Alerts to be maintained in the RSA NetWitness Suite and be available to view, download reports as PDF or CSV format, download charts as PDF and be added as dashlets.

For the Reporting Engine to run reports and alerts based on the data drawn from a data source, you must associate a data source, or multiple data sources to a Reporting Engine. There are three types of data sources:

- NWDB Data Sources - The NetWitness Database (NWDB) data sources are Decoders, Log Decoders, Brokers, Concentrators, Archiver, and Collection. Generation of reports, alerts, and charts on NWDB data sources is supported in Reporting Engine.
- Warehouse Data Sources - The Warehouse data sources are Horton Works and MapR which collects information from the Warehouse Connector and generates reports and alerts. This data source generated Reports only.
- Respond Data Sources - Respond is used to generate reports on alerts and incidents. This data source generated Reports only.

Workflow

This following workflow shows an overview of the Reporting Engine configuration which enables the user to generate Reports, Charts, and Alerts.


Configure Data Source to Reporting Engine
Configure Data Source Permissions for Reporting Engine
(Optional) Configure Data Privacy for Reporting Engine
Define Reports, Charts and Alerts
Configure Reporting Engine Settings
Manage Reporting Engine Notifications

Configure the Reporting Engine

On installation of the Netwitness Server, the Reporting Engine service is automatically available and some parameters are pre-populated with default values to achieve optimal results.

You must also ensure that the data sources are deployed and configured in the NetWitness Suite. For more information, see "Add Service or Edit Service Dialog" topic in the *Host and Service Configuration Guide*.

You can perform the following tasks:

- Check Live for the latest data source content and deploy it on a regular basis. (For more information, see "Manage Live Resources" topic in the in *Live Services Guide*).
- (Optional) Add Additional Space for Large Reports.

Configure the Data Sources

You must configure data sources such as NWDB, Warehouse, or Respond. You can configure NWDB, Warehouse, and Respond to generate Reports, Charts, and Alerts respectively. Optionally, you can also configure Archiver, Collection, and Workbench data sources.

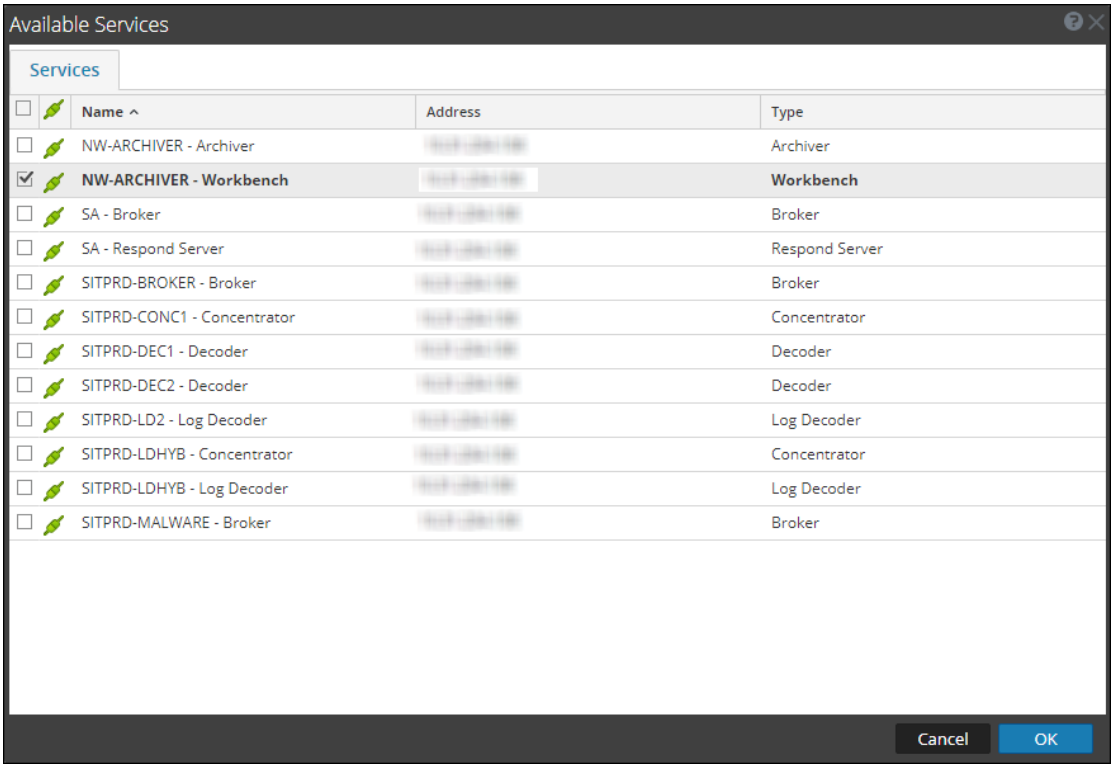
Configure a NWDB Data Source

To add a NWDB data source:

1. Go to **ADMIN** > **Services**.
2. In the **Services**, select **Reporting Engine** service.
3. Click > **View** > **Config**

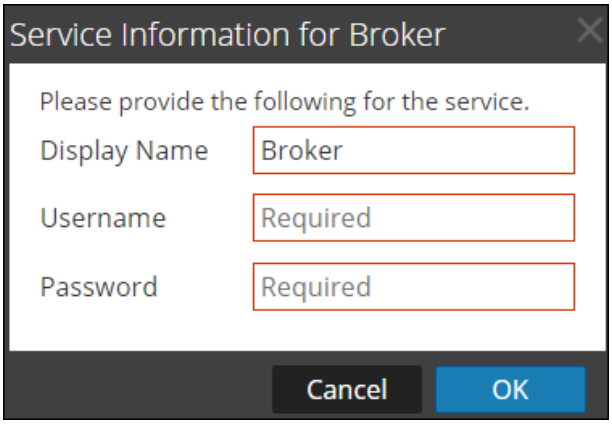
   The Services Config View of Reporting Engine is displayed.
4. On the **Sources** tab, click > **Available Services**.

   The **Available Services** dialog is displayed.

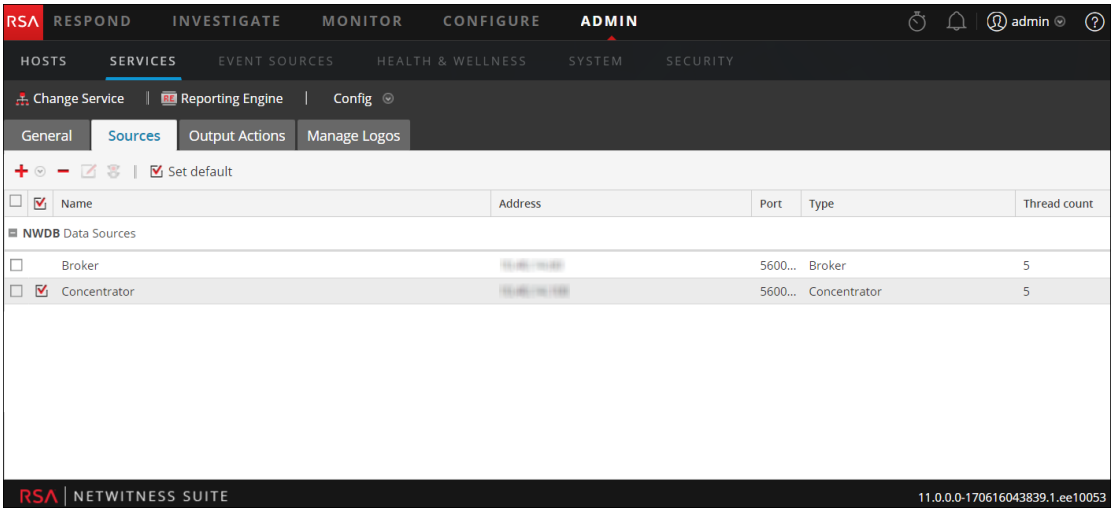


5. Select a NWDB service you want to add and click **OK**.

6. In the Service Information for Broker dialog, enter the service information for the service and click **OK**. In this example, we are adding a Broker service.



7. The service is displayed in the Sources tab when it is successfully added.



Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

Configure a Warehouse Data Source

You can add the warehouse data source to Reporting Engine, so that you can extract the data from the required services, store them in MapR or Horton works and generate Reports and Alerts. The procedure to configure Warehouse as a data source differs. To extract data from a Warehouse data source, you must configure it using the following procedure.

Note: Warehouse Analytics is not supported in Netwitness Suite 11.0 or later release.

Prerequisite

Make sure you:

- Add a Warehouse Data Source to Reporting Engine
- Set Warehouse Data Source as the Default Source
- HIVE server is in running state on all the Warehouse nodes. Use the following command to check the status of the HIVE server:

  ```
  status hive2 (MapR deployments)
   service hive-server2 status (Horton Works deployments)
  ```

- Warehouse Connector is configured to write data to the warehouse deployments.
- If Kerberos authentication is enabled for HiveServer2, make sure that the keytab file is copied to the `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/` directory in the Reporting Engine Host.

  Note: The **rsasoc** user should have read permissions for the keytab file. For more information, see Configure Data Source Permissions.

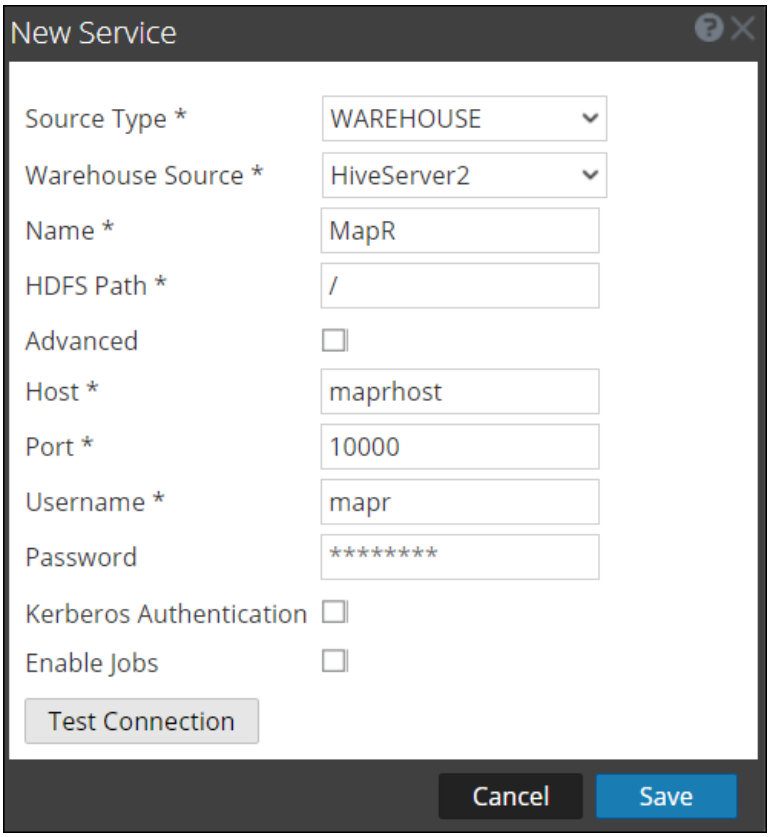
  Also, make sure that you update the keytab file location in the **Kerberos Keytab File** parameter in the Reporting Engine Service Config View. For more information, see General Tab.

To add Warehouse data source for MapR:

1. Go to **Admin** > **Services**.
2. In the **Services** list, select the **Reporting Engine** service.
3. Click > **View** > **Config**.
4. Click the **Sources** tab.

   The **Service Config** view is displayed with the Reporting Engine **Sources** tab open.
5. Click and select **New Service**.

   The New Service dialog is displayed.



6. In the **Source Type** drop-down menu, select **WAREHOUSE**.
7. In the **Warehouse Source** drop-down menu, select the warehouse data source.
8. In the **Name** field, enter the host name of the Warehouse data source.
9. In the **HDFS Path** field, enter the HDFS root path to which the Warehouse Connector writes the data.

   For example:
   If **/saw** is the local mount point for HDFS that you have configured while mounting NFS on the device. And if you have installed the Warehouse Connector service to write to SAW. For more information, see "Mount the Warehouse on the Warehouse Connector" topic in the *Warehouse (MapR) Configuration Guide*.

   If you have created a directory named **Ionsaw01** under **/saw** and provided the corresponding Local Mount Path as **/saw/Ionsaw01**, then the corresponding HDFS root path would be **/Ionsaw01**.

   The **/saw** mount point implies to /as the root path for HDFS. The Warehouse Connector writes the data **/ Ionsaw01** in HDFS. If there is no data available in this path, the following error is displayed:

   "No data available. Check HDFS path"

Make sure that **/lonsaw01/rsasoc/v1/sessions/meta** contains avro files of the meta data before performing test connection.

10. Select the **Advanced** checkbox to use the advanced settings, and fill in the **Database URL** with the complete JDBC URL to connect to the HiveServer2.

    For example:
    If kerberos is enabled in HIVE then the JDBC url will be:

    jdbc:hive2://<host>:<port>/<db>;principal=<Kerberos serverprincipal>

    If SSL is enabled in HIVE then the JDBC url will be:

    jdbc:hive2://<host>:<port>/<db>;ssl=true;sslTrustStore=<trust_store_path>;trustStorePassword=<trust_store_password>

    For more information on HIVE server clients, see https://cwiki.apache.org/confluence/display/Hive/HiveServer2+Clients.

11. If not using the advanced settings, enter the values for the **Host** and **Port**.

    - In the **Host** field, enter the IP address of the host on which HiveServer2 is hosted.

      Note: You can use the virtual IP address of MapR only if HiveServer2 is running on all the nodes in the cluster.

    - In the **Port** field, enter the HiveServer2 port of the Warehouse data source. By default, the port number is **10000**.

12. In the **Username** and **Password** field, enter the JDBC credentials used to access HiveServer2.

    Note: You can also use LDAP mode of authentication using Active Directory. For instructions to enable LDAP authentication mode, see Enable LDAP Authentication.

13. To run warehouse analytics reports, see Enable Jobs in Configuring Data Sources For Reporting.

14. Enable Kerberos authentication: see Enable Kerberos Authentication in Configuring Data Sources For Reporting.

15. If you want set the added Warehouse data source as default source for the Reporting Engine, select the added Warehouse data source and click Set default.

To add Warehouse data source for Horton Works (HDP):

Note: Make sure you download the `hive-jdbc-1.2.1-with-full-dependencies.jar`. This jar contains the driver file of HIVE 1.2.1 which connects to Reporting Engine for Hive 1.2.1 Hiveserver2, from RSA Link (https://community.rsa.com/docs/DOC-67251).

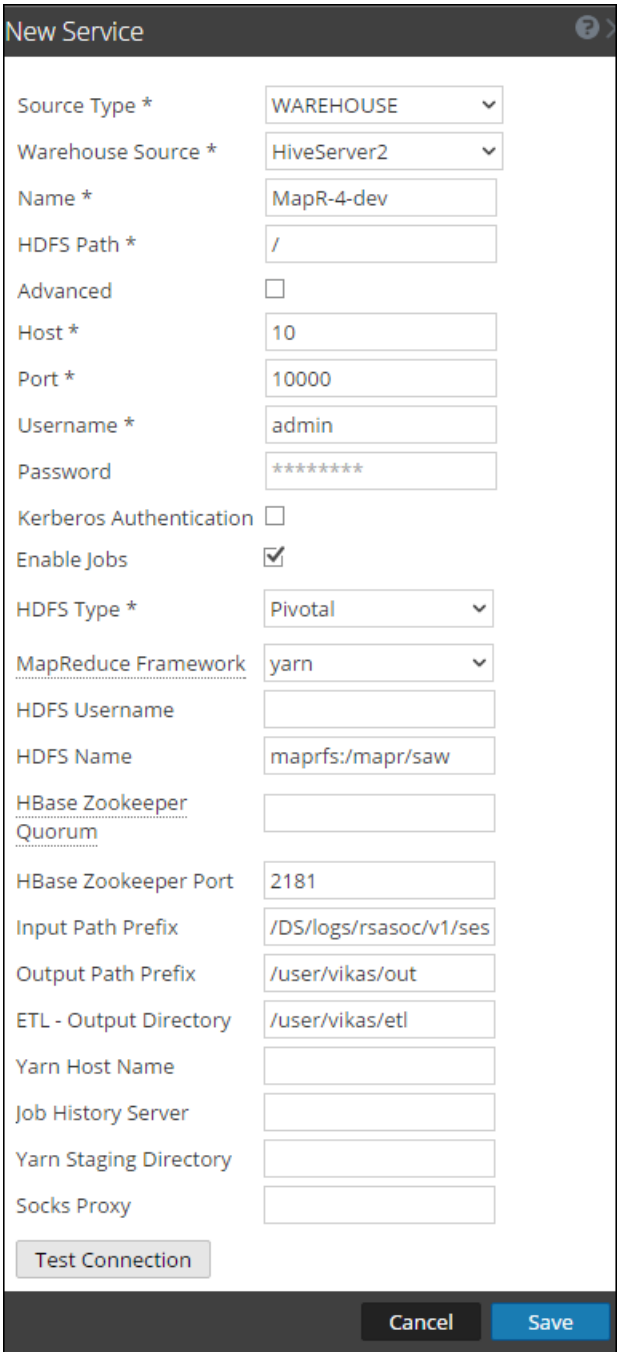
1. SSH to the Netwitness Suite server.
2. In the `/opt/rsa/soc/reporting-engine/plugins/` folder, take a backup of the following jar:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` or `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
3. Remove the following jar:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` or `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
4. In the /opt/rsa/soc/reporting-engine/plugins folder, copy the following jar using WinSCP:
   `hive-jdbc-1.2.1-with-full-dependencies.jar`
5. Restart the Reporting Engine service.
6. Log in to NetWitness Suite UI.
7. Select the **Reporting Engine** service and select > **View** > **Explore**.
8. In the **hiveConfig**, set **EnableSmallSplitBasedSchemaLiteralCreation parameter** to **true**.

Enable Jobs

Note: Warehouse Analytics is not supported in Netwitness Suite 11.0 or later release.

To run warehouse analytics reports, perform this procedure.

1. Select the **Enable Jobs** checkbox.



Note: Do not select Pivotal in the HDFS field as it is not supported for this release.

2. Enter the following details:

a. Select the type of HDFS from the **HDFS Type** drop-down menu.

- If you select the Horton Works HDFS type, enter the following information:

Field	Description
HDFS Username	Enter the username that Reporting Engine should claim when connecting to Horton Works. For standard horton works DCA clusters, this would be 'gpadmin'.
HDFS Name	Enter the URL to access HDFS. For example, hdfs://hdm1.gphd.local:8020.
HBase Zookeeper Quorom	Enter the list of host names separated by a comma on which the ZooKeeper servers are running.
HBase Zookeeper Port	Enter the port number for the ZooKeeper servers. The default port is 2181.
Input Path Prefix	Enter the output path of the Warehouse Connector (`/sftp/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) until the year directory. For example, `/sftp/rsasoc/v1/sessions/data/`.
Output Path Prefix	Enter the location where the data science job results are stored in HDFS.
Yarn Host Name	Enter the Hadoop yarn resource-manager host name in the DCA cluster. For example, **hdm3.gphd.local**.
Job History Server	Enter the Hadoop job-history-server address in the DCA cluster. For example, **hdm3.gphd.local:10020**.
Yarn Staging Directory	Enter the staging directory for YARN in the DCA cluster. For example, `/user`.

Field	Description
Socks Proxy	If you are using the standard DCA cluster, most of the hadoop services will be running in a local private network, not reachable from Reporting Engine. Then, you must run a socks proxy in the DCA cluster and allow access from outside to the cluster. For example, **mdw.netwitness.local:1080**.

- If you select the MapR HDFS type, enter the following information:

Field	Description
MapR Host Name	The user can populate the public ip address of any one of the MapR warehouse hosts.
MapR Host User	Enter a UNIX username in the given host that has access to execute map-reduce jobs on the cluster. The default value is 'mapr'.
MapR Host Password	(Optional)To setup password-less authentication, copy the public key of the “rsasoc” user from **/home/rsasoc/.ssh/id_rsa.pub** to the “authorized_keys” file of the warehouse host located in **/home/mapr/.ssh/authorized_keys**, with the assumption that “mapr” is the remote UNIX user.
MapR Host Work Dir	Enter a path that the given UNIX user (for example, “mapr”) has write access to. **Note:** The work directory is used by Reporting Engine to remotely copy the Warehouse Analytics jar files and start the jobs from the given host name. You must not use “/tmp” to avoid filling up of the system temporary space. The given work directory will be remotely managed by Reporting Engine.
HDFS Name	Enter the URL to access HDFS. For example, to access a specific cluster, maprfs:/mapr/<cluster-name>.

Field	Description
HBase Zookeeper Port	Enter the port number for the ZooKeeper servers. The default port is 5181.
Input Path Prefix	Enter the output path (`/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) until the year directory. For example, `/rsasoc/v1/sessions/data/`.
Input Filename	enter the file name filter for avro files. For example, **sessions-warehouseconnector**.
Output Path Prefix	Enter the location where the data science job results are stored in HDFS.

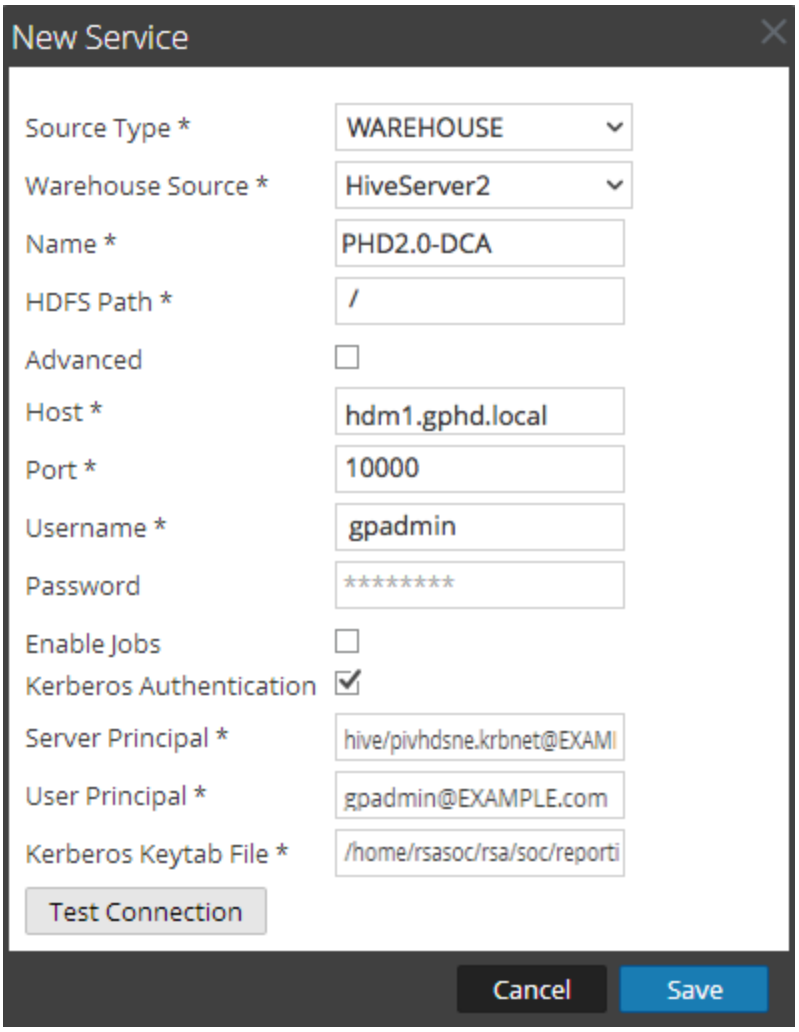
b. Select the MapReduce Framework as per the HDFS type.

> **Note:** For HDFS type MapR, select MapReduce framework as Classic. For HDFS type Horton Works, select MapReduce Framework as Yarn.

Next, enable Kerberos authentication.

Enable Kerberos Authentication

1. Select **Kerberos Authentication** checkbox, if the Warehouse has Kerberos enabled HIVE server.



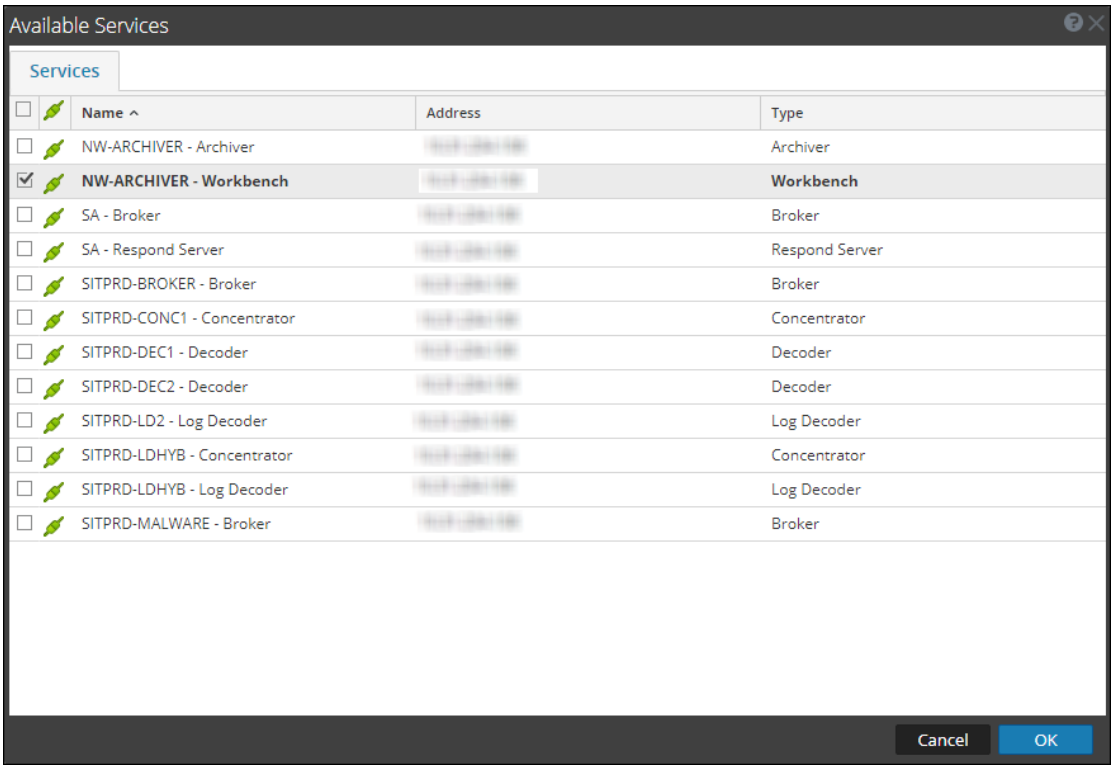
2. Fill in the fields as follows:

Field	Description
Server Principal	Enter the Principle used by the HIVE server to authenticate with the Kerberos Key Distribution Center (KDC) Server.
User Principal	Enter the Principle that HIVE JDBC client uses to authenticate with the KDC server for connecting the HIVE server. For example, **gpadmin@EXAMPLE.COM**.
Kerberos Keytab File	View the Kerberos keytab file location configured in the HIVE Configuration panel on the Reporting Engine General Tab. **Note:** Reporting Engine supports only the data sources configured with the same Kerberos credentials, like, User Principal and key tab file.

3. Click **Test Connection** to test the connection with the values entered.
4. Click **Save**.

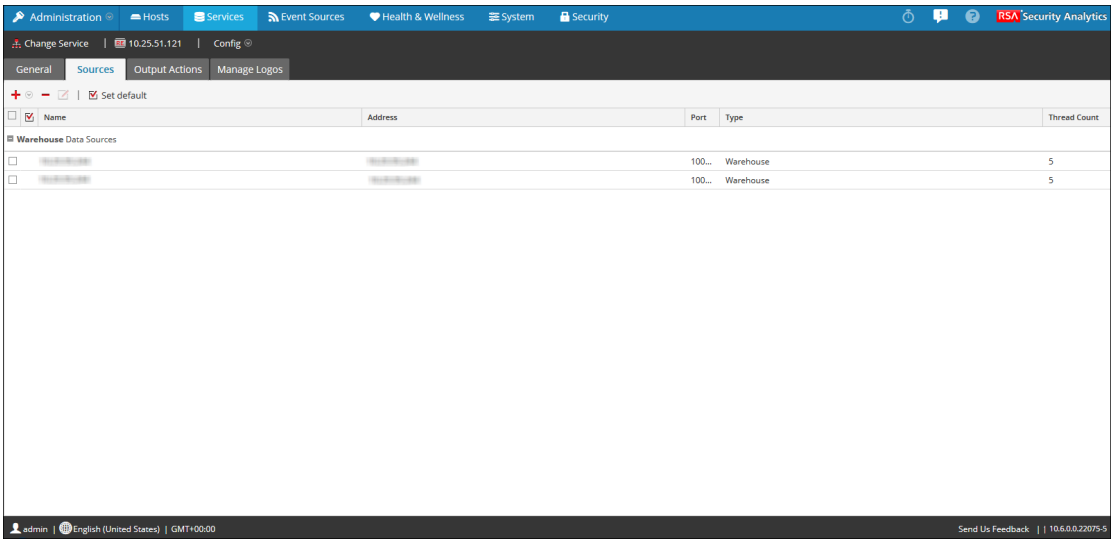
   The added Warehouse data source is displayed in the Reporting Engine Sources tab.
5. Click + > **Available Services**.

   The Available Services dialog box is displayed.



6. In the Available Services dialog box, select the service that you want to add as data source to the Reporting Engine and click **OK**.

   NetWitness Suite adds this as a data source available to reports and alerts against this Reporting Engine.



Note: This step is relevant only for an Untrusted model.

Set a Data Source as the Default Source

To set a data source to be the default source when you create reports and alerts:

1. Go to **Dashboard** > **Administration** > **Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Select > **View**> **Config**.

   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The **Services Config View** is displayed with the Reporting Engine Sources tab open.
5. Select the source that you want to be the default source (for example, Broker).
6. Click the **Set Default** checkbox.

   NetWitness Suite defaults to this data source when you create reports and alerts against this Reporting Engine.

(Optional) Add Workbench as Data Source

You have to carry out the following Workbench configurations to you to be able to use data from Workbench data source to generate Reports and Alerts. This topic provides following instructions describes on how to add Workbench service as a data source to Reporting Engine to generate report for the data collected by Workbench.

Prerequisites

Make sure you have:

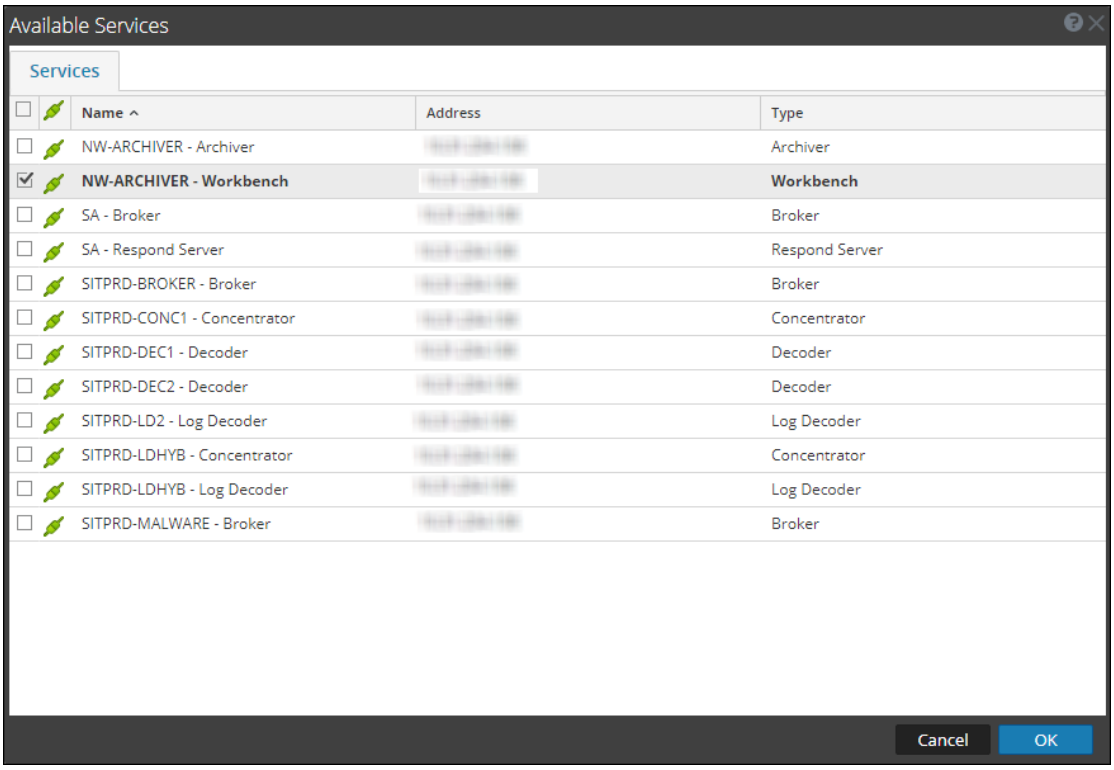
1. Added Workbench as a service to your NetWitness Suite deployment. For more information, see the *Archiver Configuration Guide*.
2. Added a Collection on the Workbench service.

To add Workbench as a data source to Reporting Engine:

1. Go to ADMIN > **Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Select > **View** > **Config**.

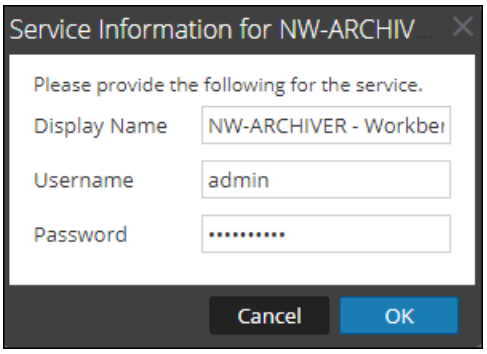
   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click and select **Available Services**.

   The Available Services dialog is displayed:

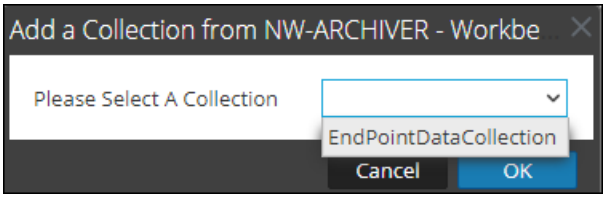


6. Select the Workbench service and click **OK**.
   A list of collections are displayed.

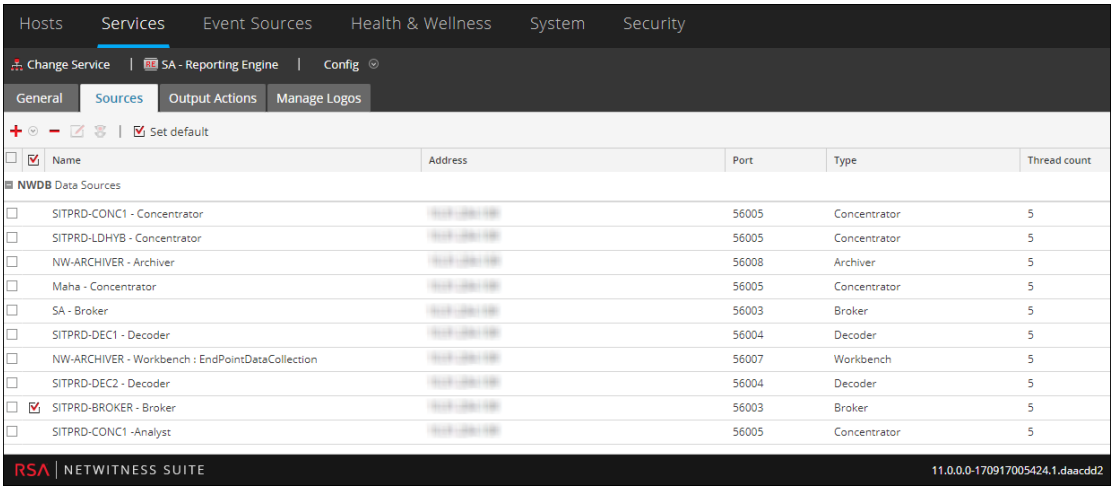
7. Enter the service information, and click **OK**



8. Select a collection from the dropdown.



9. The data source is displayed in the Sources tab.



The workbench service is now added as a data source to the Reporting Engine.

Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

(Optional) Add Archiver as Data Source

You have to carry out the following Archiver configurations to you to be able to use data from Archiver data source to generate Reports and Alerts:

Prerequisites

Ensure that you have:

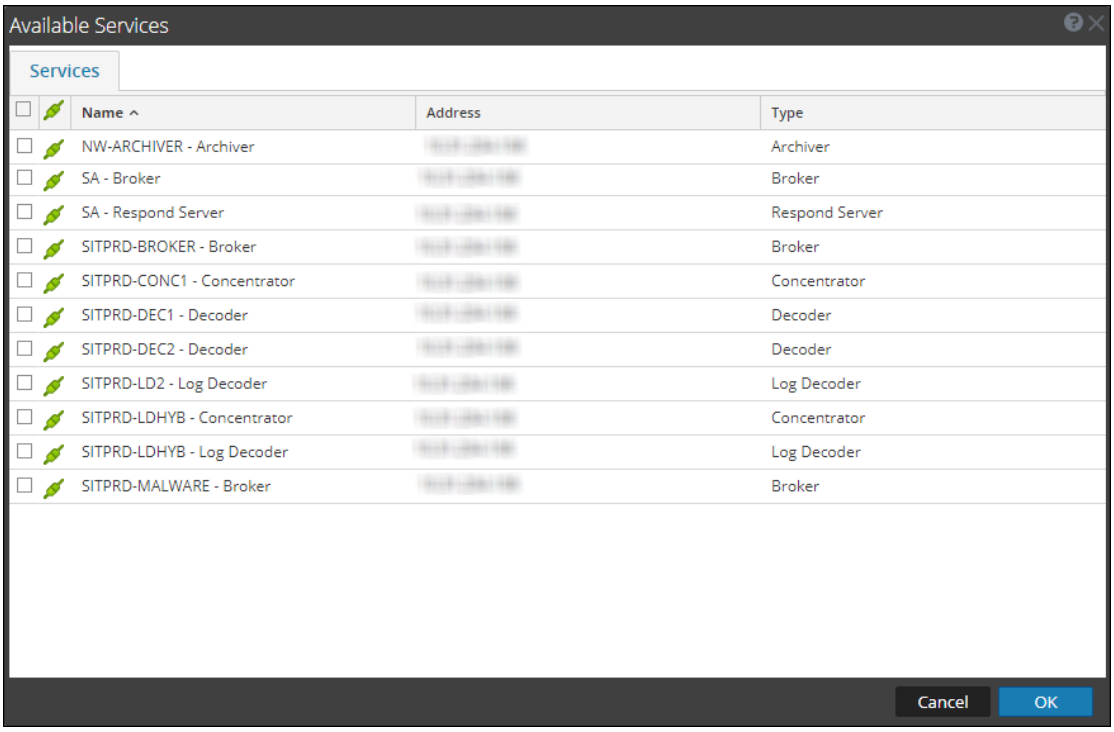
1. Installed the NetWitness Suite Archiver host in your network environment. For more information, see the *Hosts and Services Getting Started Guide*.
2. Installed and configured Log decoder in your network environment. For more information, see "Add Log Decoder as a Data Source to Archiver" in the *Archiver Configuration Guide*.
3. Reporting Engine as a service is available in your NetWitness Suite deployment.
4. Added Archiver as a service to your NetWitness Suite deployment. For more information, see "Add the Archiver Service" in the *Archiver Configuration Guide*.
5. Applied license to the Archiver service.

To add Archiver Data Source to Reporting Engine:

1. Go to **ADMIN** > **Services**.
2. In the **Services** list, select the **Reporting Engine** service.
3. Click > **View** > **Config**.

   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Archiver service and click **OK**.

   The service authentication dialog box is displayed.

   Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

7. Type the Username and Password for the Archiver.
8. Click **OK**.

   The selected Archiver is listed in the Aggregate Services pane.

(Optional) Integrate Endpoint Information Into Reports

You can use the Endpoint data by using the following instructions and adding the Endpoint information into Reports. *Endpoint Integration Guide* provides an overview of Endpoint integration into RSA NetWitness Suite.

Prerequisites

Make sure that:

- You have configured the Endpoint alerts via syslog into a Log Decoder. For more information see, "Configure Endpoint Alerts Via Syslog into a Log Decoder" topic in *Endpoint Integration Guide*).

To integrate Endpoint information into Reports:

1. In **Reporting Engine**> **View**> **Config**> **Sources**.
2. Add the Concentrator that is consuming data from the Log Decoder as a data source. Endpoint meta is populated in Reporting Engine.
3. Run reports by selecting the appropriate meta.

(Optional) Add Collection as Data Source to Reporting Engine

You have to carry out the following Collection configurations for you to be able to use data from Collection data source to generate Reports, Charts, and Alerts:

Prerequisites

Make sure that you have:

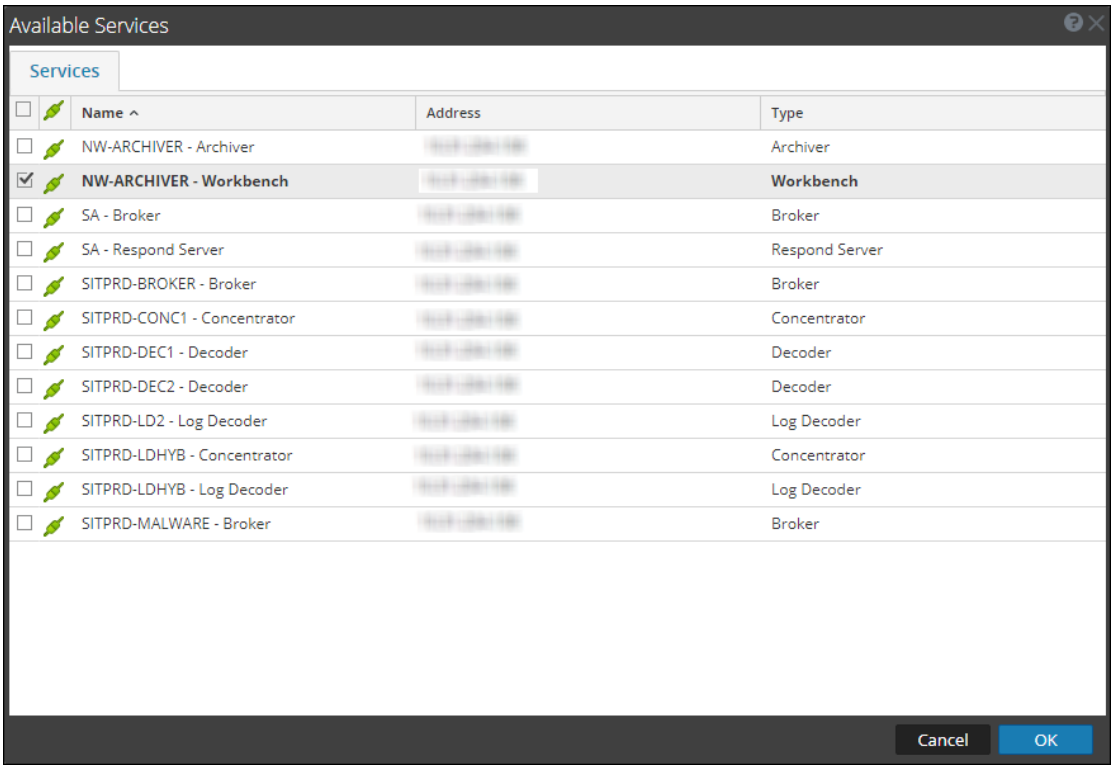
- Installed a Workbench service on a Reporting Engine host.
- Backed up data in a known location on your local host, if you are adding a collection using the data restored from the backed up data.

To associate a Collection as a data source with Reporting Engine:

1. Go to **ADMIN** > **Services**.
2. In the **Services** list , select a **Reporting Engine** service.
3. Click > **View** > **Config**.

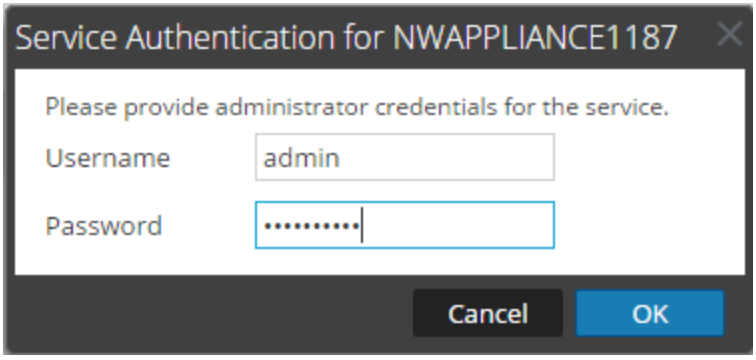
   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Workbench service and click **OK**.

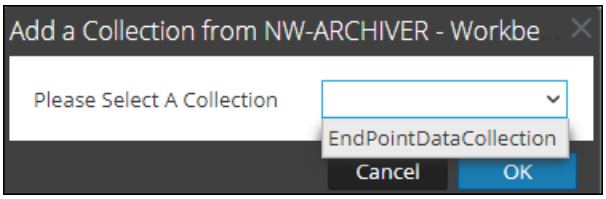
   The Service Authentication dialog for the selected service is displayed.



Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

7. Type the username and password for admin credentials for the service.
8. Click **OK**.

   The add collection dialog is displayed.



9. Select a collection from the drop-down list and click **OK**.

   The workbench service is now added as a data source to the Reporting Engine.

Configure Data Privacy for the Reporting Engine

You can configure the data privacy for all data sources of Reporting Engine using the Sources tab of the Services > View > Config view.

With the addition of the Data Privacy feature to NetWitness Suite 11.0 and above, access to sensitive meta in NetWitness Suite Core services can be restricted by configuring separate data sources for Data Privacy Officer (DPO) users and non-DPO users, and limiting access to those data sources by assigning appropriate permissions.

In the Services Config view, you can add each Core service as two separate data sources: one with a service account having privileges equivalent to a DPO and the other with a service account having privileges equivalent to any other user. Then, to limit access to those data sources based on roles, you can assign read access or no access to those data sources for individual roles. To limit access to Warehouse data sources, you can do the same.

For more information, see Configure Data Source Permissions.

Note: A user assigned to the `Data_Privacy_Officers` role (or an equivalent custom role), can create a report, chart and alert. Also, configure a report or alert output actions in the Reporting module. In an environment where data privacy features of NetWitness Suite are enabled and one or more meta keys are configured as protected, these actions can result in the following:
- When an alert is created by a DPO user, any protected or sensitive meta involved in the alert is automatically available in Respond. This may inadvertently provide all the users of Respond module access to the sensitive meta values, regardless of their roles. One option to prevent this is to disable publishing into Respond from Reporting.
- When an Output Action is configured by a DPO user, either sensitive meta values, reports with sensitive meta values or both, may become available to target users or destinations of that Output Action, regardless of the role assigned to the target user.

It is strongly recommended that DPO users completely avoid creating alerts or configuring output actions for a report or alert in the Reporting module. If they do such configuration, the above implications must be carefully considered.

NetWitness Suite Core services (for example, Concentrator, Broker, or Archiver) support the ability to restrict meta data based on the configured user role. To make use of the data privacy feature for Reporting Engine, you can configure two separate service accounts against Core. One service account for general purpose reporting that does not include any sensitive data and the other account for privileged users with access to all data including sensitive data. The access to restricted meta data for the two service accounts is configured as part of the data privacy plan on each Core service.

In Reporting Engine, you can add each Core service as two separate data sources (one being the regular data source and the other a privileged data source) using the two separate service accounts. You can configure Reporting Engine to allow only users with privileged roles to access the sensitive data source. Hence, Reporting Engine can connect to a NWDB Data source in two ways:

- Using a service account with DPO role.
- Using a service account without a DPO role.

Note: You can also add two or multiple data sources for the same Core service.

After adding two data sources with different service accounts for the same Core service, you can configure data source permissions to manage access to these data sources. For more information, see Configure Data Source Permissions.

Note: If the content is changed to utilize the transformed meta key, the hash value of the original meta is displayed in its place when viewing reports, charts and alerts.

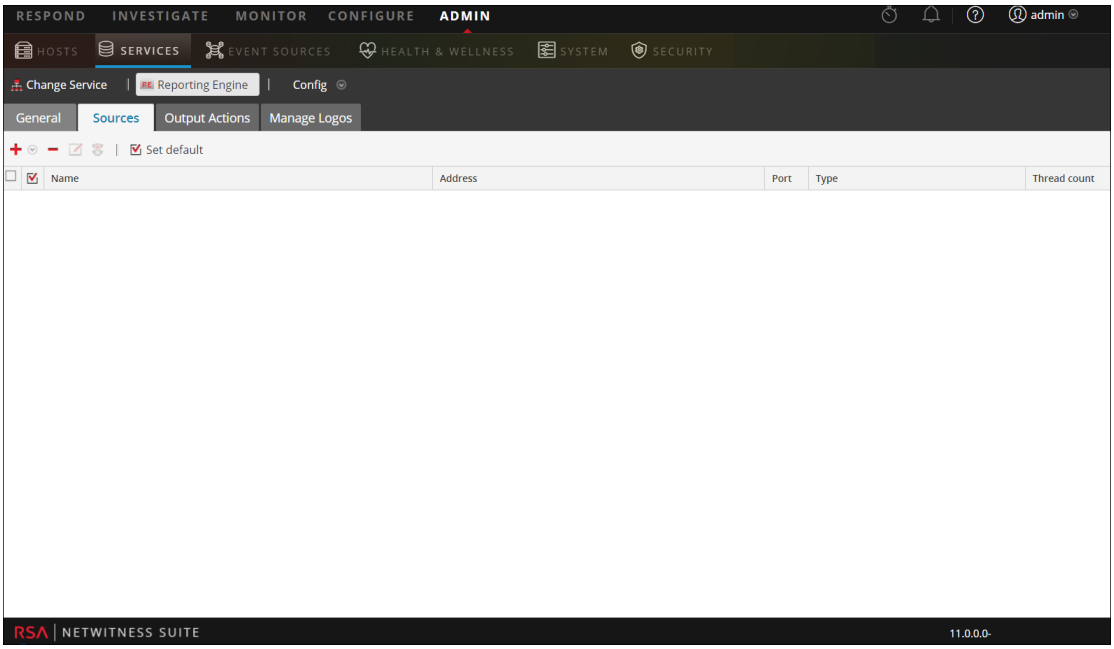
Add a NWDB Data Source with Different Service Accounts

To add a NWDB data source:

1. Go to **ADMIN** > **Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Click **View** > **Config**.

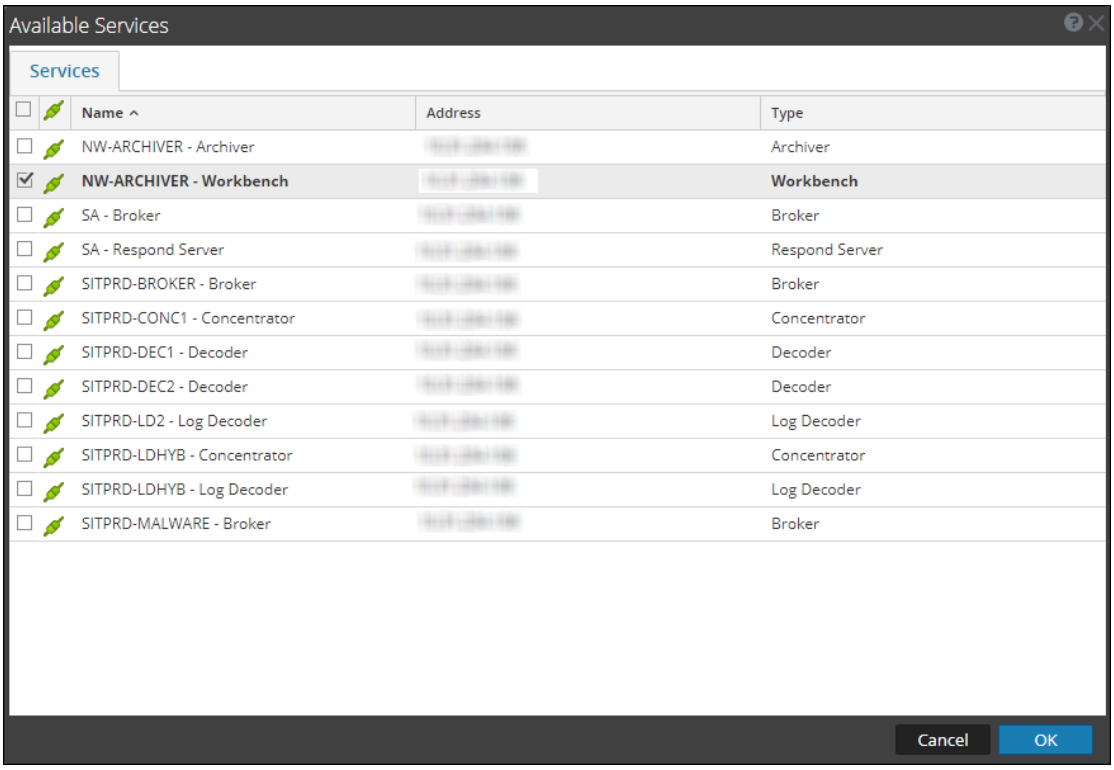
   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Services Config View is displayed.



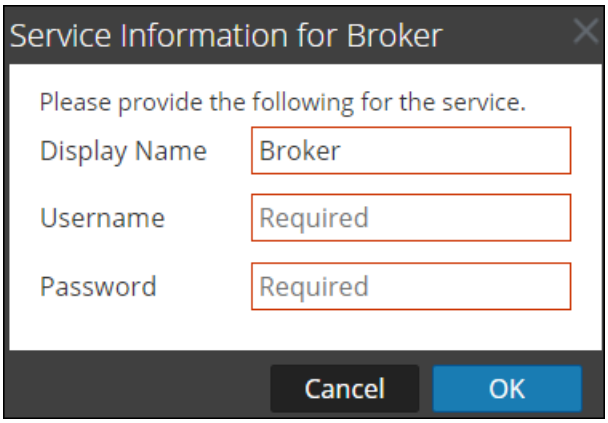
5. Click + and select Available Services.

   The Available Services dialog is displayed. All services are listed, including those that have already been added to the Reporting Engine.



6. Select the checkbox next to the service and click **OK**.

   The Service Information dialog for the selected service is displayed.

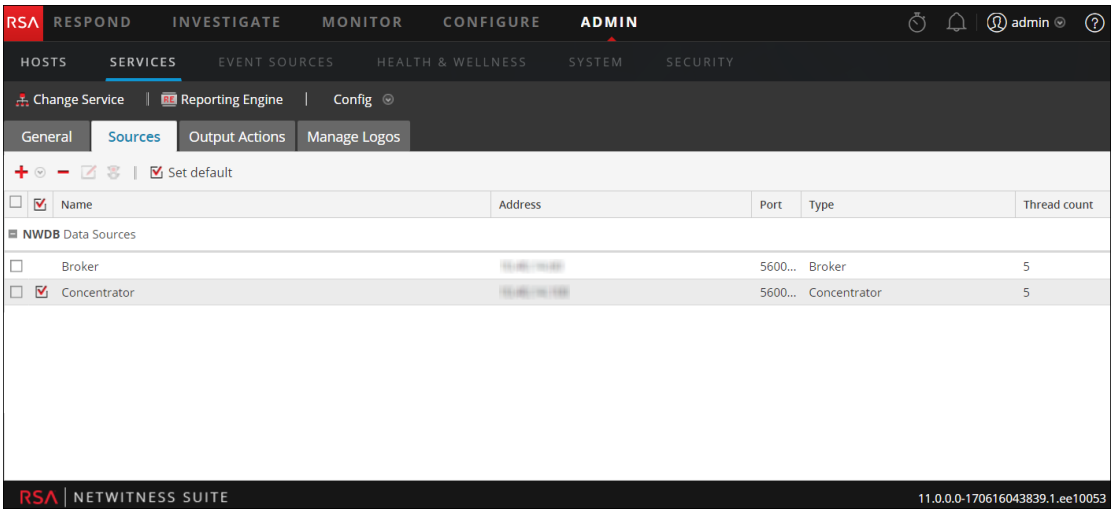


Note: NetWitness Suite prompts you to provide a username and password for the selected service. To limit access to sensitive data, DPO users must use their credentials while adding the source instead of using the admin credentials. These credentials need to be applied to the host even if using trusted connections between the NetWitness Suite server and NetWitness Suite Core hosts.

Repeat the step for Non-DPO data source.

7. Type the username and password for the required service account.
8. Click **OK**.

   The required service is added as a data source to the Reporting Engine. Two data sources are added to Reporting Engine for the same Core device.



Configure Data Source Permissions

You can configure data source permissions using the Sources tab of the Services Config view for the Reporting Engine. This helps manage access control to the data sources by setting the data source permissions. Now, with the ability to add more than one data source for the same Core service, you can configure different permissions to each data source of the same Core service. For example, data privacy officers (DPO) can create a Warehouse source using their credentials, and that allows them to execute reports against the Warehouse while restricting everyone else from being able to use that source.

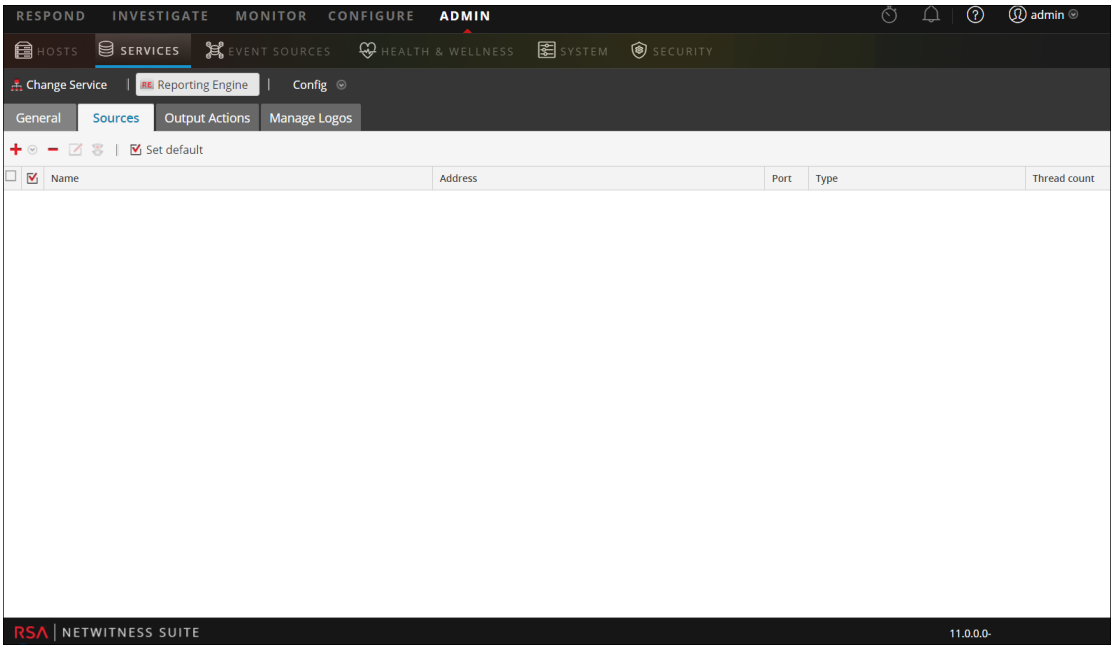
Note: In 11.0, the permissions for NWDB and Warehouse data sources are automatically set based on the permissions of the reporting objects. For example, if the role had the permissions set as **Read Only**/**Read & Write** for any reporting object in 10.5, then that role is automatically assigned read only permission for all the data sources that existed in 10.5. If no permission is set for the role, then the data source permission is automatically set to No Access.

To configure permissions to data sources:

1. Go to **ADMIN** > **Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Click > **View** > **Config**.

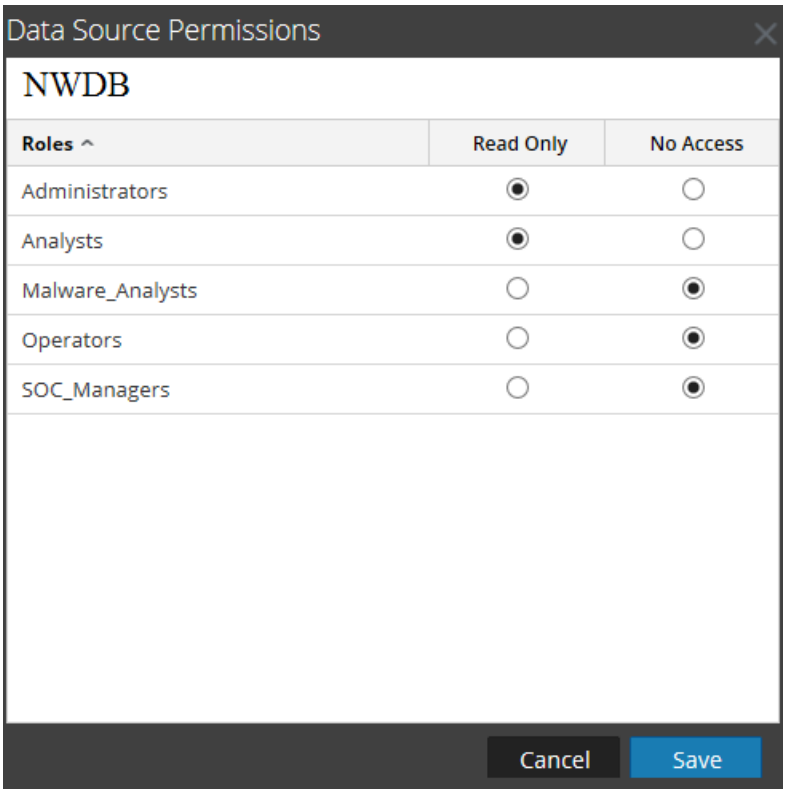
   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Service Config View displays the Sources tab.



5. Select the data source for which you want to configure permissions by selecting the checkbox.
6. Click .

   The Data Source Permissions dialog is displayed.



7. Modify the access permission for different users based on the type of service account of the data source. The permission can be either **Read Only** or **No Access**.
8. Click **Save**.

   The required permissions are configured for the data source.

For more information, see the *Reporting Guide*.

Configure Reporting Engine Settings

After you configure the Reporting Engine and required data sources based on your requirements, you can modify some of the configurations to customize your Reports, Charts, and Alerts.

To configure the settings:

1. Go to **ADMIN** > **Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Click > **View** > **Config**.

   The Services Config View of Reporting Engine is displayed with the General tab highlighted. For more information on Reporting Engine General tab, see General Tab.
4. Edit the Reporting Engine service settings and click **Apply**.

   The service settings are configured on Reporting Engine.

Enable LDAP Authentication

To enable LDAP mode of authentication using Active Directory for HiveServer2 for Warehouse data source, follow these steps.

1. Log on to the RSA Analytics Warehouse appliance as root user.
2. Navigate to `/opt/mapr/hive/hive-0.11/conf.new/` directory. Type the following command and press ENTER:

   ```
   cd /opt/mapr/hive/hive-0.11/conf.new/
   ```
3. Edit the file `hive-site.xml`. Type the following command and press ENTER:

   ```
   vi hive-site.xml
   ```
4. Add the following properties under `<Configuration>` tag:

   ```
   <property>
       <name>hive.server2.authentication</name>
       <value>LDAP</value>
   </property>
   <property>
       <name>hive.server2.authentication.ldap.url</name>
       <value>LDAP_URL</value>
   </property>
   ```

Where `LDAP_URL` is the URL of the LDAP Server.

5. Restart HiveServer2.

Add Additional Space for Large Reports

To add additional disk space to the Reporting Engine for large reports, follow the below steps. If large compliance reports have to be generated for Warehouse, the Reporting Engine disk space might get consumed quicker than expected. In such cases, you can mount any external storage such as SAN or NAS for storing reports.

The directories that tend to fill up disk space are `resultstore` and `formattedReports` under the Reporting Engine home directory. It is recommended to move only these two directories to SAN or NAS and replace the original locations with soft links pointing to the new locations. It is also recommended to leave the remaining directories in the local disk itself for reliable and high I/O performance.

Note: The following steps assume that the Reporting Engine home directory is located at `/var/netwitness/re-server/rsa/soc/reporting-engine/` and the external storage is mounted under `/externalStorage/`. Also, the 'rsasoc' user must have read-write access to the specified external storage path.

To move disk space for the Reporting Engine to external storage:

1. Stop Reporting Engine service as a root user.

   ```
   service rsasoc_re stop
   ```

2. Switch to `rsasoc` user.

   ```
   su rsasoc
   ```

3. Change to RE home directory.

   ```
   cd /var/netwitness/re-server/rsa/soc/reporting-engine/
   ```

4. Move the resultstore directory to a mounted external storage. Type the following command and press ENTER:

   ```
   mv resultstore /externalStorage
   ```

5. Move the formatted Reports directory to a mounted external storage. Type the following command and press ENTER:

   ```
   mv formattedReports /externalStorage
   ```

6. Create a soft link for resultstore. Type the following command and press ENTER:

   ```
   ln -s /externalStorage/resultstore /var/netwitness/re-server/rsa/soc/reporting-engine/resultstore
   ```

7. Create a softlink for formattedReports. Type the following command and press ENTER:

```
ln -s /externalStorage/formattedReports /var/netwitness/re-server/rsa/soc/reporting-engine/formattedReports
```

8. Exit the `rsasoc` user.

   ```
   exit
   ```

9. Start Reporting Engine service as a root user.

   ```
   service rsasoc_re start
   ```

   Note: If the external storage is offline, you cannot perform the following tasks:
   1) Execute Reports or Reporting Alerts
   2) View existing Reports or Reporting Alerts
   However, you can create new Reporting objects such as Reports and Charts, and access Charts and Live Dashboard created for charts. Therefore, you must ensure that the external storage is reliable and has the required space.

   Additionally, if you want to store reports beyond 100 days, change the retention configuration appropriately in the Configure Reporting Engine Settings.

Accessing Reporting Engine Log Files

You can access the Reporting Engine log files which are stored in the following logs directory `/var/netwitness/re-server/rsa/soc/reporting-engine/logs/`

- Current logs in the `reporting-engine.log` file.
- Backup copies of previous logs in the `reporting-engine.log.*` file.
- All UNIX script logs in the files that have the following syntax: `reporting-engine.sh_timestamp.log` (for example, `reporting-engine.sh_20120921.log`)

The Reporting Engine rarely writes command line error messages to the **rsasoc/nohup.out** file.

The Reporting Engine appends the log messages and output written by systemd system and the commands used to start the reporting-engine to the directory `/var/log/messages`.
A `/var/log/messages` log file is a system log file so only the root user can read it.

Configuring Task Scheduler for a Reporting Engine

You can configure queues and pools in the reporting engine to schedule NWDB or Warehouse reports. For more information on Task Schedulers, see "Task Scheduler for Warehouse Reporting" in the *Reporting Guide*

Prerequisites

Make sure that you have identified the following:

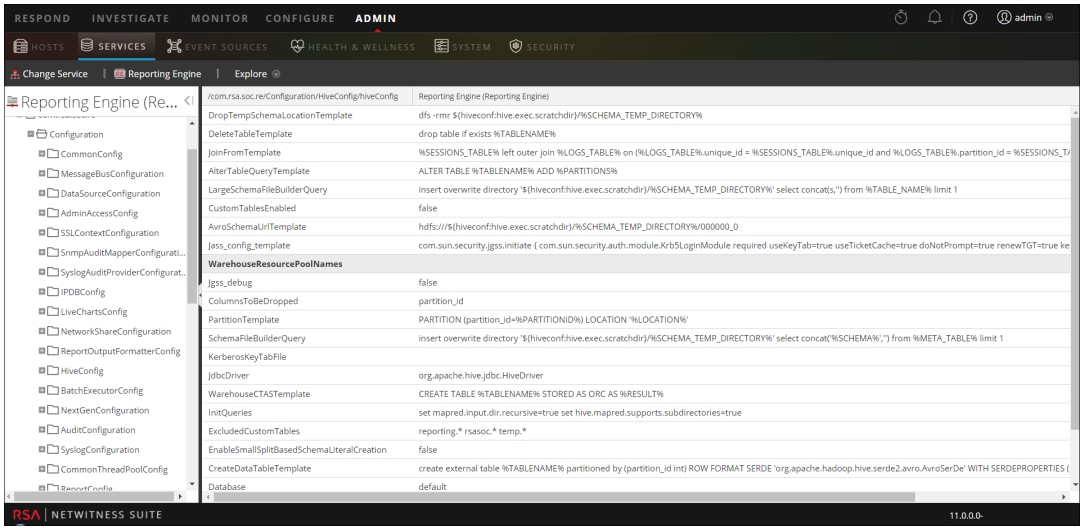
- Scheduler type and pools or queues you want to use. You can configure only one scheduler for the Reporting Engine. By default the Fair Scheduler is configured.
- Names of the queues or pools, and the resources given to each queue and pool.
- NetWitness Suite does not support multiple queues or pools per cluster. RSA recommends that you either provide unique names to queues or pools in all the clusters or use the same queue or pool names in both the clusters. If cluster size is large, there may be more than 3 pools or queues.
- If you are using an unsupported scheduler, the Reporting Engine does not set any property for the jobs that it launches.
- If the name of the pool or queue does not exist in the cluster, then Capacity Scheduler will use the default queue for the report. The Fair Scheduler may not execute the rule or it will create a new pool with the lowest share. This is based on the value specified for the Fair Scheduler property `mapred.fairscheduler.allow.undeclared.pools`.
- If you do not specify a pool or queue, the job launched by the test rule is in the `mapr` pool or the default queue. RSA recommends that you configure a pool mapr with low (around 1/10 of total capacity) share with `maxRunningJobs = 2` so that these rules do not disrupt running reports. Make sure that you do not specify this pool name for any reports.

Specify the Pools and Queues

To specify the pools and queues:

1. Go to **ADMIN** > **Services**.
2. Select **Reporting Engine** and click > **View** > **Explore**.
3. Select **com.rsa.soc.re** > **Configuration** > **HiveConfig** > **hiveconfig** > **WarehouseResourcePoolNames**.
4. In the **WarehouseResourcePoolNames** field, enter the pool or queue names separated by spaces. For example, to configure four pools or queues with the names pool1, pool2,

wrong and default, enter the names separated by a space.



Define Reports, Charts, and Alerts

After you configure the Reporting Engine and required data source based on your requirement, you can generate your Reports, Charts, and Alerts.

Define Reports, Charts, and Alerts

How to define Reports

After creating the data sources and configuring the user permissions to these data sources, you can now use these data sources to perform the following tasks for Reporting module:

- **Define a Rule**
- **Test a Rule**
- **Schedule Reports**
- **Add an Alert**
- **Add a Chart**
- **Test a Chart**

For more information, see the above topics in the *RSA Netwitness Reporting Reports Guide*.

How to define Charts

After creating the data sources and configuring the user permissions to these data sources, you can now use these data sources to perform the following tasks for Reporting module:

- **Define a Chart and Chart Groups**
- **Test a Chart**
- **Investigate Charts**
- **Manage Charts**

For more information, see the above topics in the *RSA Netwitness Reporting Reports Guide*.

How to define Alerts

After creating the data sources and configuring the user permissions to these data sources, you can now use these data sources to perform the following tasks for Alerting module:

- **Configure Alerts**
- **Generate Alerts**

- **Add an Alert**
- **View an Alert**
- **View Alerts Schedule**
- **Investigate an Alert**

For more information, see the above topics in the *RSA Netwitness Reporting Alerting Guide*.

Configure Reporting Engine General Settings

On adding and configuring the Reporting Engine service, the system settings are defined with default values to achieve optimal results. However, you can modify and customize the Reporting Engine notifications based on your requirement by navigating to the General tab in the Services Config view for a Reporting Engine.

Access the General Tab

You need to open the General tab to configure the general parameters for Reporting Engine.

To access this view:

1. Go to **ADMIN** > **Services**.
2. In the Available Services list, select a **Reporting Engine** service.
3. Click **View** > **Config**.
4. Select the **General** tab.
5. Click **Apply** after you edit the parameters.

After you navigate to the general tab, you can modify the following parameters.

- System Configuration
- Logging Configuration
- Warehouse Analytics Output Configuration
- Warehouse Analytics Model Configuration
- Warehouse Kerberos Configuration

For more information see, General Tab for details on the configuration parameters.

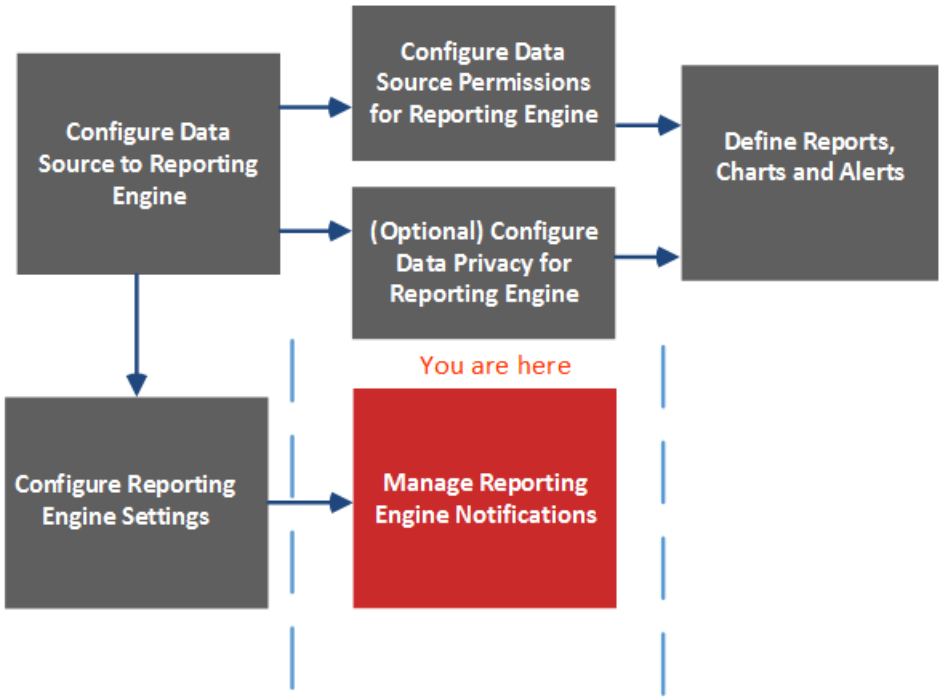
References

To be able to customize and make optimum use of the service, you can modify the Reporting Engine settings in the Services Config view, which has parameters that specifically pertain to the Reporting Engine.

General Tab

The General tab for the Reporting Engine service controls several settings that can tune the performance of a service and specify the user credentials for the service. Navigate to Services > View > Config > Reporting Engine > General. These settings are used for the Reporting Engine service exclusively.

The required permission to access this view is Manage Services.



What do you want to do?

Role	I want to ...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions

Role	I want to …	Refer to…
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts, and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator / SOC Manager	Configure System Settings*	Configure Reporting Engine General Settings
Administrator / SOC Manager	Configure Logging *	Configure Reporting Engine General Settings
Administrator / SOC Manager	Configure Warehouse Analytics Output *	Configure Reporting Engine General Settings
Administrator / SOC Manager	Configure Warehouse Analytics Model *	Configure Reporting Engine General Settings
Administrator / SOC Manager	Configure Warehouse Kerberos *	Configure Reporting Engine General Settings

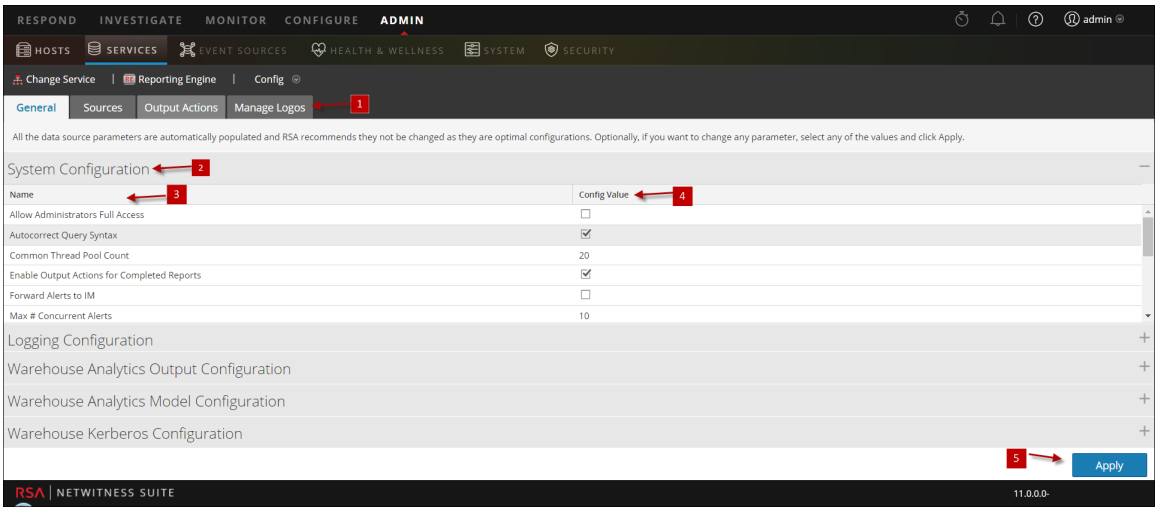
*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look

Here is example of the General tab where service configurations are displayed.



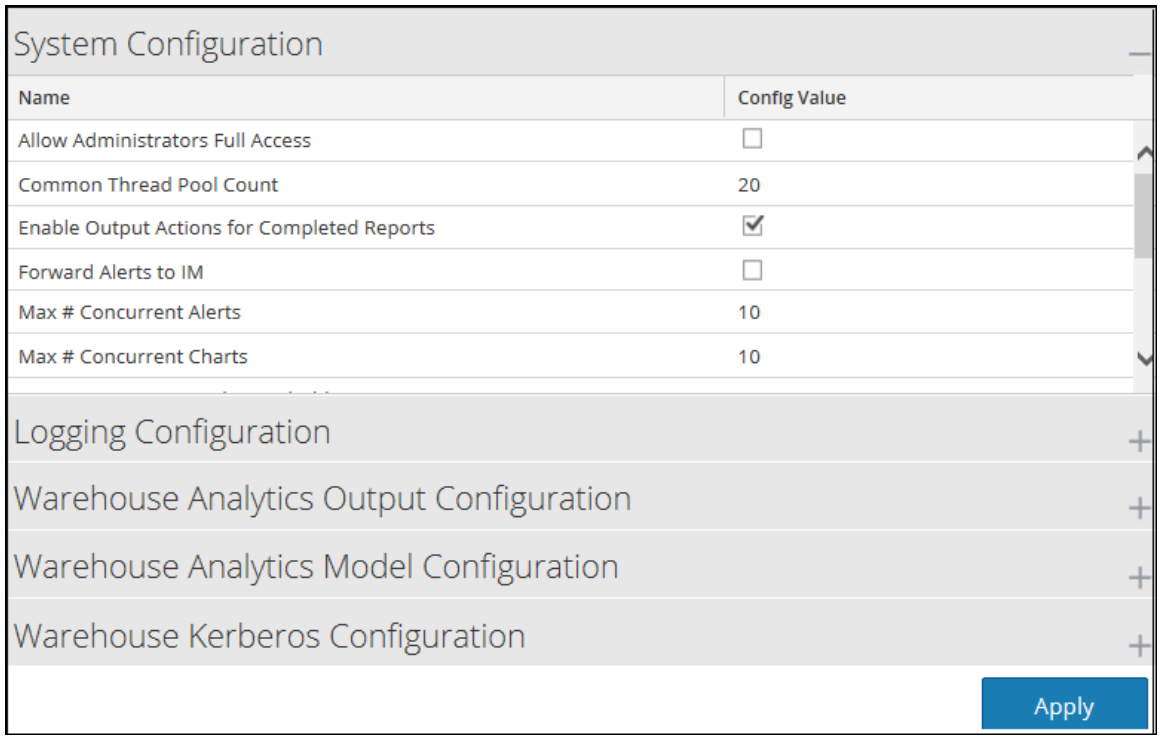
1. Displays all the available configurable tabs.
2. Displays the available configuration parameters for the system.
3. Displays the name of the parameter.
4. Displays the set values for each parameter.
5. Applies the changes.

Note: Warehouse Analytics is not supported in NetWitness Suite11.0 or later release.

System Configuration

The System Configuration panel parameters for the Reporting Engine manage service configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. The default values are designed to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

The following figure displays the fields that can be configured in the System Configuration panel:



The following table describes the System Configuration panel features.

Name	Config Value
Allow Administrators Full Access	Select the checkbox if you want to access all the Reporting Engine objects (Reports, Rule, Charts, Schedule, and List) created by other users (non-admin). By default, this is not enabled. **Note:** If you enable the checkbox and then disable it, the access on all Reporting Engine objects that were enabled by selecting the checkbox will not be accessible. But, if you have defined the access on specific objects via Permissions window (**Reports > Manage > RE Object >** > **Permissions**), enabling/disabling this checkbox will not have impact on these objects.
Common thread pool count	The number of thread pools assigned for executing common tasks on the Reporting Engine. A valid value is an integer (**20** default).

Name	Config Value
Enable Output Actions for Completed Reports	Select the checkbox to process the output actions only for reports with all rule executions successful. By default, this is enabled. If disabled, the output actions are processed for all scenarios (completed, partial, failure).
Forward Alerts to Respond	Select the checkbox to forward all the alerts to Respond. By default, this is not enabled.
Max# of Concurrent Alerts	The maximum number of alerts that can be run simultaneously. This has a direct impact on the RSA service against which the alerts are run, as each alert consumes a query thread on the RSA service. A valid value is an integer (**10** default).
Max # of Concurrent Charts	The maximum number of charts that can be run simultaneously. A valid value is an integer (**10** default).
Max # of Concurrent LookupAndAdd Queries	The maximum number of parallel LookupAndAdd Queries that can be run per NWDB rule. A valid value is an integer (**2** default). When you increase this value, for better performance, you must ensure the NWDB data source is configured to handle the parallel queries.
Max # Concurrent List Value Reports	The maximum number of list value reports per schedule that can be generated in parallel. A valid value is an integer (**1** default).
Max # List Value Reports	The maximum number of list value reports generated, irrespective of the number of values in the list. A valid value is an integer (**10000** default).

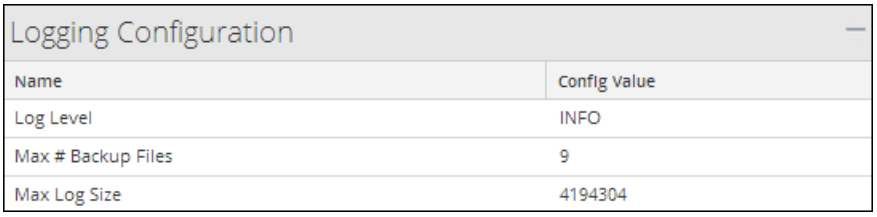
Name	Config Value
Max rows stored per Rule (Billions)	The maximum number of rows that a rule can fetch when queried. A valid value is an integer (**100** default).
Maximum disk space threshold	The maximum disk space threshold allotted (in GB) to execute reports, alerts and charts. The initial value is configured based on the available system space.
Minimum disk space threshold	The minimum disk space threshold allotted (in percentage) required to execute reports, charts, and alerts. By default, this is value is set to 5. **Note:** Note: If the minimum threshold is reached, then the execution of reports, charts and alerts will stop even if the service is running.
NWDB Info Queries Time Out	The info queries time out in seconds for NWDB server. A valid value is an integer (**0** default).
NWDB Maximum aggregate Rows	The maximum number of rows that is returned when an aggregation is used in the NWDB rule. A valid value is an integer (**1000** default).
NWDB Query Time out	The time out in seconds for NWDB server to time out the rule execution, if it cannot process the result in configured time. The default value is set to 0 which implies that there is no time out. A valid value is an integer.
Process output actions for successful reports only	Select this checkbox to process output actions only for reports whose all rule executions are successful. When you de-select this checkbox, output action will be triggered for partial, completed, and failed reports. **Note:** This is applicable for all output actions except for dynamic list output actions.

Name	Config Value
Retain Alert history for # days	The maximum number of days to retain the alert history and alert status. A valid value is an integer (**100** default).
Retain Chart history for # days	The maximum number of days to retain the chart history and chart status. A valid value is an integer (**30** default).
Retain Report history for # days	The maximum number of days the system retains report history and report status. A valid value is an integer (**100** default).
Schedule Thread pool count	The number of thread pools assigned for scheduled tasks (for example, clearing history) on the Reporting Engine. A valid value is an integer (**5** default).

Logging Configuration

The Logging Configuration panel parameters of the Reporting Engine manages the logging configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance of the Reporting Engine.

The following figure displays the fields that can be configured in the Logging Configuration panel.



The following table describes the Logging Configuration panel features.

Name	Config Value
Log Level	The logging level that determines the scope of information included in log files. Possible values are: • ERROR • WARN • INFO (default) • DEBUG • ALL
Maximum # Backup Files	The maximum number of backup log files the system retains. A valid value is an integer (**9** default).
Max Log Size	The maximum size (in bytes) of the primary log file. A valid value is an integer (**4194304** default).

For more information on Reporting Engine logging, see Accessing Reporting Engine Log Files.

Warehouse Analytics Output Configuration

Note: Warehouse Analytics is not supported in Netwitness Suite 11.0 release.

The Warehouse Analytics Output Configuration panel provides a way to specify the Warehouse Analytics Output configuration on this Reporting Engine.

The following figure displays the fields that can be configured in the Warehouse Analytics Output Configuration panel:

After an upgrade, make sure you update the centralized **Mongo DB** details to be able to use Warehouse Analytics.

The following table describes the Warehouse Analytics Output Configuration panel features.

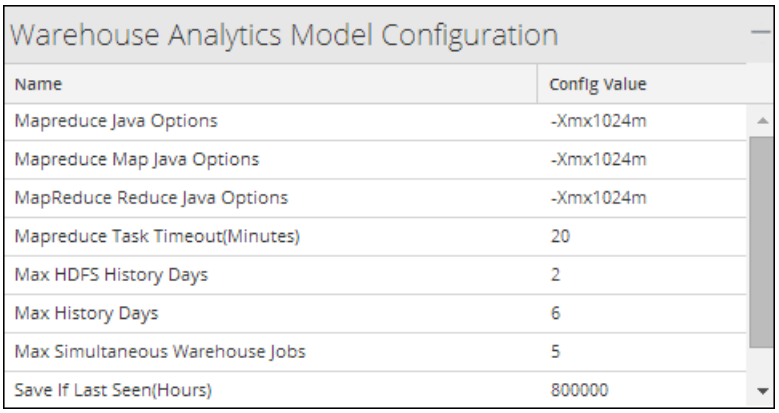
Name	Config Value
Name	**Config Value**
Username	The username for the warehouse analytics user.
Port	The port of the Mongo DB used by warehouse analytics.
Host	The host of the Mongo DB used by warehouse analytics.

Name	Config Value
Password	The password for the warehouse analytics user.

Warehouse Analytics Model Configuration

The Warehouse Analytics Model Configuration panel provides a way to specify the Warehouse Analytics Model configuration on this Reporting Engine.

The following figure shows the fields that can be configured in the Warehouse Analytics Model Configuration panel:



The following table describes the Warehouse Analytics Model Configuration panel features:

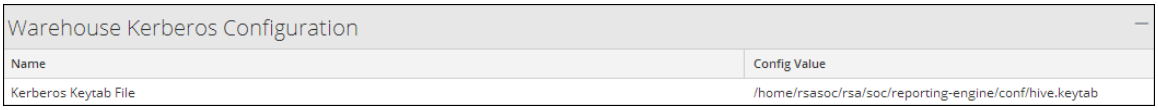
Name	Config Value
Mapreduce Java Options	The JVM Parameters for Hadoop MapReduce task tracker child JVM. By default, the value is **-Xmx1024m**.
Mapreduce Map Java Options	The parameter which controls the JVM parameters for Map jobs inside the Hadoop cluster. By default, the value is **-Xmx1024m**.
MapReduce Reduce Java Options	The parameter which controls the JVM parameters for Reduce jobs inside the Hadoop cluster. By default, the value is **-Xmx1024m**.

Name	Config Value
Mapreduce Task Timeout (Minutes)	The number of minutes before a task is terminated when a MapReduce framework titles it as non-responsive or idle. A valid value is an integer (**20** default).
Max HDFS History Days	The maximum number of days to maintain the temporary and output files of the job in HDFS. A valid value is an integer (**2** default).
Max History Days	The maximum number of days to maintain the job output in Mongo DB. A valid value is an integer (**6** default).
Max Simultaneous Warehouse Jobs	The parameter which controls the maximum number of parallel jobs executed through the Warehouse Analytics framework. A valid value is an integer (**1** default).
Save If Last Seen (Hours)	The parameter to save the keys from the job output is they were not seen in the last 'n' hours. A valid value is an integer (**800000** default).
Threshold Score	The parameter to save the keys from the job output to watchlists for use by ESA only if the score is greater than 'n'. A valid value is an integer (**55** default).

Warehouse Kerberos Configuration

The Warehouse Kerberos Configuration panel provides a way to specify the Kerberos Keytab file on this Reporting Engine.

The following figure displays the field that can be configured in the Warehouse Kerberos Configuration panel:



The following table describes the Kerberos Configuration panel features:

Name	Config Value
Kerberos Keytab File	The Kerberos keytab file location. For example, `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/hive.keytab`.

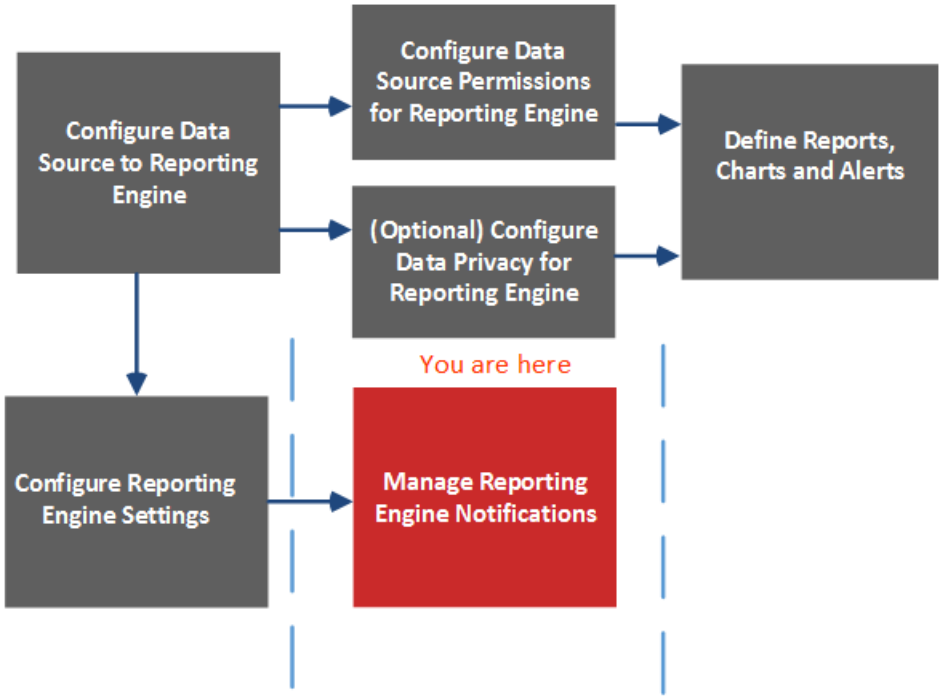
The default Kerberos configuration file is located at, `/etc/kbr5.conf` in the Reporting Engine. You can modify the configuration file to provide details for Kerberos realms and other parameters related to Kerberos.

Added the host name (or FQDN) and IP address of the Horton Works nodes and Warehouse Connector to the DNS server. If the DNS server is not configured, add the host name (or FQDN) and IP address of the Horton Works nodes and Warehouse Connector to the `/etc/hosts` file in the host on which the Warehouse Connector service is installed.

Sources Tab

The services configuration parameters are available in the Sources tab of the Services Config view for the Reporting Engine. The Sources tab for the Reporting Engine service in the Services Config view controls that data sources associated with a Reporting Engine. The Source tab consists of a single panel with a toolbar and a grid that lists the data sources associated with the Reporting Engine.

Workflow



Role	I want to…	Refer to…
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions

Role	I want to...	Refer to...
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts, and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator	Add, delete or edit a new or available service*	Configure the Data Sources
Administrator	Set a data source as default*	Configure the Data Sources
Administrator	Configure data source permissions*	Configure Data Source Permissions

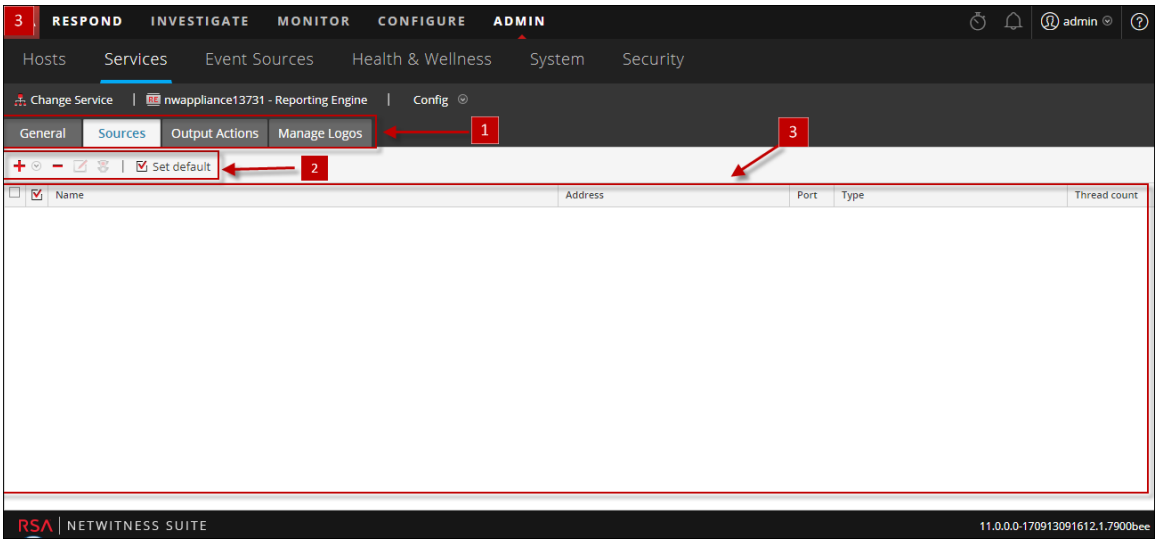
*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look

Here is example of the Sources tab where the available services are displayed.



1 Displays all the available configurable tabs.

2 Displays the available configuration parameters for the selected service .

3 Displays the field parameters for the selected service.

The data sources available to the Reporting Engine for which you are defining reports, charts and defining alerts are:

- **NWDB Data Sources** - The NetWitness Database (NWDB) data sources are Decoders, Log Decoders, Brokers, Concentrators, Archiver, and Collection.

  Note: When a data privacy plan has been implemented to limit access to sensitive data on a data source, you must configure different service accounts in Reporting Engine for privileged and non-privileged users. To configure different service accounts for data privacy, you can add more than one NWDB data source. This procedure is available under Configure Reporting Engine Settings.

- **Warehouse Data Sources** - The Warehouse data sources are Horton Works and MapR.
- **Respond Data Sources** - Respond is used to generate reports on alerts and incidents. The Respond data sources are Reporting Engine, ESA, Malware, EndPoint, and Web Threat Detection. Respond is used to store the alerts and incidents reports.

If you set a source as the default data source, NetWitness Suite uses that source when you create reports and alerts unless you choose to override it with one of the other sources listed in this tab.

Note: You can manage access control to NWDB and Warehouse Data Sources. For more information, see Configure Reporting Engine Settings.

Features

You can perform the following actions on the Sources tab:

Icon	Actions
	This option adds new services as data sources for Reporting Engine. Add existing services (Archiver, Workbench, and Collection) as data sources for Reporting Engine.
	This option removes data sources from a Reporting Engine.
	This option configures the Data Source Permissions. This is enabled only for NWDB and Warehouse Data Sources. For more information, see Configure Data Source Permissions.
	This option sets the default data sources for a Reporting Engine. This is the source to which NetWitness Suite defaults in the **Data source** field of the following views: • Rule Definition view. • Create or Modify Alert view.

The NetWitness Suite data sources are listed under the different categories as follows:

- NWDB Data Sources category displays the NetWitness data sources.
- Warehouse Data Sources category displays the Warehouse data sources.

Column	Description
	Clicking the check box selects the data source. After you select it, you can use toolbar to remove the source or set the source as the default.
Name	Displays the name of the data source.
Address	Displays the IP Address of the data source.

Column	Description
Port	Displays the port of the data source.
Type	Displays the service type of the data source.
Thread Count	Displays the thread pool size used for executing rules on the data source.

Output Actions Tab

You can configure output actions for a Reporting Engine to determine the format you want the data to be presented to you based on your requirements. The service configuration parameters are available in the Output Actions tab of the Services Config view configured for a report or an alert execution. This tab consists of the following panels:

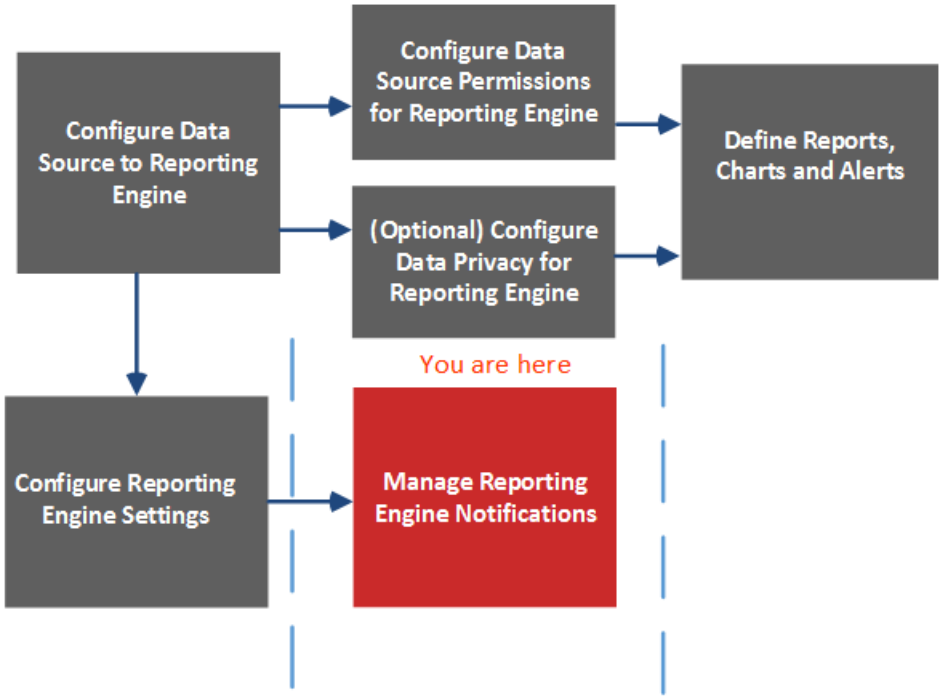
- NetWitness Suite Configuration
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Syslog
- Simple File Transfer Protocol (SFTP)
- Uniform Resource Locator (URL)
- Network Share

For instance, Syslog output action is used specifically for Reporting Engine Alerts, whereas, SFTP, URL, and Network Share output action is used specifically for Reporting Engine Reports.

You can configure the required permission to access this view in Manage Services.

You must ensure that the Reporting Engine is up and running and the data source from which you want to generate a report is configured in the NetWitness Suite.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts, and Alerts

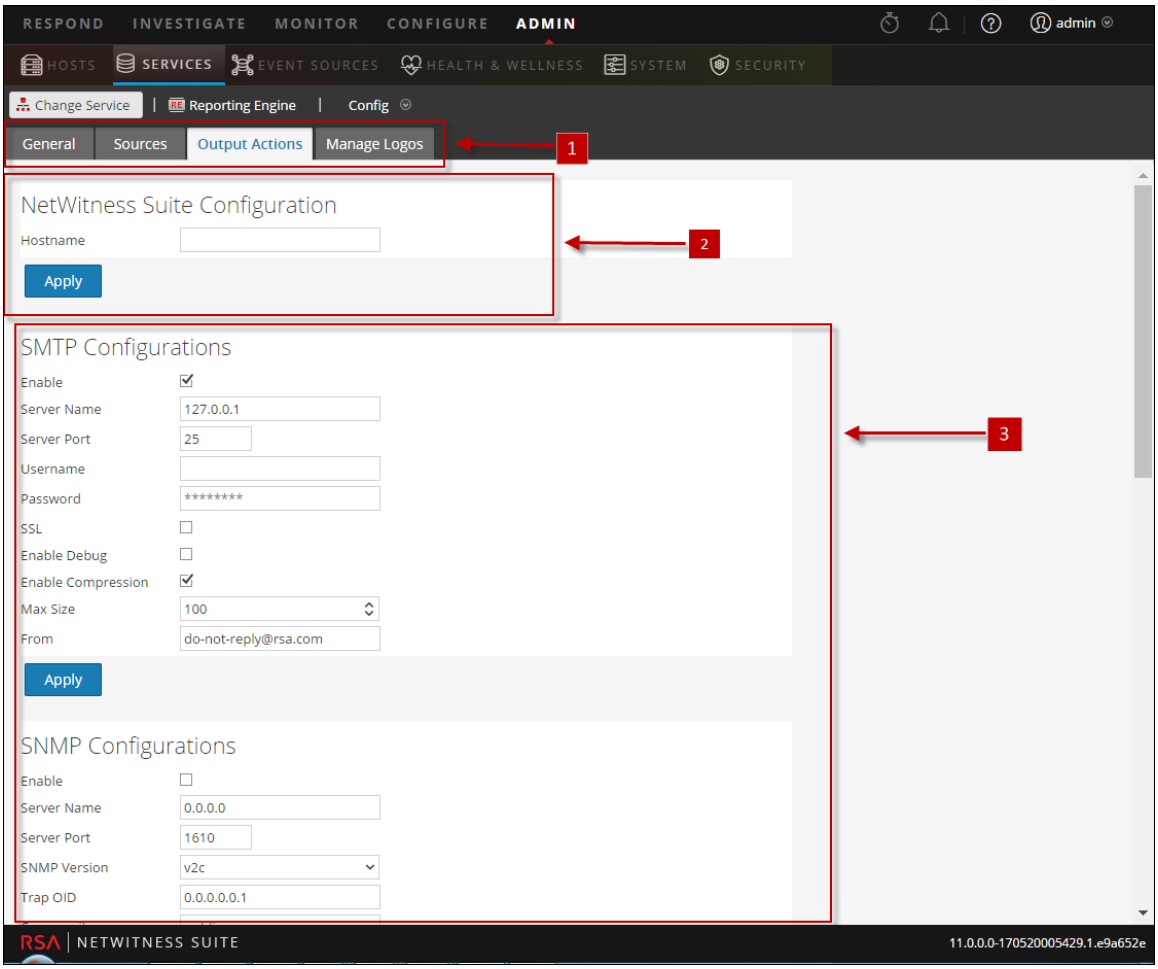
Role	I want to…	Refer to…
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator	Configure Netwitness Suite Configuration *	Configure Reporting Engine General Settings
Administrator	Configure SMTP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure SNMP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure Syslog Configuration*	Configure Reporting Engine General Settings
Administrator	Configure SFTP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure URL Configuration*	Configure Reporting Engine General Settings
Administrator	Configure Network Share Configuration*	Configure Reporting Engine General Settings

*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

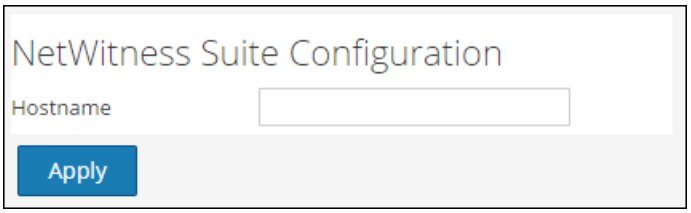
Quick Look



1	Displays all the available configurable tabs.
2	Displays the NetWitness Suite configuration host.
3	Displays all the types of output action that can be configured.

NetWitness Suite Configuration

The following figure shows the NetWitness Suite Configuration on the Output Actions Tab.



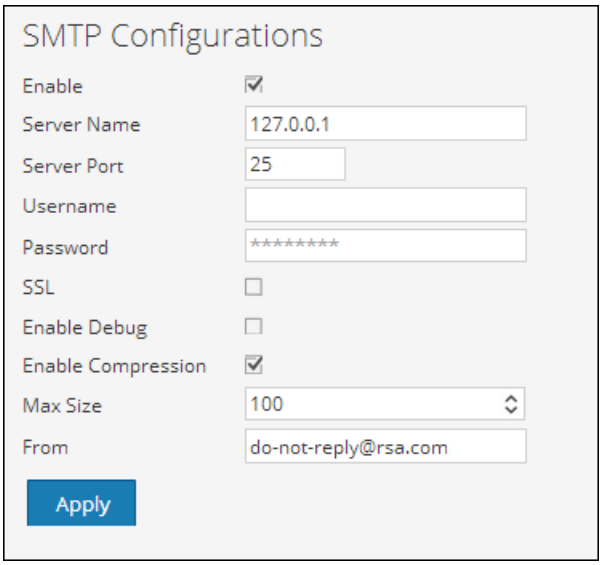
The following parameters identify the NetWitness Suite host that is associated with the Reporting Engine.

Name	Config Value
Host Name	IP Address or Hostname of the NetWitness Suite server. You must specify this parameter for all kind of deployments so that you can refer to this address to create investigation links to NetWitness Suite from Reports, Alerts, and so on. The NetWitness Suite uses this parameter to correctly generate: • SMTP Output Action • SNMP Output Action • Syslog Output Action • SFTP Output Action • URL Output Action • Network Share Output Action • Hyperlinks for meta values in Report PDFs
Apply	Update the configuration.

SMTP

After an execution is completed, an email notification is sent to the user based on the SMTP configuration.

The following figure shows the SMTP Configuration on the Output Actions Tab.



The following parameters manage SMTP (email) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

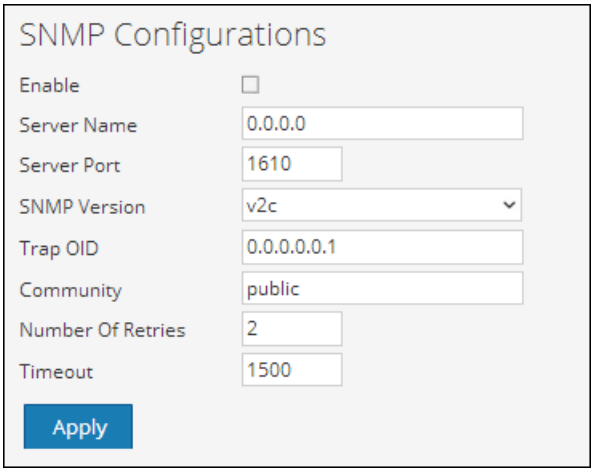
Name	Config Value
Enable	Check this box to enable SMTP as an output action for both alert and report from this Reporting Engine. By default, this value is enabled.
Server Name	Specify the hostname or IP Address of the server on which the target SMTP server runs. Default value is 0.0.0.0.
Server Port	Specify the SMTP server port number. Default value is 25.
Username	Specify the username of your SMTP account. Default value is blank. Password Specify
Password	Specify the password of your SMTP account.
SSL	Check this box to use Secure Socket Layer (SSL) to communicate with the SMTP server. Default value is do not use SSL.

Name	Config Value
Enable Debug	Check this box to enable debugging. Default value is do not enable debug.
Enable Compression	Check this box to enable compression. Default value is enable compression. If this value is enabled, the output files will have `.zip` extension.
Max Size	Specify the maximum size of attachments that can be sent. Default value is 100.
From	Specify the email address from which Security Analytics sends all messages. Default value is `do-not-reply@rsa.com`.
Apply	Update the configuration.

SNMP

After an execution is completed, a trap notification is sent to the user based on the SNMP configuration.

The following figure shows the SNMP Configuration on the Output Actions Tab.



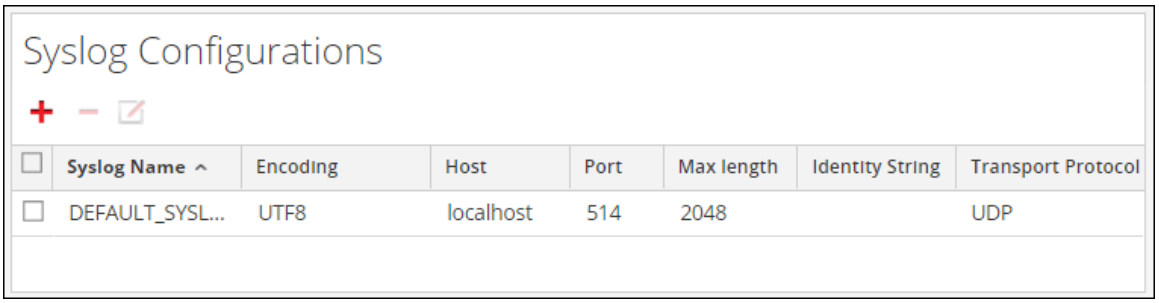
The following parameters manage SNMP (messages to network-attached services) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Enable	Check this box to enable SNMP output action as an output for alert messages from this Reporting Engine. Default value is Disable.
Server Name	Specify the hostname or IP Address of the server on which the target SNMP server runs. Default value is **0.0.0.0**.
Server Port	Specify the port number of the server on which the target SNMP server listens for faults and exceptions. Default value is **1610**.
SNMP Version	Specify the version number of the SNMP protocol NetWitness Suite uses to send SNMP traps.
Trap OID	Specify the object identification number that identifies the type of trap to send. Default value is **0.0.0.0.0.1**.
Community	Specify the SNMP group to which NetWitness Suite belongs. The default value is **public**.
Number Of Retries	Specify the maximum number of times NetWitness Suite tries to resend the alert message through SNMP. Default value is **2**.
Timeout	Specify the number of seconds after which NetWitness Suite times out (stops trying to send SNMP alerts). Default value is **1500**.
Apply	Update the configuration.

Syslog

After an execution is completed, all notifications are sent via Syslog messages to a particular host based on the Syslog configuration. Multiple Syslog servers can be configured on the Syslog Configuration panel.

The following figure displays the Syslog Configuration on the Output Actions Tab.



The following parameters manage syslog output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Syslog Name	The name of the Syslog configuration. **Note:** You cannot create a Syslog configuration with a name that already exists in the Reporting Engine Syslog configuration list.
Encoding	Specify the internationalization encoding for Syslog messages. Default value is **UTF8**.
Server Name	Specify the hostname or IP Address of the server on which the target Syslog process runs. Default value is blank.
Server Port	Specify the port number of the server on which the target Syslog server listens for faults and exceptions. Default value is **514**.
Max Length	Specify the maximum size (in bytes) of each Syslog alert message. Default value is **2048**. If **UDP** is the transport type and the Syslog message size is greater than 1024 bytes, you must configure a Syslog server that supports message sizes greater than 1024 bytes.
Identity String	Specify the string NetWitness Suite inserts as a prefix in all Syslog alert messages. Default value is blank.

Name	Config Value
Include Local Hostname	Check this box to include the local hostname in all Syslog alert messages. Default value is do not include local hostname.
Truncate Message	Check this box to truncate all Syslog alert messages. Default value is do not truncate Syslog messages.
Use Identity	Check this box to use the IDENT protocol. Default value is does not use this protocol.
Include Local Timestamp	Check this box to include the local timestamp in all Syslog alert messages. Default value is do not include local timestamp.
Transport Protocol	Specify the transport type for Syslog message delivery. There are three parts to the Syslog transport type: UDP, TCP, and SECURE_TCP. Default value is **UDP**.
Syslog Message Delimiter	Specify the delimiter for the Syslog message. There are three delimiters: CR, LF, and CRLF. By default the value is **CR**. **Note:** This field populates when you select TCP or SECURE_TCP as the transport protocol.
Trust Store Password	Specify the password for the Trust store. **Note:** This field populates when you select SECURE_TCP as the transport protocol.
Key Store Password	Specify the password for the Key store. **Note:** This field populates when you select SECURE_TCP as the transport protocol.
Apply	Save the configuration.

SFTP

After an execution is completed, you can send or transfer files to a remote location based on the SFTP configuration.

The following figure displays the SFTP Configuration on the Output Actions Tab.

The following parameters manage SFTP (file transfer to a local drive) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

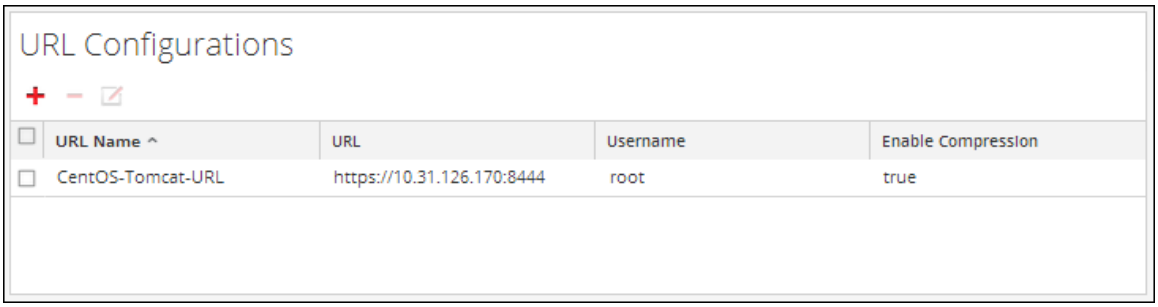
Name	Config Value
SFTP Name	The name of the SFTP configuration. **Note:** You cannot create an SFTP configuration with a name that already exists in the Reporting Engine SFTP configuration list.
Host	The IP Address or Hostname of the Reporting Engine server associated with the file transfer.
Port	If you want to use a different port than the default port, enter a port number. Default value is **22**.
Username	Specify the username for the SFTP configuration.
Password	Specify the password for the SFTP configuration.

Name	Config Value
Custom Folder	Select an SFTP location where you want to transfer the file to. You can use the pre-defined Windows or Linux directory structure in the custom folder path. For example, **/root/Downloaded_Files**. **Note:** If the directory does not exist, RE will create the directory in the custom folder path and copy files to this directory.
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

URL

After an execution is completed, the output files are published to a URL based on the URL configuration.

The following figure shows the URL Configuration on the Output Actions Tab.



The following parameters manage URL (file transfer to a URL) output action configuration for a Reporting Engine service. When you add an Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the Config Values of these parameters according to the requirements of your enterprise.

Name	Config Value
URL Name	The name of the URL configuration. **Note:** You cannot create a URL configuration with a name that already exists in the Reporting Engine URL configuration list.
URL	The URL address associated with the file transfer.

Name	Config Value
Username	Specify the username for the URL configuration.
Password	Specify the password for the URL configuration.
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

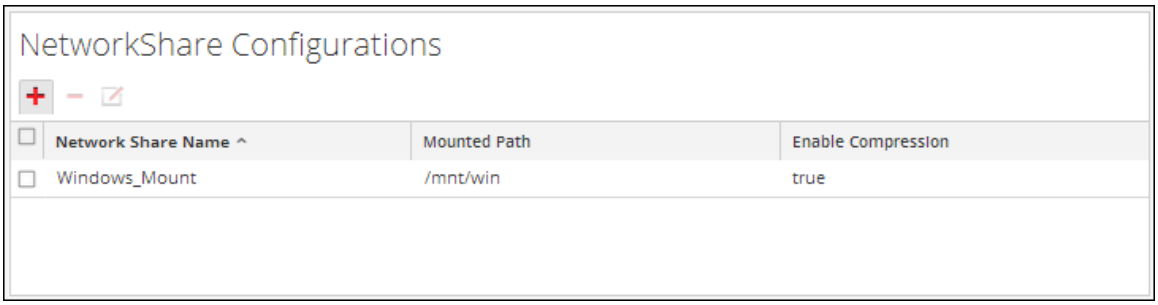
After the URL is configured, the files will be copied under the "URL_OUTPUT_ACTION" directory and the following parameters are sent to the server along with the compressed file.

Name	Config Value
filename	The name of the file.
filesize	The file size in bytes.
filetype	The file type associated with the file.
filechecksum	The number computed from a file that can be used to confirm that this is the one you expect and has been downloaded and stored properly.
hashingalgorithm	The hashing algorithm used to calculate the file checksum.
reportname	The name of the downloaded report.
executionid	The execution id associated with the report execution.
reportexecutionstarttime	The start time the report was executed.
status	The report creation status.
status description	The status description.

Network Share

After an execution is completed, you can transfer the output files to a mounted path or shared location based on the Network Share configuration.

The following figure shows the Network Share Configuration on the Output Actions Tab.



The following parameters manage Network Share (file transfer to a shared location on the network) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Network Share Name	The name of the Network Share. **Note:** You cannot create a Network Share configuration with a name that already exists in the Reporting Engine Network Share configuration list.
Mounted Path	The path (location) associated with the file transfer. You can use the pre-defined Linux directory structure in the mounted path. For example, **/mnt/win**. **Note:** The 'rsasoc' user must have read-write access to the specified Network Share mounted path.
	Click to view how the mounted path is created. This pop-up notifies that you must manually create the mounted path.
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

The following table lists the common operations you can perform in the Syslog, SFTP, URL and Network Share sections.

Operation	Description
	Create a Syslog, SFTP, URL and Network Share configuration.
	Delete a Syslog, SFTP, URL and Network Share configuration.
	Edit a Syslog, SFTP, URL and Network Share configuration.

Manage Logos Tab

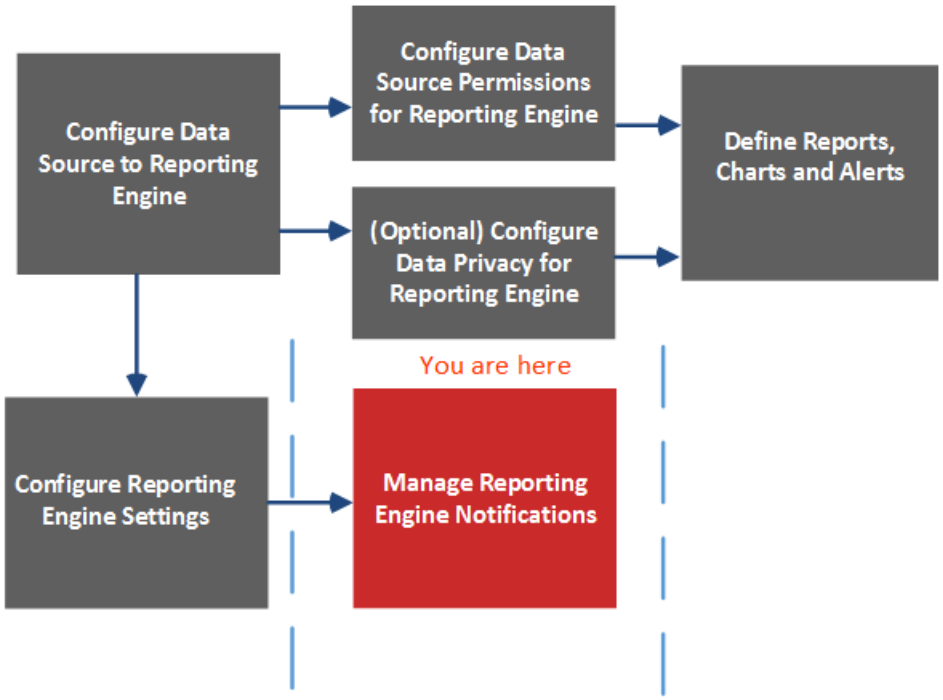
The Manage Logos option available in the **Services Config View** > **Manage Logos** tab, helps you to manage the logos associated with the Reporting Engine. The Manage Logos tab consists of a single panel with a toolbar and a grid that lists the logos.

You can upload the logos that you want to use in your report. After you upload the logo, you can set any logo as a default logo which will be automatically used in all the scheduled reports. You can choose to override the default logo with any other logo listed in this tab when you schedule a report. For more information, see "Select a Logo Dialog" topic in the *Reporting Guide*.

The supported image formats are:

- .jpg
- .png
- .gif

Workflow



What do you want to do?

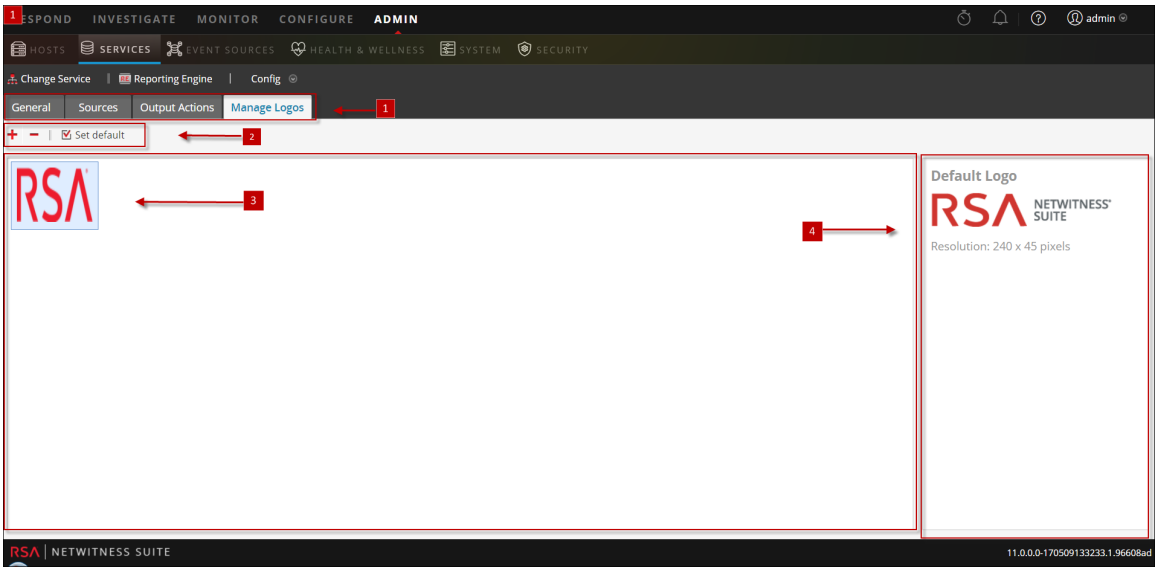
Role	I want to...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts, and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator / SOC Manager	Add, or delete logos*	Configure Reporting Engine General Settings
Administrator / SOC Manager	View the list of logos*	Configure Reporting Engine General Settings
Administrator / SOC Manager	Set a logo as default*	Configure Reporting Engine General Settings

*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look



Note: The logo to be uploaded should not exceed 500 KB. The required permission to access this view is Manage Services.

1. Displays all the available configurable tabs.
2. Displays edit actions.
3. Displays all the logos that have been used
4. Displays the default logo used.

You can perform the following actions on the Manage Logos Tab.

Icon	Actions
+	Add new logos from the local directory of the system to the Reporting Engine. **Note:** The logo size cannot exceed 500 KB. The logos chosen must be of the following file types: * .jpg * .gif * .png

Icon	Actions
	Removes logos from the Reporting Engine. **Note:** By performing (Ctrl+click), you can select multiple logos to delete.
	Sets the default logo for a Reporting Engine. This is the logo NetWitness Suite defaults to in the **Log** panel of the Schedule a Report view. **Note:** If no default logo is selected, the RSA logo is displayed.

RSA NETWITNESS® SUITE

Warehouse Connector Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

How Warehouse Connector Works **5**

Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid **8**

Configure a Warehouse Connector Service **9**

Configure the Data Source for Warehouse Connector **10**

Update the Port Number and SSL Settings of the Data Source 11

Configure the Destination **13**

Configure the Destination Using NFS 15

Configure the Destination Using SFTP 18

Configure the Destination Using WebHDFS 23

Configure a Stream **28**

Create a Stream 29

Finalize the Stream 31

Start the Stream 32

Monitor a Warehouse Connector **33**

Add Warehouse as a Data Source to Reporting Engine **35**

Analyze a Warehouse Report **36**

View the Warehouse Connector Service **37**

Troubleshoot the Warehouse Connector **38**

Manage a Stream and Lockbox **40**

Warehouse Connector Configuration References **49**

General Tab Settings 50

Appliance Service Configuration Tab Settings 53

Sources and Destinations Configuration 56

Add Stream Dialog 60

Streams Configuration 64
Lockbox Settings 72

How Warehouse Connector Works

Warehouse Connector collects meta and events from Decoder and Log Decoder and writes them in AVRO format into a Hadoop-based distributed computing system. You can set up Warehouse Connector as a service on existing Log Decoders or Decoders.

The Warehouse Connector contains the following components:

- Data Source
- Destination
- Data Stream

Data Source

A data source is the service from which the Warehouse Connector collects data to store in the destination. The supported data sources are Log Decoder and Decoder services.

Destination

Destination is the Hadoop-based distributed computing system that collects, manages, and enables reporting on security data. The following are the supported destinations:

- RSA NetWitness Warehouse (MapR) deployments
- HortonWorks Data Platform
- Any Hadoop-based distributed computing system that supports WebHDFS or NFS mounting of HDFS file systems.
- Example: Commercial MapR M5 Enterprise Edition for Apache Hadoop

Data Streams

A data stream is a logical connection between the data source and destination. You can have multiple streams for different subsets of data collected. You can setup streams to segregate data from multiple Decoder and Log Decoder services. You can create a stream with multiple data sources and a single destination or with a single data source and destination.

The Warehouse Connector does the following:

- Aggregates session and raw log data from Decoders and Log Decoders.
- Transfers the aggregated data into supported destinations like Hadoop based deployments.
- Serializes the aggregated data that includes both schema and data into AVRO format.

In addition the Warehouse Connector also supports the following:

Meta Filters

Meta filters enables you to filter the meta keys that should be written into the Warehouse. For more information, see Specify Meta Filters for a Stream.

Support for Multi-Valued Meta Keys

RSA NetWitness Warehouse supports multi-valued meta keys. The multi-valued meta keys is the meta field with the array type. You can use the meta keys library to determine the meta fields of type array and write HIVE queries with the correct syntax for arrays. By default, the following meta keys are treated as multi-valued and are defined in the file, **multivalue-bootstrap.xml** located at **/etc/netwitness/ng** in the Warehouse Connector:

- alias.host
- action
- username
- alias.ip
- alias.ipv6
- email
- device.group
- event.class

Checksum Validation

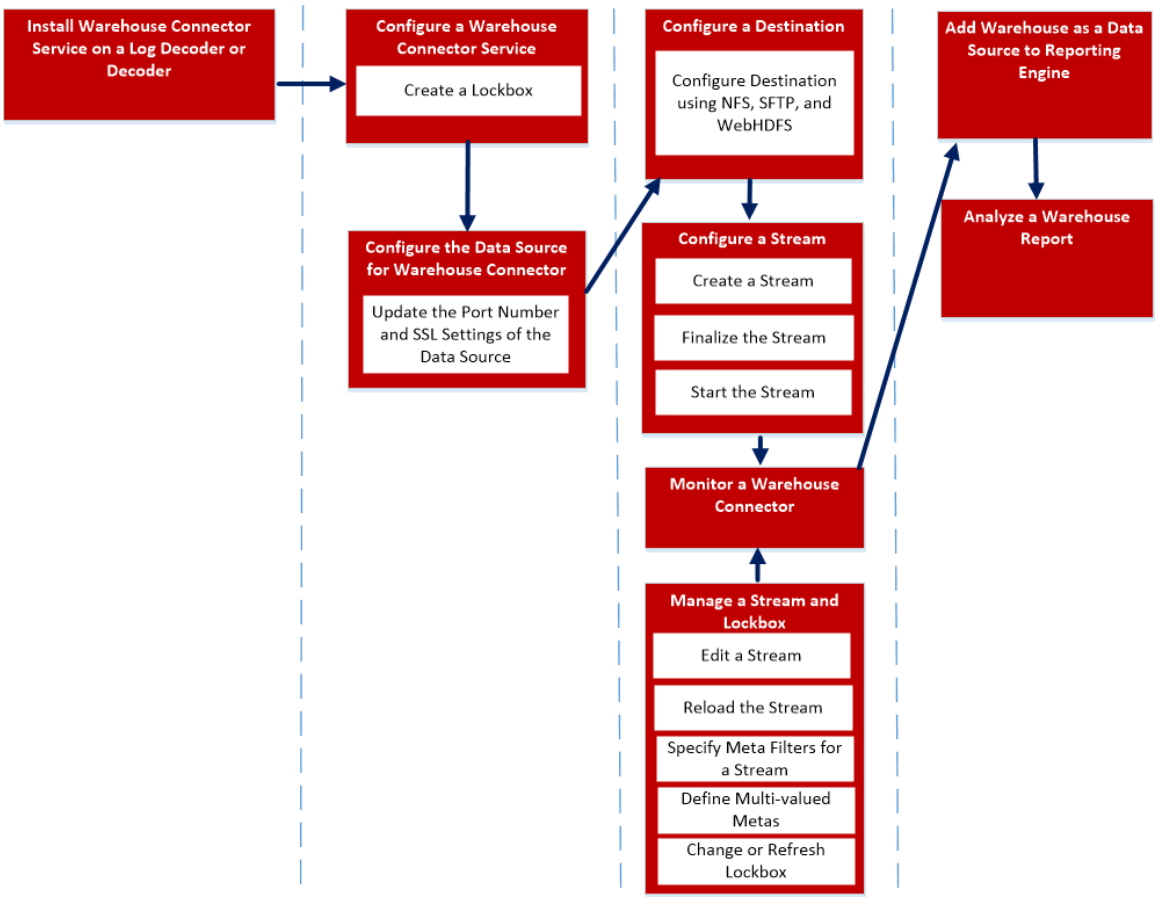
Warehouse Connector enables you to validate the file integrity of the AVRO files that are transferred from the Warehouse Connector to the data destinations. You need to enable checksum validation while you configure the Warehouse Connector.

Lockbox Support

Lockbox provides an encrypted file that Warehouse Connector uses to store and protect sensitive data. You need to create the lockbox by providing a lockbox password while configuring the Warehouse Connector for the first time.

You can orchestrate Warehouse Connector on a Log Decoder or a Decoder appliance.

The following is an overview of the entire process of installing and configuring the Warehouse Connector service on Log Decoder or Decoder, configuring the Warehouse Connector service on NetWitness, configuring data sources, destinations, streams for Warehouse Connector, and configuring alert notifications on NetWitness.



To install and configure the Warehouse Connector service, perform the following:

1. Install Warehouse Connector service on a Log Decoder or Decoder
2. Configure a Warehouse Connector service
3. Configure the Data Source for Warehouse Connector
4. Configure a Destination
5. Configure a Streams
6. Monitor a Warehouse Connector
7. Add Warehouse as a Data Source to Reporting Engine
8. Analyze a Warehouse Report
9. Manage a Stream and Lockbox

Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid

To install (fresh install) the Warehouse Connector service on a Log Decoder or Decoder or Hybrid:

1. Log on to the Log Decoder or Decoder host.
2. Enter the following command on NetWitness Server:
   `warehouse-installer --help`
   The command line interface (CLI) usage descriptions are displayed.
4. Install Warehouse Connector service by executing either of the following commands:
   `warehouse-installer --host-addr 10.0.0.0`
   `warehouse-installer --host-id 5928b9d8-83be-4143-9602-fa936de5c41e`
   `warehouse-installer --host-name NW11AdminServer`
   Where,
   10.0.0.0 - IP address of the Host
   5928b9d8-83be-4143-9602-fa936de5c41e - Host ID
   NW11AdminServer - Host name

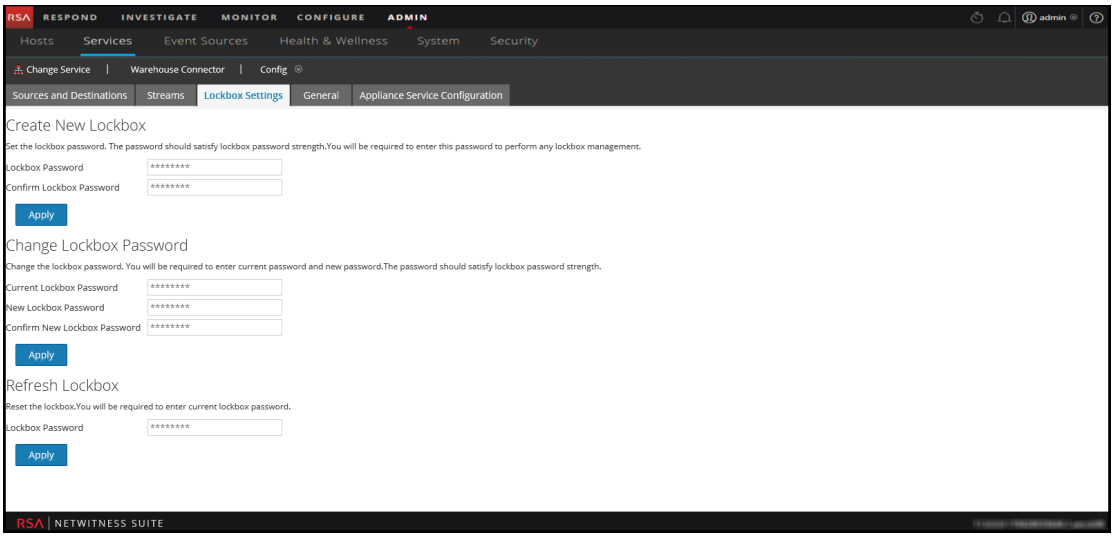
The Warehouse Connector service is successfully installed on the Log Decoder or Decoder or Hybrid.

Configure a Warehouse Connector Service

You can configure the Warehouse Connector service using the following procedure.

To set the Lockbox password:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service, and select **> View > Config**.
4. In the Services Config view of Warehouse Connector, click the **Lockbox Settings** tab.



5. In the **Create New Lockbox** section, perform the following:
   a. In the **Lockbox Password** field, enter the new lockbox password.

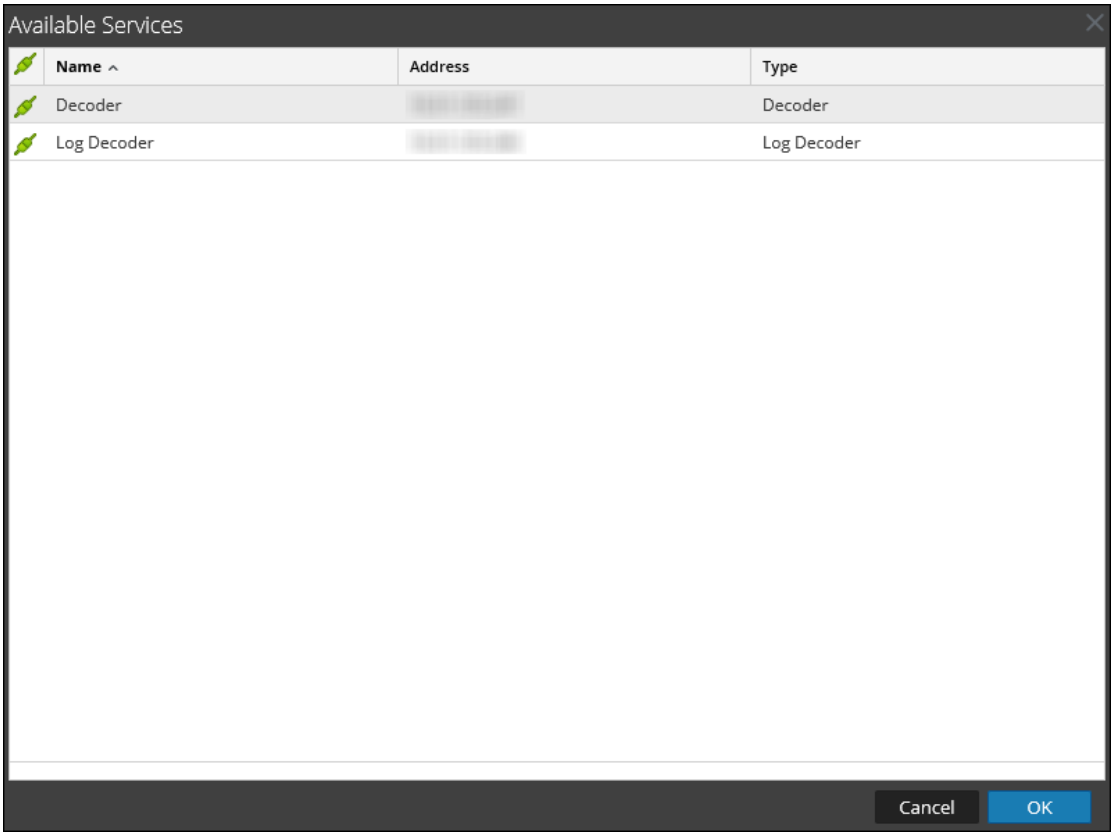
      Note: The lockbox password must be at least eight characters in length and it must contain at least three of the following groups: one uppercase character [A-Z], one lowercase character [a-z], one numeral [0-9], and one special character.

   b. In the **Confirm Lockbox Password** field, enter the added lockbox password to confirm.
   c. Click **Apply**.
      The Lockbox password is set.

Configure the Data Source for Warehouse Connector

To configure the data source:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service, and select **> View > Config**.
   The Services Config view of Warehouse Connector is displayed.
4. On the **Sources and Destinations** tab, in the **Source Configuration** section, click .



5. In the **Available Services** dialog, select the Log Decoder or Decoder services that you want to add as a source to the Warehouse Connector service and click **OK**.
   The selected Log Decoder and Decoder services are listed in the **Source Configuration** section.

Update the Port Number and SSL Settings of the Data Source

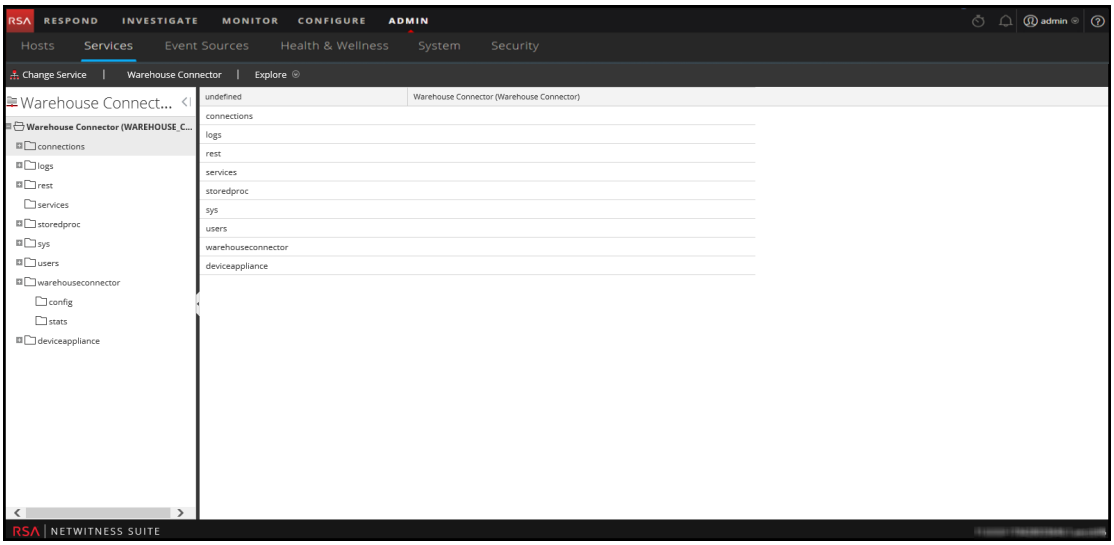
If there is change in the port number or SSL settings of the data sources used in the Warehouse Connector, you can directly update these details in Warehouse Connector, using the Explore view of the Warehouse Connector.

Make sure that:

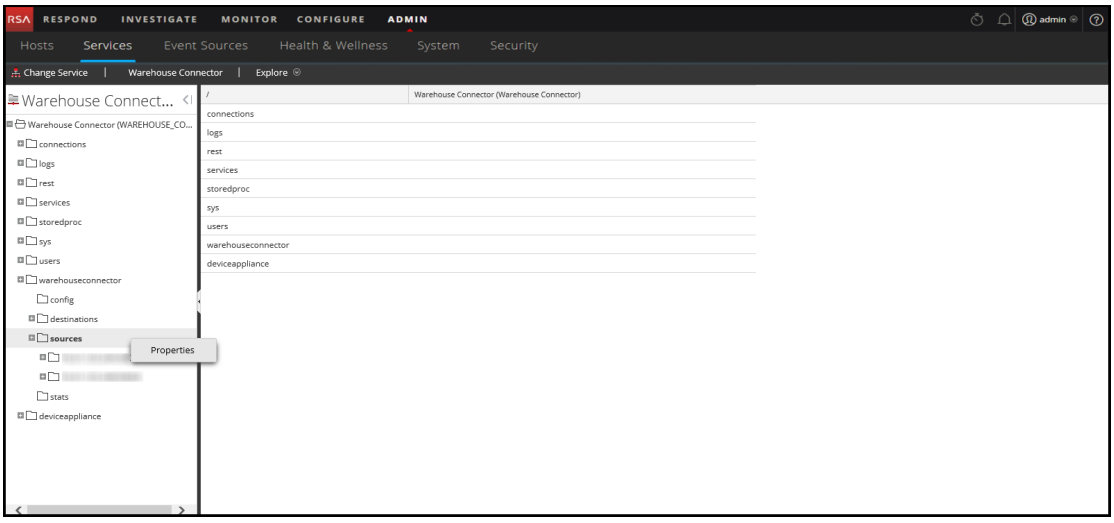
- You have the updated port number or SSL settings of the data source.
- You stop the streams related to the data source that you want to update the port number or SSL settings.

To update the port number or SSL settings:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service and select **> View > Explore**.
   The Service Explore view of Warehouse Connector is displayed.

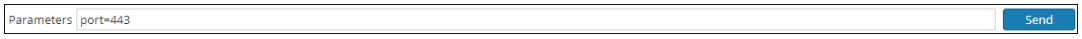


4. Navigate to **warehouseconnector/sources**, right-click the source, and click **Properties**.
   The Properties section of the source is displayed.



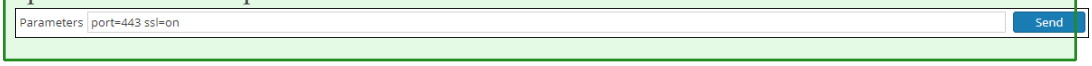
5. In the drop-down menu, select **update**. In the Parameters field, perform the following:

   - To update the port number of the source, enter `port=<new_source_portnumber>` and click **Send**.

   - To update the SSL settings of the source, enter `ssl=<new_ssl_settings>` and click **Send**.

     Note: You can also update the port number and ssl settings simultaneous by adding space between the parameters.

6. Restart the Warehouse Connector service.
7. Start the streams.

Configure the Destination

You can configure the destination using NFS, SFTP, and WebHDFS. Change the destination to which the Warehouse Connector service needs to write the collected data using NFS:

- RSA NetWitness Warehouse (MapR) deployments
- Commercial MapR M5 Enterprise Edition for Apache Hadoop deployments

You can configure the Warehouse Connector to write to a remote destination using Secure File Transfer Protocol (SFTP). The remote destination can be a remote server that is NFS mounted to the MapR cluster or it can be a remote staging server.

By default, in the remote destination the Warehouse Connector writes data in the following directory structure:

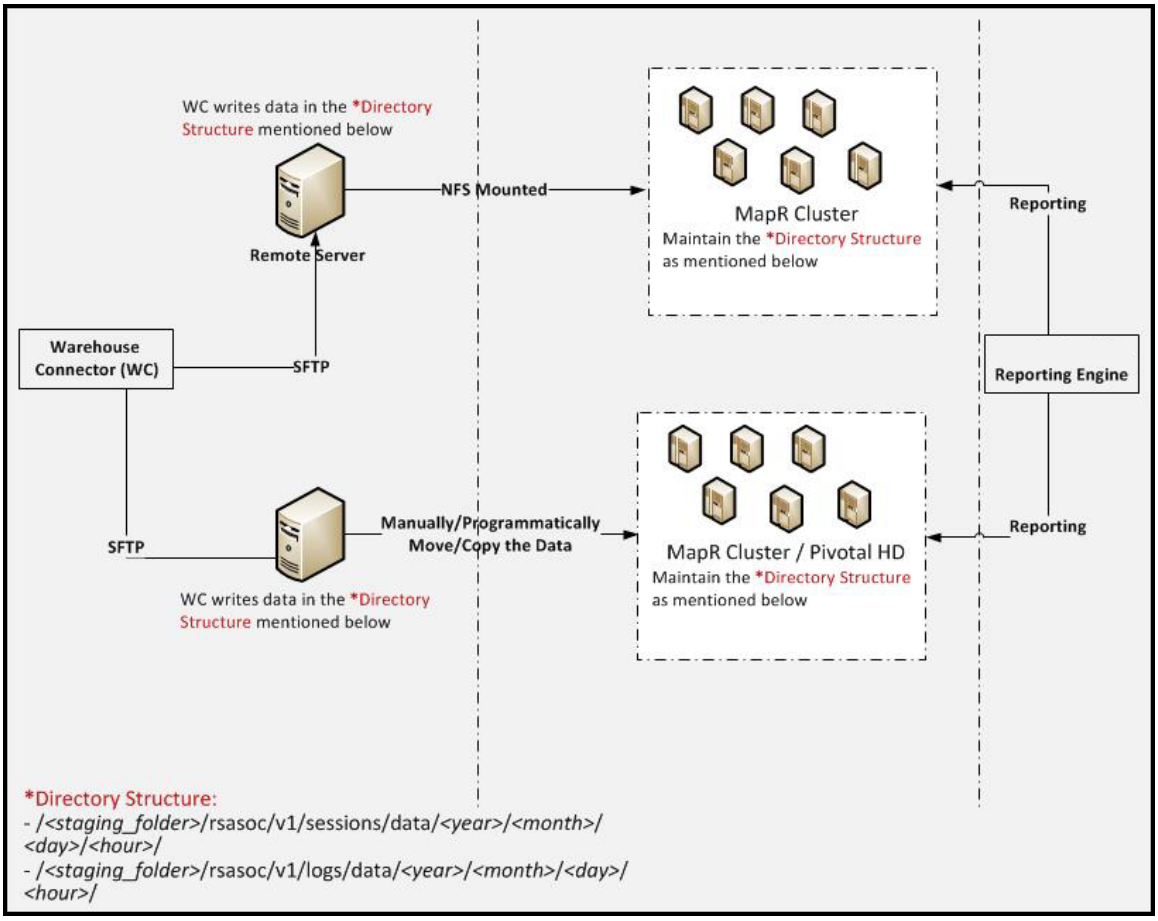
- `/<staging_folder>/rsasoc/v1/sessions/data/<year>/<month>/<day>/<hour>/`
- `/<staging_folder>/rsasoc/v1/logs/data/<year>/<month>/<day>/<hour>/`
  Where <staging_folder> is the folder on the remote server where the Warehouse Connector writes the data.

If you are using a remote staging server as the remote destination, you need to manually copy or move the directory structure to any of the following deployments:

- RSA NetWitness Warehouse (MapR)
- Commercial MapR M5 Enterprise Edition for Apache Hadoop
- HortonWorks HD

To generate reports from the data written by Warehouse Connector, make sure that in your Hadoop deployment you maintain a similar directory structure that is created by Warehouse Connector in the remote destinations.

The following illustration describes how you can use SFTP to write data from Warehouse Connector to a remote destination.



You can configure the Warehouse Connector service to write the collected data to a Hadoop-based distributed computing system that supports WebHDFS.

Configure the Destination Using NFS

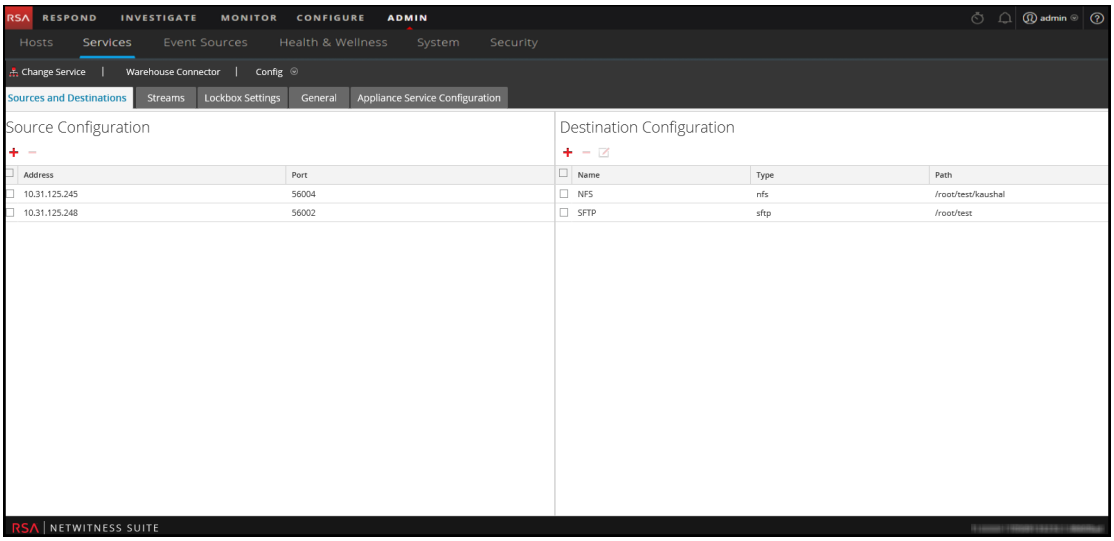
Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Set up NFS on Warehouse Connector. For more information on how to set up NFS on Warehouse Connector, see "Configure Warehouse Connector to Write to Warehouse" in the *Warehouse (MapR) Configuration Guide*.

To configure the destination using NFS:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the Warehouse Connector service, and select **> View > Config**.

   The Services Config View of Warehouse Connector is displayed.

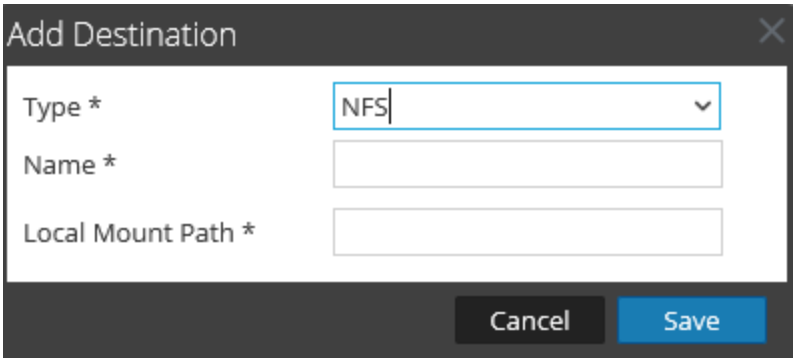


4. On the **Sources and Destinations** tab, in the **Destination Configuration** section, click +.
5. In the **Add Destination** dialog, select **NFS** from the **Type** drop-down list.
6. In the **Name** field, enter a unique symbolic name for the destination.

Note: The **Name** field does not support spaces or special characters except underscore (_).

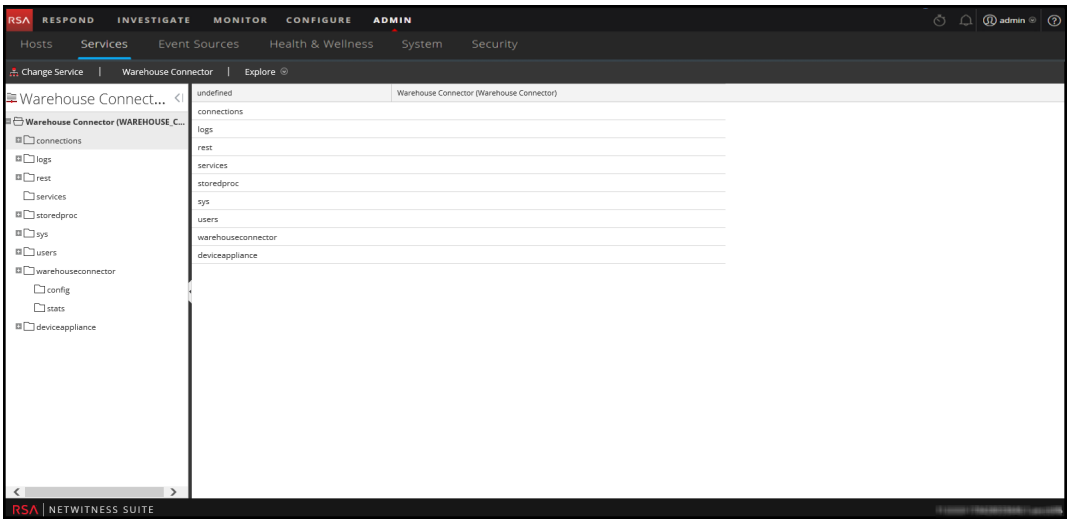
7. In the **Local Mount Path** field, enter the locally mounted directory for HDFS where you want the Warehouse Connector to write the data. For example:
   If **/saw** is the local mount point for HDFS that you have configured while mounting the mapr NFS cluster on the host where you have installed the Warehouse Connector service to write to RSA NetWitness Warehouse (MapR), create a directory named **Ionsaw01** under **/saw** and the corresponding Local Mount Path for the destination would be **/saw/Ionsaw01**.

   For more information, see "Mount the Warehouse on the Warehouse Connector" topic in the *Warehouse (MapR) Configuration Guide*.



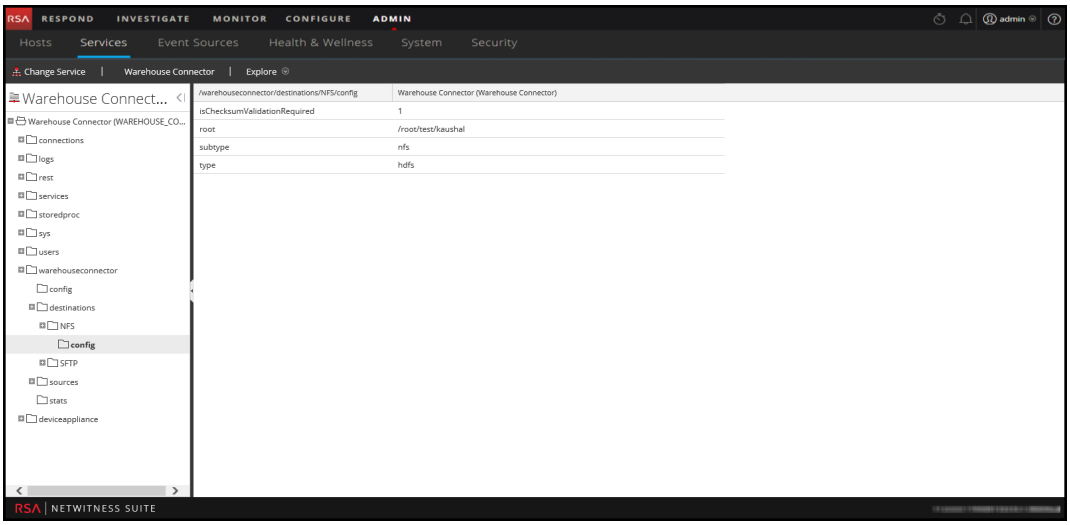
   The **/saw** mount point implies to / as the root path for HDFS. The Warehouse Connector writes the data to **/Ionsaw01** in HDFS.

8. Click **Save**.
9. (Optional) If you want to enable checksum validation, perform the following:
   a. Go to **ADMIN > Services**.
   b. In the Services view, select the added Warehouse Connector service, and select **> View > Explore**.
      The Explore view of Warehouse Connector is displayed.



c. In the options panel, navigate to **warehouseconnector/destinations/nfs/config**. This is the name of the destination and is dynamic.

d. Set the parameter `isChecksumValidationRequired` to **1**.



e. Restart the respective stream.

Configure the Destination Using SFTP

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- For the SFTP destination type, the destination host should be listed in the **/root/.ssh/known_hosts** file used by the ssh service (for example, sshd) running on the Warehouse Connector.

Add Destination from Warehouse Connector Host

To add the destination host to the **/root/.ssh/known_hosts** file, from the Warehouse Connector host, initiate a secure connection to the destination host:

1. Login to the Warehouse Connector.
2. Enter `ssh root@<SAWIP>` or `ssh username@<SAWIP>`.
3. Select **Yes** and enter the password.
4. Add the host key in the **/root/.ssh/known_hosts** file

> **Note:** After you upgrade Warehouse Connector to 11.0, you must make sure that the destination host is listed in the /root/.ssh/known_hosts file used by the ssh service (i.e. sshd) running on the Warehouse Connector. If you do not perform this action, the streams configured with SFTP in Warehouse Connector will not start.

- If you want to use SFTP to write data into the destination using SSH key-based access, you need to configure SSH key-based access between the Warehouse Connector and the Warehouse host or Hadoop node. For more information, see **Configure SSH Keys** below.

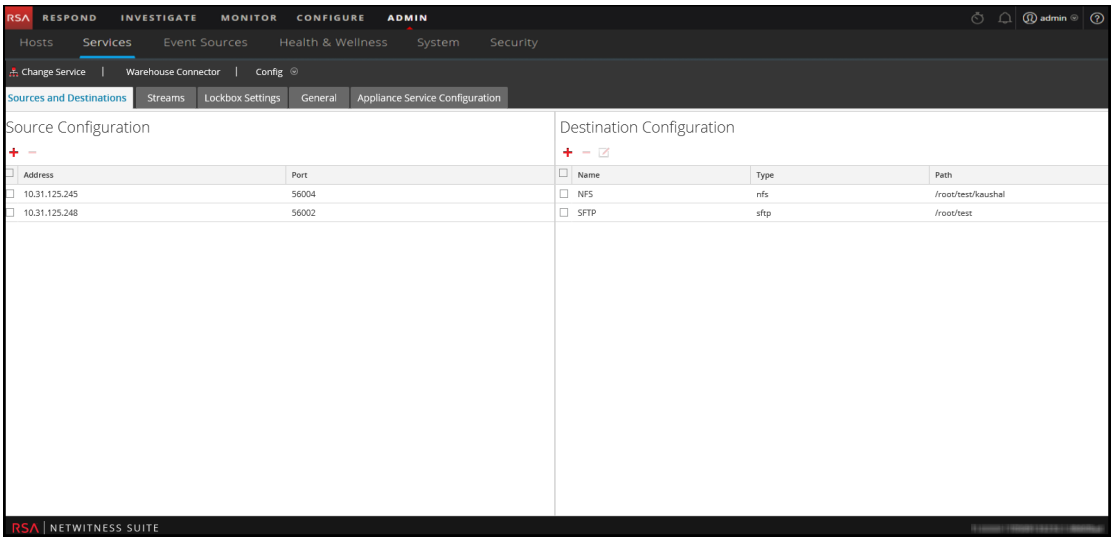
> **Note:** If you want to enable checksum validation to validate the integrity of the AVRO files that are transferred from the Warehouse Connector to the destinations, make sure that you generate the keys without setting the passphrase and do a key exchange between warehouse connector and the warehouse nodes.

Configure Warehouse Connector to use SFTP destination

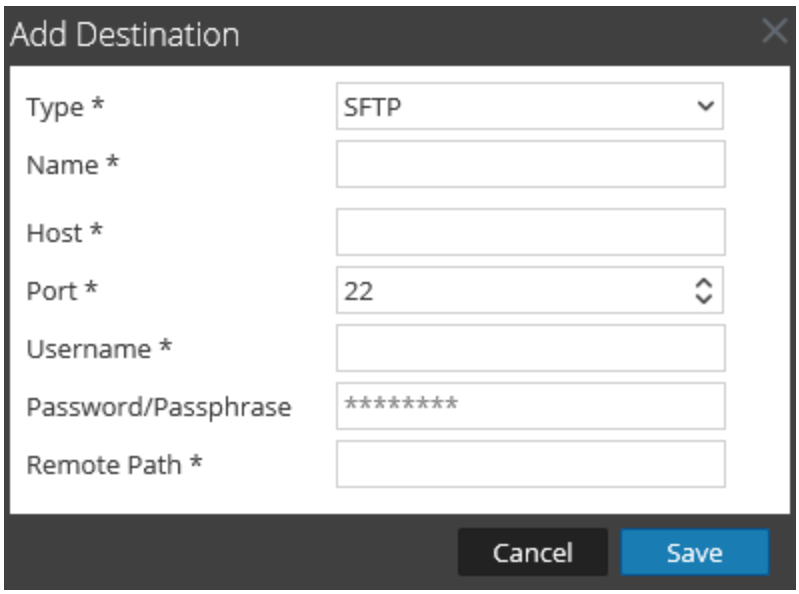
To configure the destination:

1. Log on to NetWitness
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service, and select **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.



4. On the **Sources and Destinations** tab, in the **Destination Configuration** section, click .
5. In the **Add Destination** dialog, select **SFTP** from the **Type** drop-down list.



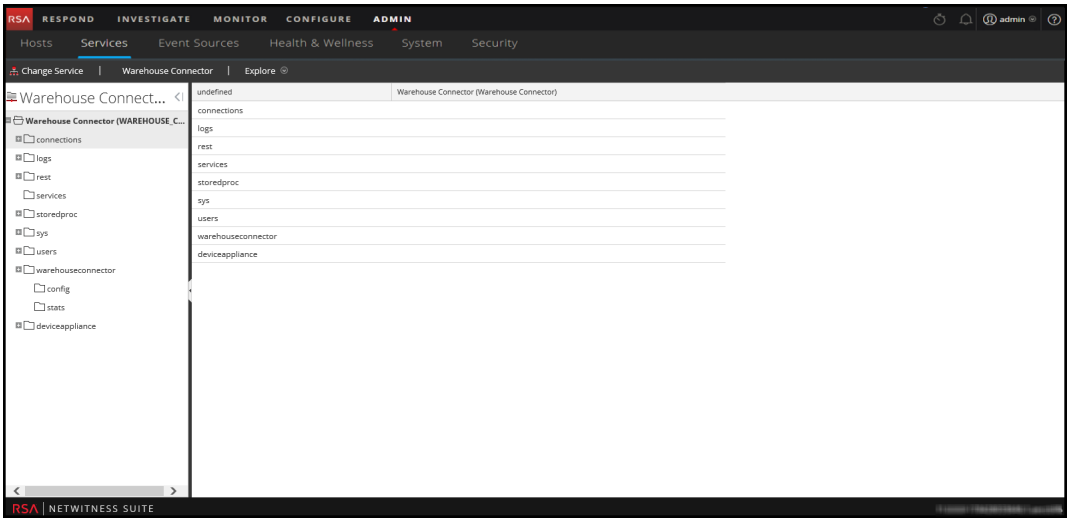
6. In the **Name** field, enter a unique symbolic name for the destination.

   Note: The **Name** field does not support spaces or special characters except underscore (_).

7. In the **Host** field, enter the remote server IP address.
8. In the **Port** field, retain the default port, **22**.
9. In the **Username** field, enter the SSH username.

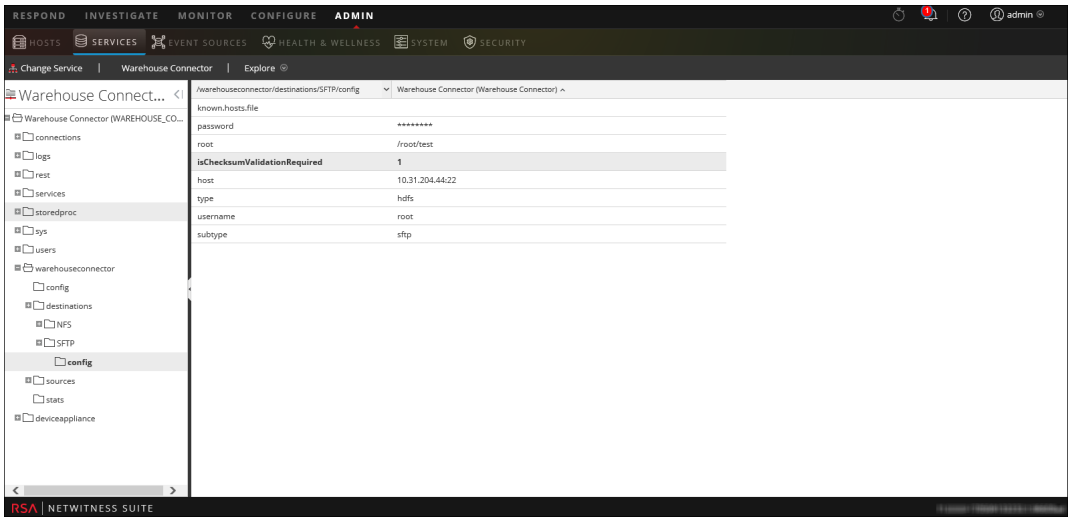
   Note: In the case of HortonWorks HD, ensure that the username is gpadmin and for password based access the password for gpadmin should be used. For passphrase-based access, the passphrase used to generate the keys for gpadmin user should be used.

10. In the **Password/Passphrase** field, enter one of the following:
    - SSH password - If you are using SFTP to write data into the destination using password-based access.
    - SSH passphrase - If you are using SFTP to write data into the destination using SSH key-based access.
11. In the **Remote Path** field, enter the path of the directory present on the SFTP server.
12. Click **Save**.
13. (Optional) If you want to enable checksum validation, perform the following:
    a. Go to **ADMIN > Services**.
    b. In the Services view, select the added Warehouse Connector service, and select **> View > Explore**.
    The Explore view of Warehouse Connector is displayed.



c. In the options panel, navigate to **warehouseconnector/destinations/sftp/config**.

d. Set the parameter `isChecksumValidationRequired` to **1**.



e. Restart the respective stream.

Configure SSH Keys

To configure SSH key-based access between the Warehouse Connector and the Warehouse host or Hadoop node:

1. Generate SSH keys on the Warehouse Connector at the default location. Perform the following:

   a. Log on to the Warehouse Connector.

   b. Type the following command and press ENTER:

   ```
   $ OWB_FORCE_FIPS_MODE_OFF=1 ssh-keygen -t dsa
   ```

   c. The command prompts you to enter the file in which to save the generated key.

   ```
   Enter file in which to save the key (/root/.ssh/id_dsa):
   ```

   d. Enter the file in which you want to save the key and press ENTER.

   The command prompts you to enter and confirm the passphrase.

   Note: If you want to enable checksum validation to validate the integrity of the AVRO files that are transferred from the Warehouse Connector to the destinations, make sure that you do not set the **passphrase**. Then, the below steps e, f, g, and h are not applicable.

```
Enter passphrase (empty for no passphrase):
 Enter same passphrase again:
```

The public key is generated and is saved in the location that you provided.

e. Change the directory by entering the following command:

```
cd /root/.ssh/
```

f. Move the generated key to the below location:

```
mv id_dsa id_dsa.old
```

g. Type the following command and press ENTER:

```
$ OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_
dsa.old -out id_dsa
```

The command prompts you to enter and confirm the passphrase.

h. Enter the encryption passphrase.

i. Run the following command to change the file permission:

```
chmod 600 id_dsa
```

2. Append the generated public key to the remote Warehouse host or Hadoop node's authorized keys list located at: `~/.ssh/authorized_keys`

> **Note:** Make sure that you copy the public keys to the Hadoop node and while copying the public key ensure that you provide the login details of the user using which the WebHDFS destination would be added.

You can now securely communicate between Warehouse Connector and Warehouse nodes or Hadoop nodes.

Configure the Destination Using WebHDFS

Make sure that you have:

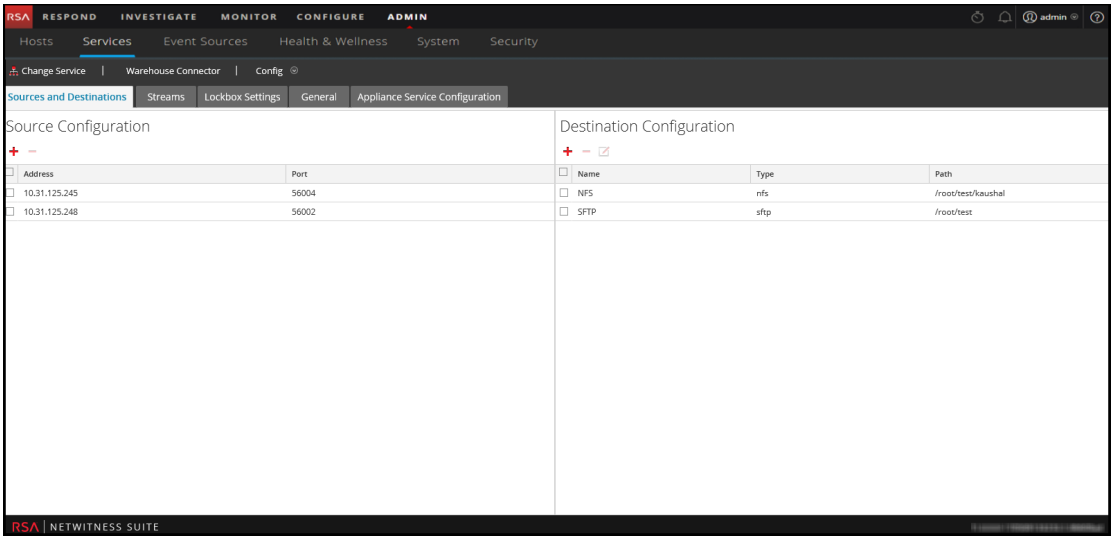
- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Added the hostname (or FQDN) and IP address of the warehouse nodes and Warehouse Connector to the DNS server. If the DNS server is not configured, add the hostname (or FQDN) and IP address of the warehouse nodes and Warehouse Connector to the file in the host on which the Warehouse Connector service is installed.
- If you want Kerberos authentication between the warehouse connector and the warehouse cluster, make sure that you perform the following:
  - Kerberos Key Distribution Center (KDC) Server is configured in your network environment and the Kerberos Keytab file is copied to the host on which you have installed Warehouse Connector.
  - Kerberos authentication is enabled in the warehouse cluster.
- If you want to enable checksum validation to validate the integrity of the AVRO files that are transferred from the Warehouse Connector to the destinations, make sure that you generate the keys without setting the passphrase and do a key exchange between the Warehouse Connector and the warehouse nodes. You need to configure SSH key-based access between the Warehouse Connector and the Warehouse host or hadoop node. For more information, see 'Configure SSH Keys' in Configure the Destination Using SFTP.

Configure Warehouse Connector to Write to SFTP destination

To configure the destination:

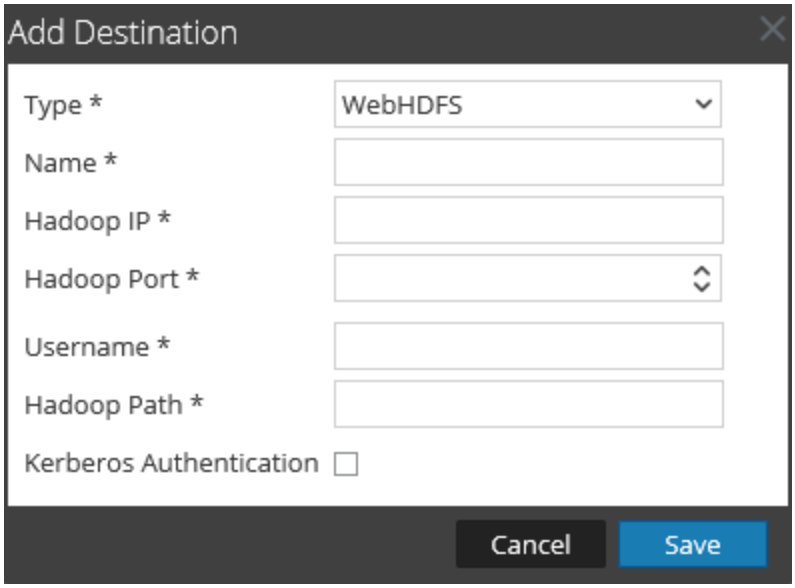
1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service and select **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.



4. On the **Sources and Destinations** tab, in the **Destination Configuration** section, click +.

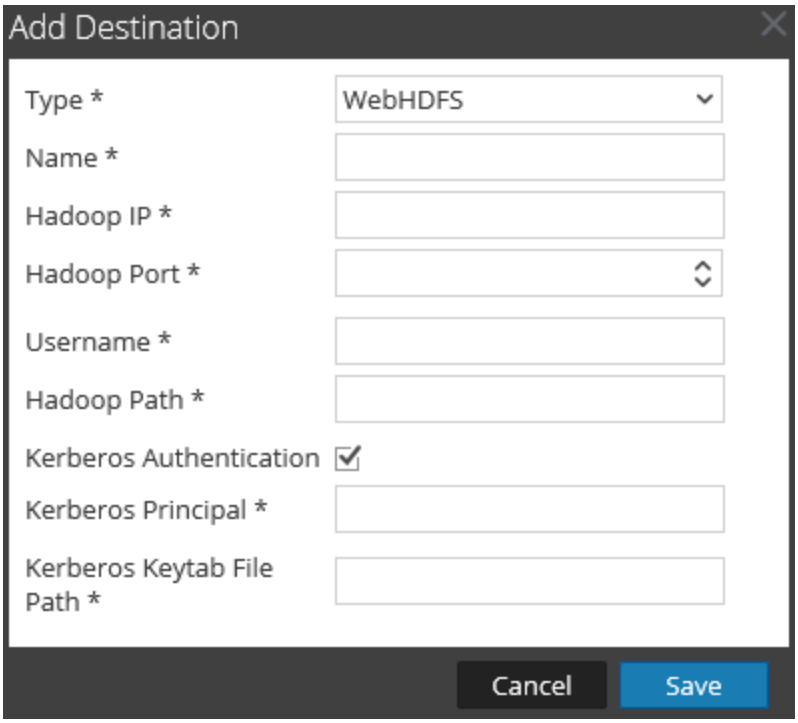
5. In the **Add Destination** dialog, select **WebHDFS** from the drop-down list.



6. In the **Name** field, enter a unique symbolic name for the destination.

   Note: The **Name** field does not support spaces or special characters except underscore (_).

7. In the **Hadoop IP** field, enter the namenode IP address of the warehouse cluster.
8. In the **Hadoop Port** field, enter the base port that is used by the namenode web user interface.
9. In the **Username** field, enter the owner of the directory in the warehouse to which Warehouse Connector should write the data.
10. In the **Hadoop Path** field, enter the path of the directory in the warehouse to which Warehouse Connector should write the data.
11. Select the **Kerberos Authentication** checkbox, if you want the warehouse connector to securely communicate with the warehouse using Kerberos authentication.



Perform the following:

a. In the **Kerberos Principal** field, enter the KDC Principal used for Kerberos authentication.

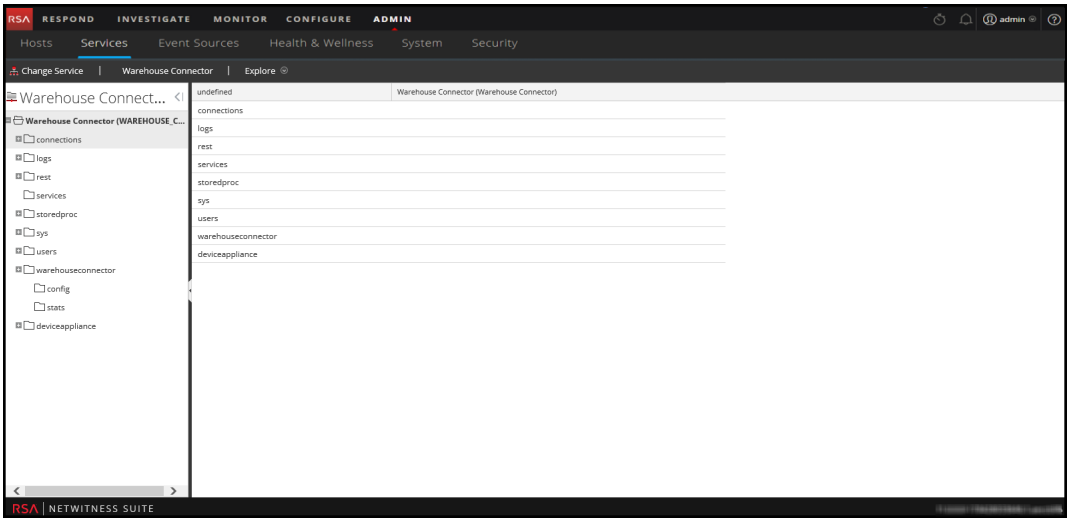
b. In the **Kerberos Keytab File Path** field, enter the path of the Kerberos Keytab file in the Warehouse Connector.

12. Click **Save**.

13. (Optional) If you want to enable checksum validation, perform the following:

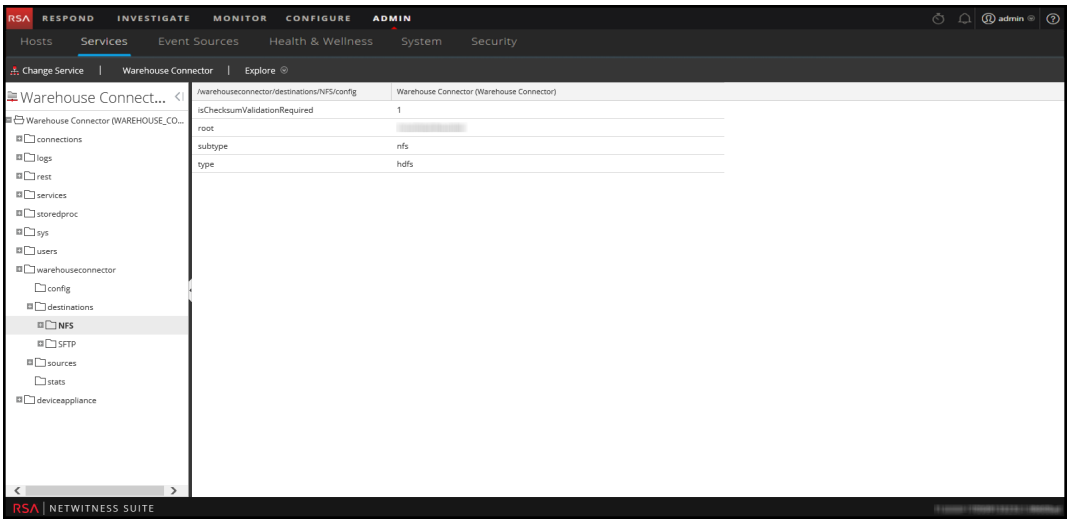
    a. Go to **ADMIN > Services**.

    b. In the Services view, select the added Warehouse Connector service and select > **View > Explore**.
    The Explore view of Warehouse Connector is displayed.



c. In the options panel, navigate to **warehouseconnector/destinations/webhdfs/config**.

d. Set the parameter `isChecksumValidationRequired` to **1**.



e. Restart the respective stream.

Configure a Stream

You can configure the data stream to define the data source and destination combinations.

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Configured the data source from which the Warehouse Connector service needs to collect data. For more information, see Configure the Data Source for Warehouse Connector.
- Configured the destination to which the Warehouse Connector service needs to write the collected data. For more information, see Configure the Destination.

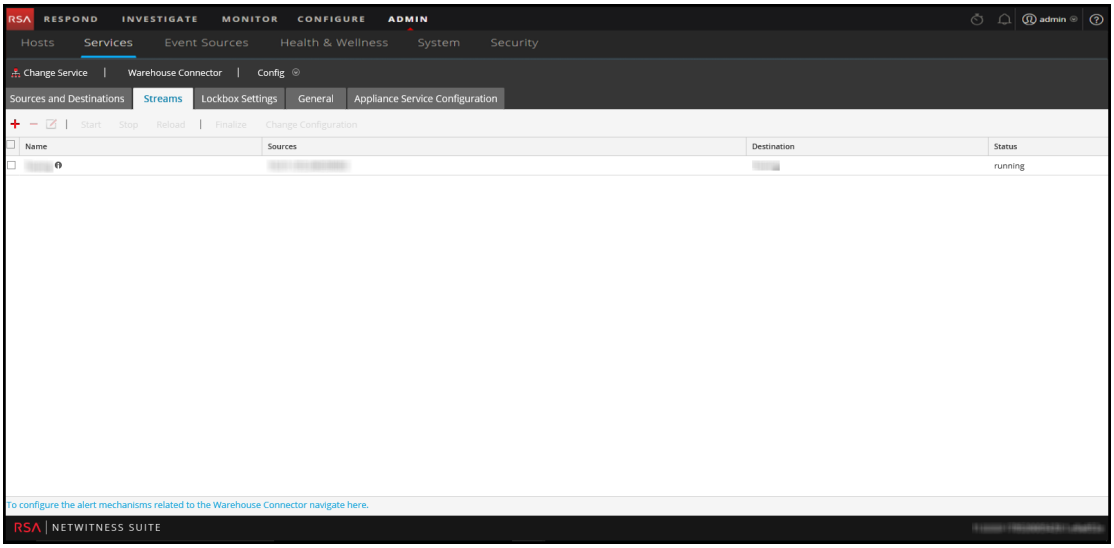
To configure the stream:

1. Create a stream
2. Finalize the stream
3. Start the stream

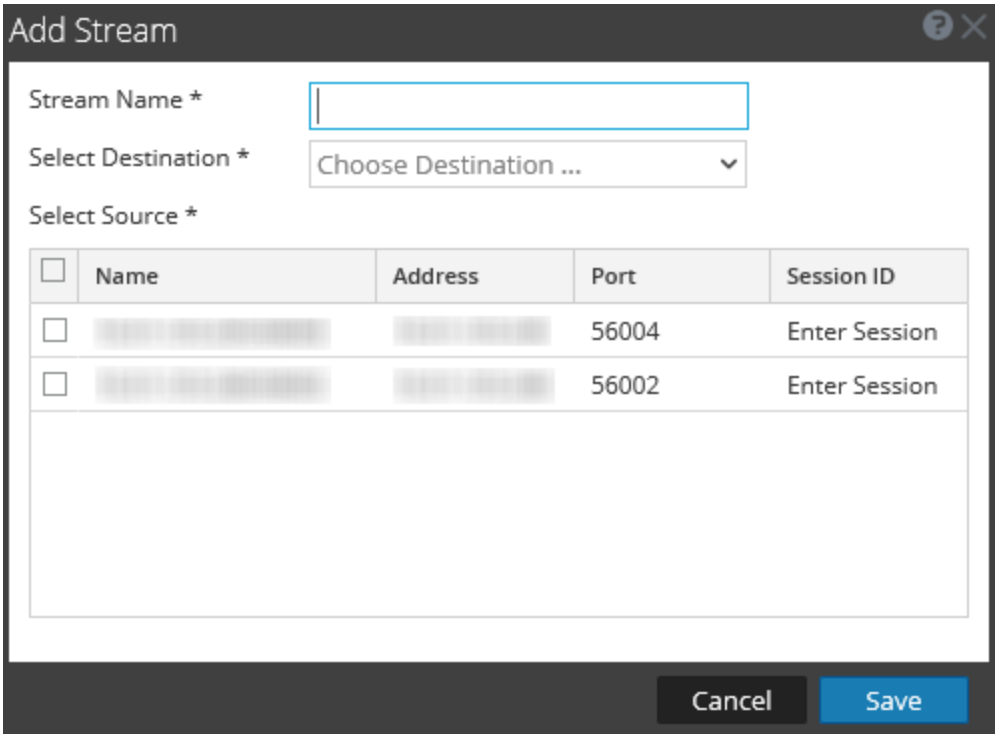
Create a Stream

To create a stream:

1. Go to **ADMIN > Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.
   The Services Config view of Warehouse Connector is displayed.
3. Click the **Streams** tab.



4. On the **Streams** tab, click ✚.



5. In the **Add Stream** dialog, perform the following:

   a. In the **Stream Name** field, enter a name for the stream.

   Note: The **Stream Name** field does not support spaces or special characters except underscore (_).

   b. In the **Select Destination** drop-down menu, select a destination from the list of destinations added to the Warehouse Connector.

   c. In the **Select Source** field, select sources from the list of sources displayed.

   d. In the **Session ID** column, enter the last session id.
   If you provide any session id, the Warehouse Connector will start the aggregation from that session, whereas if this is left blank, the aggregation will start from the current session.

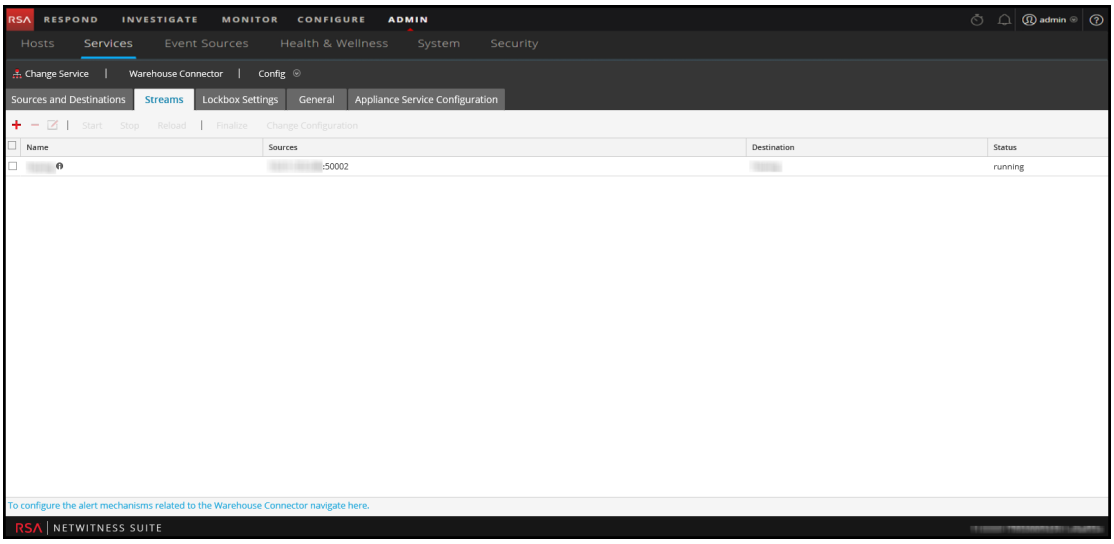
   e. Click **Save**.

Finalize the Stream

Make sure that you have created a stream.

To finalize the stream:

1. Go to **ADMIN > Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.
   The Services Config view of Warehouse Connector is displayed.
3. On the **Streams** tab, select the stream that you have created.



4. Click **Finalize**.

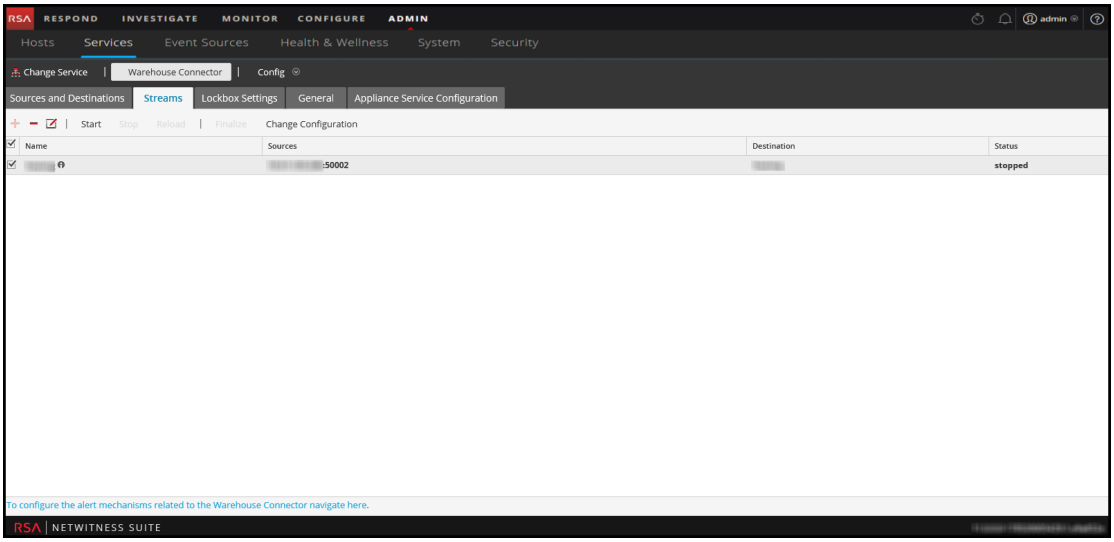
Start the Stream

Note: If you have deployed a Warehouse Connector Virtual Appliance, make sure that you change the default value of the `Maximum Message Hold Count` parameter to 800000. For more information, see General Tab Settings.

To start the stream:

1. Go to **ADMIN> Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.
3. On the **Streams** tab, select the stream that you have created.



4. Click **Start**.

Monitor a Warehouse Connector

By monitoring a Warehouse Connector, you can automatically generate notifications when critical thresholds concerning Warehouse Connector and its storage have been met.

To monitor a Warehouse Connector:

1. Go to **ADMIN > Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.
   The Services Config view of Warehouse Connector is displayed.
3. Click the **Streams** tab.
4. At the bottom of the **Streams** tab, click **To configure the alert mechanisms related to the Warehouse Connector navigate here**.
   The Warehouse Connector Monitoring page is displayed.

Caution: This page is deprecated and will be removed in a future release.

5. In the **Source or Destination Status** section, select the number of minutes or hours in the **Notify After Failing For** field.
   You will receive a notification if the source or destination connection fails for the defined number of minutes or hours.
6. In the **Stream Status** section, perform the following:
   a. In the **Notify Stopped For** field, define the number of minutes or hours after which you would like to receive a notification when the stream goes offline.
   b. In the **Disk Is** field, define the limit on the percentage of disk usage after which you would like to receive a notification.
   c. In the **Source is Behind** field, define the number of sessions. A notification is raised if the source goes behind the defined number of sessions.
   d. In the **Rejected Folder Size is** field, define the limit on the percentage of folder usage after which would like to receive a notification.
   e. In the **Number Of Files in Permanent Failure Folder** field, define the limit on the number of files in the permanent failure folder after which you would like to receive a notification.

7. In the **Notification Type** field, perform the following:
   a. Click **Configure email or distribution list** to configure email so that you can receive notifications in NetWitness. For more information, see the "Configure Email Server and Notification Account" topic in the *System Configuration* guide.
   b. Click **Configure Syslog and SNMP Trap servers** to configure audit logs. For more information, see the "Configure Syslog and SNMP Settings" topic in the *System Configuration* guide.
   c. Select the following notification mechanisms as per your requirement:
      - **NetWitness Console** - To get notifications on the NetWitness UI notification toolbar.
      - **Email** - To get email notifications.
      - **Syslog Notification** - To generate syslog events.
      - **SNMP Trap Notifications** - To get audit events as SNMP traps.

Add Warehouse as a Data Source to Reporting Engine

You must add Warehouse as a data source to Reporting Engine to make this data source available to reports against this Reporting Engine. For more information, see "Add Warehouse as a Data Source to Reporting Engine" topic in the *Reporting Engine Configuration Guide*.

Analyze a Warehouse Report

The Warehouse modules provide analysts with reports of early indicators of compromise. The following Warehouse reports can be analyzed in NetWitness:

- Suspicious Domains report
- Suspicious DNS Activity report
- Host Profile report

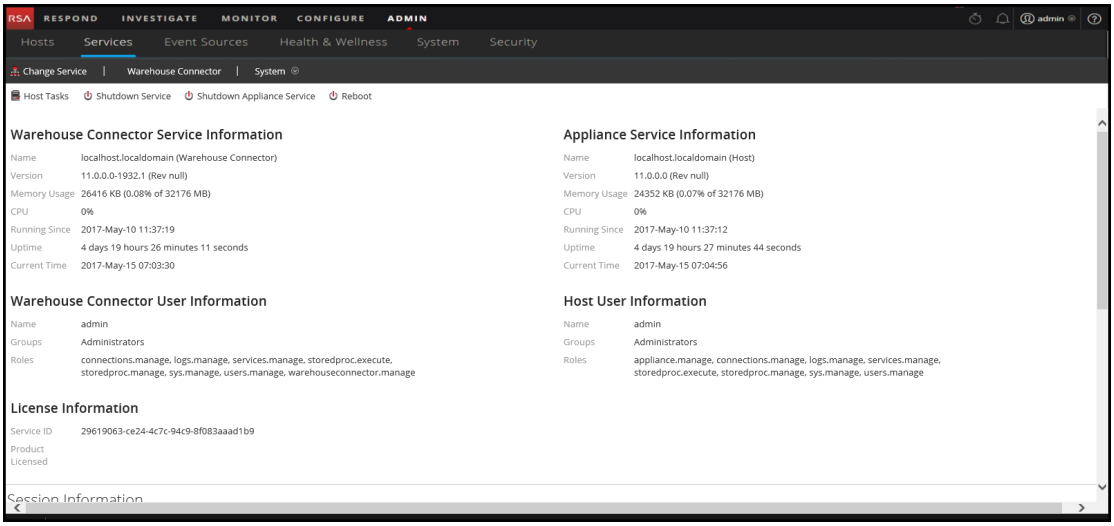
For more information, see "Step 4. Analyze a Warehouse Report" topic in the *Warehouse Guide*.

View the Warehouse Connector Service

While the information displayed in the Services System view is the same for all types of core services, several options in the toolbar are relevant only for Warehouse Connector.

To access this view:

1. Go to **ADMIN > Services**.
2. In the Services view, select a Warehouse Connector and select **> View > System**. The Systems view for the selected Warehouse Connector is displayed.



The following is an example of toolbar options for Warehouse Connectors.

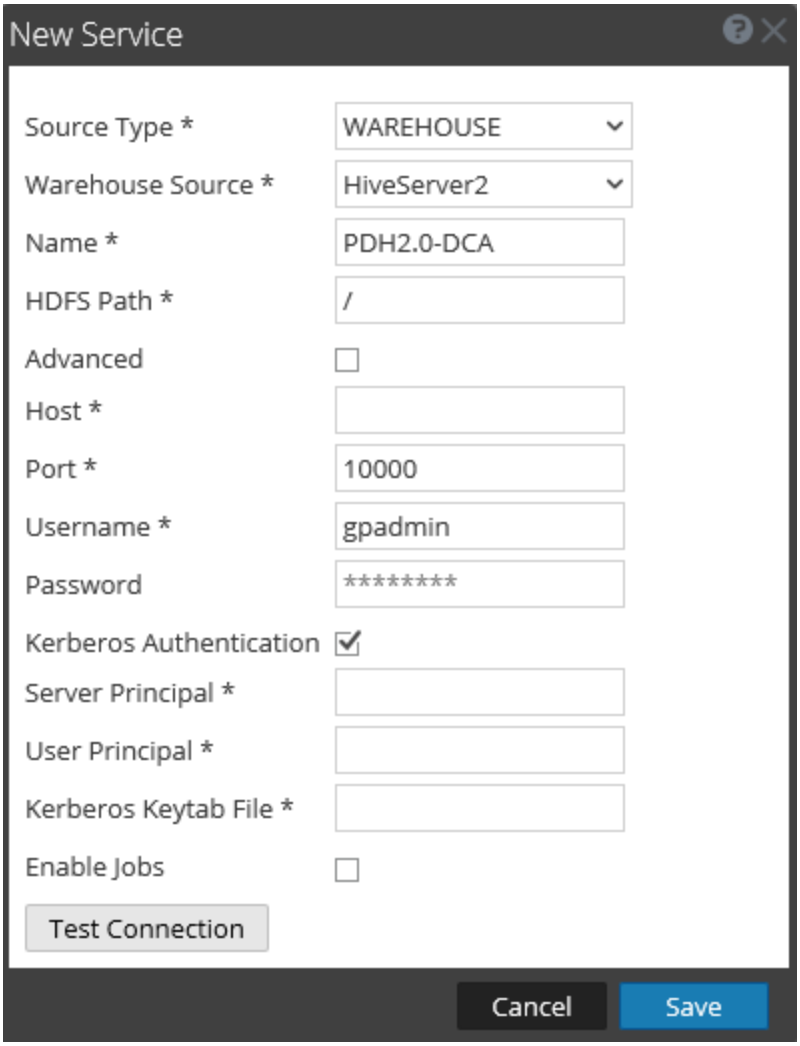
Host Tasks, Shutdown Service, Shutdown Appliance Service or (Shutdown Appliance), and Reboot are common to all services and are described in the *Hosts and Services Getting Started Guide*.

Troubleshoot the Warehouse Connector

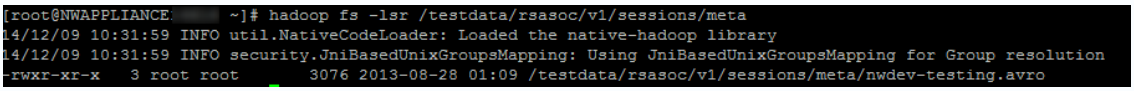
The following information suggests the possible issues that NetWitness users may encounter when adding a Warehouse service to the Reporting Engine as a data source for reporting in NetWitness. Look for explanations and solutions in this section.

While adding a Warehouse service to the Reporting Engine as a data source for reporting, you may observe some of the errors listed in this document. Information is provided on how to troubleshoot the errors and add the data source successfully.

The following figure shows the New Service dialog.



For more information, see "Add Warehouse as a Data Source to Reporting Engine" topic in the *Reporting Engine Configuration Guide*.

Error	Possible Solutions
Could not open connection to HiveServer	• Ensure that the HiveServer2 is running on the Host. • Check if the port provided can be accessible from the Reporting Engine server.
No Schema found in HDFS path	Ensure that meta avro data file(s) are available in the HDFS path (**<HDFS Path>/rsasoc/v1/sessions/meta**) mentioned. The following figure shows an example of the command to check the files in hdfs.
	
Could not open connection to HiveServer, GSS initiate failed	GSS initiate failed errors will be observed only in the case of Kerberos enabled Hive. Ensure that the proper keytab file is provided and it should have read options for the rsasoc user (user on which the Reporting Engine Server runs). Ensure that the system time is synchronized between KDC, Hadoop (HortonWorks) server, and the Reporting Engine system.

Manage a Stream and Lockbox

You can manage a stream using the following procedures:

- Edit a Stream
- Reload the Stream
- Specify meta filters for a Stream
- Define muti-valued metas

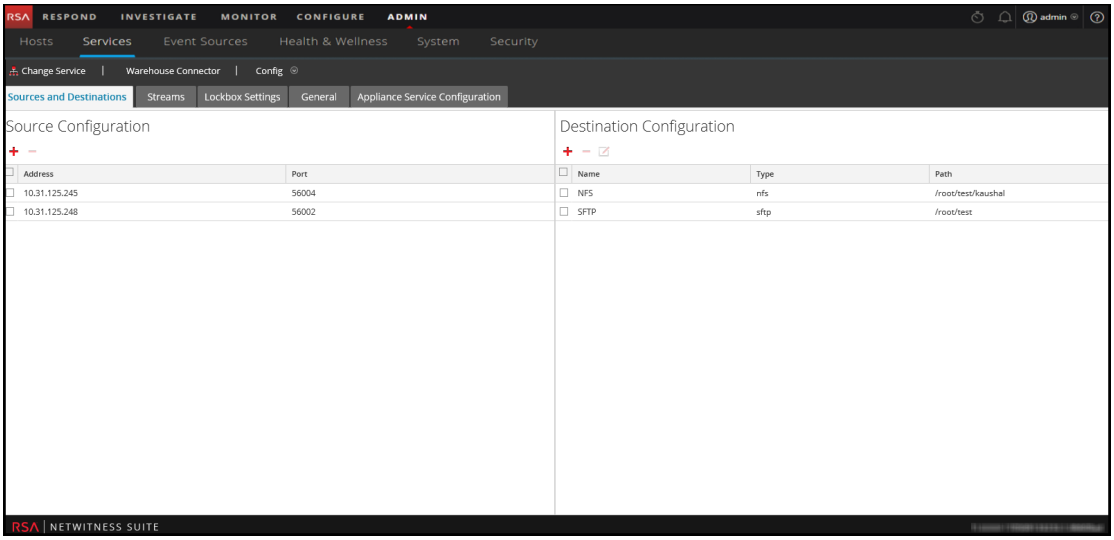
Edit a Stream

You can edit a stream to perform the following:

- Add more data sources to the stream.
- Delete existing data sources from the stream.

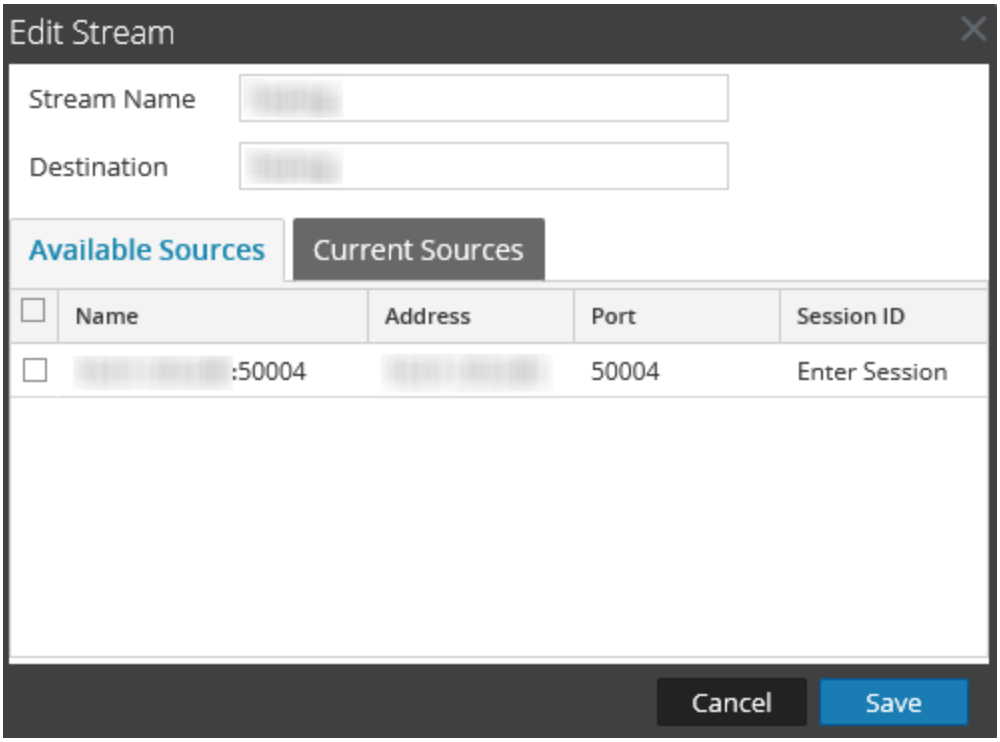
To edit a stream:

1. Go to **ADMIN > Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.
   The Services Config view of Warehouse Connector is displayed.



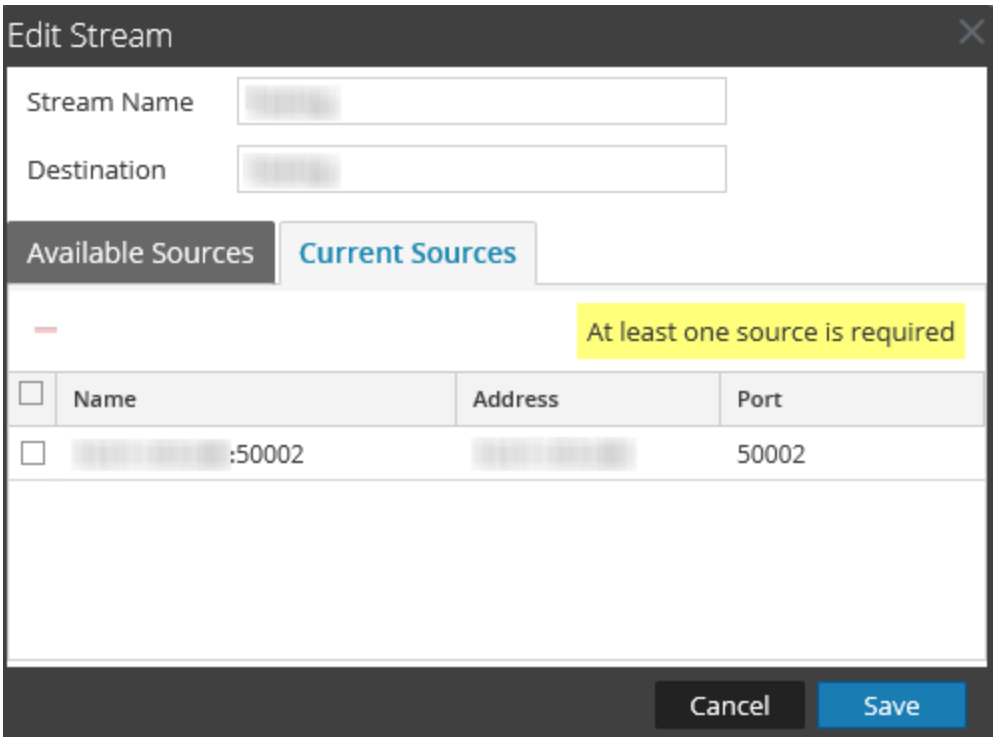
3. On the **Streams** tab, click .
4. In the **Edit Stream** dialog, you can perform the following:

- On the **Available Sources** tab, you can select the available data sources to add to the stream and click **Save**.



- On the **Current Sources** tab, you can delete an existing data source from the stream.

  Select the data source and click − .



Reload the Stream

When you reload the stream, the Warehouse Connector updates the schema file for the stream. You should reload the stream whenever you add a new custom meta to the Log Decoder or Decoder.

To reload the stream:

1. Go to **ADMIN > Services**.
2. In the Services view, select the added Warehouse Connector service and select **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.
3. On the **Streams** tab, select the stream that you want to reload.
4. Click **Reload**.

Specify Meta Filters for a Stream

You need to specify the filter for each stream in the `export.session.meta.fields` parameter in the Explore view of the Warehouse Connector.

The following table lists the values that you can provide as a filter:

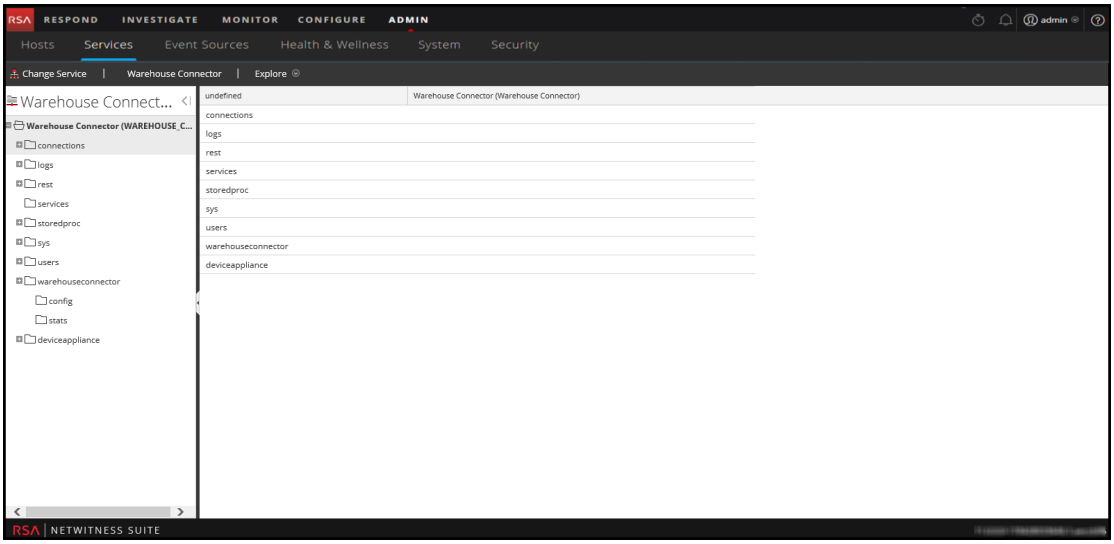
Values	Description
*	All the collected metas are written to SAW.
*, *meta1*, *meta2*	All the metas except the defined metas are written to SAW. For example, **Filter:** `*,ip.src` All the metas except `ip.src` is written to SAW.
meta1, meta2, meta3	Only the defined metas are written to SAW.

Note: By default, the following metas are written to Warehouse even if you specify them in the filter:
- ng_source
- unique_id
- time

To specify meta filters for a Stream:

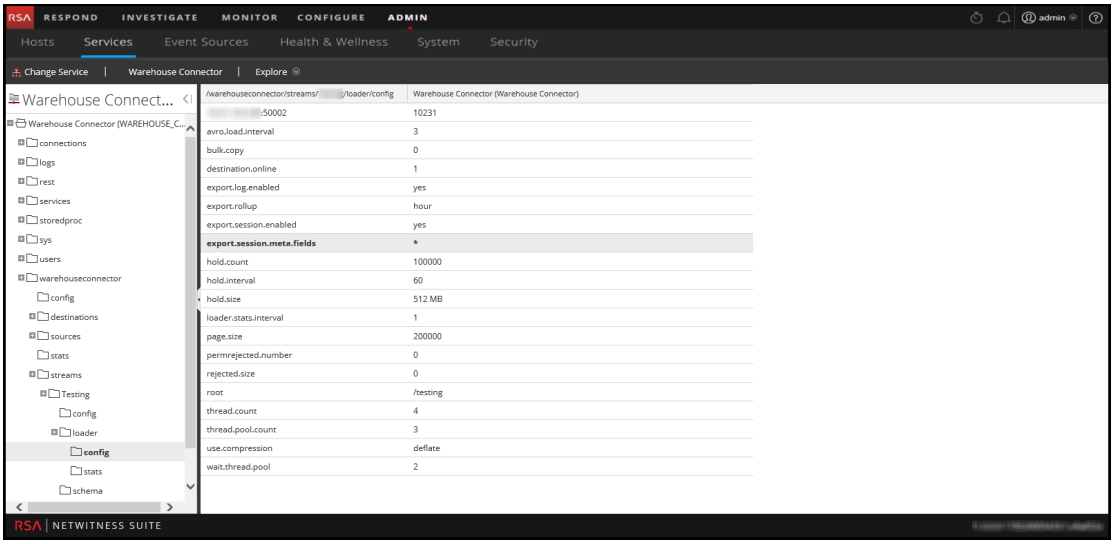
1. Go to **ADMIN > Services**.
2. In the Services view, select a Warehouse Connector services and select **> View > Explore**.

The Explore view of the Warehouse Connector service is displayed.



3. In the options panel, select **warehouseconnector > streams > <stream_name> > loader > config**.

4. In the `export.session.meta.fields` parameter, enter the filter.



5. Restart the stream.

Define Multi-valued Metas

You can also define an existing meta or a custom meta to be treated as multi-valued meta.

To define multi-valued metas:

Caution: Defining an existing meta to be treated as multi-valued may change the data type of the meta and cause the associated reports to fail.

1. Create a new file with the filename **multivalue-users.xml** in the **/etc/netwitness/ng** directory.
2. Add the following entries:

```
<?xml version="1.0" encoding="utf-8"?>

<Netwitness>
    <MultiValueMetas>
<Meta>NEWMETANAME</Meta>
    </MultiValueMetas>
</Netwitness>
```

   Where *NEWMETANAME* is the existing meta or a custom meta to be treated as multi-valued meta.

   Caution: Make sure that you do not add metas that are by default treated as non multi-value.

3. Restart the stream.

Manage a Lockbox

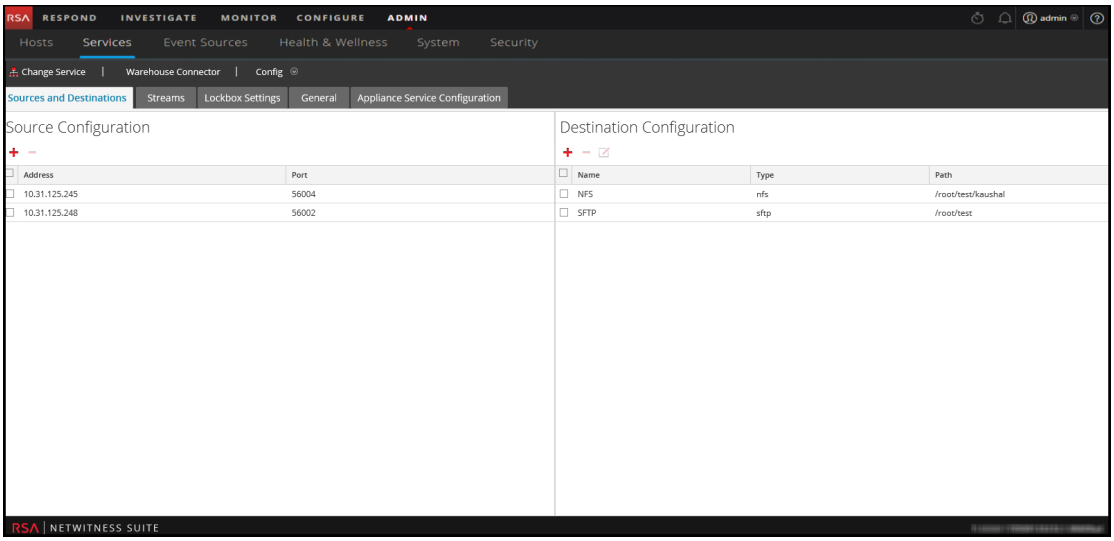
You can manage a lockbox using the following procedures:

- Change the Lockbox password
- Refresh the Lockbox

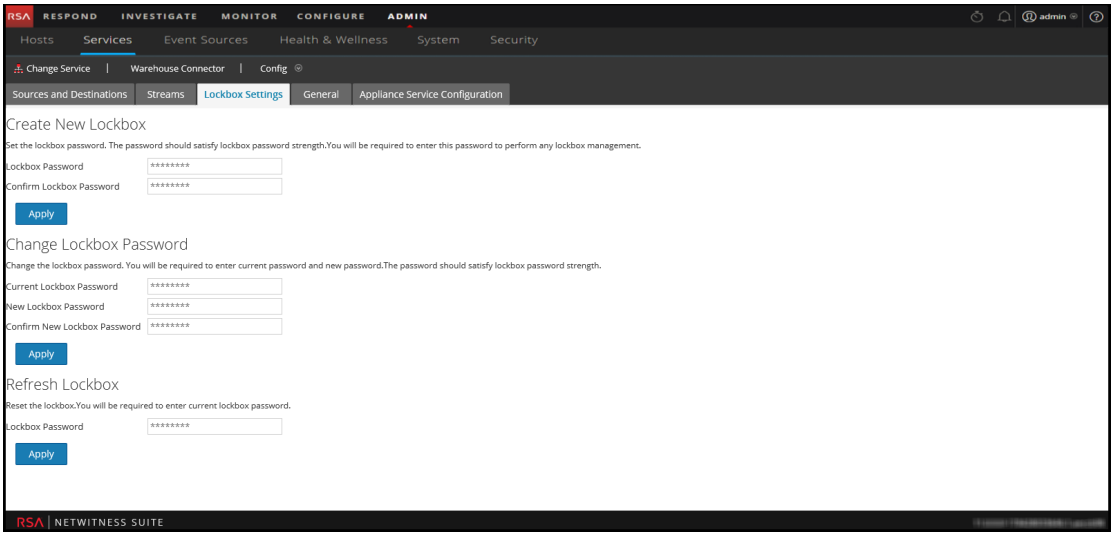
To change the Lockbox password:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service, and select **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.



4. Click the **Lockbox Settings** tab.



5. In the **Change Lockbox Password** section, perform the following:
   a. In the **Current Lockbox Password** field, enter the current lockbox password.
   b. In the **New Lockbox Password** field, enter the new lockbox password.

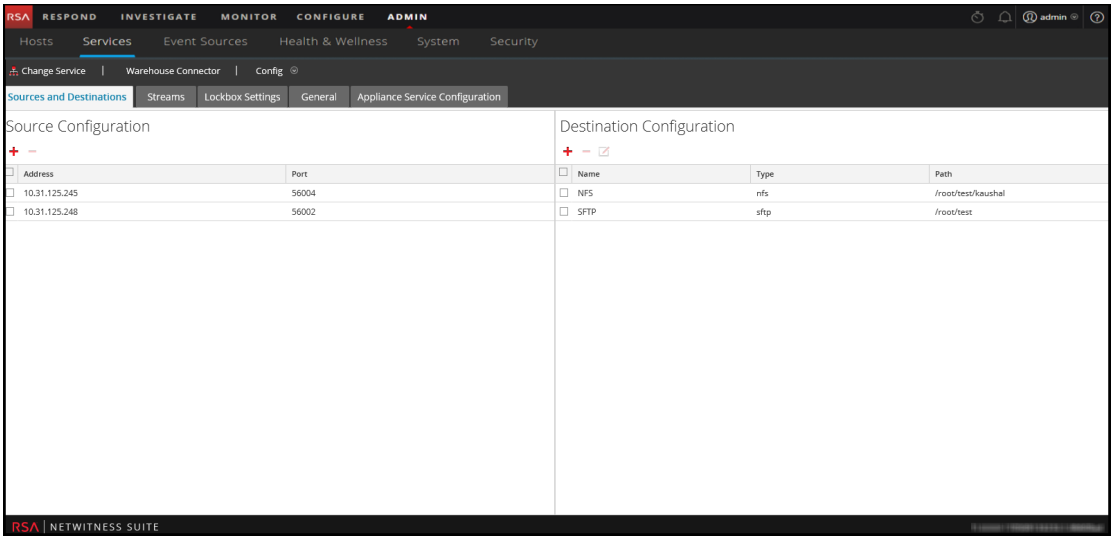
      Note: The lockbox password must be at least eight characters in length and it must contain at least three of the following groups: one uppercase character [A-Z], one lowercase character [a-z], one numeral [0-9], and one special character.

   c. In the **Confirm New Lockbox Password** field, enter the new lockbox password to confirm.
   d. Click **Apply**.
      The Lockbox password is successfully changed.

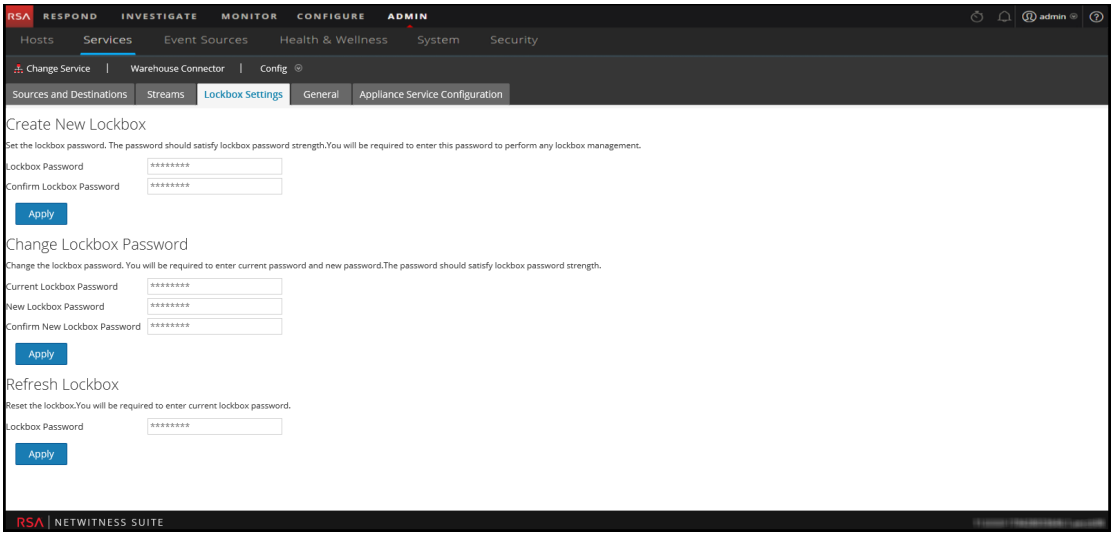
To refresh the Lockbox:

1. Log on to NetWitness.
2. Go to **ADMIN > Services**.
3. In the Services view, select the added Warehouse Connector service, and select **> View > Config**.

The Services Config view of Warehouse Connector is displayed.



4. Click the **Lockbox Settings** tab.



5. In the **Refresh Lockbox** section, enter the current lockbox password in the **Lockbox Password** field.
6. Click **Apply**.
   The Lockbox is reset.

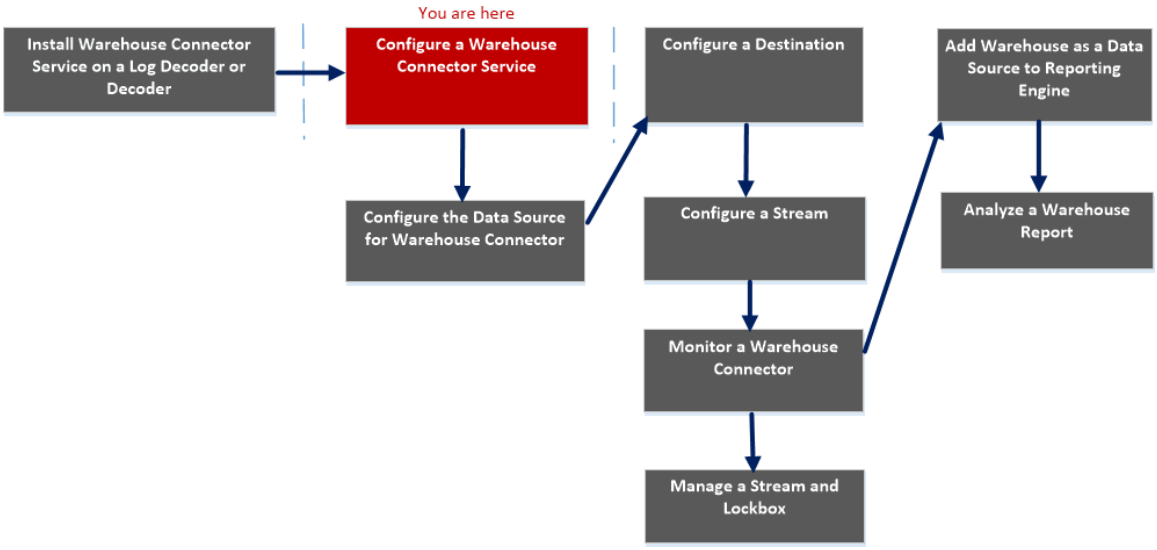
Warehouse Connector Configuration References

This section contains descriptions of the user interface as well as other reference information.

General Tab Settings

The General tab displays the general configuration settings for Warehouse Connector service.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS

Role	I want to...	Refer to...
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

*You can complete these tasks here.

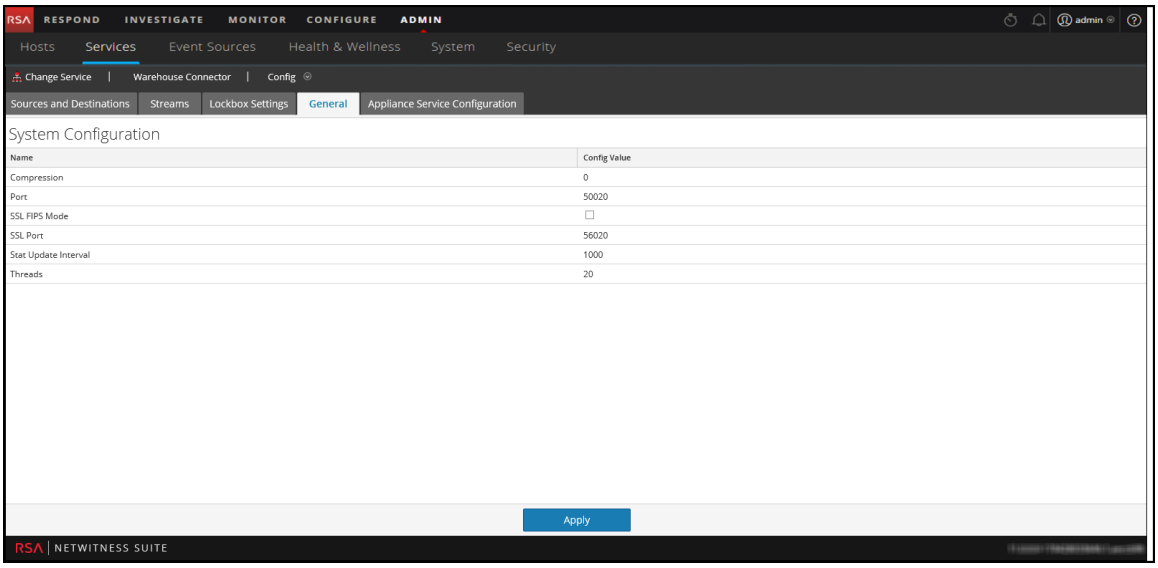
Related topics

- Configure a Warehouse Connector Service

Quick Look

The following figure shows the General tab on the Warehouse Connector Services Config view.

The General tab displays the system configuration parameters for the Warehouse Connector service.



When you add a Warehouse Connector service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

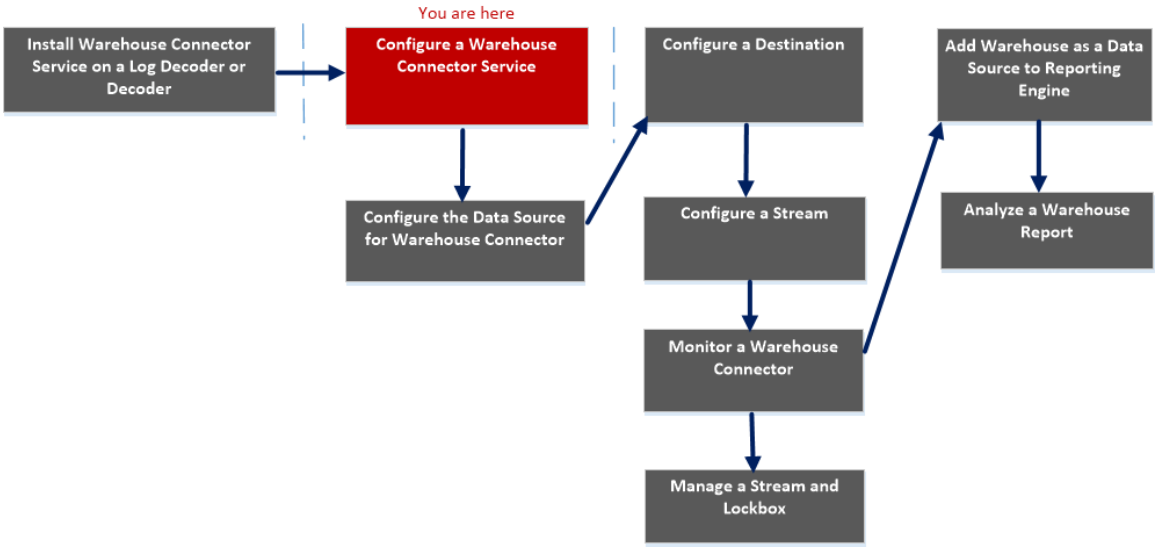
The following table describes the System Configuration parameters:

Name	Config Value
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.
Port	Determines the port used by the service. **Note:** If you change the port number, ensure that you restart the service.
SSL	If enabled, all the data transferred in the network will be encrypted using SSL.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system.
Threads	Determines the number of threads in the thread pool to handle incoming requests.

Appliance Service Configuration Tab Settings

The Appliance Service Configuration tab displays the appliance configuration settings for Warehouse Connector service. For more information, see "Appliance Service Configuration" topic in the *Hosts and Services Getting Started Guide*.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector

Role	I want to...	Refer to...
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

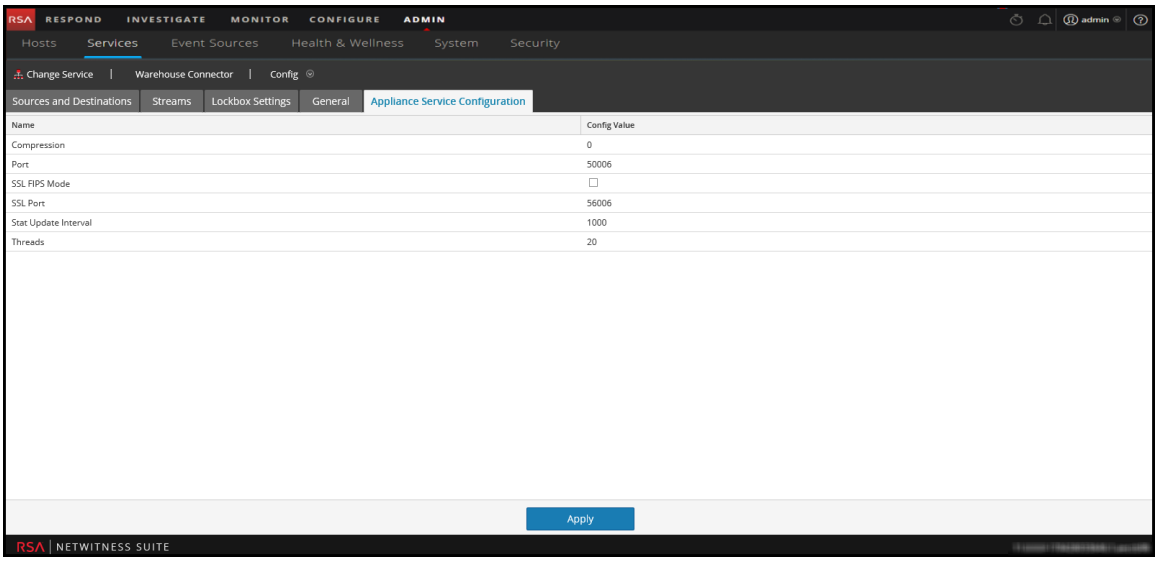
*You can complete these tasks here.

Related topics

- Configure a Warehouse Connector Service

Quick Look

The following figure shows the different settings on the Appliance Service Configuration tab.



When you add a Warehouse Connector service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

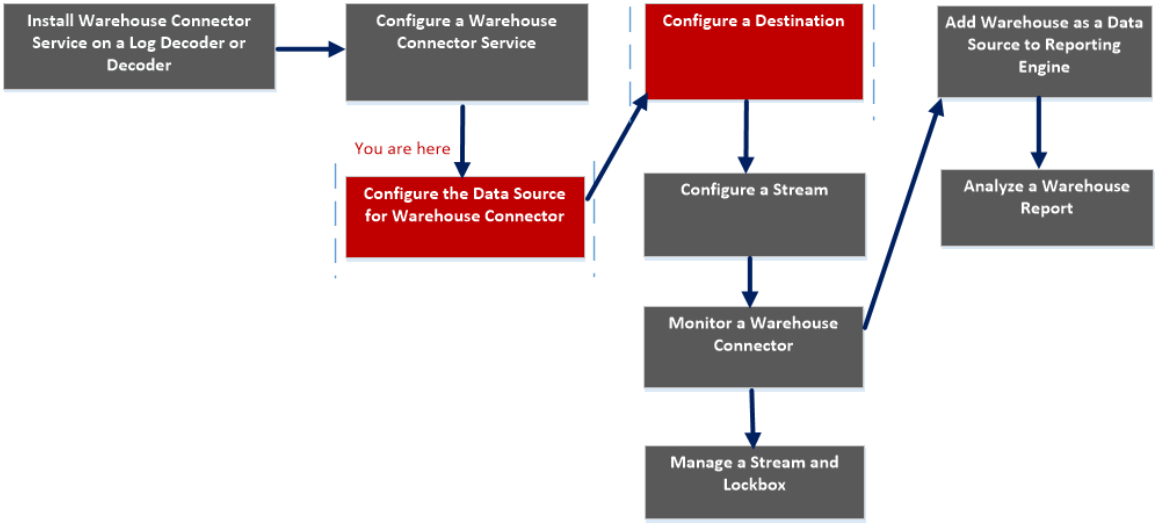
The following table describes the Appliance Service Configuration parameters:

Name	Configuration Value
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.
Port	Determines the port used by the service. **Note:** If you change the port number, ensure that you restart the service.
SSL FIPS Mode	If enabled, all the data transferred in the network will be encrypted using SSL FIPS.
SSL Port	Determines the SSL port used by the service.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system.
Threads	Determines the number of threads in the thread pool to handle incoming requests.

Sources and Destinations Configuration

The Sources and Destinations tab for a Warehouse Connector in the Services Config view provides a way to manage basic service configuration and configure source and destination.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector*	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS*	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS

Role	I want to...	Refer to...
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

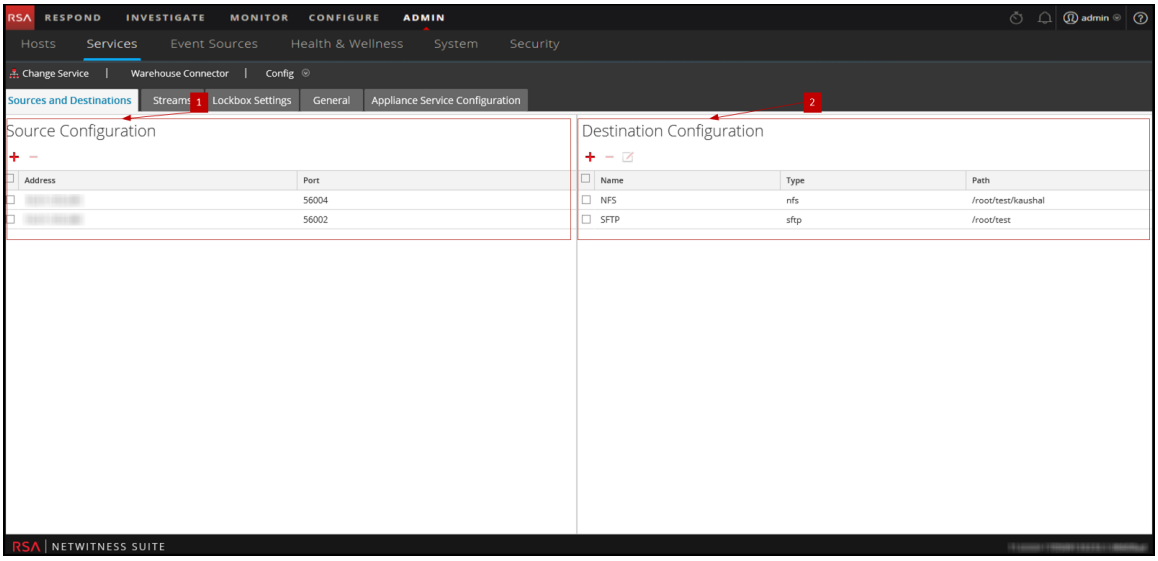
*You can complete these tasks here.

Related topics

- Configure the Data Source for Warehouse Connector
- Configure the Destination

Quick Look

The following figure shows the Sources and Destinations tab on the Warehouse Connector Services Config view.



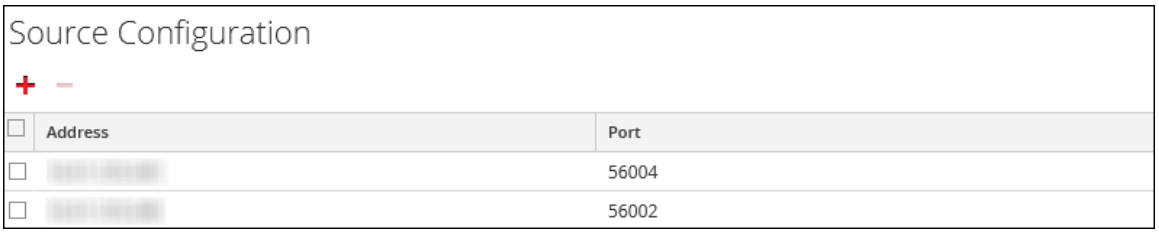
The Sources and Destinations tab includes the following two sections:

1. Source Configuration
2. Destination Configuration

Source Configuration

The Source Configuration section allows you to configure the data sources from which the Warehouse Connector service needs to collect data.

The following is an example of the Source Configuration section.

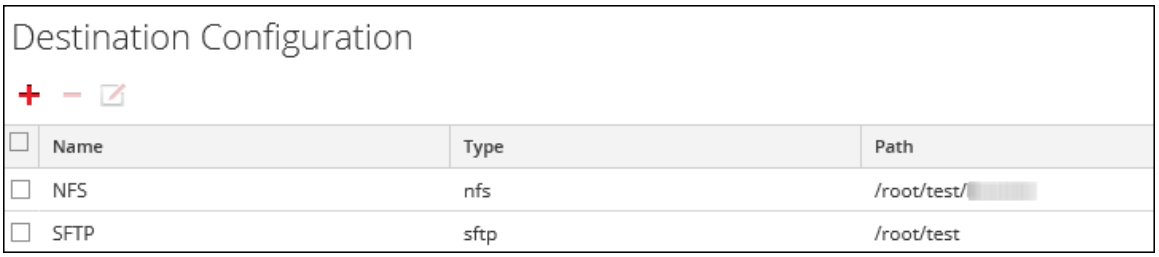


The Source Configuration section allows you to perform the following:

Features	Description
+	Add the data source.
−	Delete the data source.

Destination Configuration

The Destination Configuration section allows you to configure the destination to which the Warehouse Connector service needs to write the collected data.



The Destination Configuration section allows you to perform the following:

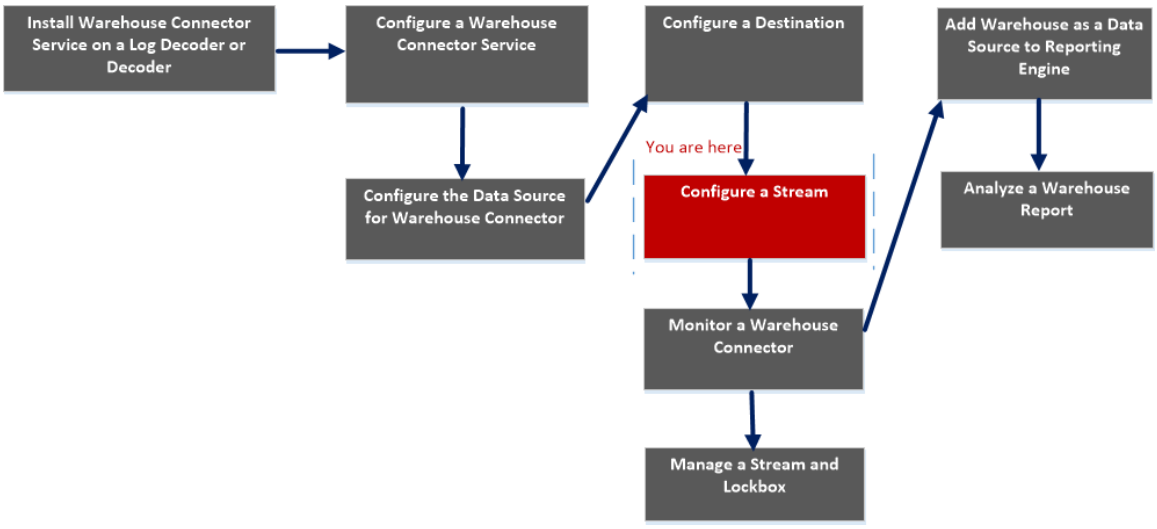
Features	Description
+	Add the destination.

Features	Description
	Delete the destination.
	Edit the destination. **Note:** You can only edit the SFTP destination type.

Add Stream Dialog

You can configure and add a stream to a Warehouse Connector in this dialog

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS

Role	I want to...	Refer to...
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

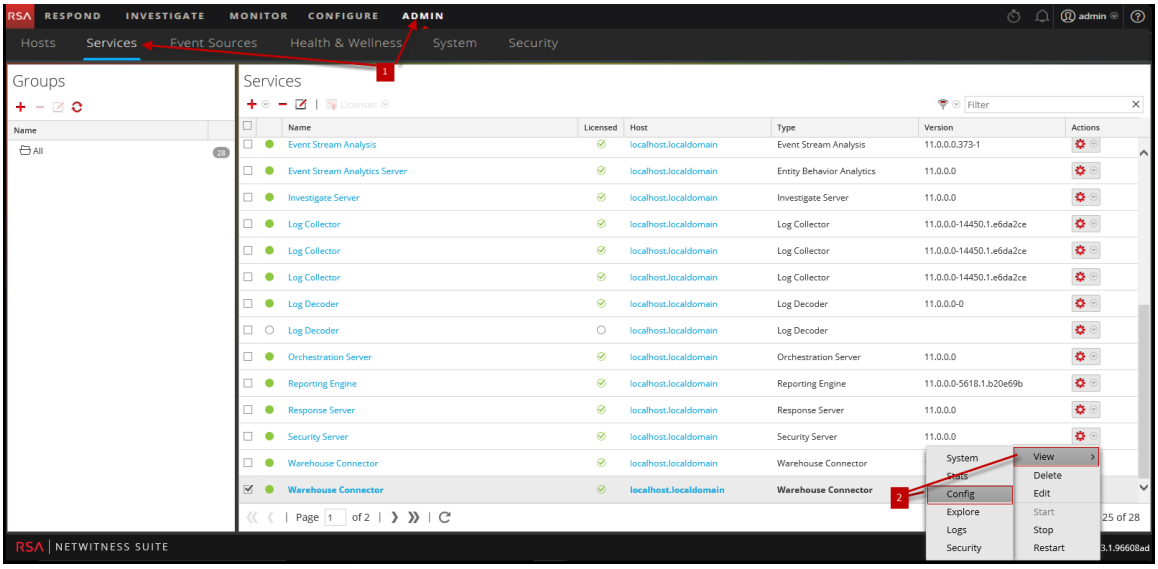
*You can complete these tasks here.

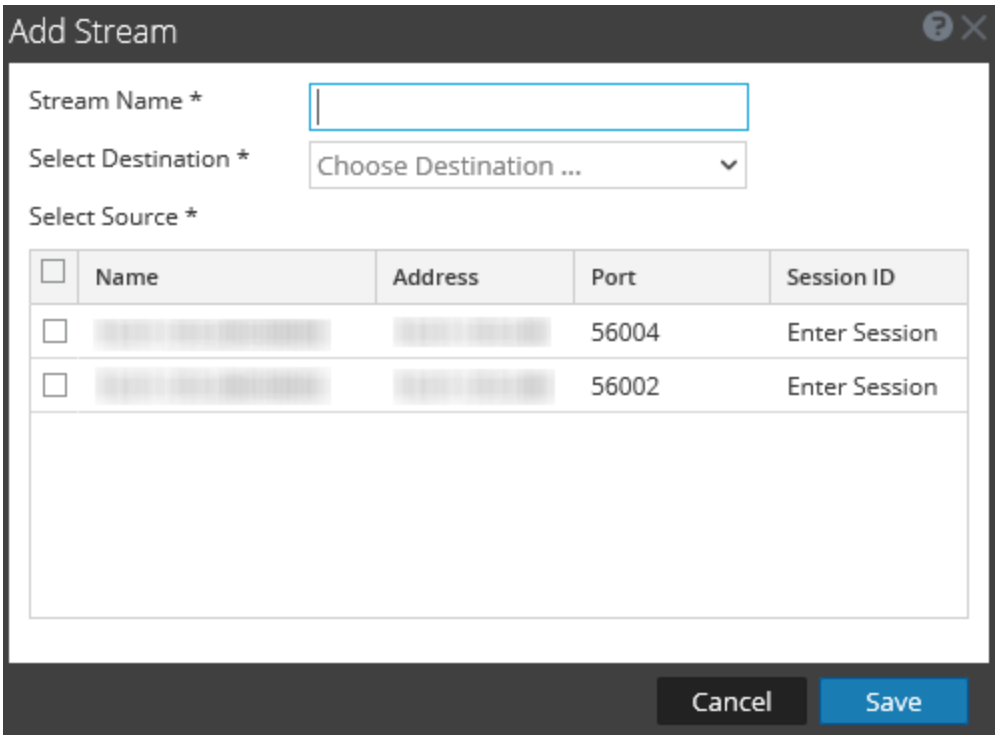
Related Topics

- Configure a Stream

Quick Look

The following figure is an example with the important features labeled.





1. Go to **ADMIN > Services**.
2. In the services view, select a Warehouse Connector service and select

   >view>config
3. In the **Streams** tab, click + to view the add stream dialog.

The following table describes the fields in the Add Stream dialog:

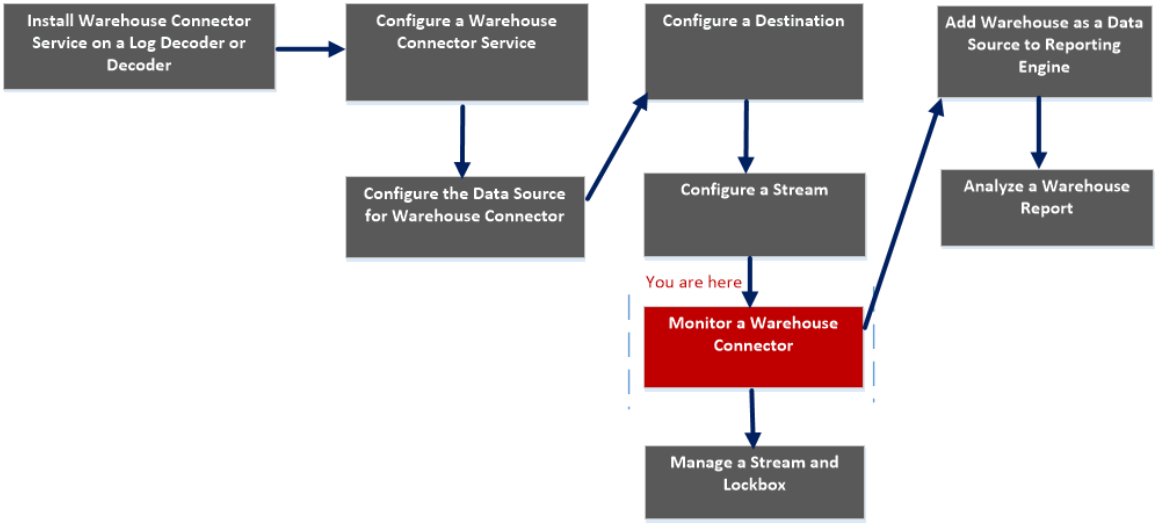
Parameter	Description
Stream Name	Type the name of the stream. The stream name may only contain alphanumeric characters and underscores. It cannot exceed 20 characters in length.
Select Destination	Select a destination from the drop-down list.

Parameter	Description
Select Source	Select a source from the grid at the bottom section of the dialog.
Name	The name of the source.
Address	The address of the source.
Port	The port of the source.
Session ID	The session ID of the source.

Streams Configuration

The Streams tab for a Warehouse Connector in the Services Config view provides a way to manage stream configuration.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS

Role	I want to...	Refer to...
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector*	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

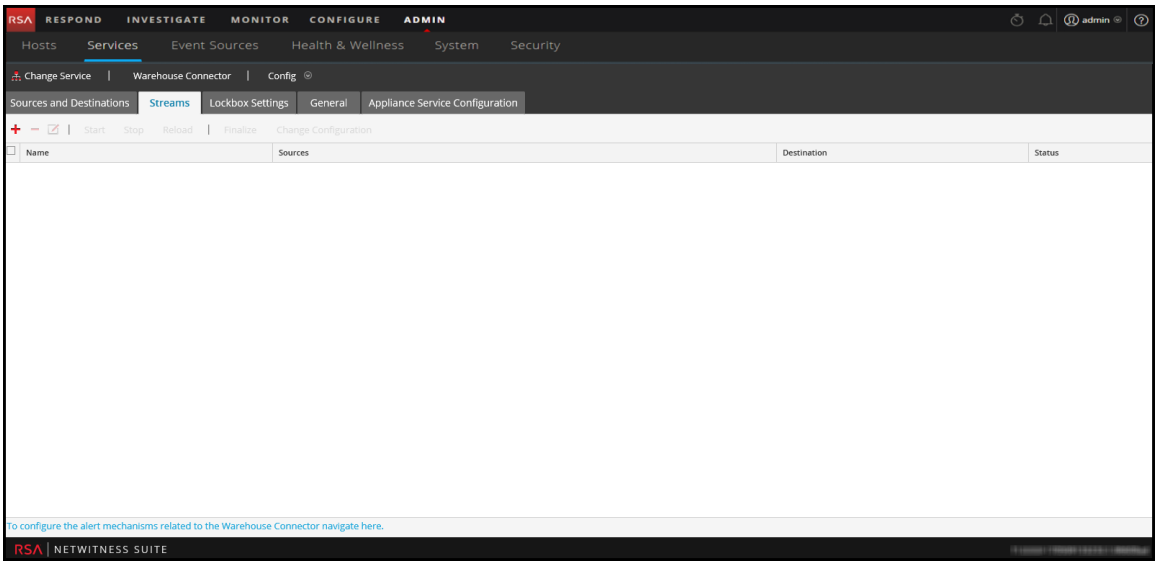
*You can complete these tasks here.

Related topics

Configure a Stream

Quick Look

The following figure shows the Streams tab on the Warehouse Connector Services Config view.



The Streams tab allows you to perform the following:

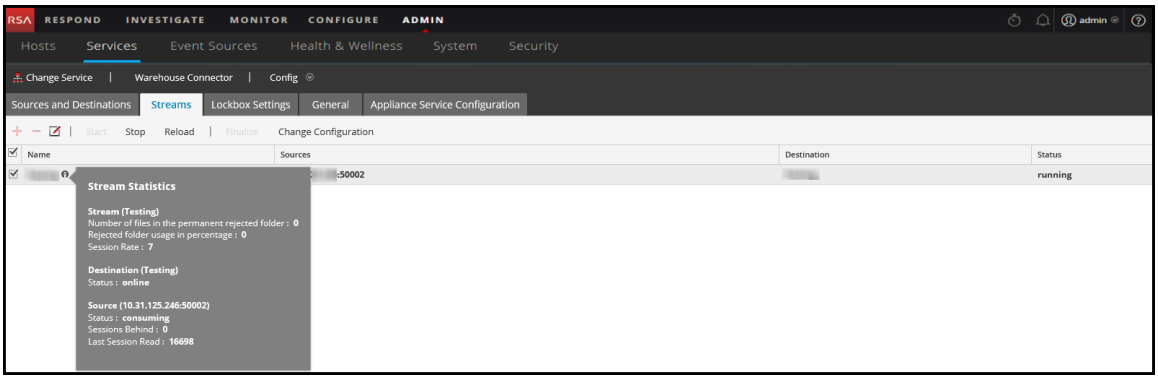
Features	Description
	Add a stream.
	Delete a stream.
	Edit the stream.
Start	Start the stream.
Stop	Stop the stream.
Finalize	Finalize the stream.
Reload	Reload the stream. If you have added a new meta or if a new meta is added as part of content update to any of the sources, Log Decoder or Decoder, you need to reload the stream for the meta to be visible in the schema for the Reporting Engine. Reloading a stream does not have any impact on the data, but only the new meta list is fetched from the sources.

The following table describes the fields in the Streams tab:

Parameter	Description
Name	Name of the stream.
Sources	The sources associated with the stream.
Destination	The destinations associated with the stream.
Status	Status of the stream.

Stream Statistics

You can view the statistics of a configured stream. Click the icon next to the name of the stream.



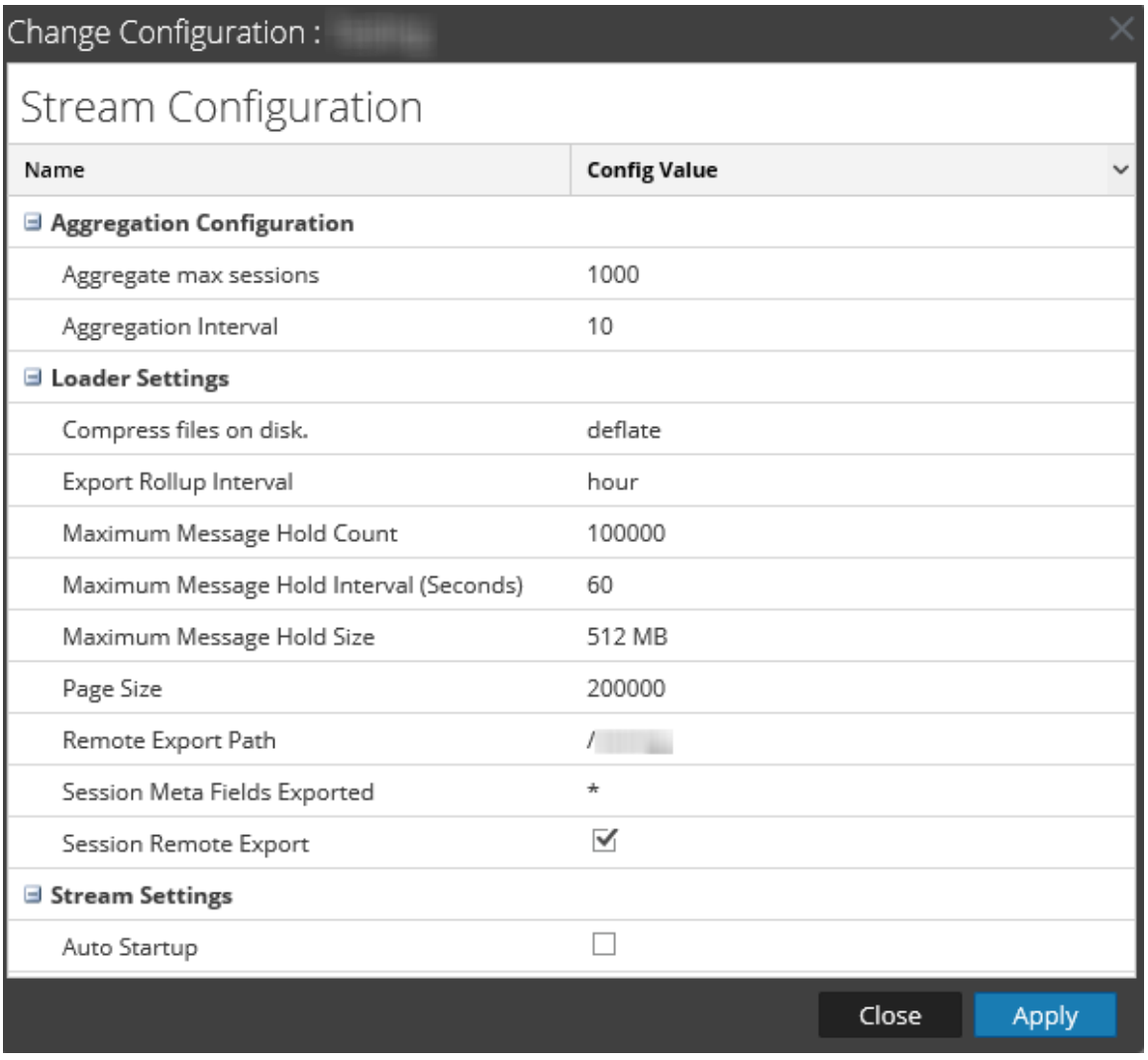
The following parameters are displayed in the Stream Statistics:

Section	Parameter	Description
Stream		
	Number of files in the permanent rejected folder	Determines the number of files in the permanent rejected folder (named, **permfail**) in the Warehouse Connector. The permanent rejected folder contains the files that Warehouse Connector failed to write to the destination.
	Rejected folder usage in percentage	Determines the disk usage of the rejected folder.
	Session Rate	Determines the rate at which the session is processed by the Warehouse Connector for the source.
Destination		
	Status	Indicates the status of the destination.
Source		
	Status	Indicate the status of the source.
	Sessions Behind	Determines that number of sessions that needs to be processed by the Warehouse Connector.

Section	Parameter	Description
	Last Session read	Determines the last session id processed by the Warehouse Connector.

Change Stream Configuration

You can change configuration of a stream in runtime. In the **Streams** tab, click **Change Configuration** to change the configuration of the selected stream.



You can change the following parameters of the Stream Configuration:

Note: If you change the value of any parameter in stream configuration, make sure that you restart the stream.

After upgrading, if the values of Maximum Message Hold Count, Maximum Message Hold Interval and Maximum Message Hold Size are 3000000, 60 and 128 respectively, ensure that you assign the following values to the streams:

- Maximum Message Hold Count - 2400000
- Maximum Message Hold Interval - 600
- Maximum Message Hold Size - 512

You can assign these values by modifying the existing Stream configuration.

Section	Parameter	Description
		Aggregation Configuration
	Aggregate max sessions	Determines the maximum number of sessions in a response for an aggregation request from the Warehouse Connector to the source .
	Aggregation Interval	Determines the time between the responses from the source.
		Loader Settings
	Compress files on disk	Enable to compress files on disk. Supported values: • Deflate - Provides smaller compressed files and good performance while generating reports. • Off By default, the parameter is set to **deflate**.

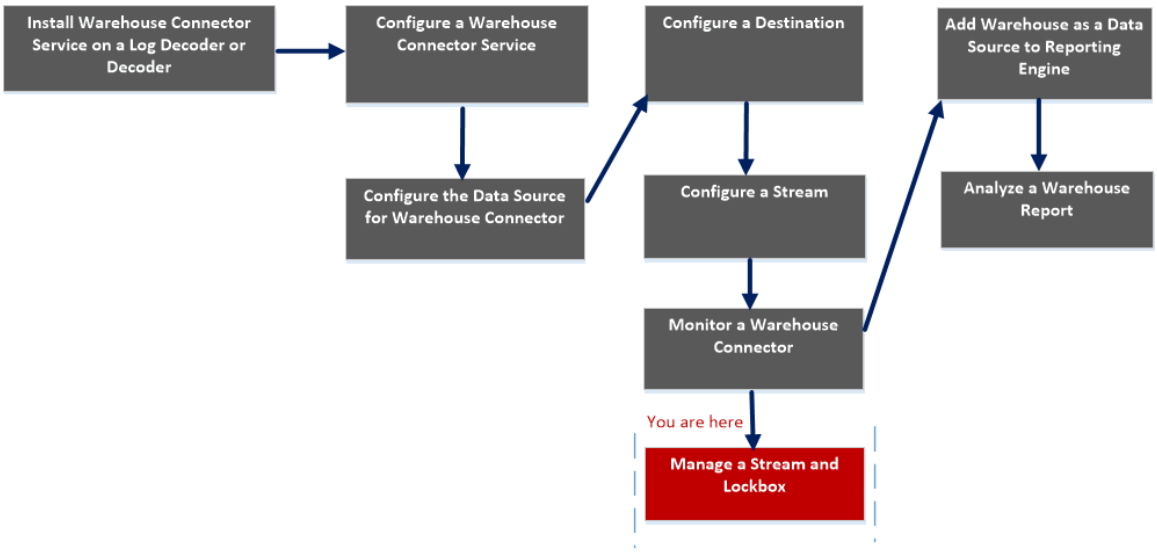
Section	Parameter	Description
	Export Rollup Interval	Determines the roll-up interval for export files and also the directory structure the Warehouse Connector writes to the destination. For example: If the parameter is set to: **Value** **Directory Structure** hour /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day}/{hour} minute /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day}/{hour}/{minute} day /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day} If you change the value of the parameter, ensure that you restart the stream. Recommended value is **hour**.
	Maximum Message Hold Count	Determines the maximum number of sessions to store in the memory before processing. **Note:** If you have deployed a Warehouse Connector Virtual Appliance, make sure that you change the default value of the parameter to 800000.
	Maximum Message Hold Interval (Seconds)	Determines the maximum time (in seconds) to hold the sessions in memory before processing.
	Maximum Message Hold Size	Determines the maximum size for the sessions to store in the memory before processing.

Section	Parameter	Description
	Remote Export Path	Determines the remote local mount point for HDFS (nfs://) and the location to export the data.
	Page Size	
		Stream Settings
	Auto Startup	Enable to automatically start the stream whenever the Warehouse connector process is restarted. By default, the parameter is set to **off**.

Lockbox Settings

The Lockbox Settings tab for a Warehouse Connector in the Services Config view provide a way to manage the lockbox settings.

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector

Role	I want to...	Refer to...
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the *Warehouse Guide*.
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

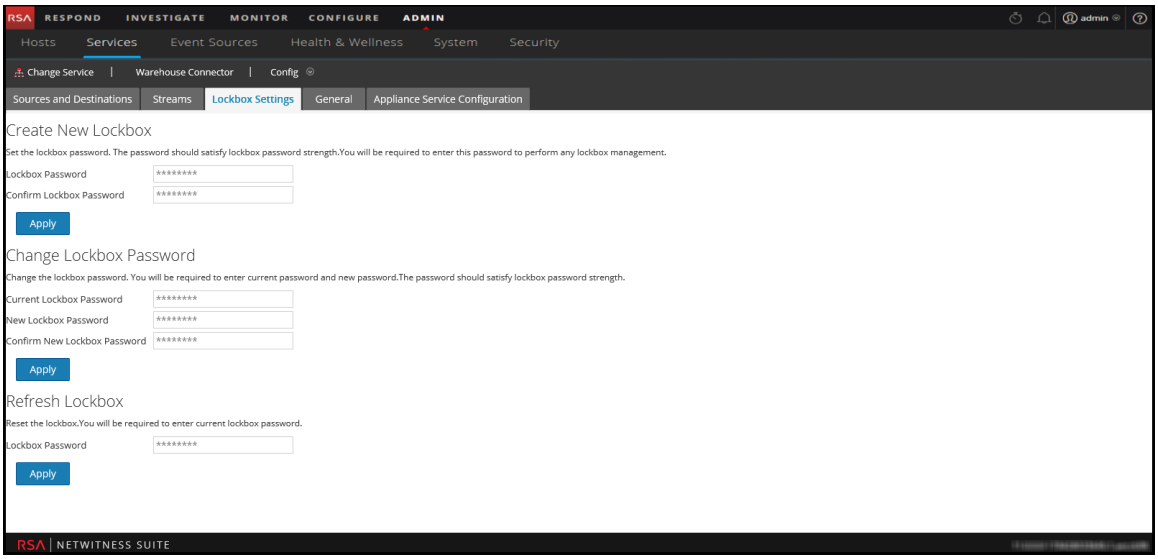
*You can complete these tasks here.

Related topics

- Configure a Warehouse Connector Service
- Manage a Stream and Lockbox

Quick Look

The following figure shows the Lockbox settings tab on the Warehouse Connector Services Config view.



The Lockbox Settings tab allows you to set, change, or refresh the lockbox password of the Warehouse Connector.

RSA NETWITNESS® SUITE

Warehouse (MapR) Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

RSA NetWitness Warehouse Overview 4

How Warehouse (MapR) Works 5

Configure MapR 7

Generate and Update the Default UUID in Appliances 7

Update the Configuration Template File 7

Upgrade the Warehouse Cluster 9

Install the Warehouse License File 10

Generate the Virtual IP Address for Primary Appliance 11

Configure other NetWitness Suite Services 12

Stop the Hbase Services Using the Command Line 12

Stop the Hbase Services Using the MapR Control System 14

Configure Warehouse Connector to Write to NetWitness Warehouse 18

Verify the Network File System (NFS) Services Status 18

Install the Network File System Packages 18

Mount the Warehouse on the Warehouse Connector 19

Manage MapR Cluster 22

Access MapR Control System UI for Cluster Administration 22

Enable MapR Metrics on RSA NetWitnessWarehouse Cluster 23

Edit and Remove Virtual IP Addresses (Command Line) 24

Add and Remove a Virtual IP Address (MapR UI) 25

Add a Virtual IP Address with Multiple Nodes (MapR UI) 30

Optimal VIP Configuration 30

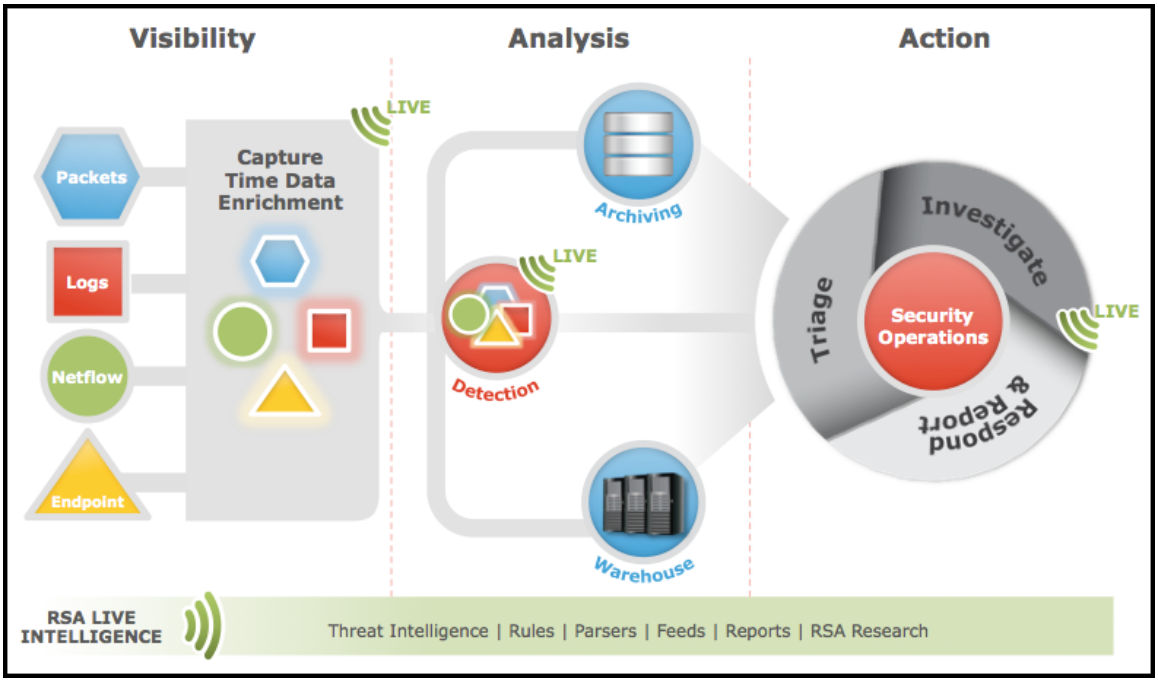
Optimal Configuration with the Warehouse Connector 30

RSA NetWitness Warehouse Overview

RSA NetWitness Warehouse provides the capacity to process large amounts of current and long term data through a Hadoop-based distributed computing system that collects, manages, and enables advanced analytics and reporting on NetWitness Suite data. RSA NetWitness Warehouse requires a service called Warehouse Connector to collect metadata and events from Decoder and Log Decoder and write them in Avro format into a Hadoop-based distributed computing system. For more information on the Warehouse Connector, see "How Warehouse Connector Works" topic in the *Warehouse Connector Configuration Guide*.

The Warehouse is made up of three or more nodes depending on the organization's analytic, archiving, and resiliency requirements.

The following figure depicts the architecture of a NetWitness Suite network that implements the RSA NetWitness Warehouse component.



How Warehouse (MapR) Works

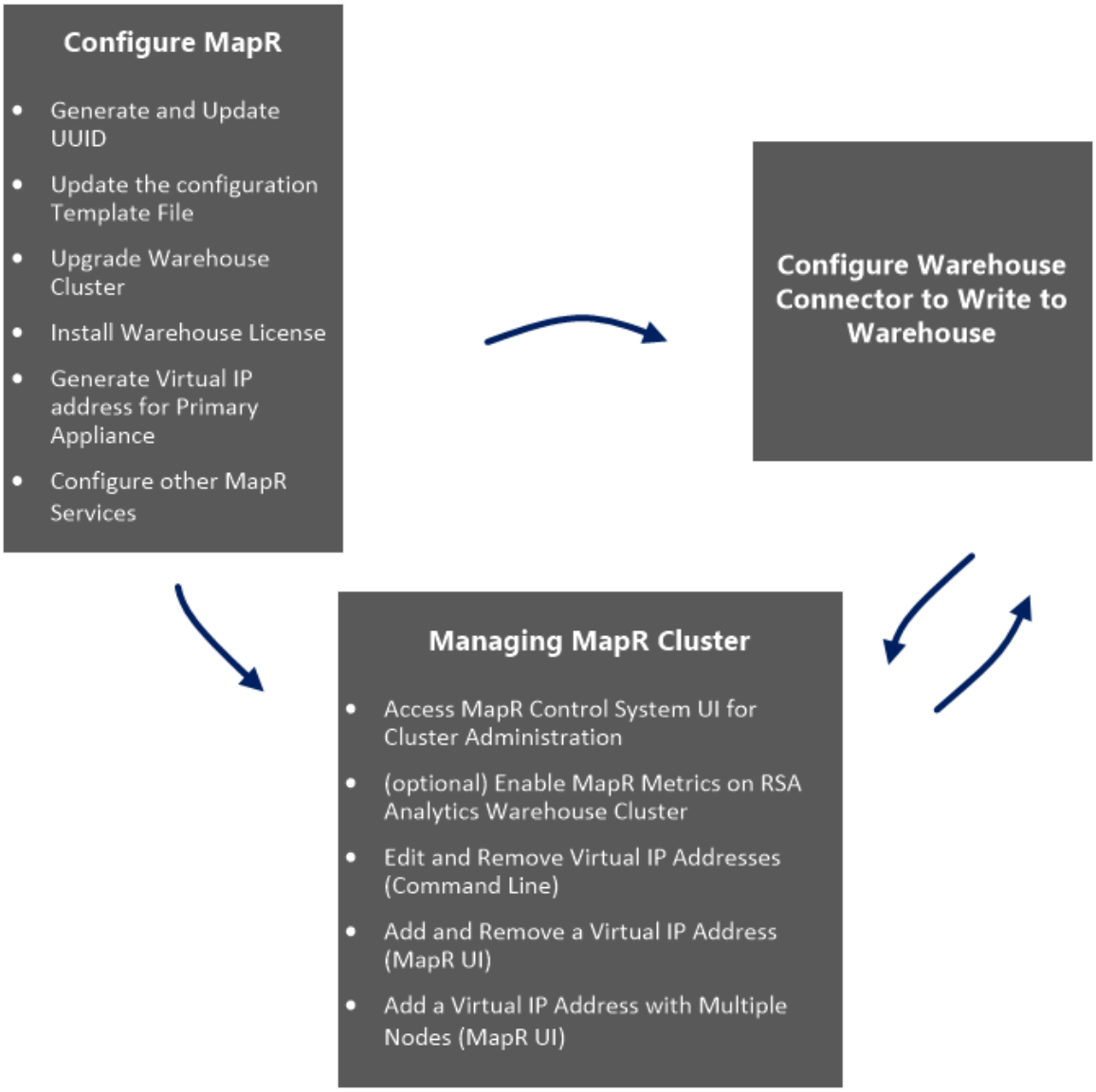
You must configure the nodes for the RSA NetWitness Warehouse (MapR). It only applies to RSA NetWitness Warehouse instances running MapR.

Prerequisites

Make sure that you have:

- Installed the RSA NetWitness Warehouse appliance in your network environment. For more information, see "RSA Analytics Warehouse (MapR) Setup Guide" in the *Hardware Setup guides*.
- Configured the network interface of the Warehouse appliance.

This figure is an overview of the entire process of configuring Warehouse appliance in your network.



To configure the nodes for the RSA NetWitness Warehouse (MapR), perform the following:

Note: If you are planning to have a cluster of Warehouse appliances, make sure you perform the following tasks on all the appliances in the cluster.

Caution: Prerequisites are mandatory. Your installation will fail if you have not set the network configuration as described in the *RSA Analytics Warehouse (MapR) Setup Guide* or *Virtual Host Setup Guide* depending on your deployment.

1. Configure MapR
2. Configure Warehouse Connector to Write to NetWitness Warehouse
3. Manage MapR Cluster

Configure MapR

You can configure MapR using the following procedure:

Generate and Update the Default UUID in Appliances

You need to manually generate and update the default Universally Unique Identifier (UUID) on the Appliances in the cluster. The UUID must be unique to the Appliance in the cluster.

To generate and update the default UUID in the Appliance:

1. Log on to the Appliance as root user.
2. Generate the UUID and copy it in the correct files, using the following commands:
   - `/opt/mapr/server/mruuidgen > /opt/mapr/hostid`
   - `cp /opt/mapr/hostid /opt/mapr/server/hostid.xxxxx`

   Where, xxxxx refers to the 5-digit number randomly assigned to the existing file.

   Note: Review `/opt/mapr/server` for the full name of this file.
3. Restart the appliance, using the following command:
   `reboot`

Update the Configuration Template File

You must update the configuration template file in the RSA NetWitness Warehouse Appliance. The configuration template file in the RSA NetWitness Warehouse appliance must include the following parameters:

- nodes
- Internalnetworks
- clustername
- disks

By default, a configuration template is provided with the RSA NetWitness Warehouse appliance and is located on the RSA NetWitness Warehouse appliance at `/opt/rsa/saw/install`.

Prerequisites

Make sure that you validated the volume in the server to identify available drive space for Warehouse to store data. The total drive space of the additional volume is considered as a single drive by the HDFS. In Warehouse, the AVRO files are stored in the drive space.

Note: The server contains additional volumes of identical size other than the operation system volume.

To check free space, enter the command `fdisk -l | grep /dev/s |sort` in the Warehouse node. You will get a list of disks that are not partitioned for usage. You need to list the identified disks in the configuration template file so that Warehouse utilizes this space for the Hadoop Cluster.

To update the configuration template file in the RSA NetWitness Warehouse Appliance:

1. Log on to the appliance as the root user.
2. Navigate to `/opt/rsa/saw/install`, enter the following command:

   ```
   cd /opt/rsa/saw/install
   ```
3. Create a copy of the configuration template, enter the following command:

   ```
   cp conf.template conf.template-<name>
   ```

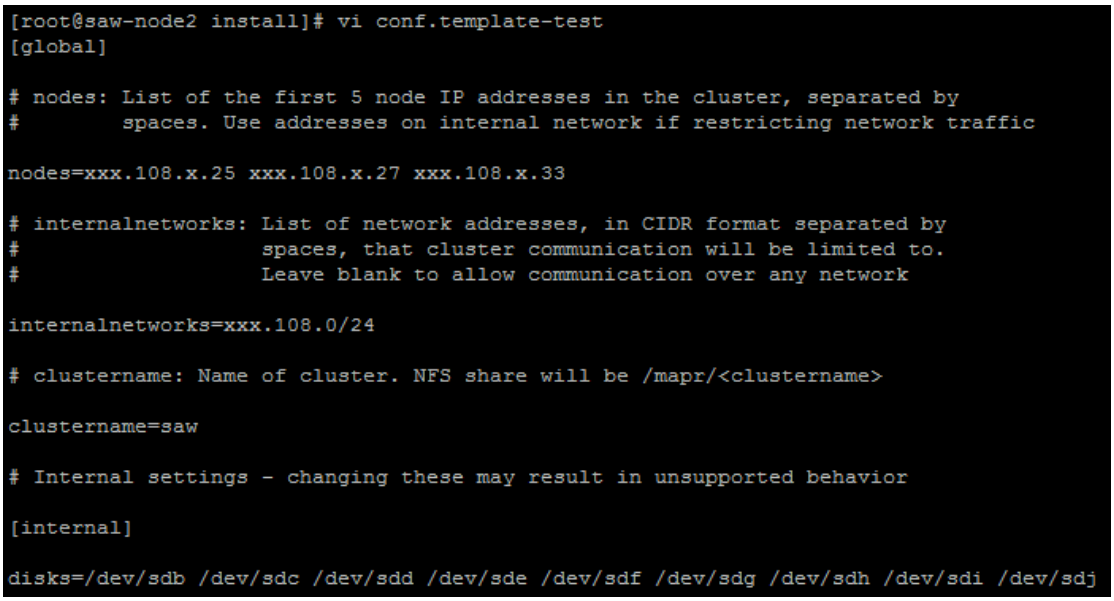
   where `<name>` is the custom name of the configuration template file.
4. Edit the configuration template file, enter the following command:

   ```
   vi conf.template-<name>
   ```

Parameter	Description
Nodes	List the IP addresses of the appliances in the cluster separated by spaces. All the appliances in the cluster must be listed in the same order in every configuration file for each RSA NetWitness Warehouse appliance.
Internalnetworks	List the network addresses in CIDR format separated by spaces. This Warehouse appliance cluster communication is limited to the provided network addresses. **Note:** RSA recommends that you do not leave this parameter blank.
Clustername	Name of the cluster. The cluster name is used to identify the Network File System (NFS) share.

Parameter	Description
Disks	Displays the list of disks recognized by the operation system, and these disks will be formatted in HDFS for the Warehouse when this configuration script is executed.

The following figure displays a sample configuration template file:



5. Execute the configuration template file, using the following command:

   ```
   ./configure.py conf.template-<name>
   ```

6. Restart the appliance, using the following command:

   ```
   reboot
   ```

Upgrade the Warehouse Cluster

You must upgrade the warehouse cluster after updating the configuration template file and reboot the RSA NetWitness Warehouse appliance.

To Upgrade the Warehouse Cluster

You must manually open Hiveserver port 10000, which is not opened by default:

1. Get the line number where the REJECT statement appears in the Iptable.
2. Make sure that the Iptables service is running, using the following command:

   ```
   NUM=$(iptables -L INPUT -n --line-numbers |grep 'reject-with'
   |awk ' {print $1}')
   ```

Note: The ACCEPT statements that follow the REJECT statement in the Iptables will not take effect. You can incorporate the line number of the REJECT statement in the command to ensure that the ACCEPT statements proceed the REJECT statement.

3. Add the firewall exception for port 10000 to the Iptables. Enter the following command:

   ```
   iptables -I INPUT $NUM -m state --state NEW -p tcp --
   dport 10000 -j ACCEPT
   ```

4. Save the Iptables. Enter the following command:

   ```
   /etc/init.d/iptables save
   ```

5. Restart the Iptables. Enter the following command:

   ```
   /etc/init.d/iptables restart
   ```

6. Verify if the firewall exceptions for the ports are added. Enter the following command:

   ```
   Service iptables status | grep 10000
   ```

   The following output should be displayed:

   ```
   ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:10000
   ```

Install the Warehouse License File

You need to manually install the Warehouse license file on the Warehouse appliance. If you have a cluster of Warehouse appliances, you need to install the license file on the first Warehouse appliance in the cluster.

Prerequisites

Make sure that you have:

- Obtained the Warehouse license file.
- Copied the license file to `/root/` on the first Warehouse appliance in the cluster using a USB drive or through SCP.

To install the Warehouse license file:

1. Log on to the appliance as a root user.
2. Install the license file, using the following command:

   ```
   maprcli license add -is_file true -license <license_filename>
   ```

where <license_filename> is filename of the RSA NetWitness Warehouse license file. The license file is installed without any output messages. If you included a network range in the internalnetworks parameter in the configuration template file, a warning message appears suggesting that the Warehouse is configured only to communicate with the network entered in the configuration template file. You can ignore this warning as this does not have any functional issue.

3. Confirm the license file installation, using the following command:

   ```
   maprcli license list
   ```

   The output messages appears on the console screen. The last two lines of the output message should be similar to the following sample:

   ```
   hash: "b8xO1flW8EMNSqq7zztn8D2BXnQ="
    3 May 14, 2013
   ```

4. Retrieve a list of directories, run the following command:

   ```
   hadoop fs -ls /
   ```

Generate the Virtual IP Address for Primary Appliance

Generate a virtual IP address for the primary RSA NetWitness Warehouse (Warehouse) appliance.

Prerequisites

Make sure you note down the MAC addresses of all the Warehouse appliances in the cluster. Use the following command on the appliance to view the MAC address of appliance:

```
ifconfig <interface> | grep HWaddr
```

where <interface> is the network interface.

To generate a virtual IP address for the primary Warehouse appliance:

1. Log on to the primary appliance as root user.
2. Create the virtual IP address. Enter the following command:

   ```
   maprcli virtualip add -virtualip <VIP_address> -netmask
   <netmask> -macs <mac_node1> <mac_node2> <mac_node3> ……< mac_
   node n>
   ```

   where:

   - <VIP_address> is the virtual IP address for the primary Warehouse appliance.
   - <netmask> is the netmask address of the primary Warehouse appliance.

- <mac_node1> is the MAC address of the first node in the Warehouse cluster.
- <mac_node2> is the MAC address of the second node in the Warehouse cluster.

For example, if the MAC address for node 1 is 01:Z1:1X:00:20:Y1 and node 2 is 32:Y2:4Z:40:10:X3, and the IP address is 192.168.100.10, then enter the command as following:

```
maprcli virtualip add -virtualip 192.168.100.10 -
netmask <netmask> -macs 01:Z1:1X:00:20:Y1 32:Y2:4Z:40:10:X3
```

3. Verify the virtual IP address, using the following command:
   ```
   maprcli virtualip list
   ```
4. To add or remove virtual IP addresses, you can use the command line or the MapR Control System. For more information, see "Edit and Remove Virtual IP Addresses (Command Line)" and "Add and Remove a Virtual IP Address (MapR UI)" sections in Manage MapR Cluster.

Configure other NetWitness Suite Services

Configure other NetWitness Suite services for the RSA NetWitness Warehouse (MapR).

1. If you are not using Vulnerability Response Management (VRM), disable the Hbase services to return the configured memory so that it is available for use elsewhere in the cluster. To stop the Hbase services, you can use the command line or the MapR Control System. For more information, see Stop the Hbase Services Using the Command Line and Stop the Hbase Services Using the MapR Control System.
2. Add Warehouse data sources to the Reporting Engine. For the detailed procedure, see "Add Warehouse as Data Source to Reporting Engine" topic in the *Reporting Engine Configuration Guide*.

Stop the Hbase Services Using the Command Line

This section provides the steps to stop the Hbase services using the command line. If you are not using Vulnerability Response Management (VRM), stop the Hbase services to return the configured memory so that it is available for use elsewhere in the cluster.

To stop the Hbase services using the command line:

1. Stop the **Hbase RegionServer** service on *all of the appliances*, using the following command:
   ```
   maprcli node services -hbregionserver stop -filter "[hn==*]"
   ```

2. Stop the **Hbase RegionServer** service on *a specific node*, using the following command:
   `maprcli node services -hbregionserver stop -filter "[hn==<Hostname>]"`
   Where `<Hostname>` is the specific node hostname.
3. Stop the **Hbase Master** service on *all of the appliances*, using the following command:
   `maprcli node services -hbmaster stop -filter "[hn==*]"`
4. Stop the **Hbase Master** service on *a specific node*, using the following command:
   `maprcli node services -hbmaster stop -filter "[hn==<Hostname>]"`
   Where `<Hostname>` is the specific node hostname.

Hbase Services Stop and Start Commands Summary

The following tables summarize the commands used to stop and start the Hbase services for the **HBase RegionServer** and **HBase Master** services.

HBase RegionServer	Command to run using the Command Line
Stop on All the Appliances	`maprcli node services -hbregionserver stop -filter "[hn==*]"`
Start on All the Appliances	`maprcli node services -hbregionserver start -filter "[hn==*]"`
Stop on Specific node	`maprcli node services -hbregionserver stop -filter "[hn==<Hostname>]"`
Start on Specific node	`maprcli node services -hbregionserver start -filter "[hn==<Hostname>]"`

HBase Master	Command to run using the Command Line
Stop on All the Appliances	`maprcli node services -hbmaster stop -filter "[hn==*]"`

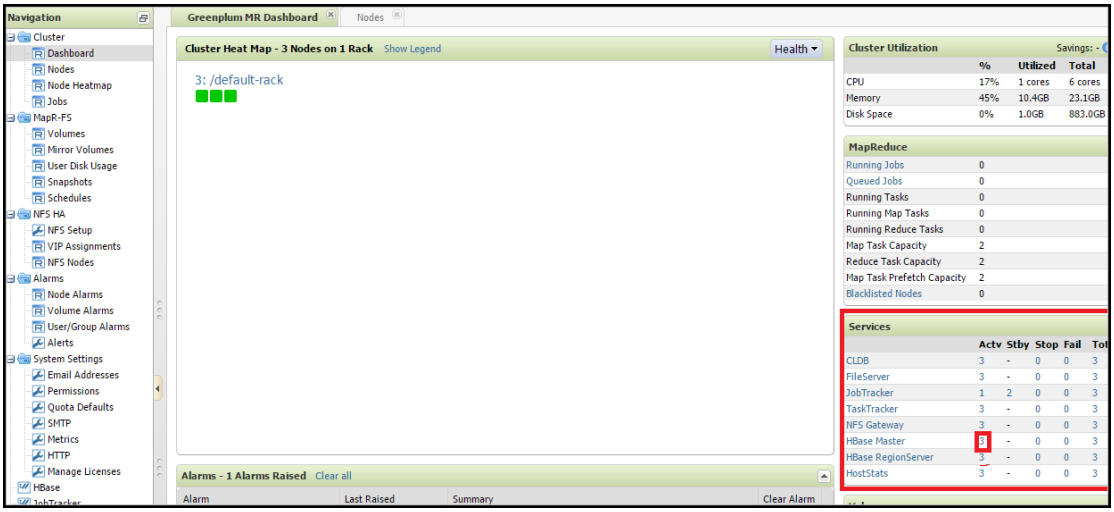
HBase Master	Command to run using the Command Line
Start on All the Appliances	`maprcli node services -hbmaster start -filter "[hn==*]"`
Stop on Specific node	`maprcli node services -hbmaster stop -filter "[hn==<Hostname>]"`
Start on Specific node	`maprcli node services -hbmaster start -filter "[hn==<Hostname>]"`

Where `<Hostname>` is the specific node hostname.

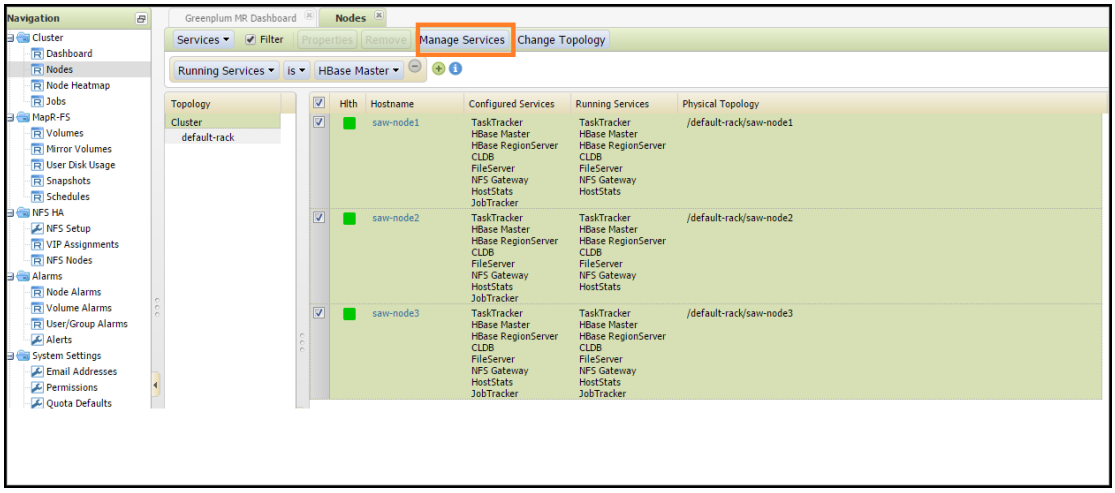
Stop the Hbase Services Using the MapR Control System

This section provides the steps to stop the Hbase services using the MapR Control System. If you are not using Vulnerability Response Management (VRM), stop the Hbase services to return the configured memory so that it is available for use elsewhere in the cluster.

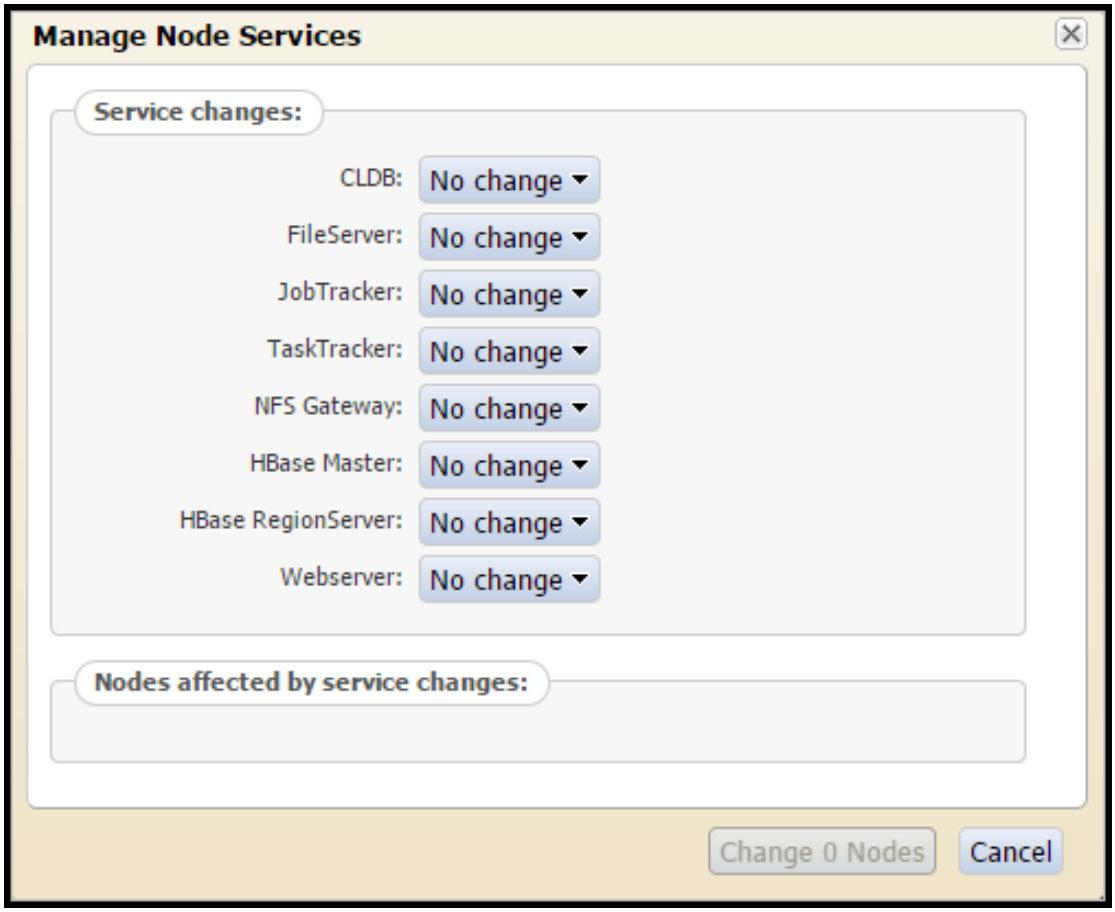
1. Log on to the MapR Control System user interface. For more information see "Access MapR Control System UI for Cluster Administration" section in Manage MapR Cluster.
2. Stop the **HBase Master** services, in the **Services** section of the dashboard, click the number in the **Actv** column for the **HBase Master** service. This is the number of active services for the **HBase Master** service.



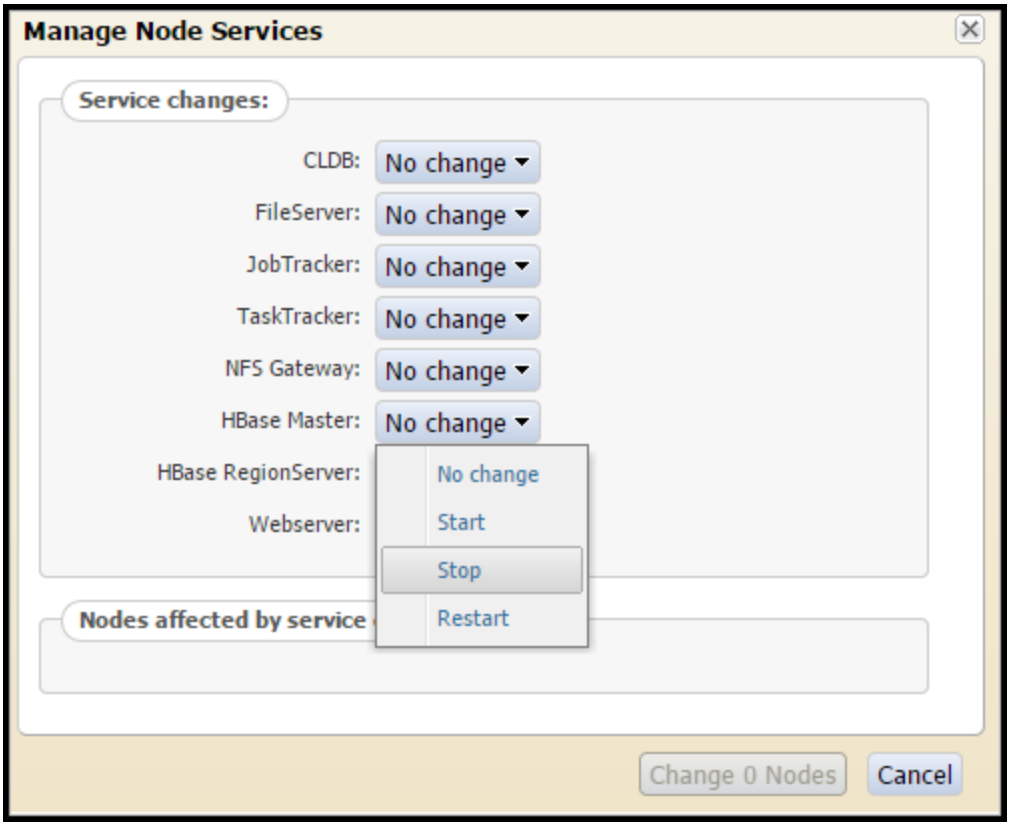
3. On the **Cluster Nodes** tab, click **Manage Services**.



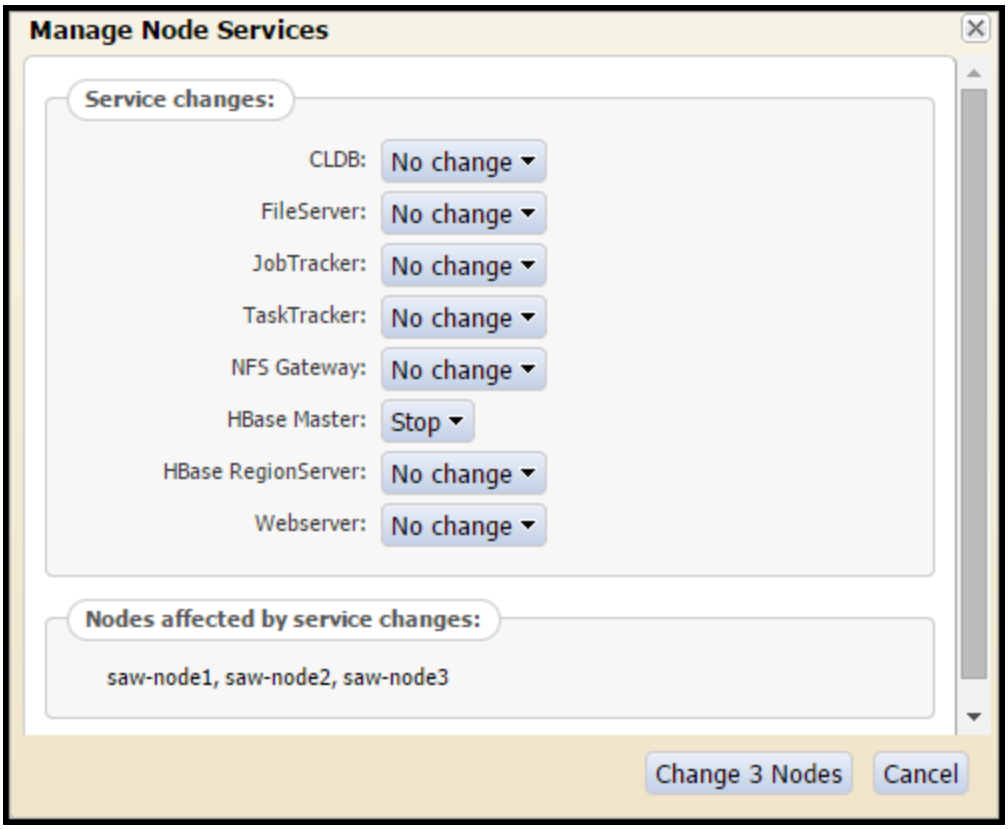
The **Manage Node Services** dialog is displayed.



4. In the **HBase Master** field, select **Stop**.



5. Click **Change <number_of_nodes> Nodes.**
   Where <number_of_nodes> is the number of active nodes selected.
   For example, click **Change 3 Nodes**.



The **Hbase Master** service on the selected nodes must be in a stopped state.

6. Stop the **Hbase RegionServer** services, repeat steps 2 to 5 for the **Hbase RegionServer** services.

Configure Warehouse Connector to Write to NetWitness Warehouse

You must enable the Warehouse Connector services to write to RSA NetWitness Warehouse.

To configure Warehouse Connector to write to the NetWitness Warehouse, perform the following tasks on the Log Decoders and Decoders where the Warehouse Connectors are installed:

Note: If you are configuring on a virtual environment, perform these tasks on a standalone Warehouse Connector server.

Verify the Network File System (NFS) Services Status

To verify the NFS services status:

1. Log on to the Warehouse Connector appliance where you have installed the Warehouse Connector service.
2. Enter the following command:
   ```
   rpm -qa |grep nfs
   ```
   The NFS package names appear in the output message. For example:
   ```
   nfs-utils-lib-1.1.5-6.el6.x86_64
   nfs-utils-1.2.3-36.el6.x86_64
   ```
3. If the output message is empty, install the NFS packages.

Install the Network File System Packages

Prerequisites

If the NFS packages are already downloaded on the appliances manually, install the packages and mount RSA NetWitness Warehouse. You need to have internet access to complete this task. If internet access is not available, you must download the RPM packages offline and copy them to this machine for installation.

Note: Install the NFS packages only if the NFS packages are not displayed when you verify the status of NFS in the Warehouse Connector appliance or on the appliance where you have installed the Warehouse Connector service.

To install NFS packages:

1. Log on to the Warehouse Connector appliance or on the appliance where you have installed the Warehouse Connector service.
2. Verify the NFS status, using the following command:

   ```
   rpm -qa |grep nfs
   ```

   The NFS package names appear in the output message. For example:

   ```
   nfs-utils-lib-1.1.5-6.el6.x86_64
    nfs-utils-1.2.3-36.el6.x86_64
   ```

   If the `nfs-utils` and `nfs-utils-lib` are properly identified, you can skip the remaining steps in this procedure (*Install the Network File System Packages*).
3. Search for NFS package, using the following command:

   ```
   yum search nfs-utils
   ```

   The output ends with the following message:

   ```
   "name and summary matches only, use "search all" for
   everything."
   ```

   Note: Contact RSA Customer Support if the output ends with the following message: `"no matches found"`
4. Install the NFS programs, using the following command:

   ```
   yum install nfs-utils nfs-utils-lib
   ```

   The output prompts for **y** or **n**. Type **y** and press **ENTER**.

The NFS packages are successfully installed.

Mount the Warehouse on the Warehouse Connector

To mount RSA NetWitness Warehouse on the appliance:

1. Create a new directory named **/saw**, using the following command:

   ```
   mkdir /saw
   ```
2. Enter the following command:

   ```
   ll /
   ```

   The new directory is displayed.
3. Mount the Warehouse, using the following command:

   ```
   mount -t nfs -o nolock,tcp,hard,intr <IP_Address_for_
   ```

`SAW>:/mapr/<cluster-name> /saw`

Where `<IP_Address_for_SAW>` is the IP address of the primary Warehouse appliance in the cluster and `<cluster-name>` is the name provided in the template file.

Note: If a virtual IP address is configured for the Warehouse, you have to use it as the IP address in `<IP_Address_for_SAW>`.

4. Verify if the Warehouse is mounted successfully, using the following command

   `mount`

   The IP address of the primary Warehouse appliance and other details you have provided in **step 3** appear in the last line of the output message.

5. List the content in the newly created directory, **/saw**, using the following command:

   `ll /saw`

   The following directories are displayed:

   hbase

   index-scratch

   jars

   logs

   user

   var

6. To add NFS to the Auto-mount options. Do the following:

   a. To check if the IP address of the primary Warehouse appliance and other details you have provided while mounting Warehouse appears in `/etc/fstab`, enter the following command:

      `cat /etc/fstab`

      If the detail does not appear in the `/etc/fstab` file, perform the following steps.

   b. Enter the following command:

      `tail –n 1 /etc/mtab`

      The IP address of the primary Warehouse appliance and other details you provided while mounting Warehouse appear in the last line of the output message.

   c. Enter the following command:

      `tail –n 1 /etc/mtab >> /etc/fstab`

   d. Edit the /etc/fstab file to add the word ‘auto’ at the end of the file. Enter the following command:

      `vi /etc/fstab`

For example, `10.11.111.11:/mapr/saw /saw nfs rw,nolock,tcp,auto,addr=10.11.111.11 0 0`

Manage MapR Cluster

You can manage the MapR cluster using the following procedures:

Access MapR Control System UI for Cluster Administration

You can access the MapR Control System user interface for RSA NetWitnessWarehouse cluster administration. MapR Control System user interface enables you to administer the RSA NetWitnessWarehouse cluster. The MapR Control System user interface provides details of the following:

- Nodes
- Node Heatmap
- Jobs
- MapR Tables
- Volumes
- Mirrors
- User Disk Usage
- Snapshots
- Schedules
- NFS Setup
- Virtual IP Assignments
- NFS Nodes
- Node Alarms
- Volume Alarms
- User/Group Alarms
- HBase
- JobTracker
- CLDB

To access the MapR Control System user interface:

1. Log on to one of the appliances in the RSA NetWitnessWarehouse cluster.
2. Start the webserver. Enter the following command:

   ```
   /opt/mapr/adminuiapp/webserver start
   ```

   Note: The default port used by the webserver is **8443**.

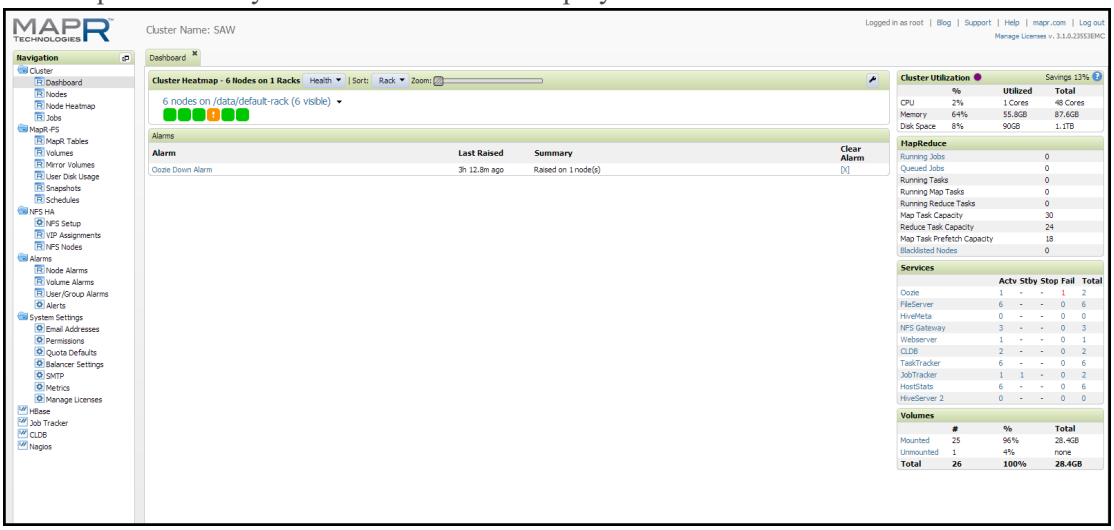
   Note: If you receive the error `/opt/mapr/conf/ssl_keystore (No such file or directory)` in the `/opt/mapr/logs/adminuiapp.log` after executing the command `/opt/mapr/adminuiapp/webserver start`, enter the following commands:

   ```
   ./configure.sh -R -genkeys
   service mapr-warden restart
   ```

3. Using a web browser to access the MapR Control System, type the following url:

   ```
   https://<NODE-IP-OR-HOSTNAME>:8443
   ```

   The MapR Control System user interface is displayed.



Enable MapR Metrics on RSA NetWitnessWarehouse Cluster

You can enable MapR Metrics on the RSA NetWitnessWarehouse cluster. This optional procedure enables Administrators to see job details in the MapR Control System UI rather than going to the JobTracker for details.

Prerequisites

Make sure that you have the following MapR Metrics dependencies installed in your environment:

- MySQL Server installed and configured.
- Libraries hosted on the EPEL Repository.
- Libraries hosted on the CentOS base repositories.

To Enable MapR Metrics

To enable MapR Metrics on the RSA NetWitnessWarehouse cluster, follow the instructions at the following links:

- http://doc.mapr.com/display/MapR/Setting+up+the+MapR+Metrics+Database
- http://doc.mapr.com/display/MapR/MapR+Metrics+and+Job+Performance

Note: Make sure you install MapR Mertics on the nodes in your RSA NetWitnessWarehouse Cluster where Job Tracker or Web Server is running.

Edit and Remove Virtual IP Addresses (Command Line)

You can edit and remove virtual IP addresses in the Warehouse cluster using the command line. This procedure is optional and used when you want to change the virtual IP addresses in the Warehouse cluster.

Adding and removing Warehouse appliances to and from a virtual IP group is accomplished by executing an **edit** command. This is the same as the add command, except that ALL of the MAC addresses are replaced with ONLY the MAC addresses that you enter.

Prerequisites

Make sure you note down the MAC addresses of all the Warehouse appliances in the cluster. Use the following command on the appliance to view the MAC address of the appliance:

```
ifconfig <interface> | grep HWaddr
```

where `<interface>` is the network interface.

Also note the MAC addresses of the Warehouse appliances that you want to add.

To add or remove a virtual IP address in the primary Warehouse appliance:

1. Log on to the primary appliance as root user.
2. Edit the virtual IP address. Enter the following command:

```
maprcli virtualip edit -virtualip <VIP_address> -netmask
<netmask> -macs <mac_node1> <mac_node2> <mac_node3> ……< mac_
node n>
```

where:

- `<VIP_address>` is the virtual IP address for the primary Warehouse appliance.
- `<netmask>` is the netmask address of the primary Warehouse appliance.
- `<mac_node1>` is the MAC address of the first node in the Warehouse cluster.
- `<mac_node2>` is the MAC address of the second node in the Warehouse cluster.

For example, if the IP address of the primary warehouse is `192.168.100.10` and the MAC address for node 1 is `01:Z1:1X:00:20:Y1`, node 2 is `32:Y2:4Z:40:10:X3`, and you want to add node 3, which is `20:Y2:4Z:20:10:X3`, then enter the following:

```
maprcli virtualip edit -virtualip 192.168.100.10 -
netmask <netmask> -
macs 01:Z1:1X:00:20:Y1 32:Y2:4Z:40:10:X3 20:Y2:4Z:20:10:X3
```

3. Verify the virtual IP addresses. Enter the following command:

```
maprcli virtualip list
```

To remove the virtual IP address of the primary Warehouse appliance group entirely:
Enter the following command:

```
maprcli virtualip remove -virtualip 192.168.100.10
```

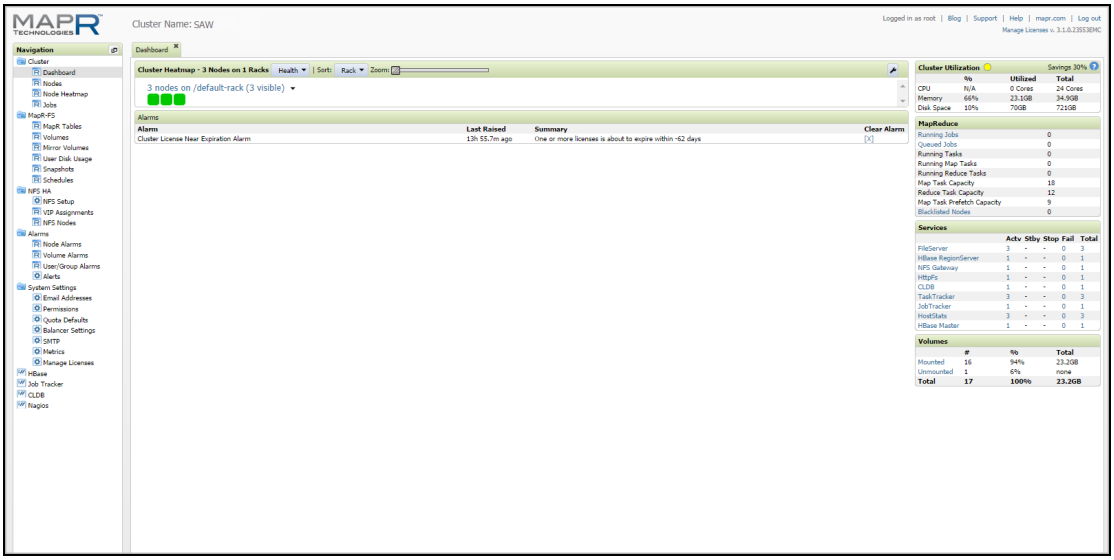
Add and Remove a Virtual IP Address (MapR UI)

You can add a virtual IP address in the Warehouse cluster using the MapR Control System. This procedure is optional and used when you want to add a virtual IP address (VIP) in the Warehouse cluster.

Prerequisites

Follow the instructions in Access MapR Control System UI for Cluster Administration before completing this procedure.

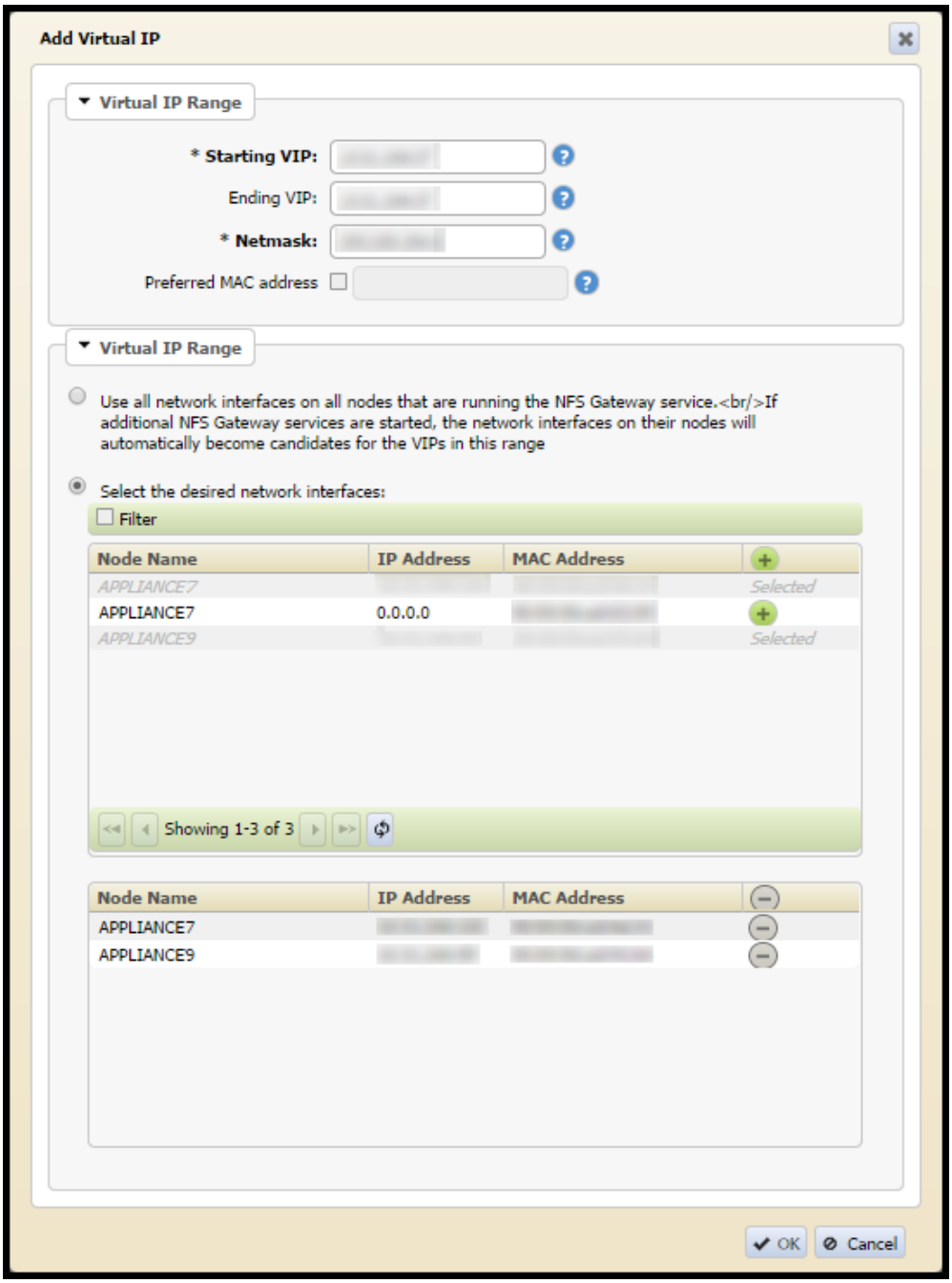
1. Log on to the MapR Control System.



2. In the Navigation panel, select **NFS HA > NFS Setup**.
   The NFS Setup tab is displayed. The NFS Setup tab enables you to edit, remove or add VIPs in the Warehouse cluster.

3. On the **NFS Setup** tab, click the **Add VIP** button.

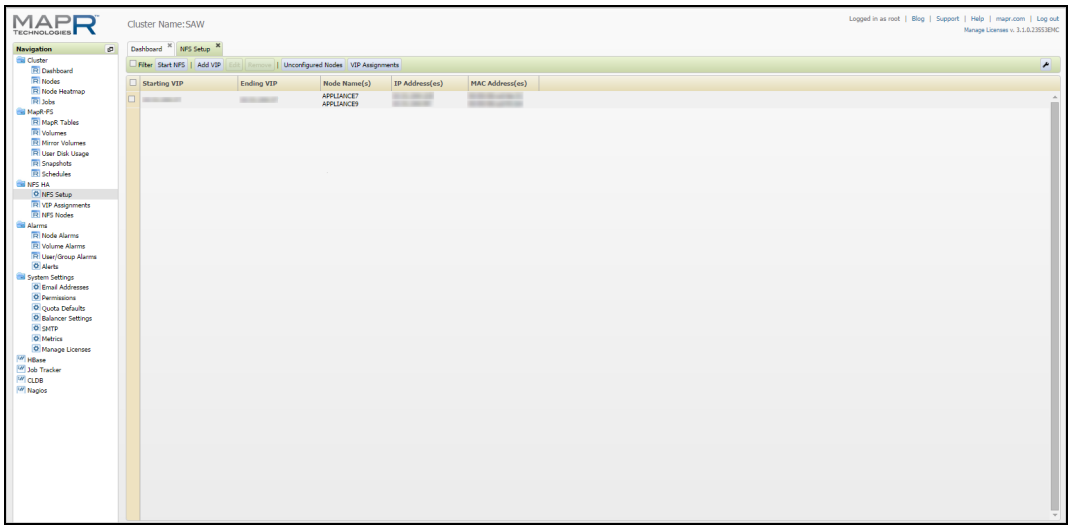
The **Add Virtual IP** dialog is displayed.



4. In the **Add Virtual IP** dialog, do the following:
   a. In the **Starting VIP** field, type the starting IP Address for VIP.
   b. In the **Ending VIP** field, type the ending IP Address for VIP. If this field is left blank, only one IP address is used for VIP allocation.
   c. In the **Netmask** field, type the Netmask for the deployment.

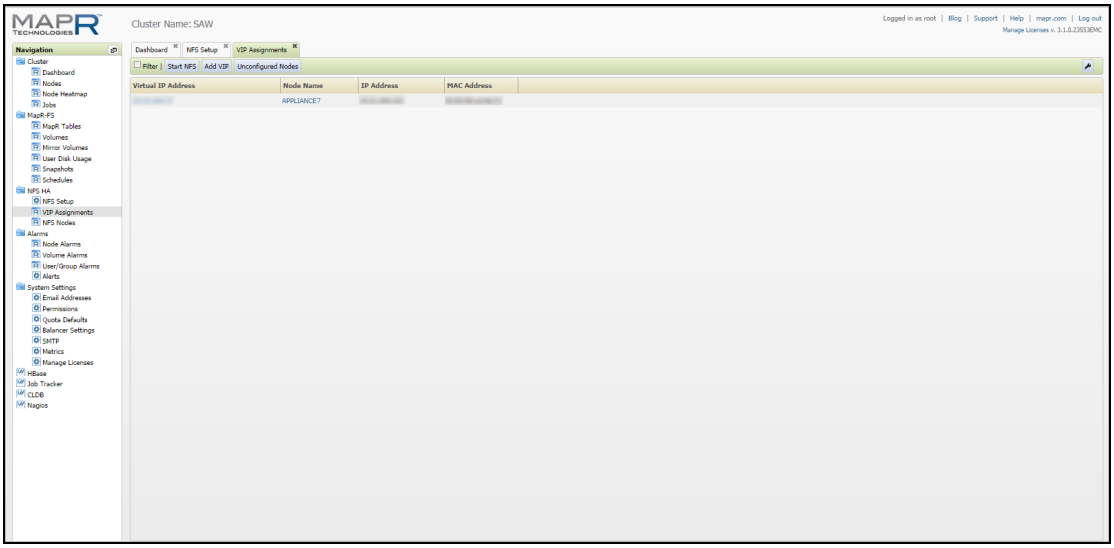
d. Select **Select Desired Network Interfaces** to choose the available Network Interfaces that need to be used for VIP assignment. Select all of the external Interfaces from the list of available nodes by clicking the plus button next to the interface entry. Selected Interfaces will appear in the bottom list.

e. Click **OK** to add the VIP.
The newly added VIP appears in the list on the **NFS Setup** tab.



Note: VIP allocation can also be removed or edited from the **NFS HA > NFS Setup** tab by selecting a VIP and clicking the **Edit** or **Remove** button.

5. In the Navigation panel, select **NFS HA > VIP Assignment** to view the node that is assigned to the newly added VIP.



Add a Virtual IP Address with Multiple Nodes (MapR UI)

You can add a virtual IP address (VIP) with multiple nodes. Virtual IP (VIP) is a technique used to load balance data access into HDFS by using a floating IP Address among the cluster nodes. This technique is mostly used by the MapR Hadoop Distribution along with the MapR-NFS Service. VIP can provide High Availability and Load Balancing by dynamically allocating the Floating IP among the nodes.

Optimal VIP Configuration

We recommend using one VIP for every three Nodes, because the replication factor for HDFS is 3 by default. This also helps in optimizing the performance of the cluster.

In the case of High Data Load (>20K EPS), a single NFS might overload while replicating the file into the cluster. If the NFS Server crashes before the data is replicated, you may lose data.

Multiple NFS Servers also allow more distributed data locality which helps in High Availability and Fault Tolerance.

Prerequisites

Calculate how many VIPs you can afford.

- We suggest **One VIP per 3 Nodes**.
- In case the number of nodes that you have is not a multiple of three, you can allocate multiple VIPs to more than three nodes. For example, two VIPs among five Nodes.

The steps to add the VIP are the same as adding any other VIP, but instead of choosing “all nodes” for VIP, you choose a subset of nodes to participate in the VIP.

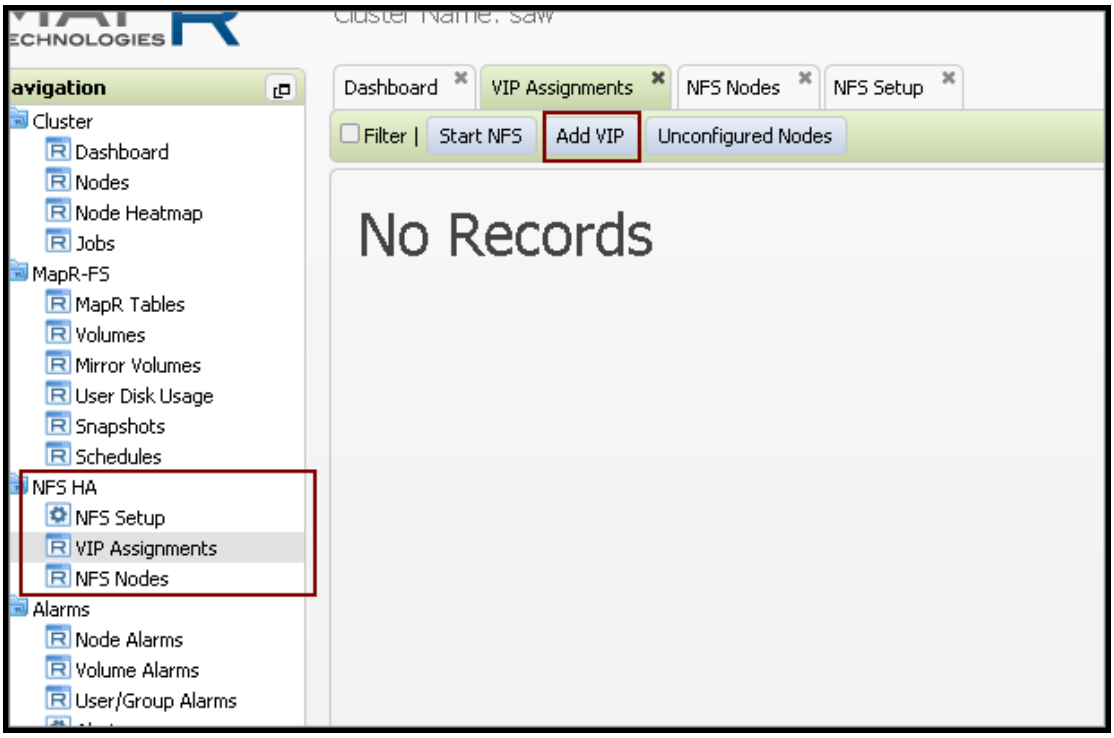
- A node can participate in Multiple VIPs.
- For more information, see http://doc.mapr.com/display/MapR/Setting+Up+VIPs+for+NFS

Optimal Configuration with the Warehouse Connector

The recommended configuration is to have one VIP per Warehouse Connector. In cases where Warehouse Connector numbers are higher than VIPs, configure multiple Warehouse Connectors to write to a VIP in a way so that traffic on VIPs can be normalized.

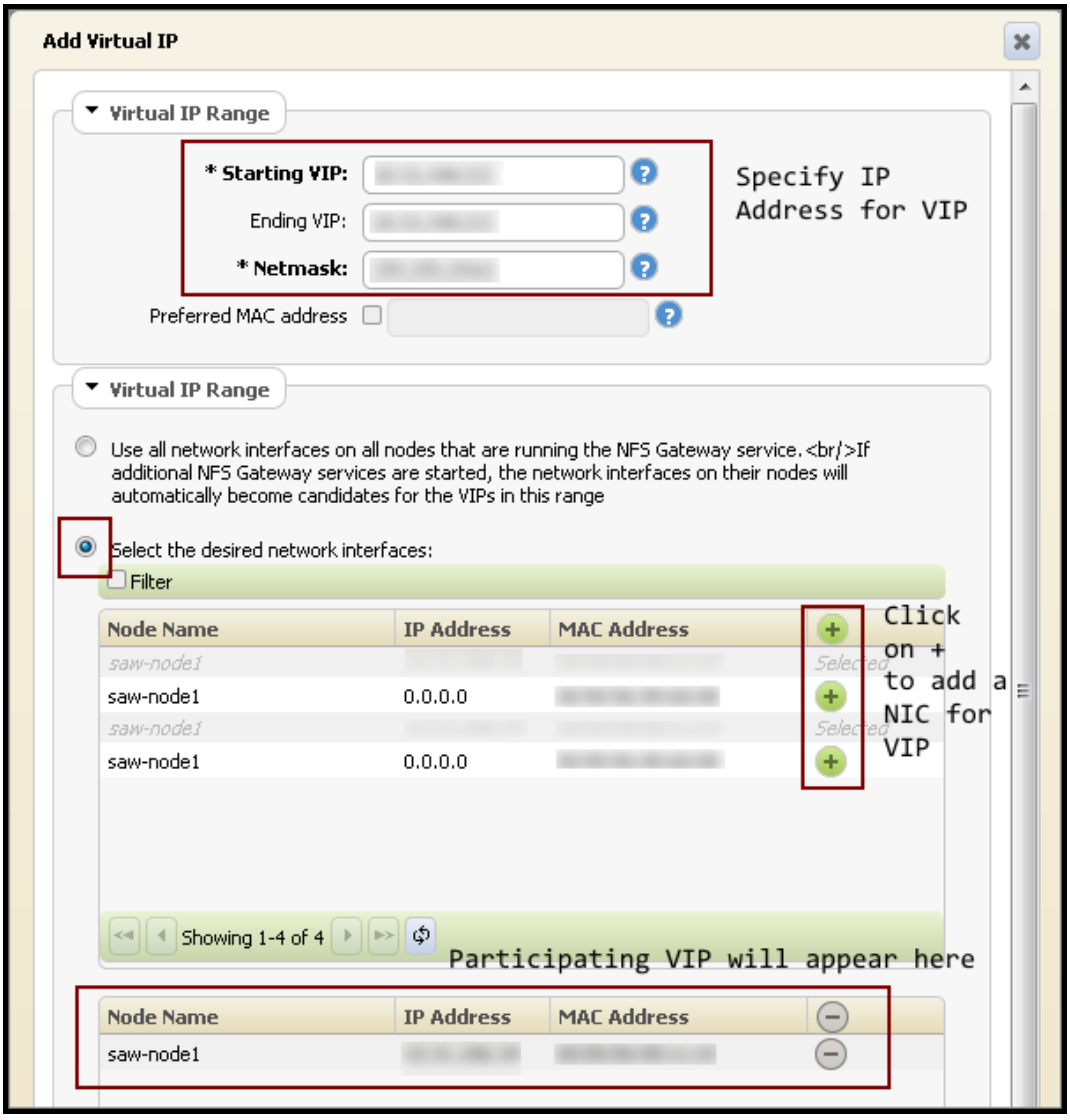
Add a Virtual IP Address that has Multiple Nodes

1. Log on to the MapR Control System.
2. In the Navigation panel, select **NFS-HA > VIP Assignments**.
3. On the **NFS Setup** tab, click the **Add VIP** button.



4. In the **Add Virtual IP** dialog, do the following:

a. Specify the Starting and Ending VIP as the same IP address.



b. Select **Select the Desired Network Interfaces** to choose the available Network Interfaces that need to be used for the VIP assignment. Select the NIC Cards that you want to participate in the VIP. A node can have multiple NICs, so depending on the Network Configuration you can select them.

c. Click **OK** to add the VIP.

Example VIP Configurations

The following table shows example configurations of virtual IP addresses (VIPs) with different numbers of nodes in the cluster.

Number of Nodes in Cluster	Number of VIPs
3 Nodes	1 VIP
5 Nodes	2 VIPs (3 Nodes each, 1 Common Node)
7 Nodes	2 VIPs (3 Nodes each, 1 Free Node)
8 Nodes	3 VIPs (3 Nodes each, 1 Common Node among 2 VIPs)
11 Nodes	4 VIPs (3 Nodes each, 1 Common Node among 2 VIPs)
11 Nodes	3 VIPs (3 Nodes each, 2 Free Nodes)

RSA NETWITNESS® SUITE

Workbench Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Workbench Overview 5

Workbench Configuration Procedures 6

Adding Workbench Service as a Data Source to Broker 8

Adding Workbench as a Data Source to Reporting Engine 11

Managing Collections 13

- Mount Archiver Directories 13
- Create a Collection 13
- Delete a Collection 15
- Example Procedure: How to Restore a Collection for Reporting and Investigation 17
- Investigate a Collection 18
- View Workbench Collection Statistics 20
- View Workbench Logs 21

References 22

Services Config View - Workbench 23

Services Config View - Collections Tab 26

- Toolbar 28

Services Config View - General Tab 30

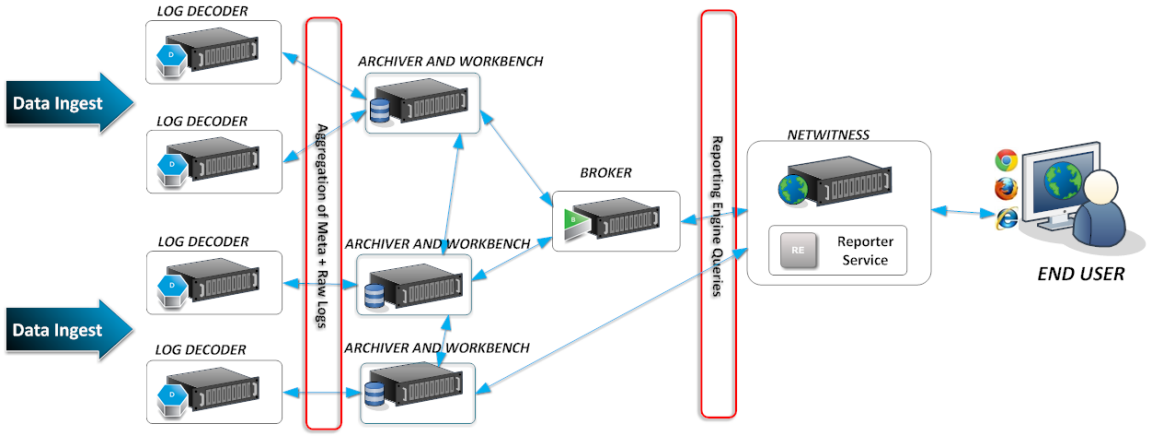
- System Configuration Panel 31
- Workbench Configuration Panel 32

Troubleshooting 33

Workbench Overview

The NetWitness Suite Workbench service allows collections to be created with restored data that was saved offline from an Archiver. Once the data has been copied and saved into a collection, it can be analyzed from Investigation and Reporting.

The following diagram depicts the architecture of a NetWitness Suite network that implements the Workbench.

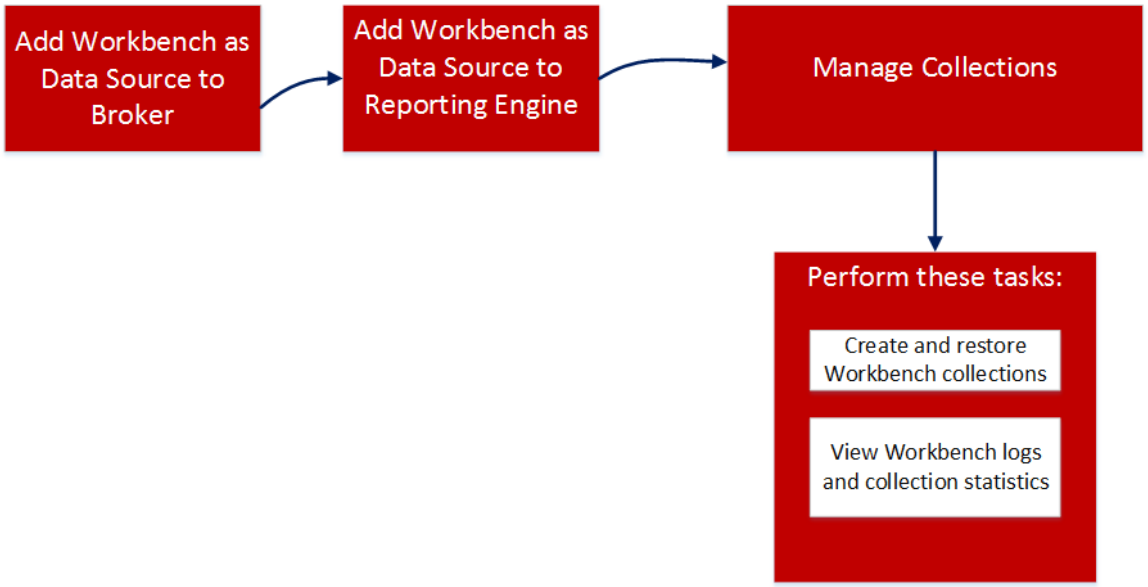


Workbench Configuration Procedures

Note: While NetWitness Suite 11.1 continues to support the Workbench, and some customers may have configured Workbench to handle restoring of data, the best practice for restoring data is to use the Archiver. to configure archival and restoring of data, following the instructions provided in the *Archiver Configuration Guide*.

Workflow

These are the basic steps for configuring and managing a Workbench service.



1. Add a Workbench service as a data source to Broker (see Adding Workbench Service as a Data Source to Broker).
2. Add a Workbench service as a data source to Reporting Engine (see Adding Workbench as a Data Source to Reporting Engine
3. Manage collections on a Workbench service (see Managing Collections).
4. Investigate a Workbench (see Managing Collections).

Prerequisites

Before configuring the Workbench service, you must:

- Add the NetWitness Suite workbench service to the host in your network environment. (Refer to Workbench Overview.)
- Install the NetWitness Suite Workbench host in your network environment. For more information, refer to the *Host and Services Getting Started Guide*.

The steps to configure the Workbench service are:

1. Adding Workbench Service as a Data Source to Broker
2. Adding Workbench as a Data Source to Reporting Engine

When configuration is complete, you can create and manage collections as described in Managing Collections.

Adding Workbench Service as a Data Source to Broker

Prerequisites

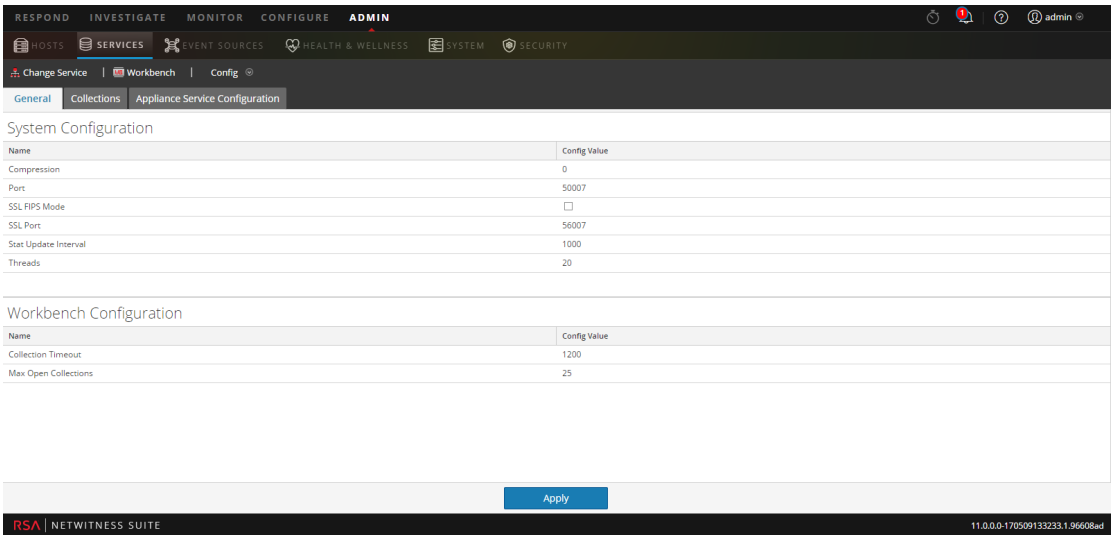
Before adding the Workbench service, you must:

- Install the Workbench service on the Archiver appliance.
- Add a collection on the workbench service.

To add the Workbench service as a data source on the Broker:

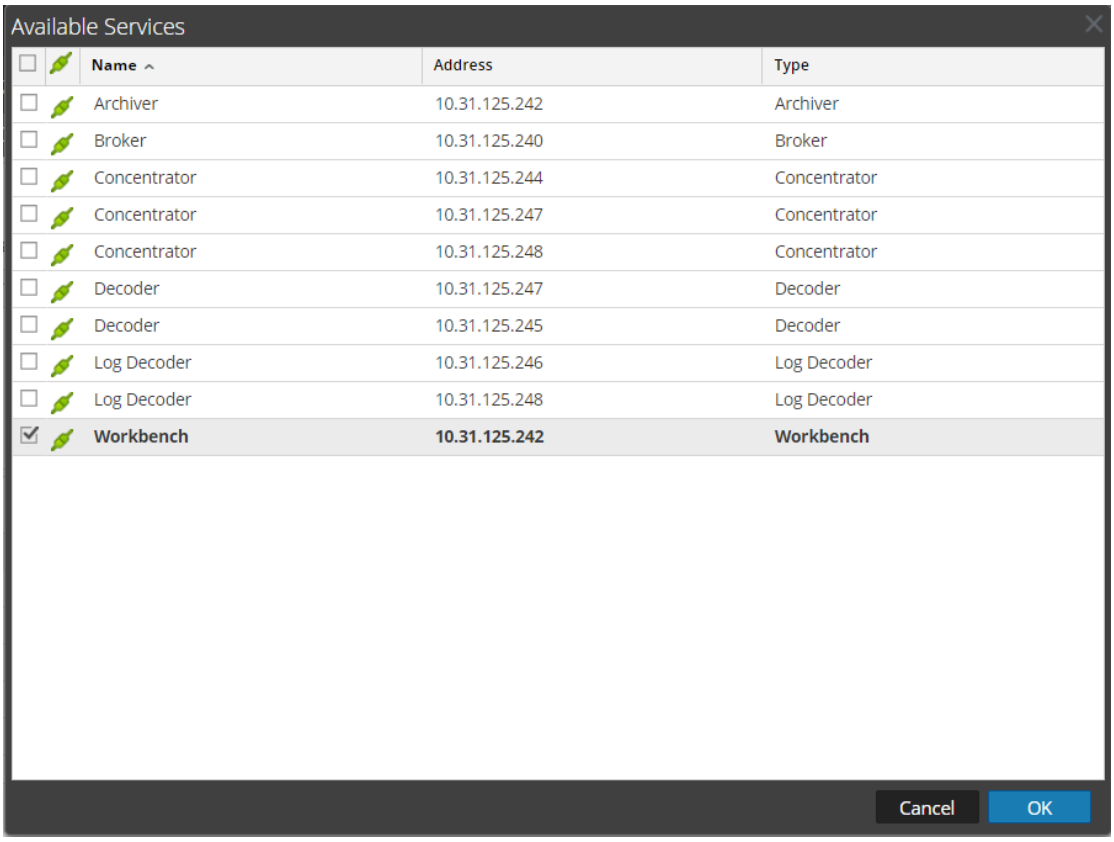
1. Go to **ADMIN >Services**.
2. Select a Broker service, and select **> View > Config.**

   The Service Config view is displayed.

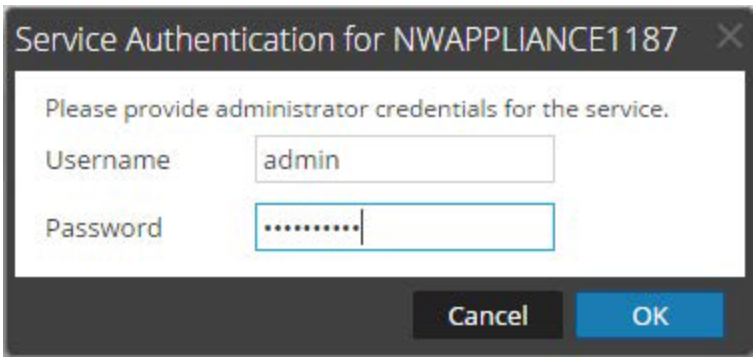


3. Select the **General** tab.
4. Click and select **Available Services**.

   The Available Services dialog is displayed.

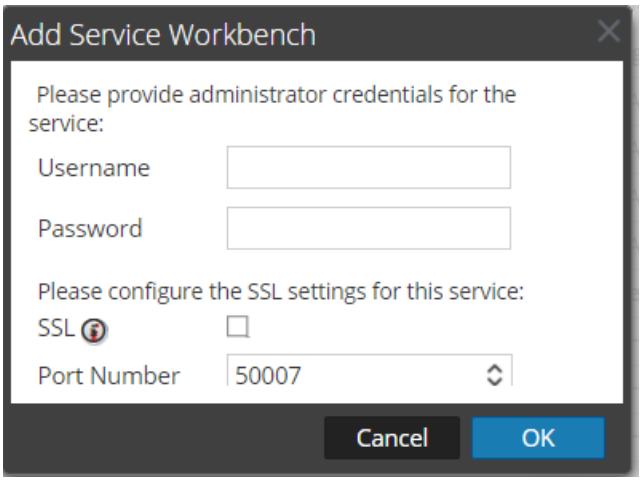


5. Select the Workbench service and click **OK**.
6. If the Workbench service is using a Trust Model, a Service Authentication dialog for the selected service is displayed.



7. Type the username and password for admin credentials for the service and click **OK**.

   The Add Service Workbench dialog is displayed.



8. Type the username and password for admin credentials for the service and click **OK**.

   The workbench service is now added as a data source to the Broker and is listed in the NWDATA Sources list.

Note: This procedure has to be performed for each collection.

Adding Workbench as a Data Source to Reporting Engine

Prerequisites

These are the tasks required before adding the Workbench as a data source to Reporting:

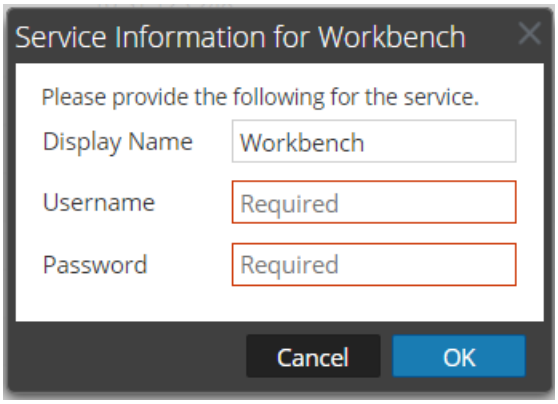
1. Add the Reporting Engine as a service to your NetWitness Suite deployment.
2. Add the Workbench as a service to your NetWitness Suite Archiver host (if not already installed).

Note: Adding Workbench collections as a data source to Reporting Engine depends on a trusted connection. If the Workbench is established with a trusted connection, you must manually add Workbenchcollections as a source to the Reporting Engine.

To associate the Workbench data source with the Reporting Engine:

1. Go to **ADMIN > Services**.
2. Select a **Reporting Engine** in the Services grid. Select **View > Config**.
3. Switch to the **Sources** tab.
4. Select .
5. Select **Available Services**. Select a Workbench service in the Available Services dialog.
6. Click **OK**.

   The Service Information dialog is displayed.



7. Enter User Name and Password.

- Required if the Workbench service is Trusted.
- Optional if the Workbench service is not trusted (added manually).

8. Click **OK**.
9. Select **Collection** in Add a Collection from Workbench dialog.
10. Click **OK**.

Result

You can now create reports on the data collected by the Workbench.

Managing Collections

An Administrator can create and delete Workbench collections and view Workbench statistics and logs. This topic provides all of these procedures and an example procedure for restoring a collection for Reporting and Investigation.

- Mount Archiver Directories
- Create a Collection
- Delete a Collection
- Investigate a Collection
- View Workbench Collection Statistics
- View Workbench Logs

Mount Archiver Directories

If data is in offline storage or cold-tier storage, you need to mount the Archiver directories in order to restore the data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select an **Archiver** from the Services grid and select **> View > Explore**.
   The Explorer view for the Archiver is displayed
3. Right-click on the **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
4. Run the **manifest** command for a time range, for example, 2017-April-01 to 2017-April-10.
   The search returns all files that need to be restored for the selected query.

Create a Collection

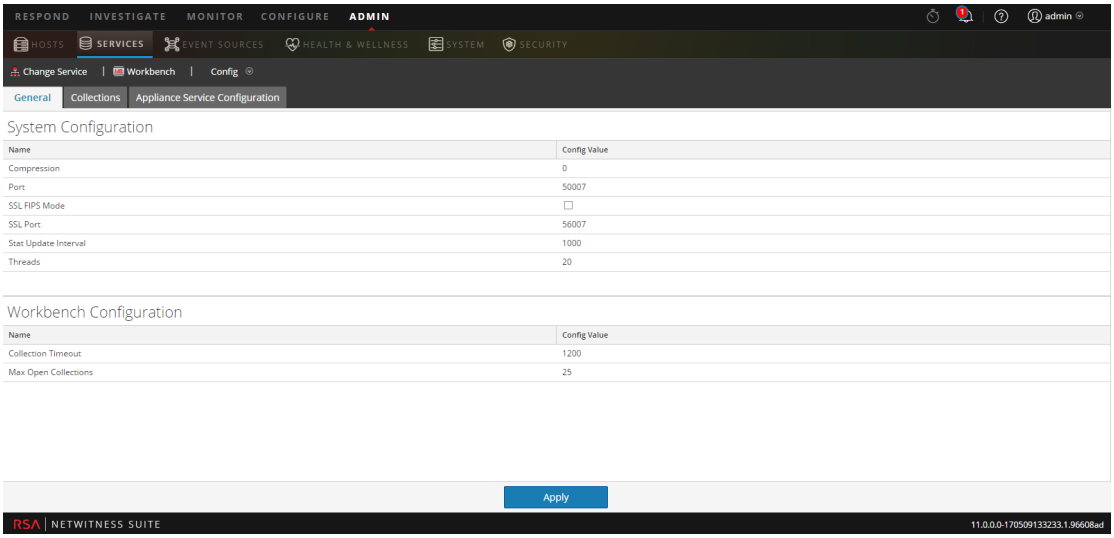
Administrators can create collections of restored data from a backup or from an existing set of data.

Note: You can point the source path to the location of the database files and the restore command copies them to the workbench. You need to mount those directories to the Archiver (where the Workbench is installed) before a restoration collection can be created.

To create a collection using data restored from the backed up data or existing subset of data:

1. Go to **ADMIN> Services.**
2. In the Services view, select a **Workbench**, then select **> View > Config**.

   The Services Config view is displayed with the General tab open.

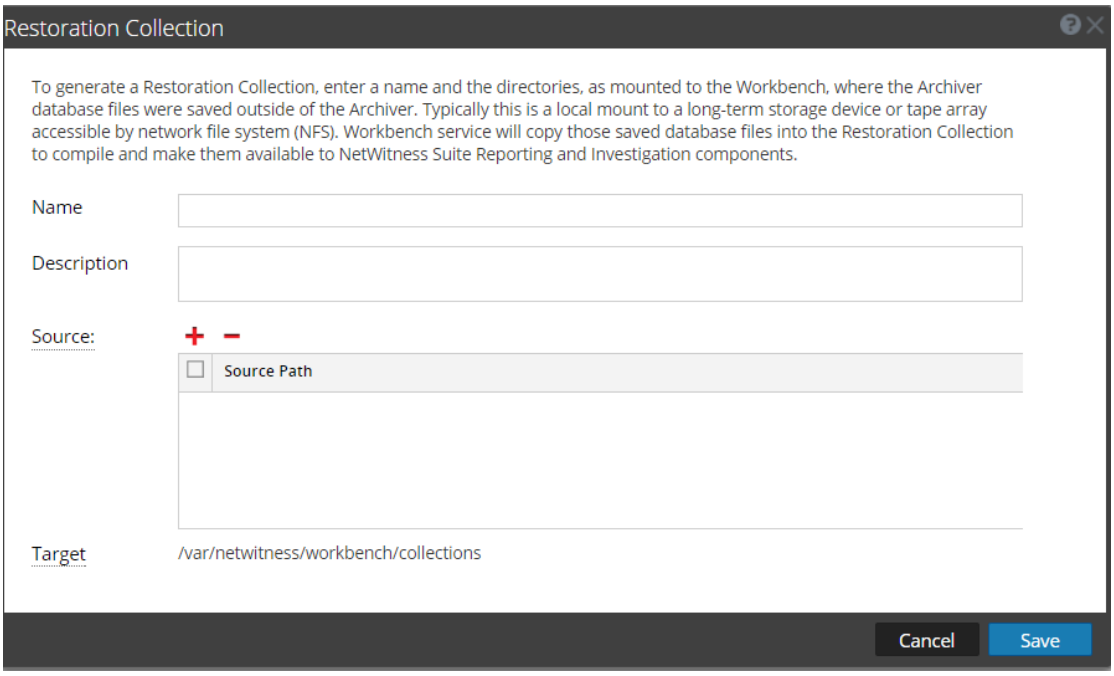


3. Click the **Collections** tab.

   The Collections grid is displayed.

4. Click in the toolbar.

   The Restoration Collection dialog is displayed.



5. Provide the following information:

- **Name:** Name of the Workbench collection that you want to restore.
- **Source:** Location where the Archiver database files have been moved from cold storage.

Note: Target is the location where the collection is created.

6. Click **Save** to restore the collection.

Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:

```
The source path does not exist '/xxx/xxx/'.
```

If there is insufficient storage to restore your collection, the following error is displayed:

```
Error during disk space checking. Insufficient disk space in
location '/xxx/xxx'.
```

The Schedule Job dialog is displayed with the following message:

```
Restoring data into a new collection. Check the jobs page for
progress.
```

7. Click the **Jobs** icon in the NetWitness Suite toolbar to expand the list of restoration collection jobs with their current status.

Note: Restoring a collection that is larger than 550 GB may take several hours to process.

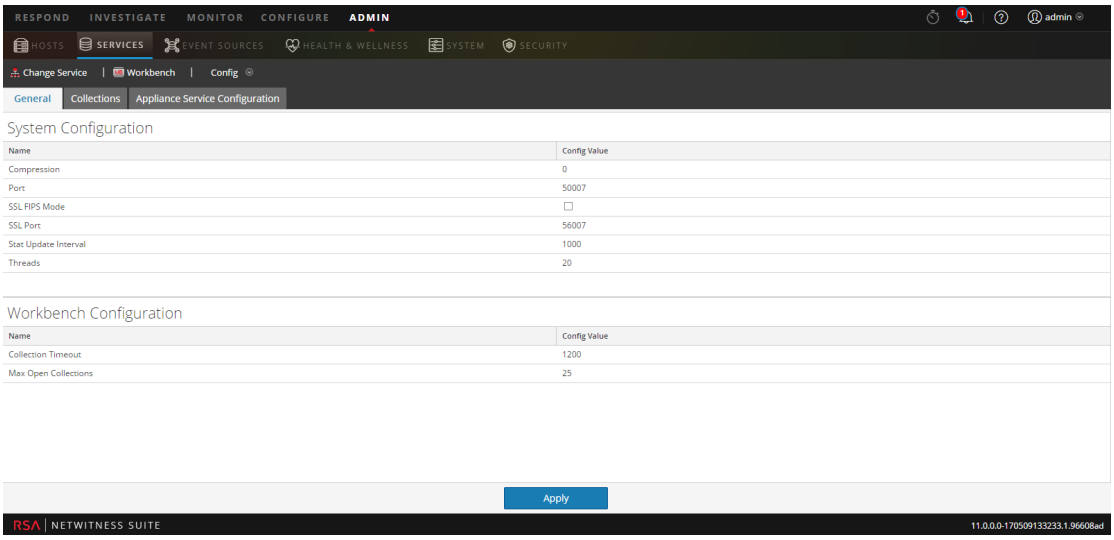
Delete a Collection

Administrators can delete collections from the Workbench service.

Perform the following steps to delete a collection:

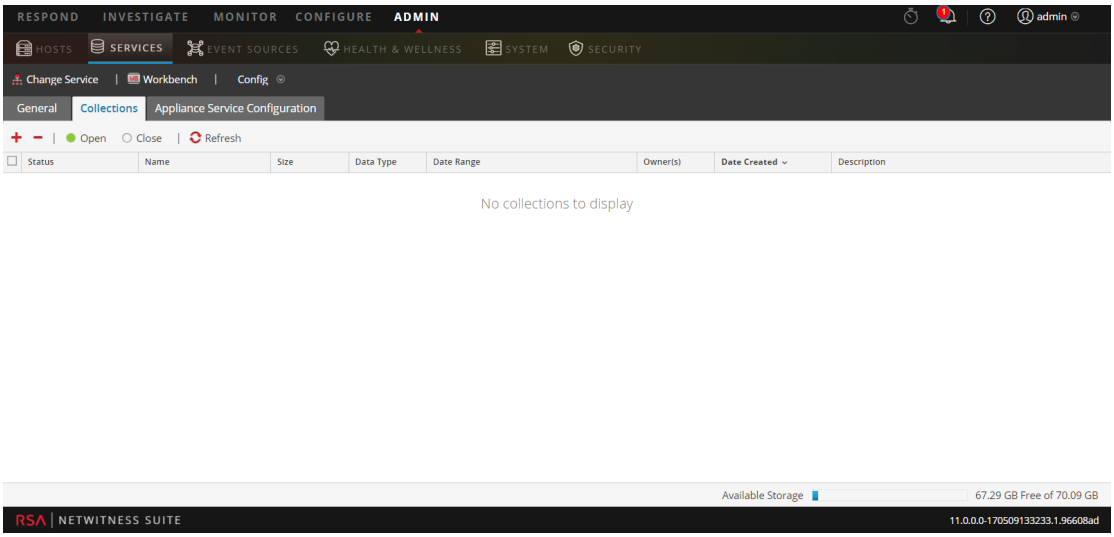
1. Go to **ADMIN > Services.**
2. From the Services view, select a **Workbench** and click **> View > Config**.

   The Services Config view opens with the General tab displayed.



3. Select the **Collections** tab.

   The Collections grid is displayed.



4. In the Collections grid, select the collection that you want to delete.
5. Click − from the toolbar.

   A warning dialog requests confirmation.
6. If you want to delete the collection, click **Yes**.

   The collection is removed from the Workbench service.

Example Procedure: How to Restore a Collection for Reporting and Investigation

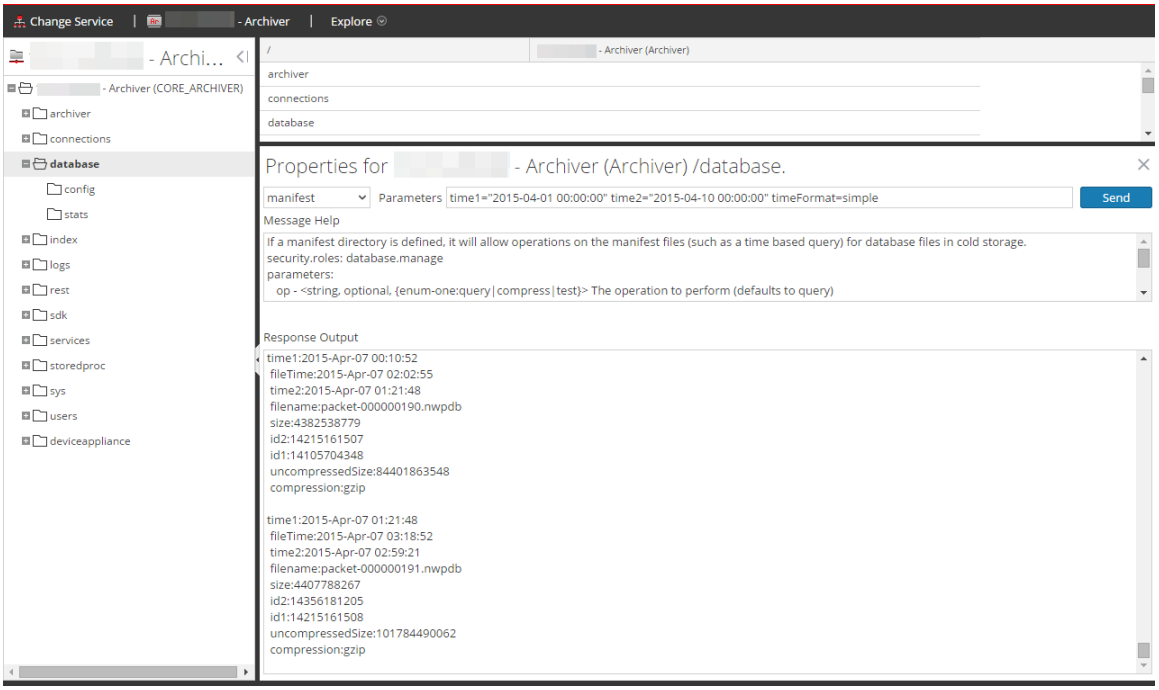
The following steps illustrate how to restore data for reporting and investigation purposes that is in offline storage or cold-tier storage. In the following example, data is restored for the time range beginning on 2015-April-01 through 2015-April-10.

To restore data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select the **Archiver** from the Services grid.
3. Navigate to the Explorer view of the Archiver appliance by selecting **> View > Explore**.
   The Explorer view for Archiver is displayed
4. Right click on **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
5. Run the **manifest** command for the selected time range 2015-April-01 to 2015-April-10.
   The search returns all files that need to be restored for your selected query.

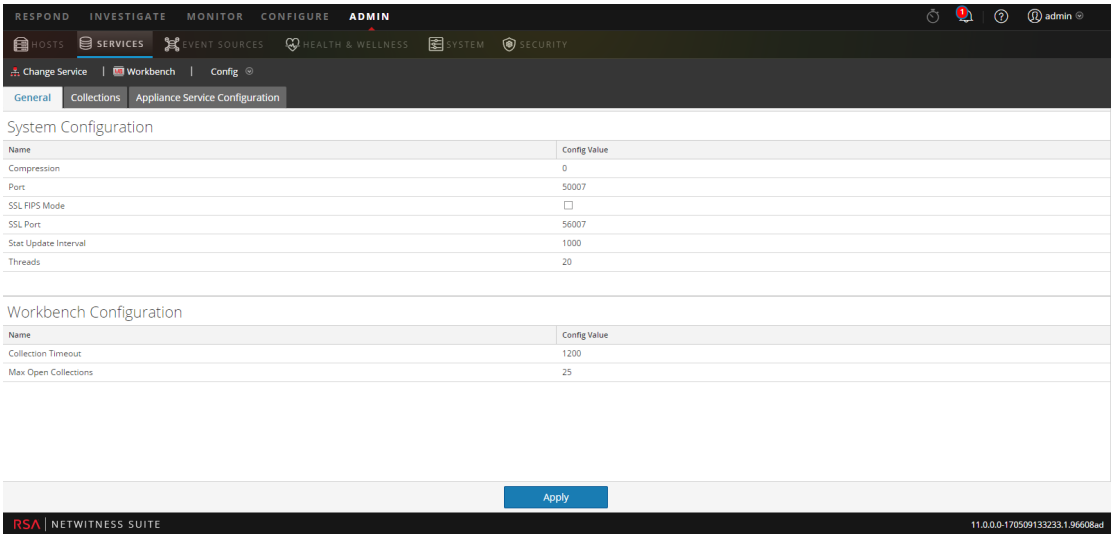
Example Search:

```
time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
timeFormat=simple
```



6. Go to **ADMIN > Services**.
7. In the Services view, select a **Workbench**, then select **> View > Config**.

   The Services Config view is displayed with the General tab open.



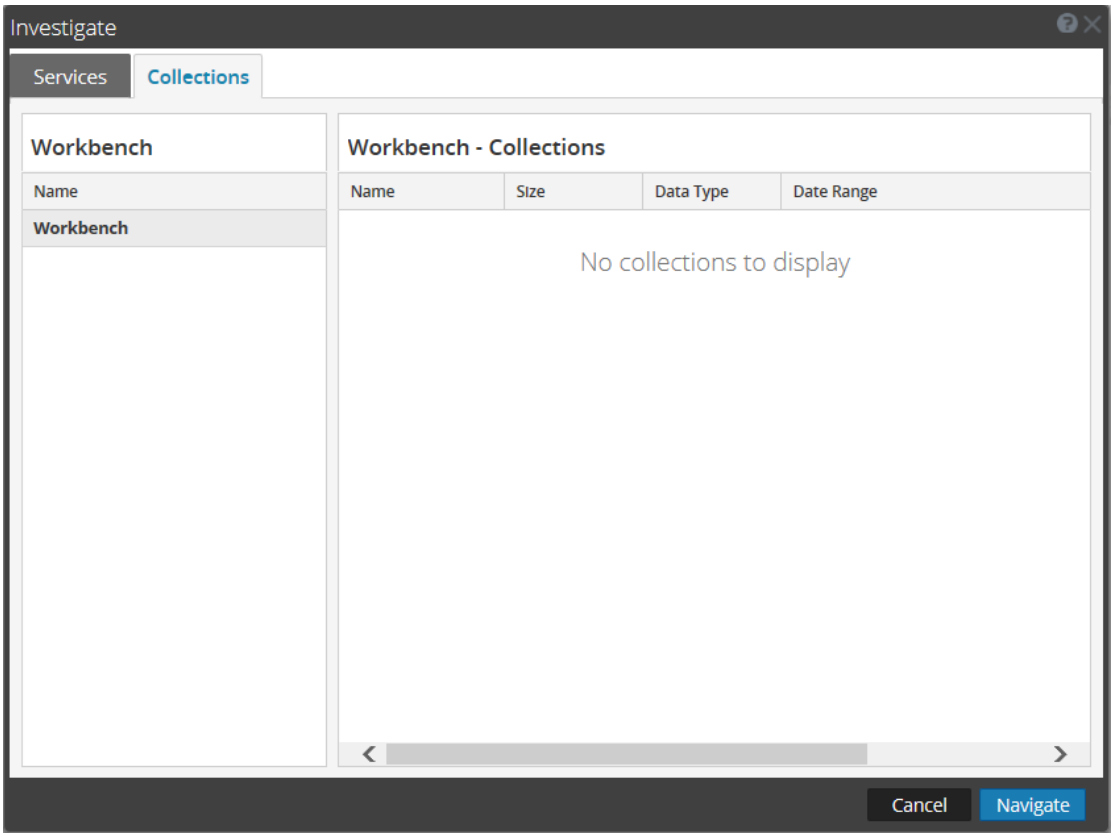
8. Select the **Collections tab.**
9. Create a restoration collection with the source path pointing to files listed in the manifest command output.
10. Save the collection.

    After successfully creating a collection, you can use this collection for reporting and investigation purposes.

Investigate a Collection

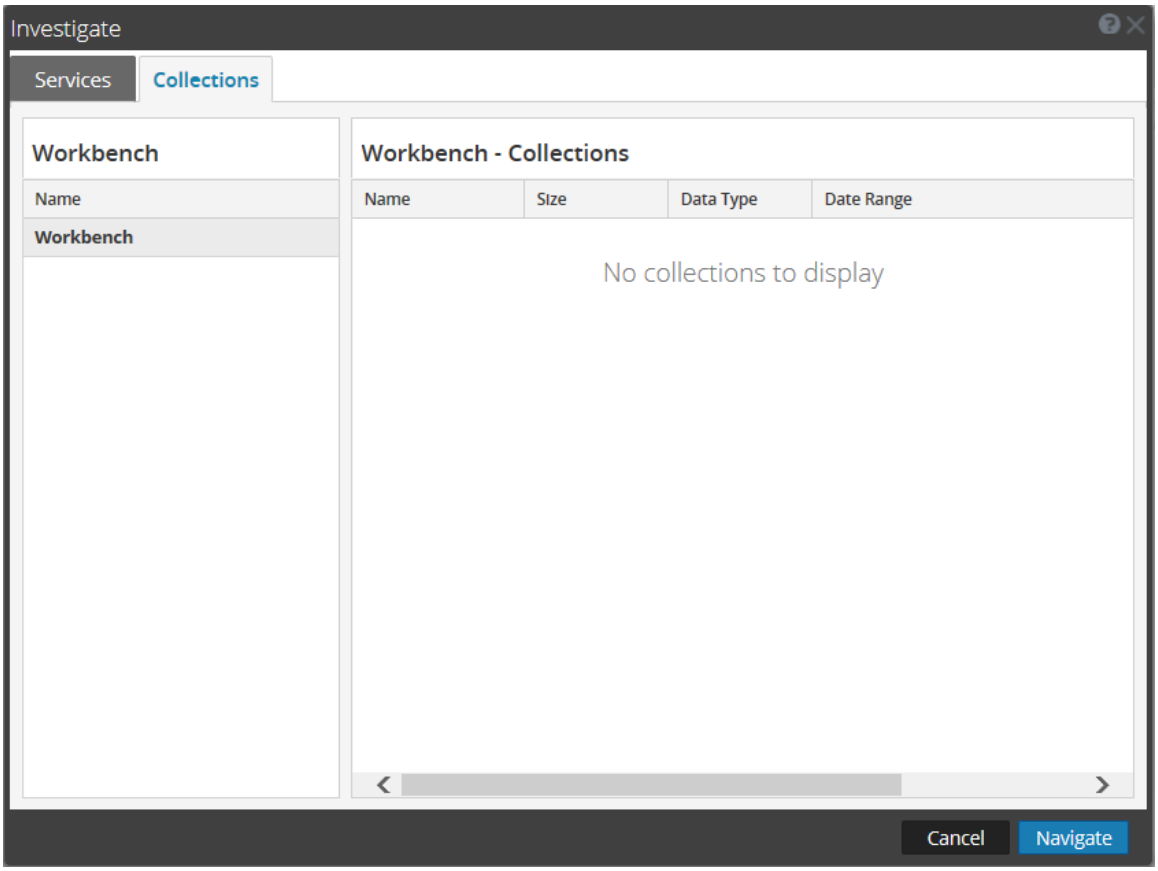
To perform an investigation on a workbench collection:

1. Select **Investigate**.
   The Investigate dialog is displayed.



2. Click the **Collections** tab in the Investigate dialog.
3. Select a Workbench service in the left panel.
4. Select the collection you want to investigate in the right panel.
5. Click **Navigate**.

The Navigate view is displayed showing data pertaining to the Workbench collection that you selected.



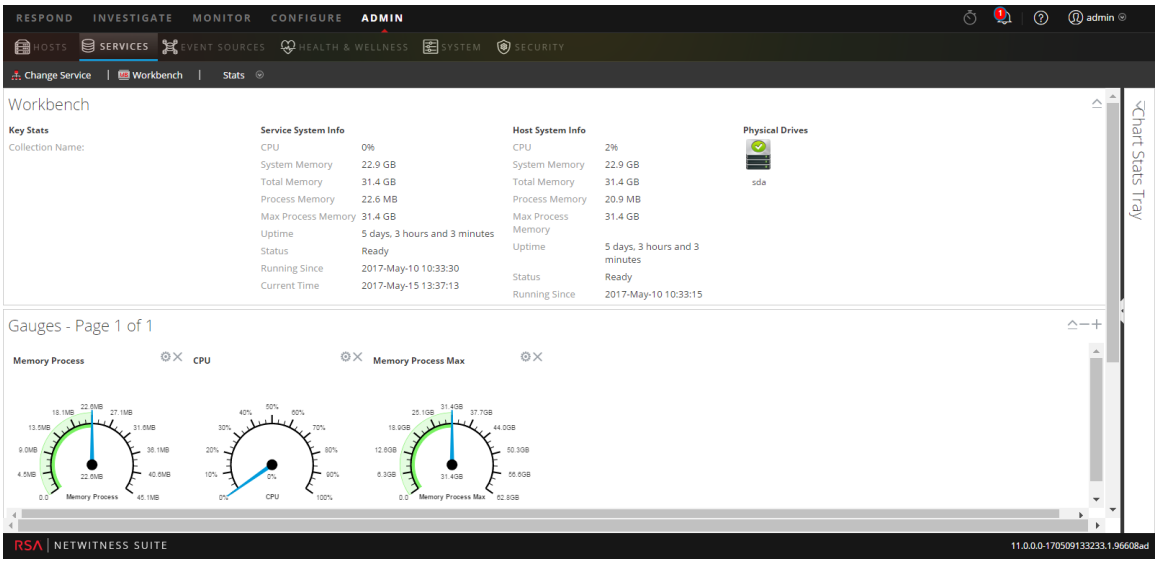
Note: For detailed information about using Investigation, see *Investigation and Malware Analysis Guide*.

View Workbench Collection Statistics

The same statistics available for other services are provided for the Workbench service. The Services Stats view displays key statistics and system information that pertain to your selected Workbench service. The information is displayed in several different sections within the Stats view: Workbench, Gauges, Timeline Charts and Chart Stats Tray. The Chart Stats Tray lists all available statistics for the Workbench. Any statistic in the Chart Stats Tray can be displayed in a gouge or a timeline chart.

Perform the following steps to view workbench statistics:

1. Go to **ADMIN > Services**.
2. In the Services view, select a **Workbench**, then select **> View > Stats**.
   The Services Stats view is displayed.



Note: For more information about Workbench statistics, see the *Host and Services Getting Started Guide*.

View Workbench Logs

Perform the following steps to view logs on a Workbench service:

1. Go to **ADMIN > Services.**
2. In the Services view, select a **Workbench**, then select **> View > Logs**.
   The Services Logs grid is displayed.

Note: For information about viewing and configuring audit logs, see the topic "Configure Global Audit Logging" in the *System Configuration Guide* .

References

Workbench Reference Topics:

- Services Config View - Workbench
- Services Config View - Collections Tab
- Services Config View - General Tab

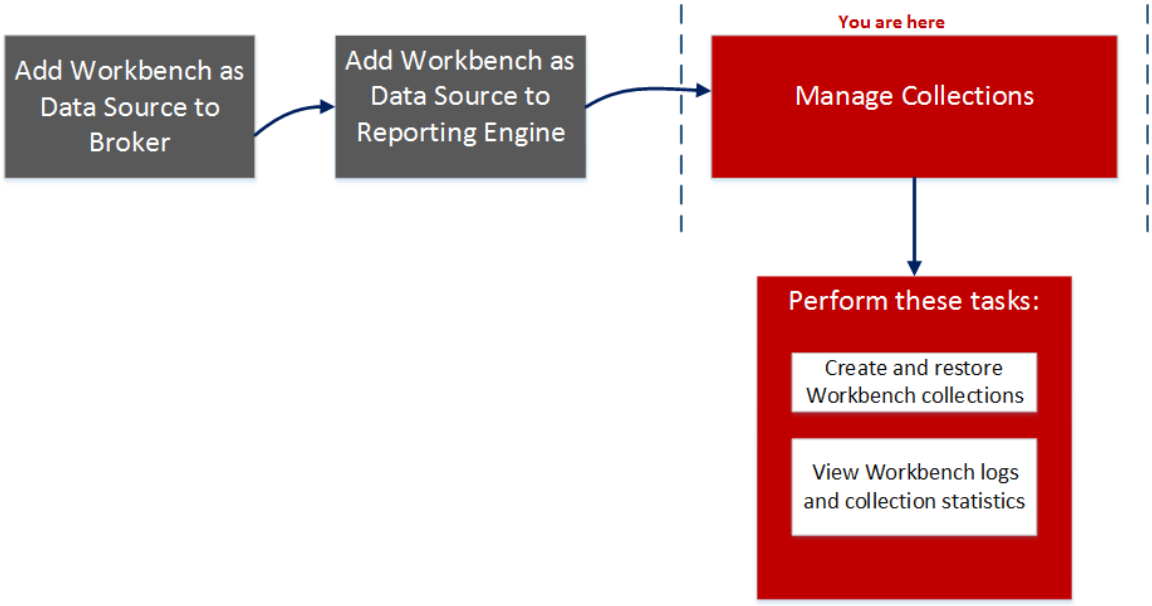
Services Config View - Workbench

In the Services Config view for workbench, some of the parameters are the same as other NetWitness Suite services, while others are specific to the Workbench service.

The Services Config view - Workbench (ADMIN > Services >, select Workbench service and select View > Config) provides a way to configure a Workbench service.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Add Workbench as data source to Broker	Adding Workbench Service as a Data Source to Broker
Administrator	Add Workbench as a Data Source to Reporting Engine	Adding Workbench as a Data Source to Reporting Engine
Administrator	*Create or delete a collection	Managing Collections

Role	I want to...	Show me how...
Administrator	*View Workbench statistics and logs	Managing Collections
Administrator	View configuration information about appliances that are connected to the Workbench service.	Select the **Appliance Service Configuration** tab. The Appliance Service Configuration tab is the same for all NetWitness Suite services. It provides configuration information about appliances that are connected to the Workbench service. For information on the **Appliance Service Configuration** tab, see **Appliance Service Configuration Tab** in the *Host and Services Getting Started Guide*.

*You can perform this task here.

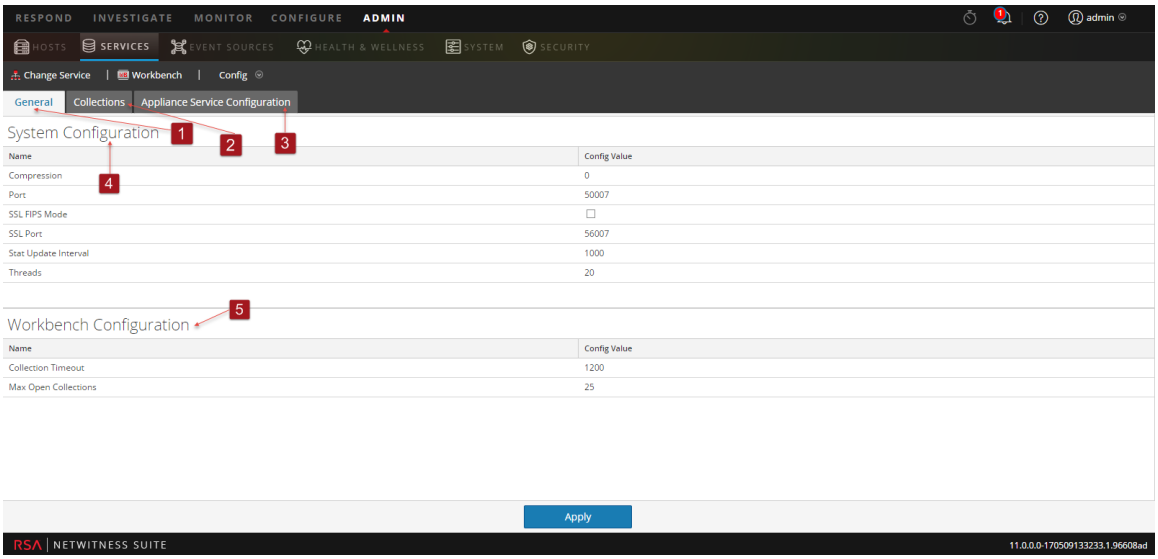
Related Topics

- Workbench Configuration Procedures

Quick Look

The Workbench service has three tabs and two panels in the Config view:

- General tab
- Collections tab
- Appliance Service Configuration tab
- System Configuration panel
- Workbench Configuration panel



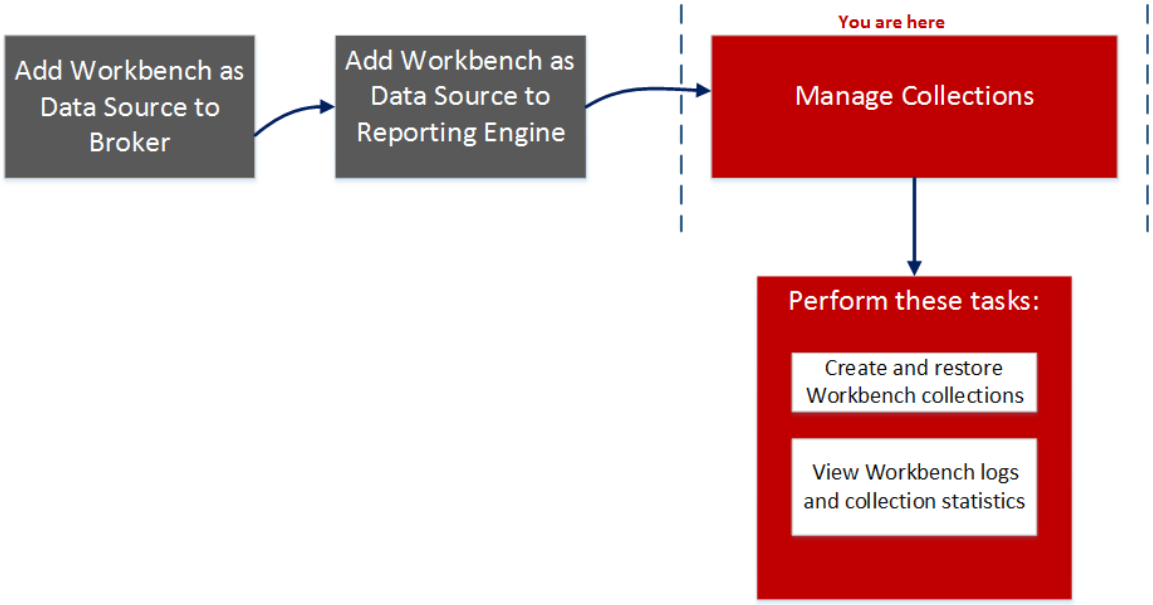
1	General tab provides a way to manage basic Workbench service configuration.
2	Collections tab provides a way to manage collections on a Workbench service.
3	Appliance Service Configuration tab provides a way to configure a Workbench service.
4	System Configuration panel provides a way to manage service configuration for a Workbench service.
5	Workbench Configuration panel provides a way to start and stop a Workbench service.

Services Config View - Collections Tab

The Collections tab for the Workbench service provides a way to manage workbench collections. To access the Collections tab, go to **ADMIN > Services >** select a Workbench service, select **View > Config** and select the **Collections** tab.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Documentation
Administrator	*Create and restore Workbench collections.	Managing Collections
Administrator	*View Workbench logs and collection statistics.	Managing Collections

Role	I want to...	Documentation
Administrator	View configuration information about appliances that are connected to the Workbench service.	Select the **Appliance Service Configuration** tab. The Appliance Service Configuration tab is the same for all NetWitness Suite services. It provides configuration information about appliances that are connected to the Workbench service. For information on the **Appliance Service Configuration** tab, see **Appliance Service Configuration Tab** in the *Host and Services Getting Started Guide*.

*You can perform this task here.

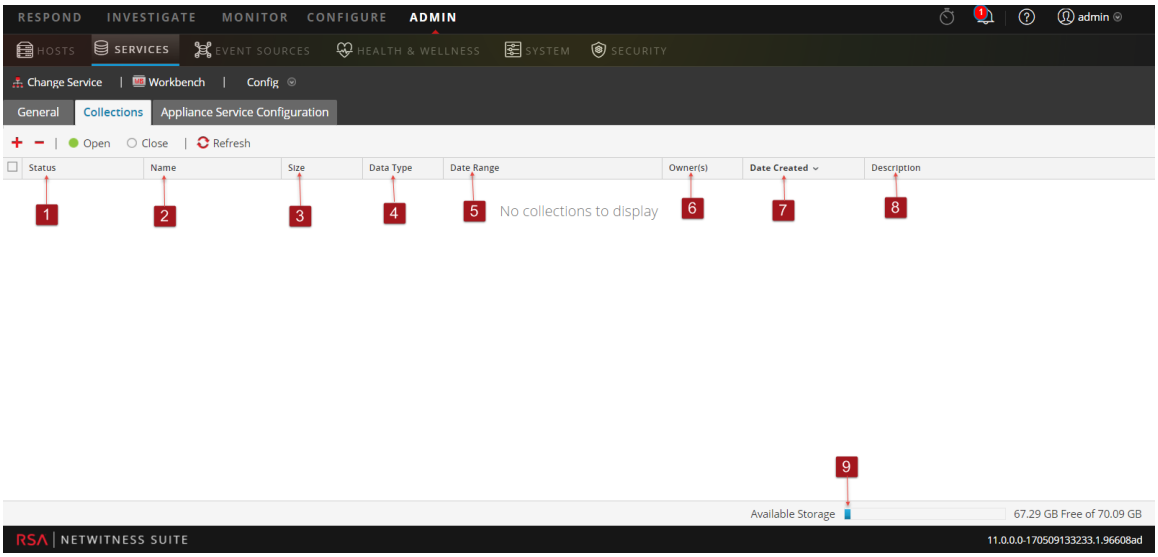
Related Topics

- Workbench Configuration Procedures

Quick Look

The Collections tab has a toolbar and a grid that lists relevant information about the Workbench collections.

The following figure is an example of the Collections grid.



1	Status of the Restoration Collection: • **Resorting Data** - Data restoration is in progress. • **Closed** - Data is restored. • **Opening** - Data is being indexed. • **Ready** - Indexing is complete. • **Closing** - Collection is closing.
2	**Name**: Name of the file being restored.
3	**Size**: Collection size.
4	**Data Type**: Logs.
5	**Date Range**: Lists the range of dates when the collection is being restored.
6	**Owner**: Lists the Collection creator.
7	**Date Created**: Shows the date when the collection was created.
8	**Description**: Description of the Restoration collection.
9	**Available Storage Indicator**: Shows the available disk space, given in gigabytes (GB). The Workbench validates to ensure there is enough available space when attempting to create a restoration collection.

Toolbar

These are the toolbar options.

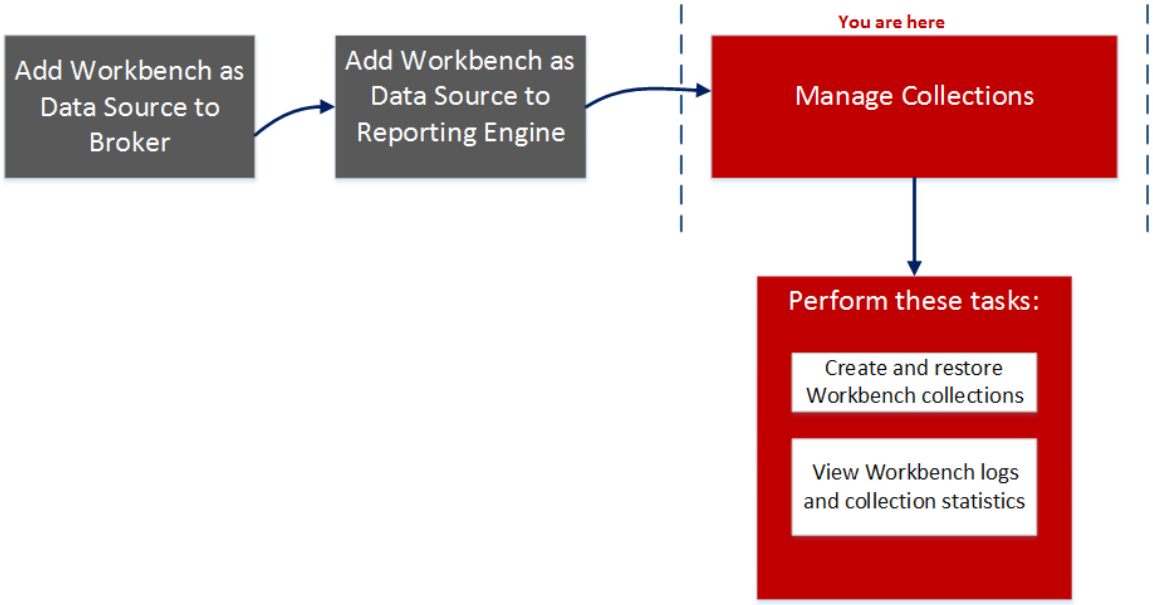
Parameter	Description
	Creates a new restoration collection.
	Deletes the selected Workbench collection.
Open and Close - Refers to the status of the restoration collection.	Open - Makes collection available for investigation and reporting. Close - Makes collection unavailable for investigation and reporting while preserving resources.
	Refreshes the list of Workbench collections.

Services Config View - General Tab

The General tab for the Workbench service provides a way to manage basic service configuration. To access the General tab, go to **Admin** > **Services** > select service and select > **View** > **Config**.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Show me how...
Administrator	*Create and restore Workbench service collections.	Managing Collections
Administrator	*View Workbench logs and collection statistics.	Managing Collections
Administrator	*Process Workbench collections.	Managing Collections

*You can perform this task here.

Related Topics

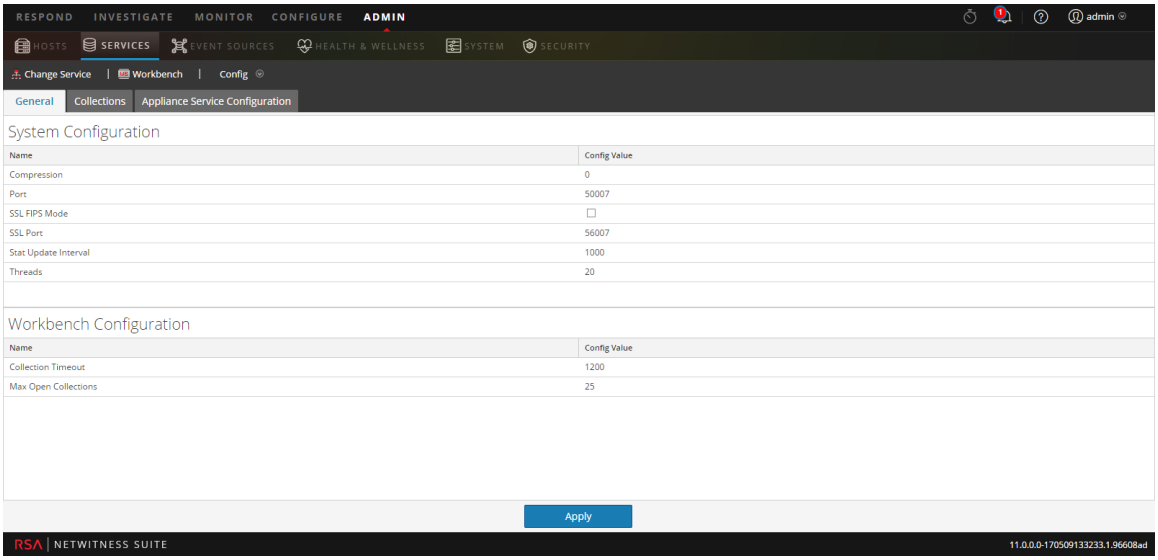
- Workbench Configuration Procedures

Quick Look

The General tab has two panels:

- System Configuration
- Workbench Configuration

The following figure is an example of the General tab.



System Configuration Panel

The System Configuration panel displays configuration parameters for the Workbench service. The following table describes the System Configuration panel features.

Parameter	Description
Compression	When set to a positive value, the minimum amount of bytes before a message is compressed. **0** means no compression for any message. Change takes effect on subsequent connections.
Port	The unencrypted port this service will listen on. **0** means disabled. Change takes effect on service restart.
SSL FIPS Mode	Determines whether the OpenSSL library will enter FIPS mode. Change takes effect on service restart.

Parameter	Description
SSL Port	The SSL port this service will listen on. **0** means disabled. Change takes effect on service restart.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system. Change takes effect immediately.
Threads	The number of threads in the thread pool to handle incoming requests. Change takes effect immediately.

Workbench Configuration Panel

The Workbench Configuration panel displays configuration parameters for the Workbench collections. The following table describes the Workbench Configuration panel features.

Parameter	Description
Collection Timeout	The number of seconds before an idle collection is automatically closed.
Max Open Collections	The number of collections that can be open at once. A setting of 0 disables the limit.
Apply	Updates the modified configurations in the panel.

Troubleshooting

NetWitness Suite notifies users of issues using popup notifications.

NetWitness Suite Workbench returns the following types of error messages explained in the following table.

Problem	Possible Causes	Solutions

Unable to connect to workbench service from NetWitness Suite **user interface Administration page.**	NetWitness Suite service is not running.	Verify that your NetWitness Suite service is running. Log in to your NetWitness Server and run the following command:
		`status nwworkbench`
		Firewall rules should allow connections from 50007, 50607 and 50107.
		Verify your connection by running the following command:
		`service iptables status`
		Verify that you are able to launch REST. Execute the following command for your appliance:
		`https://<IPAddress>:50107 service`
		If you are able to launch REST service for your appliance, you can confirm that there is no problem with the appliance. Navigate to the NetWitness Suite side for further investigation as follows:
		• Enable debug mode and watch for sa.log errors located at:
		`/var/lib/netwitness/uax/logs`
		• Enable developer tools using the shortcut `Ctrl+Shift+I` for Chrome and verify the preview and response for the request.

Problem	Possible Causes	Solutions
Not able to view Appliance service configuration tab for workbench appliance running in SSL mode.		Enable SSL for appliance service and restart the appliance service.

The following error message is displayed when trying to load meta in order to create a report on a workbench collection: "Unable to fetch schema from data source when trying to load meta."		Load meta for the appliance from the NetWitness Suite User Interface Rule library and watch for any errors in Reporting Engine log located at:
		`/home/rsasoc/rsa/soc/reporting-engine/logs`
		Launch REST for the device and watch for any error if you run the following query:
		`/sdk?msg=language&force-content-type=text/plain&expiry=600&size=10`

Problem	Possible Causes	Solutions
No results are displayed after running query from NetWitness Suite User Interface via the Reporting Engine.		Run the query on the Reporting Engine and watch for `/var/log/messages` on the data source. Look for an exact query that matches the data source. **TIP**: Search for `[SDK-Query]` in log file. Copy the exact query and run from REST SDK to see if you get any results. REST Query: /sdk?msg=query&force-contenttype=text/plain&expiry=600&query=select%20user.dst&size=10
Workbench Available storage indicator in Workbench Collections Tab is not accurate.	Available storage indicator in the User Interface displays the default Collections directory shown below: /VAR/NETWITNESS/WORKBENCH/COLLECTIONS	None.
Unable to open new collections after opening existing collections.	There is a workbench configuration called “Max Open Collections” that is set to 25 by default. This configuration specifies the number of collections that can be open at the same time.	You can modify this number. A setting of zero disables the limit of maximum open collections.

Problem	Possible Causes	Solutions
Successfully opened a collection that got to Ready state. But after a while, the collection automatically changed to Closed state.	There is a workbench configuration called “collection.timeout” that is set to 1200 seconds by default. This configuration specifies the number of seconds before an idle collection is automatically closed. Maximum time allowed before timeout occurs is 86,400 seconds (24 hours).	A setting of zero disables the timeout.
Querying for a time range using `/database manifest` command returned blank output.	Blank output indicates that there are no **nwdb** files available for the time range.	None.
Created collection, but collection status is not available in Jobs, and collection is not displayed in workbench Collections tab.	You might be running in a mixed mode environment (for example, creating a collection on a 10.4.x version of workbench from a 10.5 NetWitness Suite User Interface.	The collection is displayed in the workbench Collections tab after you reload the page.

Problem	Possible Causes	Solutions
Noticed blank Date Range and Date Created values for collections.	All collections display blank Date Range and blank Date Created values.	Date Range and Date Created values are displayed after upgrading to 10.5.
Discrepancy in behavior of adding workbench collections as a data source to Reporting Engine.	This behavior depends on whether you have a trusted connection or a non-trusted connection.	If your workbench service is established with a trusted connection, you should manually add workbench collections as a source to Reporting Engine. If your workbench service is not established with a trusted connection when the workbench restoration collection was created, it automatically sends a message to the Reporting Engine to add it as a source in the Reporting Engine.
Collection attributes (size, date range and date created) are not displayed.	Date range is not displayed for a collection if Jetty service is restarted while restoration is in process. Restoration collections created from an Explorer view display a blank Date Range. Any collections created on a 10.4 Workbench will display blank Date Range and blank Date Created values after upgrading to 10.5. In a mixed mode environment (10.5 NetWitness Server and 10.4.x workbench), size, date range, and date created are not displayed.	None.

Problem	Possible Causes	Solutions
Exception or blank page is displayed when drilling down on a workbench collection.	Collection closed because it exceeded the collection time out.	Investigate the collection from the beginning.
Empty collection is created.	Empty collection is displayed if restoration fails because Workbench service is restarted during collection creation.	None.
Service abruptly shuts down.		Run the service from command line and watch for any errors. For an example, run the command from the server console `/usr/sbin/NwWorkbench` for workbench.
REST request denied.		Verify user.agent.whitelist config located at `/rest/config/`. If non-blank, this should be a regex expression to match valid HTTP user agents. If the regex fails to match, all REST requests will be denied (see allow.missing.user.agent for the potential exception). If blank, all requests are allowed.

Problem	Possible Causes	Solutions
Queries with raw meta return blank values for Raw field.		Verify that you have a relevant `packet db`.

RSA NETWITNESS® SUITE

System Configuration, Management, and API Guides

for Version 11.1.0.0

RSA NETWITNESS® SUITE

Data Privacy Management Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Data Privacy Overview **5**

Data Obfuscation 5

Data Retention Enforcement 6

Audit Logging 7

Components Covered by the Data Privacy Feature 7

Data Privacy Feature Implementation by Component 8

Component-Specific Configuration Guidelines 10

Recommended Configurations **11**

Recommended Data Privacy Configuration 11

Options for Data Retention Configurations 11

Data Storage With Data Retention Options in Effect 12

Option 1: No Original Data Saved to Disk, Only Hash Stored 14

Option 2: No Original or Obfuscated Values Stored: not recommended 15

Optional Data Overwriting Options 16

Option 1: Limit Disk Space for Continuous Overwriting of Older Data 16

Option 2: Use Tiered Storage to Overwrite Data on a Scheduled Basis 16

Option 3: Purge Data Using String and Pattern Redaction Option 17

Limitations to Data Overwriting 17

Quick Start Procedures **19**

Prepare to Configure Data Privacy 20

Configure the Recommended Data Privacy Solution 23

Configure Meta and Content Restrictions on Brokers, Concentrators, and Decoders 23

Add Data Privacy Officer and Analyst Accounts on the NetWitness Server 25

Configure Obfuscated Data on Decoders and Concentrators 27

Configure Data Retention on Concentrators and Decoders 28

Validate Data Privacy Protection 29

In-Depth Procedures **31**

Configure Data Obfuscation 32

Configure the Decoder Hash Algorithm and Salt 32

Configure Language Keys 33

Configure Metadata and Content Visibility Per User Role on Core Services 36
Configure Meta Keys Not Written to Disk Per Parser on a Decoder 40
Configure Data Retention 42
Data Retention 42
Deleting versus Retaining Log Data 43
Configure Log Retention and Storage on an Archiver 44
Schedule a Recurring Job to Check Data Retention Thresholds 44
Configure User Accounts for Use in Data Privacy 47
Customize the Default Administrators User Role at the Service Level 47
Add a User Account with the Aggregation User Role at the Service Level 48
Add Data Privacy Officer and Analyst Accounts on the NetWitness Server 48
Data Privacy References 51

Data Privacy Overview

This topic introduces the concept and implementation considerations for a data privacy officer or administrator who is managing exposure of privacy-sensitive data in RSA NetWitness® Suite. In addition, information about recommended use cases is included.

Note: A data privacy plan touches on most components of NetWitness Suite. The person who configures data privacy needs to understand NetWitness Suite network components, configuration of NetWitness Suite hosts and services as described in the *Host and Services Getting Started Guide*, and the types of information that need to be protected.

Regulatory mandates in some locations, for example the European Union (EU), require that information systems have a means of protecting privacy-sensitive data. Any data that could directly or indirectly identify "Who did what when?" may be considered privacy-sensitive data. A few examples are user names, email addresses, and host names. NetWitness Suite provides a range of controls that customers can leverage to protect privacy-sensitive data. These controls can be used in a variety of combinations to protect privacy-sensitive data, without significantly reducing analytical capability.

A user role for a Data Privacy Officer (DPO) was added in NetWitness Suite 10.5 to support the management of privacy-sensitive data. The DPO can configure NetWitness Suite to limit exposure of meta data and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness Suite include:

- Data Obfuscation
- Data Retention Enforcement
- Auditing Logging

Data Obfuscation

NetWitness Suite has configurable options for data obfuscation, Data privacy officers and administrators can specify which meta keys in their environment are privacy-sensitive and limit where the meta values and raw data for those keys are displayed in the NetWitness Suite network. In place of the original values, NetWitness Suite can provide obfuscated representations to enable investigation and analytics. In addition, DPOs and administrators can prevent persistence of privacy-sensitive meta values and raw logs or packets.

Three methods work together to implement data obfuscation:

- Obfuscation of meta values for privacy-sensitive meta keys with an optional salt. Meta keys configured as protected are represented by obfuscated values at the time of creation on a Decoder or Log Decoder; the obfuscated values are hashed and considered to be impossible

to read. To implement, you need to configure the Decoder and Log Decoder hash algorithm and salt, and configure privacy-sensitive language keys as protected on all Core services.

- Role-based access (RBAC) to the raw logs or packets and the privacy-sensitive meta values. The DPO can use roles with granular permission capabilities to restrict what an analyst versus a data privacy officer is able to view during configuration, analysis, and investigation. The *System Security and User Management Guide* provides in-depth coverage of RBAC implementation in NetWitness Suite. To implement, you need to configure meta and content visibility per role on individual Brokers, Concentrators, Decoders, Log Decoders, and Archivers.
- Preventing persistence of privacy-sensitive meta values and raw logs or packets. To implement, you need to configure meta keys on parsers for individual Decoders and Log Decoders as transient.

Data Retention Enforcement

NetWitness Suite can ensure that data is retained only as long as necessary or as specified. An administrator can configure data retention using age and time thresholds on a per-service basis. Schedulers running on each service automatically delete data meeting those thresholds. Once the data is deleted, it is no longer available through user interfaces, queries, or application programming interface (API) calls. Some of the NetWitness Suite components also support purging of data through overwrites.

An administrator can manage data retention in several ways:

- Configure how long data persists in storage on the system.
- For Core services, strategically remove privacy-sensitive data that may have been written by configuring automatic removal of data of a specific age.
- Configure NetWitness Suite so that original data is not sent or saved to the other components. If privacy-sensitive data makes its way into another database on the Reporting Engine, Malware Analysis, and NetWitness Servers, data retention can be managed there as well. This configuration for Event Stream Analysis is managed in the Services Explorer view.

Note: If a situation arises where the DPO decides that already collected data is privacy-sensitive after the system is functional, the administrator can manually overwrite the data from databases or files where the data is saved.

Audit Logging

Administrators can leverage audit logs that NetWitness Suite creates using the Global Audit Logging feature. The audit logging feature generates audit log entries about many activities, and the following are examples of log entries that are relevant to data privacy:

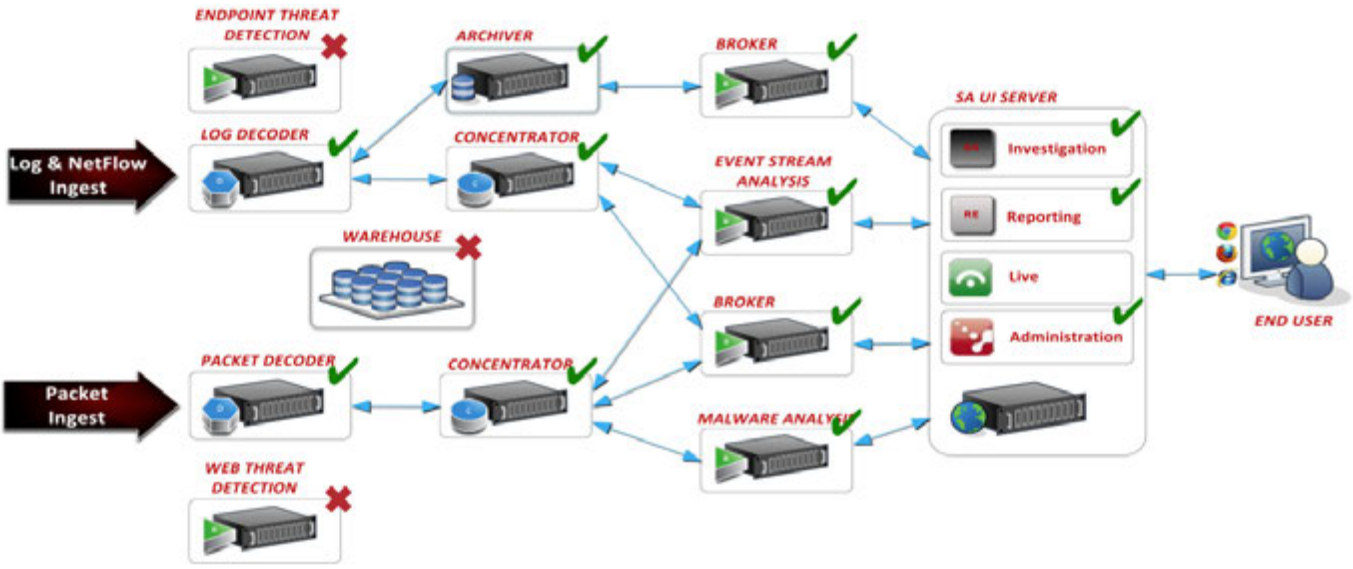
- Modifications to permissions and users assigned to roles.
- Failed and successful attempts to log on to NetWitness Suite and log off.
- Data deletion.
- Data exports and downloads.
- Navigation by users to user interfaces and queries that users performed.
- Attempts (successful or not) to view or modify privacy-sensitive data, including an identification of the user who made the attempts.

All audit log entries are part of a standard audit trail for NetWitness Suite. Administrators can configure NetWitness Suite to forward audit logs to a designated destination, including third-party systems to provide additional filtering and reporting capabilities. For more information on Global Audit Logging, see **Configure Global Audit Logging** in the *System Configuration* guide.

Components Covered by the Data Privacy Feature

The figure below identifies the NetWitness Suite components covered by the 10.5 or later data privacy feature with a green check mark. Components marked with an X are not supported by data privacy functions. The *NetWitness Suite Getting Started Guide* provides a functional description of NetWitness Suite components.

Note: NetWitness Suite data privacy features are not supported for Warehouse and protected meta data can make it to Warehouse via Warehouse Connector, unless explicitly configured to be filtered out using Warehouse Connector Meta Filters. If protected meta data makes it to Warehouse, users having direct access to Warehouse can query such data. Data privacy officers need to prevent that through administrative, technical, and procedural controls outside of NetWitness Suite.



Data Privacy Feature Implementation by Component

The following table identifies which data privacy features are supported for each NetWitness Suite component. For each component, a checkmark indicates if the component supports data obfuscation, data retention enforcement, data overwriting, and audit logging.

Component	Data Obfuscation	Data Retention Enforcement	Data Overwriting	Audit Logging
Ingestion				
Decoder	✓	✓	✓	✓
Log Decoder	✓	✓	✓	✓
Meta Aggregation				
Concentrator	✓	✓	✓	✓
Broker	n/a	✓ (stored in DPO cache only)[1]		✓
Real-Time Analysis				

Component	Data Obfuscation	Data Retention Enforcement	Data Overwriting	Audit Logging
Investigation	✓	✓ (stored in DPO cache only)[2]		✓
Event Stream Analysis	✓			✓
Malware Analysis	✓	✓		✓
Respond	✓	✓		✓
Reporting				
Reporting Engine	✓	✓		✓
Long-Term Analytics				
Archiver	✓	✓	✓ (uncompressed)[3]	✓
Warehouse				

Notes:
1 - Brokers can cache data and this needs to be cleared by configuring an independent rollover and other removal of cache as required. The administrator can configure cache rollover for a Broker using the Scheduler in the Services Config view Files tab.
2 - Investigation and the NetWitness Server cache data, and this is cleared automatically every 24 hours.
3 - The overwriting procedure described in Configure Data Retention applies to uncompressed data.

Component-Specific Configuration Guidelines

NetWitness Suite components and modules that obtain access to privacy-sensitive meta data and their obfuscated counterparts are Investigation, Event Stream Analysis (ESA), Malware Analysis, Respond, and Reports. They get access to data based on the permissions defined for the role to which the user belongs. The Administrator or DPO configures each Decoder or Log Decoder to identify meta keys that are flagged for obfuscation.

These components have additional guidelines to ensure that they function as expected with a data privacy scheme:

- **Event Stream Analysis**. When ESA receives privacy-sensitive data from NetWitness Suite core, ESA passes on only the obfuscated version of the data. ESA does not store or show protected data. There are some additional guidelines for configuring advanced EPL rules and enrichment sources (described in the **Sensitive Data** topic in the *Alerting with ESA Correlation Rules User Guide*). Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
- **Malware Analysis**. Malware Analysis references certain meta keys during scoring, including `alias.host`, `client`, and others. To ensure no loss of analytical functionality Malware Analysis should be configured as a trusted client; that is, configured to connect to the NetWitness Suite Core infrastructure with an account equivalent to a user in DPO role. Otherwise, if meta keys referenced by Malware Analysis do get tagged for obfuscation and are not accessible to Malware Analysis, some of the Indicators of Compromise (IOCs) may be rendered ineffective.
- **Respond Server service.** The Respond Server service uses a data privacy mapping file to display obfuscated data in alerts.(see the **Obfuscate Private Data** topic in the *Respond User* guide) and has a configurable data retention period for alerts (see the **Set a Retention Period for Alerts and Incidents** topic in the *Respond User* guide). Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
- **Reports.** In Reporting Engine, each Core service is added as two separate data sources, using the two separate service accounts; one data source has a service account representing the Data Privacy Officer role and the other data source has a service account representing a non-Data Privacy Officer role. The **Configure Data Privacy for Reporting Engine** topic in the *Reporting Engine Configuration Guide* provides procedures to configure data privacy for Reporting Engine. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Recommended Configurations

This topic describes the recommended data privacy implementation for NetWitness Suite and several additional use cases for managing exposure of privacy-sensitive data in NetWitness Suite. Administrators can set up the NetWitness Suite hosts and services to meet data privacy requirements for their environment. RSA has recommended configurations for both data privacy and data retention.

Recommended Data Privacy Configuration

The recommended configuration to obtain the best analytical value with data obfuscation enabled is to define privacy-sensitive meta data and keep both original and obfuscated (hash) values of privacy-sensitive data on disk for Decoders, Log Decoders, Concentrators, and Brokers.

The assumption is that only a handful of meta data (approximately 10 meta keys) will be classified as protected and a FIPS 140-compliant algorithm for hashing will be used along with a salt to make reverse engineering the original value difficult. The recommended solution is SHA-256 with a salt of length at least 16 characters and up to 60 characters.

Note: By default, hash values are stored in binary format for faster response times and because it requires less storage space in the database when compared to saving them in string format. The recommended storage method is text/string.

Brokers and Investigation may have original and obfuscated data in cache due to data privacy officers using Investigation to confirm the original value to which the obfuscated value maps during investigations. Downstream services can also limit the use of the original sensitive values to in-memory processing so that data does not persist on disk in those downstream systems; this holds true for ESA and Malware Analysis.

The recommended solution to delete data when ready is the built-in and automatic data retention enforcement, which deletes data at a certain threshold. You can use this method for the following components in NetWitness Suite 10.5: Decoder, Log Decoder, Log Collector, Archiver, Malware Analysis, Incident Management, and Reporting Engine. You can manually configure Event Stream Analysis to support similar automatic data retention enforcement.

To manage cache storage, the NetWitness Server clears cache related to investigations of events every 24 hours. The Broker can also be configured to execute a periodic removal of locally stored cache.

Options for Data Retention Configurations

NetWitness Suite provides alternative controls that the administrator can apply to enforce stronger restrictions on privacy-sensitive data storage when data obfuscation is enabled.

Data Storage With Data Retention Options in Effect

The following table summarizes where data is stored in the default configuration with no data privacy as well as for each data retention alternative. A checkmark indicates that privacy-sensitive data is saved on the component; an X indicates that no privacy-sensitive data is stored on the component.

Component	Default Configuration	Data Storage Options		
	Original Data Stored	Original Data and Hash Stored (recommended)	Only Hash Stored	No Data Stored (all meta data is transient)
Ingestion				
Decode	✓	✓	X	X
Log Decoder	✓	✓	X	X
Meta Aggregation				
Concentrator	✓	✓	X	X
Broker	✓ (Cache only)	✓ (Cache only)	X	X
Real-Time Analysis				
Investigation	✓	✓ (Cache only)	X	X
Event Stream Analysis	✓	X	X	X
Malware Analysis	✓	X	X	X
Respond Server service	✓	X	X	X

Component	Default Configuration	Data Storage Options		
	Original Data Stored	Original Data and Hash Stored (recommended)	Only Hash Stored	No Data Stored (all meta data is transient)
Reporting				
Reporting Engine	✓	✓ (Optional)	X	X
Long-Term Analytics				
Archiver	✓ (Optional)	✓ (Optional)	X	X
Warehouse	✓ (Optional)	✓ (Optional)	X	X
Content				
Live	n/a	n/a	n/a	n/a
Fraud Analysis				
RSA Fraud and Risk Intelligence Suite	n/a	n/a	n/a	n/a
End Point Protection				
NetWitness Endpoint	n/a	n/a	n/a	n/a

Component	Default Configuration	Data Storage Options		
	Original Data Stored	Original Data and Hash Stored (recommended)	Only Hash Stored	No Data Stored (all meta data is transient)

Notes:

Cache Only means that sensitive data is in the Broker or NetWitness Server cache. Configure Data Retention provides details about automated and manual clearing of cache.

Optional means that sensitive data storage does occur, but can be limited by optional configurations. For example, to limit where sensitive data is stored, do not enable DPO access for Reporting and do not aggregate original protected data into the Archiver.

Option 1: No Original Data Saved to Disk, Only Hash Stored

Administrators can eliminate the persistence of sensitive data to disk and store only an obfuscated value if the risk of exposure is too great. In this scenario, meta data generated during parsing on the Decoders and Log Decoders is used only in memory and not written to disk. Administrators can configure individual meta keys on a Decoder or Log Decoder as transient to ensure that sensitive meta data is not written to disk. Downstream services do not see original values and must use obfuscated values to conduct investigation and analytics.

To configure this data privacy scheme, data obfuscation must be enabled with hash values configured. You can configure individual meta keys on a Decoder or Log Decoder as transient to ensure that original values are not written to disk.

- Original values identified as sensitive are extracted from the raw data during parsing on the Decoder and Log Decoder and are accessible to the system during parsing (parsers, rules, feeds).
- The Decoder does not save the original values for meta keys identified as sensitive, storing only the hash of original values along with other non-sensitive meta data related to the event.

A side effect of these options is some loss in analytical capability, but you can configure these to suit the needs of your environment.

- By configuring all sensitive data as Transient, sensitive values are not persisted to disk, and the analytic capabilities using the original value are available at parse time only (parsers, rules, feeds).
- Event stream analysis (ESA) and malware analysis systems must rely only on the obfuscated meta values when doing their correlation and scoring respectively.
- Reporting Engine is limited to pulling reports using the non-sensitive and obfuscated values.
- The data privacy officer cannot view the original value, but can use the configured hash and salt to determine if an obfuscated value represents a specific known original value.

Option 2: No Original or Obfuscated Values Stored: not recommended

Administrators can eliminate the persistence of the original value to disk entirely if the risk of exposure is too great. As in Option 1, in this scenario, meta data generated during parsing on the Decoders and Log Decoders is used only in memory and not written to disk. Administrators can configure individual meta keys on a Decoder or Log Decoder as transient to ensure that sensitive meta data is not written to disk. Downstream services do not see original values and have no obfuscated values to conduct investigation and analytics.

To configure this data privacy scheme, configure individual meta keys on a Decoder or Log Decoder as transient to ensure that original values are not written to disk.

- Original values identified as sensitive are extracted from the raw data during parsing on the Decoder and Log Decoder and are accessible to the system during parsing (parsers, rules, feeds).
- The Decoder does not save not save the original values for meta keys identified as sensitive, storing only non-sensitive meta data related to the event.

A side effect of these options is significant loss in analytical capability, but you can configure these to suit the needs of your environment.

- By configuring all sensitive data as Transient, sensitive values are not persisted to disk, and the analytic capabilities using the original value are available at parse time only (parsers, rules, feeds). See Configure Data Retention.
- All downstream components have no visibility in the original values, obfuscated or otherwise.
- The data privacy officer has no visibility into the original value obfuscated or otherwise.

Optional Data Overwriting Options

Several options for overwriting data are available, and you should thoroughly understand each one before implementing data overwriting.

Option 1: Limit Disk Space for Continuous Overwriting of Older Data

If the desired data retention period to store the data, and therefore the amount of storage required for that data, is known the size of the underlying hardware or the partition can be limited to that size. By reducing the hard drive storage or the partition size, the amount of free space available that has to be filled before new data overwrites it would also be limited. The newly ingested data continually overwrites the older data. Either solution must be done at deployment time to be effective.

Side effects of this option are:

- The removal of some disks will limit the number of resources available to distribute the I/O, causing some degradation in performance.
- The smaller partition size may cause some degradation in performance, but would alleviate some of the performance impact of removing disks.

Option 2: Use Tiered Storage to Overwrite Data on a Scheduled Basis

If overwriting of data is required on a scheduled automatic basis, you can configure the Decoders and Concentrators to use tiered storage. The tiered storage configuration provides a mechanism for invoking a script after a database file has been removed from the application but prior to its removal from the file system. If necessary, instead of moving the file to the second tier, or cold storage, (the intended function in a tiered storage use case), the script can use a utility like the CentOS `shred` utility to overwrite the file. This tool is less effective when the database is stored in a journaling file system like XFS, in which the Core database resides, and on a RAID logical drive like the ones with which the Core hosts connect.

Most other NetWitness Suite components do not have this option; their data is stored in a database that does not support the tiered storage mechanism. The only other component that could use this overwrite method is the Reporting Engine since it saves reports and alerts as individual files. However, the Reporting Engine charts are stored in a database so they would be immune to this technique.

Option 3: Purge Data Using String and Pattern Redaction Option

Data purging provides a mechanism to strategically overwrite a specific subset of data from the system in case any sensitive data has been persisted either on purpose or by accident. The NetWitness Suite `wipe` utility allows for unique patterns to be written over the data in the meta and packet databases for Core services, which may contain RAW packets or logs for existing sessions, based on a session identifier. All Core components have the capability to overwrite a subset of data that has been found by executing a query string, including regex patterns. The session identifiers resulting from the query are fed into the NetWitness Suite wipe utility.

Note: This option is not available if the data in the Core database has been compressed (as typically done in Archiver deployments).

In most NetWitness Suite components the database in use does not provide a built-in redaction or secure deletion mechanism. The Malware Analysis component can overwrite the data object in the database with the value `private` instead of deleting it during the data retention management process, but this is not meant to be a secure deletion mechanism.

Caution: Using this method on a large number of sessions has two drawbacks: it can be time-consuming and impact performance.

Limitations to Data Overwriting

There are limitations to the overwriting techniques described as Option 2 and 3. To perform the overwrite of the data in the disk sectors, the above options for overwriting and the overwrite command line tool provided as an alternative method (`shred`, a function of CentOS) make assumptions about the disk layout. NetWitness Suite hosts use SSD drives and RAID configurations for performance and reliability reasons, and these inhibit the functionality of the overwrite techniques. If overwrite techniques alter SSD drives and RAID configurations in an attempt to increase security, there will inevitably be an associated performance cost reflected in ingest rates, query speeds, and potentially other areas. The command line tools available for overwrite are recommended only for special use cases when it is necessary to redact specific data. The tools are not for use in a real-time continuous method because of the potential performance cost that will be incurred.

Quick Start Procedures

This section provides end-to-end instructions for preparing to configure data privacy features, then completing the configuration of the recommended data privacy solution.

- Prepare to Configure Data Privacy
- Configure the Recommended Data Privacy Solution

Prepare to Configure Data Privacy

This topic provides general guidelines for planning and configuring data privacy policies in the NetWitness Suite network. Before beginning configuration, you must understand the data that needs to be protected on your network and develop a plan. You will need to:

1. Identify the meta keys that hold privacy-sensitive data and need to be protected. This decision is based on requirements specific to your site.
2. Decide which users need access to privacy-sensitive meta data and raw content. The first decision is whether to separate the DPO and administrator roles for your site by configuring a custom administrators system role on Decoder and Log Decoders and removing the `dpo.manage` permission. By default, administrators have all permissions including the ability to configure the salted hash transform used to obfuscate data; some sites may want to reserve this access for data privacy officers. The **Service User Roles and Permissions** in the *Hosts and Services Getting Started Guide* has more details on exactly what permissions each role has and the purpose of the permissions.
3. Plan the configuration changes you need to make in your NetWitness Suite deployment to support adequate data privacy.
4. Assess how your configuration may impact out-of-the-box and custom content. For example, by default content available via Live for Reporting Engine is not geared toward obfuscated meta values.

In a single deployment, certain data-privacy configurations in the Core services must be the same. The following table lists these settings and uses a checkmark to identify the services for which the configuration must be the same.

	Configure the Same For:				
Data-Privacy Setting	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**
Hash algorithm and salt for privacy-sensitive data	✓	✓			

	Configure the Same For:				
Data-Privacy Setting	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**
Language key data privacy attributes in the custom index file (includes configuring keys as protected)	✓	✓	✓	✓	✓
Transient meta keys (not persisted on disk) per service and parser	✓	✓			
Meta data and raw content visibility per system user group. (The meta keys must exist in the custom index file.)	✓	✓	✓	✓	✓
User who has the `Aggregation` service user role assigned is added.*	✓	✓	✓		

	Configure the Same For:				
Data-Privacy Setting	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**

* When trying to access data on an aggregate service, the Log Collector or Broker requests authentication. When prompted to enter user name and password, you must authenticate as a user who is assigned the `Aggregation` service role. The **Aggregation Role** topic in the *Hosts and Services Getting Started Guide* provides detailed information about this role. Follow the instructions in the **Add, Replicate or Delete a Service User** topic in the *Hosts and Services Getting Started Guide* to create a user and assign the new user the Aggregation service user role.

Configure the Recommended Data Privacy Solution

This topic tells administrators and data privacy officers how to configure the recommended data privacy solution in a NetWitness Suite network. These are the basic steps to follow to configure the NetWitness Suite system to identify sensitive data and determine who can see the sensitive data. The recommended configuration generates obfuscated values of certain original meta keys and then persists both the original and obfuscated data so that it is available to users assigned privileged role access.

This configuration has several parts:

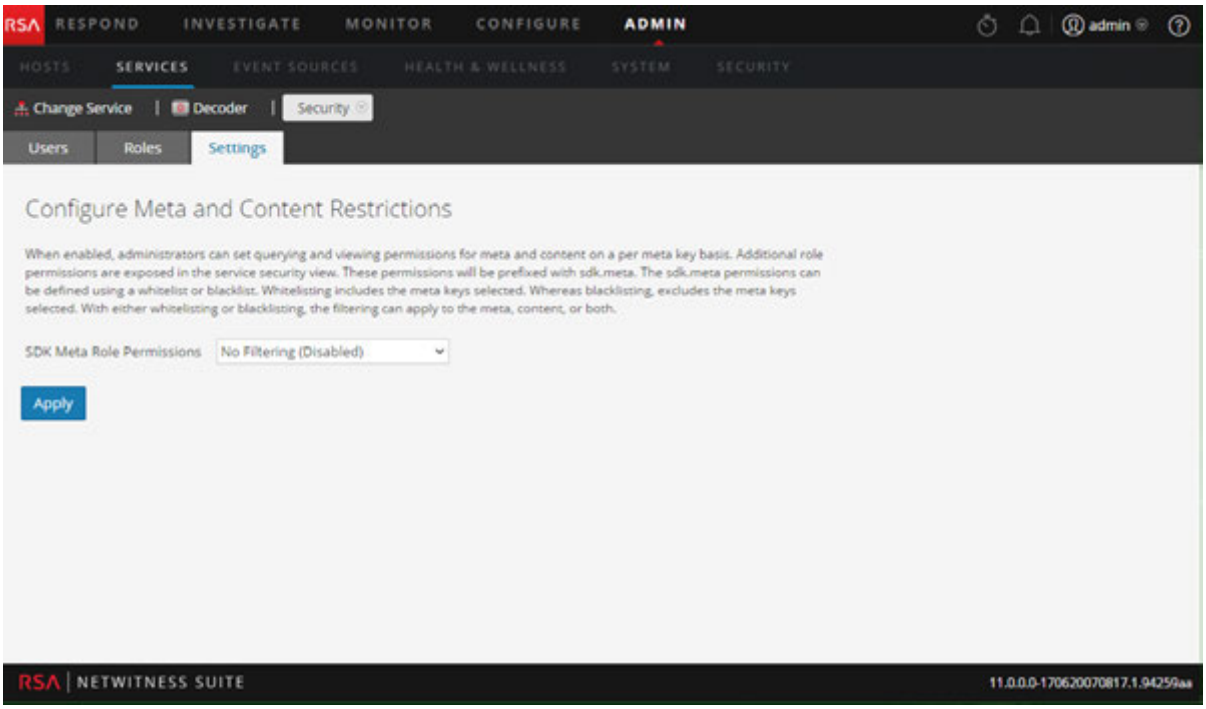
1. Create two users with different levels of permissions. One user (the data privacy officer) can view all meta data and another user (an analyst) is restricted from seeing certain meta data and content with associated meta data.
2. Set up two transforms using a salt and hash to create an obfuscated version of original `username` and `ip.src` meta keys.
3. Configure data retention on the Decoder and Concentrator services.

Note: The following conditions are required in order to complete this procedure:
-The Concentrator and Decoder must be added to the NetWitness Server using trusted connections.
-The NW Server version must be 10.5 or later.
-The Core services must be 10.5 or later.
-Aggregation must use Aggregators accounts on all Core services.

Configure Meta and Content Restrictions on Brokers, Concentrators, and Decoders

To restrict the meta and raw content that users can view, you must enable SDK system roles to allow more granular controls by configuring meta and content restrictions on each service in the Services Security view.

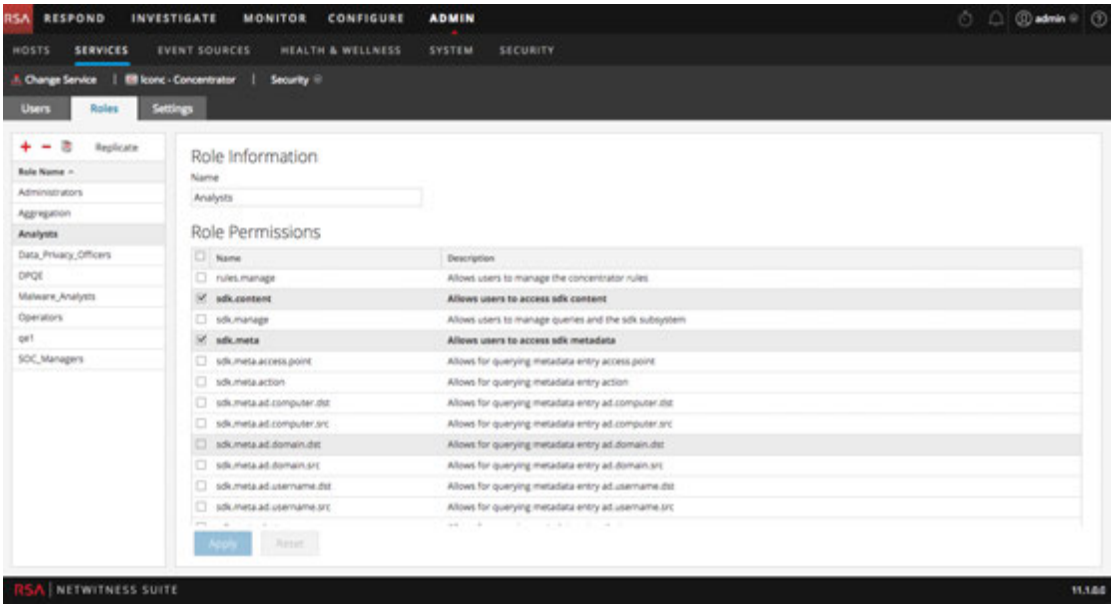
1. In the **Admin Services** view, select a service and then click **> View > Security**.
2. Click the **Settings** tab.



3. In the **SDK Meta Role Permissions** field, select **Blacklist meta and content**. Click **Apply**.

   This allows the administrator to blacklist individual meta keys so that only the data privacy officer can see the meta keys and content. New roles per meta key are added to the Roles tab.

4. Click the **Roles** tab and select a role, for example **Analysts**.



5. In the **Roles** tab,

   a. Select the meta keys that you do not want analysts to see, for example, select `sdk.meta.username` and `sdk.meta.ip.src`.
   This restricts the analyst from seeing the privacy-sensitive meta keys `username` and `ip.src` as well as any content for any session that contains that meta within it.

   b. Ensure that `sdk.packets` is selected.
   If it is de-selected, analysts lose the ability to bulk export raw packets and logs. In RSA Security Analytics 10.6, Role-Based Access Control (RBAC) for the `/sdk packets` command was either on or off, per user. Restricted users usually had access removed, so pcap generation from Investigate was not allowed even for sessions that did not have restrictions. In RSA NetWitness Suite 11.0 and above, RBAC just works for packets. Sessions that are restricted will just be skipped during pcap generation in Investigate. Sessions that are allowed will have packets returned. For more information on RBAC, see the *System Security and User Management Guide*.

   c. Click **Apply**.

6. In the Roles tab, ensure that the `Data_Privacy_Officers` role has no sdk.meta.values selected. Click **Apply**.

   A DPO can view any meta and any session.

   In the Roles tab, ensure that the `Aggregation` role has the following permissions: select `aggregate`, `sdk.content`, `sdk.meta`, and `sdk.packets`.

Add Data Privacy Officer and Analyst Accounts on the NetWitness Server

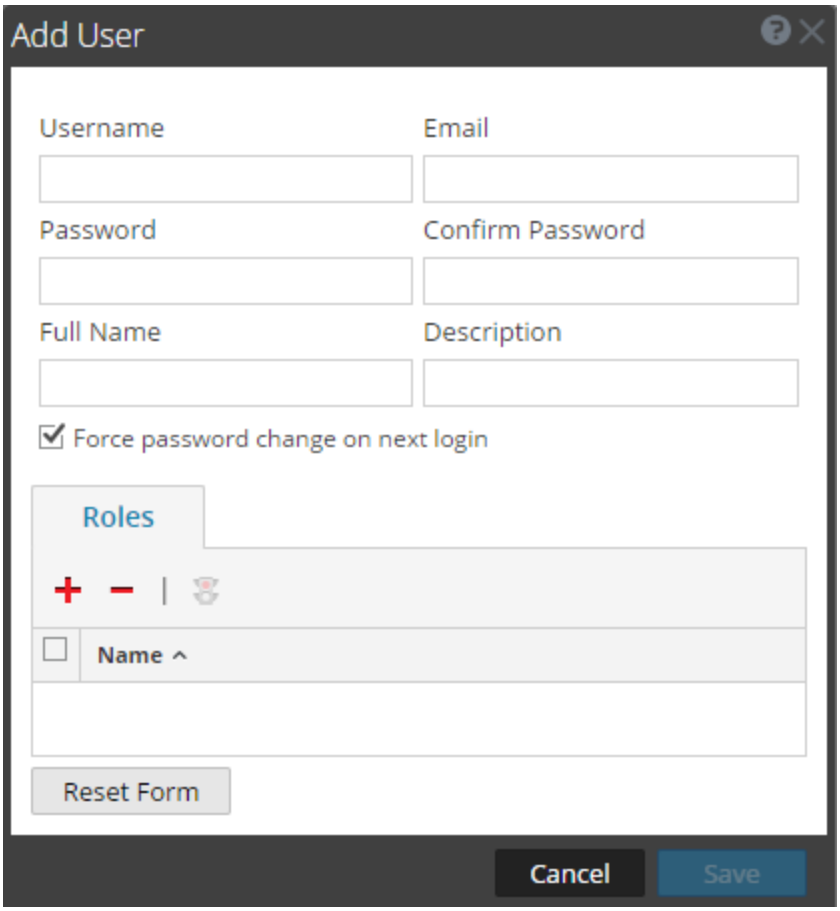
You must add two new user accounts in NetWitness Suite at the system level to depict a privileged data privacy officer and a typical analyst. If the environment is configured using the default trusted connections, you do not need to create the new user accounts on the Core services (Brokers, Concentrators, and Decoders). When a user is created in the NetWitness Server, that user can log on to the services.

Note: The role name is required to exist on both the server and the services, and the role name must be identical. If you create a new custom role on the NetWitness Server, make sure to add it to all Core services as well.

1. Create a new user account for the data privacy officer:

   a. In the **Services Security** view, select the **Users** tab. In the **Users** tab toolbar, click +.

   The Add User dialog is displayed.



b. Create the new account with the following credentials.

   Username = <new user name for logon, for example, DPOadmin>
   Email = <new user's email, for example, DPOadmin@rsa.com>
   Password = <new user's password for logging on, for example, RSAprivacy1!@>
   Full Name = <new user's full name, for example, DPO Administrator>

c. Click the Roles tab, +, and select the `Data_Privacy_Officers` role for the new user.

d. Select **Save**.

2. Create a new user account for the analyst with limited privileges:

   a. In the **Services Security** view, select the **Users** tab. In the **Users** tab toolbar, click +.

      The Add User dialog is displayed.

   b. Create the new account with the following credentials:

      Username = <new user name for logon, for example, NonprivAnalyst>
      Email = <new user's email, for example, NonprivAnalyst@rsa.com>
      Password = <new user's password for logging on, for example, RSAprivacy2!@>
      Full Name = <new user's full name, for example, Nonprivileged Analyst>

c. Click the Roles tab, +, and select the `Analysts` role for the new user.

d. Select **Save**.

Configure Obfuscated Data on Decoders and Concentrators

This procedure creates the obfuscated values to provide to users who do not have access to the original values.

1. Configure a salt so that the obfuscated value becomes unique. Different companies may have analysts of the same first name and potentially the same login username, and using a salt limits the possibility of someone outside your organization determining your obfuscation mechanism. In this example, you use a simple salt and SHA-256, but the salt is configurable and the hash algorithm can be changed. For additional information, see Configure Data Obfuscation.

   a. To define the salt and hash algorithm, select the **ADMIN > Services** view.

   b. Select a **Decoder** in the **Admin Services** view and click > **View > Config**.

   c. Click the **Data Privacy** tab, and select hash algorithm (SHA-256). In the Salt field, type a hash, for example, **rsasecurity** and click **Apply**.

2. Define the transforms, including the hash format, between the original meta key and obfuscated meta key on the Decoder. The default hash format is binary, but the recommended configuration calls for using the text/string format.

   a. Click the **Files** tab, and in the drop-down menu select **index-decoder-custom.xml.** (You can apply this same configuration to the Log Decoder in the index-logdecoder-custom.xml file.)

   b. Enter the following lines in the available input area:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key name="username" description="Username" format="Text"
protected="true"><transform
destination="username.hash"/></key>
<key name="username.hash" description="Username Hash"
format="Text"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" protected="true"><transform
destination="ip.src.hash"/></key>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text"/>
</language>
```

c. To restart the Decoder service, in the toolbar, select **System** in the **View** drop-down menu (currently labeled Config). In the Services System view, select **Shutdown Service**. The service should automatically restart.

3. Define the meta keys on the Concentrator in the index-concentrator-custom.xml file:

a. Click the **Files** tab, and in the drop-down menu select **index-concentrator-custom.xml**

b. Enter the following lines in the available input area:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexValues" defaultAction="Auto">
<key name="username" description="Username" format="Text"
level="IndexValues" protected="true"/>
<key name="username.hash" description="Username Hash"
format="Text" level="IndexValues" token="true"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" level="IndexValues" protected="true"/>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text" level="IndexValues" token="true"/>
</language>
```

c. To restart the Concentrator service, in the toolbar, select **System** in the **View** drop-down menu (currently labeled Config). In the Services System view, select **Shutdown Service**. The service should automatically restart.

Configure Data Retention on Concentrators and Decoders

Data retention configuration ensures that the data residing in the NetWitness Suite Core components is deleted after a certain time. Configuring data retention on Concentrators and Decoders is not required for all environments, but it may be necessary to be in compliance with applicable laws and regulations. It is important to evaluate an appropriate retention period for your environment. The Data Retention Scheduler settings that you set apply to ALL data on a Concentrator or Decoder.

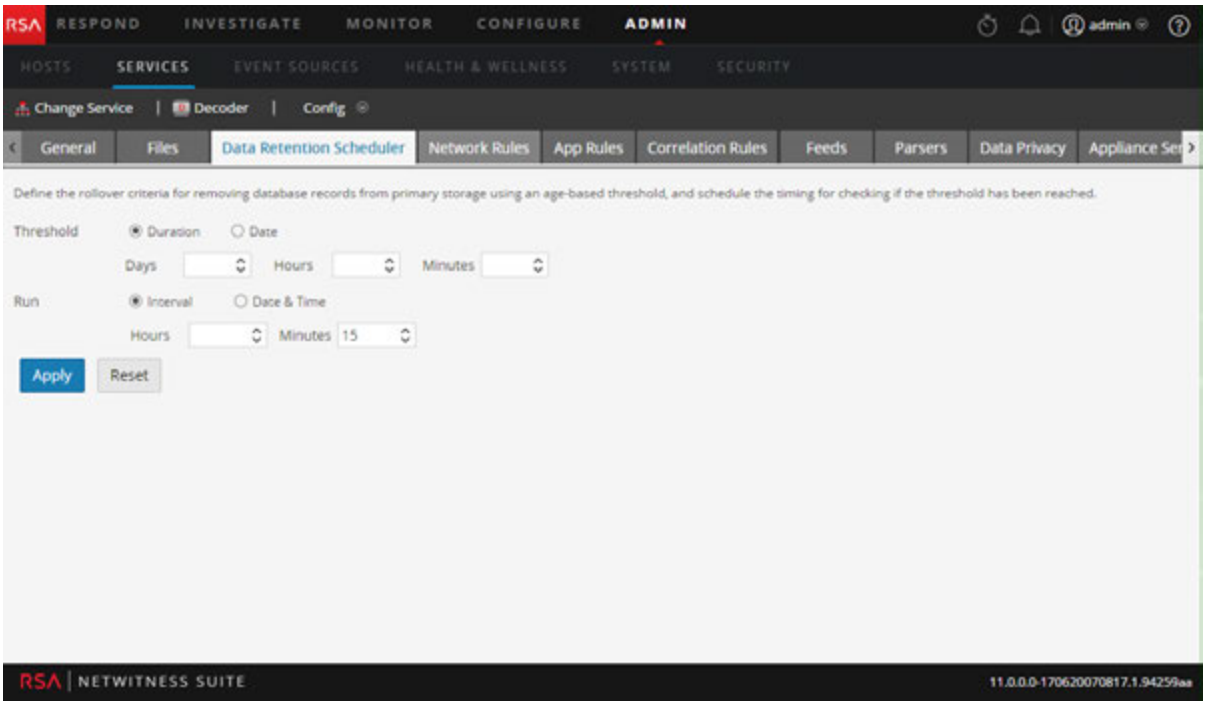
In the following example, NetWitness Suite is configured to execute a check every 15 minutes to determine if the duration threshold has been met. If the threshold is met, NetWitness Suite deletes data older than 90 days in the relevant databases.

Caution: The 90 day retention period is just an example. Adjust your rollover criteria depending on the location of the data and the applicable laws. In a strict data privacy environment, such as in Europe where laws require that Personally Identifiable Information (PII) not be saved or removed frequently, you may need to adjust the time.

This procedure is optional. If you do not set a time retention limit, the system automatically deletes the oldest data when the hard drive space is full.

(Optional) For each Concentrator and Decoder:

1. Navigate to the **Services Config** view > **Data Retention Scheduler** tab.



2. Define the data retention period. For example, set the **Threshold** to **Duration**, and in the **Days** field, type **90**.
3. Define how often the scheduler checks to see if the threshold has been met. For example, set the runtime to **Interval** and in the **Minutes** field, select **15**.
4. To save the configuration, click **Apply**.

Validate Data Privacy Protection

At this point, users have been added with roles that have permissions around specific types of meta data. The next step is to make sure the restricted user (the analyst) cannot view what the unrestricted user (the DPO) can. Also you need to ensure that the data retention configuration is limiting how long data is kept on the systems.

1. View role-based obfuscation in action:
   a. Log on as the unrestricted user (DPOadmin) and make sure this user can see all the data including the protected sensitive data `username` and `ip.src` along with any session that contains that meta.
   b. Log off and the back on as the DPO user.

c. For each Decoder and Log Decoder, import a PCAP or logfile into the Services System view. Use the **Upload Packet File** option to upload a PCAP file that contains `username` and `ip.src` meta data.

d. When the import is complete, look at the meta data in the **Investigation > Navigate** view, choosing the Concentrator connected to the Decoder to which the data was just imported.

e. Scroll down to make sure the `username` and `ip.src` meta keys and corresponding values are visible.

f. Click one of the green numbers next to a `username` or `ip.src` value and verify that the session loads in the Events view.

g. Make a note of the session ID to check when logging on as the restricted user.

h. Log off and log on as the restricted user (NonprivAnalyst).

i. Repeat steps c through f to verify that the user cannot see any `username` or `ip.src` meta or sessions with that meta including the one previously mentioned.

j. To jump to a specific session navigate to the **Investigation > Navigate** view. in the **Actions** menu, select **Go to Event** and enter the session ID.

2. Validate that the data retained in the database falls within the retention time configured in the Data Retention Scheduler.

a. Log off and log on as the unrestricted user (DPOadmin).

b. On the Concentrator, navigate to the **Services > Explore** view.

c. In the node tree, select the **database** node and then **stats**.

d. Observe the `meta.oldest.file.time` value and verify that this is not older then the threshold put on the data retention scheduler.

e. Change the service to the Decoder and repeat steps b through d, check for `stats meta.oldest.file.time` and `packet.oldest.file.time`.

In-Depth Procedures

This topic is a collection of procedures that a Data Privacy Officer uses to implement a data privacy plan for the NetWitness Suite network. These procedures are part of an overall configuration, and are performed as needed to implement the data privacy plan and manage the flow of information in the network.

- Configure Data Obfuscation
- Configure Data Retention
- Configure User Accounts for Use in Data Privacy

Configure Data Obfuscation

This topic provides the procedures for configuring data obfuscation in NetWitness Suite. In a single deployment, all Core service configurations for a data privacy solution must be the same; be sure to use the same hash and salt across all Decoders and Log Decoders.

Note: In order for data obfuscation to work, user accounts need to be configured as described in Configure User Accounts for Use in Data Privacy.

Configure the Decoder Hash Algorithm and Salt

Value hashing accomplished as part of the data privacy solution occurs at the time of meta key creation on the Decoder and Log Decoder. Both services have default settings for use with all meta keys whose values are transformed without a specified hash algorithm type or salt value. The initial NetWitness Suite values for defaults are: hash algorithm (SHA-256) and salt (none).

Note: NetWitness Suite 10.4 and below supports the use of the SHA-1 hash algorithm for backwards compatibility. RSA does not recommend the use of the SHA-1 algorithm and it is not available in NetWitness Suite 10.5 and above.

If you want to change the default settings, you can edit them in the Services Config view > Data Privacy tab or in the following nodes in the NetWitness Suite Services Explorer view:

- `/decoder/parsers/transforms/default.type`

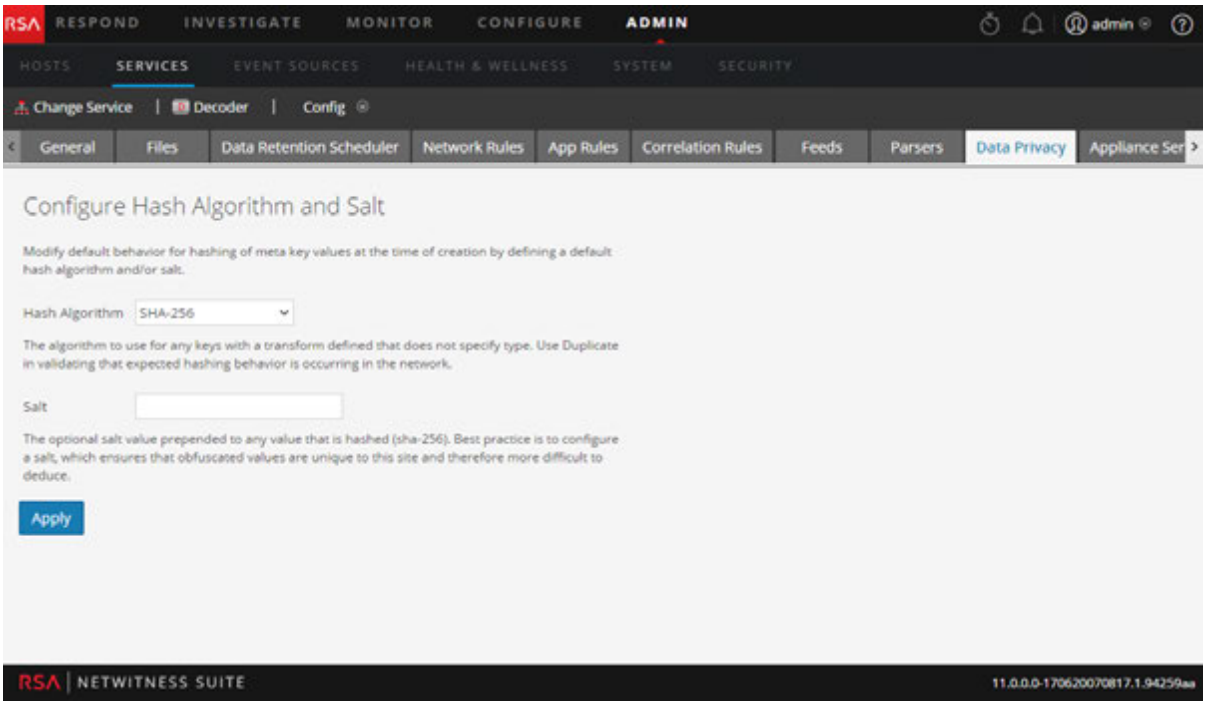
  The algorithm to use for any keys with a transform defined that does not specify `type`. The supported algorithms are: `duplicate` and `sha-256`.

- `/decoder/parsers/transforms/default.salt`

  The salt value prepended to any value that is hashed (`sha-256`). This value is optional, an empty salt is valid and produces an unsalted hash. The salt is not defined by default so that you can create a unique salt for your environment. In general, the longer and more complex the salt, the better the security. A salt of up to 60 characters can be used without any major impact. A salt of at least 16 characters is recommended.

To edit the default hash algorithm and salt:

1. In the **Admin** section, select the **Services** view.
2. In the **Services** grid, select a Decoder or Log Decoder service and click **> View > Config** . Select the **Data Privacy** tab.



3. In the **Configure Hash Algorithm and Salt** section, select a **Hash Algorithm** to use for any meta keys with a defined transform that does not specify type: `sha-256`. (A second algorithm, `duplicate`, is available for administrators to use in validating that expected hashing behavior is occurring in the network.)
4. (Optional) In the **Salt** field, enter a salt value to be prepended to any value that is hashed. This value is optional, an empty salt is valid and produces an unsalted hash. The salt is not defined by default so that you can create a unique salt for your environment. In general, the longer and more complex the salt, the better the security. Best practices for security purposes dictate a salt value that is no less than 100 bits or 16 characters in length. If a unique salt is required for each individual meta key, that needs to be configured in the index file as shown in example 3 below.
5. Click **Apply**.

   The new settings become effective immediately.

Configure Language Keys

In NetWitness Suite 10.5 the NetWitness Suite Core Language had several language key attributes added to facilitate data privacy. You can edit these attributes in the custom index file for each Decoder or Log Decoder. The custom index file (for example, index-decoder-custom.xml) is editable in the Services Configuration view > Files tab. After making changes in the index file, like the ones shown in the examples below, a service restart in a specific sequence is required.

Based on the data privacy requirements for your site, configure individual meta keys to be protected using the following `key` attributes:

- `protected`

  This attribute specifies that NetWitness Suite should consider the values as protected and tightly control any release of the value. When propagating the protected attribute, NetWitness Suite ensures that any downstream trusted system treats the values accordingly. Add this attribute to all services that create the protected values (that is, Decoder or Log Decoder) and any services that will provide trusted access (software development kit (SDK) query/values, aggregation) outside of Core services. The exception to this rule is that a Broker with no index file specified does not need to have the attribute added.

- `token`

  This attribute specifies that values for this key are stand-ins for another value and may not be visually interesting. The `token` attribute is informational, primarily for UI elements to display the value in a more useful or visually pleasing format.

- `transform`

  This child element of `key` indicates that any values for a given meta key should be transformed and the resulting value persisted in another meta key. The `transform` element is only required on Decoders and Log Decoders and is informational if specified on any other Core services. The `transform` element has the following attributes and children:

Name	Type	Description	Optional or Required
`destination`	attribute	Specifies the key name where the transformed value will be persisted.	required
`type`	attribute	The transform algorithm to apply. If not specified, the value of `/decoder/parsers/transforms/default.type` is used.	optional

Name	Type	Description	Optional or Required
param	child-element	A name/value pair, where each param element has a required attribute name and the child text is the value. The only supported param is used to specify a key specific salt value. If not specified, the value of /decoder/parsers/transforms/default.salt is used.	optional

Example 1

On a Decoder or Log Decoder, mark username as protected and hash all values into username.hash with the default algorithm and salt:

```
<key name="username" description="Username" format="Text"
protected="true"><transform destination="username.hash"/></key>
```

Example 2

On a Concentrator, mark username as protected and username.hash as token:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key description="Username" format="Text" level="IndexValues"
name="username" protected="true"/>
<key description="Username Hash" format="Binary" level="IndexValues"
name="username.hash" token="true"/>
</language>
```

Example 3

On a Decoder or Log Decoder, mark username as protected and hash all values into username.bin with the specified algorithm and salt:

```
<key name="username" description="Username" format="Text"
protected="true">
<transform destination="username.bin" type="sha-256">
<param name="salt">0000</param>
</transform></key>
```

Configure Metadata and Content Visibility Per User Role on Core Services

On individual Broker, Concentrator, Decoder, Log Decoder, and Archiver services being viewed in the Services Security view, administrators can configure the visibility of metadata and content based on the user group or role assigned to a user. This is called the SDK meta roles capability, and it is enabled by default.

Note: Administrators who want to configure metadata and content visibility per user must not disable the `sdk.content` permission (in the Roles tab). If the `sdk.content` permission has been disabled in the Roles tab, packets and raw logs are not visible to `system.roles` node. The `system.roles` node handles the filtering using the method configured in the Settings tab.

With `sdk.content` capability enabled, the next step is to select the method of filtering metadata and content in the Settings tab. Selecting a blacklist or whitelist option makes additional permissions for specific meta keys available in the Roles tab. The result is that administrators can choose a user role, such as analyst, in the Roles tab and select specific meta keys (and content) to be blacklisted or whitelisted for that user group. The permissions apply to any user in the user group.

The following table lists the options for filtering in the Settings tab and the numeric values used to disable (0) and the types of filtering (1 through 6). There is no need to know the numeric value unless configuring metadata and content visibility manually in the `system.roles` node.

system.roles Node Value	Settings Tab Option	Event Metadata	Original Event
0	**No Filtering.** System roles that define permissions on a per meta key basis are disabled.	Visible	Visible
1	**Whitelist meta and content.** By default no meta keys and no packets are visible. Selecting individual SDK meta roles per user group allows users to see metadata and packets for that SDK meta role.	Not Visible Select to Show	Not Visible Select to Show

system.roles Node Value	Settings Tab Option	Event Metadata	Original Event
2	**Whitelist only meta.** By default packets are shown, but no metadata is visible. Selecting individual SDK meta roles per user group allow users to see metadata for that role.	Not Visible Select to Show	Visible
3	**Whitelist only content.** By default metadata is visible, but no packets are visible. Selecting individual SDK meta roles per user group allow users to see packets for that role.	Visible	Not Visible Select to Show
4	**Blacklist meta and content.** By default all metadata and all packets are visible. Selecting individual SDK meta roles per user group prevents users from seeing metadata and packets for that role.	Visible Select to Hide	Visible Select to Hide
5	**Blacklist only meta.** By default all metadata and all packets are visible. Selecting individual SDK meta roles per user group prevents users from seeing metadata for that role.	Visible Select to Hide	Visible
6	**Blacklist only content.** By default all metadata and all packets are visible. Selecting individual SDK meta roles per user group prevents users from seeing packets for that role.	Visible	Visible Select to Hide

Three factors determine what a user sees:

- The SDK meta role setting (blacklist or whitelist).
- The restricted meta keys configured for the group to which the user belongs.
- The meta keys in the session being analyzed.

Caution: Be aware that with blacklisting, implicit trust is granted for all except the configured metadata. For a Decoder to have RBAC enabled and use implicit trust, it must only use a blacklist system setting; a whitelist setting will result in some issues with meta keys that are not explicitly enabled and therefore not visible. It is impossible to grant implicit trust under whitelist rules because the universe of meta keys cannot be known. If you want to use whitelisting, a workaround is to turn RBAC off for the Decoder and disable any user accounts from connecting directly to the Decoder if they should be RBACed.

Here's an example of how the SDK meta role configuration meshes with a Group that has restricted meta keys.

Configuration:

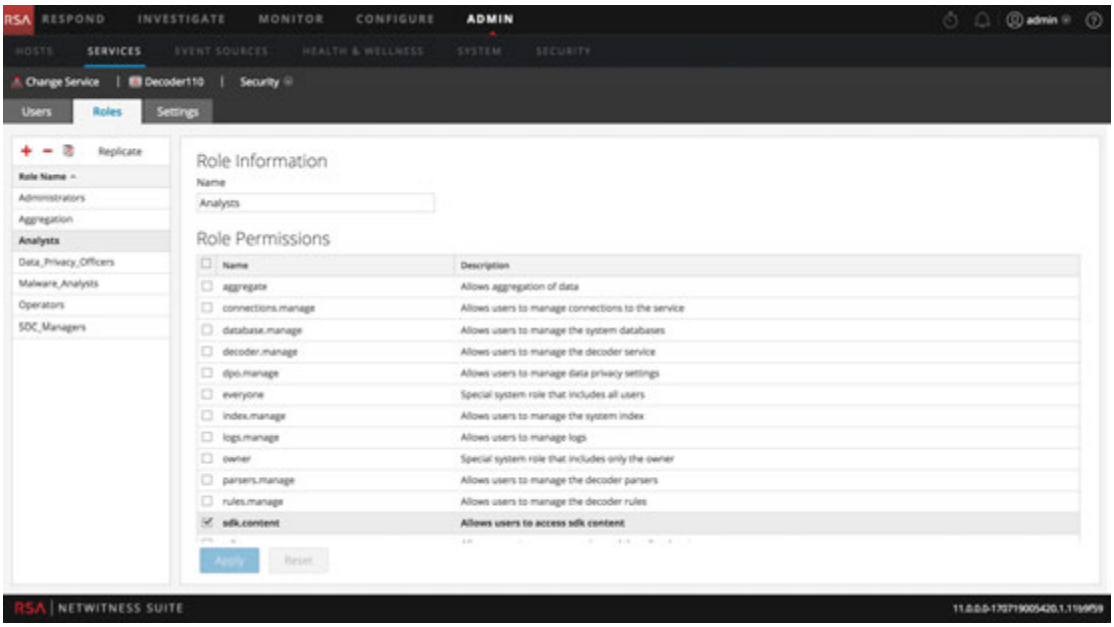
- The SDK meta role setting is **Blacklist meta and content**. With this option implemented, all meta and all content (packets and logs) are visible by default.
- The Administrator has restricted meta keys configured for the Analysts group to prevent viewing of sensitive data (for example, `username`).
- The packets and logs for any session that includes the `username` meta key are not visible to an Analyst.

Result: Now a user who is a member of the Analyst Group investigates a session. Depending on the content of the session, the results are different:

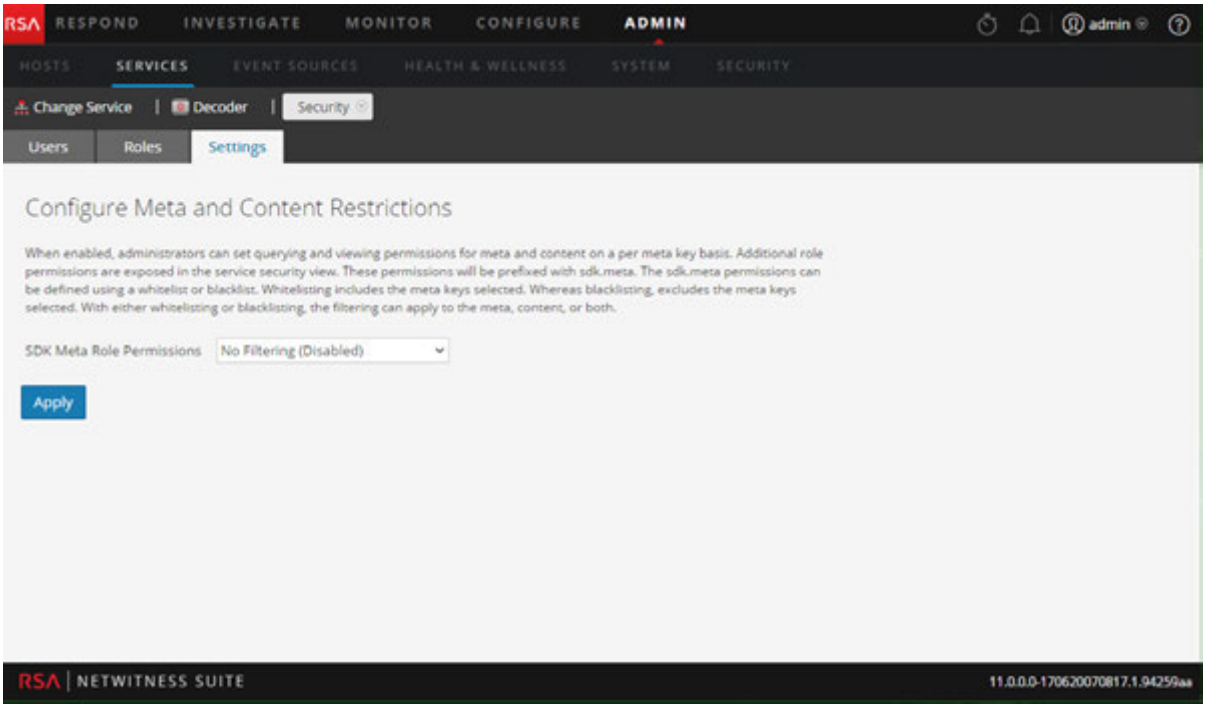
- Session 1 includes the following meta keys: `ip`, `eth`, `host`, and `file`. The session does not include `username` so all packets and logs in the session are displayed.
- Session 2 includes the following meta keys, `ip`, `time`, `size`, `file`, and `username`, Because the session includes `username` , no packets or logs from the session are displayed for the Analyst.

To configure meta and content restrictions for a Decoder or Log Decoder:

1. In the **Admin** view, select **Services**.
2. In the **Services** grid, select a Broker, Concentrator, Decoder, Log Decoder, or Archiver service and click **> View > Security**. Click the **Roles** tab, select a role, and verify the `sdk.content` role is enabled.

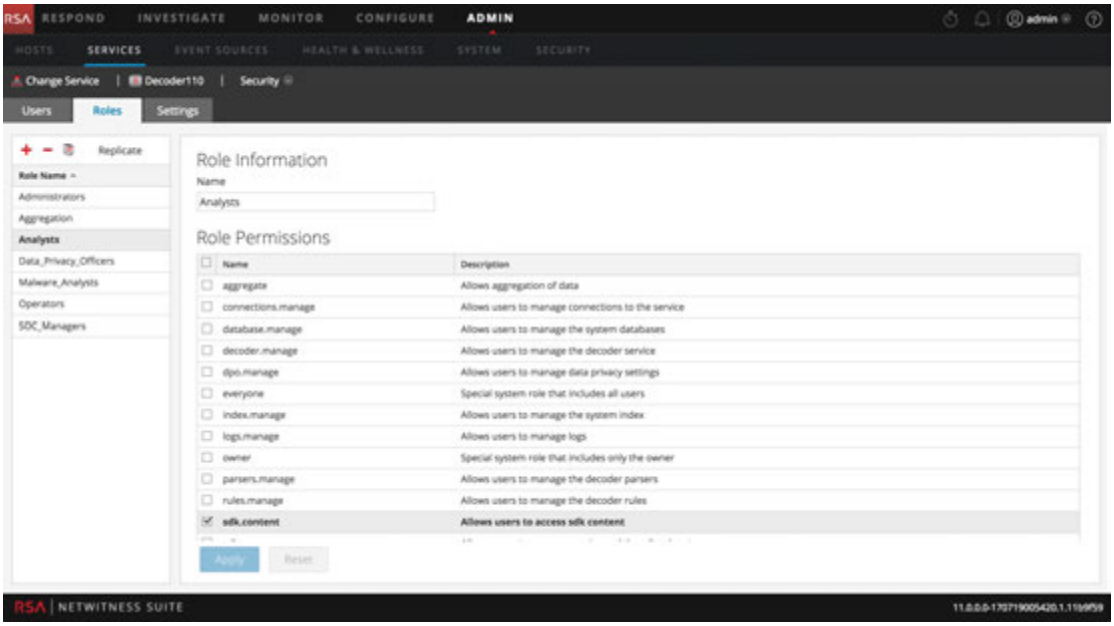


3. Click the **Settings** tab.



4. Select one of the filtering methods (blacklist or whitelist) and content types (meta and content, meta only, or content only), and click **Apply**.
5. Click the **Roles** tab and a role for which you want to allow content (whitelist) or block content (blacklist) as specified in the SDK Meta Role Permissions setting.

The Role Permissions for the selected role are displayed, and the SDK Meta Role Permissions are available for selection, for example, `sdk.meta.action`. If you selected one of the whitelist options in the SDK Role Permissions setting, you must assign each SDK meta role to make the selected content visible to users assigned that SDK meta role. If you selected one of the blacklist options in the SDK Role Permissions setting, selected content will be hidden from users assigned that SDK meta role.



6. Select the SDK meta role permissions for users assigned this role. Click **Apply**.

   The settings become effective immediately and apply to new packets and logs processed by the Decoder or Log Decoder.

Configure Meta Keys Not Written to Disk Per Parser on a Decoder

On a Decoder and Log Decoder, a Data Privacy Officer can configure individual meta keys that are not written to disk. To do so, the DPO specifies the meta keys as transient in the index and the parser configuration.

Note: The same capability was previously available on Log Decoders, and was configured when setting up parsers by modifying the table-map.xml file. Now it is integrated in the Services Config view.

To configure selected meta keys on individual parsers that will not written to disk:

1. In the **Admin** section, select **Services**.
2. In the **Services** grid, select a Decoder or Log Decoder service and > **View** > **Config**.
3. In the **Parsers Configuration** section of the **General** tab, select a parser and then select

Transient in the **Config Value** drop-down list. Access the list by clicking on the configuration value (Enabled, Disabled, or Transient).

The configuration change is marked by a red triangle.

4. Click **Apply**.

   The change is effective immediately. The parser configured as Transient will no longer store meta keys to disk.

Configure Data Retention

A NetWitness Suite user with the role of Administrator can configure NetWitness Suite to ensure that sensitive data has been removed after a specific retention period, regardless of system ingest rate. For instance, the policy might be to keep packets (both raw data and meta data) for no more than 24 hours, and to keep some logs (both raw data and meta data) for up to seven days. If sensitive data makes its way into another database on the Reporting Engine, Malware Analysis, Event Stream Analysis, and NetWitness Servers, data retention can be managed there as well. The administrator needs to set up each service individually across all NetWitness Suite components (except Event Stream Analysis) based on policy and data privacy laws.

Sensitive data may also be in cache.

- Brokers can cache data and this needs to be cleared by configuring an independent rollover and other removal of cache as required. The administrator can configure cache rollover for a Broker by editing the Scheduler file in the Services Config view Files tab.
- Investigation and the NetWitness Server cache data, and this is cleared automatically every 24 hours.
- If the Data Privacy Officer (DPO) exports data, that is the same as saving data on the NetWitness Server in the jobs queue. To clear this data, the administrator or DPO should clean up the jobs queue on a regular basis.

Data Retention

You can schedule a recurring job for Decoder, Log Decoder, and Concentrator services in NetWitness Suite to check if data is ready to be removed. The Data Retention Scheduler provides a means to configure basic scheduling (see below), and advanced Scheduler settings are also available by editing the Scheduler file in the Services Config view Files tab or the node in the Explorer view.

The Archiver has flexible data storage and retention options. You can place different types of log data into individual collections and manage them separately. These collections enable you to specify how much of the total storage space to use and how many days to store the logs in the collection. You can also determine whether to delete the log data or to move it to offline cold storage after it reaches the maximum specified storage space for the collection.

For example, you can put sensitive information in a collection and configure a limitation on how long to keep it, such as 30 days. To delete the data after 30 days, you would not enable warm or cold storage for that collection.

Deleting versus Retaining Log Data

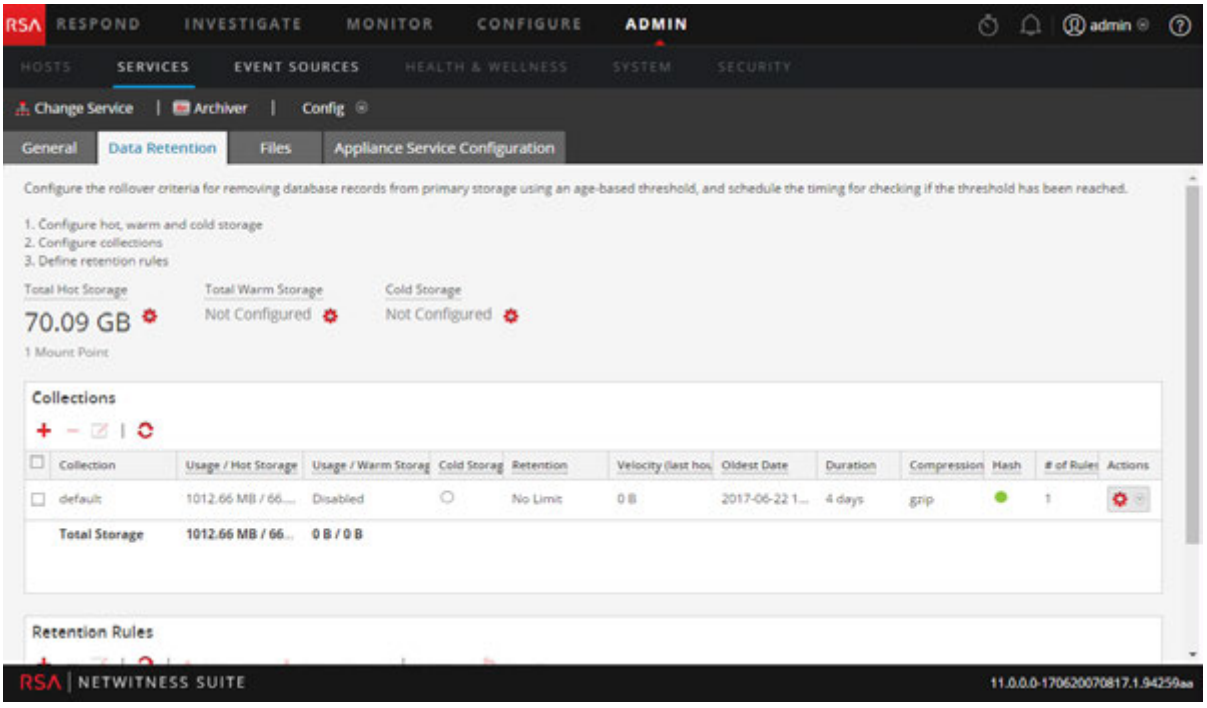
Administrators can configure hot, warm, and cold tiered storage on an Archiver. Cold storage contains the oldest log data that is either required for the operation of the business or mandated by regulatory requirements. When a collection reaches its retention limits for hot and warm storage, NetWitness Suite deletes the log data from hot or warm storage. With cold storage configured, a copy goes into cold storage before the logs are deleted from hot or warm storage. You can choose whether to enable cold storage for each log storage collection. NetWitness Suite does not manage cold storage.

Enable or Disable Cold Storage in a Log Storage Collection

When log data in a collection reaches its retention limits for hot and warm storage, you can delete it or move it to offline (cold) storage.

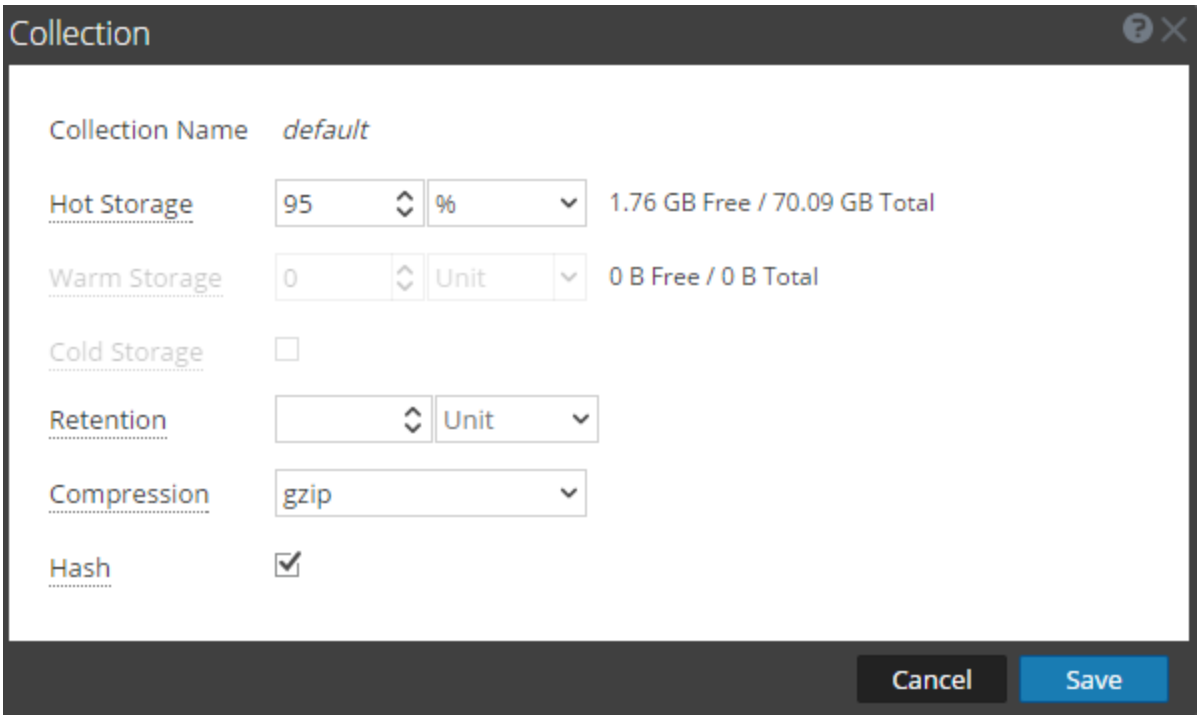
To enable or disable cold storage in a log retention storage collection on an Archiver:

1. In the **Admin** section, select the **Services** view.
2. Select the Archiver service and **> View > Config**.
3. Click the **Data Retention** tab.



4. In the **Collections** section of the Data Retention tab, select a collection and click .

   The Collection dialog is displayed.



Note: If the maximum storage size of the collection does not allow full data retention for the retention period specified, NetWitness Suite deletes the data or it goes to warm or cold storage if specified in the collection.

5. Enable or disable cold storage:
   - To delete log data when the collection reaches its specified retention limits, clear the **Cold Storage** checkbox.
   - To move log data to offline storage when the collection reaches its specified retention limits, select the **Cold Storage** checkbox.
6. Click **Save**.

Configure Log Retention and Storage on an Archiver

To configure log retention and storage on an Archiver, see the **Configure Archiver Storage and Log Retention** topic in the *Archiver Configuration Guide*.

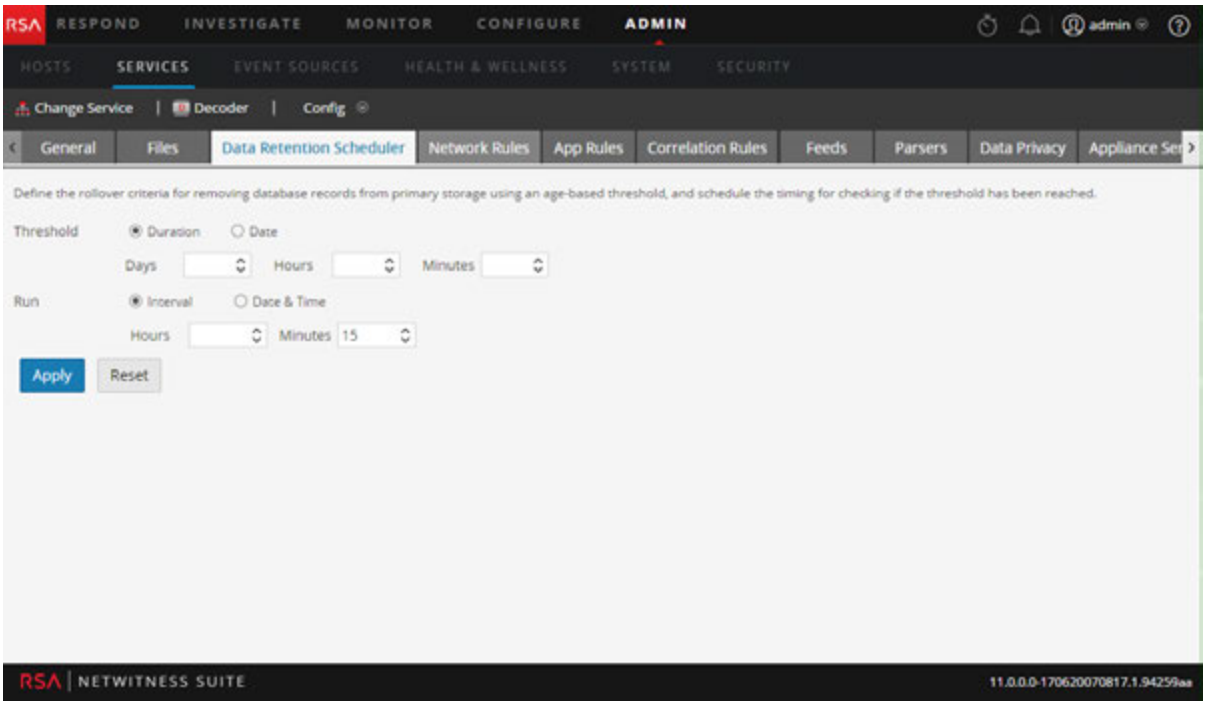
Schedule a Recurring Job to Check Data Retention Thresholds

The data retention scheduler configuration ensures that the data residing in the Decoder, Log Decoder, and Concentrator components is deleted after a certain time. For example, data retention on a Decoder might be configured to execute a check every 15 minutes to determine if the specified duration threshold has been met. If the threshold is met, NetWitness Suite deletes data older then 4 hours in the relevant databases.

Caution: The schedule overwrites any previous schedule and becomes effective immediately. If the retention period is decreased, the data exceeding this retention period is removed.

For a Decoder, Log Decoder, or Concentrator:

1. In the **Admin** section, select the **Services** view.
2. In the **Services** grid, select a Decoder, Log Decoder, or Concentrator service and click **> View > Config**.
3. Click the **Data Retention Scheduler** tab.



4. Set the threshold based on the duration of time the data has been stored or the date on which the data was stored. Do one of the following:
   a. To define the duration of time that data can be stored before removal, select **Duration**, and then specify the number of days (365 maximum), hours (24 maximum), and minutes (60 maximum) that have elapsed since the time stamp on the data.
   b. To define the removal of data based on the date of the timestamp, select **Date**, and then specify the monthly date and time in the Calendar and Time fields.
5. Do one of the following to configure the **schedule for checking rollover criteria**:

a. If you want to set a regular interval at which the scheduled database check occurs, select **Interval** and specify the **Hours** and **Minutes** between the scheduled checks.

b. If you want to set a regular date and time at which the scheduled database check occurs, select **Date and Time** and specify the system clock time in `hh:mm:ss` format for the rollover.

   - To specify the day, select **Every Day**, **Weekdays,** or **Weekends**. The Scheduler defaults to **Every Day**.
   - To specify a different set of days of the week, select **Custom** and click on each day on which the database check occurs.

   Caution: The schedule overwrites any previous schedule and becomes effective immediately. If the retention period is decreased, the data exceeding this retention period is removed.

6. Click **Apply** to complete the configuration.

Configure User Accounts for Use in Data Privacy

This topic provides the procedures for configuring user accounts that work with data obfuscation in NetWitness Suite. In order for data obfuscation to work, accounts and permissions for several types of users must be configured.

- Customize the default `Administrators` system role in NetWitness Suite to remove permissions that should be available only to the Data Privacy Officer.
- Add two new user accounts at the system level to depict a data privacy officer and a typical analyst.
- Add a user account at the service level with the aggregation role so that Decoders and Log Decoders can aggregate data to a Concentrator or Broker.
- On the Reporting Engine, configure two separate service accounts. One service account for general purpose reporting that does not include any sensitive data and the other account for privileged users with access to all data including sensitive data. This procedure is described in the *Reporting Engine Configuration Guide* under **Configure Data Source Permissions**.

Customize the Default Administrators User Role at the Service Level

To separate the data privacy officer and administrator functions on each Decoder and Log Decoder, you need to remove the `dpo.manage` permission from a clone of the Administrators role.

1. In the **Admin Services** view, select a Decoder or Log Decoder. Click **> View > Security**.
2. In the **Services Security** view, click the **Roles** tab, select **Administrators** and click .
   In the **Enter Role Name** dialog, enter a new role name such as Non_DPO_Administrators and click **Save**.
3. Select the new role.
   The Role Information is displayed for editing.
4. Click the box next to **dpo.manage** so that it is no longer checked and click **Apply**.
   The permission to manage data privacy configuration is removed for the new role.
5. In the **Users** tab, select each user who has the **Administrators** role, and change their role to the cloned role.

6. Validate that the users with the modified Administrators role can login as with admin privileges.
7. Validate that the users with the modified Administrators role cannot configure meta and content restrictions in the Settings tab.

Add a User Account with the Aggregation User Role at the Service Level

To ensure that Decoders and Log Decoders can aggregate data to a Concentrator or Broker:

1. In the **Admin Services** view, select a Decoder or Log Decoder. Click **> View > Security**.
2. In the **Users** tab, add a user with the `Aggregation` role and click **Apply**.

Note: The **Aggregation Role** topic in the *Hosts and Services Getting Started Guide* provides details about the application of this user role.

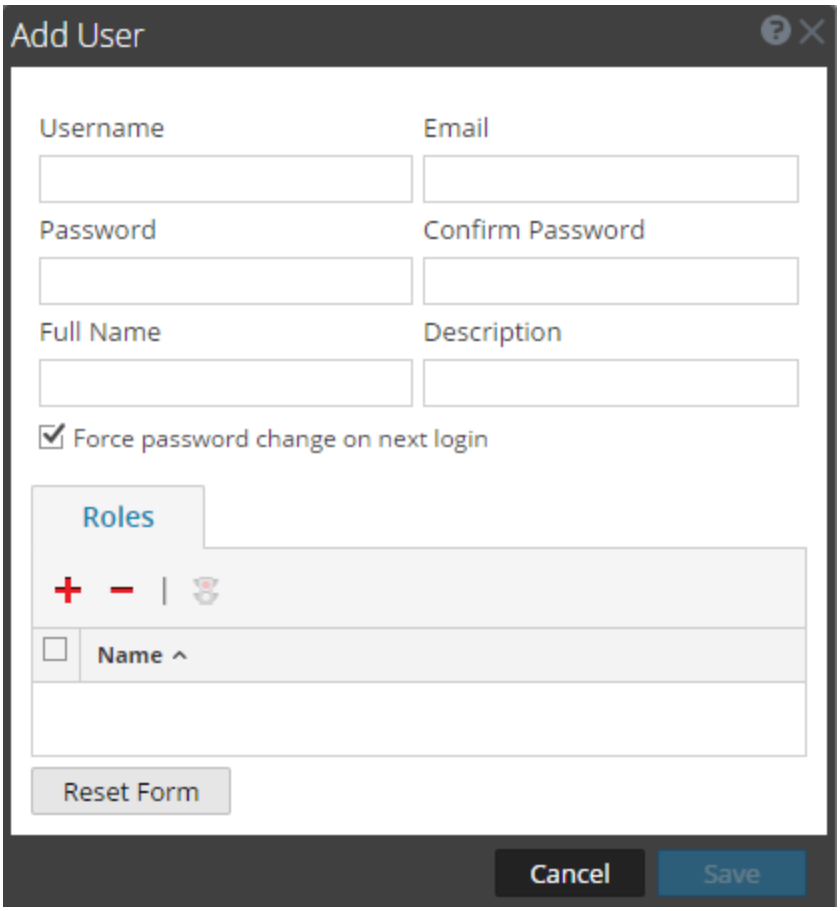
Add Data Privacy Officer and Analyst Accounts on the NetWitness Server

You need to add two new user accounts in NetWitness Suite at the system level to depict a privileged data privacy officer and a typical analyst. If the environment is configured using the default trusted connections, you do not need to create the new user accounts on the Core services (Brokers, Concentrators, and Decoders). When a user is created in the NetWitness Server, that user can log on to the services.

Note: The role name is required to exist on both the server and the services, and the role name must be identical. If you create a new custom role on the NetWitness Server, make sure to add it to all Core services as well.

1. Create a new user account for the data privacy officer:
   a. In the **Security** view, select the **Users** tab and click **+**.

      The Add User dialog is displayed.



b. Create the new account with the following credentials.

   Username = <new user name for logon, for example, DPOadmin>
   Email = <new user's email, for example, DPOadmin@rsa.com>
   Password = <new user's password for logging on, for example, RSAprivacy!@>
   Full Name = <new user's full name, for example, DPO Administrator>

c. In the **Roles and Attributes** section, click the **Roles** tab, +, and select the `Data_Privacy_Officers` role for the new user.

d. Select **Save**.

2. Create a new user account for the analyst with limited privileges:

   a. In the **Admin > Security** view, click the **Users** tab. In the **Users** tab toolbar, click +.

      The Add User dialog is displayed.

   b. Create the new account with the following credentials:

      Username = <new user name for logon, for example, NonprivAnalyst>
      Email = <new user's email, for example, NonprivAnalyst@rsa.com>
      Password = <new user's password for logging on, for example, RSAprivacy!@>
      Full Name = <new user's full name, for example, Nonprivileged Analyst>

c. In the **Roles and Attributes** section, click the **Roles** tab, +, and select the `Analysts` role for the new user.

d. Select **Save**.

Data Privacy References

The following reference materials are available for management of data privacy and data retention. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

- See the **Data Privacy Tab** topic in the *Decoder and Log Decoder Configuration Guide*.
- See the **Data Retention Tab - Archiver** topic in the *Archiver Configuration Guide*.
- See the **Data Retention Scheduler Tab** topic in the *Hosts and Services Getting Started Guide*.

RSA NETWITNESS® SUITE

Licensing Management Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

February 2018

Contents

How Licensing Works **6**

Choosing a License Type 6

Metered Licensing 7

Service-based Licensing 7

Out-of-the-Box Trial Licensing 8

Licensing at a Glance 8

Service-based 8

Metered 9

Perpetual 9

Subscription 9

Licensing Measurement 9

Out-of-Compliance Banner 10

Initial Set Up **11**

Prerequisites 11

Step 1. Register the NetWitness Server **12**

Prerequisites 12

Verify That the License Server is Installed and Running 12

Register the Server 13

Register Online 13

Register Using an Offline Capability Request 15

Map Entitlements 17

What Happens if No License is Installed 19

Step 2. Synchronize NetWitness Server **21**

Prerequisites 21

Verify That the Server Has a DNS 21

Synchronize with Download Central 21

Synchronize Automatically (Online) 21

Refresh Licenses 21

Synchronize Offline 22

Step 3: Install Product Licenses from Download Central (DLC) 25

Additional Procedures 31

Configure NetWitness Suite Notifications 32

Dismiss Out-of-Compliance Banner 34

Export Usage Stats and View Decoder Usage Stats 35

Examine Decoder Service Usage Statistics in the Explore View 36

Synchronize Local Licensing Server Offline 37

Prerequisites 37

Download a Capability Request for Submission to Download Central 37

Upload an Offline Capability Response to NetWitness Suite 38

View Current Entitlements 40

Prerequisites 40

View Current License Status 40

View and Manage License Pools on LLS 42

View Available Entitlements 42

References 43

Entitlement Capability Implementation 44

Licensing Panel 46

Metered Licenses Tab 49

Out-of-Compliance Banners 52

Out-of-Compliance State 53

License Approaching Out-of-Compliance 55

Overview Tab 56

Export Usage Statistics 58

Service-Based Licenses Tab 60

Settings Tab 63

Troubleshoot Licensing 66

Simple Error Notification about a Problem with a License 66

Common Log and Configuration Files 66
NetWitness Server Problems 66
Start Date Issue 68
License Usage Stats Issues 69
Download Central (DLC) Issues 70
Wrong License Mapping Issues 71

How Licensing Works

RSA NetWitness Suite version 11.0 entitlement uses a trust-based licensing model. Appliances continue to function even if they are out-of-compliance with current licensing.

Configuration Step	Description
Step 1. Register the NetWitness Server	Before you begin the licensing process, you must ensure that your license server is installed and running.
Step 2. Synchronize NetWitness Server	Your NetWitness Server must be registered to Download Central and entitlements must be mapped. There are two methods of synchronizing NetWitness Suite with Download Central: online and offline.
Step 3: Install Product Licenses from Download Central (DLC)	Your DLC Welcome e-mail message contains system log in instructions to Download Central. Instructions for downloading your product licenses can be found in this document, as well as the Download Central (DLC) website.

Choosing a License Type

The type of license you choose is based on your network requirements. If you want a license that is based on a throughput per day of logs (SIEM) or network packets (Network Monitoring and Network Malware), Metered licensing is your best bet.

The following types of licenses are available in RSA NetWitness Suite 11.0:

- Metered Licensing
- Service-based Licensing
- Out-of-the-box Trial Licensing

Note: You should purchase or install a license within 90 days, although the functionality will continue after the 90-day out-of-the-box trial period ends.

Metered Licensing

Metered licensing is based on a throughput per day of logs (SIEM) or network packets (Network Monitoring and Network Malware), combined with the separate purchase of the hardware needed to deploy the system and meet customers' retention requirements.

The throughput per day for logs is measured in Gigabytes per day and in Terabytes per day for packets. Customers can then acquire the amount of Gigabytes per day of logs, or Terabytes per day of packets that they require in order to meet their needs. The total amount of throughput per day is selected from one of five volume tiers of license levels, based on the total amount of throughput per day that is being licensed across the customer's entire enterprise deployment of NetWitness.

With this licensing system, organizations can scope their throughput per day capacity independently from their hardware infrastructure components, optimizing specifically for their network environment. A customer effectively licenses NetWitness software from RSA based on their network or log throughput and then purchases the infrastructure components (servers to deploy the Decoders, Concentrators, Brokers, and so on) that are required for their particular deployment.

Note: If you want to change the default allotment of licenses by moving between metered and service-based, you can do this by selecting under the actions of each license entry, provided there is support for both license types.

Service-based Licensing

RSA NetWitness Suite version 11.0 supports service-based licensing. Support for service-based licensing is applicable for all appliances that require a license. This is a per-service permanent license that has no expiration date. You do not need to activate any version 11.0 services manually.

The following list includes services that can have service-based licenses:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Archiver
- Event Stream Analysis
- Malware Analysis

Note: The one exception is a co-located instance of Malware Analysis, which is licensed by default.

Out-of-the-Box Trial Licensing

Out-of-the-Box Licensing for RSA NetWitness Suite version 11.0 ships with a default Trial out-of-the-box license that enables customers to use the product with full functionality for 90 days. The 90-day time period begins when the NetWitness Suite user interface is configured and used for the first time.

You are given a choice to include appliances under an Out-of-the-Box (OOTB) Trial Metered License, or a Service- based License. Metered licenses are only supported for Decoder, Log Decoder, and Malware Analysis.

Version 11.0 provides the flexibility to move your license to an Out-of-the-Box Trial service-based License. An Out-of-Compliance banner notifies you when you need to take action on your license.

Licensing at a Glance

Note: You are entitled to the latest software version based on your maintenance contract. If your maintenance contract expires, you can still use the product, but you are not covered for maintenance or Technical Support.

Service-based

Service-based licenses are applicable to the following services:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Archiver
- ESA
- Malware Analysis

Metered

- License usage is based on the amount of data throughput per day.
- Only applies to Log Decoder, Packet Decoder, and Malware Analysis (standalone) services.
- Throughput per day is measured in Gigabytes per day for Log Decoders and Packet Decoders, and is measured in Terabytes per day for Malware Analysis.
- Metered license usage statistics are captured hourly and made available in CSV or PDF formats for export.

Perpetual

License is based on aggregate usage, as opposed to a per-appliance service. There is no specified end date; the Metered license works indefinitely

Subscription

License is purchased for a specific period of time, such as 12 months, 24 months, or 36 months. Use of the software is discontinued at the end of your subscription period.

Licensing Measurement

- Usage stats reflect daily average usage.
- Perpetual and service-based licenses, such as Netmon or Network, or Decoder are offered in 1 TB increments
- SIEM or Log Decoder offered in 50 GB increments
- Malware Analysis offered in 1 TB increments on a per-day average usage.
- Contracted daily usage can be exceeded three times in a calendar month. Fourth spike puts the customer in an out-of- compliance state. If you are able to keep your usage within compliance for seven consecutive days until the end of the calendar month, the Out-of-Compliance banner disappears.

  For example, if the fourth spike occurs on November 23, 2017, the Grace Period ends on December 31, 2017 and the Out-of-Compliance banner disappears.
- Breach period starts immediately after Grace Period ends.
- Red banner cannot be dismissed.

Note: Even when the Red banner is displayed, there is no loss of functionality, all NetWitness appliances continue to work with full functionality. All other functionality is included in the license (ESA, storage, and so on).

- Customer pays for hardware.
- Usage is measured as an aggregate of all metered appliances.

  For example, a Decoder can be licensed for 10 GB per day. Customers are allowed to use multiple Decoders under the same license.
- Services are licensed automatically under the following conditions:
  - When services are resolved.
  - When a scheduled task runs every hour.
  - License Refresh is triggered by the user.
- Subscription-based licenses are billed yearly.

Out-of-Compliance Banner

The Out-of-Compliance banner is displayed when one of the following conditions occurs:

- License is tampered with during the out-of-the-box trial period.
- A service is not licensed.
- A license has expired, or is due to expire within the next two weeks.
- Usage exceeds entitled limit.
- Usage is approaching entitled limit.

To resolve an out-of-compliance state:

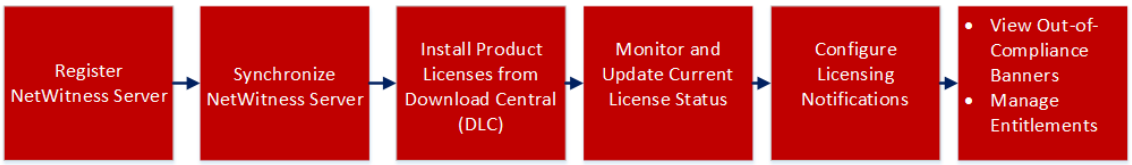
- Reduce usage, or
- Adjust contracted usage amount

Initial Set Up

This topic provides all of the steps required for installing entitlements in NetWitness Suite. The Administrator setting up licensing needs to perform each step in the proper sequence. After initial setup, refer to Troubleshoot Licensing for any maintenance or troubleshooting information.

Workflow

The following workflow illustrates the end-to-end licensing process.



Prerequisites

Before implementing the NetWitness Suite entitlements capability, ensure that the following prerequisites have been met.

- An order for entitlements is in place with RSA, and a pool of entitlements is available for the customer in the RSA Download Central site - https://download.rsasecurity.com/.
- A web browser that supports HTML5 and JavaScript.
- HTTPS access for the NetWitness Suite web Interface.
- The NetWitness Server and all appliances managed by the server must be on the same DLC Account ID or account in the order management system. Licenses on the NetWitness Server can be added only to appliances on the same DLC Account ID or account.
- Administrative access to the NetWitness Server and to other appliances running NetWitness Suite version 11.0.
- Ability of all appliances to communicate with the NetWitness Server so that appliance licenses remain activated.
- If online registration between NetWitness Suite and RSA Download Central is planned:
  - Internet access with HTTP from NetWitness Server to Download Central.
  - NetWitness Server DNS resolution of at least the Download Central site.

Step 1. Register the NetWitness Server

This topic provides instructions for the first step in the NetWitness Suite entitlement process, registering the NetWitness Server and mapping entitlements to the Local License Server (LLS).

Prerequisites

A prerequisite for registering the NetWitness Server to Download Central is to have the License Server installed and running. This is required to tie entitlements to the server.

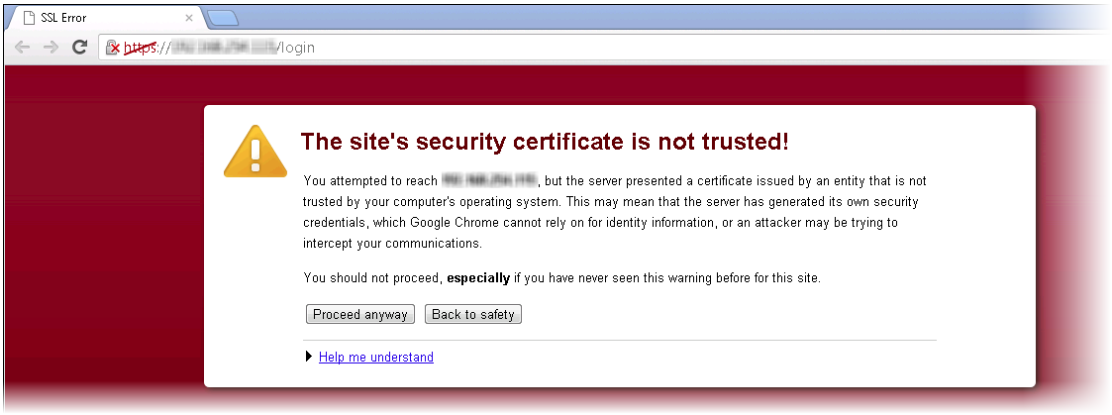
Verify That the License Server is Installed and Running

To verify the License Server is installed and running:

1. Log on to the NetWitness Server at **https://*<NW-IP>***, where ***<NW-IP>*** is the NetWitness Server IP address. You are prompted with a screen asking for your RSA Product License Number. You must enter the Serial Number of your NetWitness Server host in order to continue with the license installation process. This can be found through SSH by issuing the following command:

   dmidecode -s system-serial-number

   The following message may be displayed.



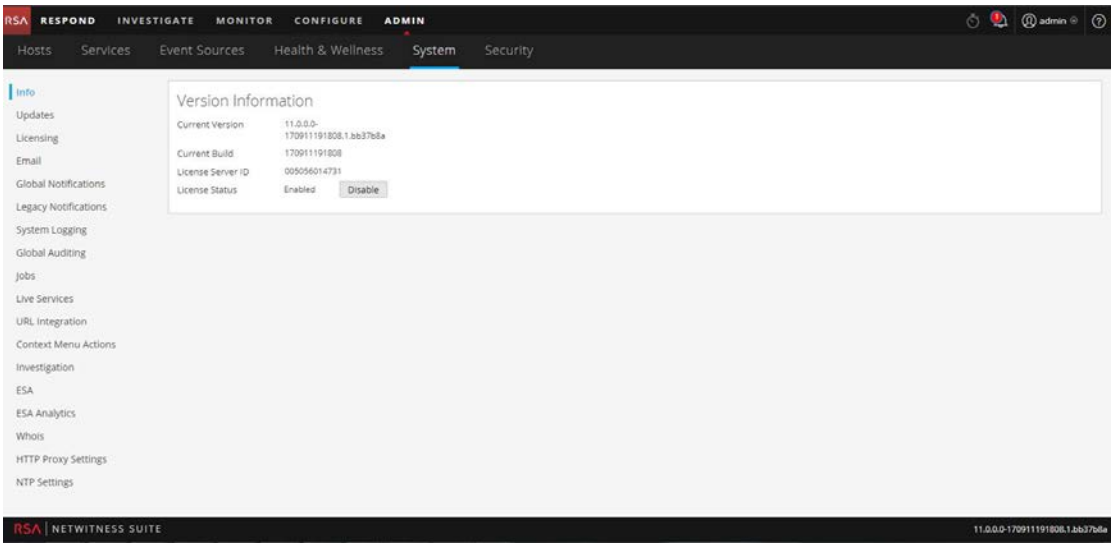
2. If you receive a message that the certificate is not installed, click **Proceed Anyway**. A document describing how to update with a self-signed or CA certificate is available at:

   https://knowledge.rsasecurity.com/scolcms/knowledge.aspx#a58829.

   The NetWitness Suite user interface is displayed.

3. Go to **ADMIN > System**.

4. The Admin System view opens to display the Version Information in the **Info** panel.



5. Under **Version Information**, locate the **License Server ID**.
   - If the field contains a value and the **License Status** is **Enabled**, the Local License Server (LLS) packages are installed and running. You can proceed with server registration.
   - If the field contains a value and the **License Status** is **Disabled**, the Local License Server (LLS) packages are installed but not running. Click **Enable** to enable the LLS before proceeding with server registration.
   - If there is no value for License Server ID, verify that the appropriate LLS packages are installed and running using the following commands:

     ```
     rpm -qa | grep fneserver
     ps aux | grep fneserver
     ```

Register the Server

You can register the server in two ways:

- Register the server online in the Download Central Portal.
- Create an offline capability request in NetWitness Suite and upload the request to the Download Central Portal.

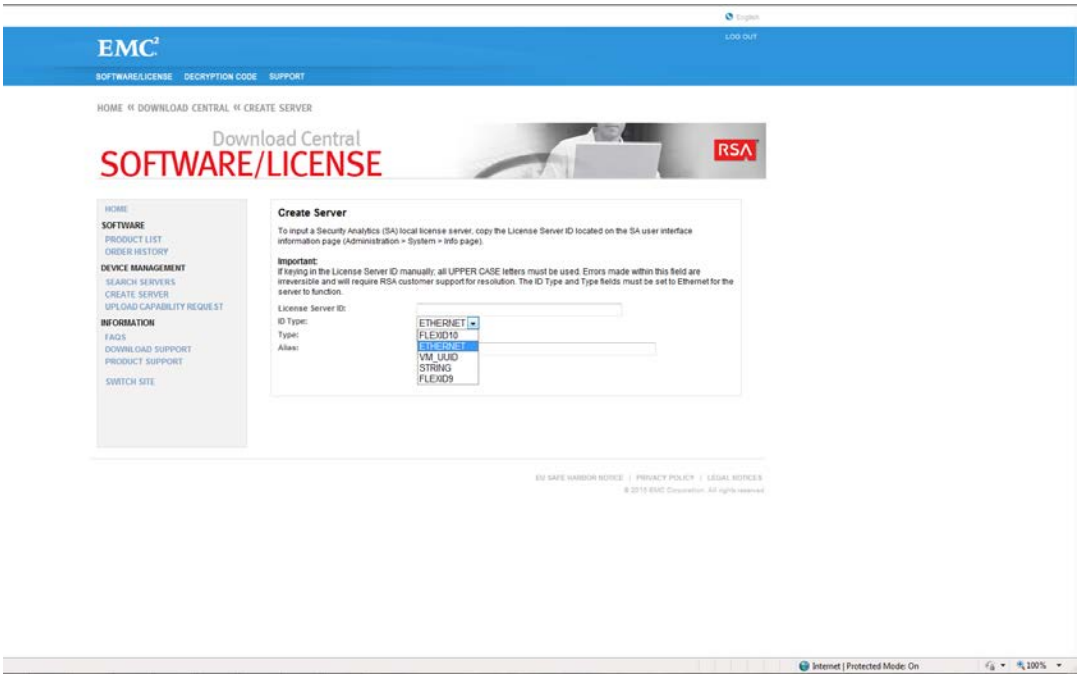
Register Online

To register the License Server ID online:

1. Navigate to the Download Central Portal at https://download.rsasecurity.com/ and log on with your user credentials.

   The **Download Central Menu** is displayed.

2. Do one of the following:
   - If you have already entered a server, under **Management** select **Search Servers** and skip to Step 3.
   - If you have not entered the server information, under **Appliance Management** select **Create Server**.
   - The **Create Server** dialog is displayed.



3. Complete these fields in the dialog:
   - Copy or enter (in uppercase letters) the License Server ID in the License Server ID field.
   - In the **ID Type** drop-down, select **ETHERNET** (the default value).

- In the **Type** drop-down, select **Ethernet** (the default value).
- (Optional) In the **Alias** field, type an alias to your Appliance ID.

4. Click **Create Server**.

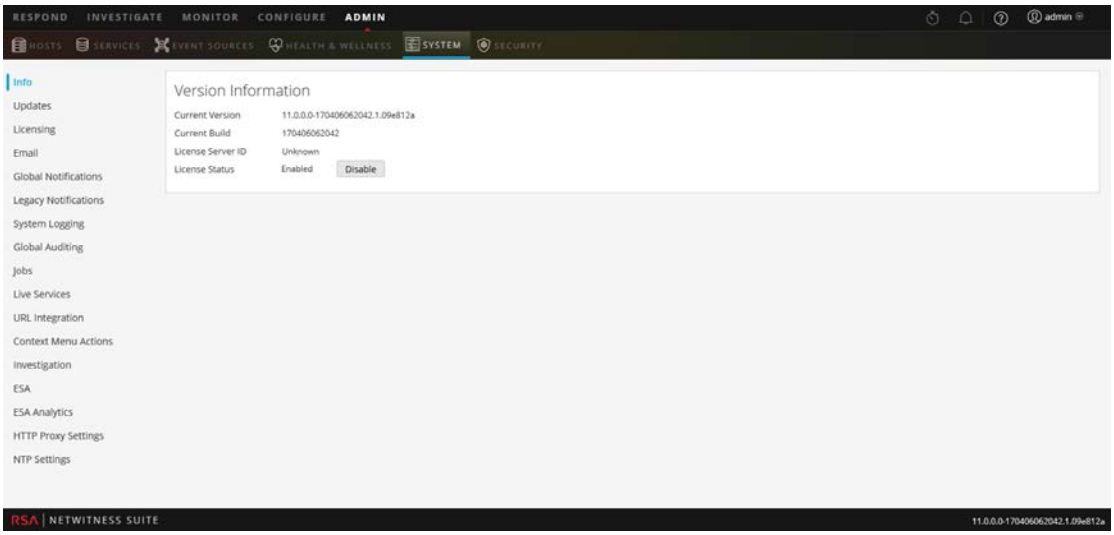
The server is registered and you can now map entitlements as described below.

Register Using an Offline Capability Request

If you do not want to register the NetWitness Server online, you can download an offline capability request in NetWitness Suite and upload that binary request to the Download Central Portal.

To register the server using an offline capability request:

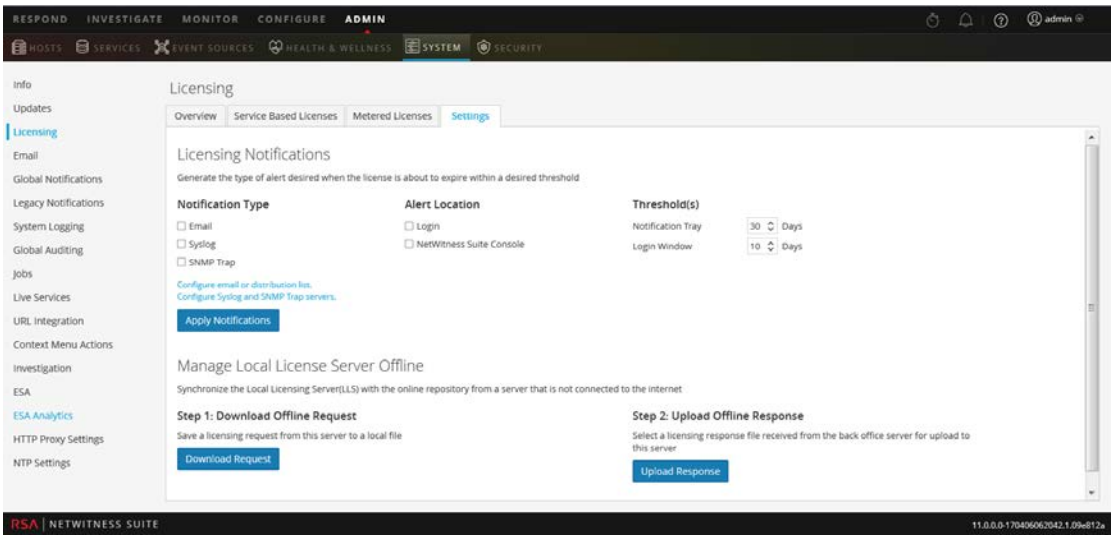
1. Log on to the NetWitness Server at **https://*<NW-IP>***, where ***<NW-IP>*** is the NetWitness Server IP address.
2. Go to **ADMIN > System**.



The Admin System view is displayed.

3. Select the **Settings** tab.

The Licensing panel is displayed.

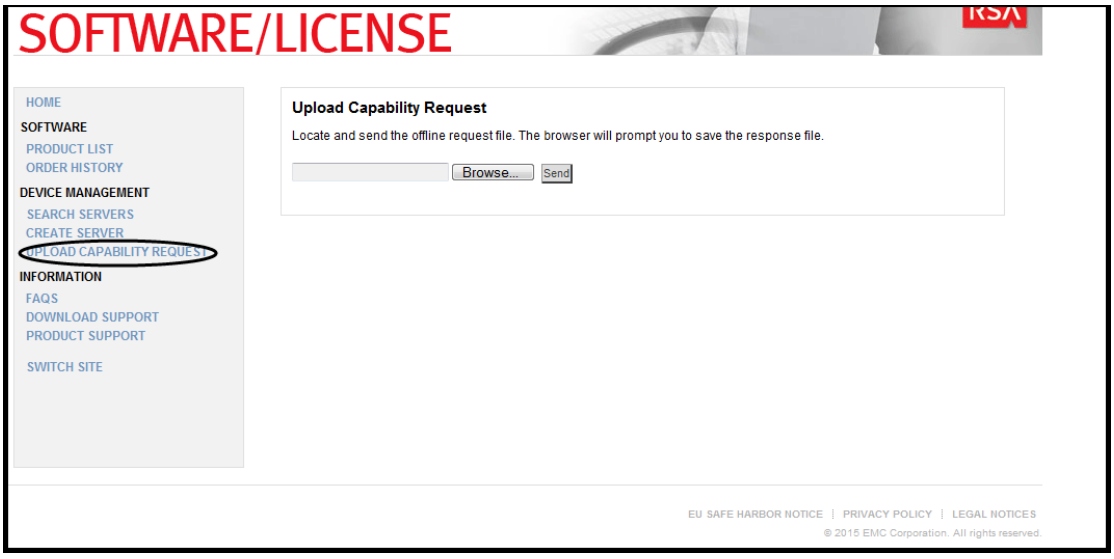


4. In the **Download Offline Request** section, click **Download Request**.
   A file called **OfflineCapabilityRequest.bin** is downloaded to the local system. This file contains current licensing information for the NetWitness Server.
5. Navigate to the Download Central Portal at https://download.rsasecurity.com/ and log on with your user credentials.

   The Download Central menu is displayed.

6. Under **Device Management**, click **Upload Capability Request**.

   The **Upload Capability Request** dialog is displayed.



7. Click **Choose File** and browse the local file system to find the file downloaded from the NetWitness Server. Select **OfflineCapabilityRequest.bin**.

   The filename is displayed next to the **Choose File** button.

8. Click **Send**.

   The server is created in Download Central, and the server information is displayed in the **View Server** dialog. This information includes the data just entered as well as information about any entitlements that have been added to the NetWitness Server. If the server has just been added, there are no entries under **Add-Ons**.

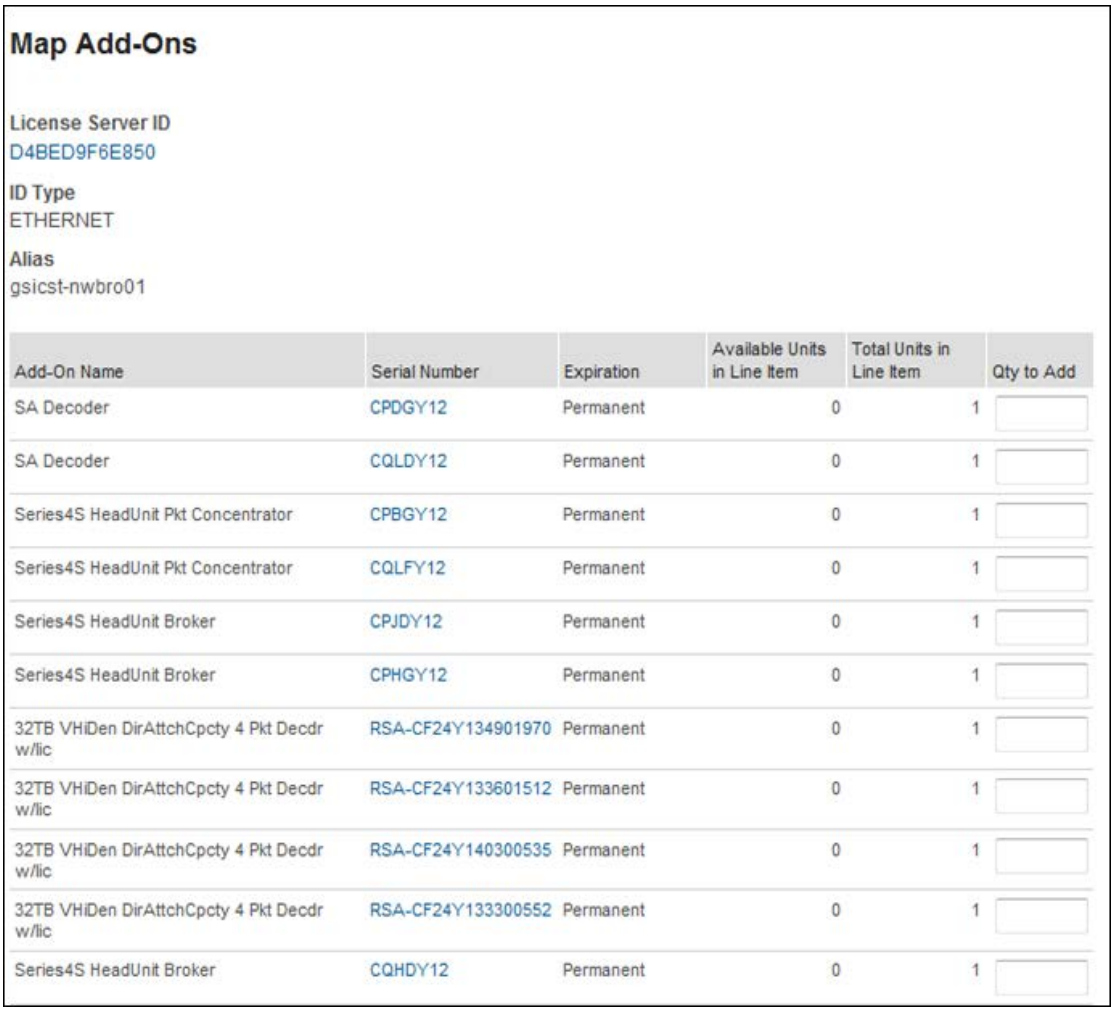
   The server is registered and you can now map entitlements as described below.

Map Entitlements

Mapping entitlements involves choosing the quantity of available licensed appliance entitlements to pull to this NetWitness Server during synchronization. To map appliance entitlements to the server:

1. In the **View Server** page, click **Map Add-Ons**.

   The Map Add-Ons section is displayed.



Map Add-Ons

License Server ID
D4BED9F6E850

ID Type
ETHERNET

Alias
gsicst-nwbro01

Add-On Name	Serial Number	Expiration	Available Units in Line Item	Total Units in Line Item	Qty to Add
SA Decoder	CPDGY12	Permanent	0	1	
SA Decoder	CQLDY12	Permanent	0	1	
Series4S HeadUnit Pkt Concentrator	CPBGY12	Permanent	0	1	
Series4S HeadUnit Pkt Concentrator	CQLFY12	Permanent	0	1	
Series4S HeadUnit Broker	CPJDY12	Permanent	0	1	
Series4S HeadUnit Broker	CPHGY12	Permanent	0	1	
32TB VHiDen DirAttchCpcty 4 Pkt Decdr w/lic	RSA-CF24Y134901970	Permanent	0	1	
32TB VHiDen DirAttchCpcty 4 Pkt Decdr w/lic	RSA-CF24Y133601512	Permanent	0	1	
32TB VHiDen DirAttchCpcty 4 Pkt Decdr w/lic	RSA-CF24Y140300535	Permanent	0	1	
32TB VHiDen DirAttchCpcty 4 Pkt Decdr w/lic	RSA-CF24Y133300552	Permanent	0	1	
Series4S HeadUnit Broker	CQHDY12	Permanent	0	1	

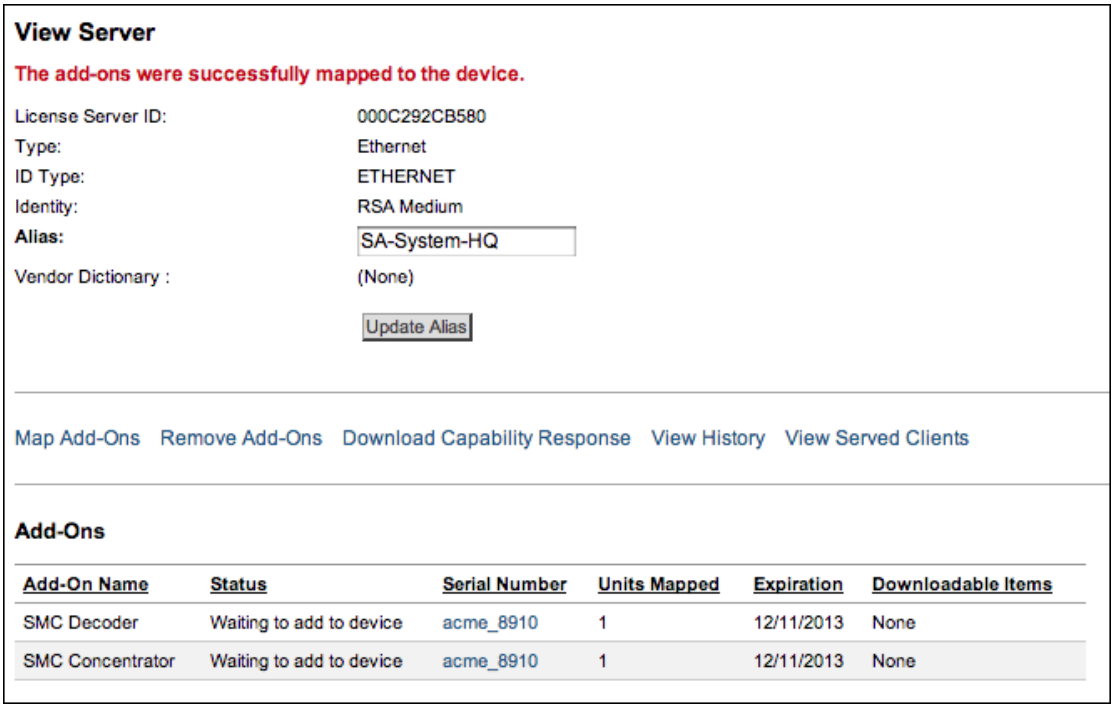
The Add-On table lists all entitlements that are available for your account. The table has a row for each appliance entitlement, with the following information:

- **Add-On Name**: The name of the entitlement; for example, SMC Concentrator or SMC Decoder.
- **Serial Number**: The serial number associated with an order.
- **Expiration**: For keys that are not permanent, the expiration information. The value in this field is a specific date (for example, 12/11/2017) or a time range (for example, 90 days). If the value is a time range, the expiration period begins when the add-on is mapped to a server.
- **Available Units in Line Item**: The quantity of entitlements currently available in an add-on order. This quantity is the difference between the Total Units and the entitlements that have been pulled to a NetWitness Server for appliance licensing.

- **Total Units in Line Item**: The total quantity of entitlements tied to a specific add-on order.
- **Quantity to Add**: The number of entitlements tied to a specific add-on order.

2. To designate the quantity of entitlements to pull to the NetWitness Server from an add-on order, type a quantity in the **Units to Configure** column.
3. Click **Map Add-Ons**.

   The View Server page displays a message indicating that the entitlements were successfully mapped to the NetWitness Server.



   Entitlements are now dedicated and set aside from an accounts pool. The message **Waiting to add to appliance** is displayed in the **Status** for each entitlement. The entitlements are not yet pulled to the server.

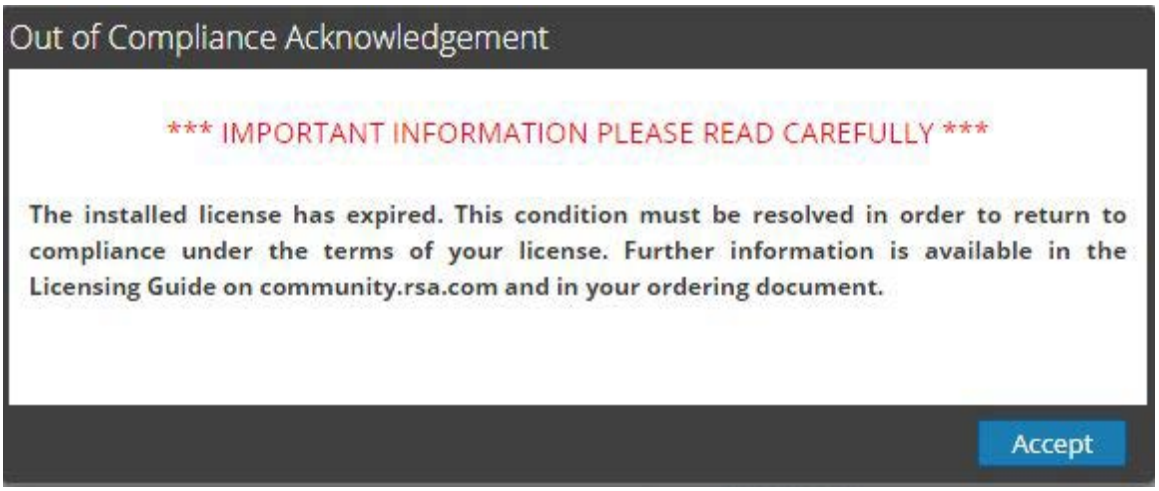
4. (Optional) If you want to add more entitlements, use the **Map Add-Ons** option.
5. (Optional) If you want to remove entitlements, use the **Remove Add-Ons** option.

Now you can synchronize to pull down the mapped entitlements to the NetWitness Server.

What Happens if No License is Installed

If you have not installed a NetWitness Suite Version 11.0 license, an Out-of-Compliance banner is displayed when you log in to the system at the end of 90 days.

The following Out of Compliance Acknowledgement message is displayed.



Click **Accept** to continue using your product.

Note: In a multiple NetWitness Suite deployment where the services are connected to both primary and secondary NetWitness Suite and the services are licensed only with the primary NetWitness Suite, a license expiry message is shown for the same services on the secondary NetWitness Suite. You can ignore the message and continue using the product.

Step 2. Synchronize NetWitness Server

This topic provides instructions for the second step of the NetWitness Suite entitlement process, synchronizing the NetWitness Server with the online repository and downloading mapped entitlements to the Local License Server (LLS).

Prerequisites

Before you perform this step, the NetWitness Server must be registered to Download Central and entitlements must be mapped. If you are doing online synchronization, NetWitness Suite must have access to the internet as well as have a designated nameserver (DNS). Internet access is not required for offline synchronization.

Verify That the Server Has a DNS

To verify that the server has a DNS:

1. Do one of the following:
   a. Manually enter the `nameserver` information within `/etc/resolv.conf` for static IP environments.
   b. Set the `BOOTPROTO` to `static` in the management IP configuration.
2. Restart the network services using the following command:

   ```
   service network restart
   ```

3. Verify the capability to reach external systems via a hostname. Update with FNO-OD hostname.

Synchronize with Download Central

There are two methods of synchronizing NetWitness Suite with Download Central: automatic (online) and offline. You can also force online synchronization by refreshing the view of LLS entitlements in the Performance Licensing tab.

Synchronize Automatically (Online)

By default NetWitness Suite is configured to synchronize with Download Central at regular intervals. No action is required.

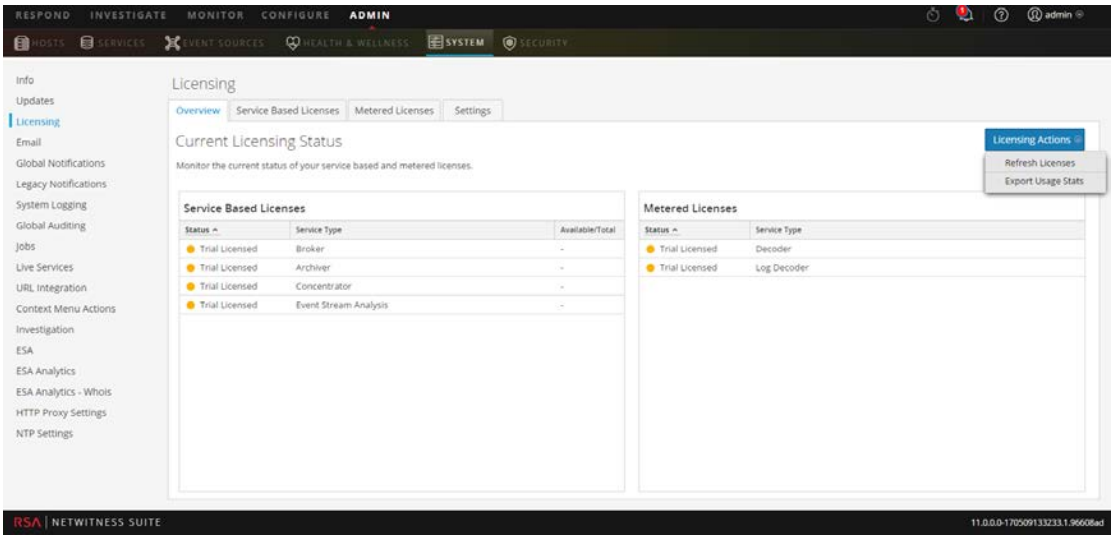
Refresh Licenses

Refreshing your licenses performs the following behind-the-scenes tasks:

- Restarts the LLS server to ensure the latest licenses are pulled down from the central Flexera server.
- Associates any unlicensed service with a valid license (if available).
- Replaces expired or Out-of-the-Box license with valid licenses (if available).

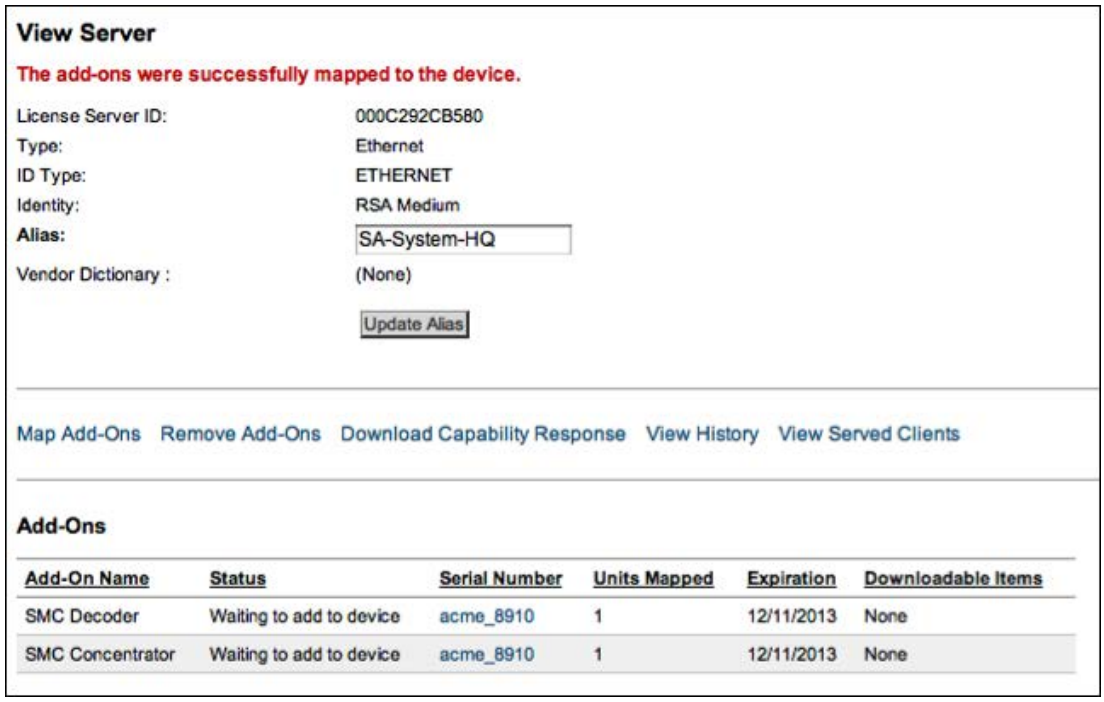
To refresh the view of available files on the Local License Server:

1. Log on to NetWitness Suite.
2. Go to **ADMIN > System.**
3. Select **Licensing** in the options panel.
   The Licensing panel is displayed.
4. Select **Refresh Licenses** from the Licensing Actions drop-down menu.

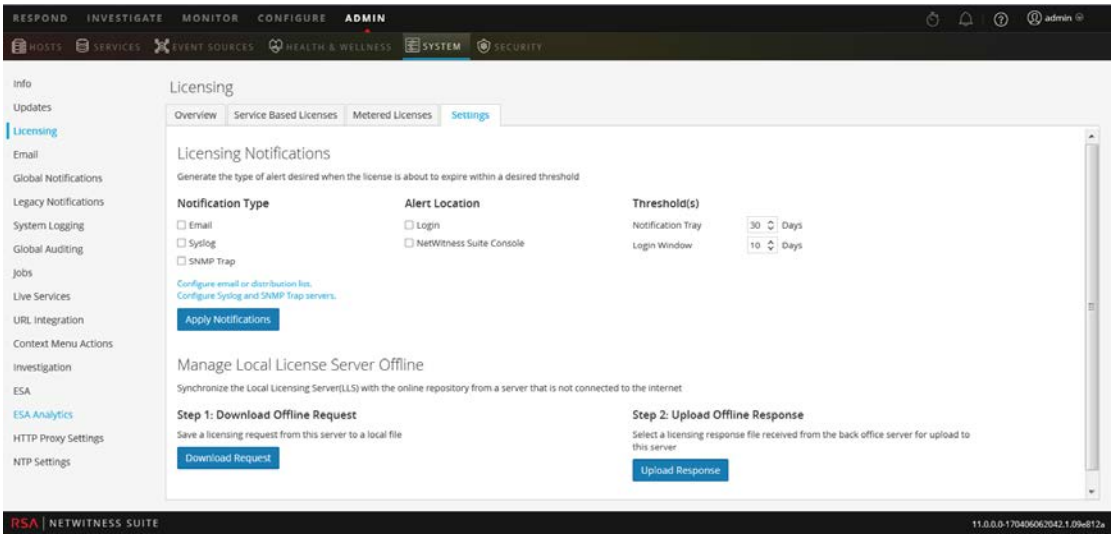


Synchronize Offline

If the NetWitness Server is not connected to the Internet, you can perform offline synchronization of entitlements through the View Server page in Download Central.



1. In the **View Server** page, select **Download Capability Response**.
   A prompt asks you to save a **response.bin** file.
2. From a system with access to the NetWitness Server, log on to the NetWitness Server at **https://*<NW-IP>***, where ***<NW-IP>*** is the NetWitness Server IP address.
3. Navigate to the Licensing panel and select the **Settings** tab.



4. In the **Manage Local License Server Offline** section, click **Upload Response**.
   The Upload Offline Capability Response dialog is displayed:

5. In the dialog, select the **response.bin** file so that it is displayed in the Upload File (bin) field.
6. Click **Upload**.
7. To verify a successful synchronization, do one or both of the following:
   - To view results in NetWitness Suite, refresh the **Performance Licensing** tab.

     The individual product entitlements that have been pulled down to NetWitness Suite are displayed in the **Available/Total** column.

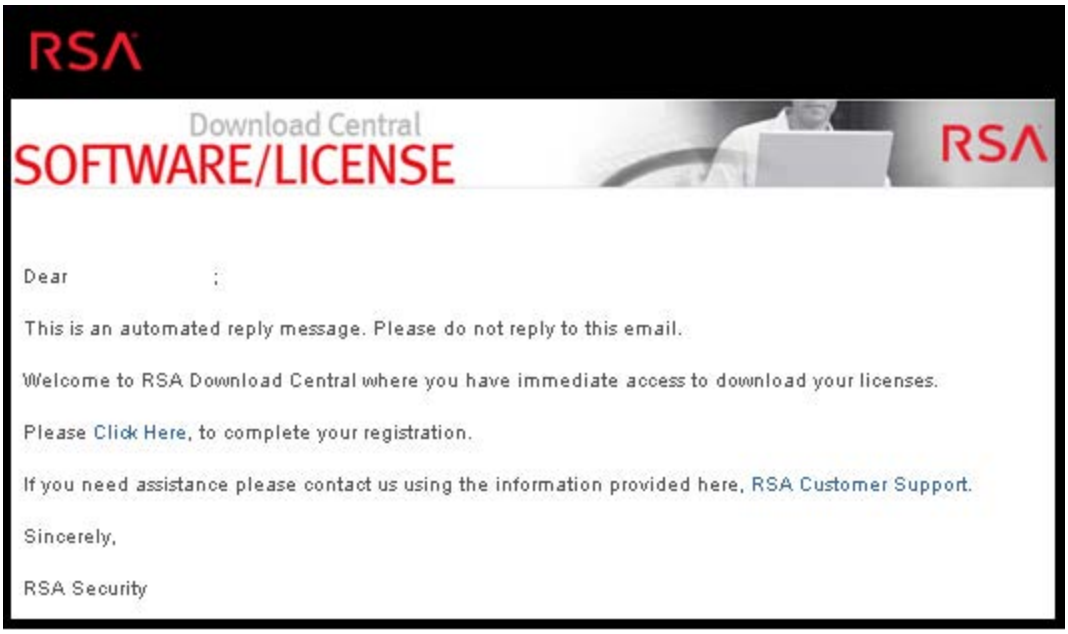
Product	Feature/Version	Available/Total
Concentrator	smcConcentrator 2013.1111	10 of 10
Decoder	smcDecoder 2013.1111	10 of 10

   - Within the Download Central interface, you can see the status for entitlements changed to **In Sync**.

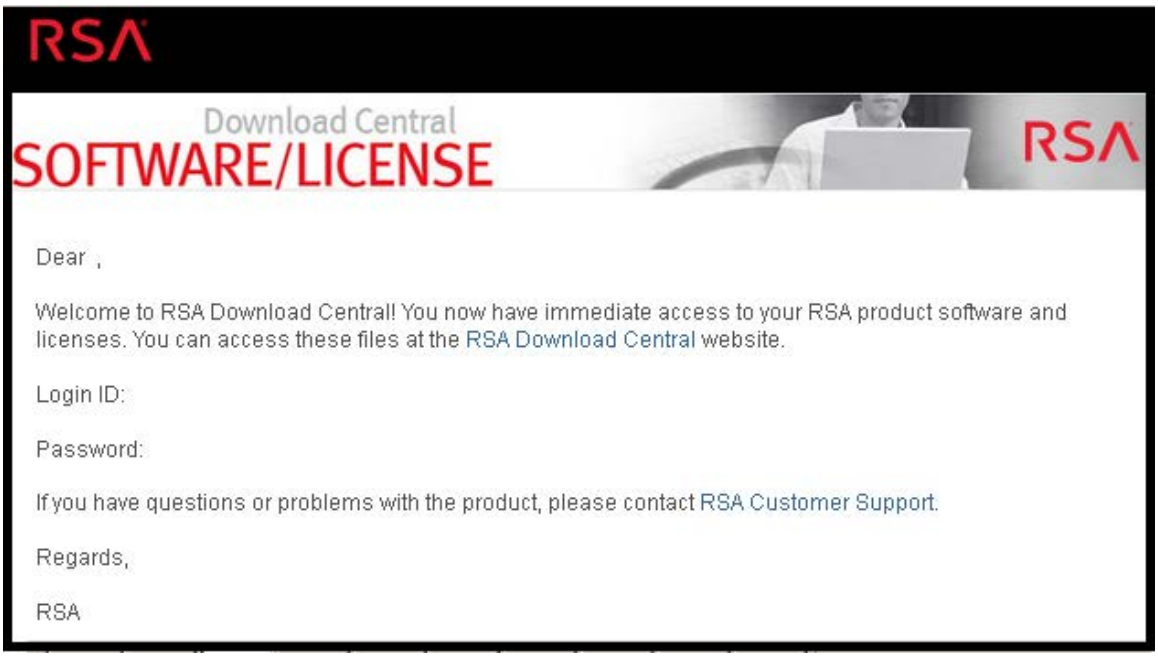
Step 3: Install Product Licenses from Download Central (DLC)

This topic provides instructions for downloading your RSA product licenses from Download Central (DLC).

1. At SAP order delivery, a DLC Welcome e-mail message is sent to all Customer Contacts that are included on the SAP Sales Order. Each contact receives an e-mail confirmation of the order. If the Customer Contact is a new DLC user, they also receive an e-mail message containing instructions explaining how to create their account.
   For new users, the Instructions e-mail message contains a **Click Here** link, as shown in the following example. This link takes you to the Enrollment Portal, where you must configure a Risk-Based Authentication (RBA) method for your account.

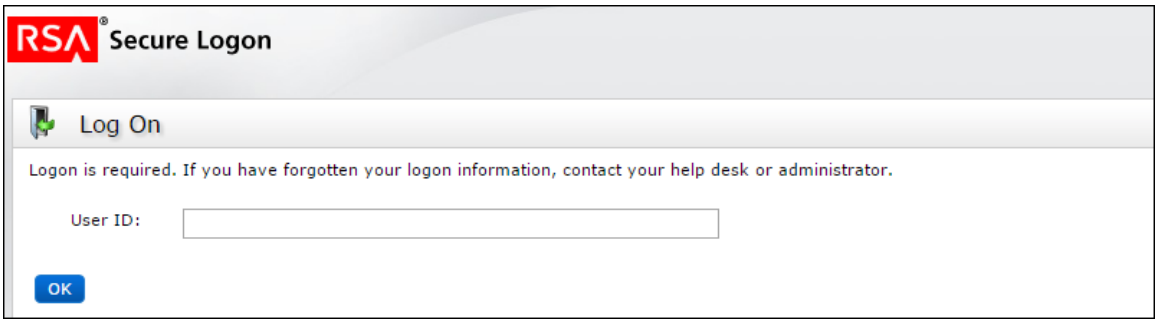


2. After the RBA method is enabled, you receive a Confirmation e-mail message containing your User ID (which is your e-mail address), along with a temporary password. During the initial login session, you are prompted to change your password. Once your password is changed, you are logged into Download Central (DLC).



Note: If the Customer Contact has a pre-existing account for the Link or RSA Online websites, they receive only one e-mail message that instructs them on how to use those existing login credentials. The Customer Contact will log into DLC with their existing User ID, password, and RSA method(s).

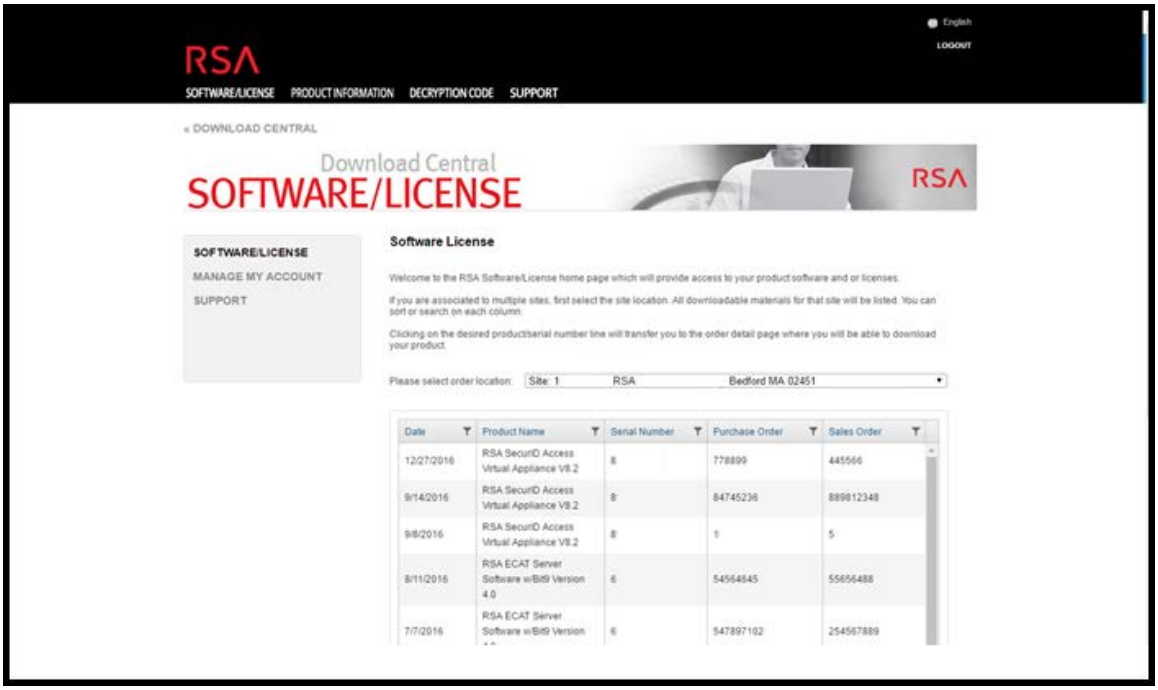
3. When you navigate to https://download.rsasecurity.com, the **RSA Secure Logon** screen is displayed, as shown in the example below.



4. Enter your User ID and click **OK**, which displays the **Password** field. After you enter your password, you are logged into Download Central.
   Your contact e-mail address is used to authenticate your User ID. If the Customer Authentication process is successful, the Download Central Software/License page displays a list of all downloadable RSA Products, Serial Numbers, Purchase Orders, and Sales Orders that is associated with this particular Customer Contact.

Note: You may be prompted to verify your identity via your RBA method if you fail the login several times in a row, or if you have not logged into DLC within the past several months.

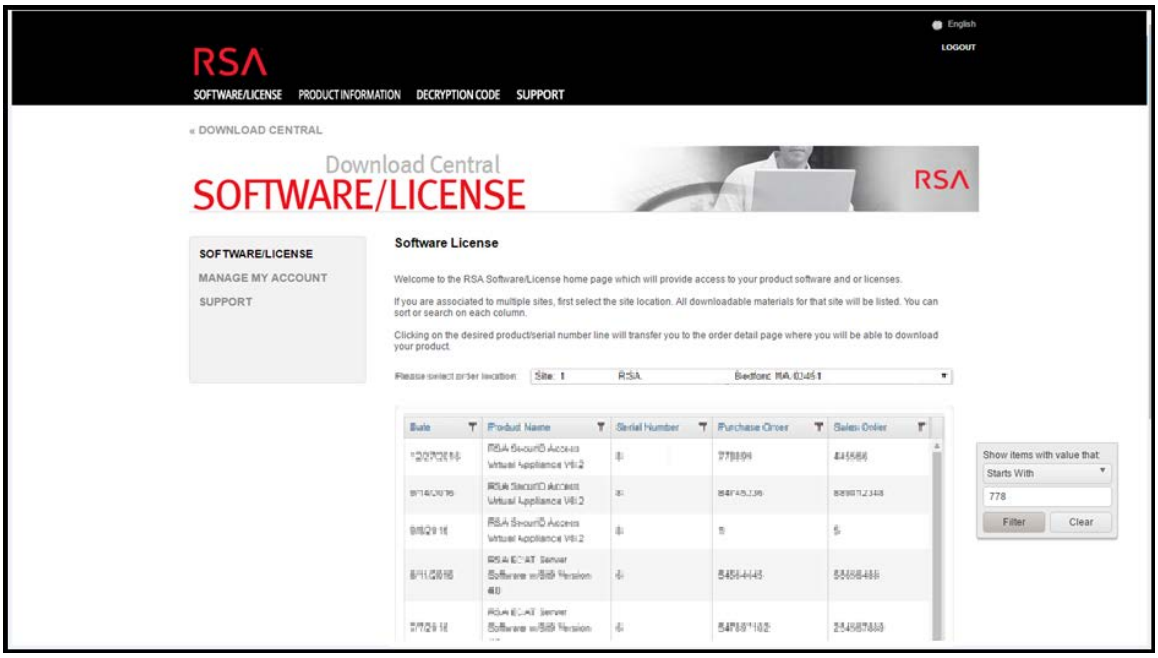
The list of products, sales orders, and purchase orders is filtered and displays only those which were ordered for the Order Location you selected in the drop-down menu, as shown in the following example.



5. If the desired order is not displayed, you can use the Column Filter to narrow your search by filtering on any of the following criteria:

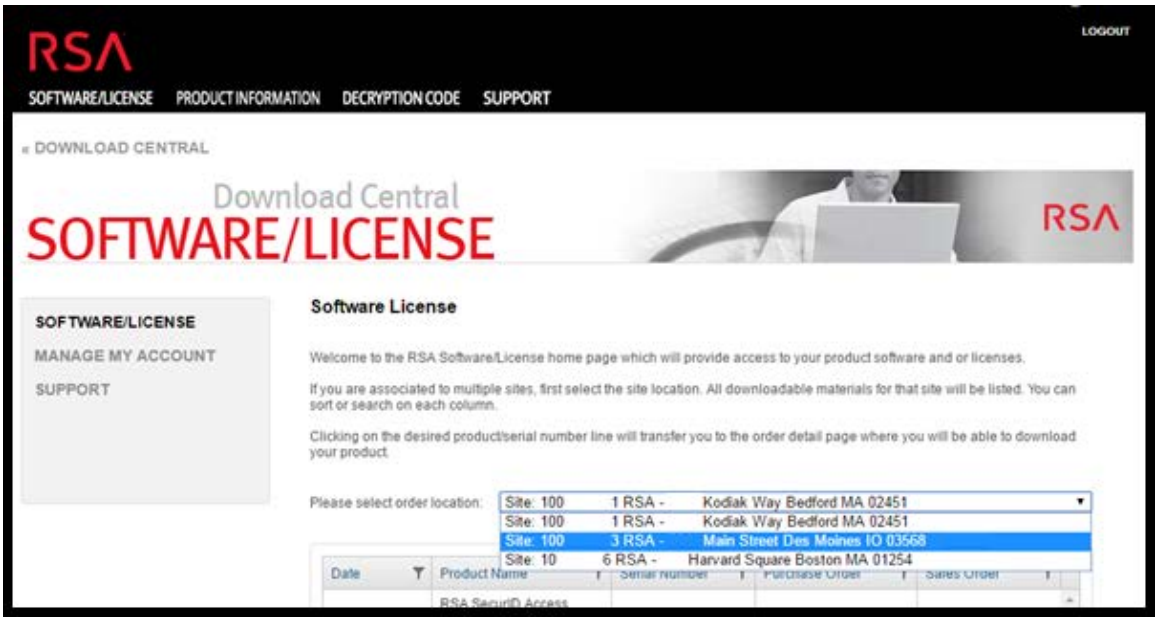
- Date
- Product Name
- Serial Number
- Purchase Order
- Sales Order

In the following example, the **Purchase Order** filter was used to locate Customer Purchase Order 778899.

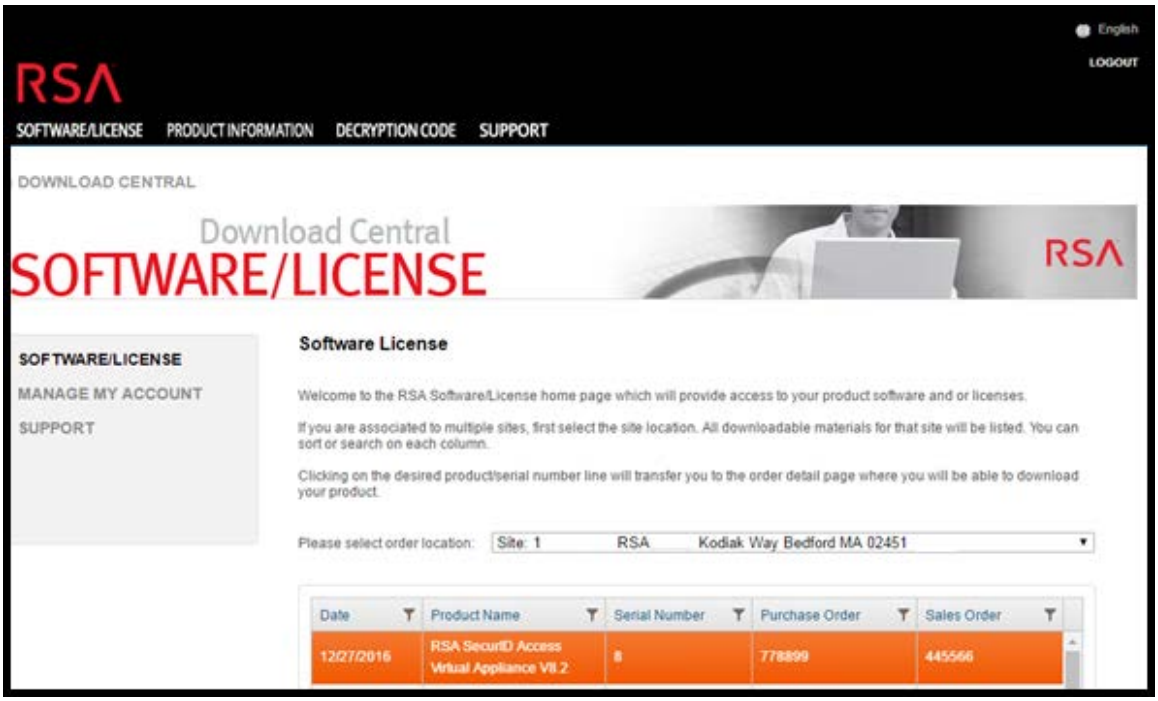


Note: Each contact is associated with at least one Customer ID Site. This Site ID is the Install At (physical location) shown in the Purchase Order that the customer submitted to RSA. Some contacts may be associated with multiple Site IDs, each with their own list of downloads.
To switch between Site IDs, click the **Please select order location** drop-down menu, and select the appropriate address.

6. When your desired download is located in the **Please select order location** drop-down menu, click on the highlighted line item, as shown in the following example.

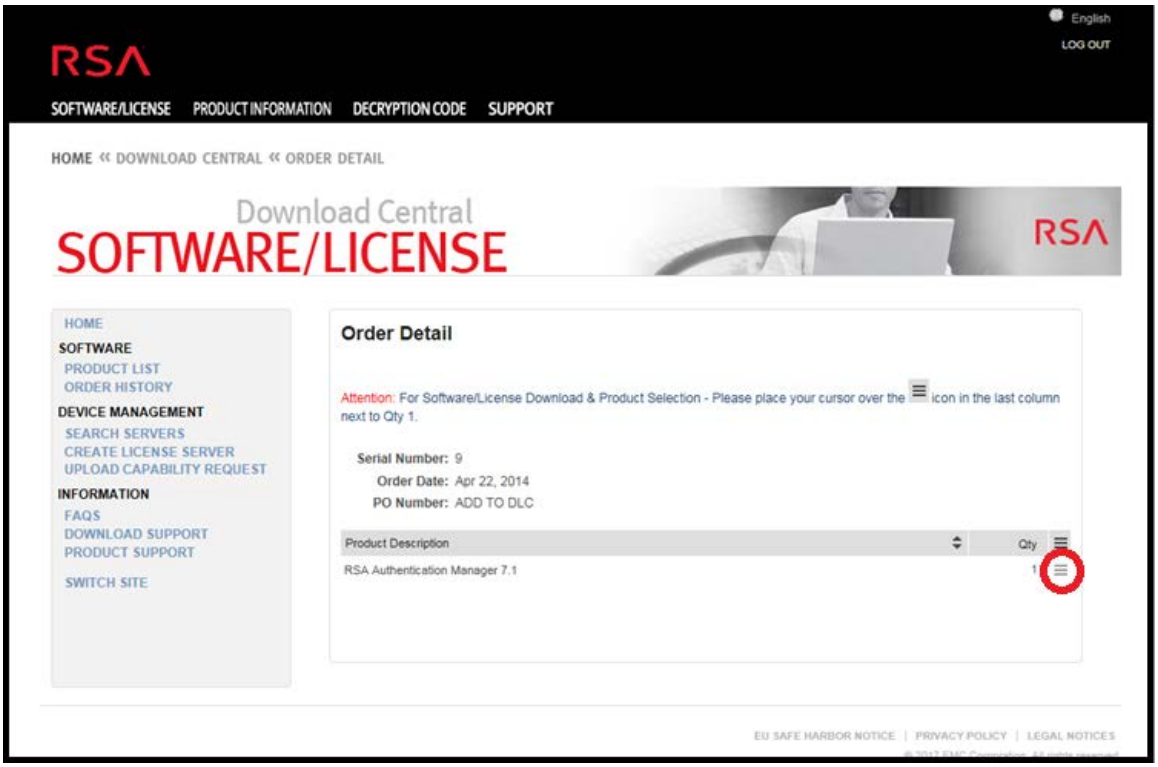


7. Click on the highlighted line item.



8. To download your product license, place your cursor over the

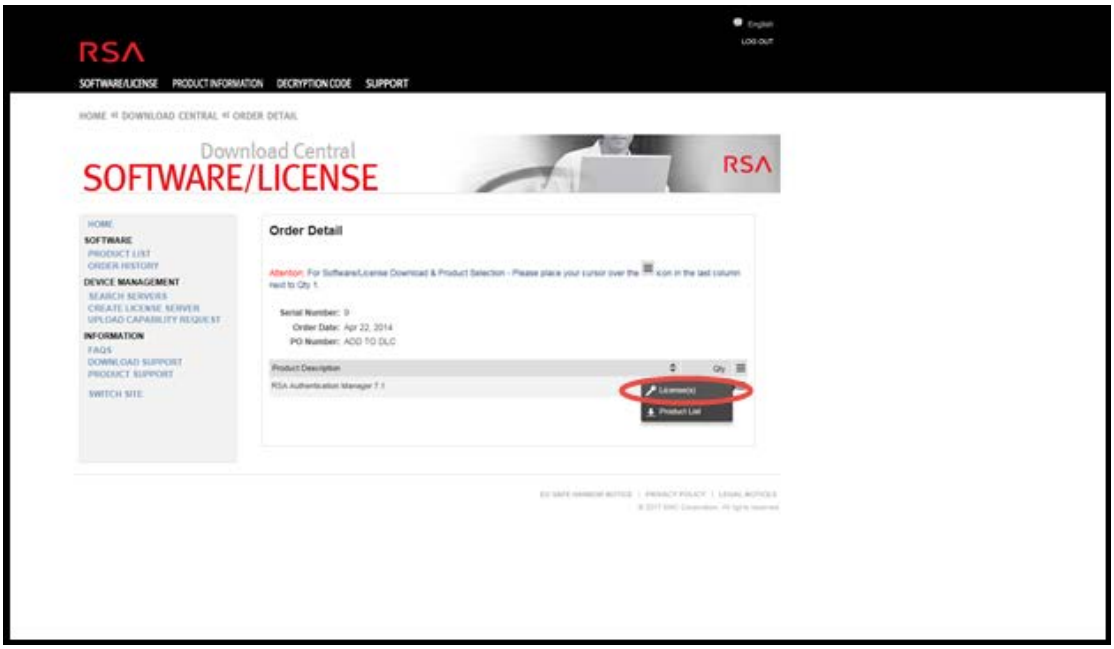
icon in the last column next to the quantity, as shown in the following example.



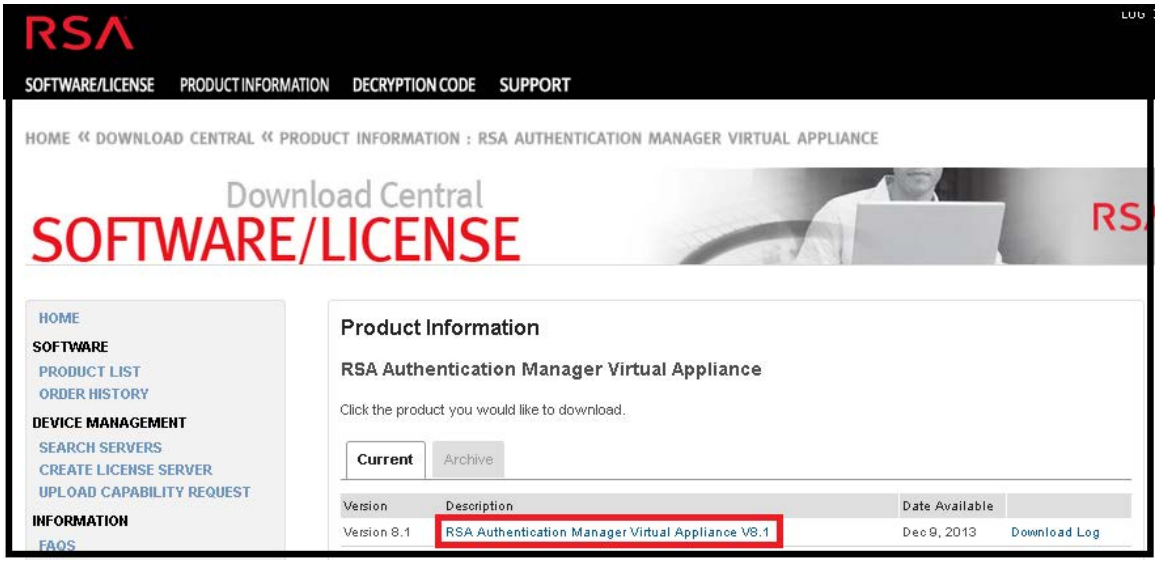
The **Order Detail** screen is displayed.

9. Two options are available for downloading your product license.

   - If you select **License(s)**, you are forwarded to the License Information page where you can download your license file by clicking the **Download** button.



   - If you select **Product List**, you are forwarded to the **Product Information** page where you can download your product software by clicking the **Description** and following the screen prompts.



Additional Procedures

This topic is a collection of individual procedures, which an Administrator may perform at any time, and they are not required for initial setup of licensing.

These procedures are presented in alphabetical order

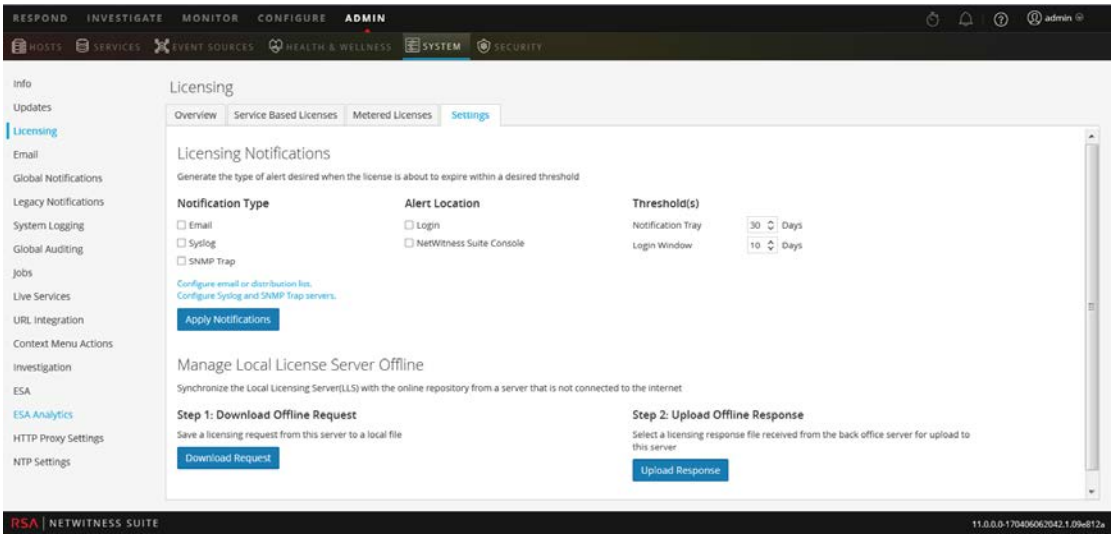
- Configure NetWitness Suite Notifications
- Dismiss Out-of-Compliance Banner
- Export Usage Stats and View Decoder Usage Stats
- Synchronize Local Licensing Server Offline
- View Current Entitlements
- View and Manage License Pools on LLS

Configure NetWitness Suite Notifications

This topic provides instructions for configuring notification settings for the Local License Server (LLS). If you wish to receive alerts about the approaching license expiration date you can configure NetWitness Suite to send notifications. You can receive notification by email, syslog and SNMP. The notification can also be viewed during system log on and also in the Notification Tray. You can also specify the number of days before expiration as a threshold for notification.

To configure the NetWitness Suite notification:

1. Log on to NetWitness Suite, and go to **ADMIN > System.**
2. Select **Licensing** in the options panel.
3. Select the **Settings** tab.



4. Select each of the methods for NetWitness Suite to use when sending a notification about the license nearing its expiration date. You can select none or all.
   a. To receive a notification at log on, select **Login** and specify the number of days before the license expires that you want to receive notification in the **Login Window Threshold** field.
   b. To receive a notification in the Notifications tray, select **NetWitness Suite Console** and specify the number of days before the license expires that you want to receive notification in the **Notification Tray Threshold** field.
   c. To receive an Email notification to a configured distribution list, select **Email** and select **Configure email or distribution list**. The Email panel is displayed in a separate tab, and you can configure NetWitness Suite notifications in the Email Server Settings section. Refer to the *System Configuration Guide* for further details.

d. To receive syslog notifications, select **Syslog** and select **Configure Syslog and SNMP Trap servers**. The System Auditing panel opens in another tab and you can configure the system auditing settings as usual.

e. To receive notifications through SNMP Trap, select **SNMP Trap** and select **Configure Syslog and SNMP Trap servers.** The System Auditing panel opens in another tab and you can configure the SNMP auditing settings as usual.

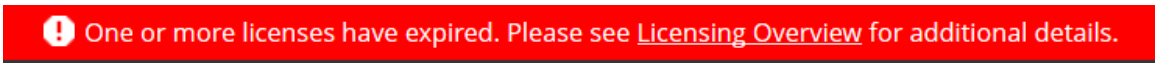
5. Click **Apply Notifications**.
   The settings are saved and go into effect immediately.

Dismiss Out-of-Compliance Banner

This topic explains what you need to do if you see a yellow or red banner displayed after you log on to your NetWitness Server. Banner notifications automatically display during system log on to let you know the status of your license and usage compliance.

A yellow banner is displayed when you are approaching your usage threshold or your licensing is approaching expiration.

A red banner is displayed when your license is out of compliance or you have exceeded your allotted threshold.



To dismiss the yellow banner, click **Dismiss**.

Note: Red banner cannot be dismissed. You must resolve your license issue.

Export Usage Stats and View Decoder Usage Stats

NetWitness Suite Version 11.0 provides the ability for Administrators to view usage statistics of device types that are eligible for a Metered license. Licensing usage statistics are made available to Administrators in CSV and PDF formats.

Hourly statistics are captured for all supported services connected to the NetWitness Server.

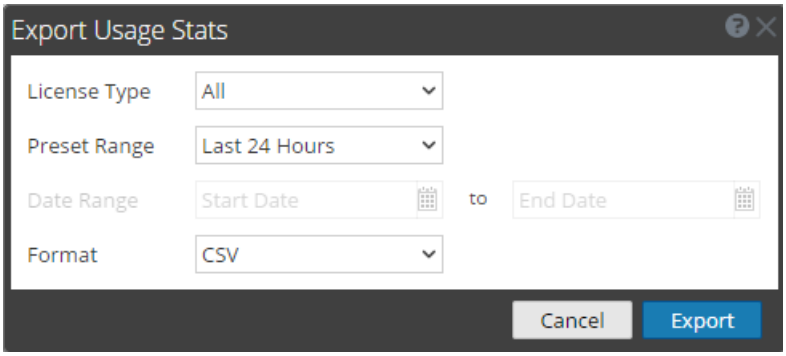
Metrics can be tracked securely, allowing Administrators to save data locally on their systems to use in reporting usage compliance.

To access Export Usage Stats:

1. Go **ADMIN > System** and select **Licensing** in the Options panel.
2. Select the **Overview** tab.

   The **Overview** tab is displayed.
3. Select **Export Usage Stats** from the Licensing Actions drop-down menu.

   The **Export Usage Stats** dialog is displayed.



4. Select a **License Type**, **Preset Range**, **Date Range**, and **Format** that you want the statistics report saved in.
5. Do one of the following:
   a. Click **Export** to export the report.
   b. Click **Cancel** to return to the **Overview** tab

Note: The downloaded file is in zip format with multiple files in it. Each zip file contains aggregate usage for all devices under each license type.

Examine Decoder Service Usage Statistics in the Explore View

The Decoder has service usage statistics that can help you determine the best way to manage packet traffic, so that the Decoder is kept within the usage limits allowed by its license. These statistics are located in the `/decoder/stats` folder for each Decoder service, and you can see them in Administration > Explore view.

- `capture.netfilter.bytes`: This statistic tracks the total size of packets that were filtered out due to matching network rules. Packets are only considered filtered at this stage if the network rule specifies that the packets will not be assembled into sessions.
- `capture.appfilter.bytes`: This statistic tracks the total size of bytes removed from the packet stream due to application rule actions. Application rules may filter packet or truncate packets. If an application rule filters packets, the entire packet is dropped from the collection. If the packet is truncated, only the packet payload is dropped, while the header is still stored. This statistics counts up how many bytes are dropped, be they from entire packets, or dropped payloads.
- `capture.processed.bytes`: This statistic is equal to the total bytes processed, minus any bytes counted in the `capture.appfilter.bytes` or `capture.netfilter.bytes` statistics.

Synchronize Local Licensing Server Offline

NetWitness Suite manages licensing through a Local License Server (LLS). Each client appliance is shipped with an installed LLS. This topic provides instructions for synchronizing the Local License Server (LLS) with the online repository from a server that is not connected to the Internet. Please refer to Entitlement Capability Implementation for a functional description of the LLS.

Prerequisites

If the NetWitness Server is not connected to the Internet, you can perform offline synchronization of entitlements through the View Server page in Download Central. You can:

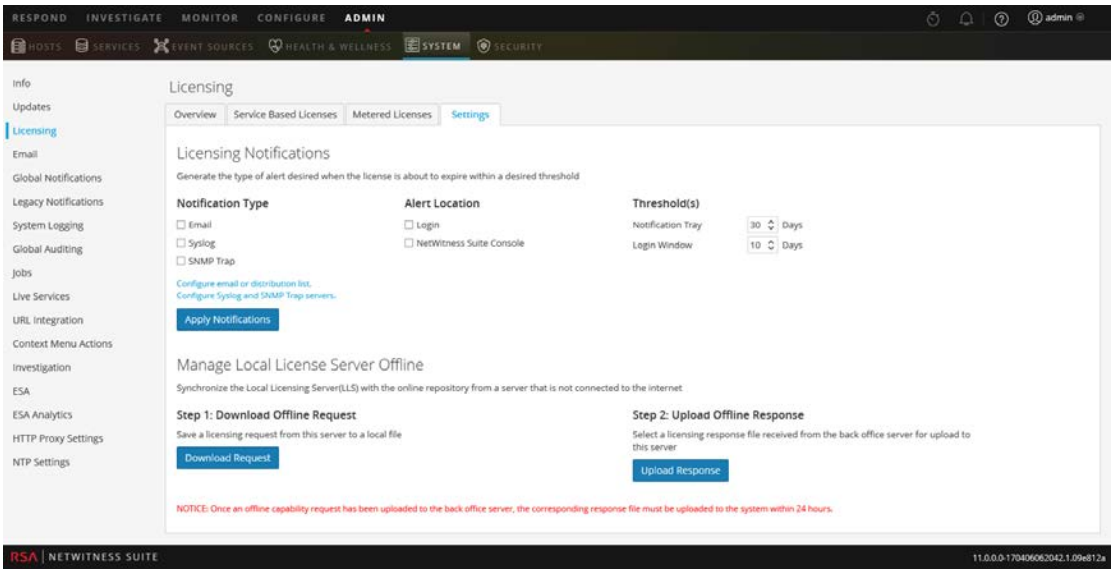
- Download an Offline Capability Request in NetWitness Suite for submission to Download Central.
- Within 24 hours, upload to NetWitness Suite an Offline Response that was received from Download Central.

Download a Capability Request for Submission to Download Central

To download an offline capability request from the NetWitness Suite LLS into a local file for processing by a back-office server.

1. Go to **ADMIN > System.**
2. In the **Options** panel, select **Licensing**.

   The Licensing panel is displayed with the **Overview** tab open.
3. Select the **Settings** tab.



4. In the **Manage Local License Server Offline** section, click **Download Request**.

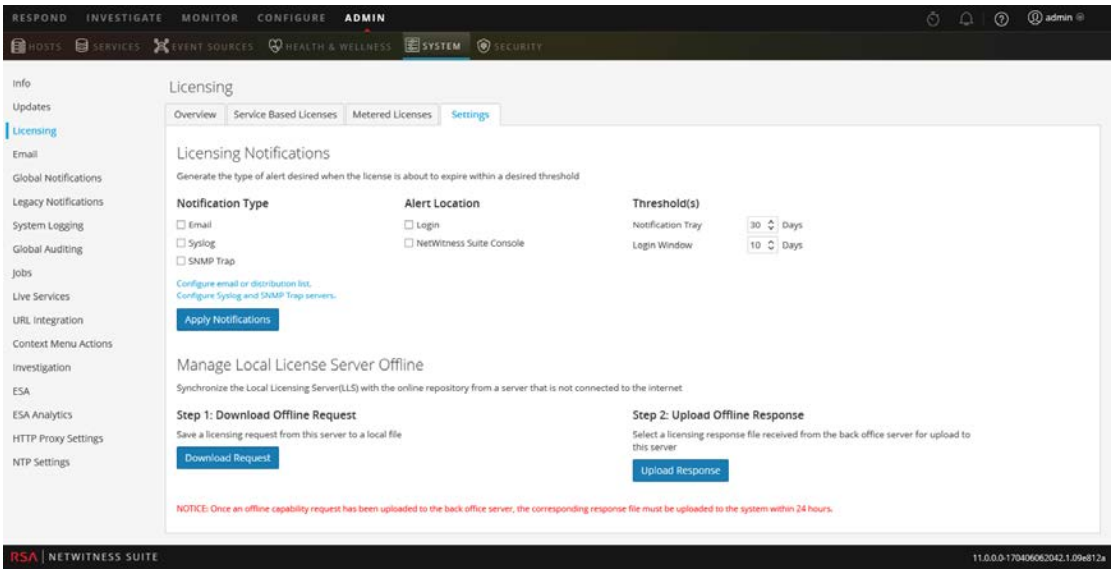
   The Offline Capability Request file (**OfflineCapailityRequest.bin**) is downloaded to the local file system.

Upload an Offline Capability Response to NetWitness Suite

If the NetWitness Server is not connected to the Internet, you can perform offline synchronization of entitlements through the View Server page in Download Central. To upload an offline capability response (**response.bin**) file saved to the local file system from Download Central:

1. Go to **ADMIN > System**.
2. In the **options panel**, select **Licensing**.

   The Licensing panel is displayed with the **Overview** tab open.
3. Select the **Settings** tab.



4. In the **Upload Offline Response** section, click **Upload Response**.

   A dialog prompts for the file.

5. Browse for and select the **response.bin** file so that it is displayed in the Upload File (bin) field.
6. Click **Upload**.

   The entitlements are uploaded to NetWitness Suite and the licenses added to the grid in the **Overview Licensing** tab. They are available for licensing appliances.

View Current Entitlements

This topic describes how to view your current licensing status on NetWitness Suite.

Prerequisites

Each NetWitness Server is a license server providing capabilities to entitle services connected to it. To make entitlements available for licensing services, the entitlements must be downloaded and mapped to the Local License Server (LLS) on the NetWitness Server.

View Current License Status

To view the current license status of individual services connected to the NetWitness Server:

1. Go to **ADMIN**> **System**.

   In the Service grid, each service connected to the NetWitness Suite is listed. Part of the information is whether the service is licensed.

   Note: If no services are listed, you need to add services before continuing.

2. To view additional information about a service license, hover over the icon in the **Licensed** column. The information displayed depends on the type of license.

   - For a permanent license, the following information is displayed: service ID and type of license.

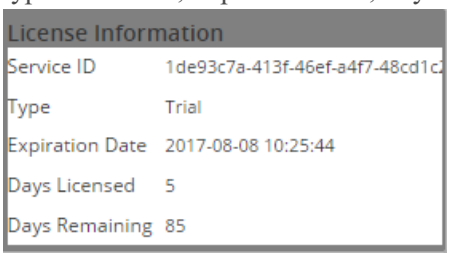
     In case of trial license the information is displayed in formats based on usage.
     Trial license without data usage

   - For trial license with zero usage of the Log Decoder or Decoder, the following information is displayed: Service ID and Type.

     Trail license with data usage

   - For a license with an expiration date, the following information is displayed: service ID,

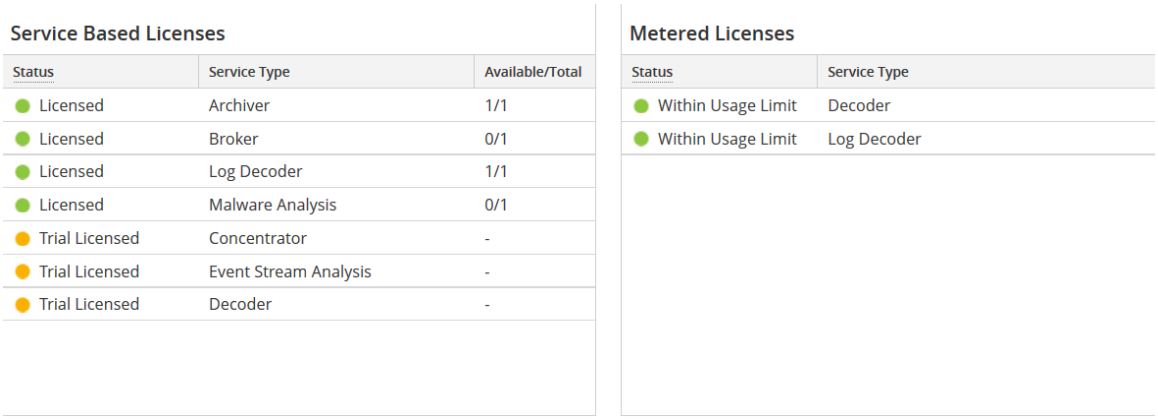
type of license, expiration date, days licensed, and days remaining.



3. To display the current license status, in the main menu, select **Licensing** from the panel in the **System** grid.

   The License status for the selected services changes to green (licensed), yellow (approaching expiration), or red (license expired), depending upon the current license status. The services that you licensed are counted and the quantity is subtracted from the **Available** quantity in the **ADMIN > System view > Licensing** panel.

   Note: If licensing a hybrid system, which has a Concentrator and Decoder on the same appliance, license each component separately. Reporting Engine, Log Collector, Warehouse Connector, Respond Server, Investigate Server, Admin Server, Security Server, Config Server, Orchestration Server and Workbench do not require a license.



View and Manage License Pools on LLS

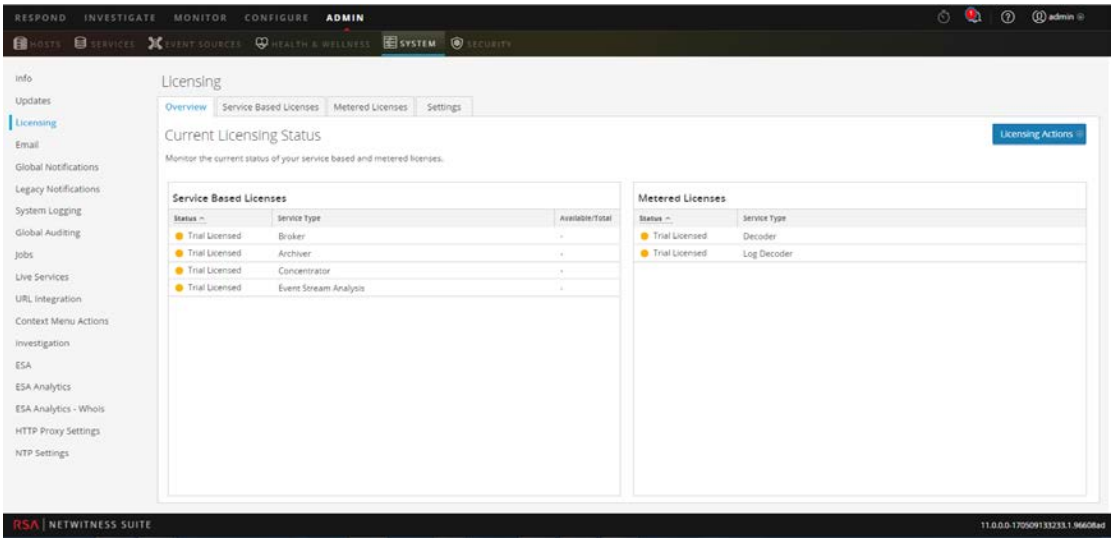
In NetWitness Suite, you can view the entitlements that are available to the Local License Server (LLS) on this instance of NetWitness Suite. You can manage the license pool with the option to refresh the view with the current LLS pool entitlements and availability.

View Available Entitlements

To view the entitlements that are available to the Local License Server (LLS) on this instance of NetWitness Suite:

1. Go to **ADMIN > System.**
2. In the **Options** panel, select **Licensing**.

   The **Overview** tab is displayed.



   Each entitlement is listed in the grid by service type, which is an add-on from a Download Central entitlement. Information includes the status of the license indicated using color-coded circles.

3. To refresh the view, select **Refresh Licenses** from the **Licensing Actions** drop-down menu.

   Entitlements pulled from Download Central are refreshed in the **Service-Based Licenses** and **Metered Licenses** panels.

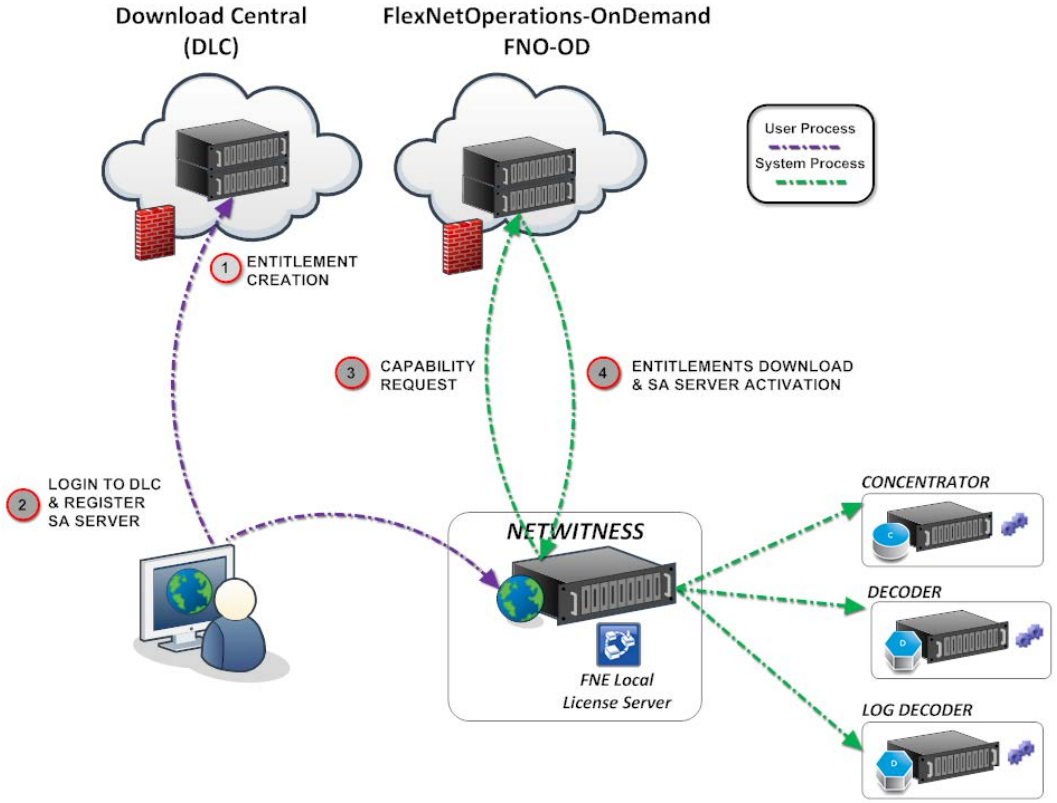
References

This topic is a collection of references, which describe the user interface and more detailed information about how licensing works in NetWitness Suite. These topics are presented in alphabetical order.

- Entitlement Capability Implementation
- Licensing Panel
- Metered Licenses Tab
- Out-of-Compliance Banners
- Overview Tab
- Service-Based Licenses Tab
- Settings Tab

Entitlement Capability Implementation

This topic introduces the way in which licensing of appliances and services is implemented in NetWitness Suite. The entitlement capability leverages RSA Download Central (https://download.rsasecurity.com/) as the mechanism for entitlement delivery.



Key	Description
1	**Entitlements Created and Available to Customer.** After a customer order is processed, the entitlements (licenses) become available in Download Central. The entitlements are tied to an individual account.

Key	Description
2	**Register NetWitness Server on Download Central and Map Entitlements to the Local License Server (LLS).** • Customers log on to Download Central and view the entitlements to which they have access within their account. • Customers map entitlements to their Local License Server using the License Server ID (displayed in the NetWitness Suite ADMIN > System > Info panel). The License Server ID is used only for mapping entitlements to a Local License Server and does not pertain to appliance activation.
3	**Synchronize the Server and Download Mapped Entitlements.** There are two methods for customers to synchronize with FNO-OD and download the mapped entitlements to their LLS. • **Sites with Internet connectivity.** If the LLS has Internet connectivity, the LLS attempts to synch with FNO-OD every 24 hours over HTTP (TCP-80). Customers with Internet connectivity can also perform on-demand synchronization, using the **Refresh** option in the ADMIN > System > Licensing panel on the NetWitness Server. • **Sites in closed environments.** Customers can synchronize the mapped entitlements by downloading a capability request and importing it on the NetWitness Server. After either synchronization method, entitlements that were mapped to the Local License Server on the NetWitness Suite appliance are synchronized, but the entitlements have not been used in any way. For example, if a customer had purchased 10 Decoders and 10 Concentrators, 10 of 10 Decoder entitlements and 10 of 10 Concentrator entitlements would be available on the NetWitness Server.

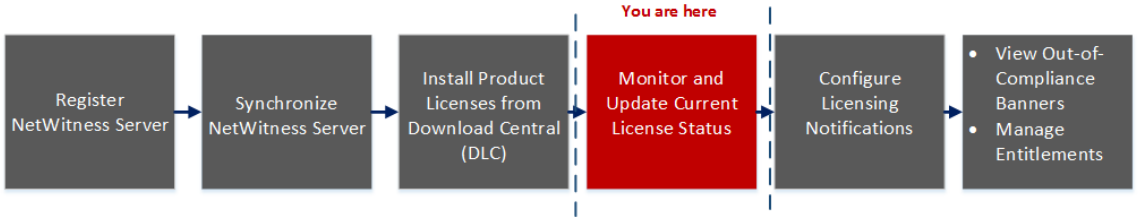
Note: FlexNet Operations-On Demand (FNO-OD) is the license server in the cloud on DLC. URL is rsasecurity.subscribenet.com. The customer's firewall must allow communications between this URL (whatever it resolves to when using lookup or whois) and the NetWitness Suite IP address.

Licensing Panel

This topic introduces the features of the System Licensing panel. NetWitness Suite manages licensing through a Local License Server (LLS). Each client appliance is shipped with an installed LLS.

Workflow

This workflow shows the end-to-end licensing process.



What do you want to do?

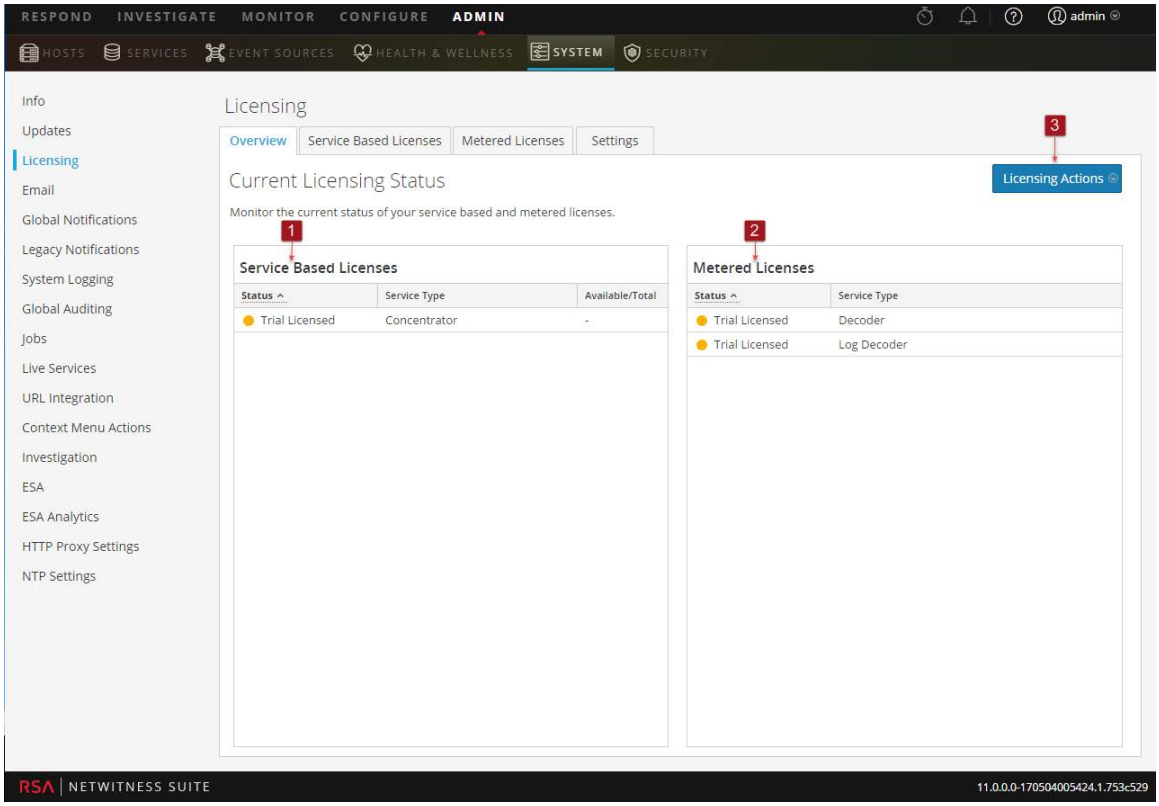
Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	*Monitor and update current licenses.	View Current Entitlements
Administrator	Configure licensing notifications.	Configure NetWitness Suite Notifications
Administrator	View Out-of-Compliance banners and manage entitlements	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

*You can perform this task here.

Quick Look

The Licensing panel has four tabs, which are described in separate subtopics:

- Metered Licenses Tab
- Overview Tab
- Service-Based Licenses Tab
- Settings Tab



The following table describes the features of the Licensing panel.

1. | | |
|---|---|
| 1 | Displays the status of your Service Based license or licenses.
There are five statuses:
• Licensed
• Expiring License
• Expired License
• Trial Licensed
• Not Licensed |
| 2 | Displays the status of your Metered license or licenses. |

There are six statuses:

- Expired License
- Over Usage Limit
- Near Usage Limit
- Within Usage Limit
- Trial License
- Expiring License

3 Displays the Licensing Actions button that offers the following options:

Refresh Licenses: Refreshes the **Overview** tab in order to display the most current license information.

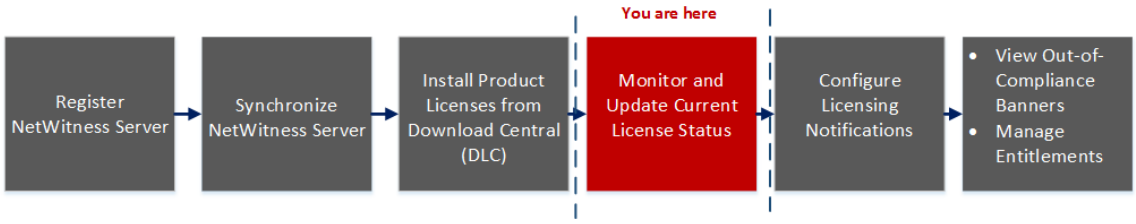
Export Usage Statistics: Exports license usage statistics.

Metered Licenses Tab

The Metered Licensing tab (System view > Licensing Metered Licenses tab) has the information you need to check the status of licenses.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	*Monitor and update current licenses.	View Current Entitlements
Administrator	Configure licensing notifications.	Configure NetWitness Suite Notifications
Administrator	View Out-of-Compliance banners and manage entitlements	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

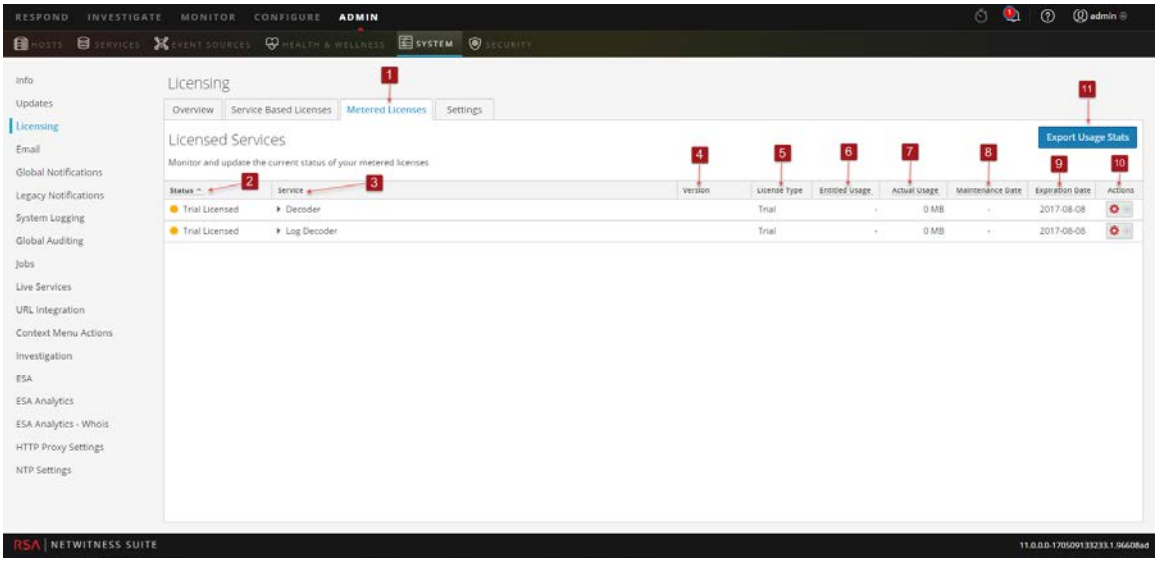
*You can perform this task here.

Related Topics

Export Usage Stats and View Decoder Usage Stats

Quick Look

The **Metered Licenses** tab has one grid and an Export Usage Stats button.



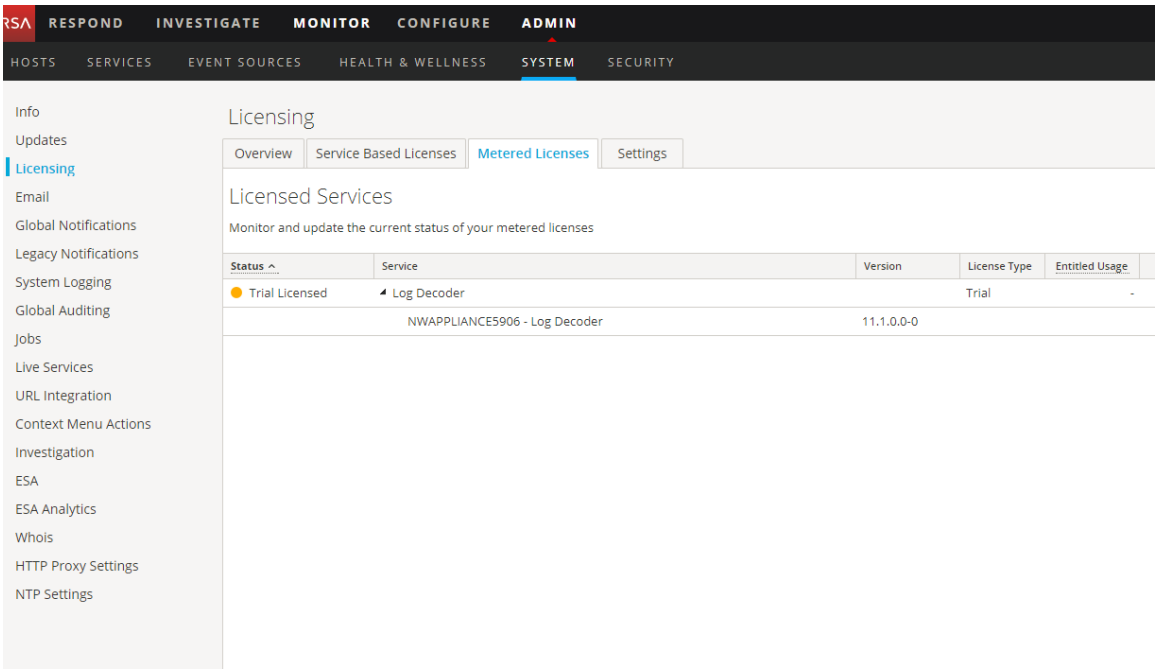
The following table describes the features of the Licensed Services grid.

1	Displays the Metered Licenses tab.
2	Displays the status of the license. There are four statuses: • Expired License • Over Usage Limit • Near Usage Limit • Within Usage Limit
3	Displays the host and type of service to which the license is assigned.
4	Displays the version number of the service.
5	Displays the type of license assigned to the service or host. There are license types: • Trial • Duration • Permanent
6	Displays the daily usage of the entitled usage.
7	Displays the daily average of the actual usage.
8	Displays the maintenance expiration date for the permanent license or licenses.
9	Displays the date on which the license or licenses expire.

10 Licenses can be sorted in either ascending or descending order.

11 Administrators can view the usage statistics available for NetWitness Suite services.

Note: For a trail license with zero usage of the Log Decoder or Decoder or Malware , the Expiration Date field will not display the license expiry date.



Out-of-Compliance Banners

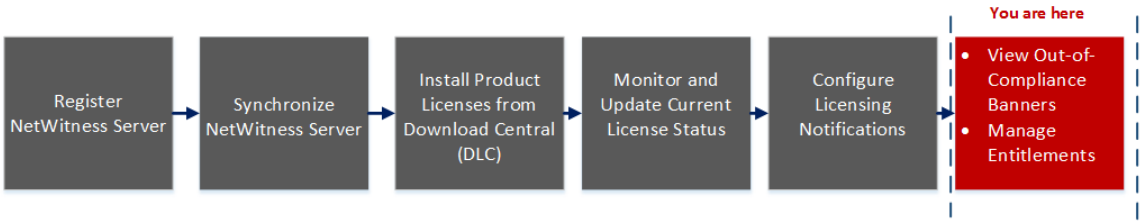
This topic explains what to do when your license is out of compliance. A red banner is displayed during system log on if your license is expired, or you have exceeded your allotted usage. You may also see a red banner if your license has internal errors.

Note: Red banner cannot be dismissed. You must resolve your license issue.

A yellow banner is displayed during system log on if your license is approaching expiration or you are nearing your allotted usage. You can dismiss the yellow banner by clicking the **Dismiss** button.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	Monitor and update current licenses.	View Current Entitlements
Administrator	Configure licensing notifications.	Configure NetWitness Suite Notifications

Role	I want to...	Show me how...
Administrator	*View Out-of-Compliance banners and manage entitlements.	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

*You can perform this task here.

Related Topics

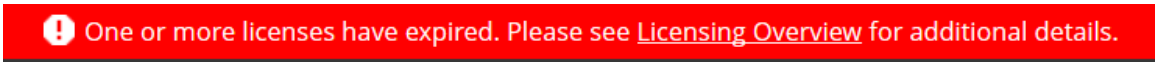
Dismiss Out-of-Compliance Banner

View Current Entitlements

Note: When metered devices are under trial period, warning messages will not be displayed unless usage is observed on the corresponding device.

Out-of-Compliance State

The following sample banner is displayed when a license is expired:



If your license has internal errors, the following banner is displayed:

In addition to a red banner being displayed during system log on, an Out of Compliance Acknowledgment dialog is also displayed. Click **Accept** to continue using your NetWitness Suite product.

Version 11.0.0.0 licenses can enter an out-of-compliance state for the reasons provided in the following table:

Red Banner Message	Possible Causes	Solutions
One or more services is not licensed.	Trial license period has expired. There are pre-11.0.0.0 services in the deployment that are not licensed.	Contact RSA Sales team to procure a NetWitness Suite license. Upgrade the services to NetWitness Suite version 11.0.0.0.
One or more licenses is expired.	Log ingestion usage has been observed after the date of renewal. The license is not valid anymore for the corresponding usage.	Contact RSA Sales team to renew or resolve the license.
You have exceeded license usage limits.	If the allotted daily usage is exceeded on four or more occasions, the Grace Period begins. The Grace Period begins on the day of the fourth occurrence and ends at the end of the following calendar month. Seven continuous days of standard usage will end the Grace Period. If the daily allotted usage is still being exceeded at the end of the Grace Period, the 30-day Breach Period begins. Seven continuous days of standard usage will end the Breach Period.	Contact RSA Sales to extend or increase your allotted usage by purchasing a NetWitness Suite license.
Your Trial license has internal errors.	An internal licensing issue was reported during your Out-of-the-Box Trial period.	Contact RSA Technical Support to resolve this issue.

Note: If a license has not been installed within 90 days, you must contact RSA Sales to purchase a NetWitness Suite Version 11.0.0.0 license.

License Approaching Out-of-Compliance

When your license is approaching expiration, or it is nearing its allotted usage, a yellow banner with a brief description is displayed. A yellow banner is displayed 14 days before your license is due to expire. You will also see a yellow banner if you are approaching your allotted license usage. You can get rid of the yellow banner by clicking the **Dismiss** button.

The following sample banner is displayed in the NetWitness Suite screen if your license is approaching its allotted usage:

The following table explains the messages that are displayed when you see a yellow banner.

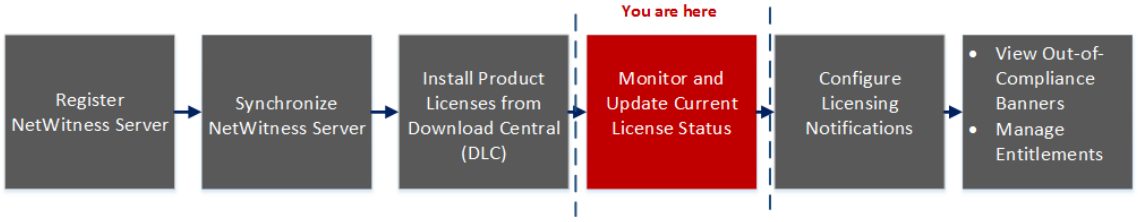
Yellow Banner Message	Possible Causes	Solutions
You are nearing license usage limits.	One or more Metered licenses has exceeded your allotted usage for three times during the current calendar month. The fourth time that you exceed your allotted usage during the current month will push the deployment into an Out-of-Compliance state.	Contact RSA Sales if your allotted usage spikes four times within a calendar month.
One or more licenses is expiring.	One or more licenses is due to expire within 14 days. Or Log ingestion usage has been observed. The license is not valid anymore for the corresponding usage.	Contact RSA Sales to purchase a new license.

Overview Tab

The Overview tab (System view > Overview tab) has the information you need to check the status of licenses and view current license statistics.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	*Monitor and update current licenses.	View Current Entitlements
Administrator	Configure licensing notifications.	Configure NetWitness Suite Notifications
Administrator	View Out-of-Compliance banners and manage entitlements	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

*You can perform this task here.

.

Related Topics

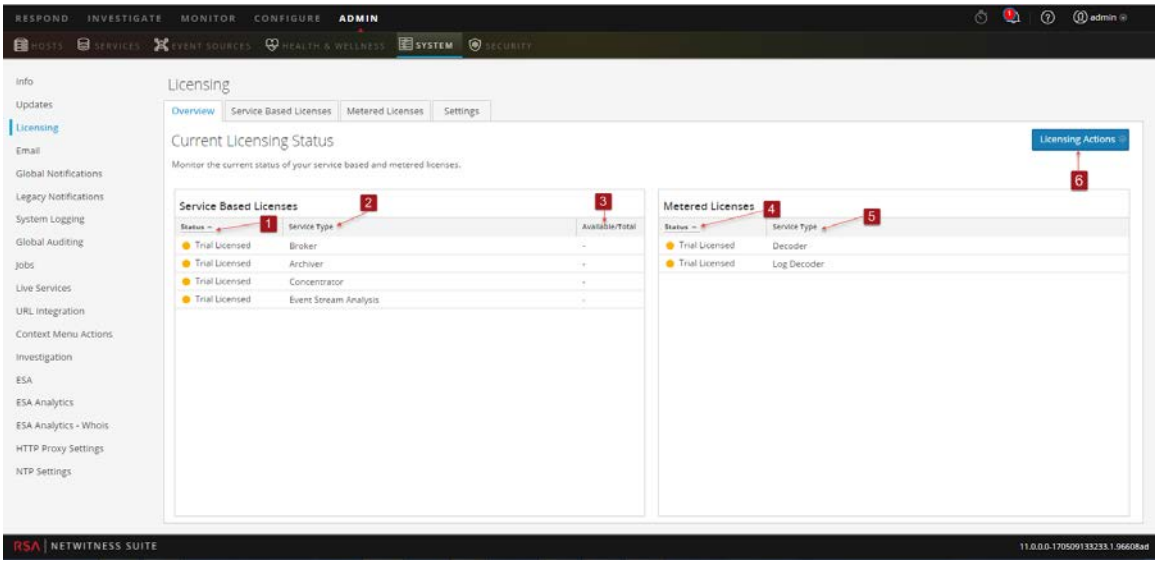
- View Current Entitlements
- Export Usage Stats and View Decoder Usage Stats

Quick Look

The **Overview** tab displays the **Licensing Actions** menu and two panels:

- Service Based Licenses
- Metered Licenses

Note: On initial start up, the usage shown in the Licensing page displays zero usage for the initial one hour.



The following table describes the **Overview** tab.

1	Displays the status of your Service Based license or licenses. There are five statuses: • Licensed • Expiring License • Expired License • Trial Licensed • Not Licensed
2	Displays the type of service to which the Service Based license is assigned.
3	Available number of Service Based licenses can be sorted in ascending or descending

	order.
4	Displays the status of your Metered license or licenses. There are six statuses: • Expired License • Over Usage Limit • Near Usage Limit • Within Usage Limit • Trial Licensed • Expiring License
5	Displays type of service to which your Metered license is assigned.
6	Displays the **Licensing Actions** menu that offers the following options: **Refresh Licenses:** Refreshes the **Overview** tab in order to display the most current information. **Export Usage Stats:** Exports license usage statistics.

Export Usage Statistics

NetWitness Suite Version 11.0.0.0 provides the ability for Administrators to view the current usage statistics of the service. Licensing usage statistics are made available to Administrators in CSV and PDF formats.

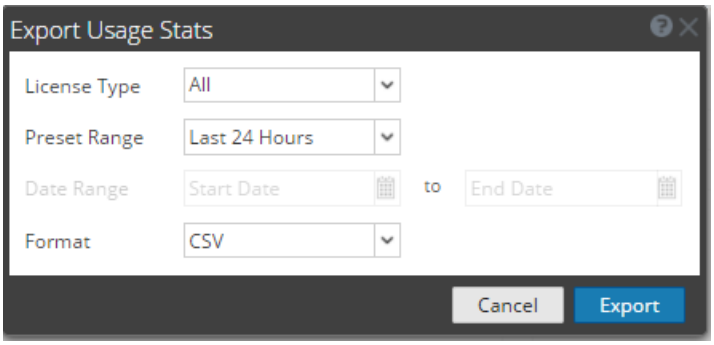
The data provided specifies the hourly statistics captured by supported services connected to the NetWitness Server.

Metrics can be tracked securely, allowing Administrators to save data locally on their systems to use in reporting usage compliance.

The following example shows the **Export Usage Stats** dialog.

To access the **Export Usage Stats** dialog:

1. Click the **Licensing Actions** button.
2. In the dialog box, select a **License Type**, **Preset Range**, **Date Range**, and **Format** that you want for the licensing usage statistics.
3. Click **Export** to save the license usage statistics. Click **Cancel** to return to the **Overview** tab.

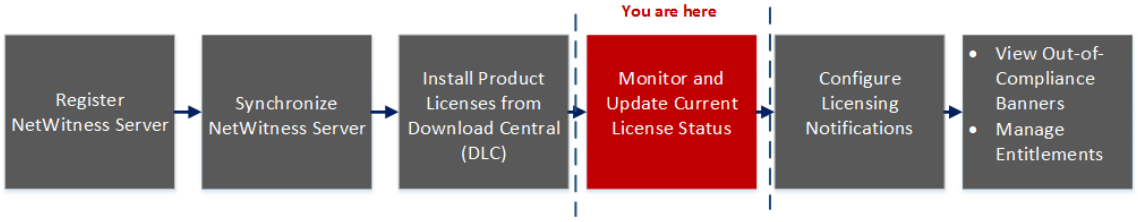

Export Usage Stats
License Type
All
Preset Range
Last 24 Hours
Date Range
Start Date
to
End Date
Format
CSV
Cancel
Export

Service-Based Licenses Tab

This topic provides a description of the System view > Licensing panel > Service-Based Licenses tab. In the Service-Based Licenses tab, you can monitor and update the current status of your Service-Based licenses.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	*Monitor and update current licenses.	View Current Entitlements
Administrator	Configure licensing notifications.	Configure NetWitness Suite Notifications
Administrator	View Out-of-Compliance banners and manage entitlements	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

*You can perform this task here.

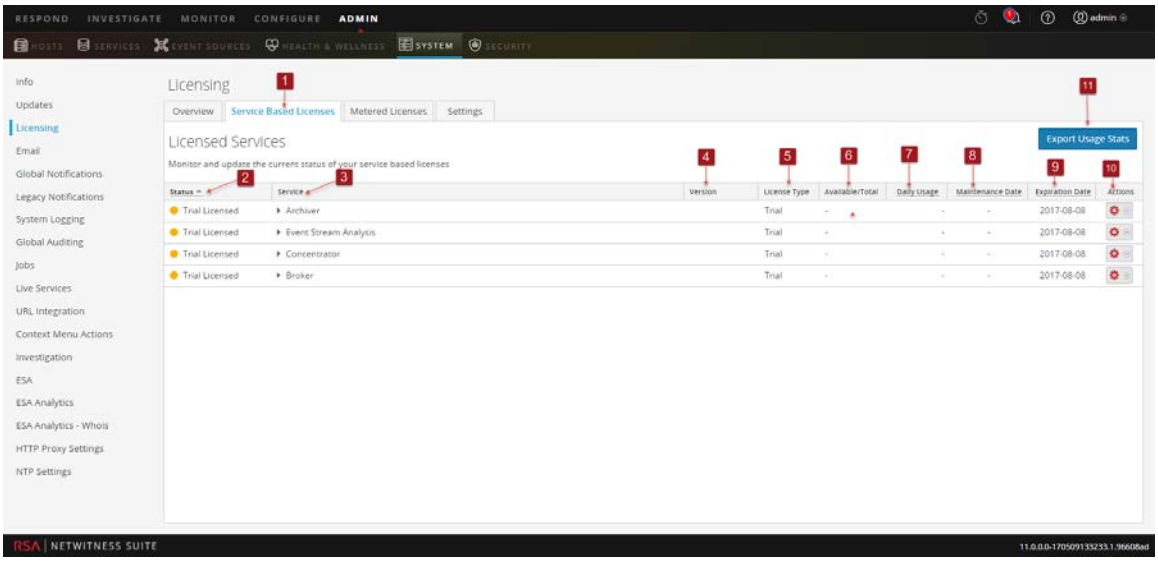
Related Topics

View Current Entitlements

Quick Look

In the **Service-Based Licenses** tab, you can monitor and update the current status of your Service- Based licenses.

The **Service-Based Licenses** tab has one grid and an **Export Usage Stats** button.



The following table describes the features of the Licensed Services grid.

1	Displays the Service Based Licenses tab.
2	Displays the status of the license. There are five statuses: • Licensed • Expiring License • Expired License • Trial License • Not Licensed
3	Displays the host and type of service to which the license is assigned.
4	Displays the version number of the service.
5	Displays the type of license assigned to the service or host. There are three license types: • Trial • Duration • Permanent
6	Displays the daily usage of the entitled usage.

7	Displays the daily average of the actual usage.
8	Displays the maintenance expiration date for the permanent license or licenses.
9	Displays the date on which the license or licenses expire.
10	Licenses can be sorted in either ascending or descending order.
11	Administrators can view the usage statistics available for NetWitness Suite services.

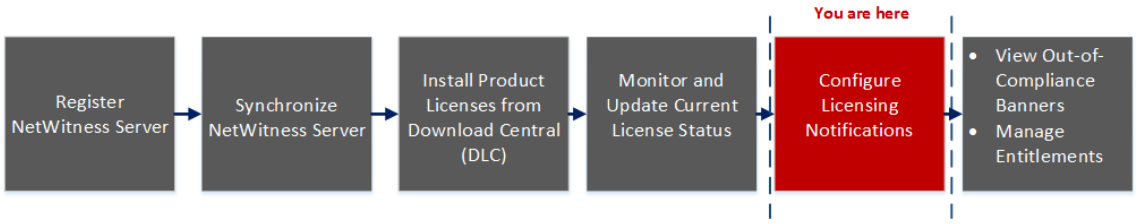
Note: For a trail license with zero usage of the Log Decoder or Decoder, the Expiration Date field will not display the license expiry date.

Settings Tab

This topic describes the notification settings for the NetWitness Suite in the Licensing panel > Settings tab.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Step 1. Register the NetWitness Server
Administrator	Synchronize NetWitness Server	Step 2. Synchronize NetWitness Server
Administrator	Install product licenses from Download Central (DLC).	Step 3: Install Product Licenses from Download Central (DLC)
Administrator	Monitor and update current licenses.	View Current Entitlements
Administrator	*Configure licensing notifications.	Configure NetWitness Suite Notifications
Administrator	View Out-of-Compliance banners and manage entitlements	Dismiss Out-of-Compliance Banner View and Manage License Pools on LLS

*You can perform this task here.

Related Topics

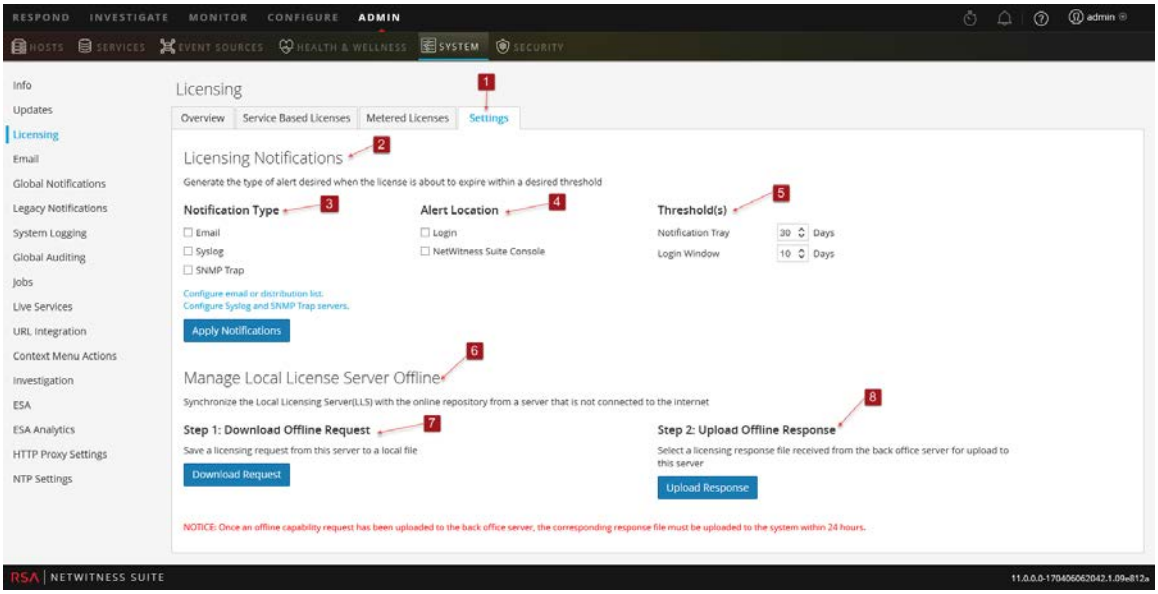
Step 1. Register the NetWitness Server

Configure NetWitness Suite Notifications.

Quick Look

From the **Settings** tab you can:

- Configure licensing notifications.
- Download an Offline Capability Request in NetWitness Suite for submission to Download Central.
- Within 24 hours, upload to NetWitness Suite an Offline Response that was received from Download Central.



The following table describes the **Settings** tab features.

1	Displays the **Settings** tab.
2	Displays the **Licensing Notifications** panel.
3	Displays the **Notification Type**. There are three types of notifications: • **Email:** Checkbox to receive a notification of approaching license expiration in an email message. The email is sent to the configured email or distribution list. • **Syslog:** Checkbox to receive a notification of approaching license expiration in an syslog message. The syslog is generated in accordance with the settings in the Syslog Auditing Settings. • **SNMP Trap:** Checkbox to receive a notification of approaching license expiration in an SNMP trap. The trap is generated in accordance with the settings in the SNMP Auditing Settings.

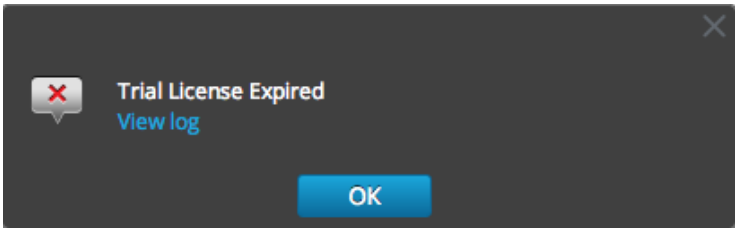
4	Displays the type of **Alert Notification**. • **Login:** Select this checkbox to receive a notification of your approaching license expiration when you log on to NetWitness Suite. The **Login Window Threshold** field specifies the number of days before the license expires to display the notification at log on. • **NW Console:** Select this checkbox to receive a notification of approaching license expiration in the Notifications tray.
5	Displays the **Threshold** field, which specifies the number of days before the license expires to send a notification to the Notifications tray.
6	Displays the **Manage Local License Server Offline** panel.
7	Displays the **Download Offline Request** button. This button enables you to download a request from the NetWitness Suite LLS into a local file for processing by a back-office server. The downloaded bin file should be uploaded to Download Central (DLC) to generate the offline response.
8	Displays the **Upload Offline Request** button. This button enables you to browse for an offline response that you received from the back-office server, and uploads the selected response to NetWitness Suite. The file must be uploaded within 24 hours after receiving the file.

Troubleshoot Licensing

This topic provides information about possible issues that NetWitness Suite users may encounter when setting up licensing in NetWitness Suite. Look for explanations and solutions in this topic. NetWitness Suite notifies users of issues using the popup notifications and the system log as described in the **Troubleshoot NetWitness Suite** topic in the *System Maintenance Guide*.

Simple Error Notification about a Problem with a License

If there is a problem with the license you are attempting to install, NetWitness Suite provides feedback in the form of a simple error notification and a log entry.



Common Log and Configuration Files

When troubleshooting licensing, the following files contain information that may help to diagnose the problem. Specific conditions for searching the files are described in the troubleshooting tables.

On the NetWitness Server

- `/var/log/messages`
- `/var/log/fneserver/fne-error.log`
- Run `wget` for the following flles when ssh'ed onto the NetWitness Server:
  - `http://localhost:3333/fne/xml/properties`
  - `http://localhost:3333/fne/xml/reservations`
  - `http://localhost:3333/fne/xml/features`
  - `http://localhost:3333/fne/xml/diagnostics`

NetWitness Server Problems

This table lists possible problems with the NetWitness Server errors that can affect entitlements.

Problem	Possible Causes	Solutions
The NetWitness Serverdisplays the Out-of-Compliance banner message that states, "Your trial license has internal errors. Please contact RSA customer support for help.”	Ensure that the mongod service is running on your NetWitness Suite appliance.	To resolve the error: 1. Execute the command `systemctl status mongod` from the NetWitness Suite appliance console. 2. If problem persists, please contact RSA customer support for help.
Some features have been mapped in the central Flexera server, but the NetWitness Server doesn’t display them.	Ensure that the NetWitness Server is connected to the internet.	To resolve the error: 1. Execute a License Refresh as follows: 2. In NetWitness Suite, navigate to **ADMIN > Services > Licensing.** 3. Under the **Licensing Actions menu,** select **Refresh Licenses**. **Note:** If the NetWitness Server is not connected to the internet, try to do an Offline Synchronization.
When you remove a service from NetWitness Server, your trial license for that service is also removed.	Various possible causes.	To resolve the error: Add the service again. Your service will continue to function fully even if a message informs you that the service is in a Not Licensed state.

Problem	Possible Causes	Solutions
The NetWitness Server displays the following message when I try to activate a license: "Cannot license this service explicitly."	Services running on NetWitness Suite Version 11.0 do not require that licenses be activated manually.	To resolve the error: 1. Execute a License Refresh as follows: 2. In main menu, navigate to **Admin > Services > Licensing**. 3. Under the**Licensing Actions** menu, select **Refresh Licenses**.
A few Version 11.0 services are not getting licensed.	Ensure that you have the required entitlements pulled down from the Flexera server.	To resolve the error: 1. Execute a License Refresh as follows: 2. In main menu, navigate to **Admin > Services > Licensing**. 3. Under the**Licensing Actions** menu, select **Refresh Licenses**.

Start Date Issue

Problem	Possible Causes	Solutions
NetWitness Suite Start date displays as "Internal Error" under System page for services licensed using SIEM licenses.	Various possible causes.	Change to your old Mac address and restart your FNE server.

License Usage Stats Issues

Problem	Possible Causes	Solutions
NetWitness Suite Licensing page not showing any license information although there are services available.	Mongod server is down or not responding.	• Check the status of the mongod server: `systemctl status mongod` • Start the server if it is down: `system start mongod`
Actual usage of service is showing no value, not even 0 MB is being displayed.	Rabbitmq-server on NetWitness Suite appliance is not running or is not responding.	• Check the status of rabbitmq-server and start if it is down: `systemctl status rabbitmq-server` `systemctl start rabbitmq-server`

Problem	Possible Causes	Solutions

Actual usage of service is always showing 0 MB usage, even though the service/appliance (for example, LogDecoder or Decoder) is processing data.	Rabbitmq-server or collectd service on appliance (for example, LogDecoder or Decoder appliance) is not running or not responding.	• Check the status of rabbitmq-server or collectd services: `systemctl status rabbitmq-server`
		
		`systemctl status collectd`
		• Start the services if not responding or down: `systemctl start rabbitmq-server`
		
		`systemctl start collectd`

Download Central (DLC) Issues

Problem	Possible Causes
Unable to refresh licenses from subscribernet. Also unable to download an offline response from DLC.	Various possible causes.

Problem	Possible Causes
Solution Contact Customer Support for assistance in installing licenses.	
Customer unable to login to Download Central.	Various possible causes.
Solution Contact Customer Support for Offline Capability Response file to re-apply license in NetWitness Server. Also reset all licenses from all services.	
Licenses were not mapped in DLC.	Various possible causes.
Solution License reset from User Interface resolved the mapping issue.	

Wrong License Mapping Issues

Problem	Possible Causes
Perpetual license appears to be in use, although there is no Service-based license.	The NetWitness Suite entitlement database contains an object that holds the entitlement for a service that is licensed to the NetWitness Server.

Problem	Possible Causes

Solution
1. From the main menu, select **ADMIN > System > Licensing > Overview.**
2. SSH into the NetWitness Server as `root`.
3. Connect to the entitlement database using the following command:
`mongo sa`
4. Check the current entitlement status as follows:
`db.entitlement.find()`
From the output, note the `ObjectId` for the services that appear to use Trial licenses.
5. Remove the `ObjectId` for the missing endpoint that appears in`/var/lib/netwitness/uax/logs/sa.log`.
`db.entitlement.remove( {_id: ObjectId("<ObjectId>") } )`
`For example:`
`db.entitlement.remove( { _id: ObjectId("5595c9a9f2806lac50735xxx") } )`
6. Repeat Step 5 for all missing `ObjectIds`, as well as the ones noted in Step 4.
7. Type exit to close the database.
8. From the NetWitness Suite User Interface, select the **Licensing Actions** menu and select **Refresh Licenses**.
9. Once the Refresh process completes, confirm that the services are entitled with the Perpetual licenses.	

Decoder license not available due to core appliances being removed from the NetWitness Server without releasing the license. Several core appliance licenses were not available for use.	Various possible causes.
Solution Reset license on NetWitness Server and re-license each appliance.	
Archiver DACs are not mapped to the license server with all other appliances' licenses.	Various possible causes.

Problem	Possible Causes
Solution: 1. Enter **1** in Quantity field to add for each license. 2. Select **Map Add-ons** at the bottom of the screen. 3. Click **Download Capability Request** and upload license to the Offline Capability Request in the User Interface under the **License** tab.	
Two new appliances were installed: Log Hybrid and one Log Archiver. Able to license the Log Hybrid, but the following error occurred when attempting to license the Archiver: "There is an issue with registering your product, please contact RSA Customer Support." Also, one of the Concentrators showed as a Trial license, and a separate Log Decoder showed as a Trial license when they should be licensed.	After looking into Flexera, Customer Support found that the new equipment had not been mapped to the License Server.
Solution Map add ons to DLC and upload the `.bin` file into the NetWitness Suite User Interface.	
Mapping to License Server ID was not created.	Various possible causes.
Solution Licenses must be re-entitled and status of all appliances is displayed as licensed.	

Problem	Possible Causes
Customer unable to delete Trial licenses when Service-based licenses are in use.	Customer had two different NetWitness Server for two different sites (CHN and NOI). Each site had separate mapped entitlements. The red compliance banner was seen on the NOI site, because some Concentrators were attached to the NOI NetWitness Server that was entitled by the CHN site. The reason for the banner was that the NOI NetWitness Server did not have any more concentrator entitlements available for the CHN concentrators attached for investigation. The customer only has Trial licenses for 90 days from the date the NOI NetWitness Server and services were marked as out-of-compliance. **Note:** When there is more than one NetWitness Server in use, NetWitness SuiteVersion 10.5 and above requires a separate license for each NetWitness Server. Also, if you move one or more appliances to a different location, check to make sure there is a valid license for each appliance. A red out-of-compliance banner is displayed if there is no valid license.
Solution Customer was informed that their services will continue to function as required. The out-of-compliance banner can be dismissed by procuring additional entitlements to map onto the NOI NetWitness Server.	
License missing after re-imaging.	Various possible causes.
Solution Download license from DLC.	

RSA NETWITNESS® SUITE

Live Services Management Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Live Services Management **6**

NetWitness Suite Live 6

The CMS Library 6

NetWitness Suite Feedback and Data Sharing 6

Live Services Required Procedures **7**

Create Live Account 8

Set Up Live Services on NetWitness Suite 12

Find and Deploy Live Resources 13

Find Resources 13

Deploy Resources in Live 14

Manage Live Resources 21

Procedures 21

Additional Procedures **23**

Export Data to RSA 24

About Live Feedback 24

Download Live Feedback Historical Data 24

Share Data to RSA 25

Packaging Resources 26

Create and Deploy Resource Package Use Case 26

Prerequisites to Create a Resource Package 26

Procedure to Create a Resource Package 27

Example: Create Threat Package 27

Example: Deploy Threat Package 28

Manage Custom Feeds 32

Custom Feed Creation 32

Sample Feed Definition File 32

Feed Definition Equivalents for Custom Feed Wizard Parameters 33

Create a Custom Feed 36

Create a STIX Custom Feed 46

Create and Manage an Identity Feed 59

Edit a Feed 71

Remove a Feed 74
Miscellaneous Live Services Procedures 76
Add Subscribed Resources for Deployment to Services 76
Delete a Subscription 76
Display Resource Details in Live Resource View 77
Download a Resource 78
Locate and Remove a Deployed Resource from Services 78
Remove Subscribed Resources from the Deployments Subscriptions Grid 79
Show Results as a List or in Detail 80
Subscribe and Unsubscribe to a Resource 80
View Resource Details 81
View Subscribed Resources Selected to Deploy on Services 82

Troubleshooting 83

References 84

Live Configure View 84
Deployments Tab 84
Subscriptions Tab 87
Discontinued Resources Tab 88
Live Feeds View 91
Toolbar 91
Feeds Grid 92
Live Resource View 93
Resource Details 94
Resource View Toolbar 96
Live Search View 96
Search Criteria Panel 97
Matching Resources Panel 100
Resource Package Deployment Wizard 103
Features 104
Package Tab 104
Resources Tab 105
Services Tab 106
Review Tab 108
Deploy Tab 109
RSA Live Registration Portal 110

NetWitness Suite Feedback and Data Sharing 112
Additional Live Services 112
Live Feedback 112
RSA Live Connect 113
Participation 115

Live Services Management

RSA NetWitness Suite Live is the gateway to a rich environment that offers access to feeds, tools, and other resources.

NetWitness Suite Live

Live is the component of NetWitness Suite that manages communication and synchronization between NetWitness Suite services and a library of Live content available to RSA NetWitness Suite customers. Live provides a simple interface for browsing, selecting, and deploying content from the NetWitness Suite Live Content Management System to NetWitness Suite services and software. In addition to managing feeds from the CMS Library, Live allows users to deploy custom feeds and packages.

The CMS Library

The content management system (CMS) library (known as *Live*) is a valuable source of the latest internet security resources for NetWitness Suite customers. It provides a view into the collective intelligence and analytical skills of the worldwide security community to ensure that users have the most current visibility into attack vectors.

Live gathers the best advanced threat intelligence and content in the global security community - the ideas, research, ongoing tracking, and analysis - and brings it directly into the user's security operations center to definitively classify computers associated with botnets, malware, and other malicious exploits. Live aggregates, consolidates, and illuminates only the most pertinent information relevant to an organization on a real-time basis.

NetWitness Suite Feedback and Data Sharing

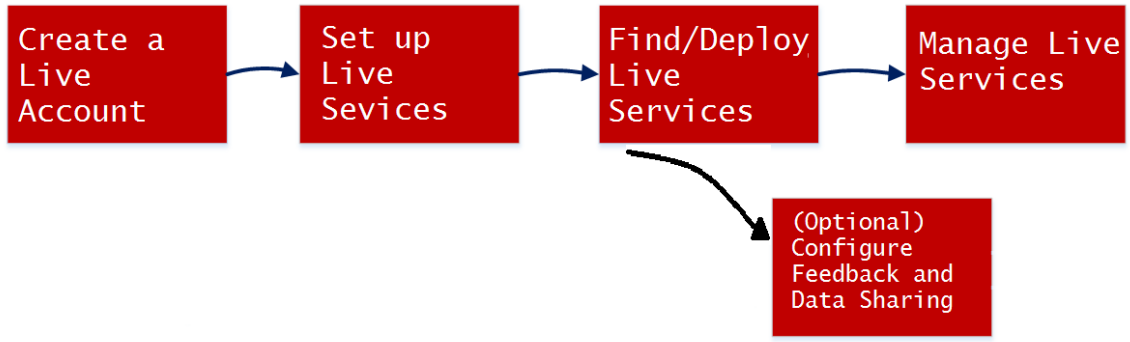
Live Feedback is intended to help improve RSA NetWitness Suite. Once you set up and configure a Live account, usage data is shared with RSA.

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources. It **Threat Insights**, which provide analysts the ability to pull threat intelligence data from the Live Connect service. It also offers **Analyst Behaviors**, an automated data collection service with the goal of sharing potential threat intelligence for analysis.

For more details, see NetWitness Suite Feedback and Data Sharing.

Live Services Required Procedures

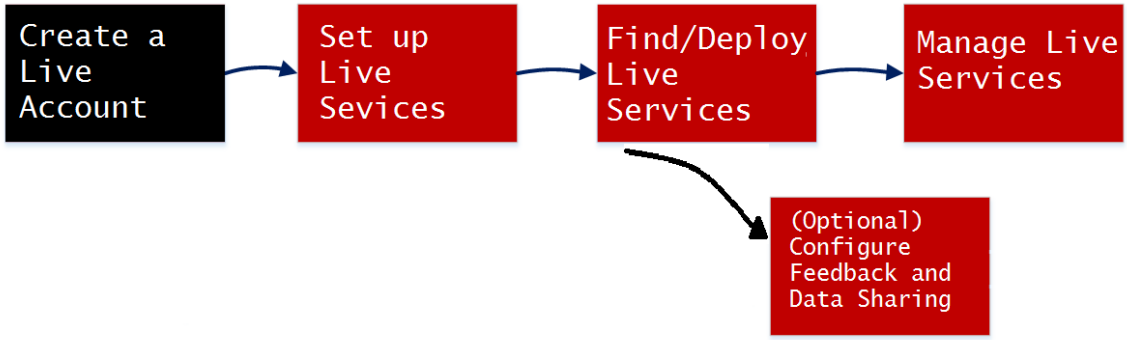
The following workflow breaks out the basic setup into four steps, which you can do individually. The easiest way to set up the Decoder is to follow the end-to-end procedure in this section, Live Services Required Procedures), which includes all of the steps.



Configuration Step	Description
Create Live Account	Create a Live Account on the RSA Live Registration portal URL: https://cms.netwitness.com/registration/. If you have an existing account, you can manage your account using this portal.
Set Up Live Services on NetWitness Suite	Set Up Live Services on NetWitness Suite by configuring a connection with the CMS server.
Find and Deploy Live Resources	Search and browse for resources in the Live Search view, an then, deploy the selected resources.
Manage Live Resources	Procedures for administrators to search for, subscribe to, and deploy resources from Live.
NetWitness Suite Feedback and Data Sharing	Describes the feedback and data sharing features provided in RSA NetWitness® Suite, from Live Services. Participation is optional, but can help to provide useful threat intelligence for the community.

Create Live Account

You must create a Live account using the RSA Live Registration Portal on the CMS server. The CMS Library provides access to all RSA content in one place where you can view, search, deploy, and subscribe to RSA content. You must register on the RSA Live Registration Portal and select a subscription level.



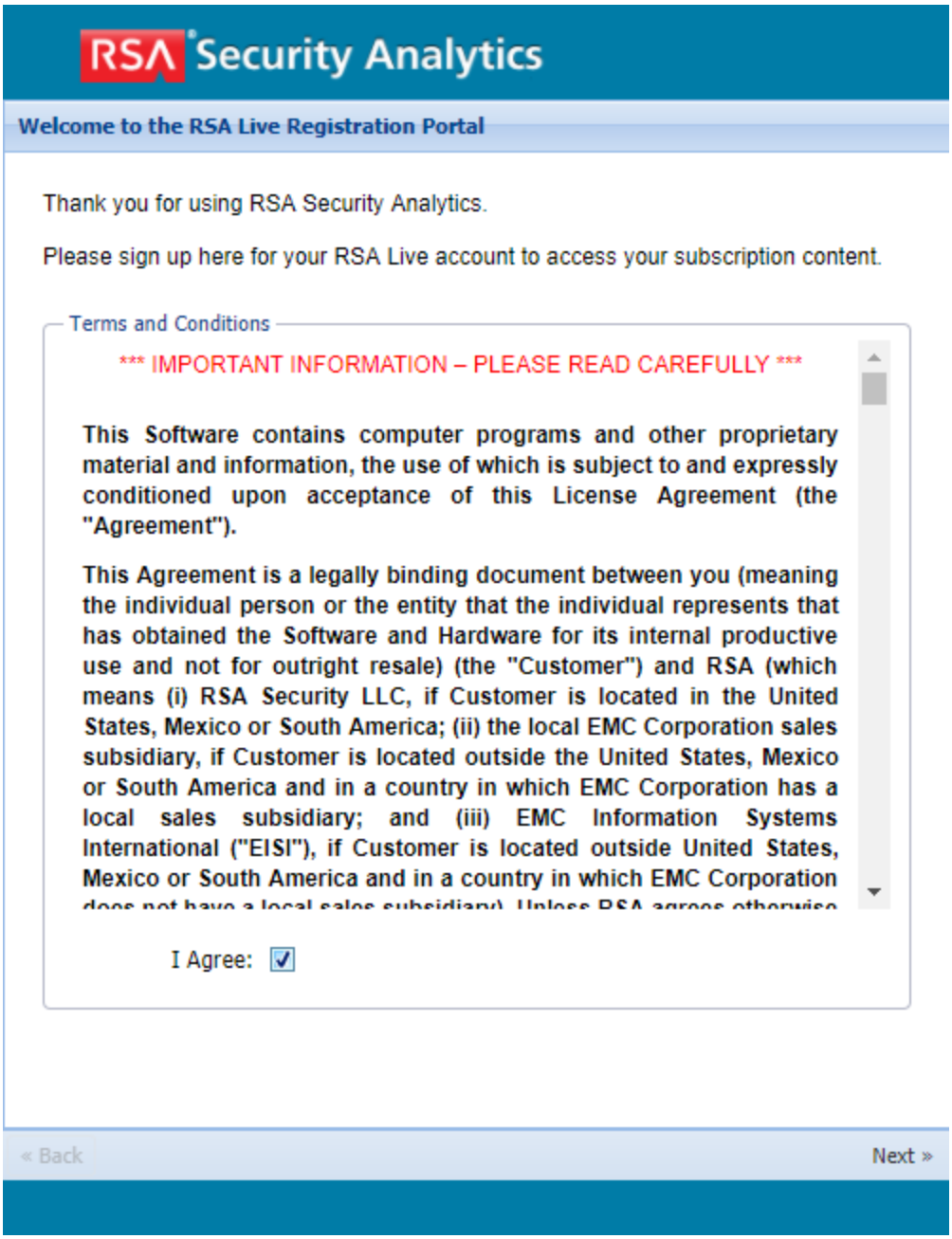
Make sure the following are available to set up a RSA Live account:

- Active internet connection to access the portal.
- A valid and registered NetWitness Suite License Server on the Flexera Server, before you can register for a Live account. You can view the License ID on the **ADMIN > System > Info** panel.

Note: If the License Server is not set up, contact RSA customer support.

To create a Live Account:

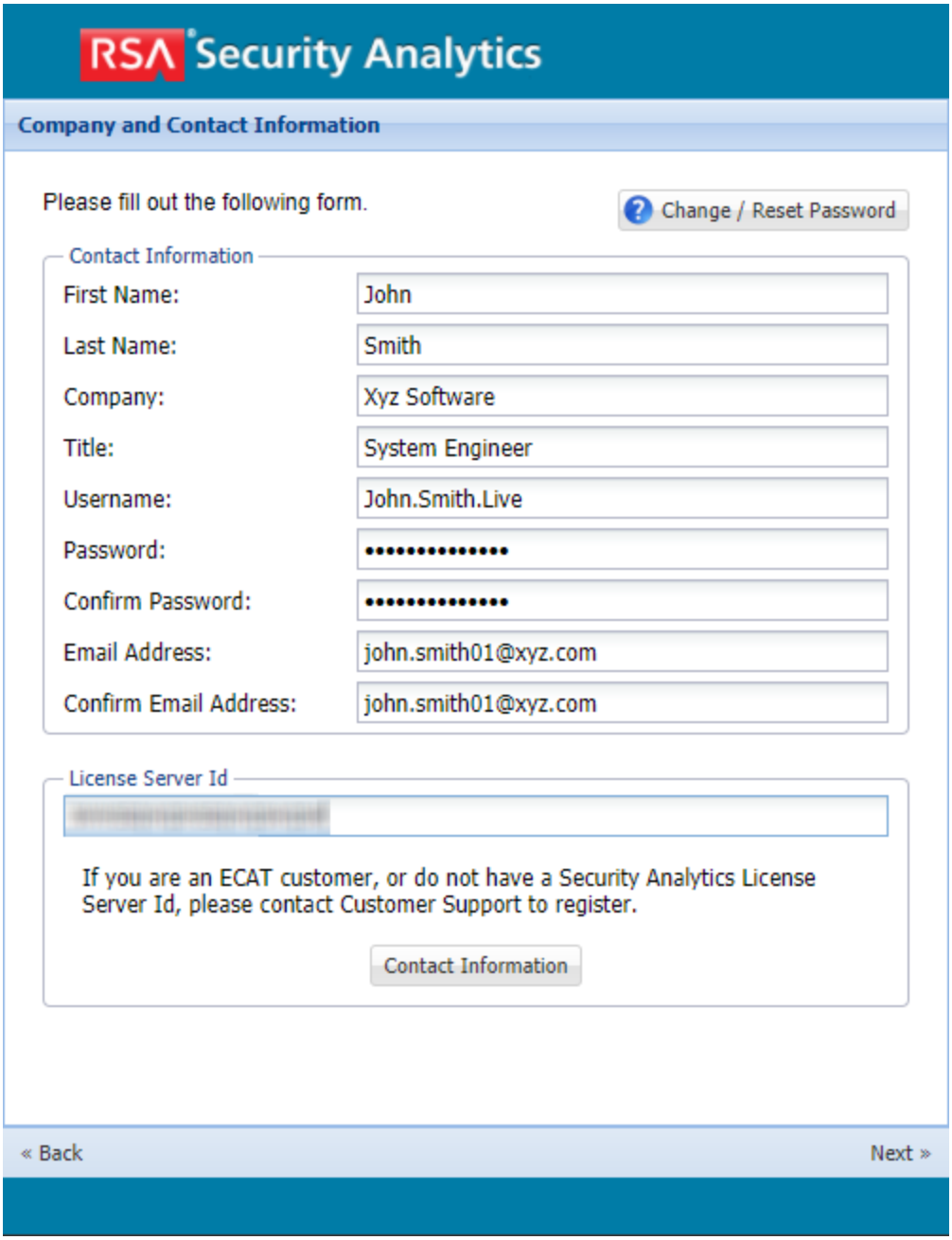
1. Access the RSA Live Registration Portal using the URL: https://cms.netwitness.com/registration/.
   The Welcome page is displayed.
2. Read the Terms and Conditions carefully and select the **I Agree** check box, as shown below:



3. Click **Next**.
4. In the **Contact Information** section, enter all the fields, as shown below:
   - The **username** must contain a minimum of nine characters and a maximum of 60 characters.
   - The **password** must contain a minimum of nine characters and a maximum of 60 characters, with at least one uppercase, one lowercase, one number, and one special

character.

- The **email address** you enter is used to send notifications related to your Live account.



5. In the **Subscription Level** section, select one of the following subscription levels:
   - **Basic** - This provides access to the Live content that is tagged for groups such as Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.
   - **Enhanced** - This provides access to the Live content that is tagged for groups such as Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.

- **Premium** - This provides access to the Live content that is tagged for groups such as Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.

6. In the **Confirm Subscription Level** section, select the subscription level once again to confirm.
7. Enter the **License Server Id**. You can view the License Id on the **ADMIN > SYSTEM > Info** page.

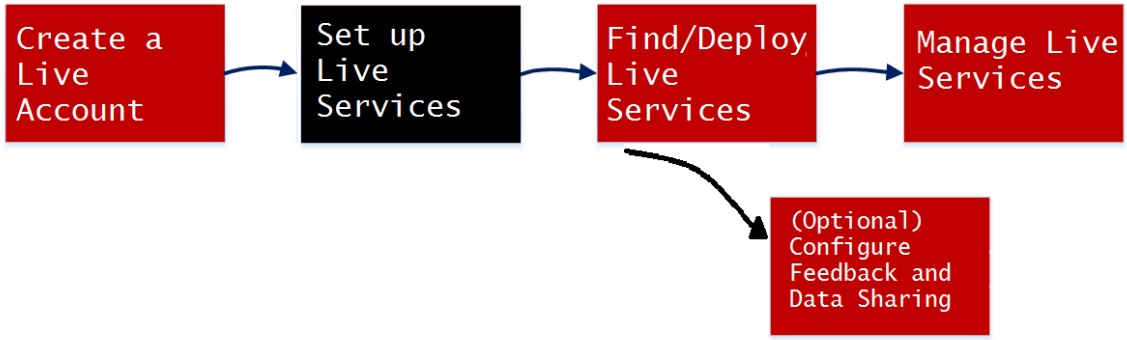
   Caution: Make sure that the license server ID on NetWitness Suite is valid and it is registered on the Flexera Server. If not, contact RSA Customer Support.

8. Click **Next**.

If the registration is successful you will receive RSA Live Account Confirmation email with your username. You now have access to the content subscribed.

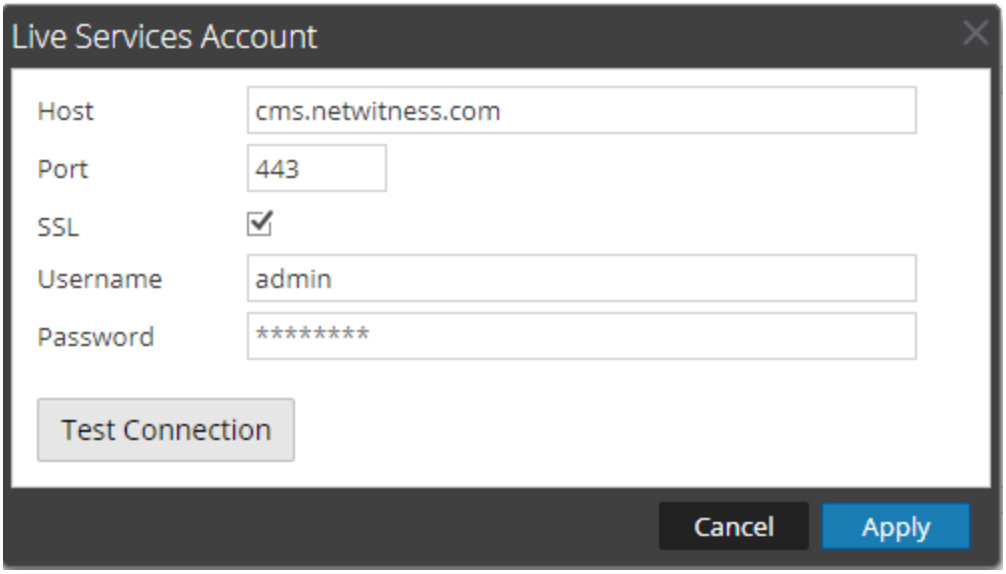
Set Up Live Services on NetWitness Suite

To set up Live on NetWitness Suite, you configure the connection and synchronization between the CMS server and NetWitness Suite. The user interface for this setup is the ADMIN > System > Live Services Configuration panel.



To configure the connection to the CMS Server:

1. Configure the connection to the CMS server and the Live account.

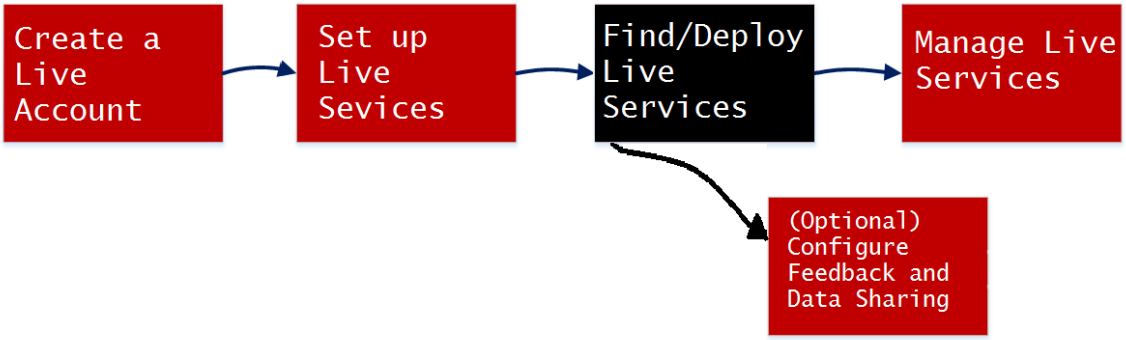


2. Configure the timing for synchronization of NetWitness Suite with updates from Live.

For more details, see the "Configure Live Services Settings" topic in the *System Configuration Guide*.

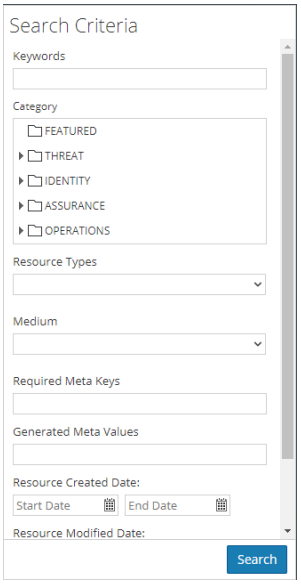
Find and Deploy Live Resources

Administrators can search for resources in the Live Search view, which is also the same as browsing the Live CMS for resources using the Search Criteria panel of the Live Search View.



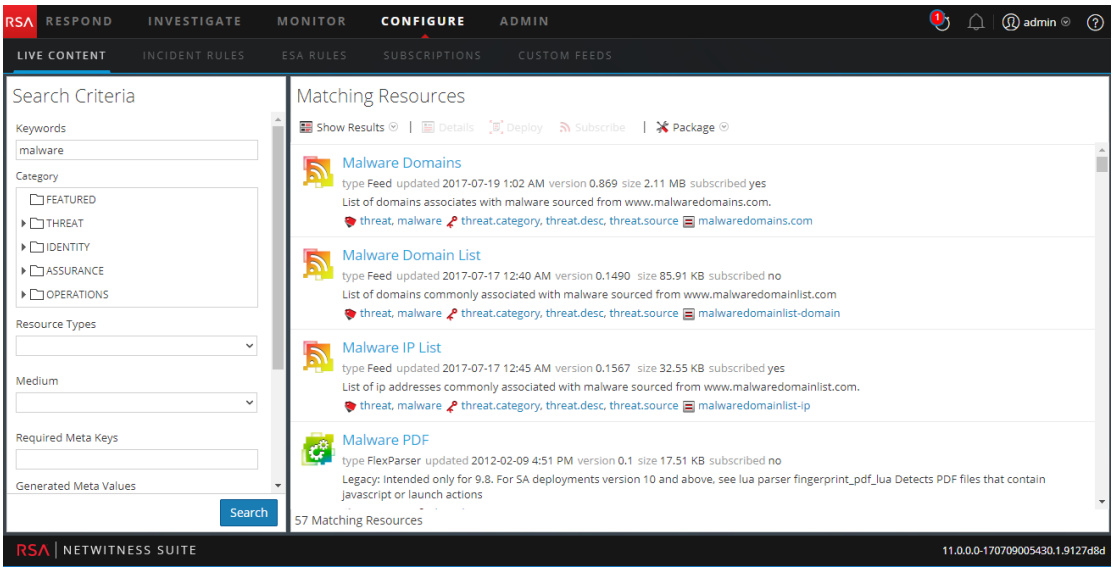
Find Resources

1. In the **Search Criteria** panel, specify search criteria. Enter any or all of these: keyword, category, type of resource, medium, meta keys, meta values, date resource was created, and date resource was modified.



2. Click **Search**.

   Detailed results are shown in the Matching Resources panel.



3. (Optional) To further narrow the results In the Matching Resources panel, click on a tag, meta key, medium or resource meta value in a result.

Deploy Resources in Live

In RSA NetWitness Suite, you can deploy selected resources manually, using the Deployment Wizard, or you can subscribe to a group of resources.

- When you have results from browsing resources in NetWitness Suite Live, you can deploy resources manually to a service or a service group without subscribing to the resources.
- Deploying resources manually deploys to services without taking advantage of the powerful resource management capabilities of NetWitness Suite. If you want to receive notification and updates for updated resources and be able to easily remove resources from a service, you must subscribe to resources in the Live Search view and deploy them in the Live Configure View.

For manual deployment, this is the basic procedure:

1. Select a resource or group of resources, or select a previously-created package of resources.
2. Click Deploy, which starts the Deployment Wizard.
3. Review the list of selected resources.
4. Select the Services or Service Groups on which to deploy the selected resources
5. Review your previous selections
6. Deploy

The following procedure describes how to deploy a group of resources or a resource package:

- You can select one or more resources in the Live Resource View , then deploy them to services.
- Or, if you have previously created and saved a resource package, you can deploy the package to services. Please refer to Resource Package Deployment Wizard for instructions on how to create a package.

To deploy resources manually:

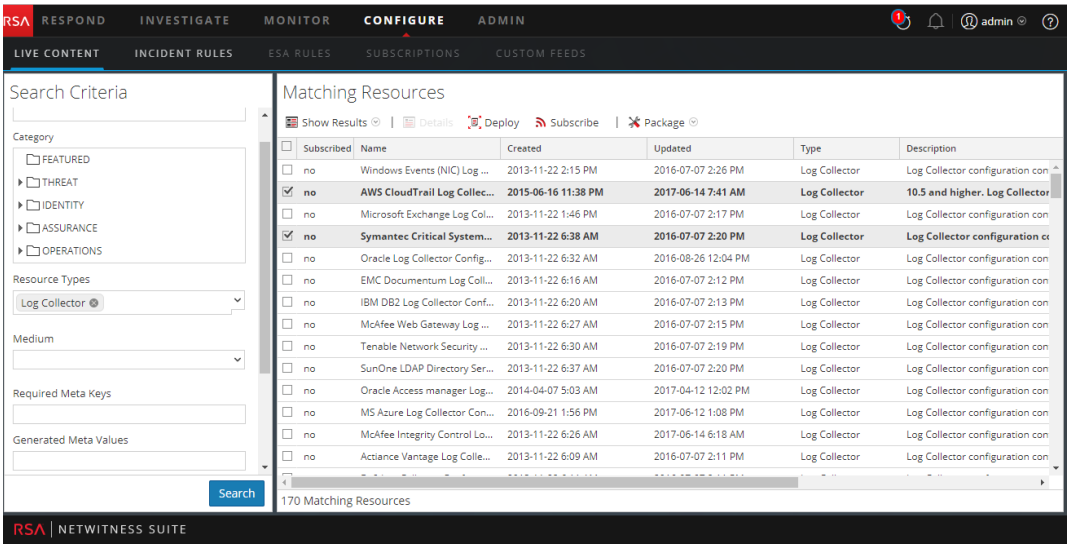
1. Go to **CONFIGURE > Live Content**.
2. Select a group of resources, or a previously created resource package.

   To select a resource or group of resources:

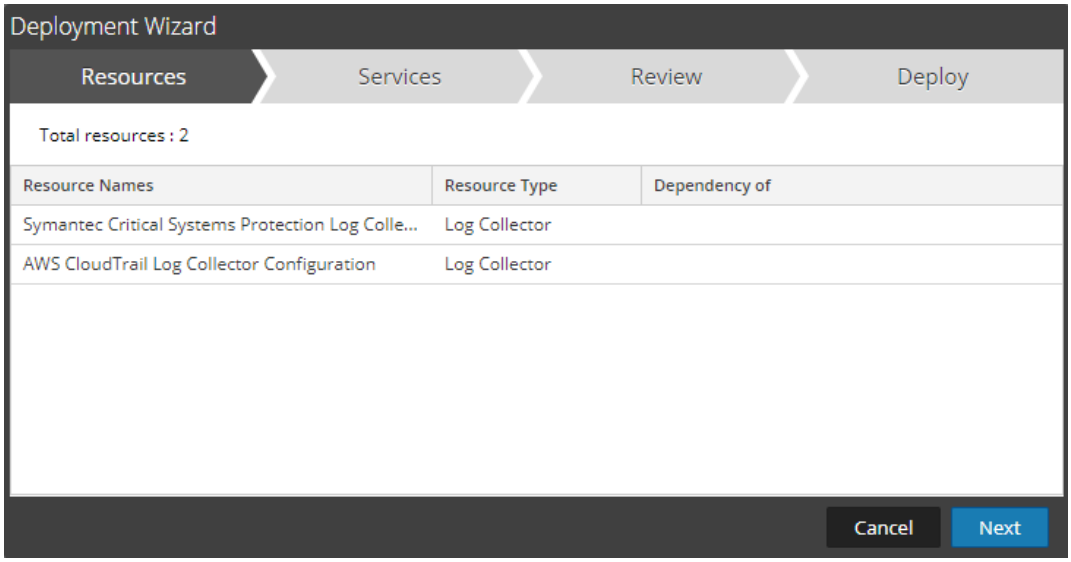
   a. In the **Live Search View,** browse Live resources (for example, search for the **Log Collector** resource Type).

   b. In the **Matching Resources** panel, select **Show Results > Grid**.

   c. Select the checkbox to the left of the resources that you want to deploy.



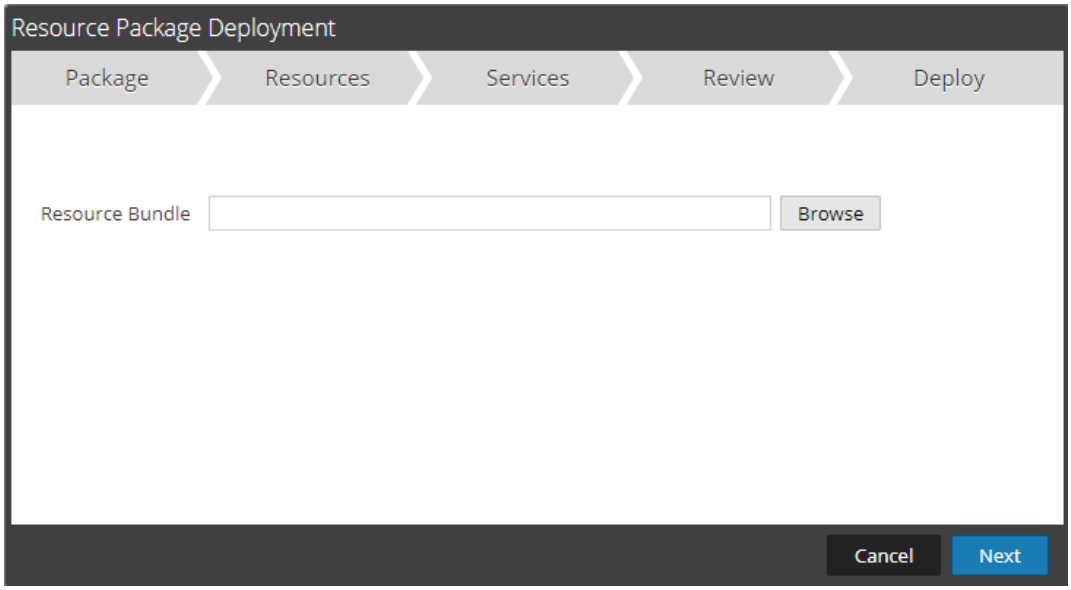
d. In the Matching Resources toolbar, click Deploy.



3. To select a resource package to deploy:

a. In the **Live Search** view **- Matching Resources** toolbar, select **Package** > **Deploy** :

The Package page of the Resource Package Deployment wizard is displayed.



b. Click Browse and select a package from your network (for example **resourceBundle-FeedsParsersContent.zip**).

c. Click **Open**.

At this point, whether you are deploying a package or a group of resources, the **Deployment Wizard** opens, and the **Resources** page is displayed.

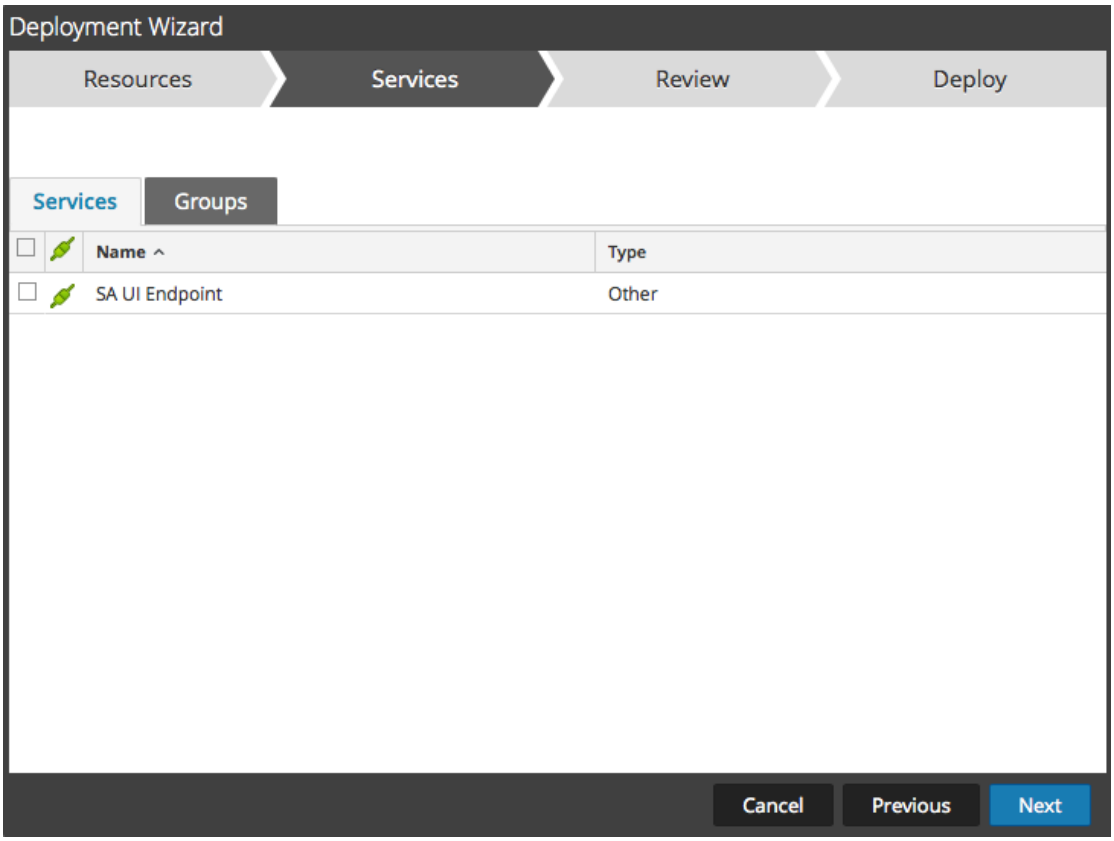
4. Click **Next**.

   The **Services** page displayed has two tabs, **Services** and **Groups**, which provide a list of services and service groups that are configured in the Admin > Services view. The columns are a subset of the columns available in the Services view.

   Note: The Live server is "smart" about deploying resources to Services. For example, it does not deploy resources that have a Medium of packets to any Log Decoders. This means that only applicable content resources are deployed to each Service.

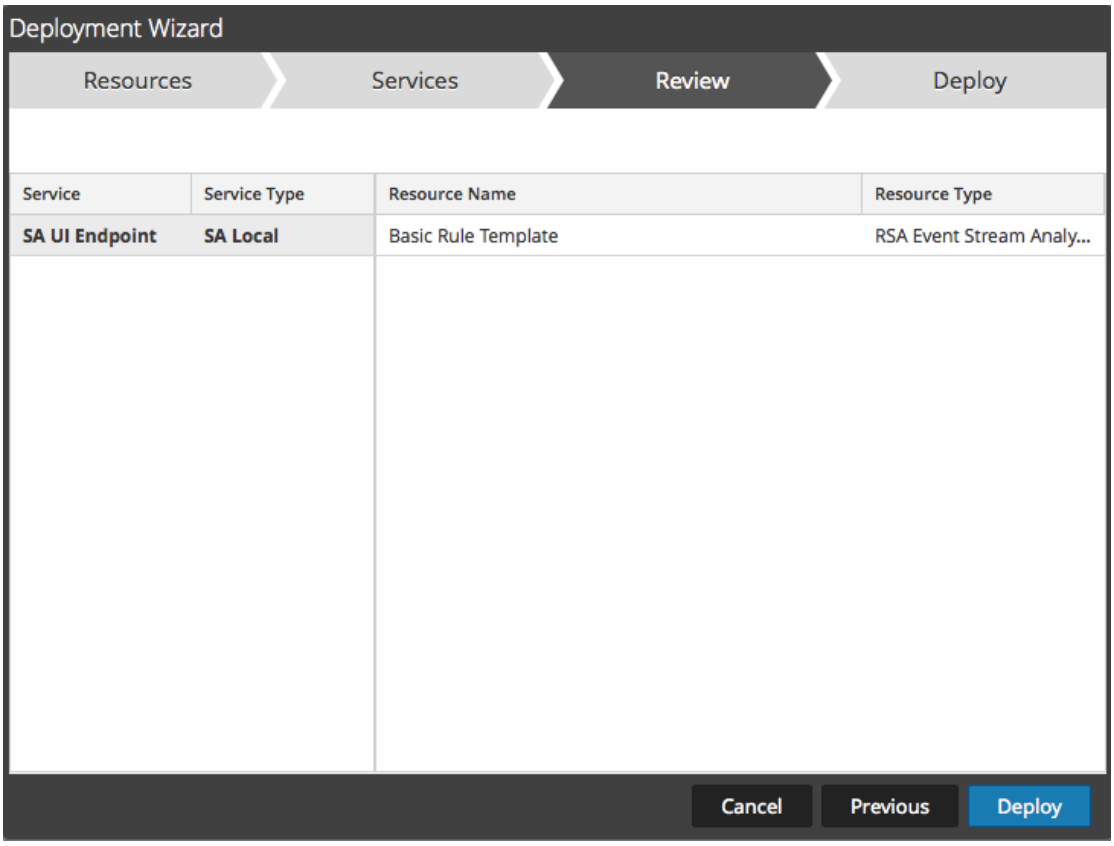
5. Select the services to which you want to deploy the content. You can select any combination of services and service groups.

   - Use the **Services** tab to select individual services, list of services and service groups that are configured in the ADMIN Services view.
   - Use the **Groups** tab to select groups of services



6. Click **Next**.

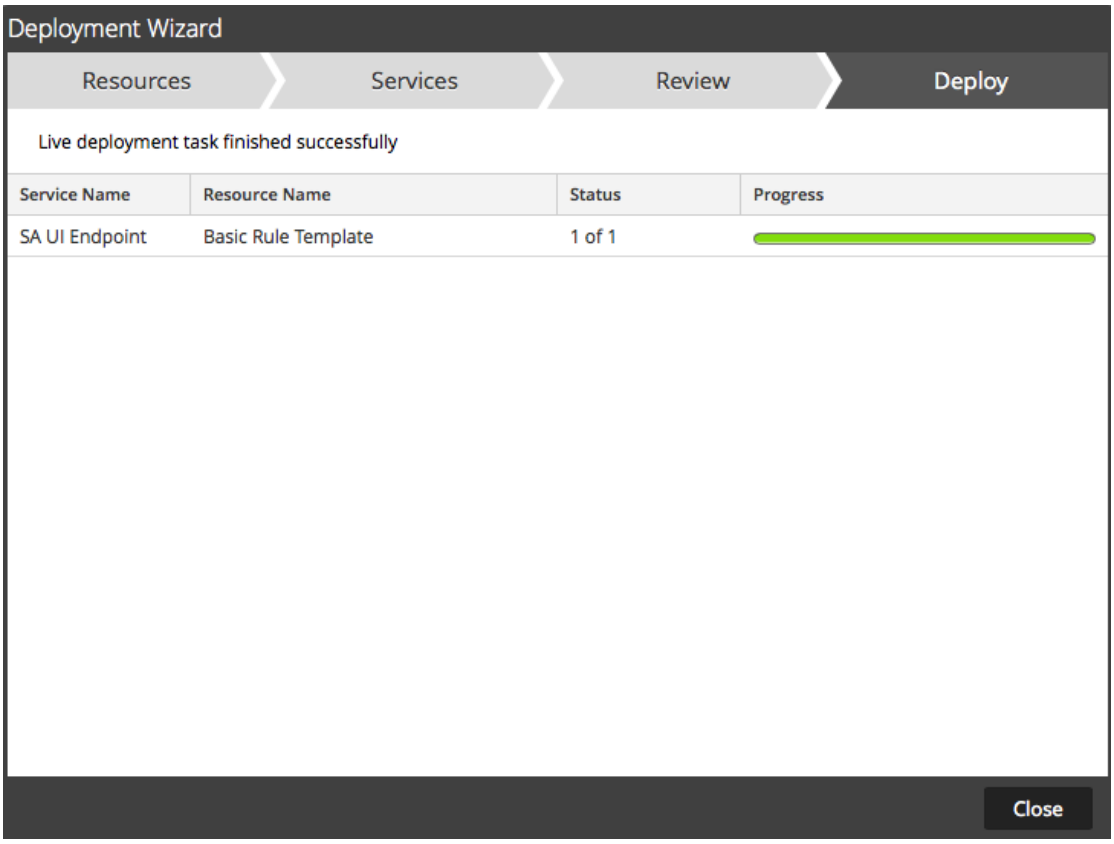
   The **Review** page is displayed.



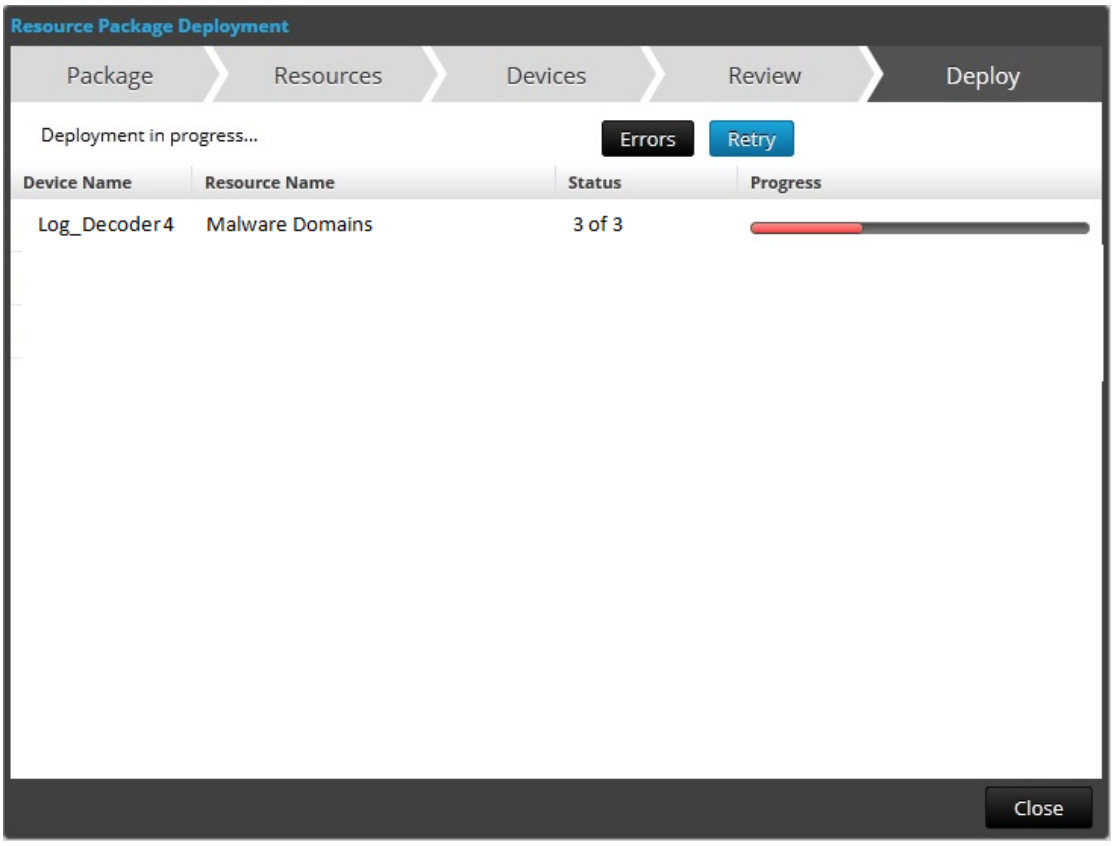
Make sure that you have selected correct resources and the services to which you want to deploy them.

7. Click **Deploy**.

   The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.



If you try to deploy resources and services that are not compatible, NetWitness Suite displays the Errors and Retry buttons, which you click to review the errors and re-attempt the deployment.



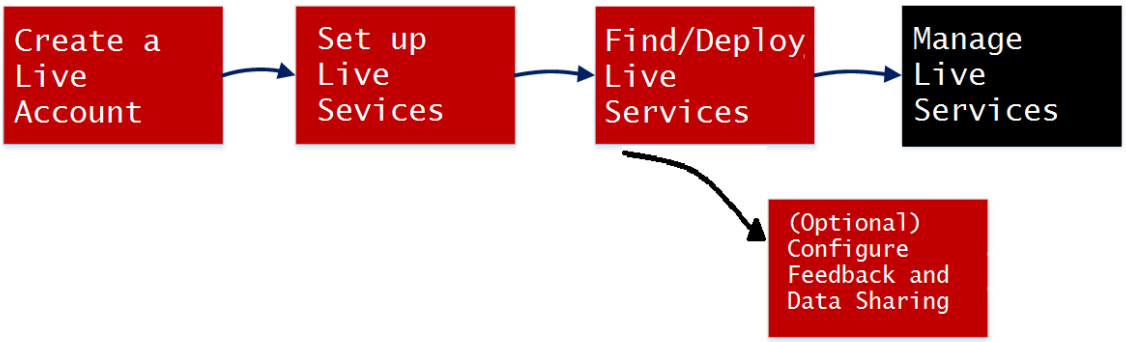
8. Click **Close**.

Next steps

After deploying parsers to Decoders and Log Decoders, you must enable parsers on the individual services as described in the *Decoder and Log Decoder Configuration Guide*.

Manage Live Resources

These procedures are required when administrators want to search for, subscribe to, and/or deploy resources from Live. With a connection to the CMS server, you can search for, subscribe to, and deploy resources from Live in accordance with your subscription level. Once you have found resources, you deploy them to services and service groups that have been configured in the Admin Services view.



Procedures

There are several possible workflows for deploying resources to services and managing those deployments. These include:

- Subscribe and deploy resources.
- Deploy a resource bundle.
- Remove deployments of resources.
- Download resources.
- Set up data feeds.

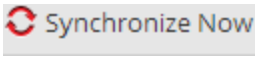
Manage Subscription and Deployment

The subscription and deployment workflow takes advantage of the resource management tools available in Live. By subscribing to resources, you agree to receive updated resources in accordance with the synchronization configured in the **ADMIN > Live Configuration** panel.

By adding subscribed resources to the deployments list, you configure NetWitness Suite to automatically push those resources to the selected services at the configured synchronization intervals. This method requires some planning of service groups and services where resources are deployed. In addition:

- You can remove a resource from the deployments list in the Deployments Tab.
- You can unsubscribe from a resource in the Subscriptions Tab and the Live Resource View.

To manage subscriptions and deployment:

1. In the **ADMIN > SYSTEM > Live** panel, specify an interval at which NetWitness Suite checks for updates to subscribed resources in Live and specify the email addresses of people to receive an email listing subscribed resources that have been updated.
2. In the **Live** > **Search** view, search for and subscribe to Live resources.
3. In the **Live** > **Configure** view > **Deployments** tab, select subscribed resources and add them to the deployment list for services groups.
4. (Optional) In the **ADMIN**> **SYSTEM**> **Live** panel, click 

to deploy the resources listed in the Deployments tab immediately.
5. In the **Live** > **Configure** view > **Deployments** tab, select deployed resources and remove them from services groups.
6. In the **Live** > **Configure** view > **Subscriptions** tab, unsubscribe from resources.

Remove a Deployed Resource

Once deployed to a service, Live resources remain on the service until removed. It is a good practice to remove unused resources from services on which they are deployed.

To remove resources, go to the Live Resource View, unsubscribe from a resource, and remove the resource from services where it is deployed.

Deploy a Resource Bundle

To deploy a content package, use the Resource Package Deployment Wizard. You can deploy a content package created in Live to one or more services. NetWitness Suite accepts packages in **.nwp** files or **.zip** files.

Download Resources

To download resources to your local file system, use the **Download** button in the Live Resource view.

Set Up Data Feeds

In the **Live** > **Feeds** view, you can set up and maintain Custom and Identify feeds.

Additional Procedures

This topic explains the additional procedures an administrator could choose to follow which are not essential for the configuration or use of Live Services.

- Export Data to RSA
- Packaging Resources
- Manage Custom Feeds
  - Create a Custom Feed
  - Create a STIX Custom Feed
  - Create and Manage an Identity Feed
  - Edit a Feed
  - Remove a Feed
- Miscellaneous Live Services Procedures

Export Data to RSA

A NetWitness Suite administrator can export the metrics in NetWitness Suite for Live Feedback.

About Live Feedback

If the Live Account is not configured, you can manually upload the usage data to RSA. For more information, see the "Configure Live Services Panel" topic in the *System Configuration Guide*.

In the Live Services Configuration panel, there is a Live Feedback Activity Log which enables you to download the usage data required for Live Feedback. This is active regardless of the Live Account configuration.

You can first download the Live Feedback historical data, and then upload it to share with RSA

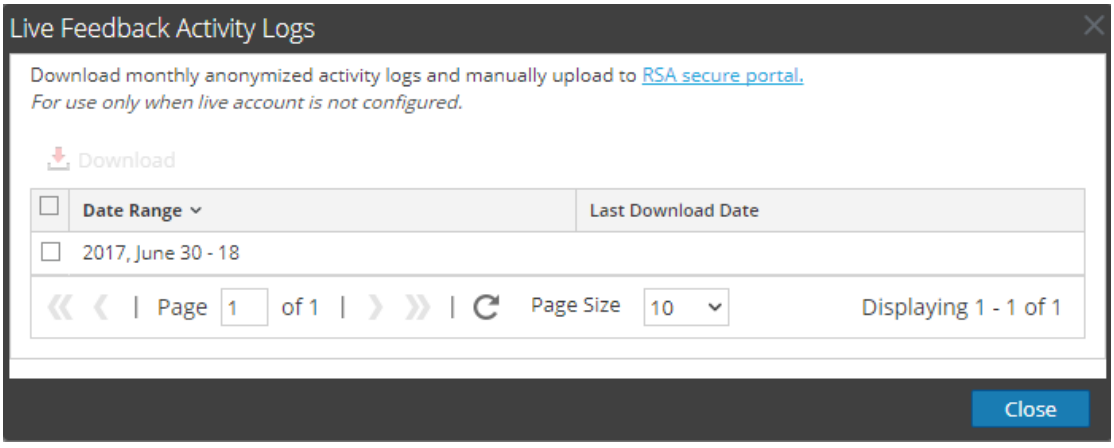
Download Live Feedback Historical Data

To download the Live Feedback historical data:

1. Go to **ADMIN** > **System**.
2. In the options panel, select **Live Services**.

   The **Live Account** screen is displayed which consists of the **RSA Live Status** and Download **Live Feedback Activity Log**.
3. Click **Download Live Feedback Activity Log**.

   The **Download Live Feedback Activity Log** window opens which allows you to download the required Live Feedback historical data.



4. Select one or multiple entries by selecting the checkboxes and click **Download**.

Note: If you select multiple entries in the history table, the downloaded zip file consists of an individual JSON file for each month.

The downloaded Live Feedback data is in JSON format, and is bundled as a .zip file. For more information, see "Live Feedback Overview" in the *System Configuration Guide*.

Share Data to RSA

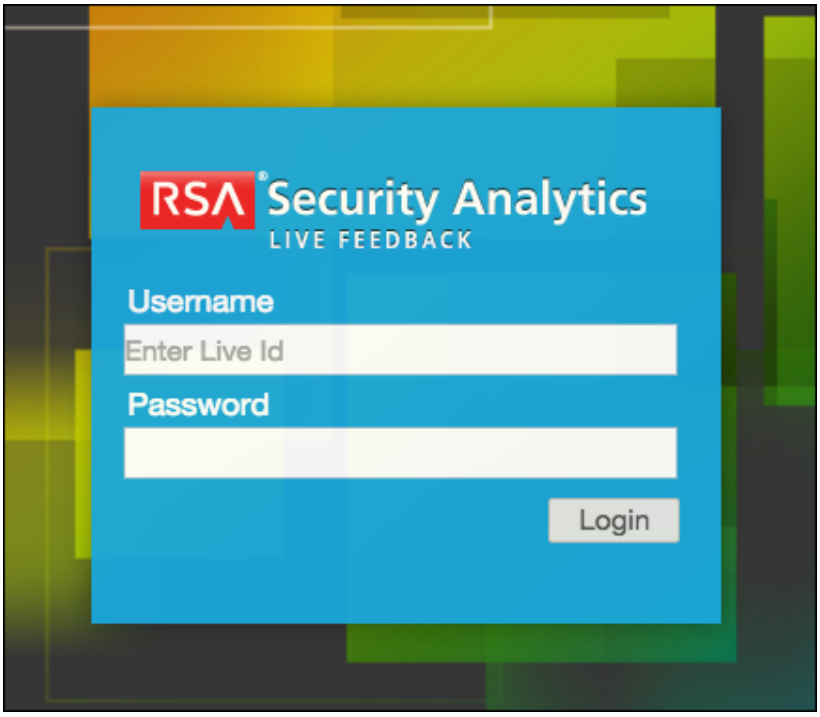
After you download the Live Feedback data, you can then upload it using the following procedure.

To share the data to RSA:

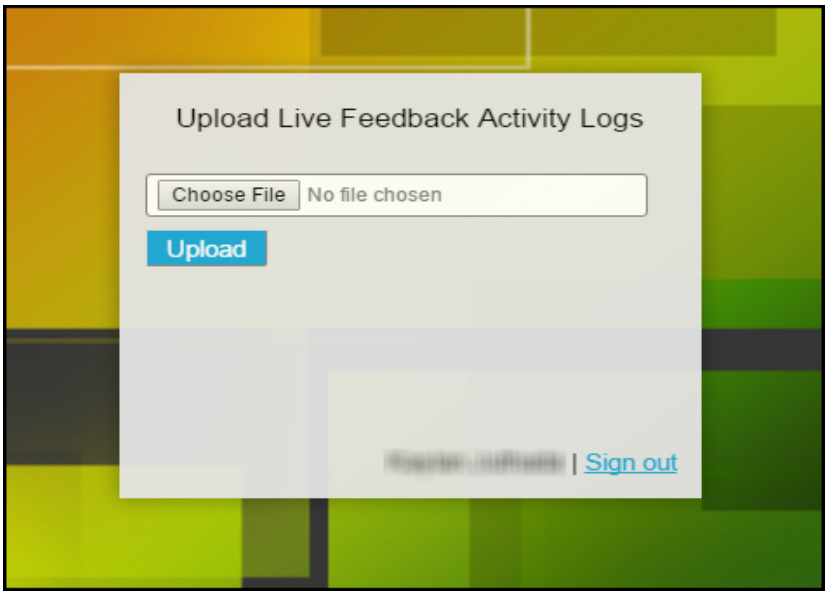
1. Click on the **RSA Secure Portal** available on the **Live Feedback Activity Logs** window.

   The RSA NetWitness Suite Live Feedback log on screen is displayed.

2. Log on to the Upload Live Feedback Activity Logs portal using your Live ID credentials.



3. Click **Download Live Feedback Activity Log**.



4. Click **Upload**.

Packaging Resources

The primary use for creating and subsequently deploying a resource package is for customers using an air gap network environment. In this case, you create a resource package on the network that is connected to the internet, and then deploy the resource package on the more secure network.

Create and Deploy Resource Package Use Case

The basic steps are as follows:

1. Access NetWitness Suite Live Services using an instance that is connected to the internet.
2. Create a Resource package as described below, adding whichever content items you need.
3. Copy the ZIP archive of the packages to your secure NetWitness Suite instance, by using a thumb drive or other manual copying process.
4. On the secure NetWitness Suite instance, deploy the resource package. Details for this procedure are in Resource Package Deployment Wizard.

Prerequisites to Create a Resource Package

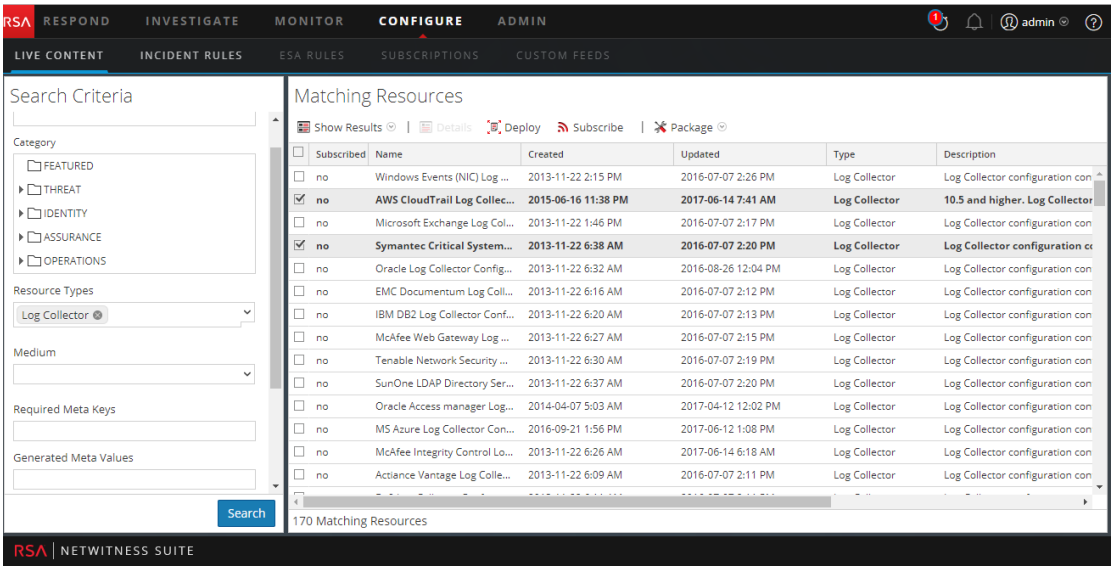
A prerequisite for creating resource packages is configuration of the connection and synchronization between the CMS server and NetWitness Suite and the ability to search for resources in the User Interface.

Procedure to Create a Resource Package

The following procedure creates a resource package, as a ZIP archive, which is saved to your local file system.

To create a resource package:

1. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
2. Select the resources that you want to package in the Matching Resources grid.



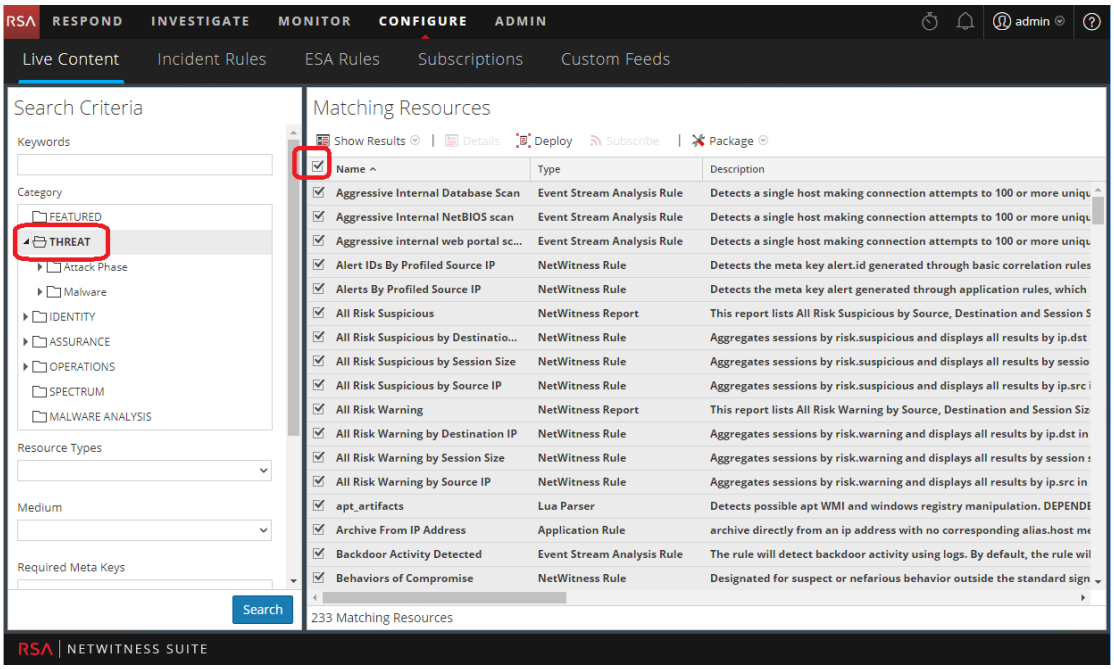
3. Select some or all of the resources that are listed in the Matches Resources pane.
4. Select Package > **Create**.

NetWitness Suite creates a **.zip** archive that contains the selected resources and downloads it to your default download folder. NetWitness Suite gives the package a generic name. You should rename it when you save it so that it identifies the resources contained in the package.

Example: Create Threat Package

In this example, we create a resource package that contains all the content that is categorized as **Threat**. Then we rename it, using the type of content and date.

1. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
2. From the **Category** section, select THREAT.
3. Select all items returned by clicking on the checkbox in the column header row of the **Matching Resources** pane.



4. Select Package > **Create**.

   A ZIP archive is saved to your Downloads folder. For example, **resourceBundle8740753704980701969.zip**.

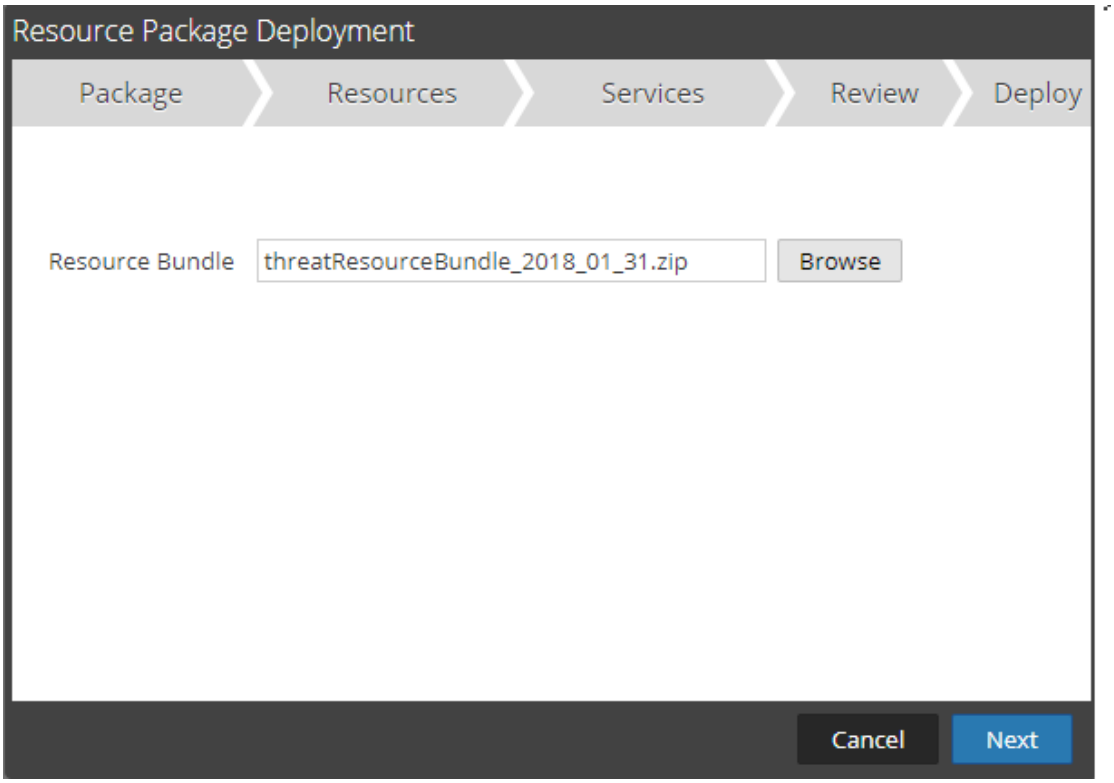
5. Rename the package to something meaningful. For example, in this case, you cold change the package name to **threatResourceBundle_2018_01_31.zip** (assuming today's date is January 31, 2018).

The resource package is now available for later deployment.

Example: Deploy Threat Package

Continuing the previous example, we deploy the resource package that we created.

1. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
2. In the **Matching Resources** pane, select Package > **Deploy**.
3. Click Browse and navigate to the **threatResourceBundle_2018_01_31.zip** file that we created earlier.



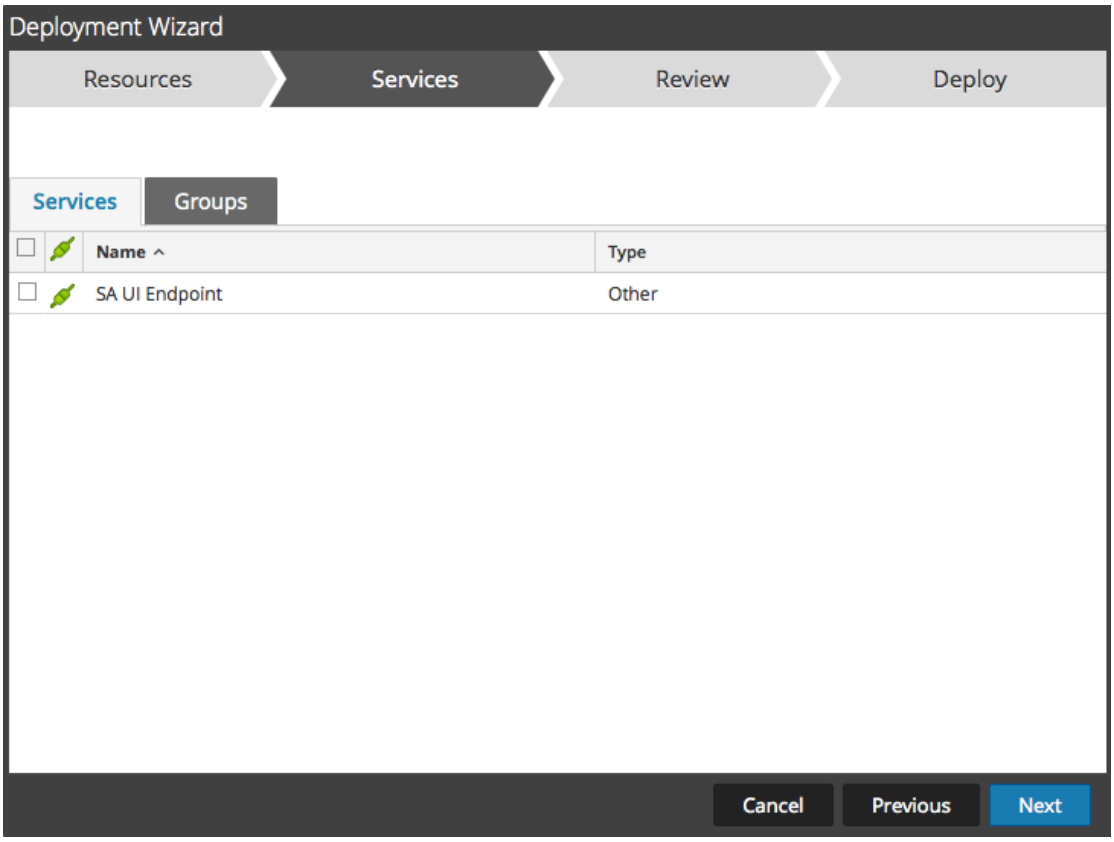
4. Click **Next**.

   The **Resources** page is displayed, showing details for the resources in the package.

5. Click **Next**.

   The **Services** page displayed has two tabs, **Services** and **Groups**, which provide a list of services and service groups that are configured in the Admin > Services view. The columns are a subset of the columns available in the Services view.

6. Select the services to which you want to deploy the content. You can select any combination of services and service groups.



Click **Next**.

The **Review** page is displayed.

Make sure that you have selected correct resources and the services to which you want to deploy them.

7. Click **Deploy** to complete the deployment process. Alternatively, you can choose **Cancel** or **Previous** to either cancel the deployment or go back to the previous screen.

Manage Custom Feeds

This topic introduces the custom feed capability, which is implemented using the Custom Feed Wizard in RSA NetWitness Suite, to quickly populate Decoders with custom and identity feeds.

Custom Feed Creation

You use the **Live** > **Feeds** > **Setup Feed** > **Configure a Custom Feed** wizard to quickly create and deploy Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides you through the process to create both on-demand and recurring feeds, you should understand the form and content of a feed file when you create a feed.

Feed file names in RSA NetWitness Suite are in the form `<filename>.feed`. To create a feed, NetWitness Suite requires a feed **data** file in `.csv` or `.xml` (for STIX) format and a feed **definition** file in `.xml` format, which describes the structure of a feed data file. The Configure a Custom Feed wizard can create the feed definition file based on a feed data file, or based on a feed data file and the corresponding feed definition file.

The files that you use to create an on-demand feed must be stored on your local file system. The files used to create a recurring feed must be stored at an accessible URL, whence NetWitness Suite can fetch the most current version of the file for each recurrence. After a NetWitness Suite feed is created, you can download the feed to your local file system, edit the feed files, and then edit the NetWitness Suite feed to use the updated feed files.

Sample Feed Definition File

This is an example of a feed definition file named `dynamic_dns.xml`, which NetWitness Suite creates based on your entries in the Feed wizards. It defines the structure of the feed data file named `dynamic_dns.csv`.

Note: The feed file path should be `.csv` regardless of the Feed Type (Default or STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
```

```
  truncdomain="true"/>

  <LanguageKeys>
           <LanguageKey name="threat.source" valuetype="Text" />
           <LanguageKey name="threat.category" valuetype="Text" />
           <LanguageKey name="threat.desc" valuetype="Text" />
  </LanguageKeys>

  <Fields>
  <Field index="1" type="index" key="alias.host" />
  <Field index="4" type="value" key="threat.desc" />
  <Field index="2" type="value" key="threat.source" />
  <Field index="3" type="value" key="threat.category" />
  </Fields>
  </FlatFileFeed>

</FDF>
```

Feed Definition Equivalents for Custom Feed Wizard Parameters

The NetWitness Suite Feeds wizard provide options to define the structure of the data feed file. These correspond directly to attributes in the feed definition (.xml) file.

NetWitness Suite Parameter	Feed Definition File Equivalent
Define Feed tab	
Feed Type	Select: **Default** - to define a feed based on a `.csv` formatted feed data file. **STIX** - to define a feed based on STIX formatted `.xml` file.
Feed Task Type	Select: **Adhoc** - to create an on-demand feed. **Recurring** - to create a feed that recurs automatically.
Name	The custom feed name in the feed data file. It corresponds to the **`flatfeedfile name`** attribute in the feed definition file; for example, Dynamic DNS Test Feed.
File/ Browse	This is the name of the feed data file. It corresponds to the **`flatfeedfile path`** attribute in the feed definition file; for example, dynamic_dns.csv.

NetWitness Suite Parameter	Feed Definition File Equivalent
(STIX, Recurring) **Trust All Certificate**	Select **Trust All Certificate**, if you do not want to validate the REST server certificate. This option is enabled by default (checked).
(STIX, Recurring) **Certificate/Browse**	For client authentication with the REST URL, in the **Certificate** field, click **Browse** and select the self signed certificate. The supported certificate formats are .cer, .crt with Base64 & DER encoded files.
	Define Feed tab - Advanced Options
XML Feed File	The name of the feed definition file, for example, `dynamic_dns.xml`.
Separator	The separator character used to separate attributes in the feed data file. It corresponds to the **`flatfeedfile separator`** in the feed definition file; for example, a comma.
Comment	The character used to identify a comment in the feed data file. It corresponds to the **`flatfeedfile comment`** attribute in the feed definition file; for example, #.
Remove STIX data older than	The number of days for which the STIX packages downloaded from TAXII server have to be stored. The STIX packages older than the specified number of days are deleted automatically. The default value is 180 days, which is also the maximum.
Select Services tab	Select the services to which you want to send the data feed.
(Define Columns tab, Define Index) **Type**	The type of lookup value in the index position of the feed data file. **IP** means that each row in the feed data file contains an IP address in the lookup value position. The IP value is in dotted-decimal format (for example, 10.5.187.42). **IP Range** means that each row in the feed data file contains a range of IP addresses in the lookup value position. The IP range is in CIDR format (for example, 192.168.2.0/24). **Non IP** means that the each row in the feed data file contains a metadata value other than IP address in the lookup value position. The Service Type and Truncate Domain, and Callback Keys fields become active for a Non IP index.

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Columns tab, Define Index) **CIDR**	Specifies that the IP value in the lookup position is in CIDR format. The **CIDR** attribute sets the IP address format in the field to Classless Inter-Domain Routing (CIDR) notation.
(Define Columns tab, Define Index) **Service Type**	For a Non IP index, the integer service type to filter meta lookups. It corresponds to **MetaCallback apptype** attribute in the feed definition file. A value of **0** indicates no filtering by service type.
(Define Columns tab, Define Index) **Truncate Domain**	For a Non IP index, for meta values that contain domain names (for example, hostnames), the system can strip off the host specific element in the data. Truncate Domain corresponds to the **MetaCallback truncdomain** attribute. If the value is www.example.com, it is truncated to example.com. A value of **False** selects no truncation, and **True** selects truncation.
(Define Columns tab, Define Index) **Callback Keys**	For a Non IP index, the available meta keys to match on instead of ip.src/ip.dst (the defaults for IP index type) are selectable from the drop-down list. The Callback Key corresponds to the **MetaCallback name** attribute, and the index column of the csv file must contain data that can match the chosen meta key. For example, if the username meta key is chosen, the index column of the csv file needs to be populated with users to be matched.
(Define Columns tab, Define Index) **Index Column**	Identifies the column in the feed data file that provides the lookup value for the row. Each position in each row of the feed data file is identified by a **Field index** attribute in the feed definition file. A field with an index of **1** is the first entry in a row, the second field has an index of **2**, the third field has an index of **3**, and so on. You can select multiple index columns, if the **Feed Type** is **STIX** and **Index Type** is **Non IP**. When you select multiple index columns the values from all the selected columns are merged in the first index column that you selected.

NetWitness Suite Parameter	Feed Definition File Equivalent
(DEFINE VALUES) **Key**	The name of the **LanguageKey**, as defined in the feed definition file, for which meta is created from this row of the feed data file. It corresponds to the **Field key** attribute in the feed definition file. A key applies only to a field whose type is set to **value**. In the feed definition file, there is a list of LanguageKeys from **index.xml**, or a summary name if Source Name and Destination Name are used. For example, **reputation** is a summary name for **reputation.src** and **reputation.dst**). This value is referenced by the Field key attribute.

Next steps

- Create a Custom Feed
- Create and Manage an Identity Feed
- Edit a Feed
- Remove a Feed

Create a Custom Feed

This topic provides instructions for creating a custom feed using a .csv or STIX formatted feed data file in RSA NetWitness Suite.

Note: From 10.6.1 or later, NetWitness Suite supports Structured Threat Information Expression (STIX). For more information about STIX and creating a STIX custom feed, see Create a STIX Custom Feed.

You can easily create a custom feed using the Custom Feed wizard. To complete this procedure, you need a feed data file in `.csv`or `.xml` format. If you also have an associated feed definition file in `.xml` format, which describes the structure of the feed data file, you can use the feed definition file to create a feed. The Custom Feed wizard can create the feed based on a feed data file, or based on a feed data file and corresponding feed definition file.

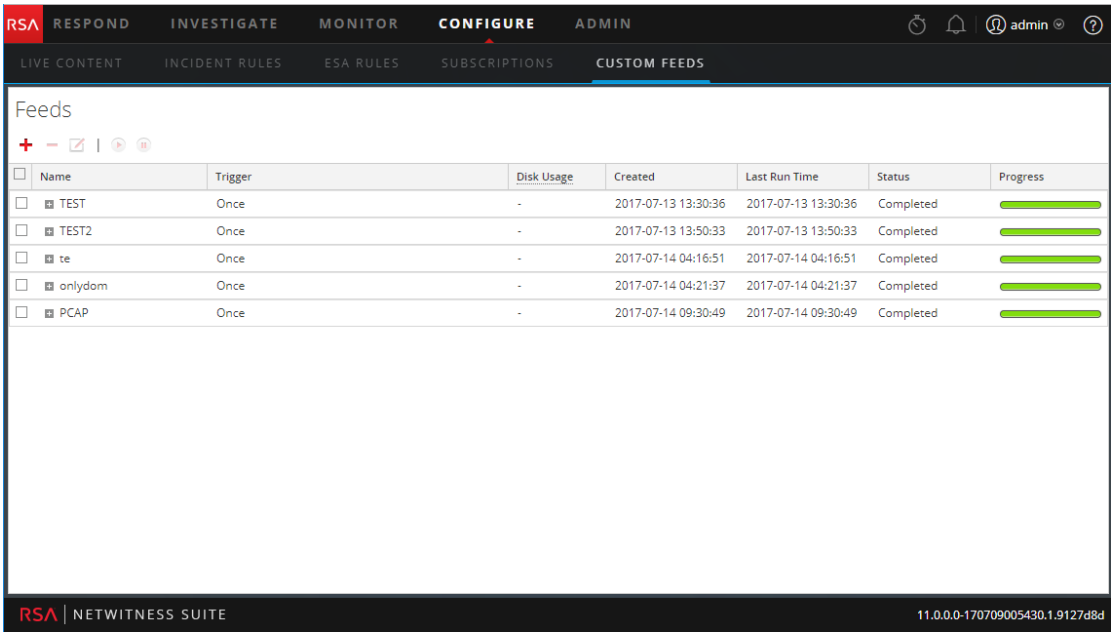
After completing this procedure, you will have created a custom feed.

The feed data file (`.csv` or STIX (`.xml`)) and optionally the feed definition file (`.xml`) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness Suite server.

To create a custom feed:

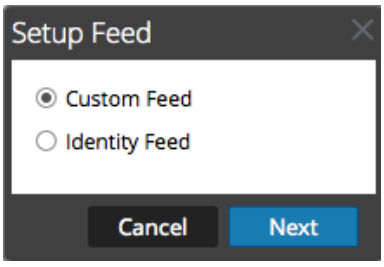
1. Go to t **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



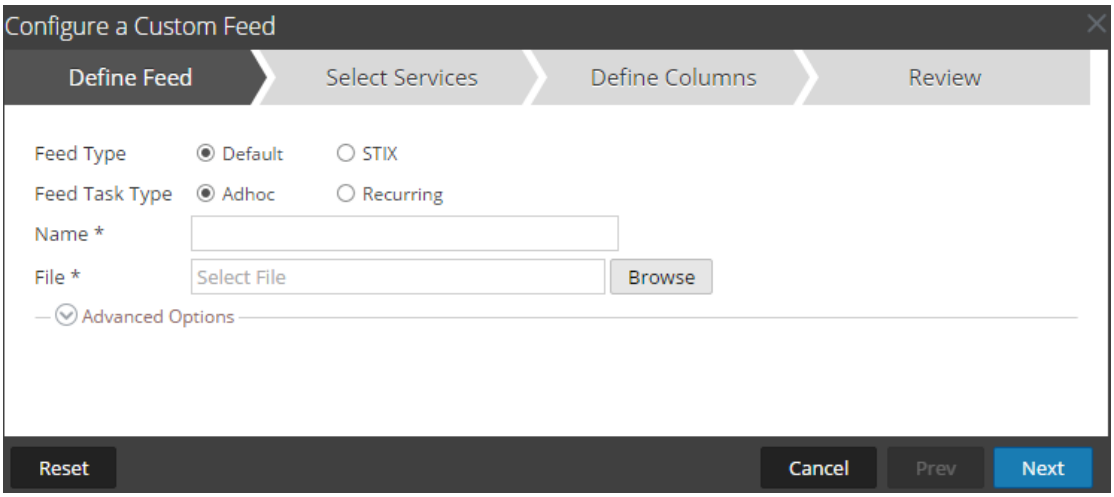
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.



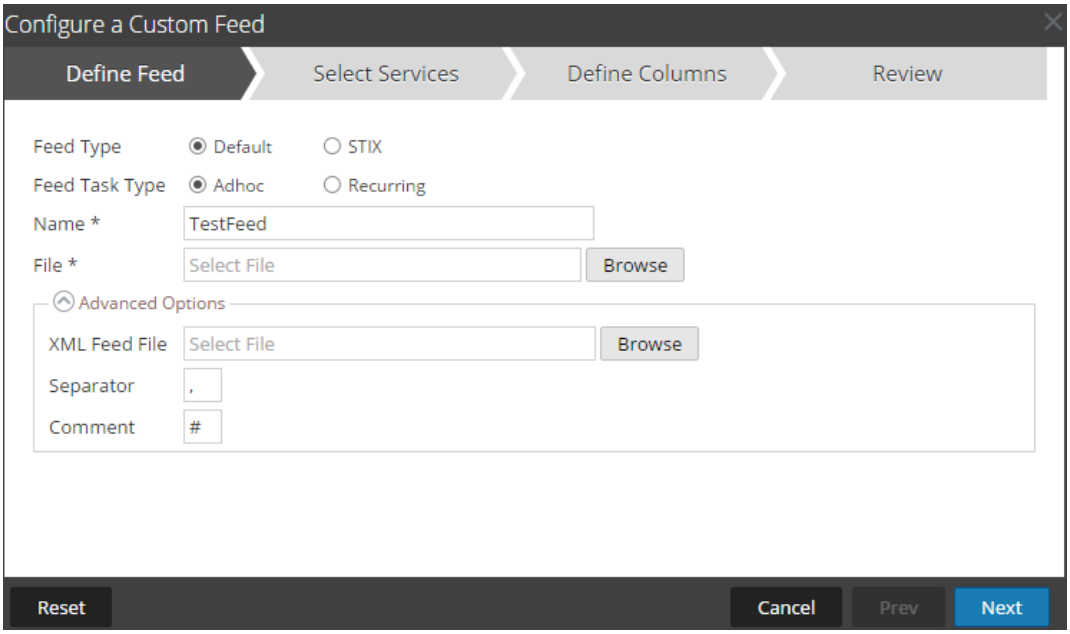
3. To select the feed type, click **Custom Feed** and **Next**.

   The Configure a Custom Feed wizard is displayed, with the Define Feed form open.



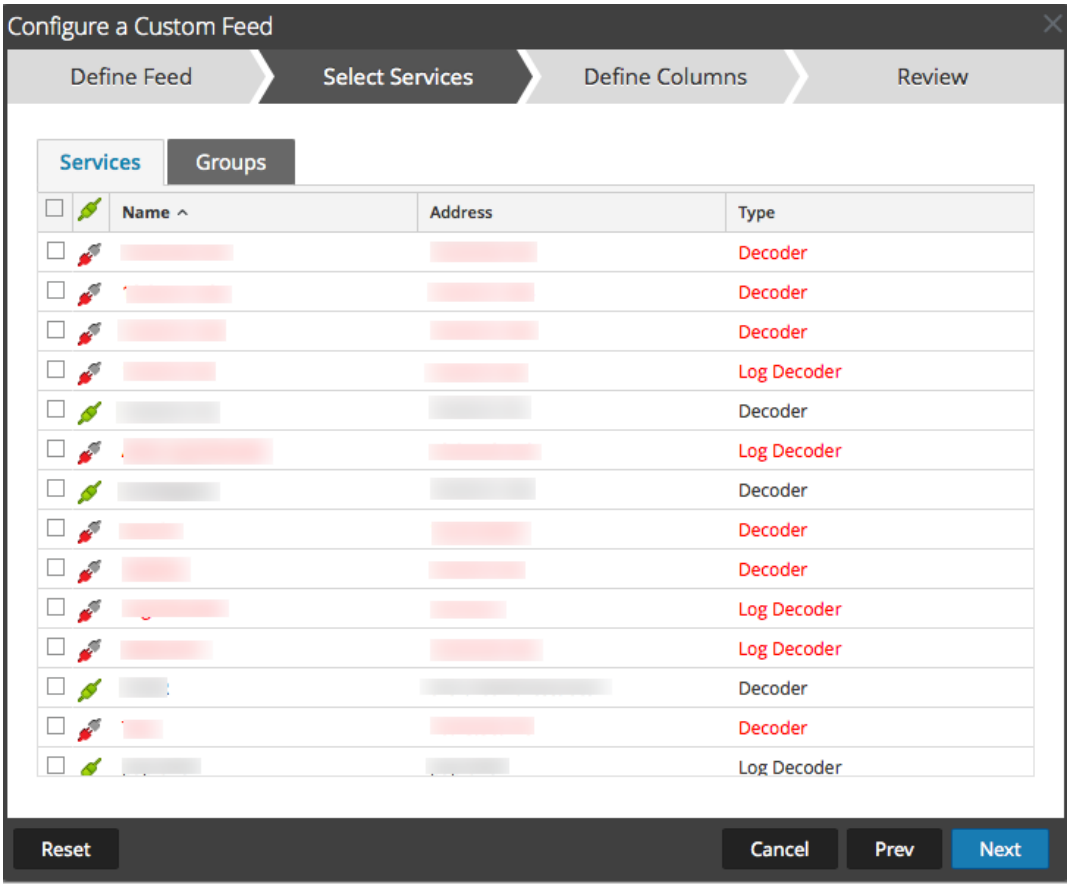
4. To define a feed based on a `.csv` formatted feed data file, select **Default** in the **Feed Type** field.
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on a .csv formatted feed data file, type the feed **Name**, select a .csv content **File** from the local file system, and click **Next**.
   b. (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

      The Advanced Options are displayed:



c. Select an XML feed file from the local file system, choose the **Separator** (default is comma), and specify the **Comment** characters used in the feed data file (default is #), and click **Next**.

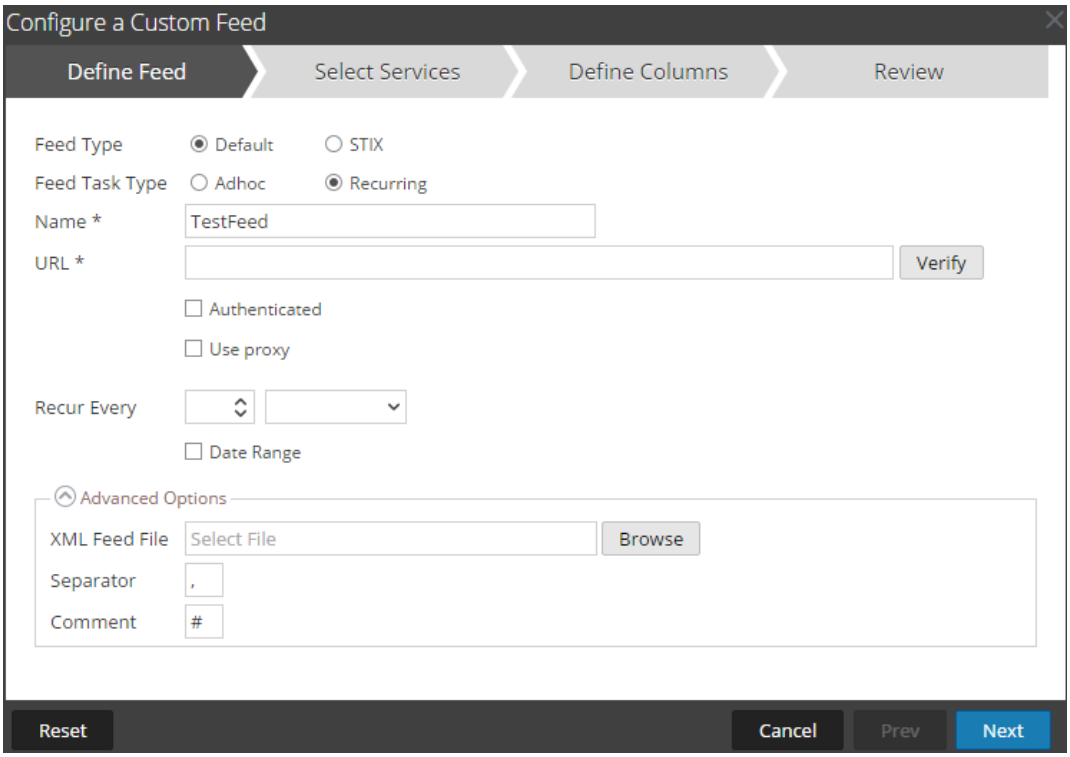
d. The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

a. Select **Recurring** in the **Feed Task Type** field.

The Define Feed form includes the fields for a recurring feed.



b. In the **URL** field, enter the URL where the feed data file is located, for example, `http://<hostname>/<feeddatafile>.csv`, and click **Verify**.

   NetWitness Suite verifiies the location where the file is stored, so that NetWitness Suite can check for the latest file automatically before each recurrence.

c. (Optional) If the URL has restricted access and requires authentication using your username and password, select **Authenticated**.

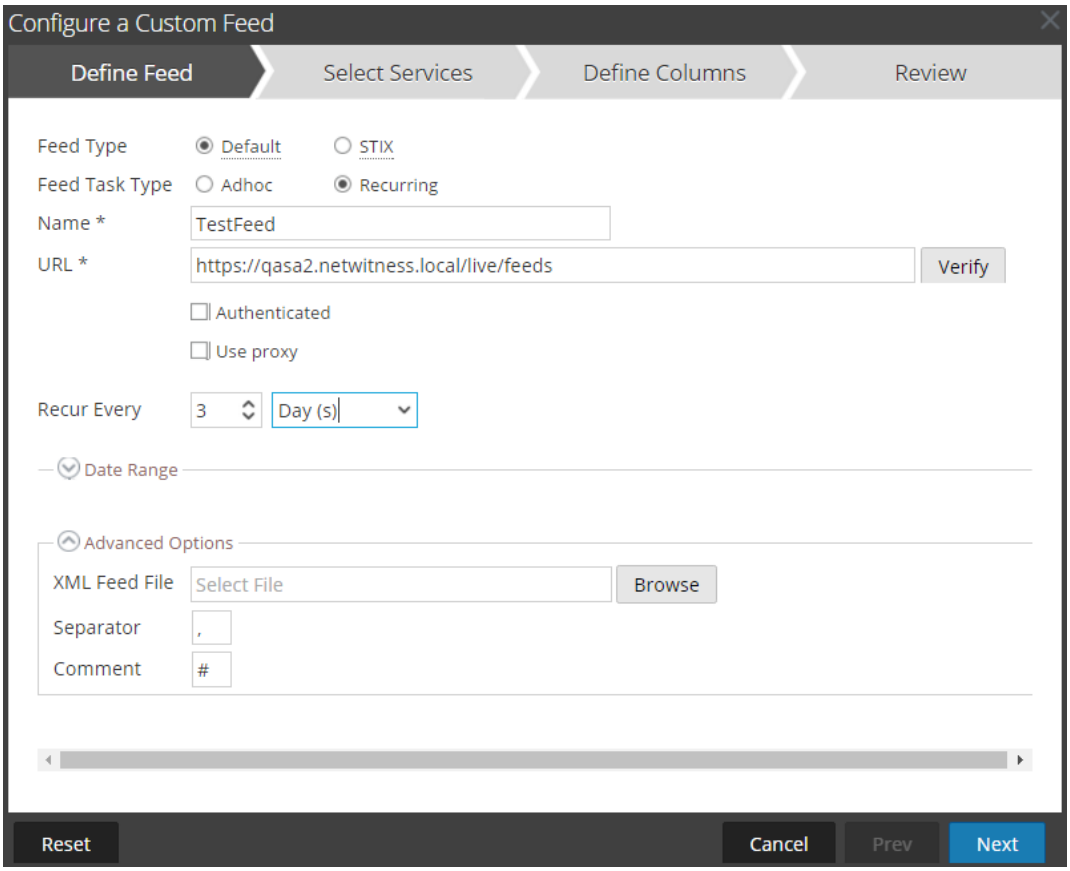
   NetWitness Suite provides your user name and password for authentication to the URL.

d. If you want the NetWitness Suite server to access the Feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see the **Configure Proxy for NetWitness Suite** topic in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

e. To define the interval for recurrence, do one of the following:

   - Specify the number of minutes, hours, or days between recurrences of the feed.
   - Specify recurrence every week, and select the days of the week.

f. To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.



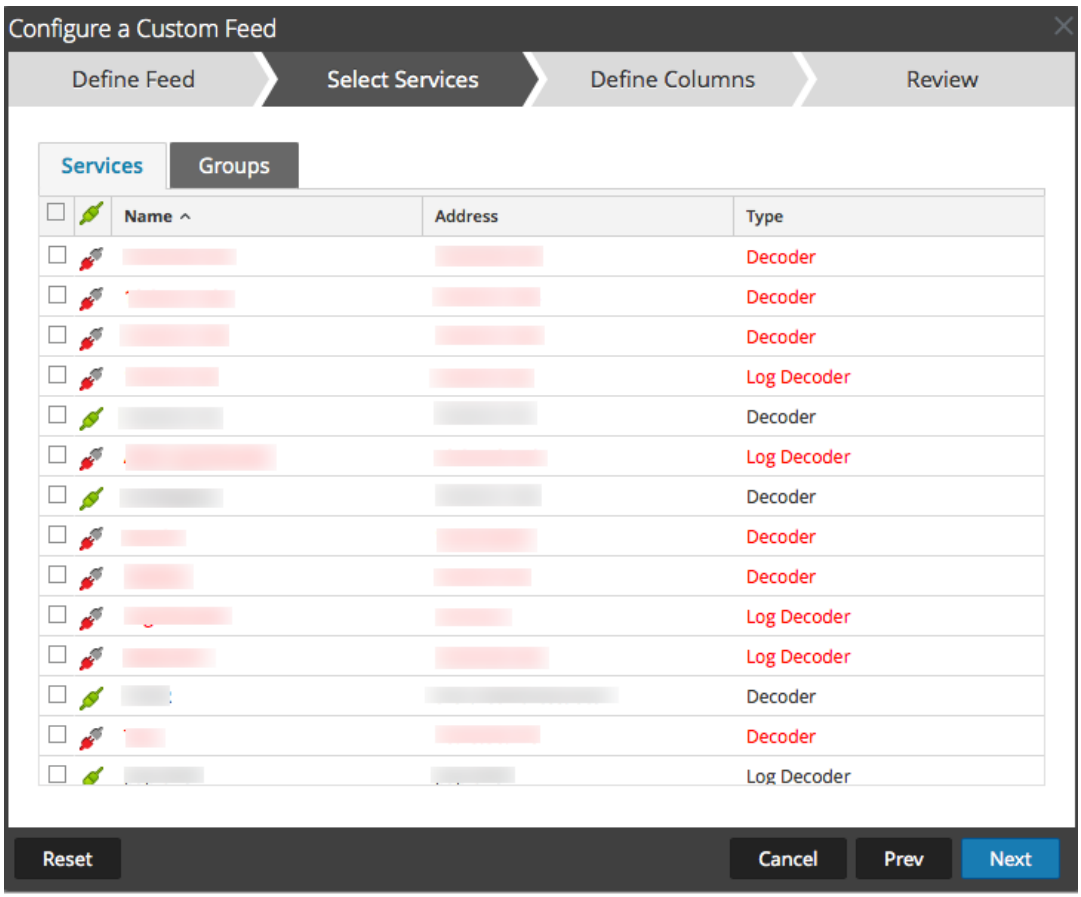
7. (Conditional) If you want to define a feed based on an XML feed file:

   - Type the feed **Name**, select **Advanced Options**.

     The Advanced Options fields are displayed.

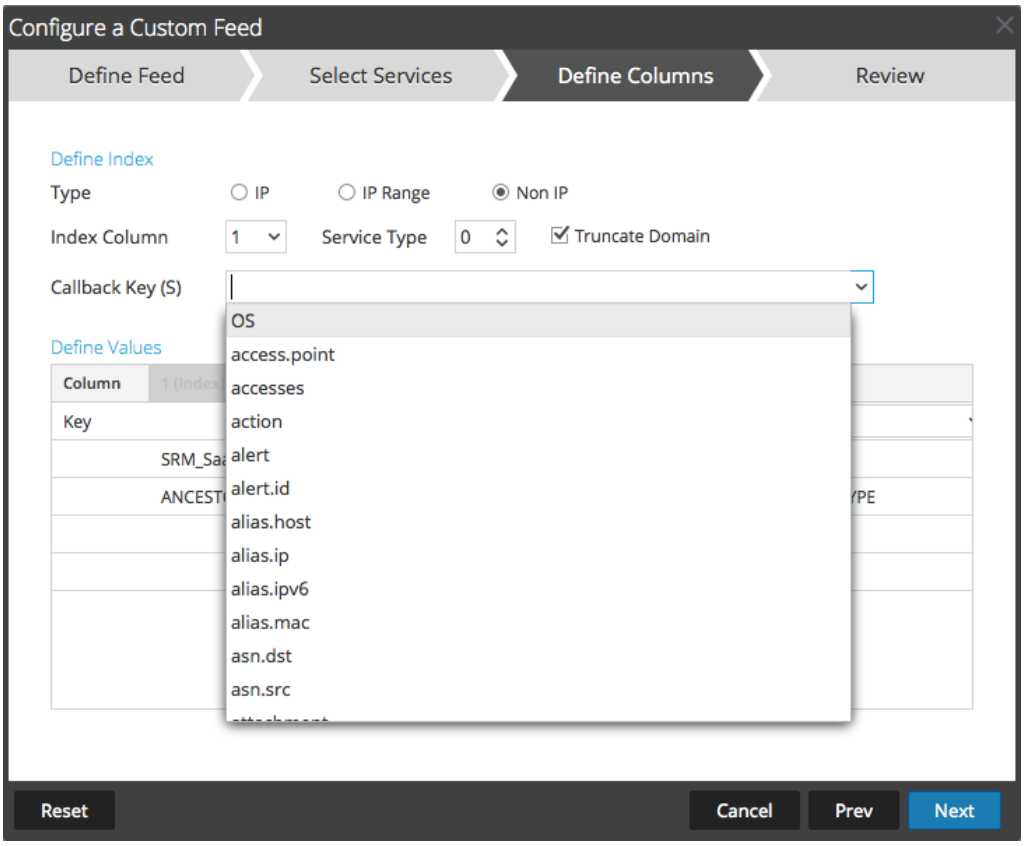
   - Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #) and click **Next**.

The Select Services form is displayed.

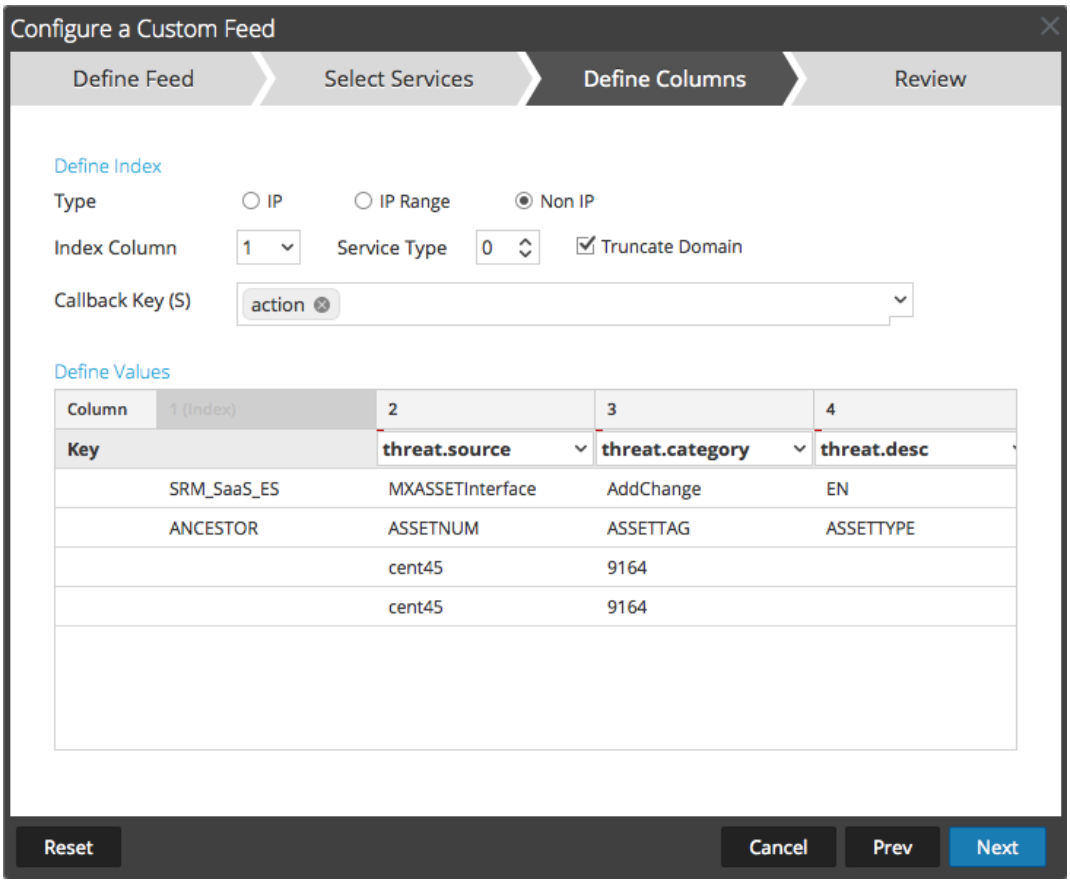


8. To identify services on which to deploy the feed, do one of the following:
   a. Select one or more Decoders and Log Decoders, and click **Next**.
   b. Click the **Groups** tab and select a group. Click **Next**.

      The Define Columns form is displayed.
9. To map columns in the Define Columns form:
   a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.
   b. (Conditional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR.**
   c. (Conditional) If the index type is **Non IP**, additional settings are displayed. Select the service type and **Callback Keys,** and optionally select the **Truncate Domain** option.

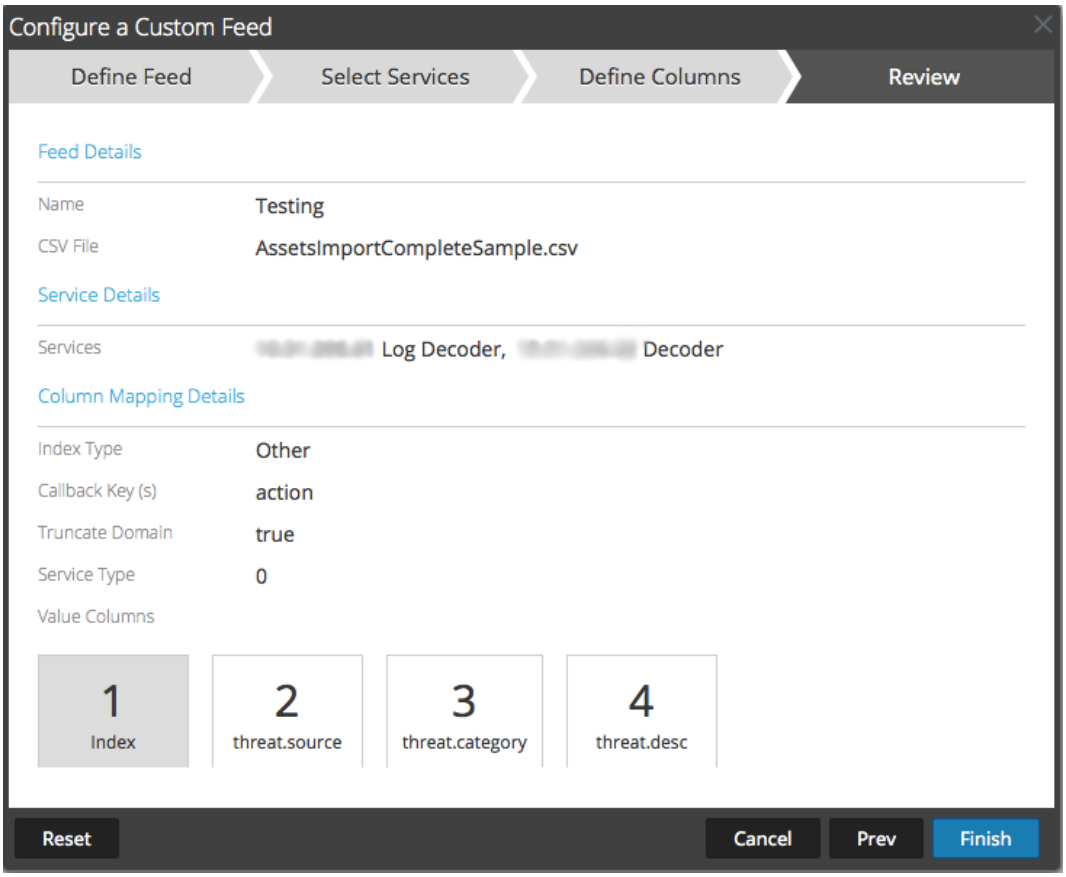


d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.



e. Click **Next**.

The Review form is displayed.



10. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form).

11. Review the feed information, and if correct, click **Finish**.
12. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.

MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6

This section describes how to use CIDR index ranges for IPv4 and IPv6 in custom MetaCallback feeds. As with other custom feeds, you must create feed data file in .csv format, and a feed definition file in .xml format.

Note: Using MetaCallback feeds with CIDR index ranges is supported only through the Advanced Configuration wizard or the REST interface.

The following example shows the contents of both a .csv file and an .xml file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

.csv file:

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
        <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">
                <Meta name="ip.dst"/>
        </MetaCallback>
        <LanguageKeys>
                <LanguageKey name="alert" valuetype="Text" />
        </LanguageKeys>
        <Fields>
                <Field index="1" type="index" range="cidr"/>
                <Field index="2" type="value" key="alert" />
        </Fields>
</FlatFileFeed>
</FDF>
```

Note: To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.

Create a STIX Custom Feed

You can create a custom feed using a .csv or STIX formatted feed data file in RSA NetWitness Suite.

Note: NetWitness Suite supports Structured Threat Information Expression (STIX) 1.0, 1.1 and 1.2 versions only.

Note: From 10.6.1 or later, Security Analytics supports Structured Threat Information Expression (STIX).

Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. For more information about STIX, see https://stixproject.github.io/.

Caution: If STIX recurring feed is configured and you update Security Analytics from 10.6.x to NetWitness Suite 11.0, you must re-configure the STIX recurring feed.

In NetWitness Suite, STIX (`.xml`) feed of type Indicator or Observable which contains the properties such as the IP addresses, File hashes, Domain names, URIs and Email addresses are supported. The properties values in the Equals operator is only supported. And, the attributes such as Type and Title are also read from the STIX (`.xml`). The STIX (`.xml`) with a single STIX_Package is only supported.

TAXII (Trusted Automated eXchange of Indicator Information) is the main transport mechanism for cyber threat information represented in STIX. Using the TAXII services, organizations can share cyber threat information in a secure and automated manner.

The STIX and TAXII communities work closely together to ensure that they continue to provide a full stack for sharing threat intelligence.

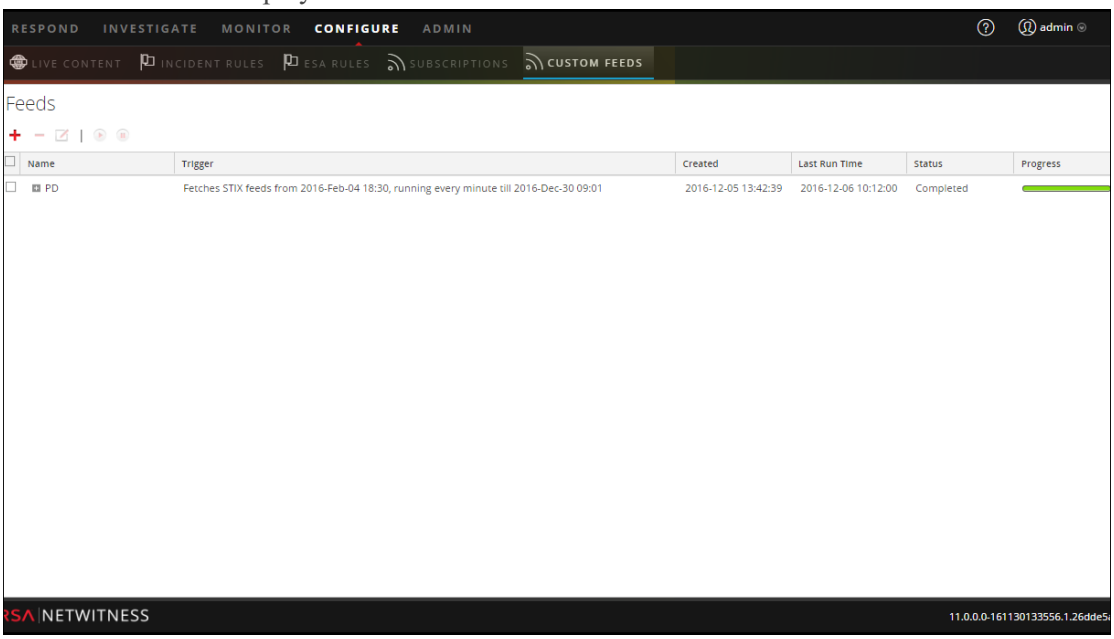
Apart from TAXII server, STIX data can also reside on REST server and you can fetch STIX file from the REST server by providing the URL of the REST server. For example, http://stixrestserver.internal.com.

The feed data file (`.csv` or STIX (`.xml`)) and optionally the feed definition file (`.xml`) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness Suite server.

To create a STIX custom feed:

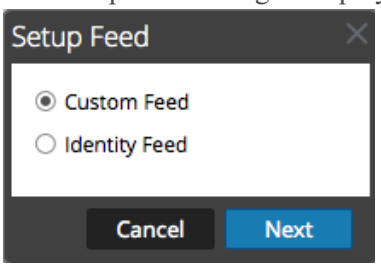
1. Go to **Configure > Custom Feeds**.

   The Feeds view is displayed.



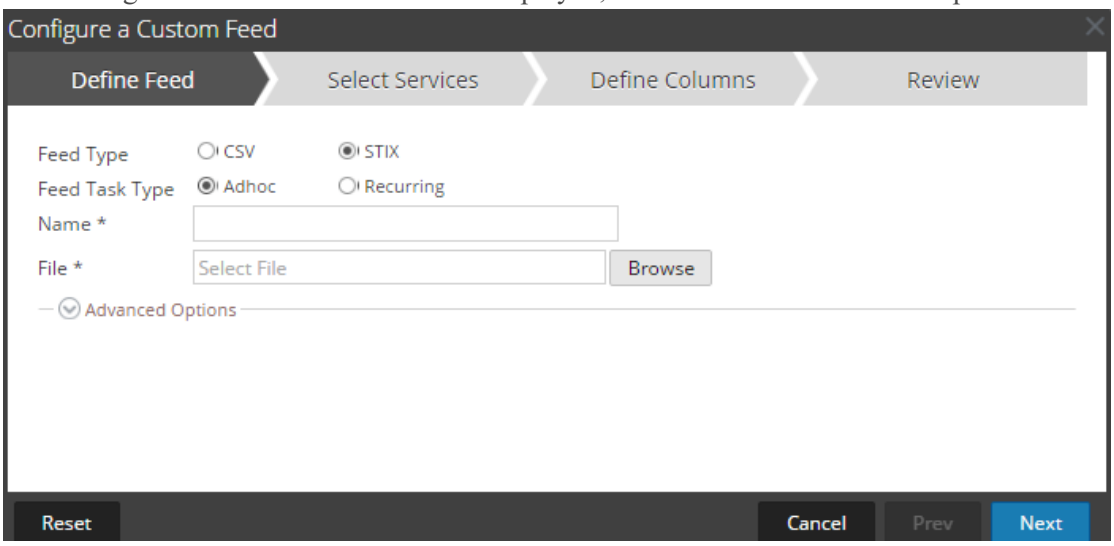
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.



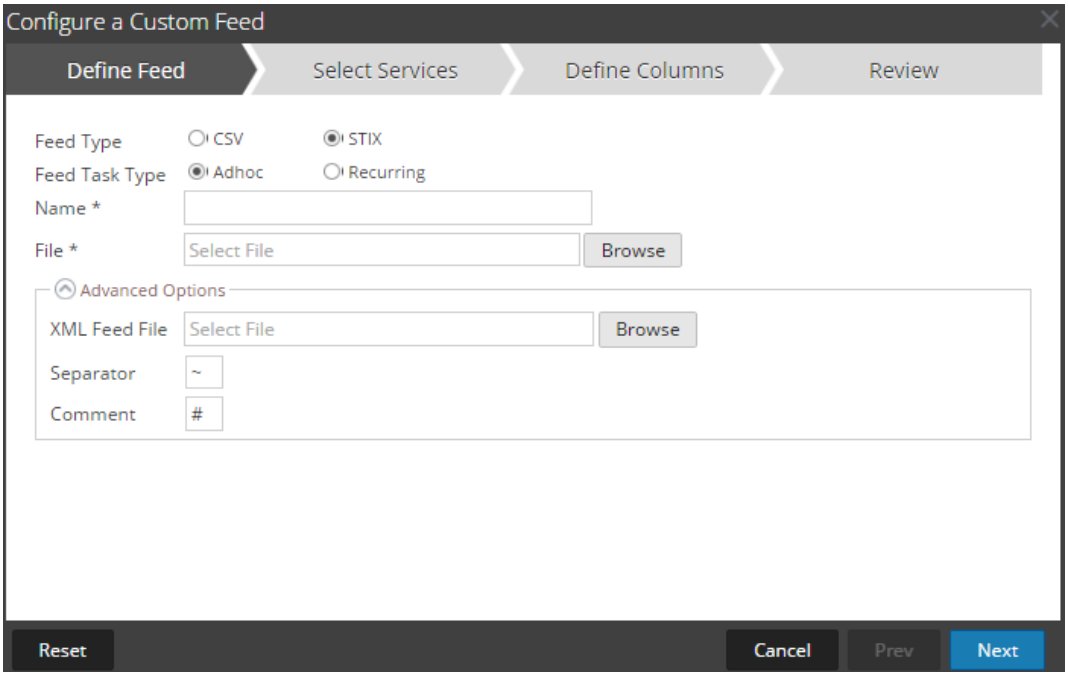
3. To select the feed type, click **Custom Feed** and **Next**.

The Configure a Custom Feed wizard is displayed, with the Define Feed form open.



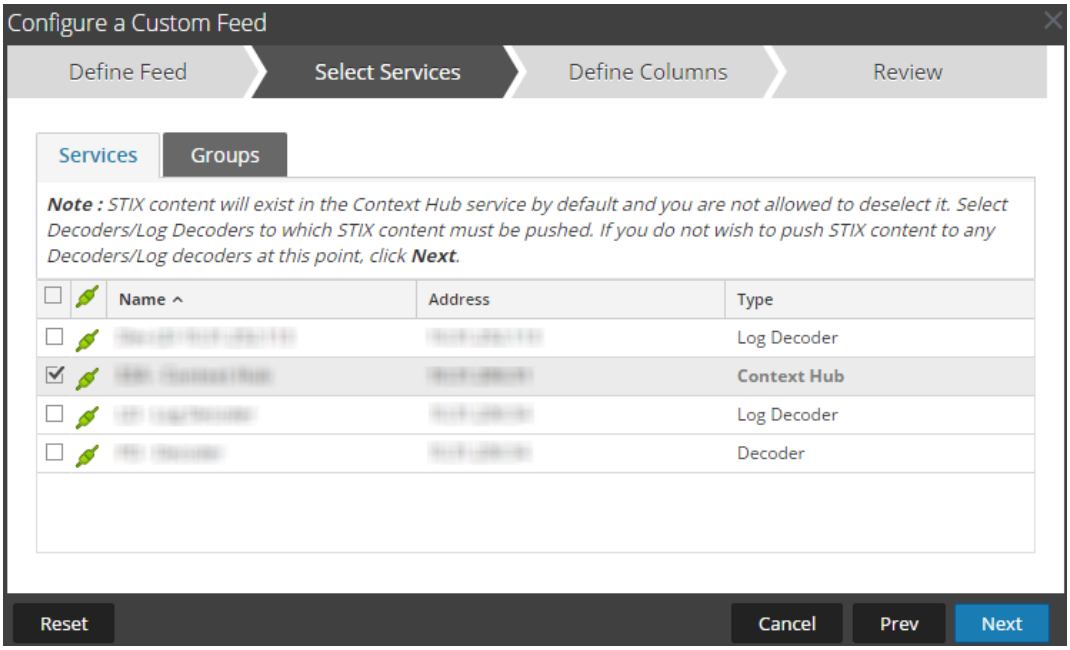
4. To define a feed based on a STIX formatted `.xml` file, select **STIX** in the **Feed Type** field.
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on STIX formatted `.xml` file, type the feed **Name**, select a STIX formatted `.xml` content **File** from the local file system, and click **Next**.
   b. (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

      The Advanced Options are displayed:



c. Select an XML feed file from the local file system, choose the **Separator** (default is comma), and specify the **Comment** characters used in the feed data file (default is #), and click **Next**.

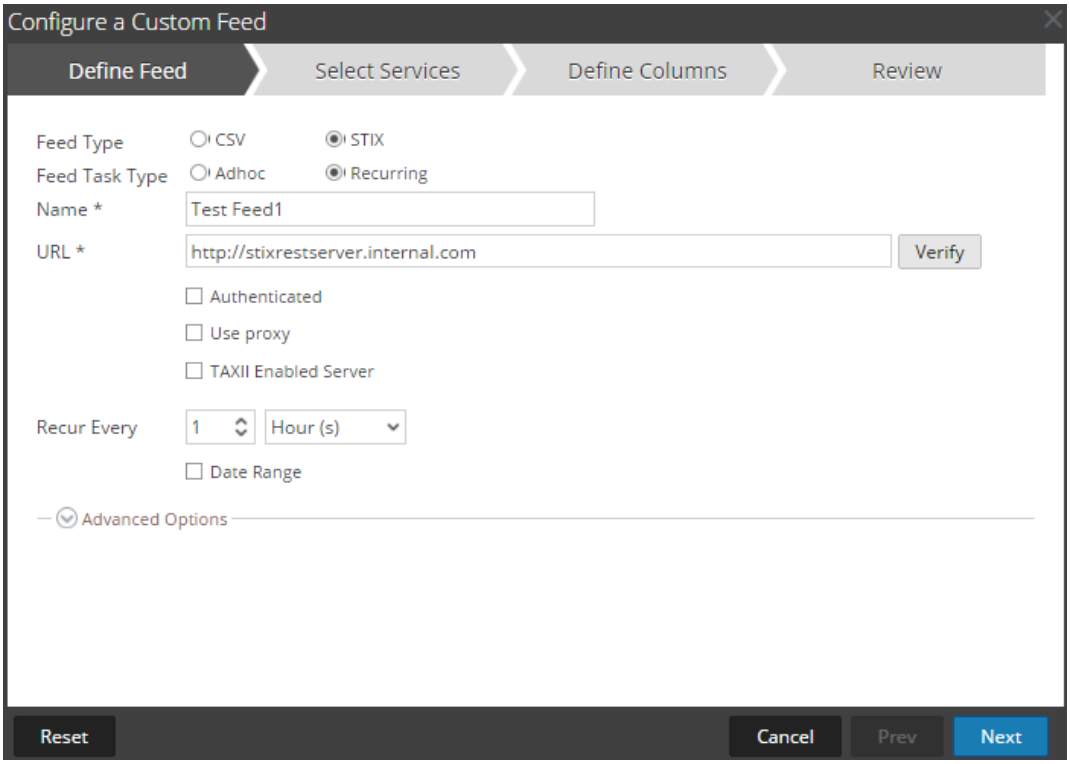
d. The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

a. Select **Recurring** in the **Feed Task Type** field.

The Define Feed form includes the fields for a recurring feed.



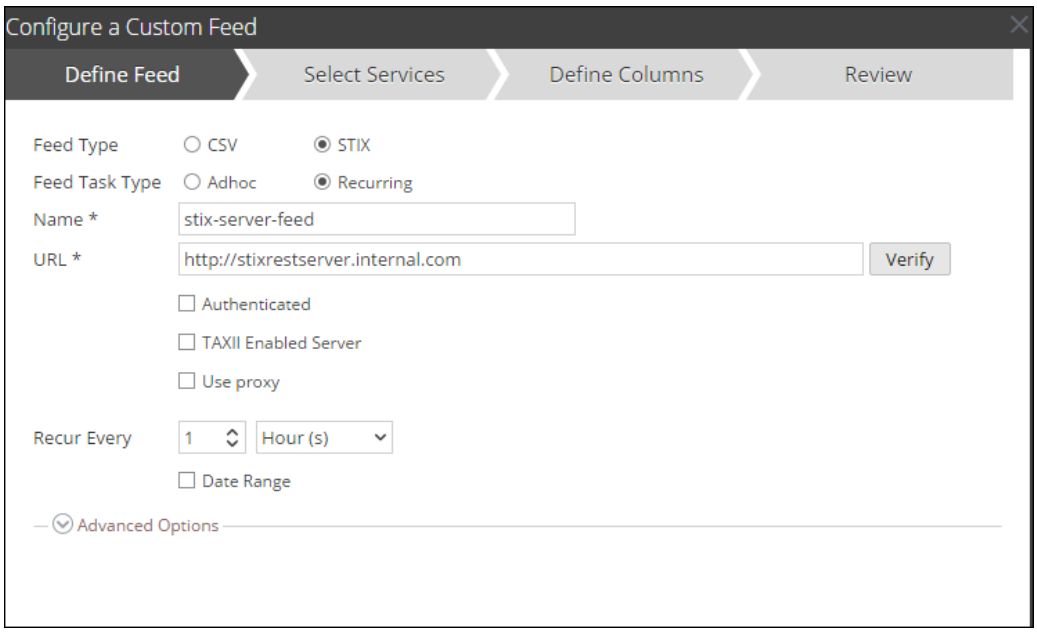
b. In the **URL** field, do one of the following:

- To define a recurring feed based on STIX which pulls STIX packages from a TAXII Server, enter the TAXII server's discovery service URL, for example, http://hailataxii.com/taxii-discovery-service.

  Note: Context Hub service installed on Event Stream Analysis host must be reachable for the specified TAXII server.

- To define a recurring feed based on a STIX formatted .xml file using REST Server, enter the URL of the REST server where the STIX data file is located, for example,

http://stixrestserver.internal.com.



NetWitness Suite verifies the connection to the server, so that NetWitness Suite can check for the latest file automatically before each recurrence.

c. If you do not want NetWitness Suite to verify the REST server's SSL certificate, Select **Trust All Certificate**. This option is enabled by default (checked)

d. For client authentication with the REST URL, in the **Certificate** field, click **Browse** and select the self signed certificate. The supported certificate formats are .cer, .crt with Base64 & DER encoded files.

e. (Optional) If the URL has restricted access and requires authentication using your username and password, select **Authenticated**.

NetWitness Suite provides your user name and password for authentication to the URL.

f. Select **TAXII Enabled Server**, if you want to select a TAXII collection from the list. For a valid URL, one or more TAXII collections that contains the STIX data file is displayed based on your credentials. Select the required TAXII collection from the list. Only one collection can be added from a TAXII server for a feed.

Note: Though multiple feeds from multiple TAXII servers are supported, only one account (username and password) is supported per TAXII server.

g. If you want the NetWitness Suite server to access the Feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see the **Configure Proxy for**

NetWitness Suite topic in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

h. (Optional) Click **Verify** to test the settings.

Note: Make sure all the required connection parameters such Authentication, Proxy, Certificate trust, TAXII Enabled Server etc. are configured before you click **Verify**.

i. To define the interval of recurrence for pushing to Decoder or Log Decoder, do one of the following:

- Specify the number of minutes, hours, or days between recurrences of the feed.
- Specify recurrence every week, and select the days of the week.

j. To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time. The Start Date should be defined from when you want to fetch the data. Make sure that the **Start Date** is not before 180 days from today.

7. (Conditional) If you want to define a feed based on an XML feed file:

- Type the feed **Name**, select **Advanced Options**.

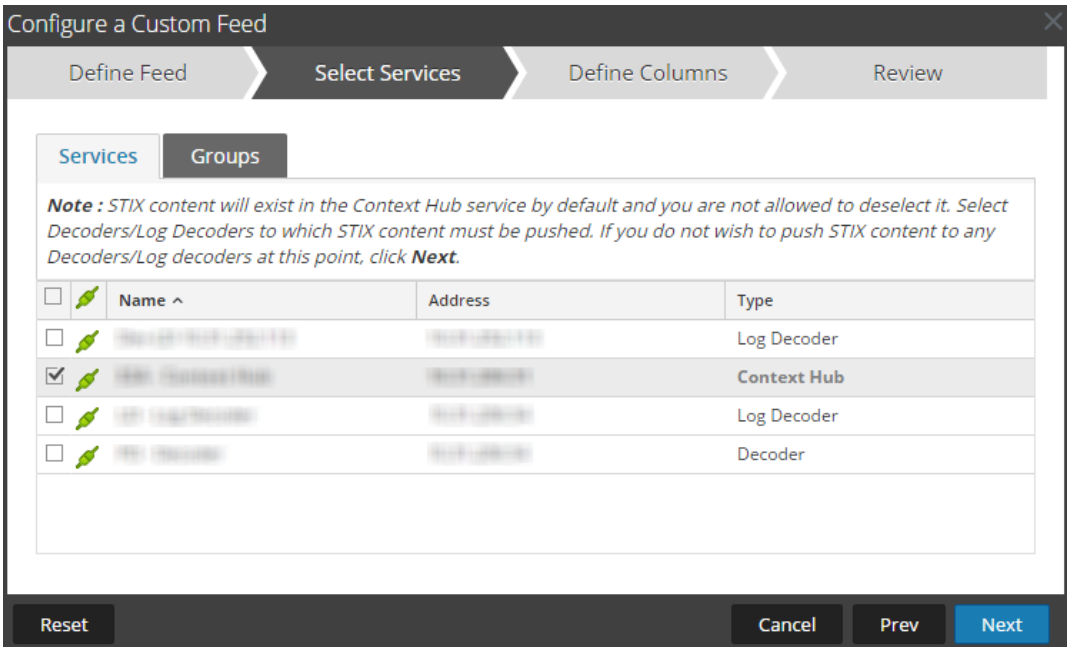
  The Advanced Options fields are displayed.
- Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #).
- In the **Remove STIX data older than** field, specify the number of days for which STIX packages pulled from TAXII server is to be stored. The STIX packages older than the specified number of days is deleted automatically.
- Click **Next**.

  The Select Services form is displayed.

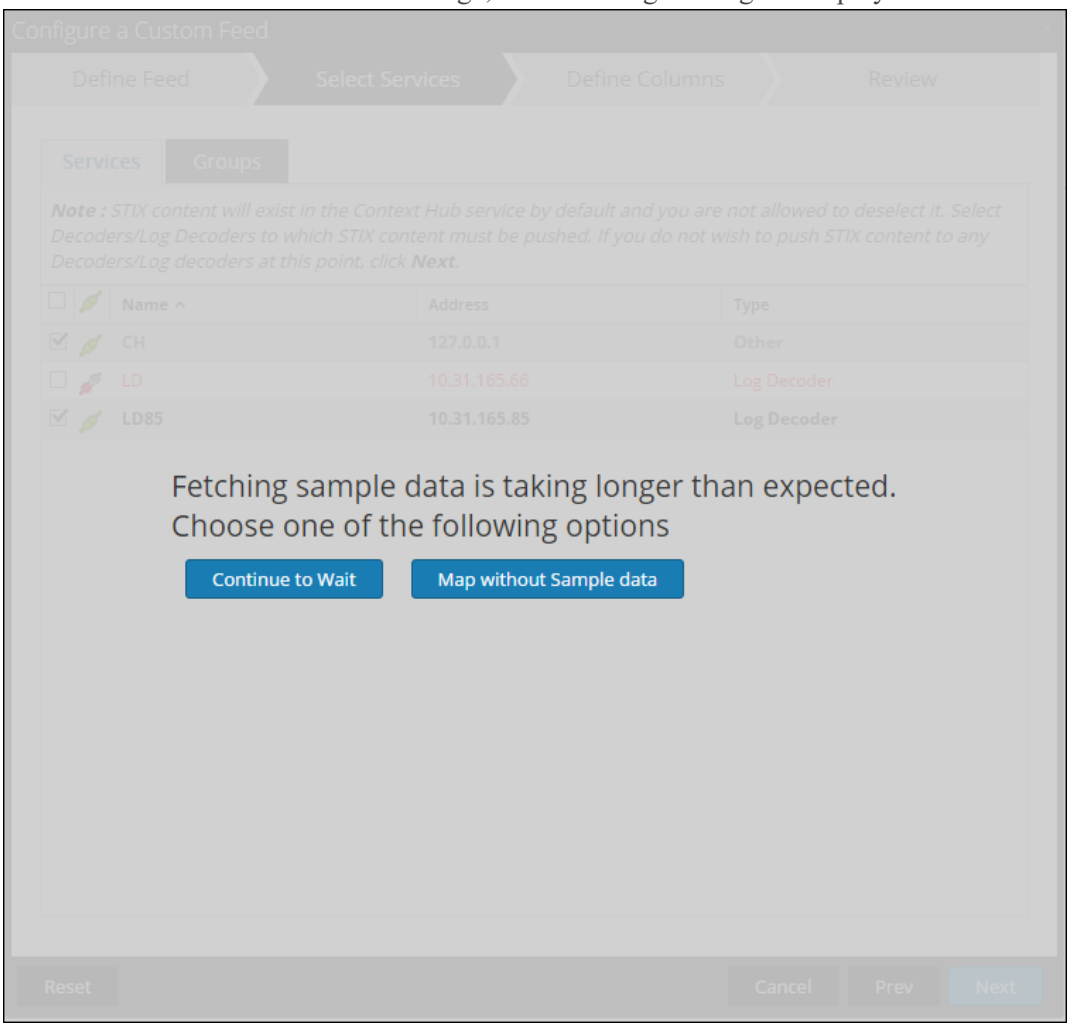
8. To identify services on which to deploy the feed, do one of the following:

a. Select one or more Decoders and Log Decoders, and click **Next**.

b. In case of STIX feed, Context Hub will be selected by default and you are not allowed to deselect it. In addition, you can select one or more Decoders and Log Decoders and click **Next** or Click the **Groups** tab and select a group. Click **Next**.


Configure a Custom Feed
Define Feed
Select Services
Define Columns
Review
Services
Groups
Note : STIX content will exist in the Context Hub service by default and you are not allowed to deselect it. Select Decoders/Log Decoders to which STIX content must be pushed. If you do not wish to push STIX content to any Decoders/Log decoders at this point, click Next.
Name
Address
Type
Log Decoder
Context Hub
Log Decoder
Decoder
Reset
Cancel
Prev
Next

If the data from the STIX server is large, the following message is displayed:

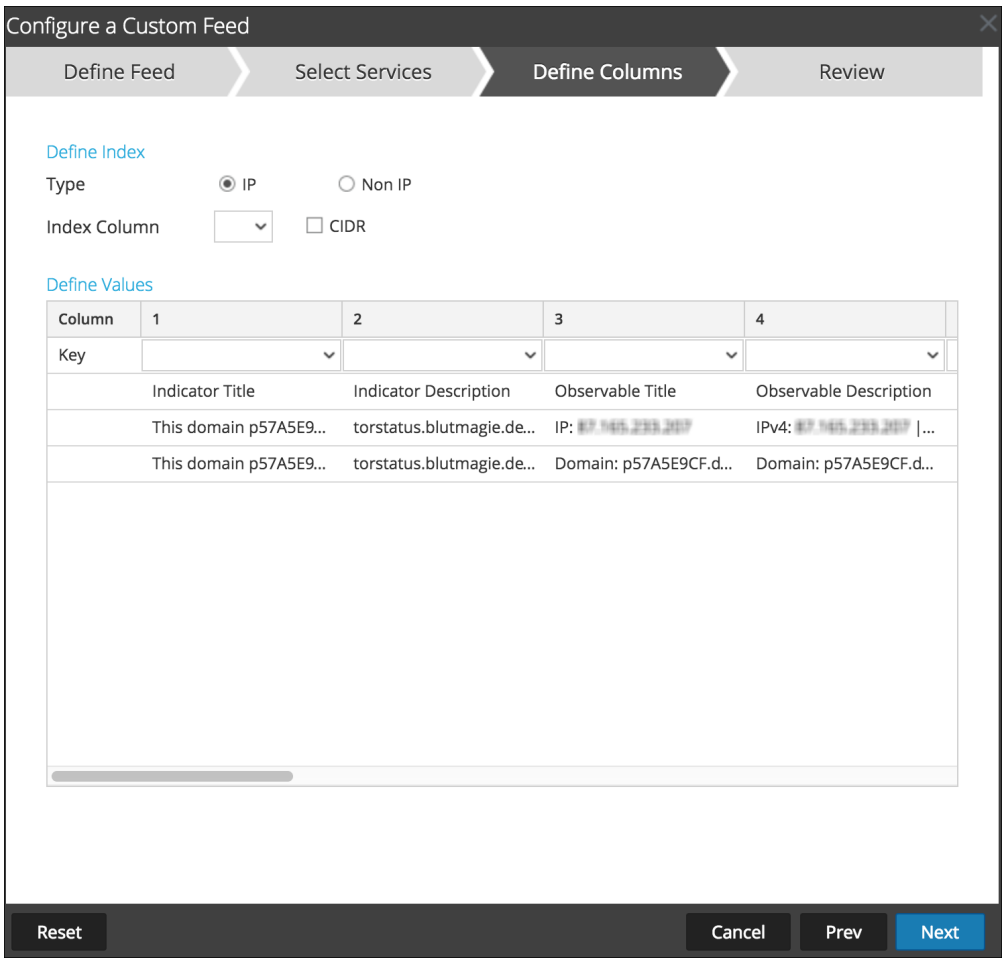


- If you click **Continue to Wait**, it continues to wait till the sample data is fetched or timeout (10 minutes) whichever is sooner. In case of timeout no sample data is retrieved even after 10 minutes.
- If you click **Map Without Sample data**, the mapping column is displayed without any sample data.

The Define Columns form is displayed.

9. To map columns in the Define Columns form:
   a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.
   b. (Conditional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR**.
   c. (Conditional) If the index type is **Non IP**, additional settings are displayed. Select the

service type and **Callback Keys,** and optionally select the **Truncate Domain** option.

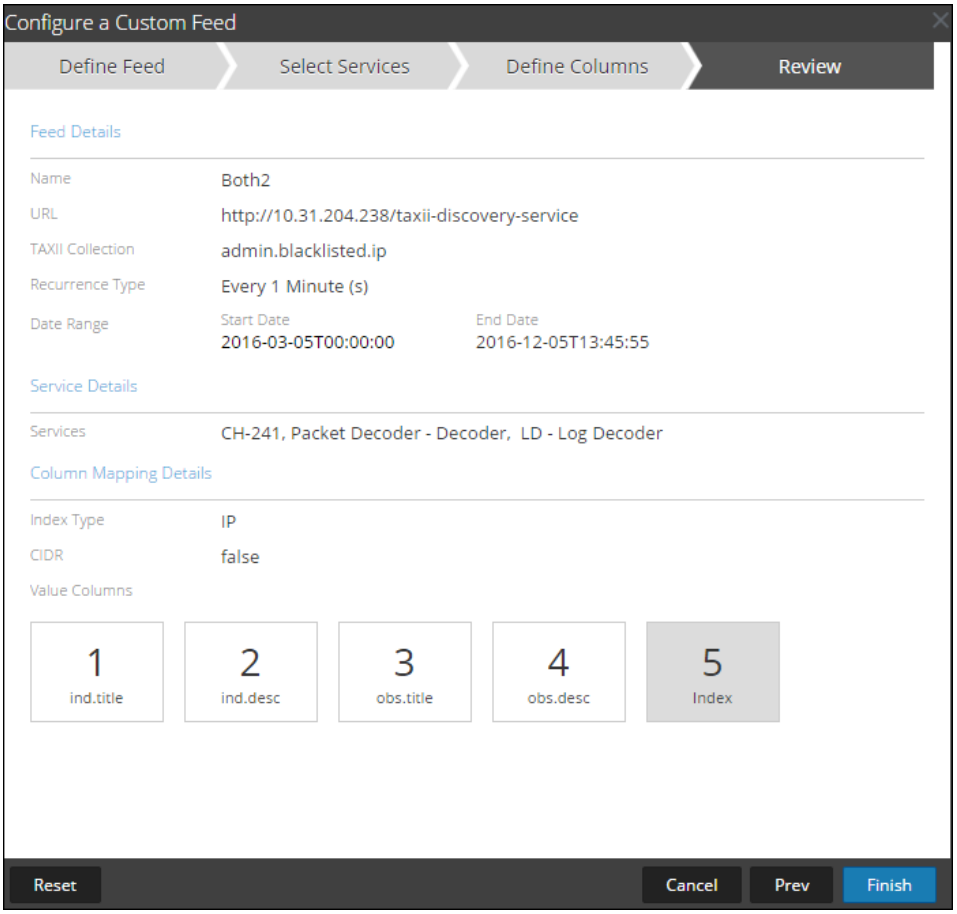


Note:
- If the **Index Type** is Non IP, you can select multiple index columns in the **Index Column(S)**. The values from all the selected columns are merged in the first index column that you selected and the merged values are pushed to the Log Decoder for parsing. For example, in the **Index Column(S)** if you select 2,4,7 as index columns the values from the 2,4 and 7 columns are merged in the column 2 and the values are pushed to Log Decoder for parsing.
- Indexing cannot be done for the columns such as Indicator Title, Indicator Description, Observable Title, Observable Description, as the look up cannot be performed for those columns.

d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.

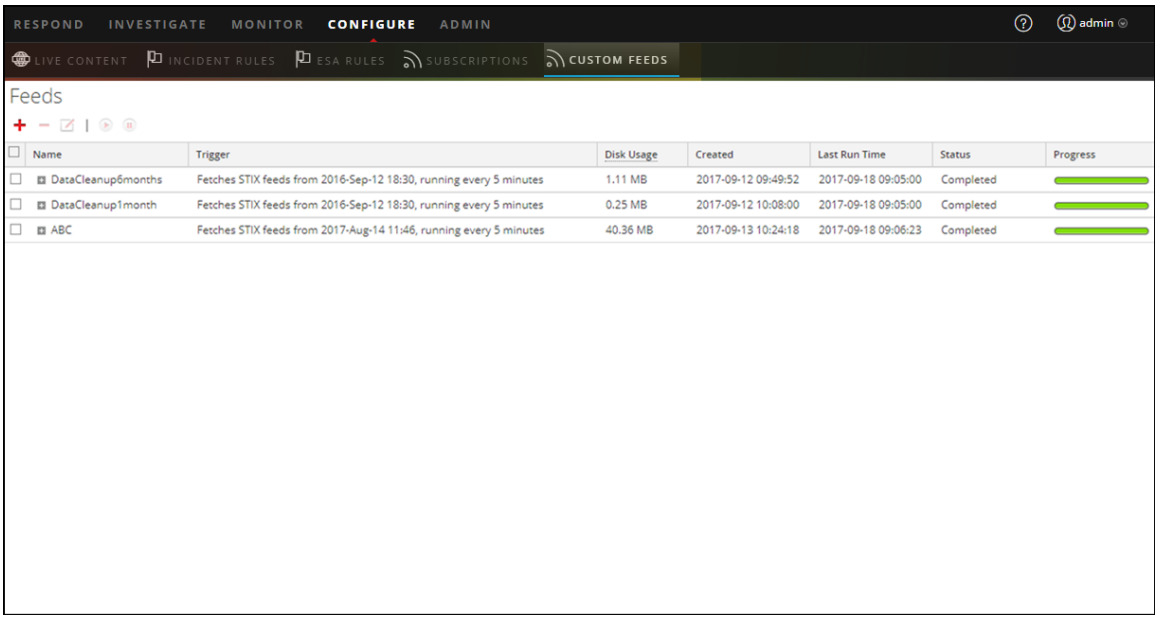
e. Click **Next**.

The Review form is displayed.



10. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form).

11. Review the feed information, and if correct, click **Finish**.
12. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.



Note: Health and Wellness raises alerts when the available heap memory of Context Hub server is critically low. If the status of Context Hub server is Unhealthy due to low memory. For more information on how to troubleshoot `OutOfMemoryError` on `Contexthub` Server, refer to "Troubleshooting" in the *Live Services Management Guide*.

MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6

This section describes how to use CIDR index ranges for IPv4 and IPv6 in custom MetaCallback feeds. As with other custom feeds, you must create feed data file in .csv format, and a feed definition file in .xml format.

Note: Using Metacallback feeds with CIDR index ranges is supported only through the Advanced Configuration wizard or the REST interface.

The following example shows the contents of both a .csv file and an .xml file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

.csv file:

192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>

<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">

        <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">

                <Meta name="ip.dst"/>
```

```
        </MetaCallback>
        <LanguageKeys>
                <LanguageKey name="alert" valuetype="Text" />
        </LanguageKeys>
        <Fields>
                <Field index="1" type="index" range="cidr"/>
                <Field index="2" type="value" key="alert" />
        </Fields>
</FlatFileFeed>
</FDF>
```

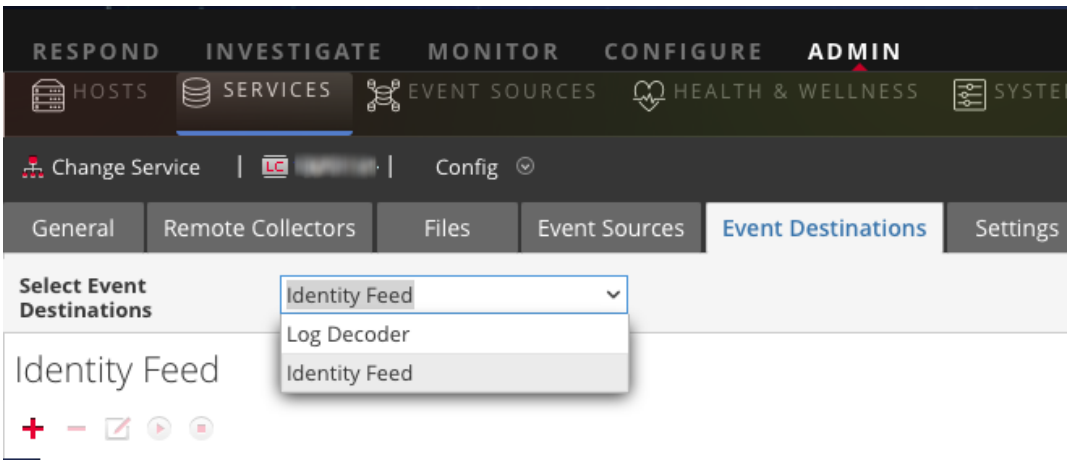
Note: To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.

Create and Manage an Identity Feed

You can easily create an Identity feed and populate it to selected Decoders and Log Decoders. After completing this procedure, you will have created an Identity feed.

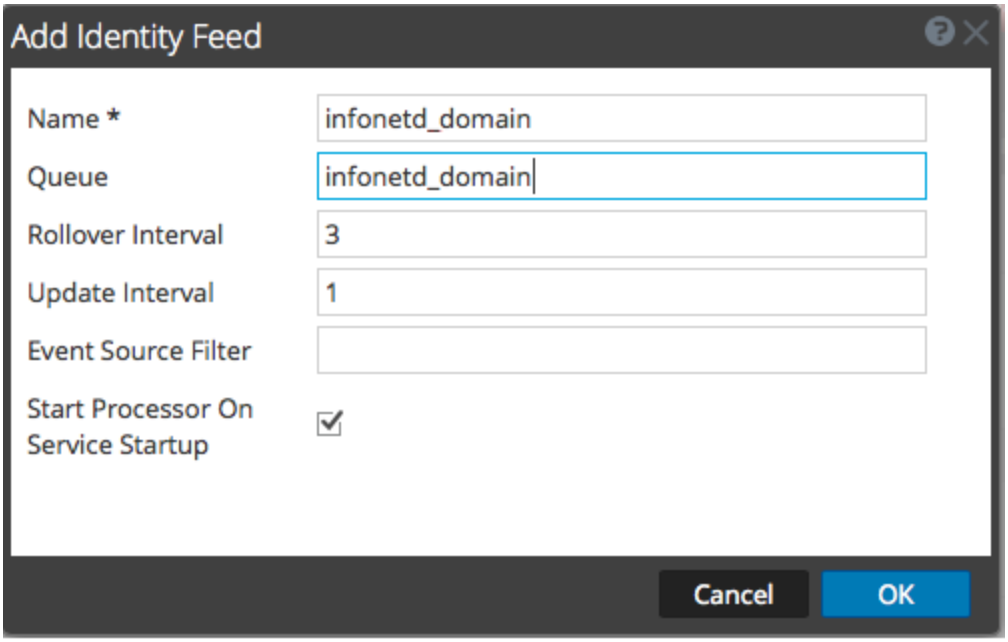
To create an identity feed:

1. Add a destination for the feed.
   a. Go to **ADMIN > Services**, in the **Services** list select a **Log Collector** service, and **View > Config**.
   b. Select the **Event Destinations** tab.
   c. In the Select **Event Destinations** field, select **Identity Feed**.



d. Click + and enter a unique name for the feed.

The Queue name identifies the feed within the log collector. Use the name of the feed for the Queue.

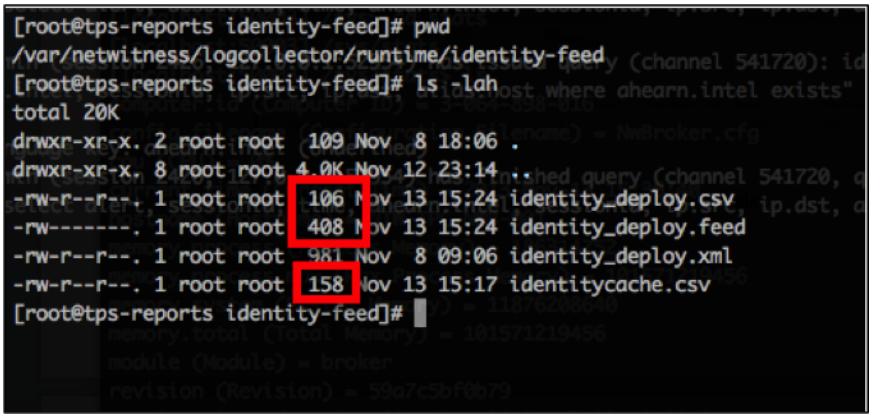


e. Click **OK**.

2. Test generation of messages.

a. Have users log into Windows boxes on the domain to generate the appropriate log messages on the domain controllers for testing.

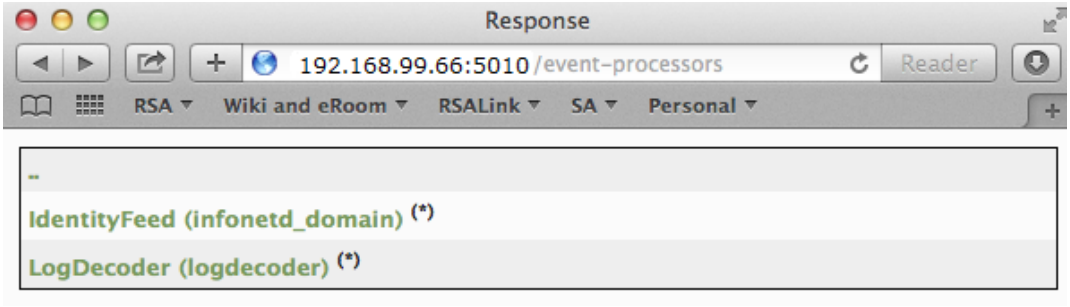
b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.



c. Open up a web browser (Non-Internet Explore browsers preferred) and log in to the REST interface of the Log Collector. Use administrative credentials when logging in. For example, if the IP address of your log collector is 192.168.99.66, the URL would be:

- SSL not enabled: **http://192.168.99.66:50101/event-processors**
- SSL enabled: **https://192.168.99.66:50101/event-processors**

The browser screen should look like this:

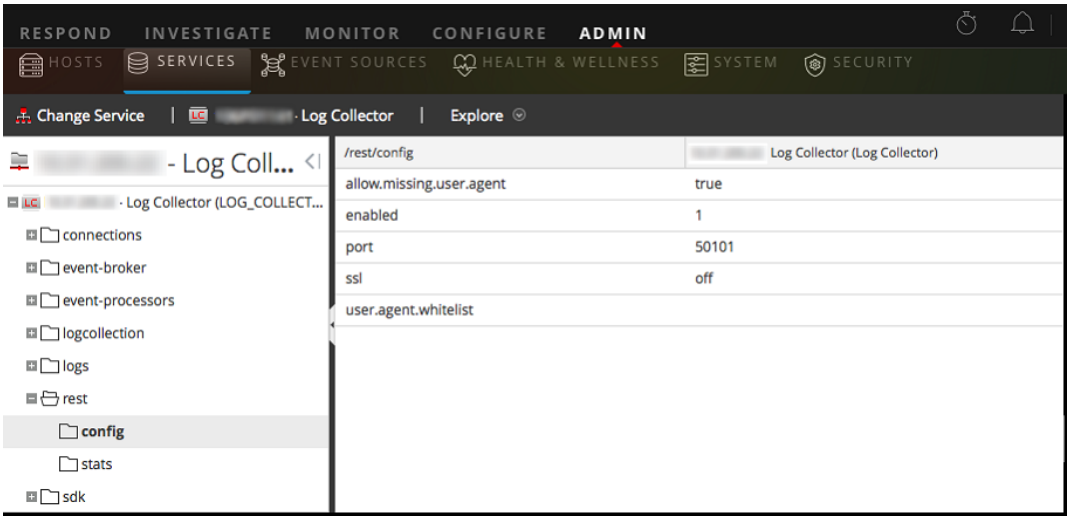


Notice the screen contains the name of the identity feed you created earlier (`infonetd_domain`, in this example).

For the identity feed to function correctly, port 50101 must be active on the Log Collector, and you must determine whether SSL encryption is active.

d. Go to **AdMIN > Services > <*Log Collector being setup*>** **> View > Explore**.

e. In the left pane, expand **rest > config**.



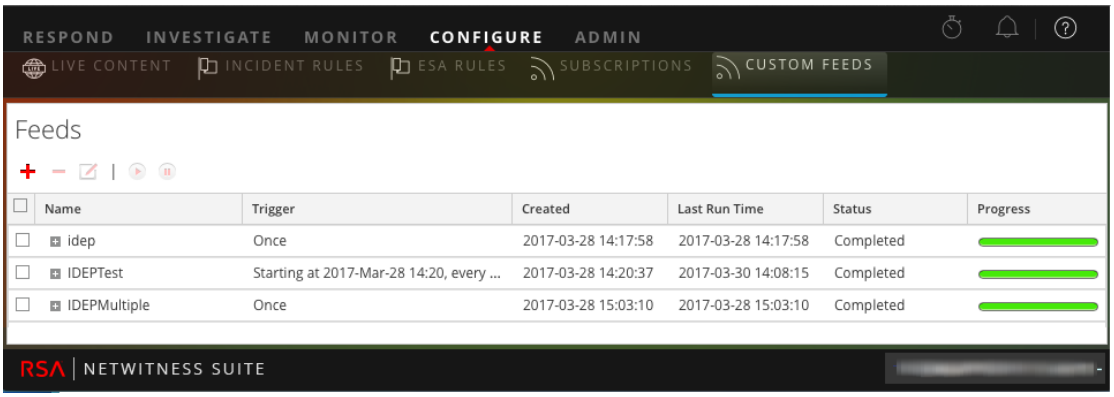
For REST to be active, **enabled** must be set to **1**.

f. Note the value for **ssl**. If SSL should be enabled for your environment, this must be set to **on**.

Note: If you changed the setting for either the **enabled** or **ssl** option you must restart the Log Collector service before moving forward.

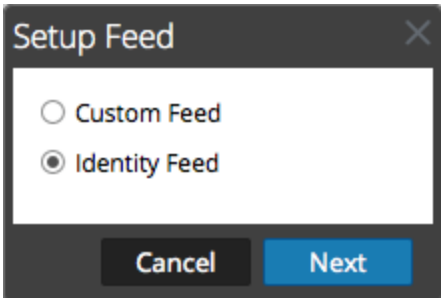
3. Go to **CONFIGURE > Live Content > Custom Feeds**.

   The Feeds grid is displayed.



4. In the toolbar, click +.

   The Setup Feed dialog is displayed.



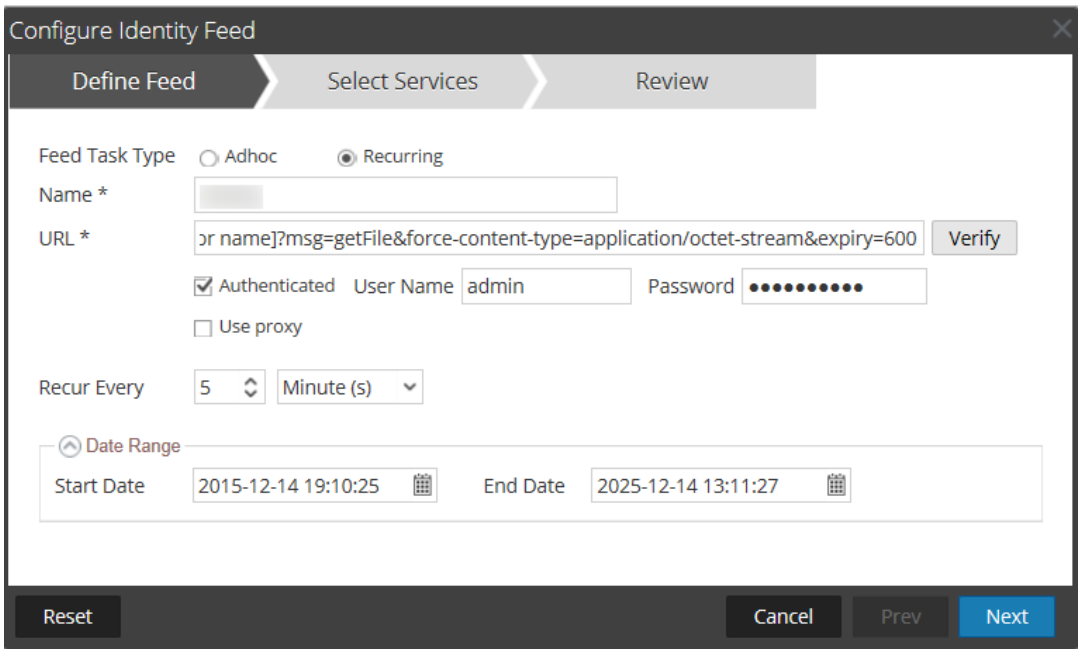
5. Ensure **Identity Feed** is selected and click **Next**.

   The Configure Identity Feed panel opens with the **Define Feed** tab displayed.

6. (Conditional) You can create an on-demand or recurring feed.

   - To define an on-demand Identity feed task that executes once, select **Adhoc** in the **Feed Task Type** field, type the feed **Name**, and browse for and open the feed.
   - To define a recurring Identity Feed task that executes on a recurring basis, select **Recurring** in the **Feed Task Type** field.

     The **Define Feed** form includes the fields for a recurring feed.



Note: RSA NetWitness Suite verifies the location where the file is stored, so that Security Analytics can check for the latest file automatically before each recurrence.

7. Fill in and verify the URL field.

   a. In the **URL** field, enter the URL where the feed data file is located. This is the REST API interface that was setup earlier. You need to know the following information to construct the URL:

   - The IP address of the log collector being used to construct the Identity Feed file.
   - The identity queue name, as set in step 2c.
   - Whether or not SSL is enabled on the log collector REST port, as set in step 2f.

   You construct this value as follows:

   - SSL enabled: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
   - SSL not enabled: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

   So, using our example from earlier, the complete value that you would enter into this field is as follows:

```
http://192.168.99.66:50101/event-processors/infonetd_
domain?msg=getFile&force-content-type=application/octet-
stream&expiry=600?msg=getFile&force-content-
type=application/octet-stream&expiry=600
```

b. For the URL verification to work correctly, it is important that the Security Analytics UI server can access the log collector's REST API port (50101). This can be tested by going to the Security Analytics UI server via SSH. Once there, run the following command:

- SSL enabled: `curl -vk https://<ip of log collector>:50101`
- SSL not enabled: `curl -v http://<ip of log collector>:50101`

If the `curl` command does not connect then there may be a network firewall or routing issue between the Security Analytics UI server and the Log Collector.

Example of Bad connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... No route to host
* couldn't connect to host
* Closing connection #0
curl: (7) couldn't connect to host
```

Example of Good connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... connected
* Connected to 192.168.99.66 (192.168.99.66) port 50105
(#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2
> Host: 192.168.99.66:50105
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Content-Length: 71
< Connection: Keep-Alive
< Pragma: no-cache
```

```
< Expires: -1
< Cache-Control: no-cache, no-store, must-revalidate
< WWW-Authenticate: Basic realm="NetWitness"
< Content-Type: text/xml; charset=utf-8
<
<?xml version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
* Connection #0 to host 192.168.99.66 left intact
* Closing connection #0
```

8. The REST API requires a username and password when attempting to pull the `identity_deploy.csv` file from the log collector. This can be any username and password that is available on the service itself. For details, see the "Services Security View" topic in the *Hosts and Services Guide*.

   To see which accounts are available, go to **ADMIN > Services > <log collector being setup> > Actions > View > Security**.

   Under the Users table, you see all the users that can be used in this step. It is suggested that a separate user account is created specifically for this setup, and is used nowhere else in the environment, for added security. For details, see "Add a User and Assign a Role" in the *System Security and User Management Guide*. (Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

9. To define the interval for recurrence, do one of the following:

   - Specify the number of minutes, hours, or days between recurrences of the feed.
   - To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.

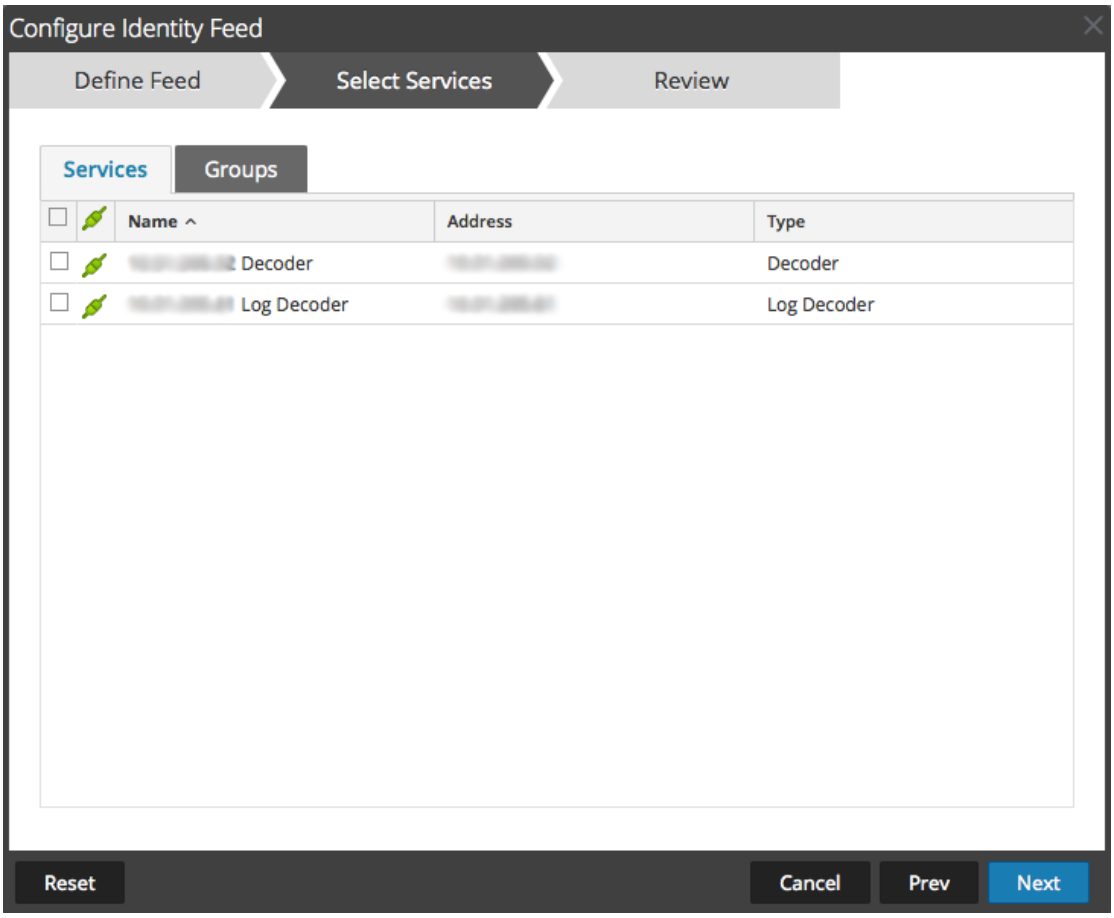
10. If using SSL encryption, you need to install the REST API SSL certificate for the log Collector into the Security Analytics UI server. For details, see Import the SSL Certificate.

    If, after importing the SSL certificate, the verification of the URL still fails, see Cannot Verify Identity Feed URL.

11. Click **Verify** to verify your identity feed configuration before you proceed to the Select Services form.

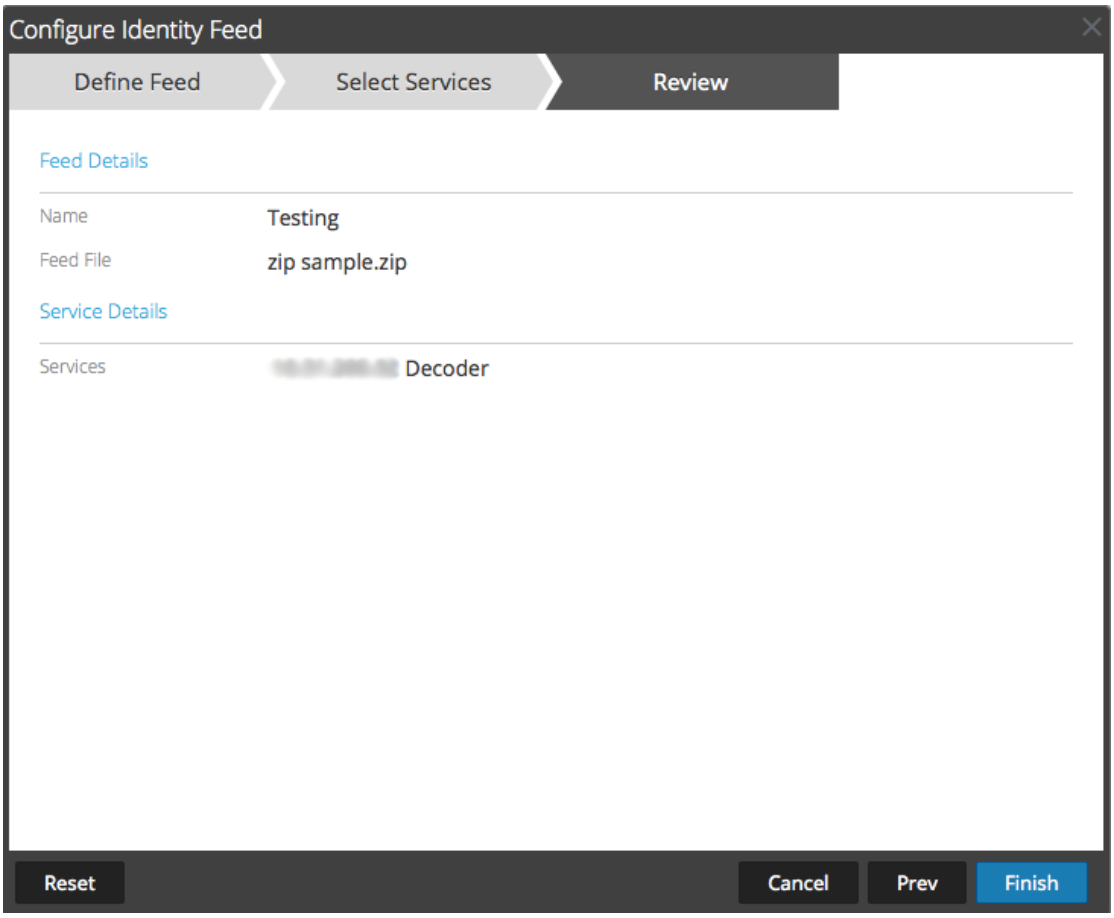
12. Click **Next**.

    The Select Services form is displayed.



13. To identify services on which to deploy the feed, select one or more Decoders and Log Decoders and click **Next**.
14. Click the **Groups** tab, select a group, and click **Next**.

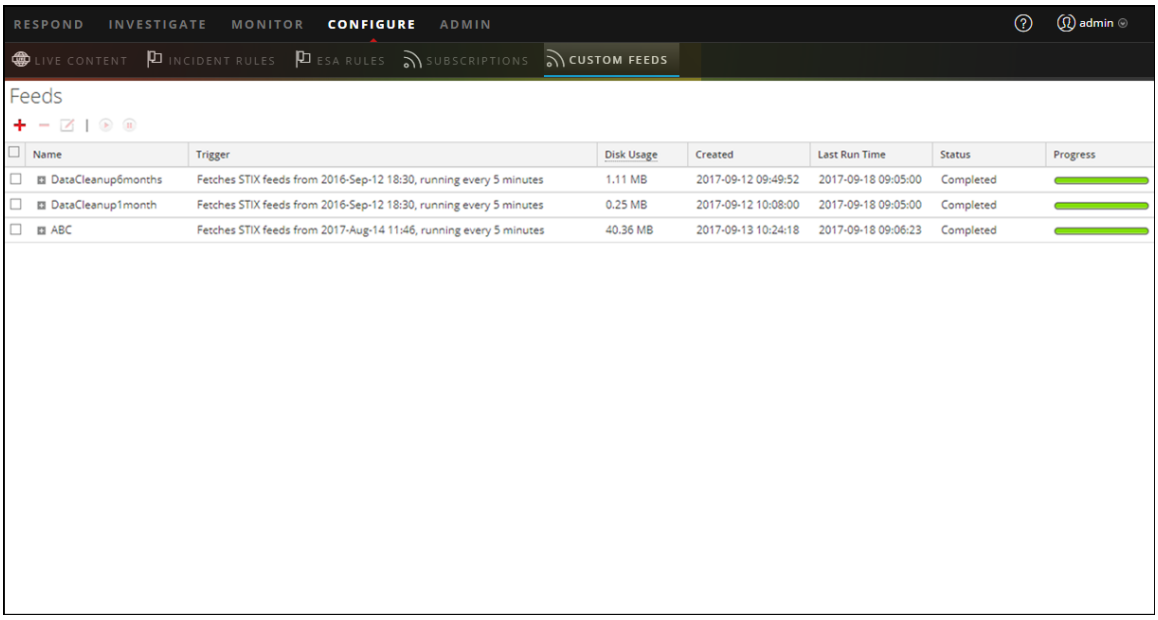
    The Review form is displayed.



Note: If a group of devices with Decoders and Log Decoders is used to create recurring or custom feeds and this group is deleted, you can edit the feed and add a new group to the feed.

15. Anytime before you click **Finish**, you can:
    - Click **Cancel** to close the wizard without saving your feed definition.
    - Click **Reset** to clear the data in the wizard.
    - Click **Next** to display the next form (if not viewing the last form).
    - Click **Prev** to display the previous form (if not viewing the first form).
16. Review the feed information, and if correct, click **Finish**.

Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.



Import the SSL Certificate

If SSL is configured on the Identity feed's Log Collector, follow these steps to import the Log Collector's SSL certificate into the Security Analytics UI server key store. If this certificate is not imported, the Security Analytics UI server will be unable to pull the Identify feed file from the Log Collector.

1. To pull the SSL certificate off the log collector, SSH into the Security Analytics UI server and run the following command:

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne
   '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/<SERVERNAME>.cert
   ```

   This command saves the SSL certificate to `/tmp/<SERVERNAME>.cert`.

   For example:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed
   -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/logcollector.cert
   ```

2. To import the SSL certificate into the Security Analytics UI server, SSH into the UI server and run the following command:

   ```
   keytool -importcert -alias <name an alias for the cert> -file
   <the cert file pathname> -keystore /etc/pki/java/cacerts
   ```

   For example:

   ```
   keytool -importcert -alias logcollector01 -file
   /tmp/logcollector.cert -keystore /etc/pki/java/cacerts
   ```

3. The system requests a password. Enter the password for the keystore on the Security Analytics UI server, not for the jetty keystore. The default password is **changeit**.
4. Restart **jettysrv** to allow jetty to read the new certificate in the store.

Cannot Verify Identity Feed URL

If the Identity feed URL cannot be verified, and you are using SSL, make sure you followed the steps in Import the SSL Certificate.

If there are still issues, it is possible that the internal name of the certificate does not match the hostname of the log collector. The following procedure checks this.

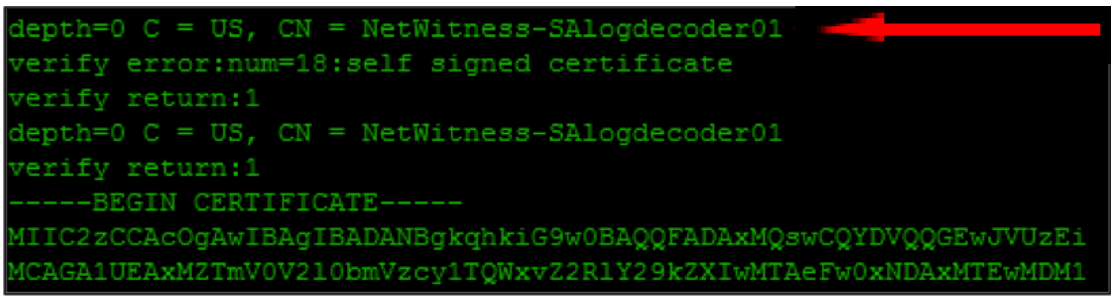
1. SSH to the Security Analytics UI server.
2. Run the following command to output the CN name of the SSL cert:

   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

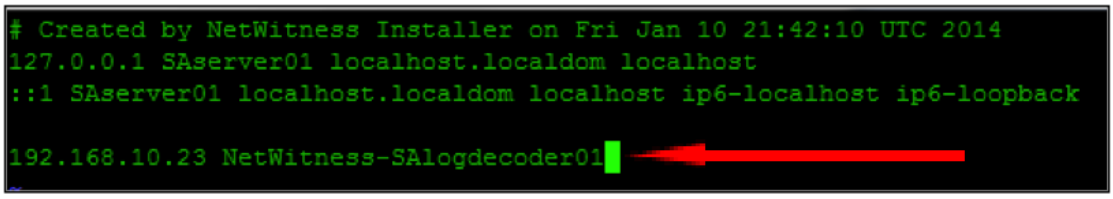
   Example:

   ```
   echo -n | openssl s_client -connect salogdecoder01:50101 | sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Retrieve the CN name of the SSL certificate.



4. Edit the `/etc/hosts` file and add the IP address and CN name to the file.



5. Restart the network service on the appliance.
6. Confirm that the name placed in the **/etc/hosts** file is used instead of the FQDN or IP address in the Identity feed URL.
7. Re-verify the Identity feed URL.

Investigate an Identity Feed

An identity feed tracks interactive log on events from the Windows operating system. Identity feeds do not track interactive log off events.

In order for an identity feed to process events and tag them, the events need to be collected using a Windows Log Collection module where an Active Domain Controller/non-Domain Controller is configured. Note that identity feeds can only be processed via an Identity Feed Event Processor.

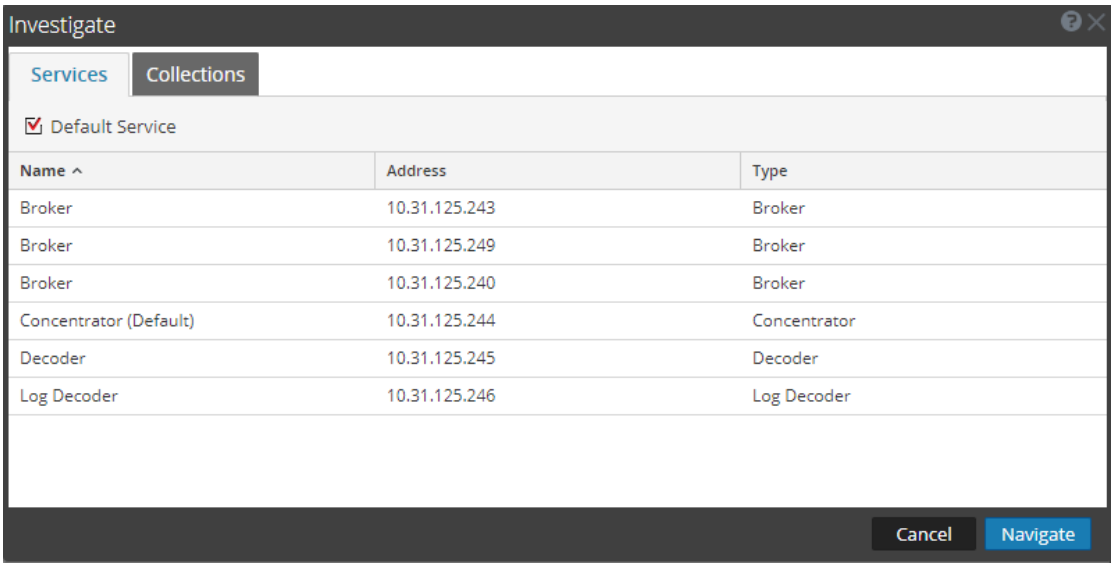
Note: An identity feed only tracks one log in at a time. If two users log in to a system at the same time, the second user will overwrite the first user's data in the identity feed.

Once you have created an identity feed, you can view the results by investigating the feed.

To investigate a configured identity feed:

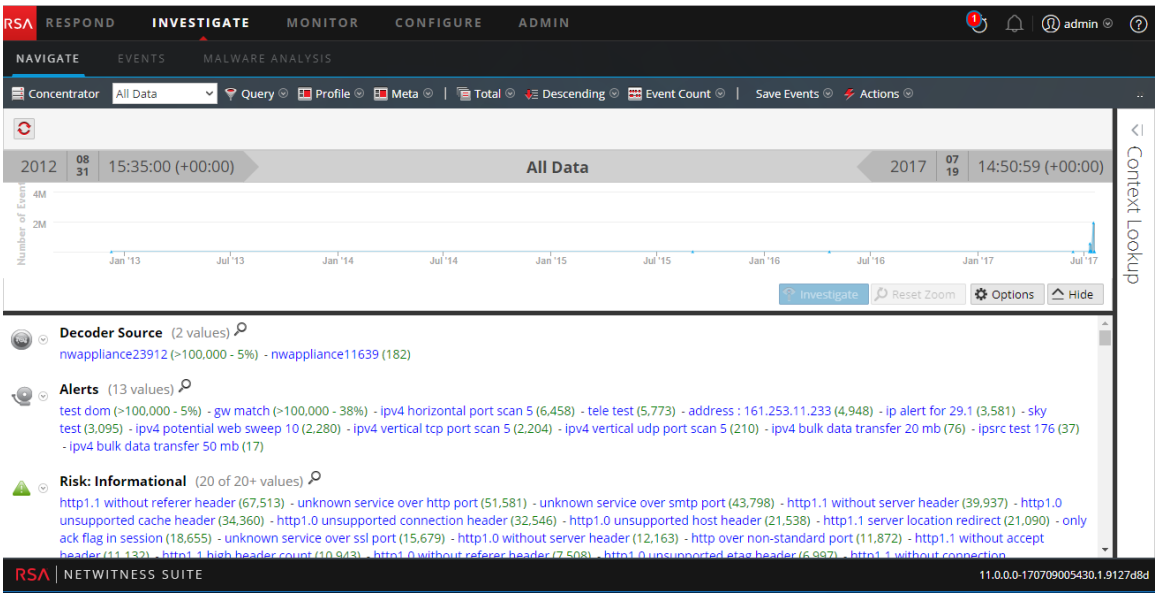
1. Go to **INVESTIGATE > Navigate**.

   If no default service is selected, the Investigate dialog is displayed.



2. Select a service, usually a Concentrator, and click **Navigate**.
3. Select **Load Values** to retrieve meta data.

In the Values panel, scroll down to find the Meta Keys shown in the following illustration.



The identity feed provides information to selected Decoders and Log Decoders. It associates the Host IP data from the Windows operating system to the user logging into that Host in order to tag all logs associated with that IP and investigate.

Edit a Feed

This topic provides instructions for editing a custom feed using the Custom Feed Wizard.

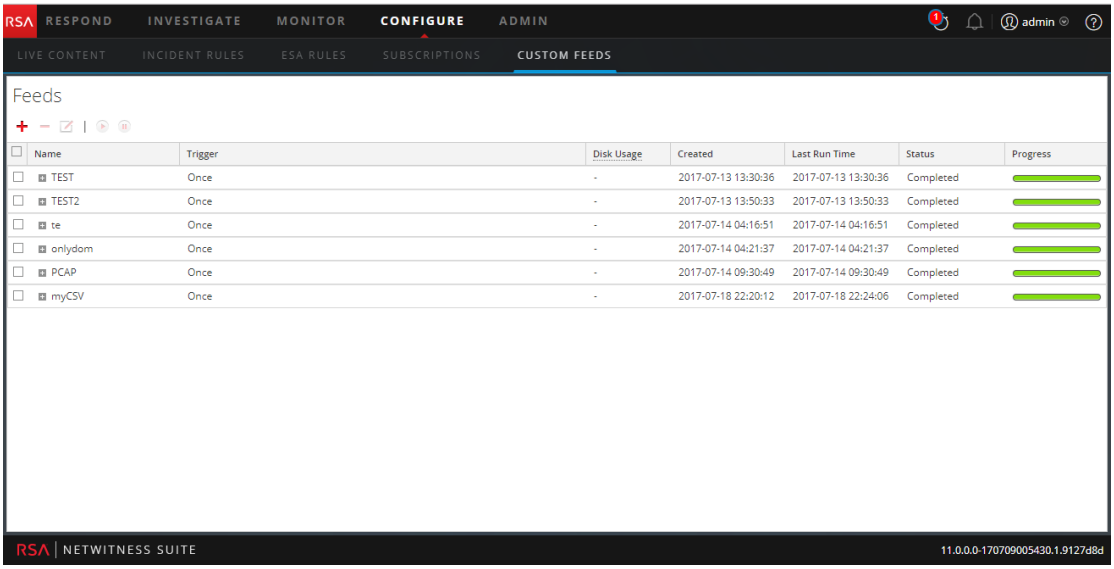
Completing this procure will result in:

- An existing custom feed opened.
- The feed (**.zip** format) or the file used to create the feed (**.csv** or **.xml**) downloaded and edited.
- The feed recreated with the updated file and new feed specifications.

To edit an existing feed:

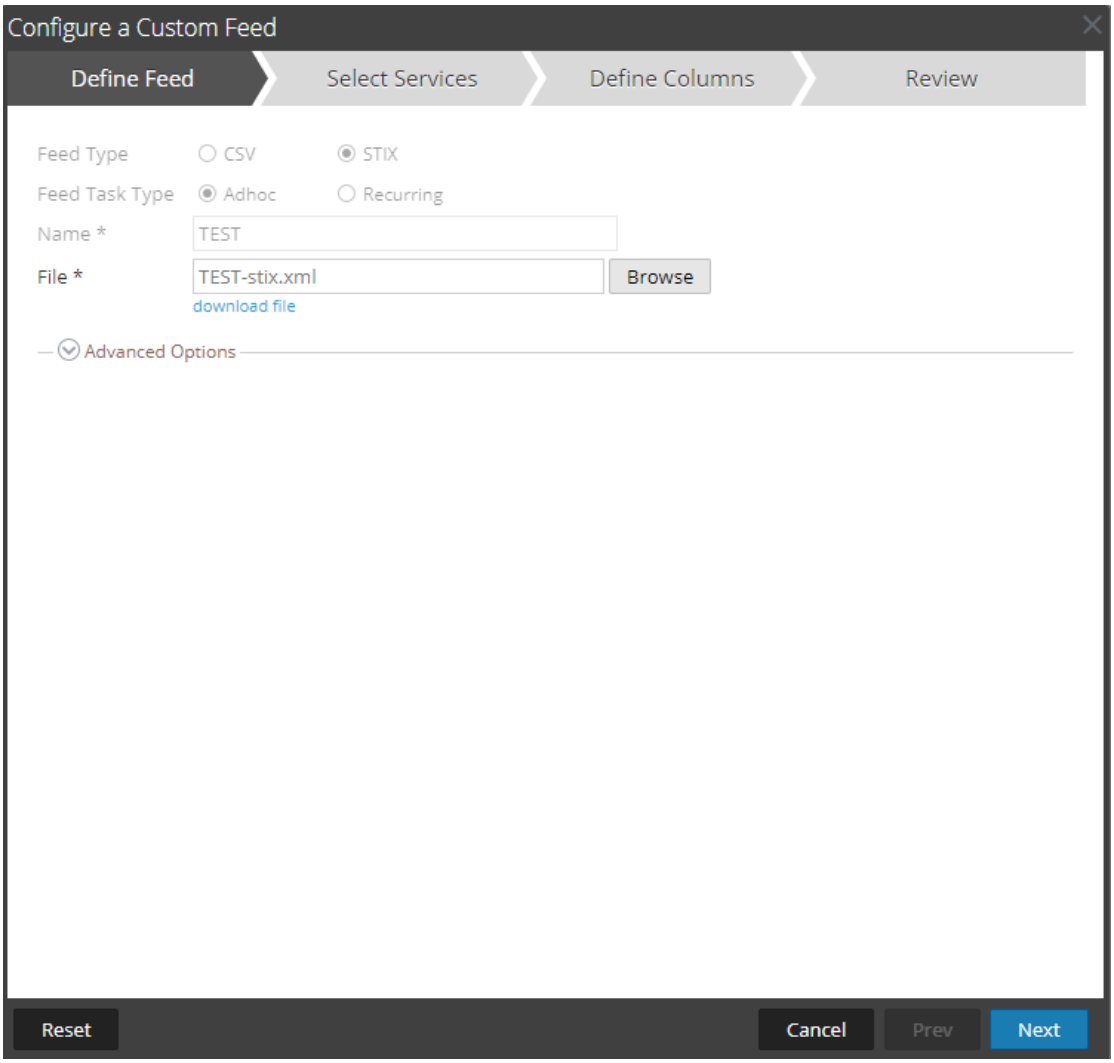
1. Go to **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



2. In the toolbar, select a feed and click .

   The Configure Custom Feed or Configure Identity Feed panel opens in the Custom Feed wizard.



3. If you want to edit the feed file:
   a. Click **download file**.

      For an Identity feed, the .zip file is downloaded. For a custom feed, the .csv or .xml file is downloaded to your local file system.

   b. Edit and save the file.

   c. In the **Define Feed** tab, browse for and open the edited file.
4. Edit any other parameters in the **Define Feed** tab, **Select Services** tab, and **Define Columns** tab that apply to the type of feed.
5. Anytime before you click **Finish**, you can:
   - Click **Cancel** to close the wizard without saving your changes.
   - Click **Reset** to clear the data in the wizard.

- Click **Next** to display the next form (if not viewing the last form).
- Click **Prev** to display the previous form (if not viewing the first form).

6. In the **Review** tab, review the feed information, and if correct, click **Finish**.

The feed is added to the feeds list and progress bar tracks completion. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file is listed in the Feeds list. You can expand or collapse the entry to see how many services are included, and which services are successful.

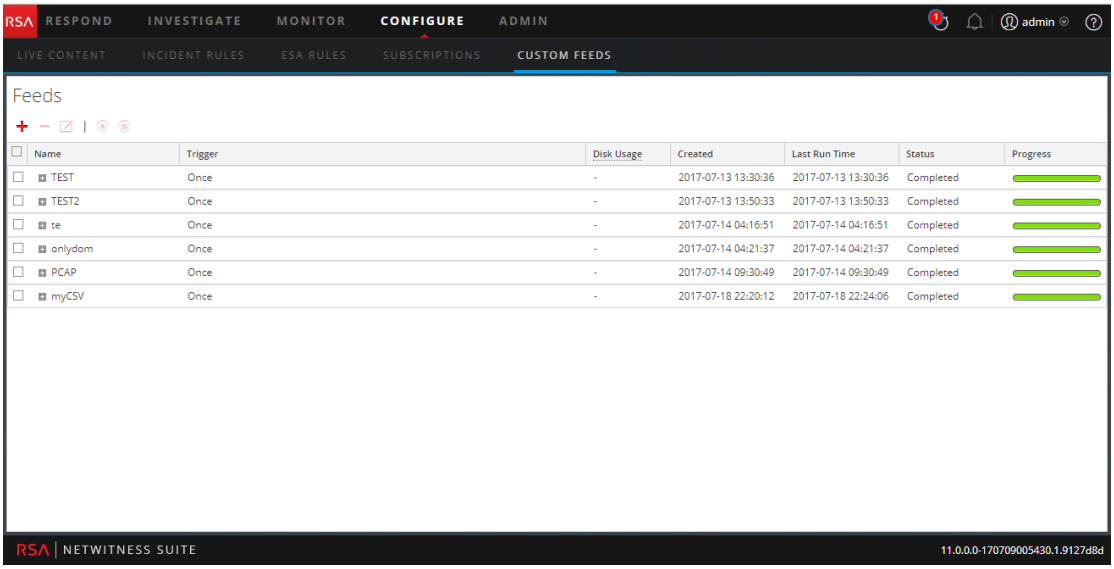
Remove a Feed

This topic provides instructions for removing a feed.

To remove a feed:

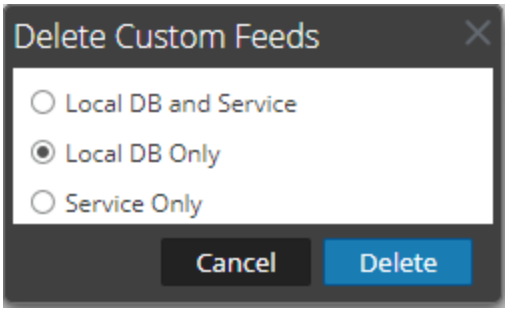
1. Go to **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



2. In the toolbar, select a feed and click − .

   The Delete Custom Feeds dialog is displayed.



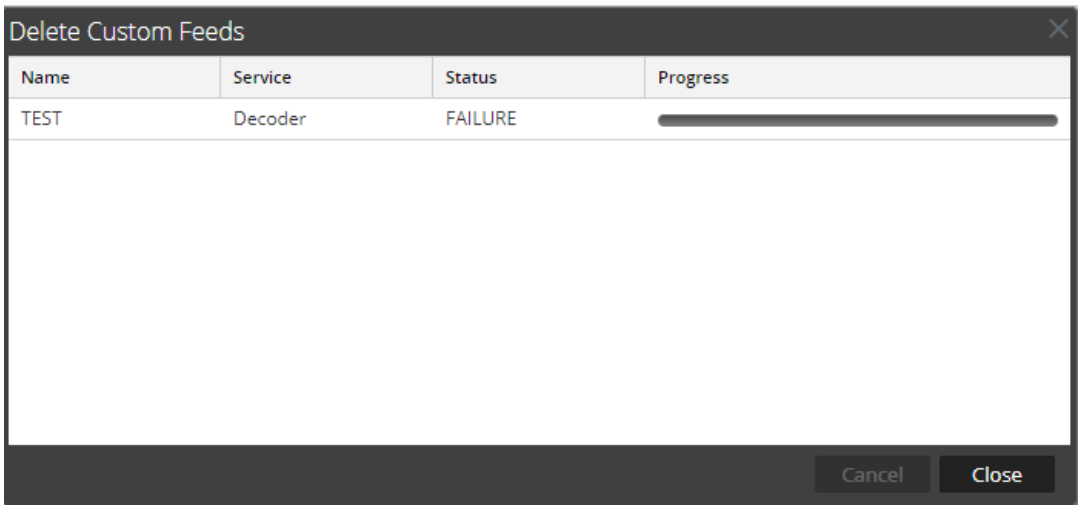
You can select one of the following options to delete the feed:

- If you choose to delete the feed from **Local DB and Service**, the feed is deleted from both the service and the local NetWitness Suite box. The deleted feed will no longer seen on the NetWitness Suite user interface.
- If you choose to delete the feed from **Local DB Only**, the feed is deleted from the local NetWitness Suite box. The deleted feed will not be seen on the NetWitness Suite user interface; however, the last deployed version of the feeds will be present on the service. The undeployed feeds will be deleted forever.
- If you choose to delete the feed from **Service Only**, the feed is deleted from the service. The deleted feed will appear on the NetWitness Suite user interface and can be deployed again

3. Select where you want to delete the feed and click **Delete**.

   A warning dialog is displayed.

4. Click **yes** to confirm that you want to delete the feed from the select areas.
   - If you chose to delete the feed from the **Local DB Only**, the feed is deleted.
   - If you chose to delete the feed from the **Local DB and Service** or **Service Only**, the Delete Custom Feeds view is displayed showing the progress of the deletion on the service.



Miscellaneous Live Services Procedures

This section covers the following procedures:

- Add Subscribed Resources for Deployment to Services
- Delete a Subscription
- Display Resource Details in Live Resource View
- Download a Resource
- Locate and Remove a Deployed Resource from Services
- Remove Subscribed Resources from the Deployments Subscriptions Grid
- Show Results as a List or in Detail
- Subscribe and Unsubscribe to a Resource
- View Resource Details
- View Subscribed Resources Selected to Deploy on Services

Add Subscribed Resources for Deployment to Services

1. Navigate to the **CONFIGURE > SUBSCRIPTIONS > Deployments Tab**.
2. In the **Groups** panel, select a group.
   Subscribed resources, if any, are listed in the Deployments tab Subscriptions panel.
3. In the **Subscriptions** panel, click +.

   The Add Subscription dialog, which lists subscriptions available for deployment, is displayed.
4. Select the subscribed resources that you want to deploy to the services group.
5. Click **Save**.

   The dialog closes and the subscriptions are added to the listing in the Deployments tab, Subscriptions panel. This stages the resources for deployment at the next synchronization.

Delete a Subscription

When you delete a subscription to a resource, deployed instances of the resource are not deleted. The deployed resource remains on services until explicitly removed, but the resource is no longer synchronized with the resource in NetWitness Suite Live.

To delete a subscription:

1. In the **Subscriptions tab**, select the subscriptions that you want to delete.
2. Click .

   A dialog asks for confirmation that you want to delete the subscription.
3. To confirm removal, click **Yes**.

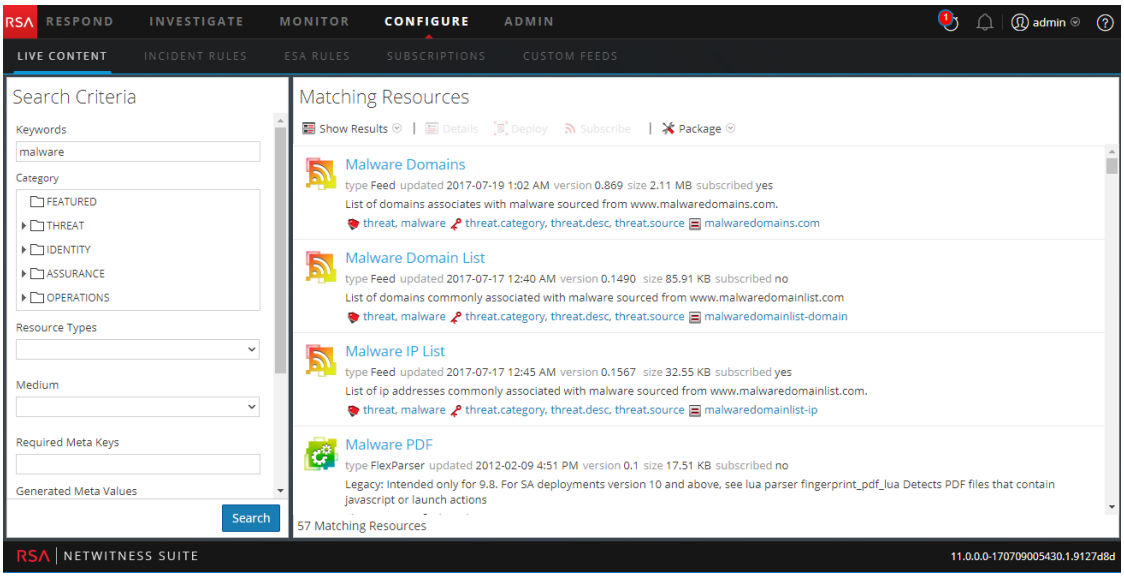
   The subscription is deleted from the subscriptions list, but any deployed instances of the subscribed resource remain on the services.

Display Resource Details in Live Resource View

After you select a resource (in the Live Resource View), you can display its detailed information.

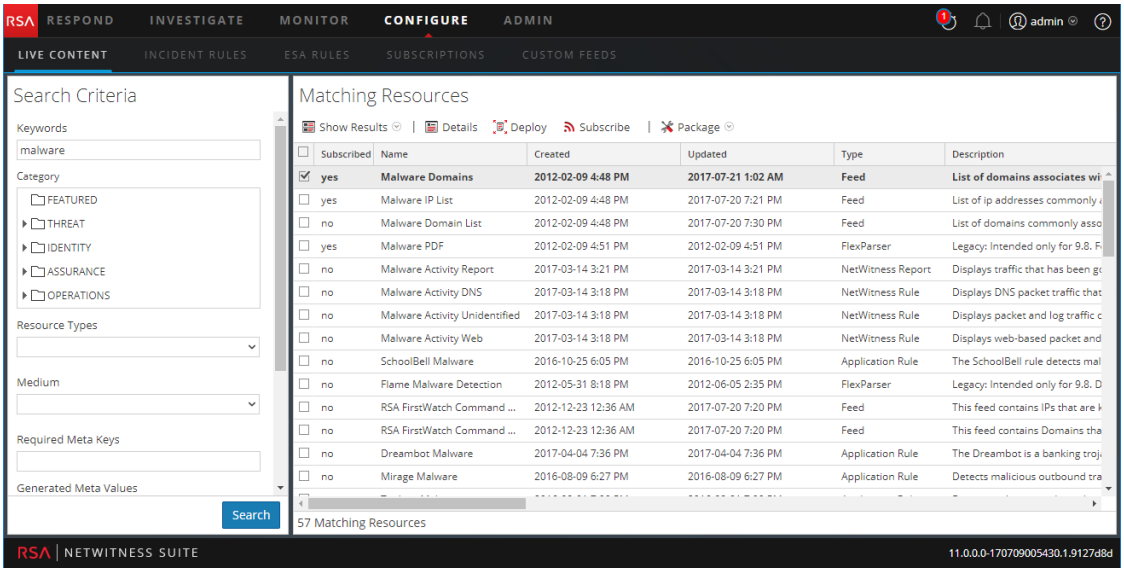
To open a separate tab in the Live Resource view with details of a selected resource, do one of the following:

- If you are viewing the **Detailed Results**, click the resource type icon or the resource name.



- If you are viewing the list results, double-click a resource or select a resource and click

Details.



Download a Resource

You can download a single resource from the Live Resource View.

To download a resource:

1. Go to **CONFIGURE > Live Content**.
2. In the **Search Criteria** panel, enter the criteria needed to return the resource that you want to download.
3. Select a single resource, then click Details.
4. Click Download.

The resource is saved as a ZIP archive to your local Downloads folder.

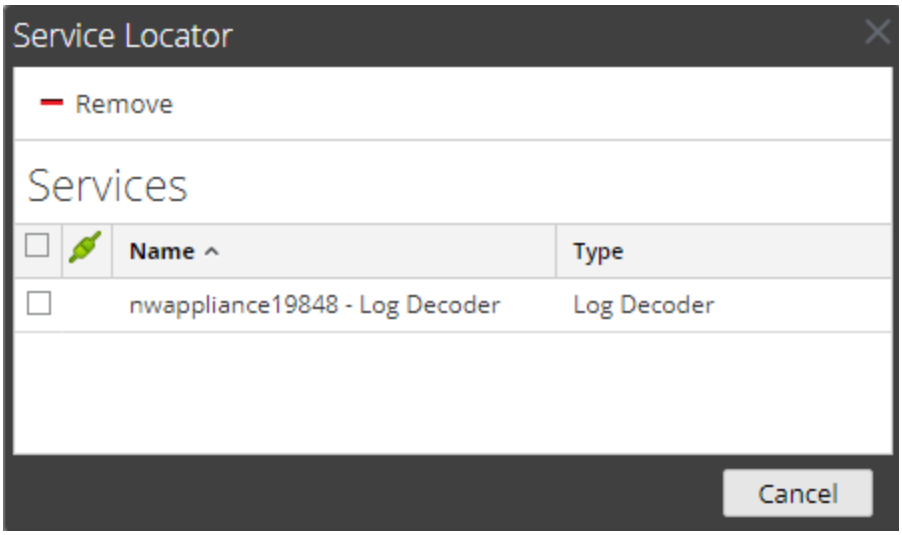
Locate and Remove a Deployed Resource from Services

You can locate and remove a deployed resource from services from the Live Resource View.

To view a list of services on which a resource is deployed:

1. With a resource displayed in the **Resource View**, click Service Locator.

   The Service Locator dialog is displayed.



2. Select one or more services in the **Services** list.
3. Click .

   The resource is removed from the selected services.

Remove Subscribed Resources from the Deployments Subscriptions Grid

Subscriptions that are selected for deployment to a service group are deployed during synchronization. You can remove subscriptions from the Live Configure view > Deployments tab > Subscriptions panel, but any that have actually been deployed to services remain deployed until someone removes them.

To remove resources from the Deployments tab Subscriptions panel:

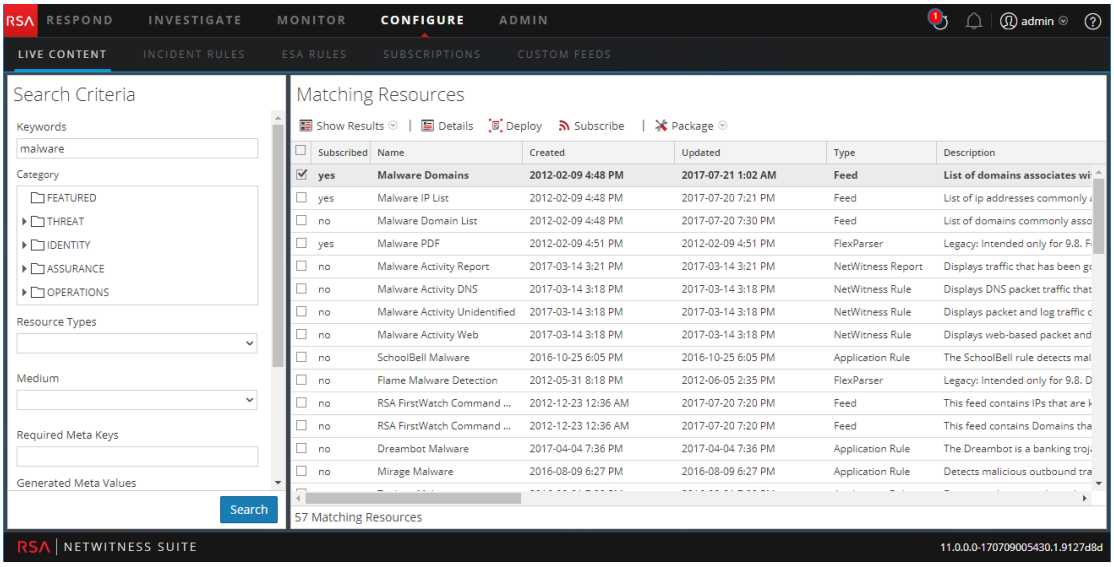
1. In the **Groups** panel, select a group.

   Subscribed resources, if any, are listed in the Subscriptions panel.
2. In the Subscriptions panel, click .

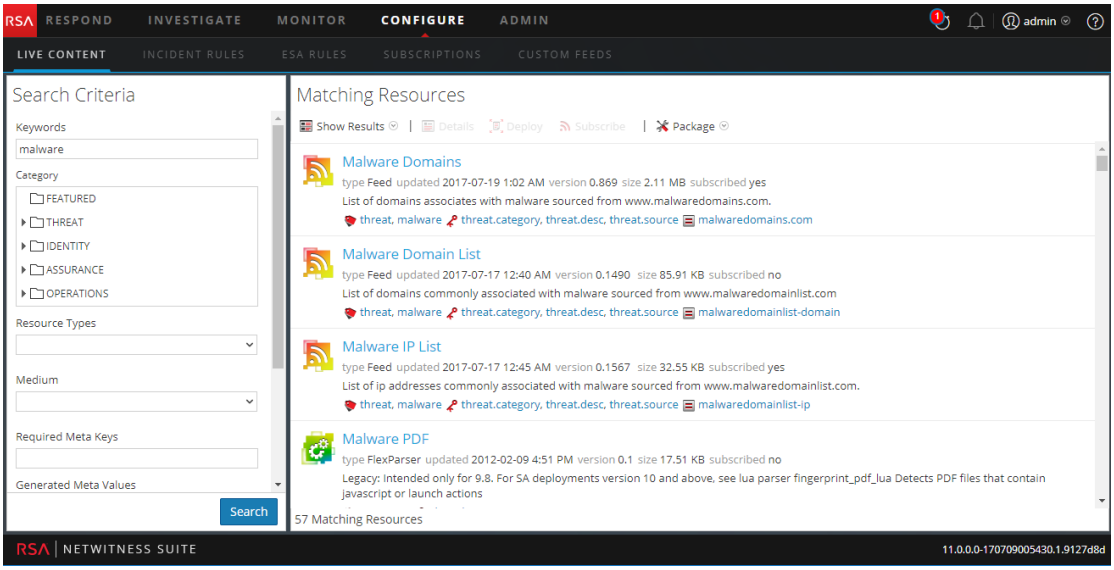
   A dialog requests confirmation that you want to delete the resource from the service group. The resource is removed from the Deployments tab Subscriptions panel, but is not removed from services on which it is deployed.

Show Results as a List or in Detail

1. To change to grid results when viewing detailed results, select **Show Results > Grid**.



2. To change to detailed results when viewing grid results, select **Show Results > Detailed**.



Subscribe and Unsubscribe to a Resource

Subscribe

When you subscribe to resources, you will receive notification when new versions of the resources are available.

To subscribe to a resource:

1. Navigate to the Live > Search view.
2. In the **Search Criteria** panel, specify search criteria and click **Search**.
3. Select one or more resources and click Subscribe.

   A confirmation dialog is displayed: **By subscribing to these resources, you are indicating that you wish to receive notification when new versions are available.**
4. To confirm that you want to subscribe to the resource, click **OK**.

   The resource is added to the subscriptions managed in the Subscriptions tab and is available for deployment in the Deployments tab.

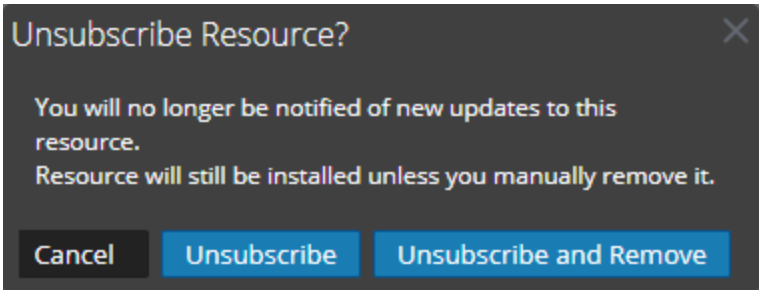
Unsubscribe

When unsubscribing from a resource, you have the option to leave the resource on services on which it is deployed or to remove it from services.

To unsubscribe from a resource:

1. With a resource displayed in **SUBSCRIPTIONS**, click Unsubscribe.

   A confirmation dialog is displayed.



2. Do one of the following:
   - To confirm that you want to unsubscribe from the resource and leave it on the services where it is deployed, click **Unsubscribe**.
   - To confirm that you want to unsubscribe from the resource and remove it from the services where it is deployed, click **Unsubscribe and Remove from Services**.
   - To close the dialog without unsubscribing, click **Cancel**.

   The selected action is applied.

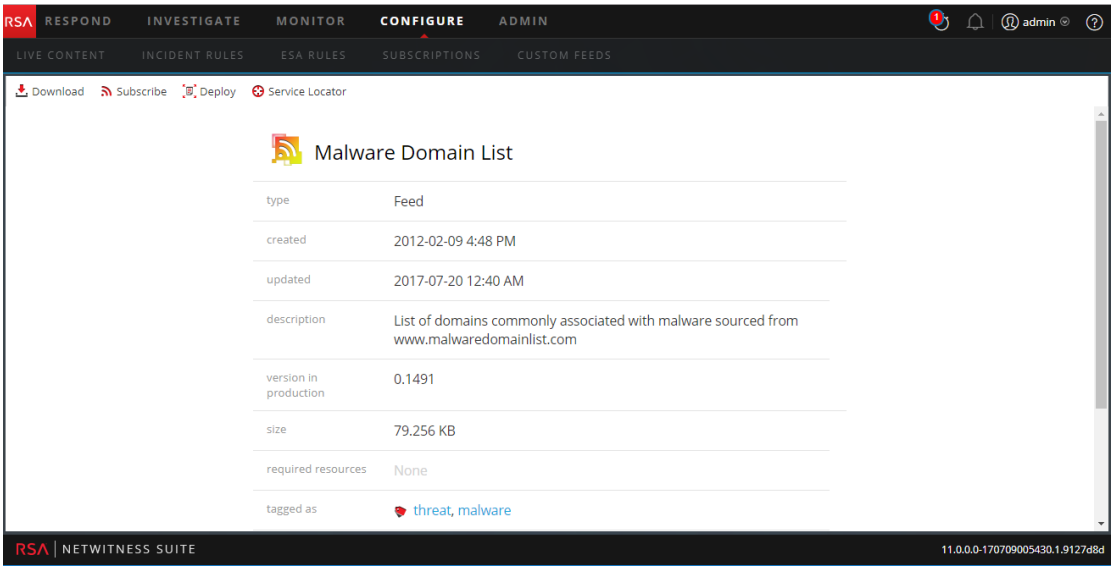
View Resource Details

You can display detailed information about a subscribed resource in the Resource View.

To view details:

1. In the **Subscriptions tab**, select a single subscription.
2. Click Details .

   The details of the resource are displayed in the Resource View.



View Subscribed Resources Selected to Deploy on Services

In the Live Configure view > Deployments tab you can view subscribed resources that have been selected for deployment on services.

To view subscribed resources that have been selected for deployment on services:

In the **Groups** panel, select a group, and expand it to view services in the group.

The resource subscriptions selected for deployment are listed in the Deployments tab Subscriptions panel.

Troubleshooting

This section provides troubleshooting instructions for issues faced when using the Live Services module in NetWitness Suite.

Troubleshooting OutOfMemoryError on Contexthub Server

This section provide troubleshooting instructions when you encounter OutOfMemoryError on Context Hub server and the service becomes unresponsive.

If there are any TAXII feeds configured, Health and Wellness raises alerts when the available heap memory of Context Hub server is critically low. If the status of Context Hub server is Unhealthy because of low memory, perform the following:

1. Make sure that the feeds **Start Date** is within 180 days.
2. Check if any TAXII feed is consuming too much disk space. A TAXII feed can consume maximum of 300 MB. If it consumes more disk space, you must reduce the value in the **Remove STIX data older than** field under **Advanced Options** in the **Custom Feed Creation Wizard** when you edit a TAXII feeds.

Note: If the issue still persists, you must execute step 3.

3. Decrease the number of parallel threads available for processing STIX, perform the following:
   a. Go to **ADMIN** > **Services** > **Context Hub service** > **View** > **Explore**.
   b. In the tree panel, navigate to **enrichment/stix/ config**.
   c. In the right panel, set the **stix-query-scheduler-pool-size** field value to 2. By default the value is 5. This setting controls how many number of threads are allowed to process queries for STIX data at the same time.
   d. Set the **taxii-poll-scheduler-pool-size** field value to 2. By default the value is 5. This setting controls how many number of threads are allowed to poll TAXII servers at the same time.
   e. Restart the Context Hub server.

References

This topic is a collection of references, which describe the user interface and more detailed information about how Live works in NetWitness Suite. These topics are presented in alphabetical order.

- Deployments Tab
- Discontinued Resources Tab
- Live Configure View
- Live Feeds View
- Live Resource View
- Live Search View
- NetWitness Suite Feedback and Data Sharing
- Resource Package Deployment Wizard
- RSA Live Registration Portal
- Subscriptions Tab

Live Configure View

In the Live Configure view, NetWitness Suite provides integrated tools for managing Live resources. You can manage resource subscriptions, deployments to services and discontinued resources. The required role to access this view is **Configure Live Resources**. For a high-level description of how to use the different views in NetWitness Suite Live, please read Live Services Management.

To access this view, go to **CONFIGURE > Subscriptions**. This view has the following tabs:

- Deployments Tab
- Subscriptions Tab
- Discontinued Resources Tab

Deployments Tab

The Deployments tab provides a user interface in the Live Configure view for:

- Viewing subscribed resources that are selected for deployment on services in a service group.
- Selecting subscribed resources to deploy to services in a service group.

- Removing resources that are selected for deployment on services in a service group.

The resources listed here are not deployed immediately after adding to a service group. Instead the subscribed resources are pushed to the services when NetWitness Suite synchronizes with RSA NetWitness Suite Live. The synchronization schedule is configured in the Live Configuration panel. If you do not want to wait for the scheduled synchronization, you can also tell NetWitness Suite to synchronize now in the Live Configuration panel.

Likewise, resources deleted from the Deployments panel are not deleted from service where they have been deployed. To delete resources from services, delete them in the Live Resource View.

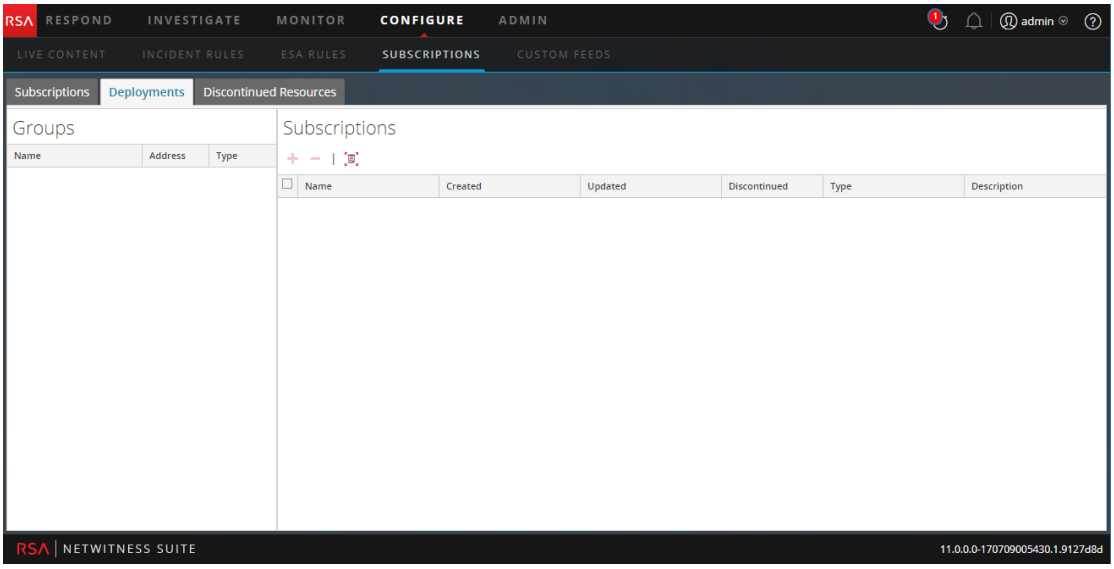
The required permission to access this view is **Manage Live Resources**.

To access this view:

1. Go to **CONFIGURE > Subscriptions**.

   The **Subscriptions** tab is open by default.

2. Click the **Deployments** tab.



The Deployments tab has two panels: **Groups** and **Subscriptions**.

Groups Panel

The Groups panel is a static display of configured service groups that were created in the Administration Services view. Selecting a group in the Groups panel populates the Subscriptions panel with a list of subscriptions that are selected for deployment on the services in the service group.

Feature	Description
Name	This is the service group name. Clicking the plus sign displays a nested list of services in the group.
Address	This is the IP address of each service in the group.
Type	This is the type of service.

Subscriptions Panel

The following table describes the features in the Subscriptions panel.

Feature	Description
	Click to open a dialog that lists subscriptions that were added in the Live Search view or in the Live Resource view and are available for deployment.
	Click to delete the selected subscriptions from the deployment list for service group.
	Click to synchronize your resources to the latest versions available on Live.
Name	This is the name of the resource.
Created	This is the date and time that the resource was created.
Updated	This is the date and time that the resource was last updated.
Type	This is the type of resource.
Description	This is a description of the resource.

Subscriptions Tab

Subscriptions are NetWitness Suite Live resources to which you subscribed in the Live Search view or Live Resource view. When you subscribe to a resource, you agree to receive updates on a regular basis from RSA NetWitness Suite Live. The choices made in the Live Configuration panel determine how often synchronization occurs and if you receive email notifications of updates. In addition, if you don't want to wait for the next update, you can force an immediate synchronization.

The Subscriptions tab provides a way to manage subscriptions. Each resource to which NetWitness Suite is subscribed is listed in this tab.

In the Subscriptions tab, you can:

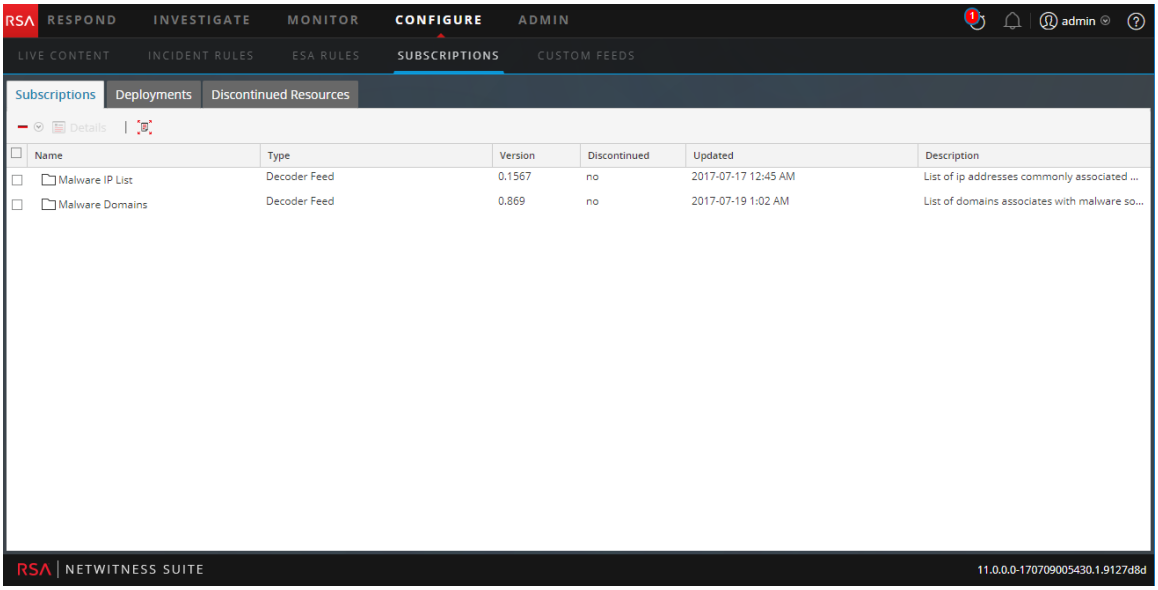
- View all resources to which this NetWitness Suite instance is subscribed.
- Open a detailed view of a subscription in the Live Resource View.
- Delete a subscription.

Note: Subscribing to a resource does not deploy the resource to any services. To deploy one or more subscribed resources, go to the Deployments tab. To deploy a single resource manually, use the Deploy option in the Resource View.

The required permission to access this view is **Manage Live Resources**.

To access this view, in the main menu, select **CONFIGURE > Subscriptions**.

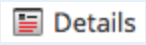
The Subscriptions tab is open by default.



The **Subscriptions** tab has a toolbar and a grid.

Toolbar

This table describes the options available in the toolbar.

Feature	Description
	Deletes the selected subscriptions.
	Displays the details of a single subscribed resource in the Resource View.
	Check the Live Server for the latest discontinued resources.

Grid

Column	Description
	Selects subscribed resources to view in detail or delete. You can view details for a single resource. You can delete one or more resources from the subscribed resources, in effect unsubscribing.
Name	This is the name of the subscribed resource.
Type	This is the type of subscribed resource.
Version	This is the version of the subscribed resource.
Discontinued	Indicates the status of the discontinued resources for the subscribed resource. **Yes** - Resource is discontinued. **No** - Resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Updated	This is the date and time when the subscribed resource was last updated.
Description	This is a description of the subscribed resource.

Discontinued Resources Tab

This topic introduces the features of the **Live Configure view > Discontinued Resources** tab.

The Discontinued Resources tab provides a user interface in the Live Configure view for:

- Scanning the services for the discontinued resources.
- Removing the discontinued resources from any service or service group.

Note: Discontinued content still appears. With discontinued content there just won't be any updates, and users won't see these items when they search in Live, unless they check the **Include Discontinued Resources** box while searching.

In the RSA Content space on RSA Link, you can view the complete, up-to-date list of discontinued resources (Discontinued Content). For each resource, there is a description of why it was discontinued. Use these details to determine whether or not to remove a discontinued resource from your installation. .

The required permission to access this view is **Manage Live Resources**.

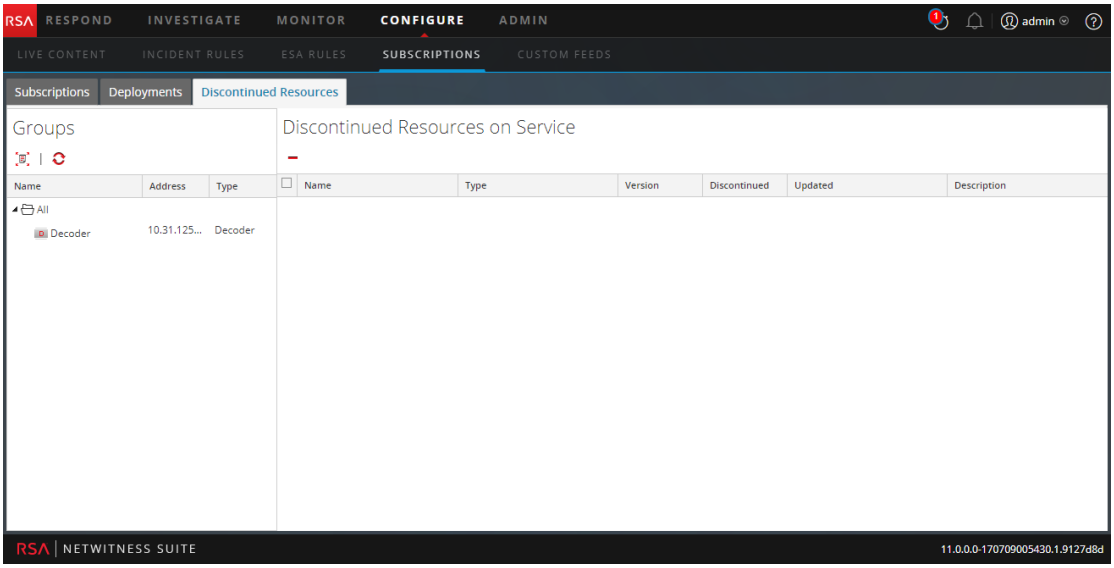
To access this view:

1. Go to t **CONFIGURE > Subscriptions**.

   The **Subscriptions** tab is open by default.

2. Click the **Discontinued Resources** tab.

   This is an example of the Discontinued Resources tab.



The Discontinued tab has two panels: Groups and Discontinued Resources on Service.

Groups Panel

The Groups panel is a static display of configured service groups that were created in the Admin Services view. Selecting a group in the Groups panel populates the Discontinued Resources panel with a list of discontinued resources which are deployment on the selected service or service group.

Feature	Description
	Click to scan the services for a discontinued resource.
	Displays the current status of the discontinued resources on a service. **Note:** The status of a service may change while the services are being scanned.
Name	This is the service group name. Clicking the plus sign displays a nested list of services in the group.
Address	This is the IP address of each service in the group.
Type	This is the type of service.

Discontinued Resources on Service Panel

The following table describes the features in the Discontinued Resources on Service panel.

Feature	Description
	Click to delete the selected resources from the service or service group.
Name	This is the name of the resource.
Type	This is the type of resource.
Version	Version of the discontinued resource.
Discontinued	Indicates the status of the discontinued resources for the subscribed resource. **Yes** - The resource is discontinued. **No** - The resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Updated	This is the date and time that the resource was last updated.
Description	This is a description of the resource.

Live Feeds View

Use the Live Feeds View to:

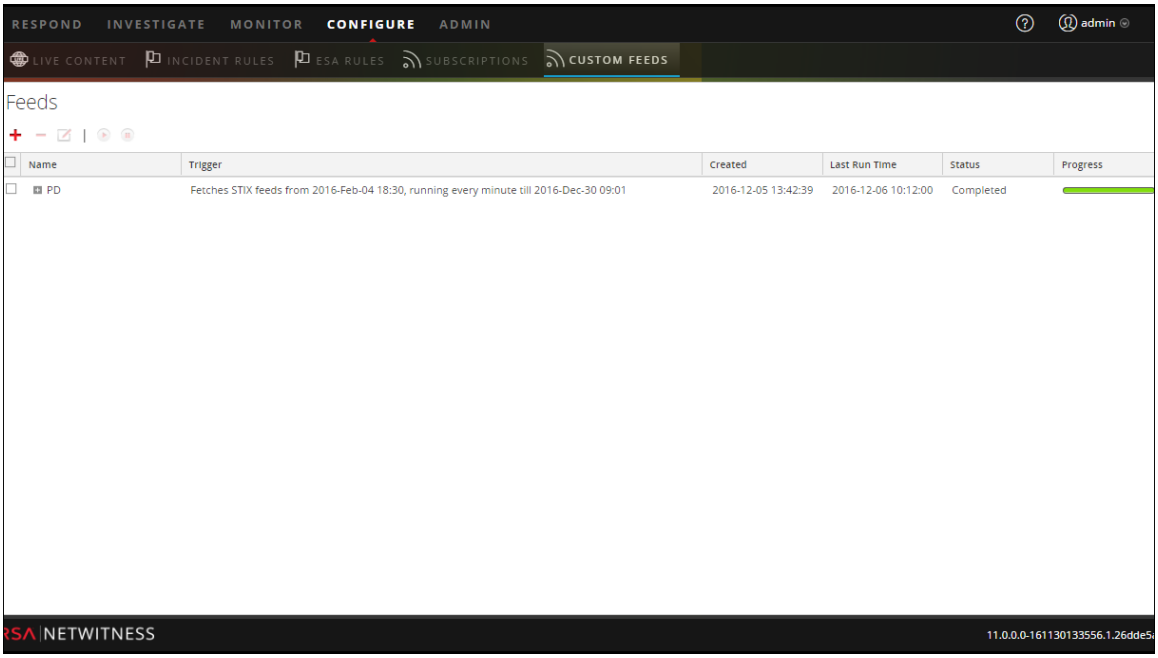
- Create custom feeds.
- Create identity feeds.
- Edit feeds.

The required role to access this view is **Manage Devices**.

To access this view, do one of the following:

- In the main menu, select **Live > Feeds.**
- From any view in the Live Module, select **Feeds** in the main menu.

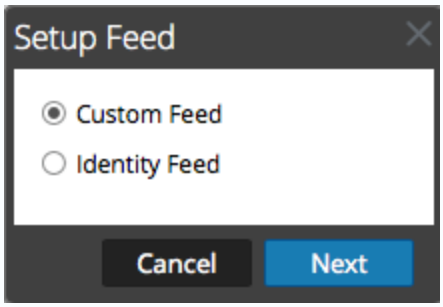
This is an example of the Feeds view.



The **Feeds** tab has a toolbar and a grid.

Toolbar

This table describes the options in the toolbar.

Feature	Description
	Initiates the creation of a custom or identify feed by displaying the **Setup Feed** dialog is displayed.  • Custom Feed opens the **Configure a Custom Feed** wizard. • Identity Feed opens the **Configure Identity Feeds** wizard.
	Deletes the feed that you selected.
	Opens the Configure Custom Feed or Configure Identity Feed wizard for the feed that you selected (see Edit a Feed.
	Start or resume data feed.
	Stop or pause data feed.

Feeds Grid

This table describes the columns in the grid.

Column	Description
	Selects a feed.
Name	Name of the feed. **Note:** You can now use special characters to define the name of the custom feed.
Trigger	Displays how often the feed runs which is determined by what you defined in **Feed Task Type** when the feed was created.
Created	This is the date and time when the feed was created.

Column	Description
Disk Usage	Displays the MongoDB storage size used by the TAXII feed.
Last Run Time	This is the date and time when the feed was last run.
Status	The status of the feed.
Progress	Progress bar.

Live Resource View

The Live Resource View shows a detailed view of a selected resource, and has options to:

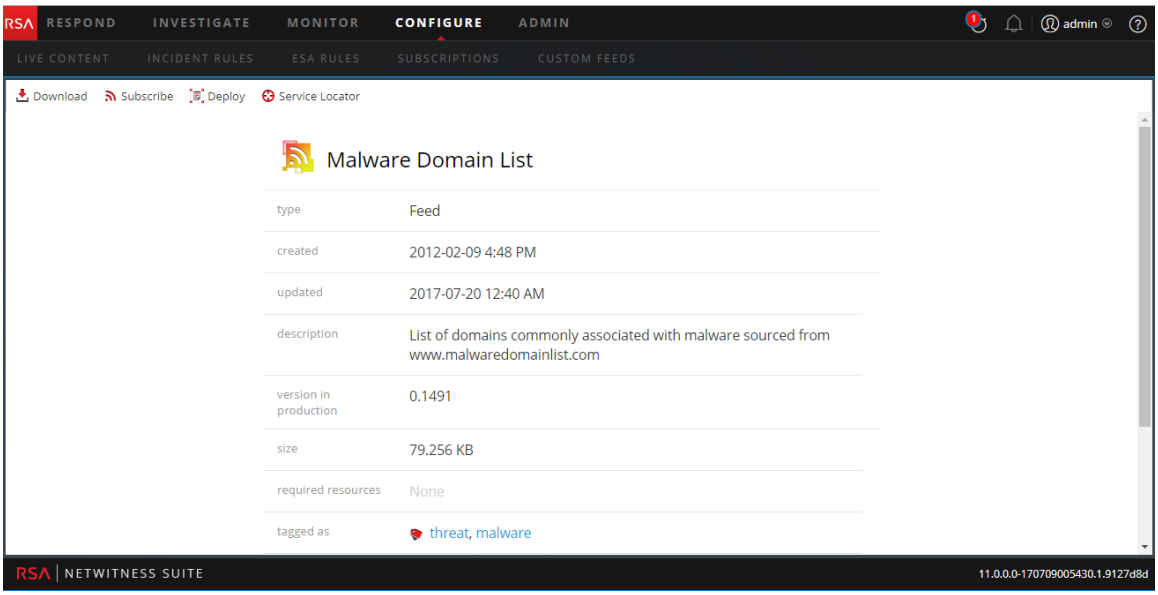
- Download the resource.
- Subscribe or unsubscribe the resource.
- Deploy the resource to services.
- Locate services on which the resource is deployed and remove the resource from services.

The required permission to access this view is View Live Resource Details.

To access this view, do one of the following:

1. In the main menu, select **CONFIGURE > LIVE CONTENT > Search Criteria**.
2. In the Live Search view, **Detailed Results**, click the resource type icon or the resource name.
3. In the Live Search view, **Grid Results**, double-click a resource or select a resource and click **Details**.

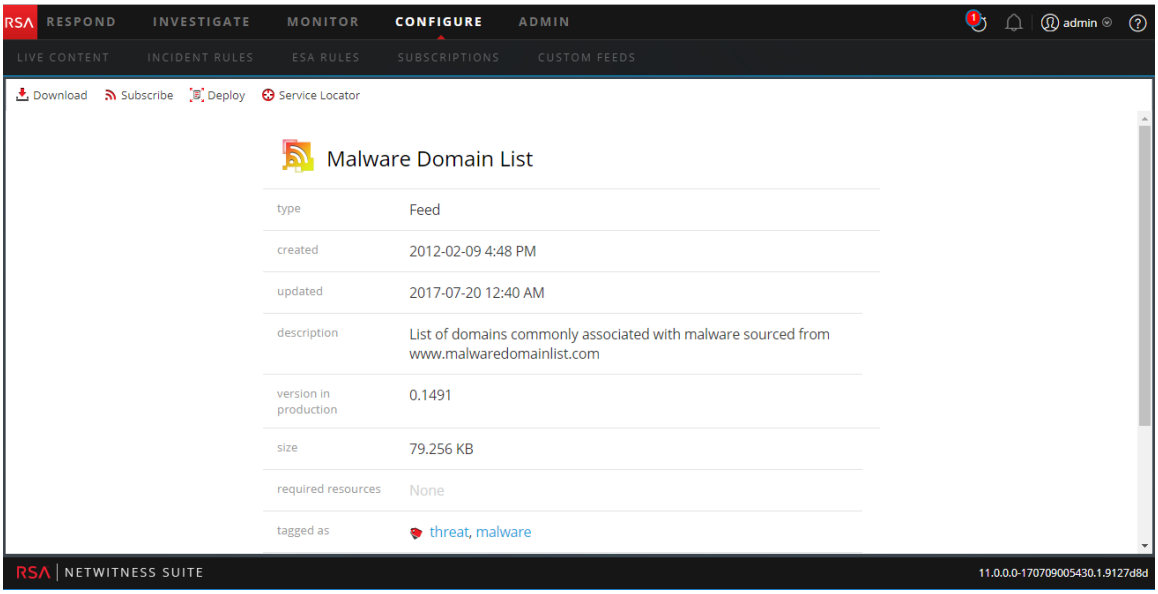
This is an example of the Resource view.



The Live Resource View has a detailed view of a single resource and a toolbar.

Resource Details

This is an example of the resource details displayed in the Resource View.



The following table describes the elements in the Resource Details section.

Feature	Description
Resource Type Icon	A graphic representation of the resource type, for example .

Feature	Description
Name	The name of the resource, for example, **fingerprint_office_lua**.
Type	The type of resource, for example, **RSA Lua Parser**.
Created	The date the resource was created, for example, **2013-09-15 02:16 PM**.
Updated	The date the resource was last updated, for example, **2013-09-15 02:16 PM**
Description	The description of the resource, for example, **Identifies Microsoft Office 95, 2007 Word, Excel, and PowerPoint documents**.
Version in production	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **9.079 KB**.
Required Resources	A list of resources on which this resource depends, for example, **NetWitness Lua Library**. Clicking a resource replaces the currently displayed details with the details of the one you clicked.
Tagged as	The tags that apply to the resource. In the example, the tag is **featured, informational**. Clicking a tag opens the Live Search View with the search narrowed to match resources with that tag.
Required Meta Keys	The meta keys that apply to the resource. In the example, there are no meta keys required. Clicking a meta key opens the Live Search View with the search narrowed to match resources with that meta key.
Generates Meta Values	The meta values that the resource generates. In the example, there are no meta values generated. Clicking a meta value opens the Live Search View with the search narrowed to match resources with that meta value.
Permissions	The permissions required for the resource.

Resource View Toolbar

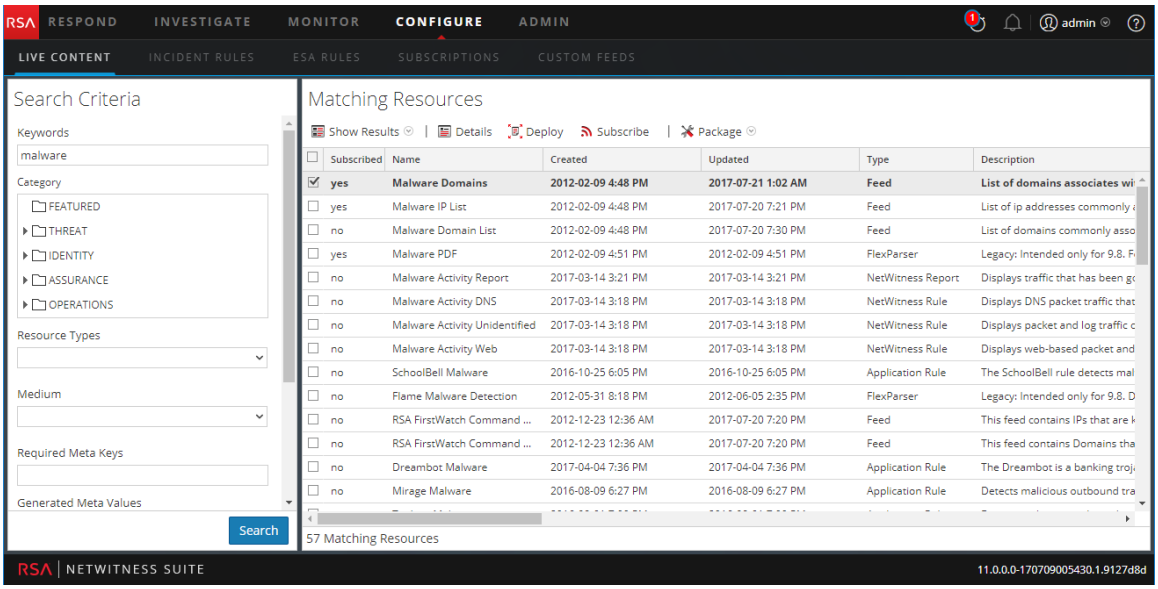
This table describes the Live Resource view toolbar options.

Feature	Icon	Description
Download		This option downloads the resource currently displayed in the Resource View.
Subscribe or Unsubscribe		This option subscribes to or unsubscribes from the resource currently displayed in the Resource View. • Clicking **Subscribe** opens a dialog notifying that you are agreeing to receive notification when the selected resources are updated. You can cancel or click **OK**. • Clicking **Unsubscribe** asks for confirmation that you want to stop receiving notification when the selected resources are updated. You can then choose to cancel or you can click **Unsubscribe** or **Unsubscribe and Remove**, which also removes the resource from services on which it is deployed.
Deploy		This option provides a way to deploy the resource currently displayed in the Resource View. Clicking **Deploy** opens the Manual Resource Deployment dialog.
Service Locator		This option displays a list of services on which the currently displayed resource is deployed. You can remove the resource from all services or selected services.

Live Search View

The Live Search view provides the ability to browse the configured Live CMS for resources. Once matching resources are found, you can view details, subscribe to resources, and deploy resources to services and service groups.

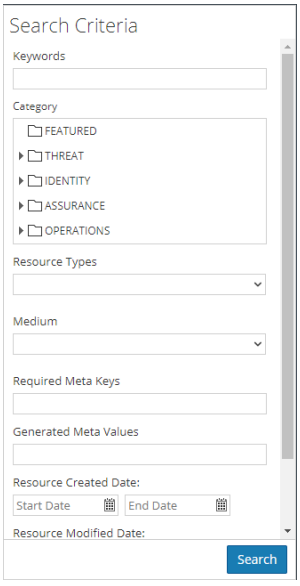
This is an example of the Search view.



The Live Search view has a panel for specifying search criteria and a panel that displays matching resources. The Search Criteria panel is collapsible to provide more width for viewing the Matching Resources panel.

Search Criteria Panel

This is an example of the Search Criteria panel.



The following table provides descriptions of the Search Criteria panel features.

Feature	Description
Keyword(s)	Enter a keyword or keywords to browse for resources that have the keyword in the resource name or the resource description. You can use wildcards when you enter a keyword.
Category	The categories mirror the hierarchical Investigation Model that RSA uses to organize resources. The purpose of the Investigation model is to deliver an accurate path to information security incident response. For more details, see the Investigation Model topic.
Resource Types	Select resources types from the drop-down list to filter resources by type of resource. Possible values are: • Advanced Analytics (Warehouse) • Application Rule • Bundle • Correlation Rule • Event Stream Analysis Rule • Feed • FlexParser • Log Collector • Log Device • Lua Parser • Malware Rules • NetWitness List • NetWitness Report • NetWitness Rule

Feature	Description
Medium	Select one or more mediums from the drop-down list to search for content based on the meta data source. Available values for medium are as follows: • **log**: applied to content that uses meta derived from log data • **packet**: applied to content that uses meta derived from network packets • **log and packet**: applied to content that correlates meta derived across log and packet data
Tags	Select meta tags from the drop-down list to browse based on how the meta is tagged. For example, to browse resources for a Log Decoder, select the **netwitness for logs** tag. Alternatively, you can click a tag in the Matching Resources panel to insert that tag in this field.
Required Meta Key(s)	Enter a specific meta key; for example, **threat.source**. Alternatively, you can click a meta key in the Matching Resources panel to insert that tag in this field.
Generated Meta Value(s)	Enter a generated meta value; for example, **netwitness**. Alternatively, you can click a generated meta key in the Matching Resources panel to insert that tag in this field.
Research Created Date	Specify a date range during which resources were created. For example, to browse resources that were created between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click and pick dates from a calendar.
Research Modified Date	Specify a date range during which resources were modified. For example, to browse resources that were modified between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click and pick dates from a calendar.

Feature	Description
Search	Click **Search** to send the search request to the Live server. More specific search criteria return matching resources more quickly.
Cancel	Click **Cancel** to cancel the search in progress.
Include Discontinued Resources	Check **Include Discontinued Resources** to include the discontinued resources in the search result. For an up-to-date list of resources that have been discontinued, see the Discontinued Content topic.

Matching Resources Panel

The Matching Resources panel presents search results based on the selections made in the Search Criteria panel. Results are initially displayed in a grid, but you can switch between two Show Results options: Detailed or Grid.

Detailed Results

In the detailed results, you can click a tag, meta key, or resource meta value to auto fill the Search Criteria panel and pivot the search results.

The following table describes the elements in the detailed results.

Feature	Description
Resource Type Icon	A graphic representation of the resource type. For example .
Name	The name of the resource, for example, **Group Management**. **Note:** (Discontinued) is displayed next to the resource name if a resource is discontinued.
Type	The type of the resource, for example, **Rule**.
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Version	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **153 B**.

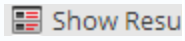
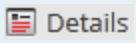
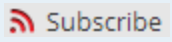
Feature	Description
Subscribed	Subscription status: • **yes**: This NetWitness Suite instance is subscribed to this content resource. • **no**: This NetWitness Suite instance has not subscribed to this content resource.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
Tags	The tags that apply to the resource. Clicking a tag narrows the search to resources with that tag. For example, .
Meta Keys	The meta keys that apply to the resource. Clicking a meta key narrows the search to resources with that meta key. For example, .
Resource Meta Values	The meta values generated by the resource. Clicking a meta value narrows the search to resources that generated the meta value. For example, .

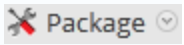
Grid Results

In the grid view, you can select one or more resources and use additional options in the toolbar to view the details of a single resource, subscribe to resources, and deploy resources.

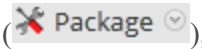
The following table describes the elements in the grid results.

Feature	Description
Subscribed	Subscription status: • **yes**: This NetWitness Suite instance is subscribed to this content resource. • **no**: This NetWitness Suite instance has not subscribed to this content resource.
Name	The name of the resource, for example, **Group Management**. **Note:** The resource name is displayed in red color if it is discontinued.
Created	The date the resource was created, for example, **2015-08-12 3:11 PM**.

Feature	Description
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Type	The type of the resource, for example, **Rule**.
Discontinued	The status of the discontinued resources: **yes** - The resource that matches the search criteria is discontinued. **no** - The resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
Toolbar	
	This menu offers two ways to view search results: **Detailed** and **Grid**.
	This option applies to a single selected resource. Clicking **Details** opens the selected resource in the Live Resource view.
	This option applies to one or more selected resources.
	This option applies to one or more selected resources. Clicking **Subscribe** opens a dialog that asks for confirmation that you want to receive notification when the selected resources are updated.

	This menu offers two packaging functions for the selected resources:
	• **Create**: creates a **resourceBundle.zip** file that contains the selected resources and opens a dialog in which you can either:
	  • open the file, or
	  • save the file for subsequent deployment.
	• **Deploy**: opens the Deployment Wizard, in which you can choose a **resourceBundle.zip** file and deploy it.

See Also

- For more details on Deployment ( ), see Find and Deploy Live Resources.
- For more details on Deploying a Package (), see the Resource Package Deployment Wizard,.

Resource Package Deployment Wizard

If you have created a package of resources and saved it on a network drive, you can use the Resource Package Deployment Wizard to deploy the resources manually to a service or a service group without subscribing to the resources. NetWitness Suite accepts packages in **.nwp** files or **.zip** files.

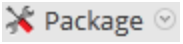
Deploying resources manually deploys them directly to the services without taking advantage of the powerful resource management capabilities of NetWitness Suite.

If you want to receive notification and updates for updated resources and be able to easily remove resources from a service, you must subscribe to resources in the Live Search view and deploy the resources in the **Live Configure** view.

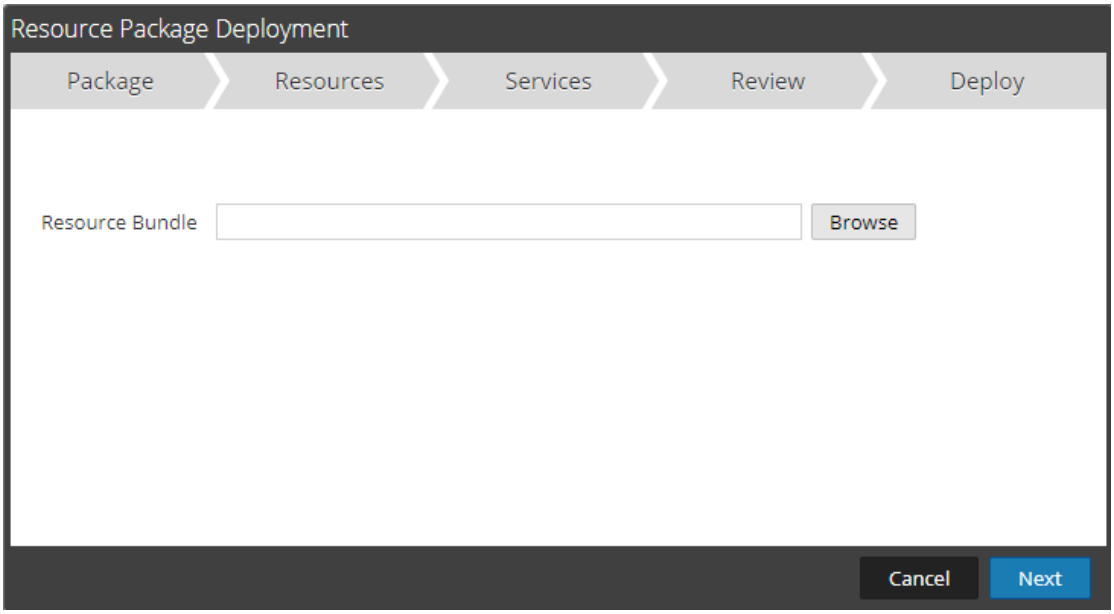
Note: Use NetWitness Suite Live to create resource bundles; this is a different application that is not part of NetWitness Suite. Selecting **Package** > **Create** in the **Live Search - Matching Resources** toolbar displays the Content Package Tool window. You can choose resources to include in a package and save the package as a NetWitness Suite Package File.

The required permission to access this view is **Deploy Live Resources**.

To access this view:

1. In the main menu, select **CONFIGURE > Live Content**.
2. In the **Live Search - Matching Resources** toolbar, select  > **Deploy**.

The Resource Package Deployment wizard is displayed.



Features

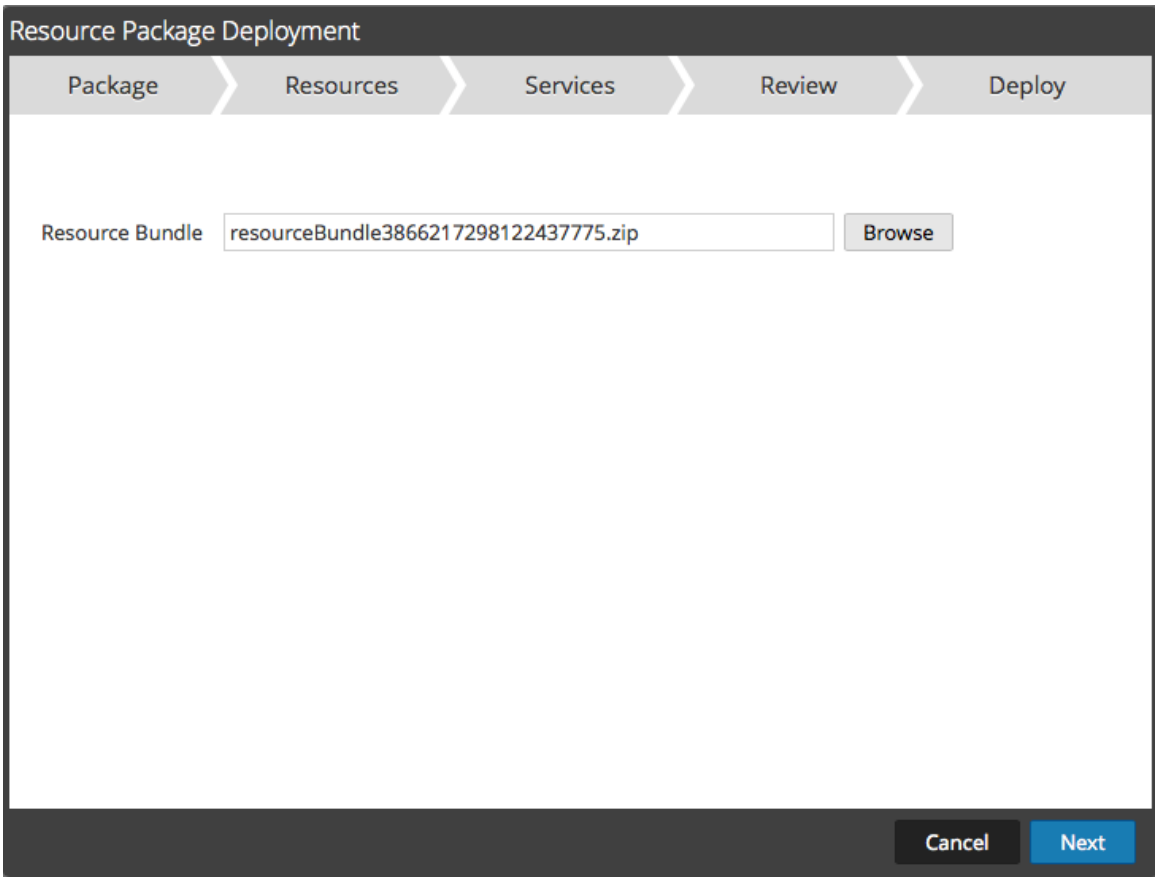
The Deployment Wizard has five tabs: **Package, Resources**, **Services**, **Review** and **Deploy**. Use **Close** to exit before you complete the wizard.

When you complete the wizard, NetWitness Suite returns to the Live Resources View.

Package Tab

You use this tab to select a resource bundle from your network in this page.

This is an example of the Package tab, with a resource bundle already selected.



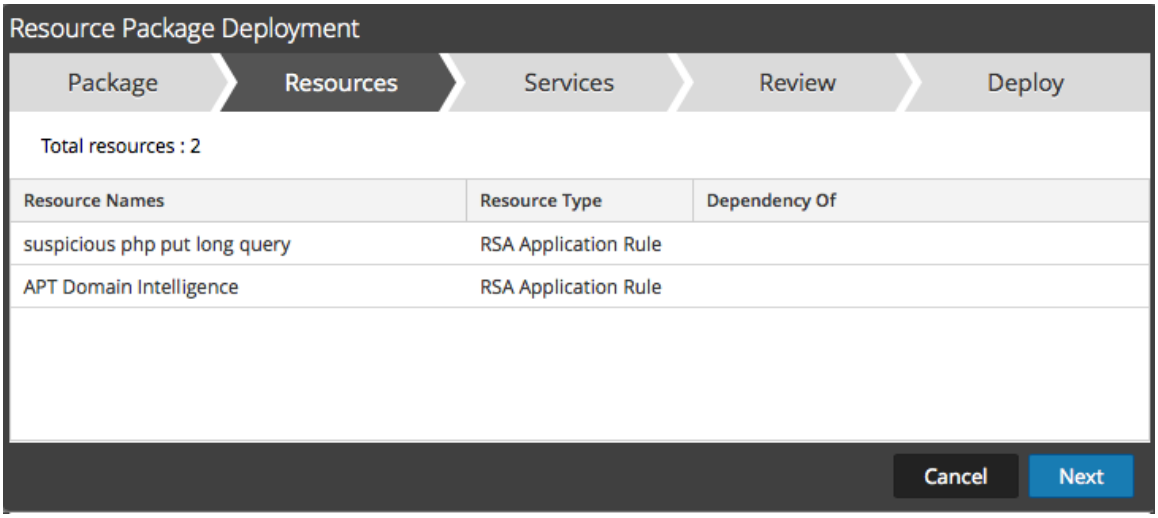
The following table describes the elements in the Package tab.

Column	Description
Resource Bundle	The input field to specify a resource bundle. You can type a path in this field or search using the Browse button.
Command Buttons	
Browse	This button opens a File Upload dialog in which you can browse the local file system and select a bundle.
Cancel	Cancels the deployment and closes the wizard.
Next	Displays the next tab of the wizard.

Resources Tab

This tab displays the resources contained in the bundle.

The following figure shows an example of the Resources tab.



The following table describes elements in the Resources tab.

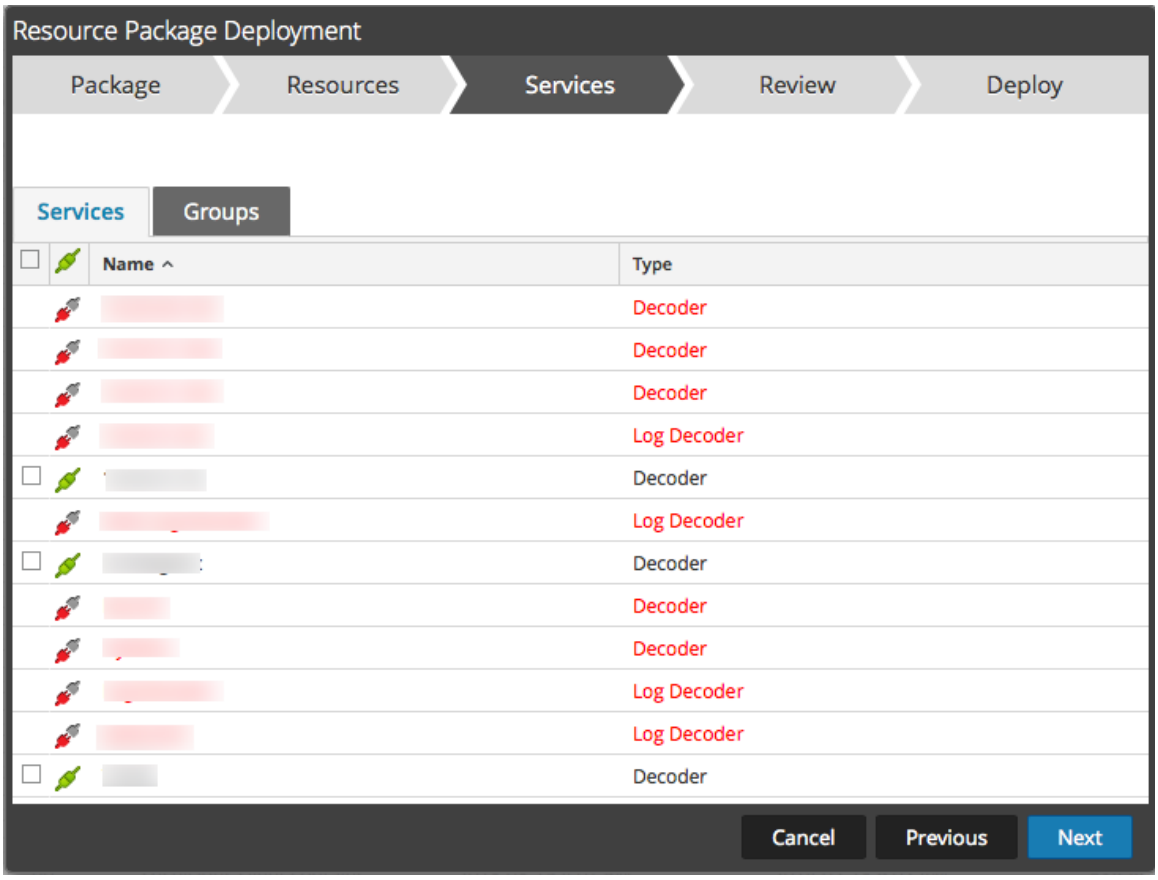
Column	Description
Resource Name	Displays the name of the resources in the bundle (for example, **NetWitness Lua Library**).
Resource Type	Displays the resource types for the resources in the bundle (for example, **RSA Lua Parser**)
Dependency Of	Displays Resources on which the selected resource depends (for example, **AIM lua**).

Services Tab

You select the services to which you want to deploy the resources in the bundle.

The Services tab has two tabs, **Services** and **Groups**. These provide a list of services and service groups that are configured in the ADMIN > Services view. The columns are a subset of the columns available in the Services view. You can select the services or the service groups to which you want to deploy the resources in the bundle.

This is an example of the Services tab.



The following table describes the elements in the Services tab.

Column	Description
Services	
	Selects services to which you want to deploy the content. You can select any combination of services and service groups.
Name	Displays the services in your environment to which you can deploy the content.
Host	Displays the name of the resource host.
Type	Displays the type of NetWitness Suite service.
Groups	
	Selects service groups (if you have service groups defined in your environment).
Name	Displays the names of the service groups.

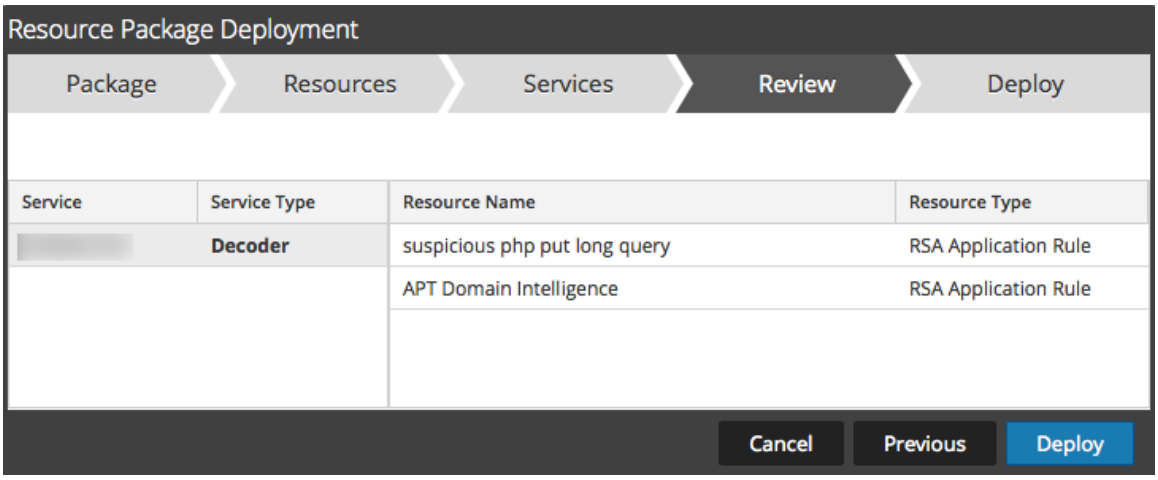
Review Tab

Displays the resources and services on which the resources will be deployed.

In this tab, you can do the following:

- Review the content and services before you deploy.
- Initiate the deployment of the resources.

The following figure shows an example of the Review tab.



The following table describes the elements in the Review tab.

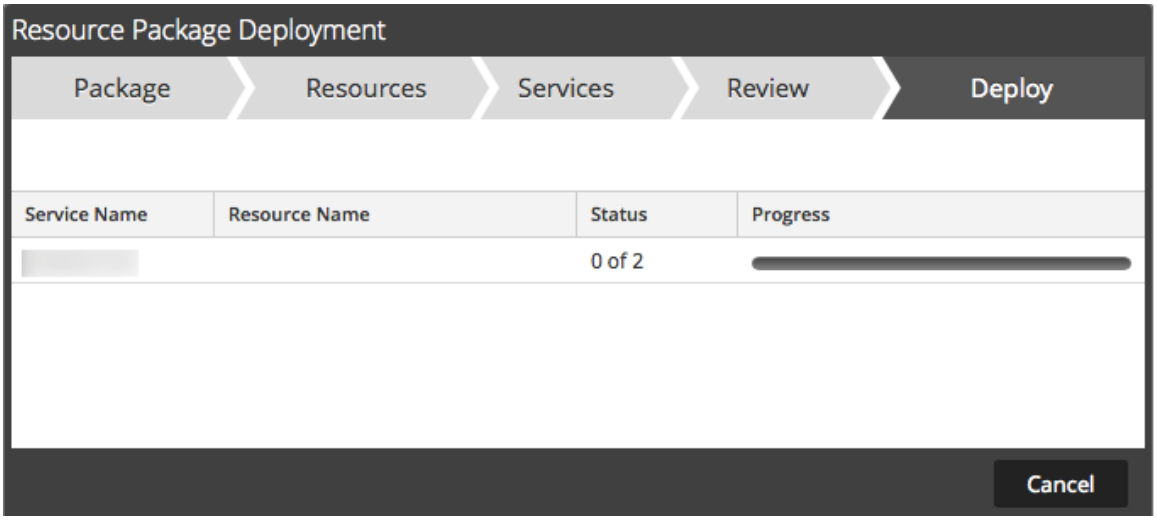
Column	Description
Service Information	
Service	Displays the services in your environment to which you can deploy the content.
Service Type	Displays the type of each NetWitness Suite service (type of host/service).
Resource Information	
Resource Name	Displays the name of the resources you have selected (for example, **NetWitness Lua Library**).
Resource Type	Displays the resource types for the resources you have selected (for example, **RSA Lua Parser**).
Deploy	Initiates the deployment of the resources and displays the **Deploy** page (final page of the wizard).

Deploy Tab

This tab allows you to do the following:

- View the progress of the job
- Cancel the job

This is an example of the Deploy tab.



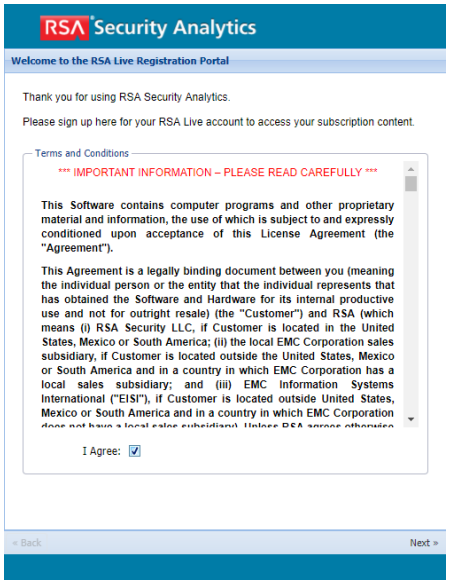
The following table describes the elements in the Deploy tab.

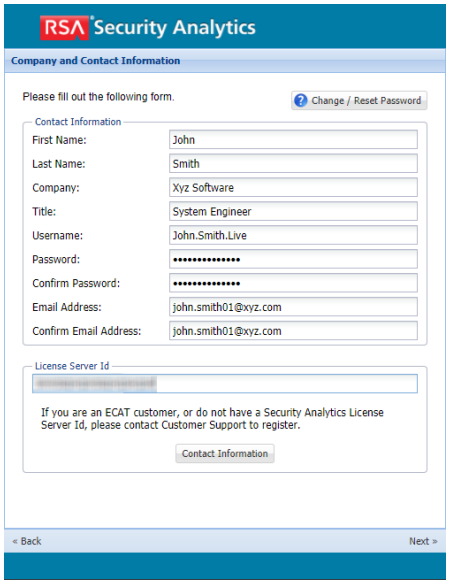
Feature	Description
Service Name	Name of the services to which resources are deployed.
Resource Name	Name of the resources.
Status	Status of the manual deployment.
Progress	Progress of the manual deployment in a progress bar. When complete, the bar is solid green.
Command Buttons	
Close	Closes the wizard.

Feature	Description
Errors	Only displays if NetWitness Suite encountered any errors. Click to display the errors.
Retry	Only displays if NetWitness Suite encountered any errors. Click this button to try to deploy the resources again using the wizard.

RSA Live Registration Portal

The RSA Live Registration Portal is a self-service wizard in which customers can set up a Live account and change or reset the password. A Live account is required to get access to the feeds, parsers, rules, and other content in RSA Live library. To access the portal, go to the following URL: https://cms.netwitness.com/registration/.





After you agree to the Terms and Conditions, click **Next**: the fields for setting up an account are displayed. These include Contact Information, Subscription Level, and License Server Id.

The following table lists the contact information section fields and its descriptions:

Parameter	Description
Change / Reset Password	Allows users to change or reset their RSA Live password.
First Name	Your first name.

Parameter	Description
Last Name	Your last name.
Company	The name of your company.
Title	Your job title or function in the company.
Username	The username used to log on to RSA Live account. The username must contain a minimum of nine characters and a maximum of 60 characters.
Password	The password for the RSA Live account. The password must contain minimum of nine characters and the maximum length is 60, with at least one uppercase, one lowercase, one number, and one special character.
Confirm Password	Confirmation of your password.
Email Address	The email address where you want to receive notifications related to the Live account.
Confirm Email Address	Confirmation of the email address.
Subscription Level / Confirm Subscription Level	• **Basic** - This provides access to the Live content that is tagged for groups like Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis. • **Enhanced** - This provides access to the Live content that is tagged for groups like Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis. • **Premium** - This provides access to the Live content that is tagged for groups like Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.
License Server Id	This is the License Id on the **ADMIN > SYSTEM > Info** page. **Caution:** The license server ID on NetWitness Suite must be valid and must be registered on the Flexera Server. If not, contact RSA Customer Support.

NetWitness Suite Feedback and Data Sharing

This topic introduces the Feedback and Data Sharing features of NetWitness Suite.

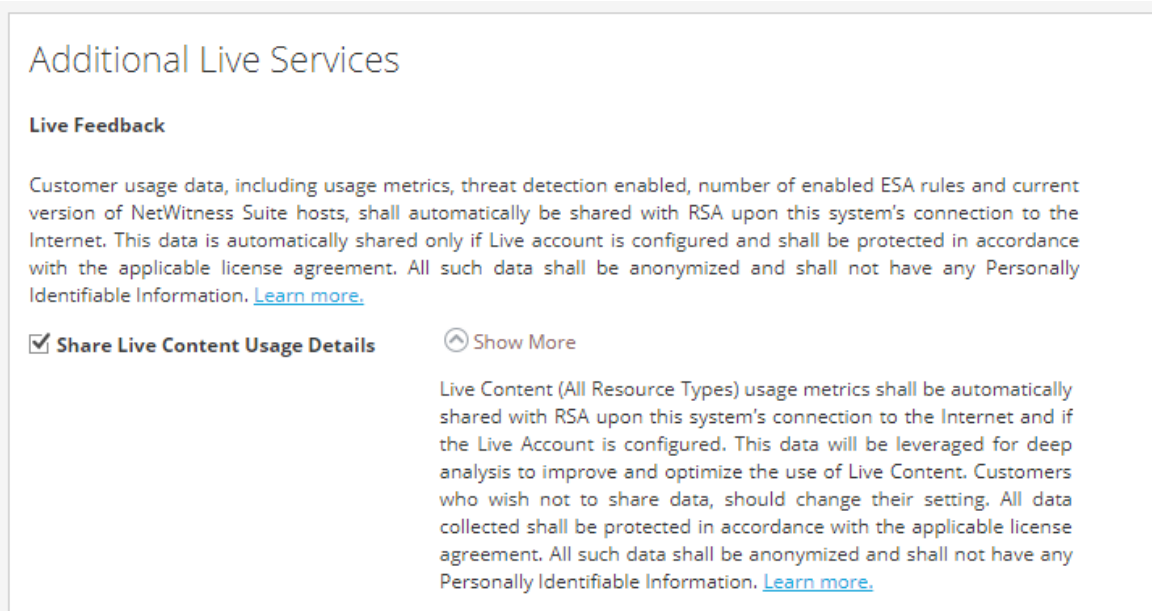
The settings for these features are available in **ADMIN** > **SYSTEM** > **Live Services** view, in the Additional Live Services section.

Additional Live Services

Participation in the Additional Live Services is configured in the **ADMIN > SYSTEM > Live Services** view.

Live Feedback

Live Feedback is intended to help improve RSA NetWitness Suite.



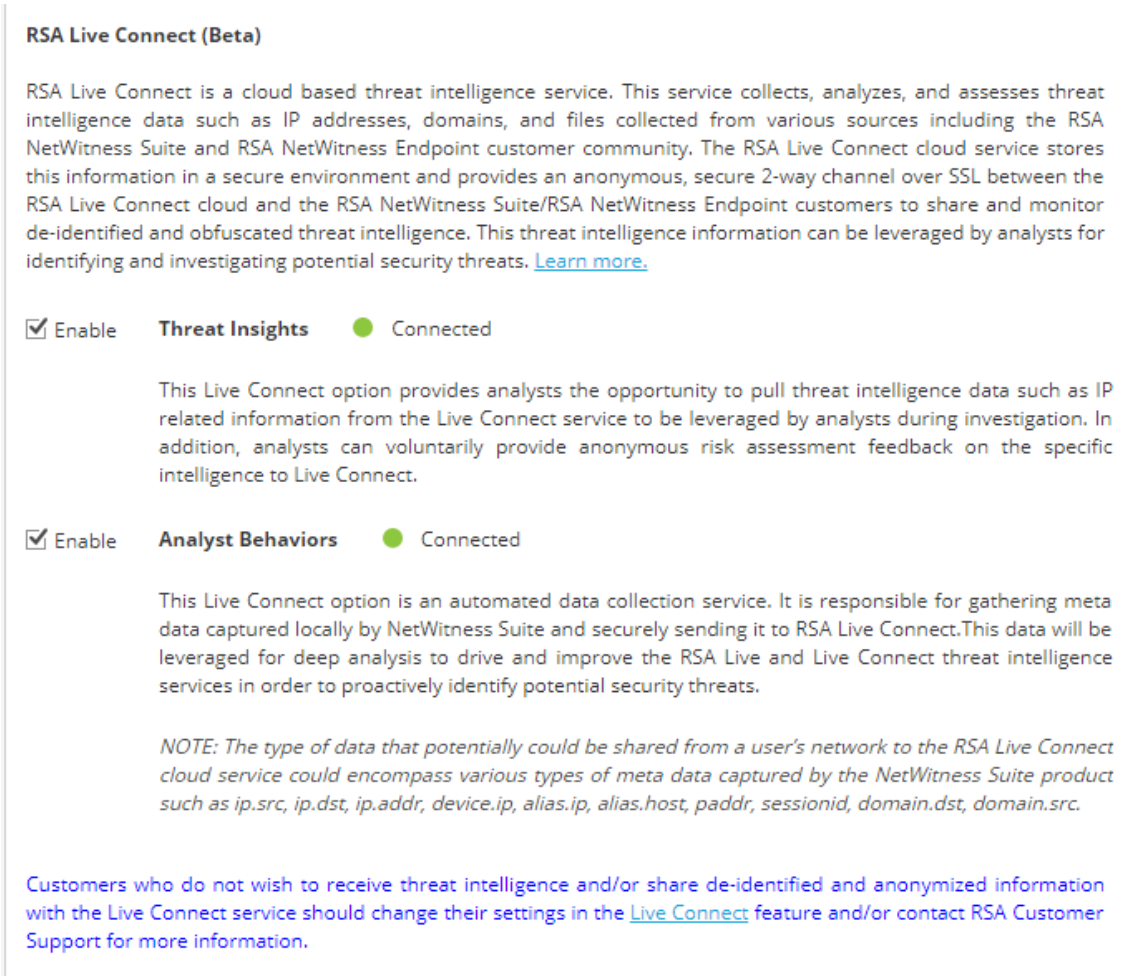
Once you set up and configure a Live account, usage data is shared with RSA. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information.

Before data is sent to RSA, all Personally Identifiable Information is removed. Thus, only anonymous usage data gets transferred to RSA.

For more information, see the **Live Feedback Overview** topic in the *System Configuration Guide*.

RSA Live Connect

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA NetWitness Suite and RSA ECAT customer community.



RSA Live Connect consists of the following features:

- Threat Insights
- Analyst Behaviors

Threat Insights

Threat Insights provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by the analysts during investigation.

By default, **Threat Insights** is enabled in **Additional Live Services** section. If Context Hub service is configured, Live Connect is automatically added as a data source for Context Hub. For more information, see the **Configure Live Connect Data Source for Context Hub** topic in the *Context Hub Configuration Guide*.

With Live Connect as a data source for context hub, you can use the Context Lookup option in Investigation > Navigate view or Investigation > Events view to fetch contextual information. For instructions, see View Additional Context for a Data Point.

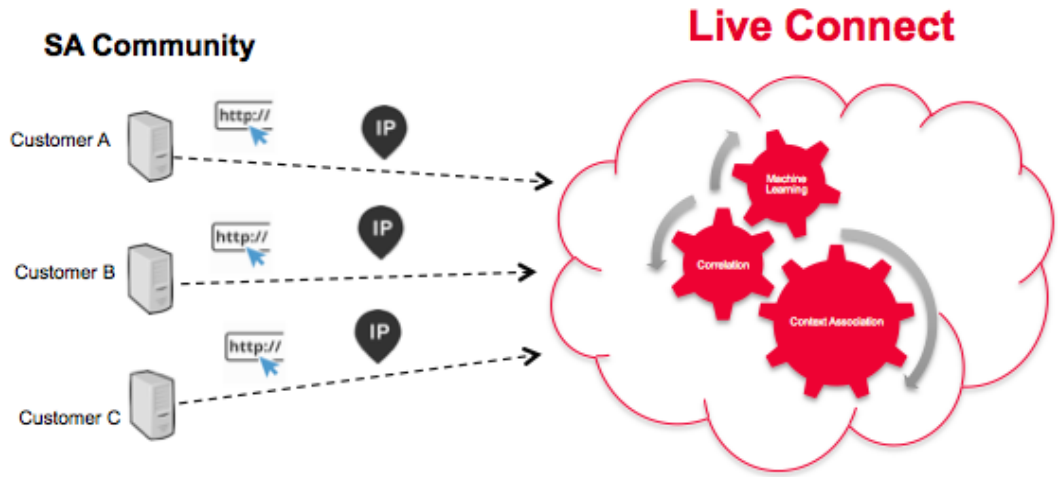
Analyst Behaviors

Analyst Behaviors is a feature where analysts participate in sharing data to RSA community. This is an automated data collection service. Its goal is to share potential threat intelligence data to the RSA Live Connect cloud service for analysis. The type of data that could be shared from your network to RSA Live Connect includes various types of meta data captured by NetWitness Suite such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.

Note: All data collected locally is de-identified and obfuscated and then sent securely and anonymously to the RSA Live Connect cloud service, where it is stored in a secure environment.

Description

Live Connect Threat Data Sharing has been developed as a Community based threat intelligence sharing platform.



It has the following characteristics and goals:

- Crowd-sourced: the RSA community contributes to the entire collection of intelligence
- Centrally collect and analyze data from the RSA community

- Reduce the intelligence cycle time from days to minutes

Some details to consider:

- We are leveraging analyst investigation activity
- We are harvesting meta data such as IP addresses and domain names
- We are doing deep data analysis: Trending, correlation, anomaly detection
- Remember, this feature is currently in Beta

Participation

Customer participation is optional. Upon initial install or upgrade to NetWitness Suite 11.0, you are presented with a confirmation screen. By default, you are entered into the program, but you can opt out at any time.

Cloud Authentication

Authentication for the program is done in the NetWitness Suite UI, where you configure the Live account in the Live services section.

Configuration

To view or change the settings for Live Connect Threat Data Sharing, in the main menu, select **ADMIN > SYSTEM > Live Services**. Check or clear the **Enable** box to participate or stop participating in the program.

Data Collection

Data is collected as follows:

- Data Attribution: Anonymous
- Data Source: Subset of meta keys and meta values of a NetWitness Suite analyst's page views from the NetWitness Suite Core Query logs.
- Query Log Harvesting Process:
  - Timing: Batch mode every 24 hours (4 AM – 6 AM UTC)
  - Log Collection: NetWitness Suite server collects NetWitness Suite core device log entries for the previous 24 hours
  - Log Entries: Only SDK-Value and SDK-Query API calls that contain a where clause are collected
  - Log Attribute Parsing: Each entry must have one of the following meta key indicators present: **ip.src**, **ip.dst**, **ip.addr**, **device.ip**, **alias.ip**, **alias.host**, **paddr**, **sessionid**,

domain.dst, or **domain.src**. If so, meta keys and meta values from the entry will be collected.

Note: Once the above criteria is met, NetWitness Suite sends all of the meta keys and values from the query to the cloud—not just the meta key indicators.

The log report is sent in JSON format, over SSL. It contains:

- Timestamps
- Live CMS username (sha256)
- NetWitness Suitelicense server ID (sha256)
- List of SA endpoint IDs (sha256)
- Harvested meta values (MD5 and SHA256 hashed)

Example

This section lists entries from a log, and then the corresponding section of extrapolated data.

Section from a log file:

```
User admin (session 204298, 10.4.50.60:57454) has issued values (channel 205237)
(thread 2332): fieldName=filter id1=1 id2=23138902 threshold=100000 size=20
flags=sessions,sort-total,order-descending,ignore-cache where="(alias.host =
'mail.google.com') && (ip.src = 161.253.31.130) && time=\"2015-12-07 18:08:00\"-
\"2015-12-07 21:07:59\""
```

Data extrapolation with hashing:

```
{
    timestamp: 1452282588000,
    session: 204298,
    id1: 1,
    id2: 23138902,
    userName: "8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918",
    loggerName: "SDK-Values",
    timeRange: "\"2015-12-07 18:08:00\"-\"2015-12-07 21:07:59\"",
  - metaList: [
      - {
            metaKey: "alias.host",
          - properties: {
                domain_hint: "mai*********.com",
                domain_tld: "com",
                md5_value: "be5cab0695415d9363d18ad1345c73eb",
                sha256_value: "3f2728499a4b29460f3e3150df508e06b19edf0f58efd051fac777844d28e452"
            }
        },
      - {
            metaKey: "ip.src",
          - properties: {
                md5_value: "03b81ffdff109a05a3dac88dbec10c59",
                sha256_value: "1d88c6893797c896070bd5470d0026e11b515d5dee97c6173771a43719fa7e78"
            }
        }
    ]
},
```


Troubleshooting

This section discusses a bit about troubleshooting Live Connect Threat Data Sharing.

Query Log Retrieval Sample

To retrieve a sample of threat intelligence data sent to Live Connect, you construct a URL by setting the following parameters:

- **sendReport**: value is **true** or **false**: true to send this report to the Live Connect server. False to just create the report for viewing. The value defaults to false.
- **hashValues**: value is **true** or **false**: true to hash the values as md5/sha256. False to show values in clear text – should use only for manual viewing. Defaults to false.
- **startDate / endDate**: Dates for time boundaries for log entries. Format: YYYY-MM-DD HH:mm:ss

The following is an example of the URL to use to retrieve query logs:

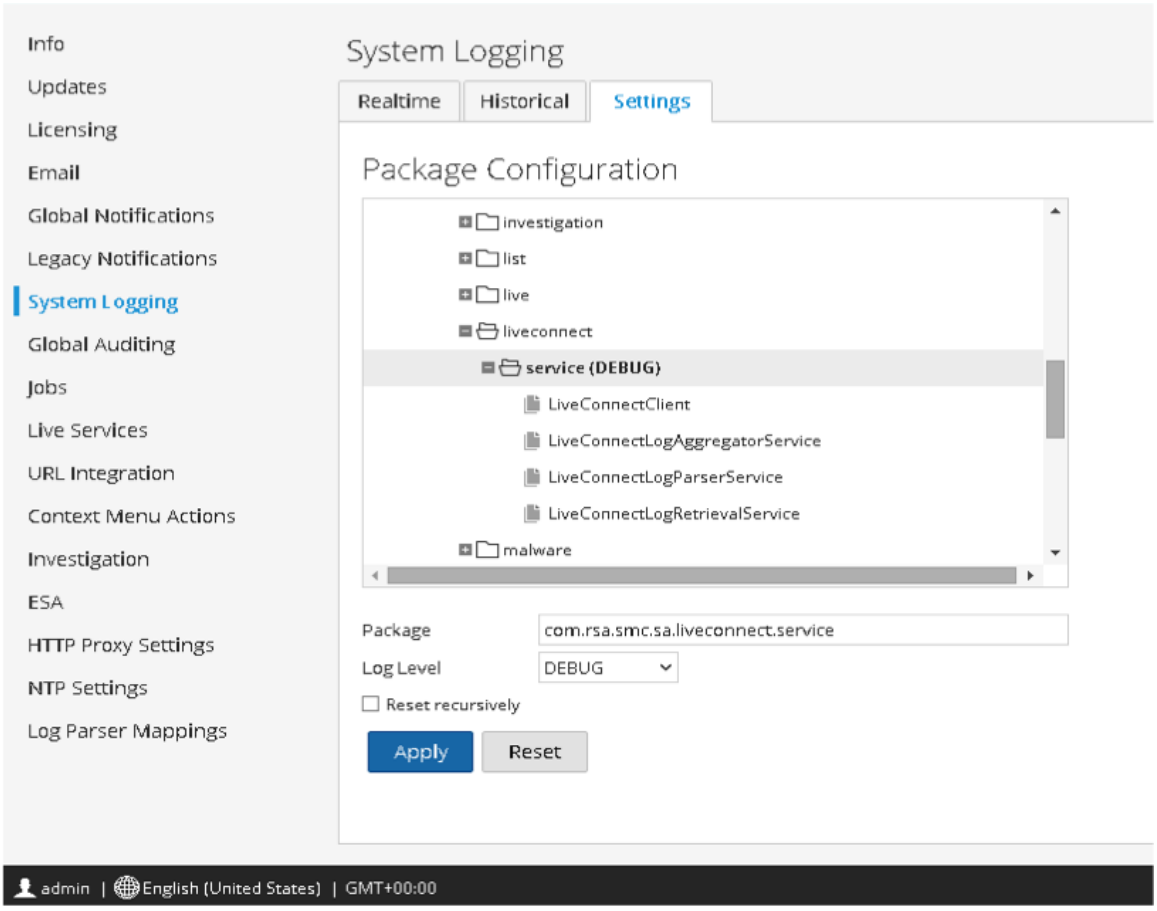
`https://<server>/admin/liveconnect/force_aggregation?startDate=2016-01-18%2000:00:00&endDate=2016-01-19%2010:10:00&sendReport=false&hashValues=true`

System Logging: Debug

You can access some debug information as follows.

1. Select **ADMIN > SYSTEM > System Logging**.
2. Select the **Settings** tab.

3. In the Package Configuration section, select **com > netwitness > platform > server > liveconnect > service (DEBUG)**.



RSA NETWITNESS® SUITE

NetWitness Suite API Documentation

for Version 11.1.0.0

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person. No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

February 2018

Table of Contents

Overview . . . 2
- Current Version . . . 2
- Schema . . . 2
- HTTP Usage . . . 2
- Case Sensitive . . . 3
- Error Response . . . 3
- Pagination . . . 4

Authentication and Authorization . . . 5
- Obtaining a Token . . . 5
  - Using a Username and Password . . . 5
  - Using a Refresh Token . . . 6
- Authorization . . . 8

Incidents . . . 9
- Attributes . . . 9
  - Incident Priority . . . 10
  - Incident Status . . . 11
  - Milestone . . . 11
- Requests . . . 11
  - Get a Single Incident . . . 11
  - Get Incidents by Date Range . . . 13
  - Update an Incident . . . 15
  - Remove an Incident . . . 17
  - Add a Journal Entry . . . 18
  - Get an Incident's Alerts . . . 19

Overview

The NetWitness Suite API can be accessed using the same host and port as the NetWitness user interface.

Current Version

By default, all requests to the REST API will automatically use the latest version of the API available. To provide API stability, clients can specify the API version to use by adding the `NetWitness-Version` HTTP header:

```
NetWitness-Version: 1.0
```

Schema

All data is sent and received as JSON. Any resources containing fields without values will have those fields included with `null` as the value instead of being omitted.

Any fields containing timestamps or dates will be in ISO 8601 format:

```
YYYY-MM-DDTHH:MM:SS.SSSZ
```

HTTP Usage

The RSA NetWitness API tries to adhere as closely as possible to standard HTTP and REST conventions in its use of HTTP verbs and status codes.

HTTP Verbs

Verb	Usage
`GET`	Used to retrieve a resource.
`POST`	Used to create a new resource.
`PATCH`	Used to update an existing resource, including partial updates. Only fields that are modified should be included in the request.
`PUT`	Used to replace an existing resource.
`DELETE`	Used to delete an existing resource.

HTTP Status Codes

Status code	Usage
`200 OK`	The request completed successfully.

`201 Created`	A new resource has been created successfully. The resource's URI is available from the response's `Location` header.
`204 No Content`	An update to an existing resource has been applied successfully.
`400 Bad Request`	The request was malformed. The response body will include an error providing further information. See Error Response.
`401 Unauthorized`	Similar to `403 Forbidden`, but specifically for use when authentication is required and has failed or has not yet been provided. See Authentication and Authorization.
`403 Forbidden`	The request was valid, but the server is refusing the action. The user might not have the necessary permissions for a resource.
`404 Not Found`	The requested resource does not exist.
`500 Internal Server Error`	An unexpected error has occurred. The response body will include a message providing further information.

Case Sensitive

All URLs, request parameters and JSON fields are case sensitive.

Error Response

A common JSON structure is always returned for errors:

Path	Type	Description
`status`	`Number`	The HTTP status code returned.
`timestamp`	`String`	The timestamp of the request.
`errors[]`	`Array`	An array of errors for the given request.
`errors[].message`	`String`	A user-friendly error message explaining what went wrong.
`errors[].field`	`String`	The field or parameter containing the error.

```
{
  "status" : 400,
  "timestamp" : "2018-02-23T18:40:52.660Z",
  "errors" : [ {
    "message" : "Value must be less than or equal to \"10\"",
    "field" : "start"
  }, {
    "message" : "Invalid range"
  } ]
}
```

Pagination

A common JSON structure is always used for paginated results:

Path	Type	Description
`items`	`Array`	An array containing the requested resources.
`pageNumber`	`Number`	The requested page number.
`pageSize`	`Number`	The requested number of items to return in a single page.
`totalPages`	`Number`	The total number of pages available.
`totalItems`	`Number`	The total number of items available.
`hasNext`	`Boolean`	Indicates if there is a page containing results after this page.
`hasPrevious`	`Boolean`	Indicates if there is a page containing results before this page.

```
{
  "items" : [ ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 3,
  "totalItems" : 25,
  "hasNext" : true,
  "hasPrevious" : false
}
```

Authentication and Authorization

All requests must include the `NetWitness-Token` HTTP header containing a valid JSON Web Token (JWT):

```
NetWitness-Token:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MTEyNDczODYyNjMsImlzcyI6InNlY3VyaXR5L
XNlcnZlci0zODA1NTA0OS0xZWMyLTQ0MDAtOTUwYS0zZTVkMmJiYTljMjIiLCJpYXQiOjE1MTEyMTEzODYyNjM
sImF1dGhvcml0aWVzIjpbIkFkbWluaXN0cmF0b3JzIl0sInVzZXJfbmFtZSI6ImFkbWluIn0.StBjg9ruIX4Fr
yfCX8qvrSBGZHF8DN3qHZM0Ei9-
thFndm1q_DLP_cnh8Fpm43fdKcs1ErcVRTqhaYvVULYmsF9ShUaSThpLts6zbJVEKlq3ldUGWWCY9bfVGRH3n5
KmWzITPi7xZ-
Rf_Kp2Sj8ecVAip3qDwha7TxYrReXefCnUj0UxgaaXjeZIFjwxFmK6NPZ7TAK9OcvcVhozaR8V92g1kUVP8_54
x7iZ2jL4JvDPaScWBjBTvVEffHNbX9_iLNoRmKqvDELSla6E_trkSREogCt6pZh709Qh70uoC3BsKwNQKbHNEO
U1tRPFaUFfRH7bCdp8v3Aeh3PTaKEuQA
```

The JSON Web Token is defined in RFC-7519. Tokens can be obtained using the methods outlined below.

In the remainder of this document, the token will be truncated to just `eyJ...AT` for brevity.

Obtaining a Token

A JSON Web Token can be obtained using the methods below.

Using a Username and Password

Users can retrieve an access token using their username and password credentials. Since the API gateway is secured using TLS, all credentials will be encrypted in transit.

```
POST /rest/api/auth/userpass
```

Request Parameters

Parameter	Description
`username`	The username of the account to authenticate.
`password`	The password of the account.

Response Fields

Path	Type	Description
`id`	`String`	The account identifier.
`roles`	`Array`	The roles assigned to the user.

Path	Type	Description
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/userpass' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d 'username=ian&password=changeMe'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:39:38 GMT
Content-Length: 106
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Using a Refresh Token

Users can also retrieve an access token using a refresh token.

```
POST /rest/api/auth/token
```

Request Parameters

Parameter	Description
token	A refresh token.

Response Fields

Path	Type	Description
id	String	The account identifier.
roles	Array	The roles assigned to the user.
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/token' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d
'token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MjIwMDMxNzk3MTQsImlzcyI6InNlY3
VyaXR5LXNlcnZlci00Yzk3MDlmYS0yODYwLTQ3MTQtODQwMC0xNTZmMTA5YmI1YjciLCJpYXQiOjE1MTk0MTEx
Nzk3MTQsInJlZnJlc2giOnRydWUsInVzZXJfbmFtZSI6ImlhbiJ9.k8K8IXjnF0NGHl8tnlK5EHXKQWGljrThL
pZQGYgo0t_wFpMsfawQcZ_jo5DdFnuo6HsFb62KNXVN-
5IW1D4xwms7O4oSwLQ3tHHgLpR8qAklPuRHUC46wKcoMFv-
LVPJ7asLs3wgheWnDsSaPpD04nZmkqloDSfvSPG9LWKpLp5Xo0ibtN9owYhpxguiRdxf6GIXK50TBQRE83xdXU
0s1TcYpa8gKqxQjy1koH-bKxxACcoQ7wR76uD0Lx-
fn2y0X53k9C87JjmctYQsSv45exv8C6vuAFPyuwIuqqkNPAmHJ2dqO4Y930ipiV3IR4MKgBQW-
W4If27aZyQzEFs3hw'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:39:39 GMT
Content-Length: 106
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Authorization

In order to make requests through the NetWitness Suite API, users must belong to roles that have the `integration-server.api.access` permission, as well as any underlying permissions required to fulfill the request.

Incidents

An Incident is a logically grouped set of alerts created automatically by the Incident Aggregation Engine and grouped by a specific criteria. An Incident, available in the Respond Interface, allows an Analyst to triage, investigate, and remediate these groups of alerts. Incidents can be moved between users, notated, and explored via the nodal graph. Incidents allow users to ensure they understand the full scope of an attack or event in their NW system and then take action.

Attributes

The incident resource is comprised of the following attributes:

Path	Type	Description
`id`	`String`	The unique identifier of the incident.
`title`	`String`	The title of the incident.
`summary`	`String`	The summary of the incident.
`priority`	`String`	The incident priority. See the valid values.
`riskScore`	`Number`	The incident risk score is calculated based on the associated alert's risk score. Risk score ranges from 0 (no risk) to 100 (highest risk).
`status`	`String`	The current status. See the valid values.
`alertCount`	`Number`	The number of alerts associated with an incident.
`averageAlertRiskScore`	`Number`	The average risk score of the alerts associated with the incident. Risk score ranges from 0 (no risk) to 100 (highest risk).
`sealed`	`Boolean`	Indicates if additional alerts can be associated with an incident. A `sealed` incident cannot be associated with additional alerts.
`totalRemediationTaskCount`	`Number`	The number of total remediation tasks for an incident.
`openRemediationTaskCount`	`Number`	The number of open remediation tasks for an incident.
`created`	`String`	The timestamp of when the incident is created.
`lastUpdated`	`String`	The timestamp of when the incident was last updated.
`lastUpdatedBy`	`String`	The NetWitness user identifier of the user who last updated the incident.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.
`sources`	`Array`	Unique set of sources for all of the alerts in an incident.

Path	Type	Description
`ruleId`	`String`	The unique identifier of the rule that created the incident.
`firstAlertTime`	`String`	The timestamp of the earliest occurring Alert in this incident.
`categories`	`Array`	The list of categories this incident is categorized under.
`categories[].id`	`String`	The unique category identifier.
`categories[].parent`	`String`	The parent name of the category.
`categories[].name`	`String`	The friendly name of the category.
`journalEntries`	`Array`	Set of notes about the incident investigation, also known as the JournalEntry.
`journalEntries[].id`	`String`	The unique journal entry identifier.
`journalEntries[].author`	`String`	The author of this entry.
`journalEntries[].notes`	`String`	Notes and observations about the incident.
`journalEntries[].created`	`String`	The timestamp of the journal entry created date.
`journalEntries[].lastUpdated`	`String`	The timestamp of the journal entry last updated date.
`journalEntries[].milestone`	`String`	Incident milestone classifier. See the valid values.
`createdBy`	`String`	The NetWitness user id or name of the rule that created the incident.
`deletedAlertCount`	`Number`	The number of alerts that are deleted from the incident.
`eventCount`	`Number`	The number of events associated with incident.
`alertMeta`	`String`	An object containing unique set of meta values, by type, across all alerts associated with this incident.
`alertMeta.SourceIp`	`Array`	Unique source IP addresses.
`alertMeta.DestinationIp`	`Array`	Unique destination IP addresses.

Incident Priority

The `priority` field can contain these values:

Value	Description
`Low`	Low Priority
`Medium`	Medium Priority
`High`	High Priority
`Critical`	Critical

Incident Status

The `status` field can contain these values:

Value	Description
`New`	New incident.
`Assigned`	Incident is assigned to a user.
`InProgress`	Incident response is in progress.
`RemediationRequested`	Remediation tasks have been requested.
`RemediationComplete`	Remediation tasks are complete.
`Closed`	Incident is closed.
`ClosedFalsePositive`	Incident is closed as it was created due to false positive.

Milestone

Each journal entry can contain a `milestone` consisting of these values:

Value	Description
`Reconnaissance`	Intruder is in the initial phase of the attack where targets and vulnerabilities are identified.
`Delivery`	Intruder transmitted malware to the target.
`Exploitation`	Malware code triggers, which takes action on target network to exploit vulnerability.
`Installation`	Malware weapon installs access point usable by intruder.
`CommandAndControl`	Malware enables intruder to have persistent access to target network.
`ActionOnObjective`	Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.
`Containment`	Incident is contained.
`Eradication`	Necessary actions taken to eliminate components of incident and restore the system status.
`Closure`	Incident is addressed.

Requests

Get a Single Incident

A single incident can be retrieved using an incident's unique identifier.

```
GET /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
`id`	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:20 GMT
Content-Length: 1329
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2018-02-23T18:42:21.147Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "ian",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Get Incidents by Date Range

Incidents can be retrieved by the date and time they were created.

```
GET /rest/api/incidents
```

The requested date range can be unbounded, by only supplying either the `since` or `until` parameter, or bounded, by providing both parameters.

Request Parameters

Parameter	Description
`pageNumber`	The requested page number.
`pageSize`	The maximum number of items to return in a single page.
`since`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and after this timestamp.
`until`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and before this timestamp.

All results will be returned using the paginated response payload sorted by the `created` date, in descending order.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents?since=2018-01-
01T04%3A00%3A00.000Z&until=2018-01-01T05%3A00%3A00.000Z&pageSize=100&pageNumber=0' -i
\
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:18 GMT
Content-Length: 1560
```

```
{
  "items" : [ {
    "id" : "INC-100",
    "title" : "Suspected C&C with suspicious-domain.com",
    "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
    "priority" : "Critical",
    "riskScore" : 100,
    "status" : "Assigned",
    "alertCount" : 1,
    "averageAlertRiskScore" : 100,
```

```
    "sealed" : true,
    "totalRemediationTaskCount" : 4,
    "openRemediationTaskCount" : 5,
    "created" : "2018-01-01T04:49:27.870Z",
    "lastUpdated" : "2017-08-04T16:49:27.870Z",
    "lastUpdatedBy" : "norm",
    "assignee" : "tony",
    "sources" : [ "Malware Analysis" ],
    "ruleId" : "55e49a79e4b01a1d2be502bc",
    "firstAlertTime" : "2017-08-04T16:49:22Z",
    "categories" : [ {
      "id" : "55e49a79e4b01a1d2be5022e",
      "parent" : "Malware",
      "name" : "Password dumper"
    }, {
      "id" : "55e49a79e4b01a1d2be50228",
      "parent" : "Hacking",
      "name" : "Path traversal"
    } ],
    "journalEntries" : [ {
      "id" : "20",
      "author" : "admin",
      "notes" : "Updated status",
      "created" : "2017-11-15T20:20:54.785Z",
      "lastUpdated" : "2017-11-15T20:20:54.785Z",
      "milestone" : "Containment"
    } ],
    "createdBy" : "norm",
    "deletedAlertCount" : 100,
    "eventCount" : 0,
    "alertMeta" : {
      "SourceIp" : [ "10.11.12.345" ],
      "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
    }
  } ],
  "pageNumber" : 0,
  "pageSize" : 100,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```


Update an Incident

Currently an incident's `status` and `assignee` can be modified using the incidents endpoint.

```
PATCH /rest/api/incidents/{id}
```

The `assignee` field must include the unique identifier for a valid NetWitness user. The list of users can be found in the security section of the administration user interface.

Request Fields

Path	Type	Description
`status`	`String`	The current status. See the valid values.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X PATCH \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"status":"InProgress"}'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:20 GMT
Content-Length: 1330
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2018-02-23T18:42:20.724Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "tony",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Remove an Incident

A single incident can be removed using the incident's unique identifier.

```
DELETE /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X DELETE \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 23 Feb 2018 18:42:22 GMT
```

```
```

Add a Journal Entry

A journal entry, or note, can be added to an existing incident.

```
POST /rest/api/incidents/{id}/journal
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Fields

Path	Type	Description
author	String	The NetWitness user id of the user creating the journal entry.
notes	String	Notes and observations about the incident.
milestone	String	The incident milestone classifier.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100/journal' -i -X POST \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"author":"duke","notes":"This incident is
contained.","milestone":"Containment"}'
```

Sample Response

```
HTTP/1.1 201 Created
Location: https://api.netwitness.local/rest/api/incidents/INC-100
Date: Fri, 23 Feb 2018 18:42:22 GMT
```

```
```

Get an Incident's Alerts

All the alerts that are associated with an incident can be retrieved using the incident's unique identifier.

```
GET /rest/api/incidents/{id}/alerts
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Parameters

Parameter	Description
pageNumber	The requested page number.
pageSize	The maximum number of items to return in a single page.

Response Fields

Path	Type	Description
items	Array	An array containing the requested resources.
pageNumber	Number	The requested page number.
pageSize	Number	The requested number of items to return in a single page.
totalPages	Number	The total number of pages available.
totalItems	Number	The total number of items available.

Path	Type	Description
hasNext	Boolean	Indicates if there is a page containing results after this page.
hasPrevious	Boolean	Indicates if there is a page containing results before this page.
items[].id	String	The unique alert identifier.
items[].title	String	The title or name of the rule that created the alert.
items[].detail	String	The details of the alert. This can be the module name or meta that the module included.
items[].created	String	The timestamp of the alert created date.
items[].source	String	The source of this alert. For example, "Event Stream Analysis", "Malware Analysis", etc.
items[].riskScore	Number	The risk score of this alert, usually in the range 0 - 100.
items[].type	String	The type of alert, "Network", "Log", etc.
items[].events	Array	The events that make up this alert.
items[].events[].source	Object	The source of the event.
items[].events[].source.device	Object	The device contains the endpoint network information.
items[].events[].source.device.ipAddress	String	The IP address.
items[].events[].source.device.port	Number	The port.
items[].events[].source.device.macAddress	String	The ethernet MAC address.
items[].events[].source.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].source.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].source.user	Object	The user contains the endpoint user information.
items[].events[].source.user.username	String	The unique username.
items[].events[].source.user.emailAddress	String	An email address.
items[].events[].source.user.adUsername	String	An Active Directory (AD) username.
items[].events[].source.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].destination	Object	The destination of the event.
items[].events[].destination.device	Object	The device contains the endpoint network information.
items[].events[].destination.device.ipAddress	String	The IP address.

Path	Type	Description
items[].events[].destination.device.port	Number	The port.
items[].events[].destination.device.macAddress	String	The ethernet MAC address.
items[].events[].destination.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].destination.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].destination.user	Object	The user contains the endpoint user information.
items[].events[].destination.user.username	String	The unique username.
items[].events[].destination.user.emailAddress	String	An email address.
items[].events[].destination.user.adUsername	String	An Active Directory (AD) username.
items[].events[].destination.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].domain	String	The top-level domain or Windows domain.
items[].events[].eventSource	String	The source of the event. This may be a fully-qualified hostname with a port, or simple name.
items[].events[].eventSourceId	String	The unique identifier of the event on the source. For Network and Log events, this is the Nextgen Session ID.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-
100/alerts?pageSize=10&pageNumber=0' -i \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:22 GMT
Content-Length: 1301
```


```
{
  "items" : [ {
    "id" : "5a6b81639491573f1e73676c",
    "title" : "LogOn Rule",
    "detail" : "Module_5a5cddb3e4b0ac40016df562_Alert",
```

```
    "created" : "2018-01-26T19:28:35Z",
    "source" : "Event Stream Analysis",
    "riskScore" : 90,
    "type" : "Network",
    "events" : [ {
      "source" : {
        "device" : {
          "ipAddress" : "58.229.117.56",
          "port" : 57429,
          "macAddress" : "00:13:c3:3b:c7:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "destination" : {
        "device" : {
          "ipAddress" : "128.164.35.184",
          "port" : 21,
          "macAddress" : "00:17:df:6b:c8:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "domain" : null,
      "eventSource" : "10.4.61.48:56005",
      "eventSourceId" : "9318"
    } ]
  } ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```

RSA NETWITNESS® SUITE

NwConsole User Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Access NwConsole and Help **5**

Prerequisites 5

Access NwConsole 5

View Help 6

View a List of Commands 6

View Detailed Help on a Command 7

View a List of Help Topics 8

View a Specific Help Topic 8

Quit NwConsole 9

Basic Command Line Parameters and Editing **10**

Basic Command Line Parameters 10

Line Editing 10

Connecting to a Service **12**

Monitoring Stats **16**

Useful Commands **17**

Feeds 17

create 17

stats 18

dump 18

Converting Packet DB Files to PCAP 18

Packets 19

Verifying Database Hashes 20

SDK Content Command **21**

SDK Content Command Examples **23**

Commands Used for Troubleshooting **28**

whatIsWrong 28

dbcheck 29

topQuery 29

netbytes 30
netspeed 30

Access NwConsole and Help

RSA NetWitness Console, also known as NwConsole, is a multi-platform terminal application that provides powerful tools and command line access to Core services, such as Decoder, Log Decoder, Concentrator, Broker, and Archiver. While most users complete their tasks and investigations through the NetWitness Suite user interface, some advanced users, such as administrators and developers, require direct access to the services without going through the user interface. NwConsole enables you to enter commands from the command line or run multiple commands from a file.

This topic describes how to access NwConsole and to view the internal help within NwConsole.

Extensive help information is available within RSA Security Analytics console, also known as NwConsole. You can access this help from the Security Analytics command line.

Prerequisites

All NetWitness Suite appliances have theNwConsole application installed. You can also install it on Windows, Mac, and CentOS to connect and interact with a Core service.

NwConsole is available from the command line on a NetWitness Suite appliance. If you are accessing a Core appliance remotely, you need to have the RSA NetWitness Console application installed on a Windows, Mac, or CentOS machine. To obtain the RSA NetWitness Console application installer, contact RSA Customer Care.

Access NwConsole

To run NwConsole from the command line on a NetWitness Suite appliance or on a terminal emulator, at the <$> prompt, type `NwConsole` (Linux) or `nwconsole` (Windows). The actual command is `NwConsole`, but Windows is not case sensitive. RSA NetWitness Console is displayed as shown in the following example.

```
Last login: Thu Sep 24 14:00:42 on console
usxx<username>m1:~ <username>$ NwConsole
RSA NetWitness Suite Console 10.6.0.0.6105
Copyright 2001-2015, RSA Security Inc.  All Rights Reserved.

Type "help" for a list of commands or "man" for a list of manual pages.
>
```

View Help

NwConsole provides help on individual commands as well as help on specific topics.

Caution: To get the latest information, view the command and help topics within NwConsole.

View a List of Commands

To view a list of available commands and their descriptions, at the (>) prompt, type `help`. The following example shows a list of available commands.

```
> help
Local commands:
    avro2nwd      - Convert AVRO files to NWD files
    avrodump      - Display schema and contents of AVRO file (for debugging)
    blockspeed    - Tests various write block sizes to determine best setting
    compileflex   - Compile all flex parsers in a directory
    createflex    - Create a flex parser that matches tokens read from a file
    dbcheck       - Perform a database integrity check over one or more
                    session, meta, packet, log or stat db files
    diskspeed     - Measures the speed of the disk(s) mounted at a specified
                    directory
    echo          - Echos the passed in text to the terminal
    encryptparser - Encrypt all parsers in a directory
    feed          - Create and work with feed files
    fmanip        - Manipulate a file with XOR and check for embedded PEs
    hash          - Creates or verifies hashes of database files
    help          - Provides help information for recognized console commands
    history       - Displays, erases or executes a command in the command
                    history
    httpAggStats  - Tests HTTP aggregation and reports statistics as it
                    continues
    log           - Perform operations on a log database
    logParse      - Parse line delimited logs on stdin and post results to
                    stdout
    logfake       - Create a fake log pcap file
    lua           - Execute a lua script
    makec3        - Generate C3 Test Data
    makepcap      - Convert packet database files to pcap or log files
    man           - Displays a list of topics or opens a specific manual page
```

```
                  on a topic
    metaspeed     - Tests read performance over an existing meta db
    netbytes      - Display statistics on network interface utilization
    nwdstrip      - Convert full NWD file into just session and meta file
    pause         - Wait for user input when running a script file
    reindex       - reindex a collection
    sdk           - Execute SDK commands based on the C SDK library, type "sdk
                    help" for more information
    sleep         - Sleeps for the specified milliseconds
    timeout       - Globally change the timeout for waiting for a response from
                    a service
    tlogin        - Open a trusted SSL connection to an existing service
    topQuery      - Returns the top N longest running queries from the audit
                    log (either a file or from the log API)
    vslice        - Validate index slices

Remote commands (executed on the connected service, see "login"):
    login         - Connect to a remote service.  Once connected, type help to
                    see commands available for remote execution.

For detailed help, type "help <command>"
>
```

View Detailed Help on a Command

To view detailed information about a command, type `help <command>`. The following example shows help for the `logParse` command after typing `help logParse`.

```
For detailed help, type "help <command>"
> help logParse
Usage: logParse {in=<pathname>} {indir=<pathname>} [out=<pathname>]
                [content=<c2|c3>] [device=<device,[device...]>]
                [path=<log-parsers-config-path>] [metaonly] [srcaddr=<src
                address>] [srcaddrfile=<filename,IP Address>]
Parse line delimited logs on stdin and post results to stdout

    in          - The input source file. "in=stdin" means interactive typing of
                  log.
    indir       - The input source files parent directory
    out         - The output file or output file parent directory if input is
                  set by indir. If not specified, use stdout as output.
```

```
    content     - Content version, either c2 or c3. Default is c2.
    device      - Comma delimited device list specifying devices that is
                  enabled. Default enable all devices.
    path        - The logparsers configuration path. Default will find
                  configuration file like logdecoder.
    metaonly    - The output will only contains parsed meta, otherwise will
                  print log message after metas.
    srcaddr     - The source address of the all the logs
    srcaddrfile - The source address for logs in one input file, in the format
                  filename,ipaddress
>
```

View a List of Help Topics

To view a list of help topics, type `man`. The following example shows a list of help topics.

```
> man
List of topics:

    Introduction
    Connecting to a Service
    Monitoring Stats
    Feeds
    Converting Packet DB Files to PCAP
    Packets
    Verifying Database Hashes
    SDK Content
    SDK Content Examples
    Troubleshooting

Type "man <topic>" for help on a specific topic, partial matches are acceptable
>
```

View a Specific Help Topic

To view help about a specific topic, type `man <topic>`. The following example shows the Packets help topic after typing `man Packets`.

```
Type "man <topic>" for help on a specific topic, partial matches are acceptable
> man Packets
                                    Packets
```

```
=======

The *packets* command can be used to generate a pcap or log file based on a
list of Session IDs, a time period or a where clause.  The command is quite
flexible and can be used on any running service that has access to the raw
data from a downstream component.  Before running the command, you must first
*login* to a service and then change directory to the appropriate sdk node,
(e.g., "cd /sdk").  Unlike the *makepcap* command, which only works on the
local file system, this command is meant to be used on a remote service.

    login ...
    cd /sdk
    packets where="service=80 && time='2015-03-01 15:00:00'-'2015-03-01
    15:10:00'" pathname="/tmp/march-1.pcap"
Write 10 minutes of HTTP only packets from March 1st, to the file
/tmp/march-1.pcap.  All times are in UTC.

    packets time1="2015-04-01 12:30:00" time2="2015-04-01 12:35:00"
    pathname=/media/sdd1/packets.pcap.gz
Write all packets between the two times to a gzip compressed file at
/media/sdd1/packets.pcap.gz

    packets time1="2015-04-01 12:30:00" time2="2015-04-01 12:35:00"
    pathname=/media/sdd1/mylogs.log
Write all logs between the two times to a plaintext file at
/media/sdd1/mylogs.log.  Any pathname ending with .log indicates that the
format of the output file should be plaintext line-delimited logs.
>
```

Caution: To get the latest information, view the command and help topics within NwConsole.

Quit NwConsole

To exit the NwConsole application, type `quit` at the command line.

Basic Command Line Parameters and Editing

markdown file is ManIntroduction.htm. Format doesn't work, but content is newer. I need to add new stuff to formatted, then export to HTML to add into Nwconsole.

NwConsole is like a Swiss army knife; there are all kinds of tools buried underneath its command line interface. NwConsole is multi-platform; executables are available for CentOS (it already ships on appliances), Windows, and Mac.

Basic Command Line Parameters

Here are some basic command line parameters:

- To run a set of commands from a file:

  ```
  NwConsole -f /tmp/somefile.script
  ```

- To pass in a list of commands from the command line:

  ```
  NwConsole -c <command1> -c <command2> -c <command3>
  ```

  This is not necessarily recommended except for very simple scripts. The bash interpreter can make mincemeat out of quoted strings if you do not escape properly. If you are having non-obvious errors passing via command line, switch over to reading from a file to see if that fixes the issues.

- Normally, console exits after running commands passed via a file or command line, but if you want to keep the interactive prompt open after the commands are executed, pass `-i` on the command line.

- And of course, you can just run NwConsole and type the commands in the console window.

Line Editing

You can use the keys in the following table when editing a command.

Key	Descripton
Ctrl-U	Clears the current line
Ctrl-W	Deletes the word that the cursor is on
Ctrl-A	Moves the cursor to the beginning of the line
Ctrl-E	Moves the cursor to the end of the line

Key	Descripton
Up arrow	Displays the previously executed command
Down arrow	Displays the command executed after the current command (only valid if the up arrow has been pressed)
Left arrow	Moves the cursor to the previous character
Right arrow	Moves the cursor to the next character
Tab	Provides context sensitive completion of most commands and their parameters. The Tab key is very helpful for editing. For example, to view the *Connecting to a Service* help topic, at the command line, you can type `mancon` and then press the `Tab` key. NwConsole completes the command for you: `man Connecting to a Service` Press enter to run the command and view the topic.
`history`	Displays a numbered list of previous commands
`history execute=#`	Executes a previous command, which is also equivalent to typing `!#` For example, `!1` executes the previous command.
`history clear`	Clears all command history
`history erase=#`	Erases a specific command from the history buffer. History is automatically stored from one session to the next.

Connecting to a Service

To connect and then interact with a Security Analytics Core service (Decoder, Concentrator, Broker, Archiver, and so on), you must first issue the `login` command. You must have an account on that service. You can `type help` login at any time for more information. Here is the syntax of the `login` command:

```
login <hostname>:<port>[:ssl] <username> [password]
```

For example: **login 10.10.1.15:56005:ssl someuser**

If you do not include the password, it prompts you and does proper password masking.

If you have set up proper trust between NwConsole and the endpoint, you can use the `tlogin` command and avoid having to enter a password. Setting up trust is beyond the scope of this documentation, but it involves adding NwConsole's SSL cert to the endpoint via the `send /sys peerCert op=add --file-data=<pathname of cert>` command. You must first use a normal login with the proper permissions before you can add a peer cert for subsequent trusted logins.

Once connected, you can interact with the endpoint service through a virtual file system. Instead of files, what you are looking at are the nodes of that service. Some nodes are folders and have child nodes, forming a hierarchical structure. Each node serves a purpose and all of them support a subset of commands like `info` and `help`. The `help` message returns information about the commands each node supports. When you first log on, you are on the root node, which is the path `/`, just like a Linux or Mac system. To see a list of nodes under `/`, type the `ls` command.

All services have nodes like `sys` and `logs`. To interact with the **/logs** API, you can first send the `help` command to the **/logs** node. To do this, you must use the `send` message, which has this syntax:

```
Usage: send {node pathname} {message name} [name=value [name=value]]

            [--file-data=<pathname>] [--string-data=<text>] [--binary-data=<text>]
            [--output-pathname=<pathname>] [--output-append-pathname=<pathname>]
            [--output-format={text,json,xml,html}]
Sends a command to a remote pathname.  For remote help, use "send <pathname>help"
for details.

    pathname                - The node pathname to retrieve information on
    message                 - The command (message) to send
    parameters              - Zero or more name=value parameters for the command
    --file-data             - Loads data from a file and send as either a BINARY
                              message or as a PARAMS_BINARY message if other
```

```
                              parameters exist
   --string-data            - Sends text as a STRING message type
   --binary-data            - Send text as either a BINARY message type or as a
                              PARAMS_BINARY message type if other parameters
                              exist
   --output-pathname        - Writes the response output to the given pathname,
                              overwriting any existing file
   --output-append-pathname - Writes the response output to the given pathname,
                              will append output to an existing file
   --output-format          - Writes the response in one of the given formats,
                              the default is text
```

So, to send a `help` message, you would send this:

```
send /logs help
```

And your response would look something like this:

```
    description: A container node for other node types
    security.roles: everyone,logs.manage
    message.list: The list of supported messages for this node
    ls:  [depth:<uint32>] [options:<string>] [exclude:<string>]
    mon:  [depth:<uint32>] [options:<uint32>]
    pull:  [id1:<uint64>] [id2:<uint64>] [count:<uint32>] [timeFormat:<string>]
    info:
    help:  [msg:<string>] [op:<string>] [format:<string>]
    count:
    stopMon:
    download:  [id1:<uint64>] [id2:<uint64>] [time1:<date-time>] [time2:<date-
time>] op:<string>
  [logTypes:<string>] [match:<string>] [regex:<string>] [timeFormat:<string>]
[batchSize:<uint32>]
    timeRoll:  [timeCalc:<string>] [minutes:<uint32>] [hours:<uint32>]
[days:<uint32>] [date:<string>]
```

To get more information about a specific message or command, you can specify the `msg=<message name>` on the help command as a parameter. For example, look at the `pull` message help:

```
send /logs help msg=pull
```

```
    pull: Downloads N log entries
    security.roles: logs.manage
    parameters:
    id1 - <uint64, optional> The first log id number to retrieve, this is mutually
```

```
exclusive with id2
    id2 - <uint64, optional> The last log id number that will be sent, defaults to
most recent log
 message when id1 or id2 is not sent
    count - <uint32, optional, {range:1 to 10000}> The number of logs to pull
    timeFormat - <string, optional, {enum-one:posix|simple}> The time format used
in each log message,
 default is posix time (seconds since 1970)
```

The built in message help says that this command grabs the last N log entries if you leave off id1 and id2. To look at the last 10 log entries this service:

```
send /logs pull count=10 timeFormat=simple
```

Almost all of the commands on the service follow this simple format. The only commands that do not are the ones that require more complicated handshaking, like importing a PCAP to a Decoder. To import a PCAP, use the NwConsole `import` command, which takes care of the complicated communication channel handshaking.

Some parameters are specific to NwConsole's `send` command and are not actually sent to the service. You can use these parameters to change the output format of the response, write the response to a file, or read a file from the local machine and send it to the service. The local parameters to NwConsole's `send` command all start with two dashes --.

- `--output-format` — This parameter changes the normal output of the command from plain text to one of these types: JSON, XML, or HTML.
- `--output-pathname` — Instead of writing the output to the terminal, it writes it to the pathname specified (truncates any existing file).
- `--output-append-pathname` — This is the same as `--output-pathname` except that it appends the output to an existing file (or creates the file if it does not exist).
- `--file-data` — Reads in a file and uses it as the command payload. This is useful for commands like `/sys fileEdit`. The following example shows how you can send an updated **index-concentrator-custom.xml** file using NwConsole:

```
send /sys fileEdit op=put filename=index-concentrator-custom.xml --file-
data="/Users/user/Documents/index-concentrator-custom.xml"
```

- `--file-format` — When reading an input file with `--file-data`, this parameter forces NwConsole to interpret the file as a specific type of input. The allowed enumerations

are: `binary`, `params`, `param-list`, `string` and `params-binary`. As an example, to send a file of application rules (`*.nwr`) to a Decoder, you can use this command:

```
send /decoder/config/rules/application replace --file-
data=/path/rules.nwr --file-format=param-list
```

- `--string-data` — Sends the command payload as a string instead of a list of parameters.
- `--binary-data` — Sends the command payload as binary instead of a list of parameters.

Example Streaming Query to JSON file (could be a large result set):

```
send /sdk query size=0 query="select * where service=80 && time='2015-
03-05 13:00:00'-'2015-03-05 13:59:59'" --output-format=json --output-
pathname=/tmp/query.json
```

One thing to note about the send command is the fact that, by default, there is a timeout of 30 seconds waiting for a response. Some commands (like the query above) may take longer to receive results. To avoid a premature client-side timeout, you can use the `timeout [secs]` command to increase the wait. For instance, `timeout 600` would wait 10 minutes for a response before timing out. Once enacted, it takes effect for all subsequent commands.

To navigate around the virtual node hierarchy of the service, you can use the `cd` command like you would on any command shell. This covers the basics of connecting and interacting with a service. Once you are connected, the `help` command lists all the commands that you can use to interact with the endpoint. These commands do not display when you are not connected to an endpoint.

Monitoring Stats

You can use NwConsole to watch statistics (stats) change on a service in real time. However, be warned that this can result in a LOT of output. If you are not careful and monitor too many nodes, the screen scrolls by too quickly to be useful.

As a simple example, if you log on to a Decoder, you can monitor the capture rate in real time. To do this, issue these commands after connecting to a Decoder:

```
decoder/stats
```

```
mon capture.rate
```

That is all you need to do! Now, any time the capture rate changes, it outputs into the console window.

You can add another monitor:

```
mon capture.avg.size
```

Now it watches those two stats and outputs those values when they change. You may have noticed that as you tried to type the second command, the output from the original monitor was messing up your display. This is the problem with monitoring stats. It is not really meant for doing more than just watching the stats after the first command is entered.

However, you can stop the monitoring by typing `delmons` and pressing **Enter**. Just ignore the output while you type and it returns you to a proper command prompt. If you want to monitor many stats at once, you can just give the path of the parent stat folder and it monitors all of the stats underneath it. For instance, typing `mon /decoder/stats` or `mon .` (they are equivalent) monitors everything. Be prepared for a lot of output! Remember to enter `delmons` if it is scrolling too fast.

Useful Commands

The following NwConsole commands are useful when interacting with NetWitness Server Core services:

- **feed**: Enables you to create and work with feed files.
- **makepcap**: Converts Packet database (DB) files to PCAP.
- **packets**: Retrieves packets or logs from the logged in service.
- **hash**: Creates or verifies hashes of database files.

The following sections as well as the NwConsole help and topic information (man) pages, provide additional information.

Feeds

The `feed` command provides several utilities for creating and examining feed files. A feed file contains the definition and data of a single feed in a format that has been precompiled for efficient loading by a Decoder or Log Decoder. For a complete reference on feed definitions, see **Feed Definitions File** in the *Decoder and Log Decoder Configuration Guide*.

create

```
feed create <definitionfile> [-x <password>]
```

The `feed create` command generates feed files for each feed defined in a feed definition file. A definition file is an XML document that contains one or more definitions. Each feed definition specifies a data file and the structure of that data file. The resulting feed files will be created in the same directory as the definition file with the same name as the data file, but with the extension changed to **.feed** (for example, **datafile.csv** results in **datafile.feed**). Any existing files with the target name will be overwritten without a prompt.

```
$ ls
example-definition.xml    example-data.csv
$ NwConsole
RSA NetWitness Console 10.5.0.0.0
Copyright 2001-2015, RSA Security Inc.  All Rights Reserved.

Type "help" for a list of commands or "man" for a list of manual pages.
> feed create example-definition.xml
Creating feed Example Feed...
done.  2 entries, 0 invalid records
All feeds complete.
```

```
> quit
$ ls
example-definition.xml    example-data.feed    example-data.csv
$
```

Optionally, feed files can be obfuscated using the option `-x` followed by a password of at least 16 characters (no spaces). This will be applied to all feeds defined in the definition file. In addition to the feed file, a token file will be generated for each feed file. The token file must be deployed with the corresponding feed file.

```
feed create example-definition.xml -x 0123456789abcdef
```

stats

```
feed stats <feedfile>
```

The `feed stats` command provides summary information for an existing, un-obfuscated feed file. Specifying an obfuscated feed file will result in an error.

```
> feed stats example.feed
 Example Feed stats:
 version  : 0
 keys count  : 1
 values count: 2
 record count: 2
 meta key  : ip.src/ip.dst
 language keys:
 alert    Text
```

dump

```
feed dump <feedfile> <outfile>
```

The `feed dump` command generates a normalized, key-value pair listing of an un-obfuscated feed file. You can use the resulting file to validate a feed file or assist in determining which records were considered invalid when the feed was created. Specifying an obfuscated feed file will result in an error. If `outfile` exists, the command will abort without overwriting the existing file.

```
feed dump example.feed example-dump.txt
```

Converting Packet DB Files to PCAP

You can use the `makepcap` command to quickly convert any Packet DB file to a generic PCAP file, preserving the capture time order. This command offers many options (see `help makepcap`), but is easy to use. All it really needs is the Packet DB directory (via the `source=<pathname>` parameter) to get started.

Note: You must stop the Decoder or Archiver service before running this command. If you want to generate a PCAP while the service is running, see the `packets` command.

```
makepcap source=/var/netwitness/decoder/packetdb
```

This command converts every Packet DB file into a corresponding PCAP file in the same directory. If the disk is almost full, see the next command.

```
makepcap source=/var/netwitness/decoder/packetdb
dest=/media/usb/sde1
```

This command writes all of the output PCAPs to the directory at **/media/usb/sde1**.

```
makepcap source=/var/netwitness/decoder/packetdb
dest=/media/usb/sde1 filenum=4-6
```

This command only converts the files numbered 4 thru 6 and skips all other files. In other words, it converts the Packet DB files: **packet-000000004.nwpdb**, **packet-000000005.nwpdb**, and **packet-000000006.nwpdb**.

```
makepcap source=/var/netwitness/decoder/packetdb time1="2015-03-
01 14:00:00" time2="2015-03-02 07:30:00" fileType=pcapng
```

This command only extracts packets with a timestamp between March 1st, 2015 at 2 PM and March 2nd, 2015 before or on 7:30 AM. It writes the file as pcapng in the same directory as the source. All timestamps are UTC.

Packets

You can use the `packets` command to generate a PCAP or log file based on a list of Session IDs, a time period, or a where clause. This command is very flexible you can use it on any running service that has access to the raw data from a downstream component. Before running the command, you must first `login` to a service and then change directory to the appropriate sdk node (for example, `cd /sdk`). Unlike the `makepcap` command, which only works on the local file system, you use this command for a remote service.

```
login ...

cd /sdk

packets where="service=80 && time='2015-03-01 15:00:00'-'2015-03-01 15:10:00'"
pathname="/tmp/march-1.pcap"
```

This command writes 10 minutes of HTTP only packets from March 1st to the file **/tmp/march-1.pcap**. All times are in UTC.

```
packets time1="2015-04-01 12:30:00" time2="2015-04-01 12:35:00"
pathname=/media/sdd1/packets.pcap.gz
```

This command writes all packets between the two times to a GZIP compressed file at **/media/sdd1/packets.pcap.gz**.

```
packets time1="2015-04-01 12:30:00" time2="2015-04-01 12:35:00"
pathname=/media/sdd1/mylogs.log
```

This command writes all logs between the two times to a plaintext file at **/media/sdd1/mylogs.log**. Any pathname ending with **.log** indicates that the format of the output file should be plaintext line-delimited logs.

Verifying Database Hashes

By default, Archiver writes an XML file for every DB file that is written. This XML file ends with the extension **.hash** and contains a hash of the file along with other pertinent information. You can use the `hash` command to verify that the DB file has not been tampered with by reading the hash stored in the XML file and then rehashing the DB file to verify that the hash is valid.

```
hash op=verify
hashfile=/var/netwitness/archiver/database0/alldata/packetdb/pa
cket-000004880.nwpdb.hash
```

This command verifies that the Packet DB file **packet-000004880.nwpdb** still matches the hash in the XML file **packet-000004880.nwpdb.hash**. For proper security, the hash file should be stored somewhere else to prevent the XML file from being tampered with (like write once only media), but the hash command itself does not care where it is stored.

SDK Content Command

One of the powerful commands in NwConsole is `sdk content`. It contains numerous options to do just about anything, at least as far as extracting content from the NetWitness Suite Core stack. You can use it to create PCAP files, log files, or extract files out of network sessions (for example, grab all of the pictures from email sessions). It can append files, have a max size assigned before creating a new file, and automatically clean up files when the directory grows too large. It can run queries in the background to find new sessions. It breaks queries into manageable groups and performs those operations automatically. When the group is exhausted, it does a requery to get a new set of data for further operations. The list of options for the sdk content command is very extensive.

Because the command has so many options, this document provides examples of commands for different use cases.

Before you can run `sdk content`, there are a few commands (like logging into a service) that you need to run first. Here are some examples:

- First connect to a service:
  `sdk open nw://admin:netwitness@10.10.25.50:50005`
- If you need to connect over SSL, use the nws protocol:
  `sdk open nws://admin:netwitness@10.10.25.50:56005`
- Keep in mind that you are passing a URL and must URL encode it properly. If the password is `p@ssword`, the URL looks like this: `sdk open nw://admin:p%40ssword@10.10.25.50:50005`
  This also applies to username.
- Once you log in, you can set an output directory for the commands: `sdk output <some pathname>`
- For command line help, type: `sdk content`

Before you try some example commands, it is important to understand the `sessions` parameter. This parameter is very important and controls how much or how little data you want to grab (the where clause is also important). The sessions parameter is either a single session id or a range of session ids. All NetWitness Suite Core services work with session ids, which start at 1 and increase by 1 for every new session added to the service (network or log session). Session ids are 64-bit integers, so they can get quite large. To keep it simple, assume we have a Log Decoder that has ingested 1000 logs and parsed them. On the service, you now have 1000 sessions with session ids from 1 to 1000 (session id 0 is never valid). If you want to operate over all 1000 sessions, you pass sessions=1-1000. If you only want to operate over the last 100 sessions, you pass sessions=901-1000. Once the command finishes processing session 1000, it exits back to the console prompt.

Many times, however, we do not care about specific session ranges. We just want to run a query over all of them and process the sessions that match a query. Here are some shortcuts that simplify this:

- The letter `l` (lowercase L) means lower bound or the lowest session id.
- The letter `u` means the highest session id. In fact, it actually means the highest session id for future sessions as well. In other words, if you pass `sessions=l-u`, this special range means operate over all the current sessions in the system, but also do not quit processing, and as new sessions enter the system, process those, too. The command pauses and waits for new sessions once it reaches the last session on the service. To summarize, the command never exits and goes into continuous processing mode. It runs for days, months, or years, unless it is killed.
- If you do not want the command to run forever, you can pass `now` for the upper limit. This determines the last session id on the service at the time the command starts and processes all sessions until it reaches that session id. Once it reaches that session id, the command exits, regardless of how many sessions may have been added to the service since the command started. So, for the example Log Decoder, `sessions=200-now` starts processing at session 200 and goes all the way to session 1000 and quits. Even if another 1000 logs were added to the Log Decoder after the command started, it still exits after processing session 1000.
- The parameter `sessions=now-u` means start at the very last session and continue processing all new sessions that come in. It does not process any existing sessions (except the last one), only new sessions.

For example commands and what they do, type `man sdk content examples` or see SDK Content Command Examples.

SDK Content Command Examples

The first NwConsole sdk content command example below is simple and shows all of the commands that you need to enter. After that, the examples show only the `sdk content` commands. The first example creates a log file and grabs the first 1000 logs out of a Concentrator aggregating from a Log Decoder:

```
sdk open nw://admin:netwitness@myconcentrator.local:50005

sdk output /tmp

sdk content sessions=1-1000 render=logs append=mylogs.log
fileExt=.log
```

This script outputs 1000 logs (assuming sessions 1 thru 1000 exist on the service) to the file **/tmp/mylogs.log**. The logs are in a plain text format. The parameter `fileExt=.log` is necessary to indicate to the command that we want to output a log file.

```
sdk content sessions=1-1000 render=logs append=mylogs.log
fileExt=.log includeHeaders=true separator=","
```

This command grabs the same 1000 logs as above, but it parses the log header and extracts the log timestamp, forwarder, and other information, and puts them in a CSV formatted file.

Example CSV: 1422401778,10.250.142.64,10.25.50.66,hop04b-LC1,%MSISA-4: 81.136.243.248...

The timestamp is in Epoch time. The `includeHeaders` and `separator` parameters can only be used on NetWitness Suite installs 10.4.0.2 and later.

```
sdk content sessions=1-now render=logs append=mylogs.log
fileExt=.log includeHeaders=true separator=","
where="risk.info='nw35120'"
```

This command writes a log file across the current session range, but only logs that match `risk.info='nw35120'`. Keep in mind that when you add a where clause, it performs a query in the background to gather the session ids for export. The query should be run on a service with the proper fields indexed (which is typically a Broker or Concentrator). In this case, since you are querying the field `risk.info`, double-check the service where you run the command to make sure it is indexed at the value level (IndexValues, see index-concentrator.xml for examples). By default, most Decoders only have time indexed. If you use any field but time in the where clause, you need to move the query from the Decoder to a Concentrator, Broker, or Archiver with the proper index levels for the query. You can find more information on indexing and writing queries in the *NetWitness SuiteCore Database Tuning Guide*.

```
sdk content sessions=1-now render=logs append=mylogs.log
fileExt=.log includeHeaders=true separator=","
where="threat.category exists && time='2015-01-05 15:00:00'-
'2015-01-05 16:00:00'"
```

This command is the same as above, but it only searches for matching logs between 3 PM and 4 PM (UTC) on Jan 5, 2015 that have a meta key `threat.category`. Again, because this query has a field other than time in the where clause (`threat.category`), it should be run on a service with `threat.category` indexed at least at the `IndexKeys` level (the operators `exists` and `!exists` only require an index at the key level, although values work fine, too).

```
sdk content sessions=1-now render=logs append=mylogs
fileExt=.log where="event.source begins 'microsoft'"
maxFileSize=1gb
```

This command creates multiple log files, each one no larger than 1 GiB in size. It prepends the filenames with **mylogs** and appends them with the date-time of the first packet/log timestamp in the file. Some example filenames: **mylogs-1-2015-Jan-28T11_08_14.log**, **mylogs-2-2015-Jan-28T11_40_08.log** and **mylogs-3-2015-Jan-28T12_05_47.log**. On versions older than Security Analytics 10.5, the T separator between date and time is a space.

```
sdk content sessions=1-now render=pcap append=mypackets
where="service=80,21 && time='2015-01-28 10:00:00'-'2015-01-28
15:00:00'" splitMinutes=5 fileExt=.pcap
```

This command grabs all packets in between the five-hour time period for service types 80 and 21 and writes a PCAP file. Every 5 minutes, it starts a new PCAP file.

```
sdk content time1="2015-01-28 14:00:00" time2="2015-01-28
14:15:00" render=pcap append=mydecoder fileExt=.pcap
maxFileSize=512mb sessions=1-now
```

Pay attention to this command. Why? It works for both packets and logs and is *extremely fast*. The downside is that you get everything between the two time ranges and you cannot use a where clause. Again, it starts streaming everything back almost immediately and does not require a query to run first on the backend. Because everything is read using sequential I/O, it can completely saturate the network link between the server and client. It starts creating files prepended with **mydecoder** and splits to a new file once it reaches 512 MiBs in size.

```
sdk tailLogs
```

or (the equivalent command):

```
sdk content render=pcap console=true sessions=now-u
```

This is a fun little command. It actually uses `sdk content` behind the scenes. The purpose of this command is to view all incoming logs on a Log Decoder. That is it. It is very simple. As logs come into the Log Decoder (you can run it on a Broker or Concentrator, too), they are output on the console screen. It is a great way to see if the Log Decoder is capturing and what exactly is coming into the Log Decoder. This command runs in continuous mode. Do not use it if the Log Decoder is capturing at a high ingest rate (this command cannot keep up with it). However, it is helpful for verification or troubleshooting purposes.

```
sdk tailLogs where="device.id='ciscoasa'"
pathname=/mydir/anotherdir/mylogs
```

This command is the same as above, except it only outputs logs that match the where clause and instead of outputting to the console, it writes them to a set of log files under `/mydir/anotherdir` that do not grow larger than 1 GiB. Obviously, you can accomplish this with the `sdk content` command as well, but it is a little less typing with this command if you like the default behavior.

```
sdk content sessions=now-u render=pcap where="service=80"
append=web-traffic fileExt=.pcap maxFileSize=2gb
maxDirSize=100gb
```

This command starts writing PCAPs of all web traffic from the most recent session and all new incoming sessions that match service=80. It writes out PCAPs no larger than 2 GiBs and if all the PCAPs in the directory grow larger than 100 GiBs, then it deletes the oldest PCAPs until the directory is 10% smaller than the max size. Keep in mind that the directory size checking is not exact and it only checks every 15 minutes by default. You can adjust the number of minutes between checks by passing `cacheMinutes` as a parameter, but this only works with Security Analytics 10.5 and later.

```
sdk content sessions=79000-79999 render=nwd
append=content-%1%.nwd metaFormatFilename=did
```

This is a poor person's backup command. It grabs 1000 sessions and outputs the full content (sessions, meta, packets, or logs) to the NWD (NetWitness Data Format) format. NWD is a special format that can be re-imported to a Packet or Log Decoder without reparsing. So essentially, the original parsed session imports without changes. The timestamp does not change as well, so if it was originally parsed 6 months ago, the timestamp upon import will be retained as 6 months ago.

Note: Do not expect great performance with this command, especially with packets. Gathering the packets for a session involves a lot of random I/O and can drastically slow down the export. Logs do not suffer as much from this problem (only one log per session), but behind the scenes this command uses the /sdk content API and this is not a performance minded streaming API like /sdk packets. So again, do not expect great performance.

The `metaFormatFilename` parameter is very helpful in this command. If this command is run on a Concentrator with more than one service, the NWD filenames will be created with the `did` meta for each session (the %1% in the append parameter is substituted with the value of `did`). Each filename will indicate exactly which Decoder the data came from.

```
sdk content session=1-u where="service=80,139,25,110"
render=files maxDirSize=200mb cacheMinutes=10
```

This is another fun little command. It works very similar to our old Visualize product if you pair the output directory with something like Windows Explorer in Icon mode. It extracts files from all web, email, and SMB traffic. This includes all kinds of files, such as images, zip files, videos, PDFs, office documents, text files, executables, and audio files. If it extracts malware, your virus scanner will flag it. Do not worry, nothing will be executed by the command, so it does not infect the machine (unless you try to execute it yourself). However, it can be useful because if you do find malware, the filename indicates the session id where it was extracted. You can then query that session id and see what host the malware possibly infected and take action. You can filter what gets extracted with the parameters `includeFileTypes` or `excludeFileTypes` (see the command help). For instance, adding `excludeFileTypes=".exe;.dmg;.msi"` prevents executables and installers from being extracted. This command just runs nonstop extracting files from all existing and any new sessions. After the directory gets littered with more than 200 MiBs of files, it automatically starts cleaning up the files every 10 minutes.

Note: This command only makes sense for packet sessions, not logs.

```
sdk content session=1-now where="time='2015-01-27 12:00:00'-'2015-01-27 13:00:00'
&& (service=25,110,80)" subdirFileTypes="audio=.wav;.mp3;.aac;
video=.wmv;.flv;.mp4;.mpg;.swf; documents=.doc;.xls;.pdf;.txt;.htm;.html
images=.png;.gif;.jpg;.jpeg;.bmp;.tif;.tiff archive=.zip;.rar; other=*"
renameFileTypes=".download|.octet-stream|.program|.exe;.jpeg|.jpg" render=files
maxDirSize=500mb
```

This command extracts files from HTTP and email sessions from a one-hour period and then groups the extracted files into directories specified by the `subdirFileTypes` parameter. For instance, any extracted audio file with the extension .wav, .mp3 or .aac will be placed into the subdirectory audio, which will be created under the specified output directory. The same goes for all the other groups specified in that parameter. Some files will also be automatically renamed based on their file extension. This is handled by `renameFileTypes`. Any file with an extension .download, .octet-stream or .program will be renamed to .exe. Files with the extension .jpeg will be renamed .jpg. Once the top-level directory exceeds 500 MiBs, the oldest files get cleaned. This command stops at the last session at the time the command started.

```
sdk search session=1-now where="service=80,25,110" search="keyword='party' sp ci"
```

This command searches all packets and logs (the `sp` parameter) for the keyword `party`. If party is found anywhere in the packets or logs, it outputs the session id along with the text it found and the surrounding text for context. The where clause indicates that it only searches web and email traffic. The `ci` parameter means that it is a case insensitive search. You can substitute `regex` for `keyword` and it performs a regex search.

```
sdk search session=1-now search="keyword='checkpoint' sp ci" render=log
append=checkpoint-logs.log fileExt=.log
```

This is an interesting command example. It searches all logs (or it could be packets) for the keyword `checkpoint` and if that keyword is seen, it extracts the log to a file **checkpoint-logs.log**. There are all kinds of possibilities with this command. Essentially, when a hit is detected, it hands off the session to the content call. So any parameters you pass to `sdk search` that it does not recognize, it just passes along to the content call. This allows the full capabilities of the `sdk content` call, but only working on those sessions with content search hits. With great power comes great responsibility!

Commands Used for Troubleshooting

NwConsole provides the following commands that are helpful when troubleshooting Security Analytics:

- **whatIsWrong**: Provides a snapshot of a service's configuration, stats, and failure and warning logs for a specified past period of time.
- **dbcheck**: Performs consistency checking of database files.
- **topQuery**: Helps pinpoint queries that are taking an excessively long time to run.
- **netbytes**: Troubleshoots the network connections on the current host
- **netspeed**: Troubleshoots the connection between the host computer running NwConsole and the remote computer connected to it using the `login` command.

The following sections as well as the NwConsole help and topic information (man) pages, provide additional information.

whatIsWrong

When a service is not working correctly, the reason is usually somewhere in the logs that the service has written. You can use the `whatIsWrong` console command to obtain a snapshot of a service's configuration, stats, and failure and warning logs (with surrounding context logs) for a specified past period of time, which defaults to the previous seven days. You can save the results of running whatIsWrong into a specified plain text file. The output of this command can be a useful starting point to help determine what is currently wrong with a service.

To use the whatIsWrong console command, log on to the service to troubleshoot using the `login` command, and run the `whatIsWrong` command.

Hint: Use `help whatIsWrong` to see all of the available parameters, including the number of days/hours to look back for events, the pathname to store results, whether or not to append or overwrite the results file, and the delimiter to use for log fields. You can also limit the number of most recent logs used to find context, and you can specify how many context logs per warning/failure log to retrieve.

Whenever you receive a request for logs for a Core service, you should run the whatIsWrong command first and use the results collected as a starting point.

dbcheck

The `dbcheck` command is used to perform consistency checking of database files (session, meta, packets, logs, stats, and so on). This might be necessary when a service cannot start because of errors in the consistency of the database files. Normally a service would automatically recover and correct any consistency issues on startup, but there are times when this does not occur. When a service starts (like Decoder), it typically does not read or open most database files in order to start quickly. It assumes most files are in a consistent state and only does a cursory check of the most recently written files. If there are problems, `dbcheck` can perform those consistency checks, but ONLY if the service is not running.

Caution: Do not attempt to run this command while a service is running.

For example, you can check a single file:

```
dbcheck /var/netwitness/decoder/packetdb/packet-000000001.nwpdb
```

You can also use wildcards to check multiple files:

```
dbcheck /var/netwitness/decoder/metadb/meta-00000002*.nwmdb
```

topQuery

The `topQuery` command can help pinpoint queries that are taking an excessively long time to run. This command parses the audit logs of a service and returns the top N longest running queries for the specified time period.

The easiest way to run it is to log on to the service (usually a Broker or Concentrator) and type `topQuery`. The default behavior is to return the top 100 longest running queries for the last seven days.

Type `help topQuery` for the list of parameters. Here are some additional examples with explanations:

```
topQuery hours=12 top=10
```

This command returns the top 10 queries for the last 12 hours.

```
topQuery time1="2015-03-01 00:00:00" time2="2015-03-14 00:00:00"
```

This command returns the top 100 queries between March 1, 2015 and March 14, 2015. Times are in UTC, not local.

```
topQuery input=/var/log/messages output=/tmp/top20.txt top=20 user=sauser1
```

Instead of connecting to a service, it parses the syslog audit messages for the top 20 queries in the last 7 days, but only for queries executed by user sauser1. It writes the top 20 queries to /tmp/top20.txt instead of the console screen. The parameter user is a regex, so you can specify multiple usernames by writing something like `user="(sauser1|sauser2)"`.

netbytes

The `netbytes` command is very useful for troubleshooting the network connections on the current host. It displays continuous send and receive statistics for all network interfaces. Once executed, you must press **Ctrl-C** to exit this command, which also exits NwConsole.

netspeed

The `netspeed` command is used to troubleshoot the connection between the host computer running NwConsole and the remote computer connected to it through the `login` command. You must supply the amount of bytes to transfer and it will time the speed of the connection. The netspeed command is very useful for troubleshooting Aggregation performance issues that might be network related.

```
login somedecoder:50004 admin ...
```

```
netspeed transfer=4g
```

To troubleshoot the connection between a Concentrator and a Decoder, SSH into the Concentrator, run NwConsole, and then log on to the Decoder and run `netspeed`. The output from the command gives you an indication of the maximum network throughput. If it is much less than the standard 1 Gbps interface, it could indicate a network issue.

RSA NETWITNESS® SUITE

RESTful API User Guide

for Version 11.x

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

RESTful API 4

Usage 5

Usage example: the "/logs" Node 5

Example Syntax 6

Find More Details 6

Access the RESTful API in NetWitness Suite 9

Packets 10

Parser/Feed Upload 11

Stat Graphing 12

SDK Commands 14

RESTful API

The RESTful API that ships with RSA NetWitness® Suite is a way to programmatically communicate with the NEXTGEN architecture. It must be enabled by setting `/rest/config/enabled` to **on**, which is the default. The default port for communication is the default port + 100 (for example, **50105** for a Concentrator), but that can be changed by setting the `/rest/config/port` parameter. SSL is controled by the setting in `/sys/config/ssl`. For information about how to perform these tasks, see Access the RESTful API in NetWitness Suite.

The API is based on HTTP and is quite easy to use. The acceptable output formats are:

- text/plain
- text/xml
- text/html
- application/json

The content type that is returned can be controlled through the **HTTP Accept** header. It is possible to set the parameter **force-content-type** to one of the previous values.

The easiest way to begin is to point a browser to the REST port (for details about how to perform these tasks, see Access the RESTful API in NetWitness Suite):

`PATH: http://<hostname or IP>:<REST port>`

This command performs the default command of **ls**, and returns a listing for the root node tree used by NEXTGEN:

Usage

The REST API accepts commands by using URL parameters and by POSTing application/json.

The special content type, `application/x-netwitness-string-params`, passes parameters, as plain text, in the format:

```
param1=value1 param2="value \"2\""
```

Note: Quotes, as part of the value, must be preceded by the backslash \ character. Any character can be escaped in this manner, including the backslash itself \\.

The format of the URL consists of the following components:

```
http://<hostname or IP>:<port>/[node1][/node2][…]?msg=<message name>
[&param1=value1][&param2=value2][…]
```

Usage example: the "/logs" Node

The /logs node supports several different messages:

- **ls**–Returns a list of child nodes. It supports the parameters depth and options.
- **mon**–Monitor this node (and possibly descendants) for changes. However, this message is not supported by the REST API because it requires a persistent connection and pipe that cannot be done via REST. Monitoring currently requires the full NextGen SDK library.
- **pull**–This command pulls logs from the service. It supports two parameters: **count**, which controls how many logs to return, and **id2**, which controls the ending log ID to return. **id2** is optional and when it is not provided, the last log written is returned.
- **info**–Returns detailed node information.
- **help**–The parameters are covered in more detail in Find More Details.
- **count**–A simple command to return the number of child nodes.
- **stopMon**–Stop monitoring the node from a previous mon command (also not supported by REST).
- **download**–A more complicated command to download a large number of log messages with several parameters to control log types and text matching capabilities. Like the **mon** command, this requires more than a simple request/response, which is not supported by the REST node interface.
- **timeroll**–Any log entries that exceed a given age are deleted.

To get a full list of NEXTGEN messages and parameters, use the help message:

```
http://<hostname>:<port>/logs?msg=help
```

The above command returns:

description	A container node for other node types
security.roles	everyone,logs.manage
message.list	The list of supported messages for this node
ls	[depth:<uint32>] [options:<string>]
mon	[depth:<uint32>] [options:<uint32>]
pull	[id2:<uint64>] [count:<uint32>] [timeFormat:<string>]
info	
help	[msg:<string>] [op:<string>] [format:<string>]
count	
stopMon	
download	[id1:<uint64>] [id2:<uint64>] [time1:<date-time>] [time2:<date-time>] op:<string> [logTypes:<string>] [match:<string>] [regex:<string>] [timeFormat:<string>]
timeroll	[timeCalc:<string>] [minutes:<uint32>] [hours:<uint32>] [days:<uint32>] [date:<string>]
debugGen	[count:<uint32>]

Example Syntax

To view the last 100 logs:

```
http://hostname:50105/logs?msg=pull
```

To view the logs in XML format:

```
http://hostname:50105/logs?msg=pull&force-content-type=text/xml
```

To see the last 10 logs in plain text:

```
http://hostname:50105/logs?msg=pull&count=10&force-content-type=text/plain
```

Find More Details

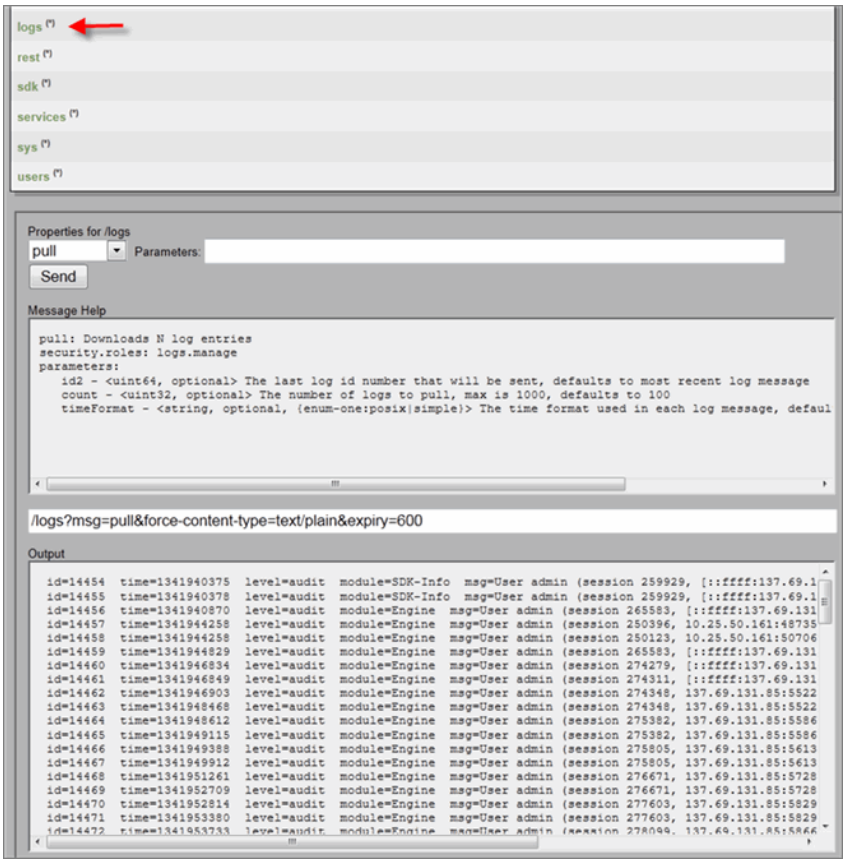
For more detailed information about a message (for example the pull message), request help specific to just that message. The **help** message displayed above uses the parameter name **msg**, but in the URL below, **message** is used, an alias for the help **msg** parameter to avoid conflicts with the REST API **msg**.

```
http://<hostname>:<port>/logs?msg=help&message=pull
```

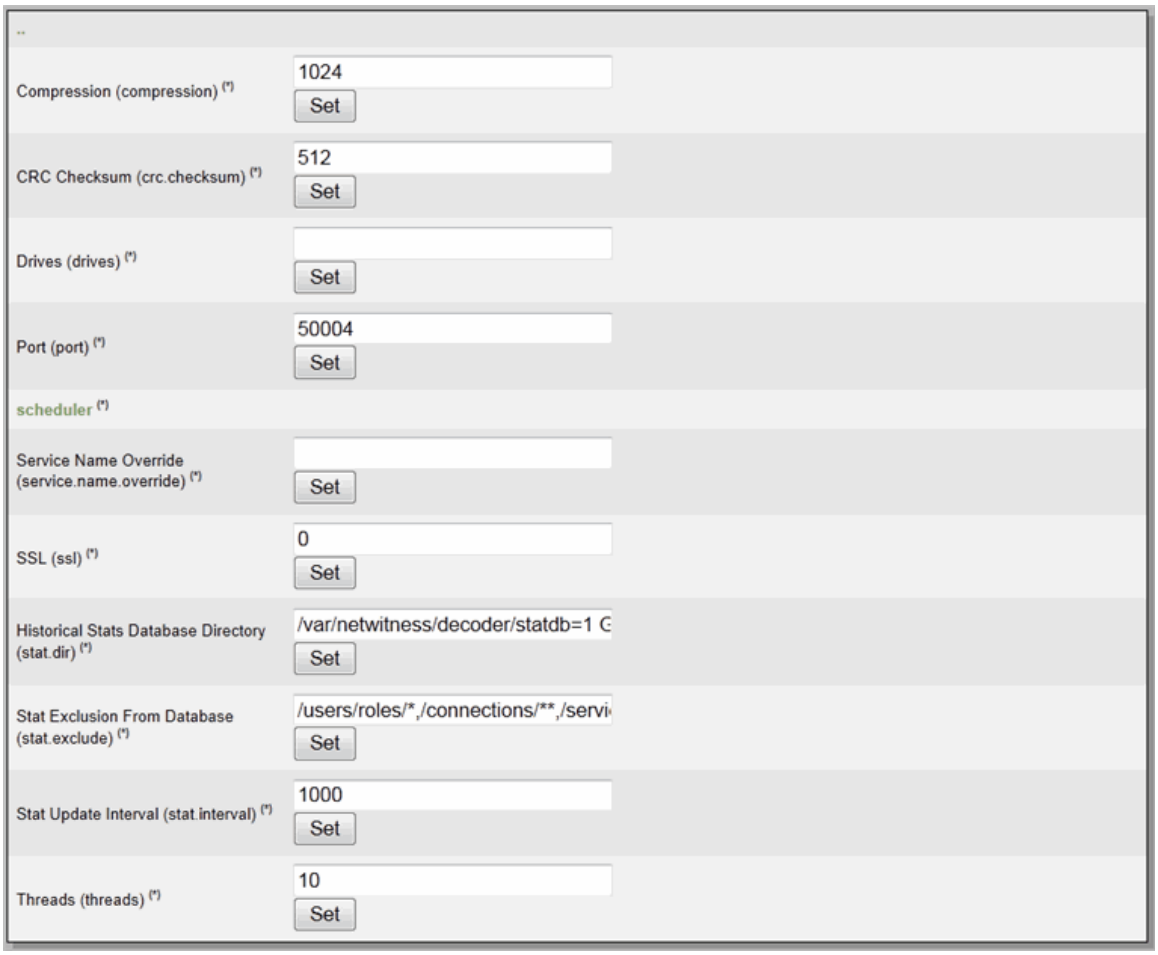
```
        Downloads N log entries
        security.roles: logs.manage
        parameters:
pull    id2 - <uint64, optional> The last log id number that will be sent, defaults to most recent log message
        count - <uint32, optional> The number of logs to pull, max is 1000, defaults to 100
        timeFormat - <string, optional, {enum-one:posix|simple}> The time format used in each log message, default is posix time (seconds since
        1970)
```

Alternately, you can go back to the browser and click the (*) in the properties pane on one of the nodes, as shown here:

When you select a command, the **Message Help** is displayed. When you click **Send**, the output is shown in a separate pane, as shown here:



In this view, you can easily navigate the node tree to use the various commands supported by NEXTGEN or to make configuration changes.



For example, from `/sys/config`, you can make configuration changes and click **Set** to send the changes.

Access the RESTful API in NetWitness Suite

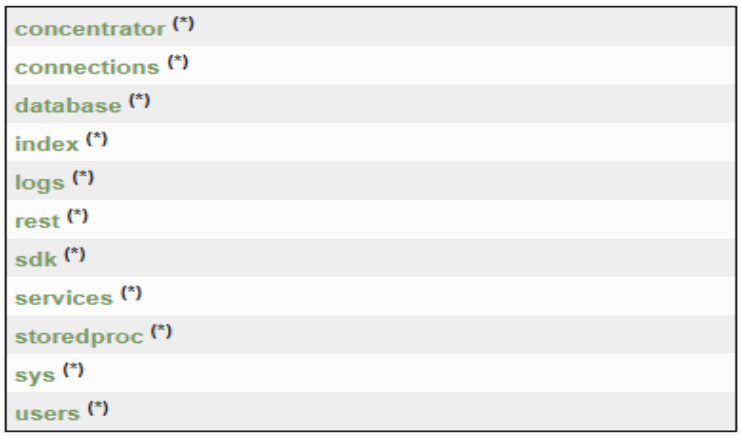
This topic describes how to enable the REST API in NetWitness Suite. The REST API must be enabled by setting `/rest/config/enabled` to **on**, which is the default. The default port for communication is the default port + 100 (for example, **50105** for a Concentrator), but that can be changed by setting the `/rest/config/port` parameter. SSL is controled by the setting in `/sys/config/ssl`.

To enable the REST port:

1. In the NetWitness Suite web user interface, go to **ADMIN** > **Services** and select a service, for example, a Concentrator.
2. In the **Host** column, click on the host name. The Hosts page opens, and the IP address of the host is displayed in the **Host** column. Make a note of the IP address.

   Note: If the IP address listed in the Host column is the same as the IP address of the NetWitness Suite web UI, the API is not available for that service.
3. Go to **ADMIN** > **Services**, select the service, and then select **View** > **Config**. Under **System Configuration**, note the port number. You will use this port number as a basis for accessing the API, but you must add 100 to it. For example, if the port number is listed as **50005**, you would enter **50105**.
4. In the browser, type the IP address of the service and append the port number to the IP address as shown here:
   `http://<hostname or IP address>:<port>`

   Note: The URL is HTTP, and not HTTPS.
5. In the Authentication dialog, enter the user name and password and click **Log in**. A listing of the root node tree used by NEXTGEN is displayed:



Packets

You can retrieve a **pcap** file using the REST service.

```
http://<hostname>:<port>/sdk/packets
```

If you point a browser to this URL, the web page lets you enter a list of session IDs or a time range. When you click **Submit**, it generates a **pcap** based on the supplied criteria.

Programmatically, using HTTP GET or POST, submit either a **sessions** parameter with a comma-separated list of session IDs and session ranges (#-#) or a **time1** and **time2** parameter. Times must be in the format **YYYY-MM-DD HH:MM:SS**, for example: **2010-Apr-20 09:00:00**.

Note: Since the list of sessions can get quite long, this API accepts the content-type `application/x-netwitness-string-params` for a **POST** command.

Importing Packets

You can import packets to a DECODER using the REST service.

```
http://<hostname>:<port>/decoder/import
```

If you point a browser to this URL, the web page lets you select a **pcap** file for upload. It also accepts pcap files POSTed to this URL.

REST begins processing incoming data immediately after the HTTP header is parsed. This means import of a **pcap** file occurs quickly and allows for large transfers. There is still a limit, but it is much larger (GBs) and is based on how well the import process can keep up with the client POST coming in. If the client posts a huge pcap (many GBs), it is still possible to overfill the current buffer. Any pcap that is 4 GBs or less should be able to process without issue.

Note: The DECODER cannot be concurrently importing or capturing, or an error results.

Parser/Feed Upload

You can upload Parsers and Feeds using the REST service.

`http://<hostname>:<port>/decoder/parsers/upload`

If you point a browser to this URL, the web page lets you select a parser or feed file for upload.

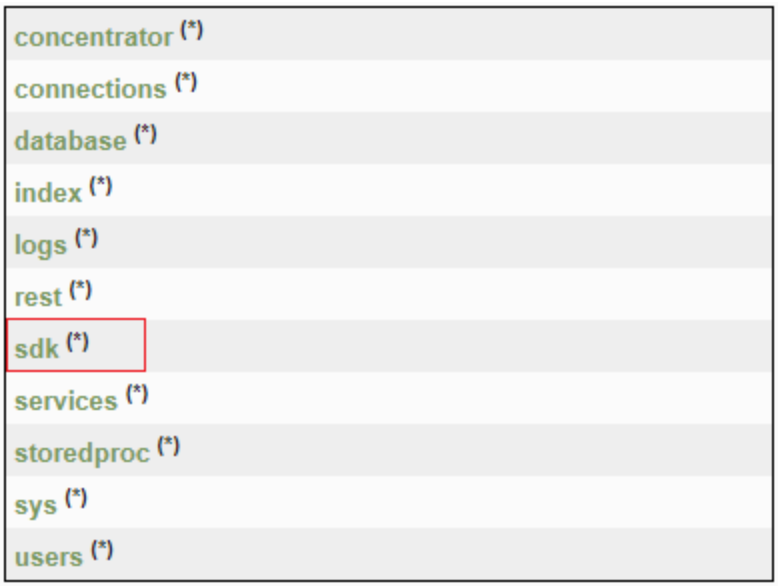
You can also force a reload by selecting the toggle or providing the parameter `reload=1` on the URL.

Stat Graphing

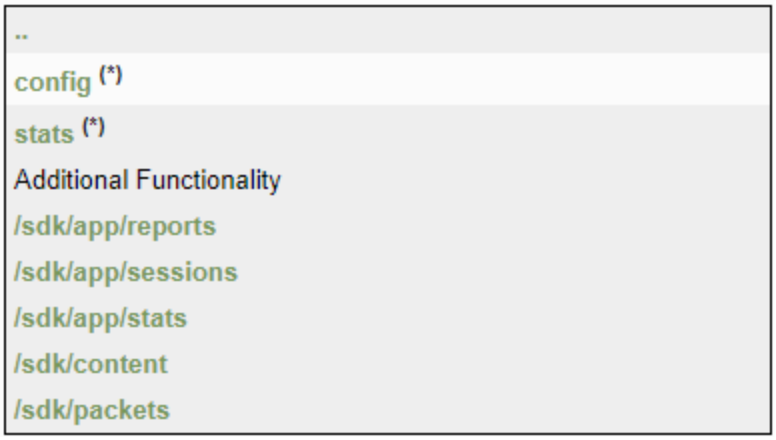
The REST interface has a built-in statistics graphing tool, which helps you monitor performance for a service during a specified time period. You can use this tool to collect and graph single or multiple statistics from a host during a specific time range. You can also graph real-time statistics.

To access the statistical graphing tool:

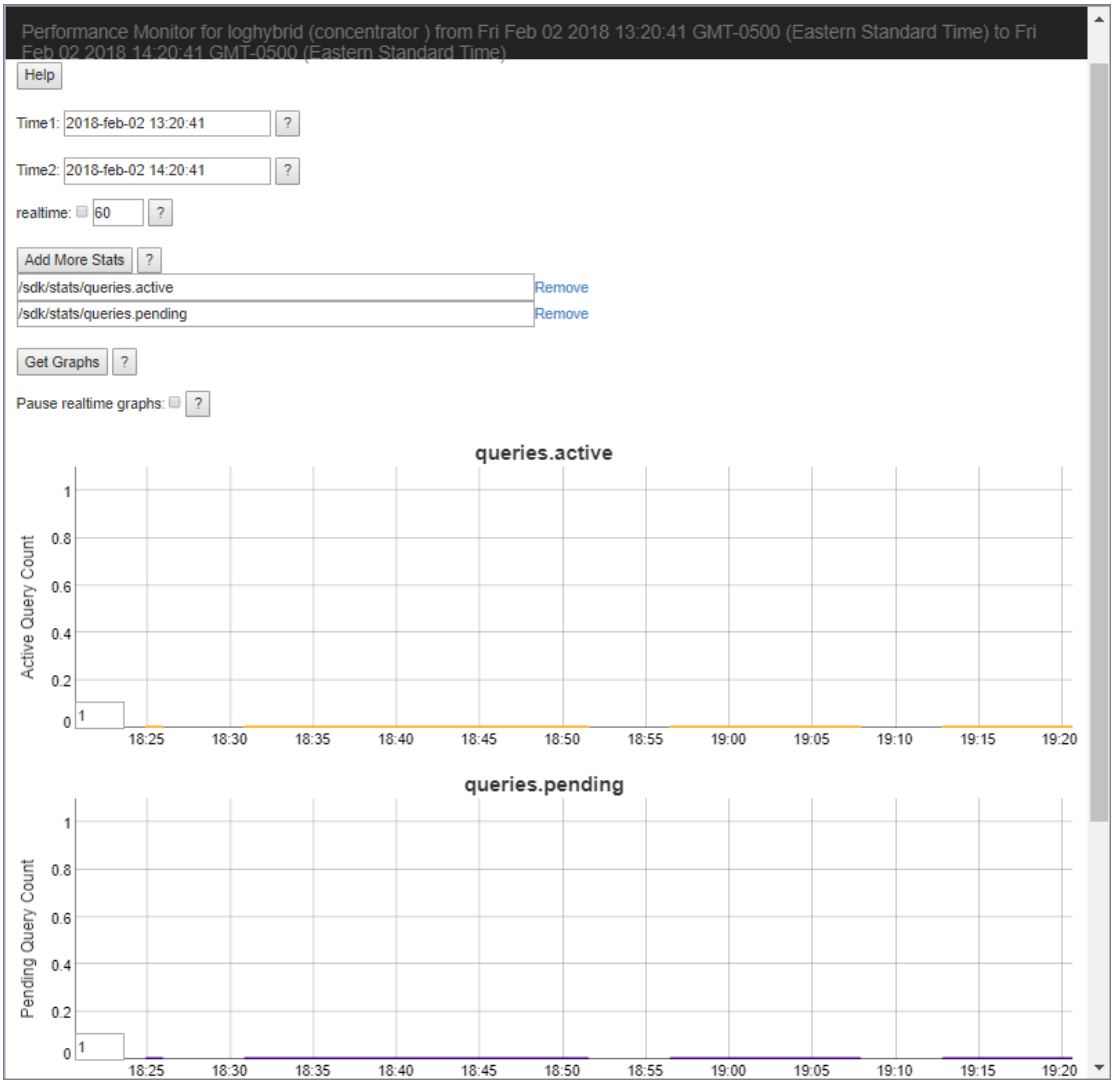
1. From the root node tree page, click `sdk`. (For information on accessing the root tree note page, see Access the RESTful API in NetWitness Suite.)



The options for additional functionality are displayed:



2. Click **sdk/app/stats**. The Performance Monitor window opens, and statistical graphs are displayed at the bottom of the page.



Click the Help buttons for detailed information about this page and the fields it contains.

SDK Commands

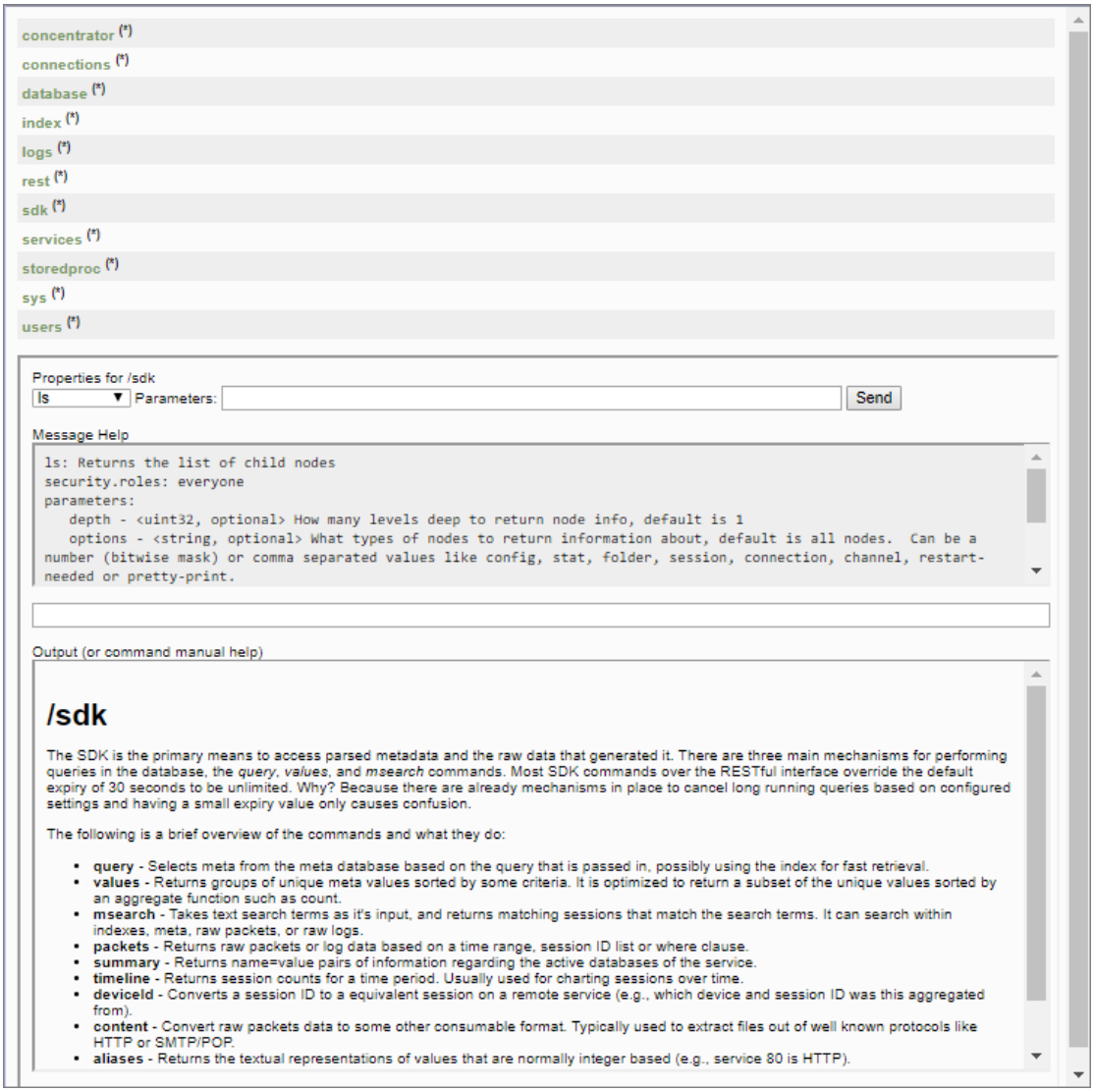
All queries on the system are performed by commands sent to the **/sdk** node.

The **/sdk** node has built-in help documentation for each message. To view the help for each command, click on the asterisk (*) beside the sdk node and then choose one of the messages from the drop-down menu. The documentation for the message is displayed in the Output window at the bottom of the screen.

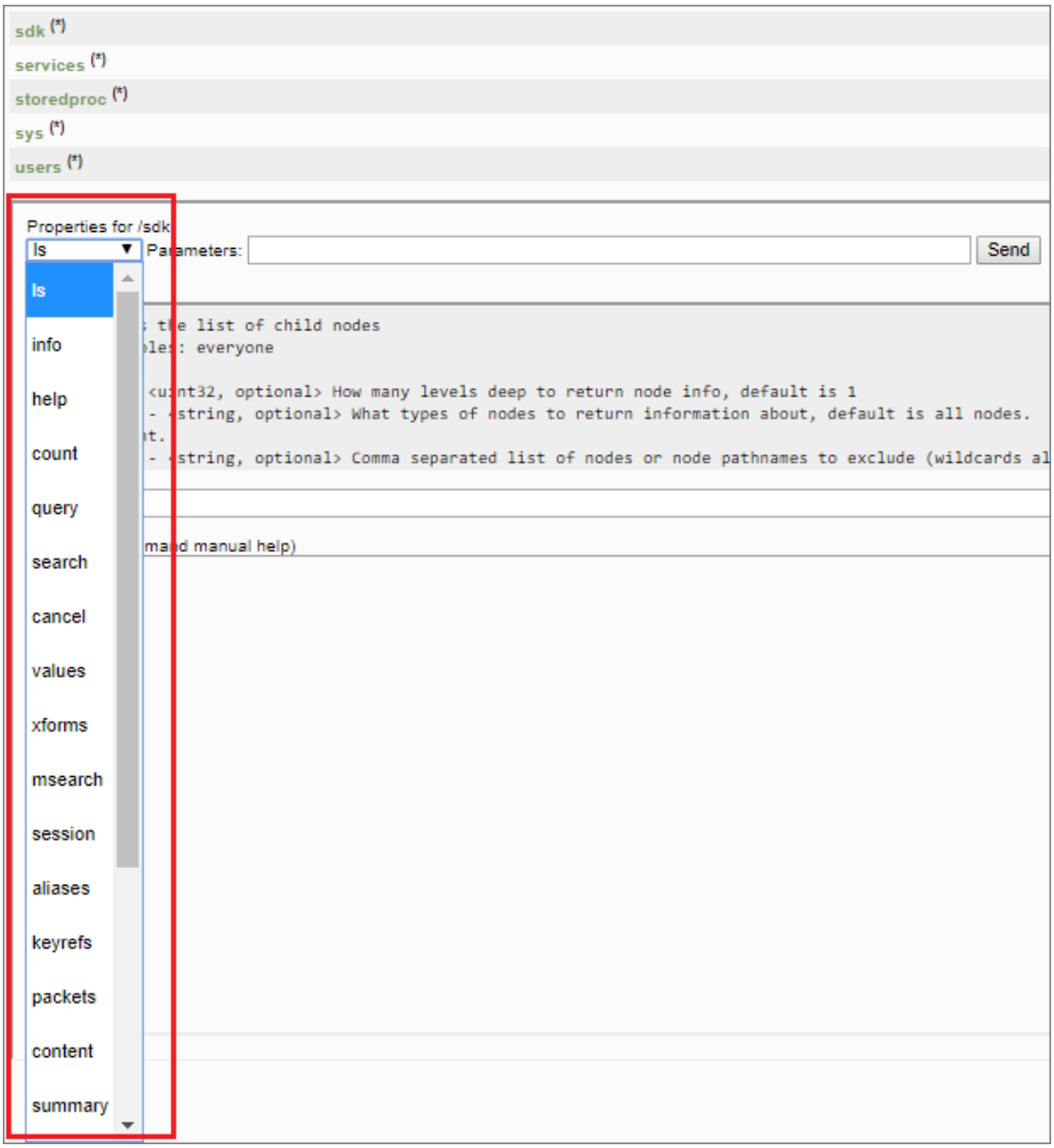
To access the help:

1. From the root node tree page, click `sdk`. (For information on accessing the root tree note page, see Access the RESTful API in NetWitness Suite.)
2. Click the asterisk (*) next to sdk.

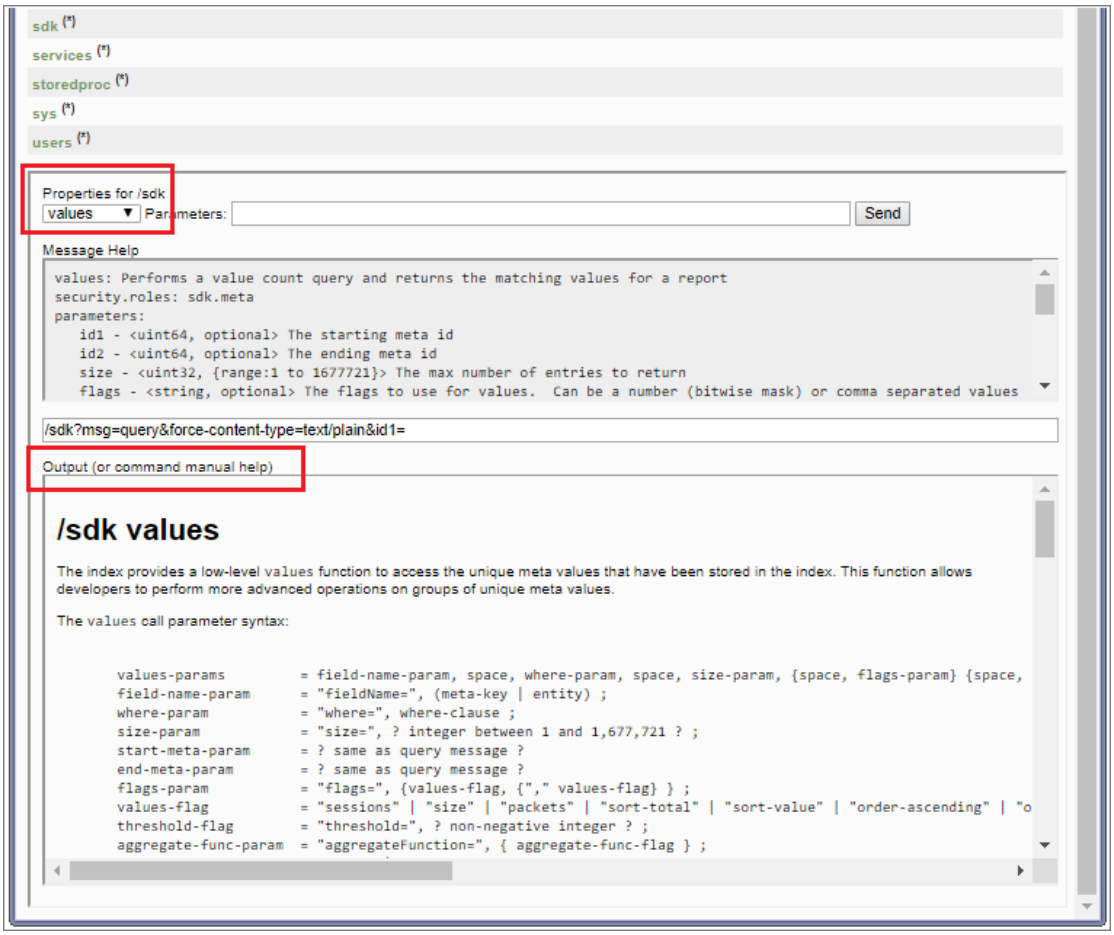
Information about the **/sdk** node is displayed.



3. To find more specific information, select a property from the **Properties for /sdk** drop-down menu:



The help for the property that you selected is displayed in the Output section:



SDK Commands Further Reference

This guide should be used in conjunction with the SDK documentation, which explains the format of queries and results. This document primarily focuses on how to send queries and parameters via the REST API, not how the queries themselves are formatted. The *Core Database Tuning Guide* explains those concepts in detail. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents. All metadata returned via REST is encoded as **UTF-8**.

There is another parameter specific to the REST API called **expiry**. This parameter can be set to the number of seconds to wait for a response before the system returns a timeout error. The default is 30 seconds, which is sufficient for most requests. For queries, the standard SDK sets an infinite timeout. If you set **expiry** to zero (`&expiry=0`), this removes the timeout for that request. It is probably a good idea to set a larger timeout for queries and other requests that may take longer than 30 seconds during normal operations.

RSA NETWITNESS® SUITE

System Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

System Configuration Overview **7**

Standard Procedures **9**

Access System Settings 10

Configure Notification Servers 11

Notification Servers Overview 11

Configure the Email Settings as Notification Server 12

Configure Script as a Notification Server 13

Configure the SNMP Settings as Notification Server 14

Configure a Syslog Notification Server 15

Configure Notification Outputs 17

Notification Outputs Overview 17

Configure Email as a Notification 18

Configure Script as a Notification 19

Configure SNMP as a Notification 20

Configure Syslog as a Notification 21

Configure Templates for Notifications 23

Configure Global Notifications Templates 23

Define a Template for ESA Alert Notifications 26

Import and Export a Global Notifications Template 28

Configure Email Servers and Notification Accounts 29

Configure Global Audit Logging 32

Global Audit Logging - High-Level Procedure 36

Configure a Destination to Receive Global Audit Logs 38

Define a Template for Global Audit Logging 42

Define a Global Audit Logging Configuration 47

Verify Global Audit Logs 50

Configure Investigation Settings 52

Configure Navigate, Events, and Context Lookup Settings 52

Clear Reconstruction Cache for Services 54

Configure Live Services Settings 55

Prerequisite 55

About Live Feedback Participation 56
Live Feedback Overview 61
Upload Data to RSA for Live Feedback 69
Configure Log File Settings 70
Configure System Log File Size and Backup Count 71
Set the Log Level for an Individual Package 71
Configure Syslog and SNMP Settings 72
Configure and Enable Syslog Settings 72
Configure and Enable SNMP Settings 73
Disable Syslog or SNMP Settings 74

Additional Procedures 75

Add Custom Context Menu Actions 75
Example Procedure: Context Menu Action to Investigate ip.dst from alias.ip 79
Configure NTP Servers 81
Add an NTP Server 82
Modify an NTP Server 83

Troubleshooting System Configuration 85

Troubleshoot Global Audit Logging 85
Basic Troubleshooting 85
Advanced Troubleshooting 86
Troubleshooting NTP Server Configuration 95
Issues Identified by Messages in the NTP Settings Panel or Log Files 95

References 97

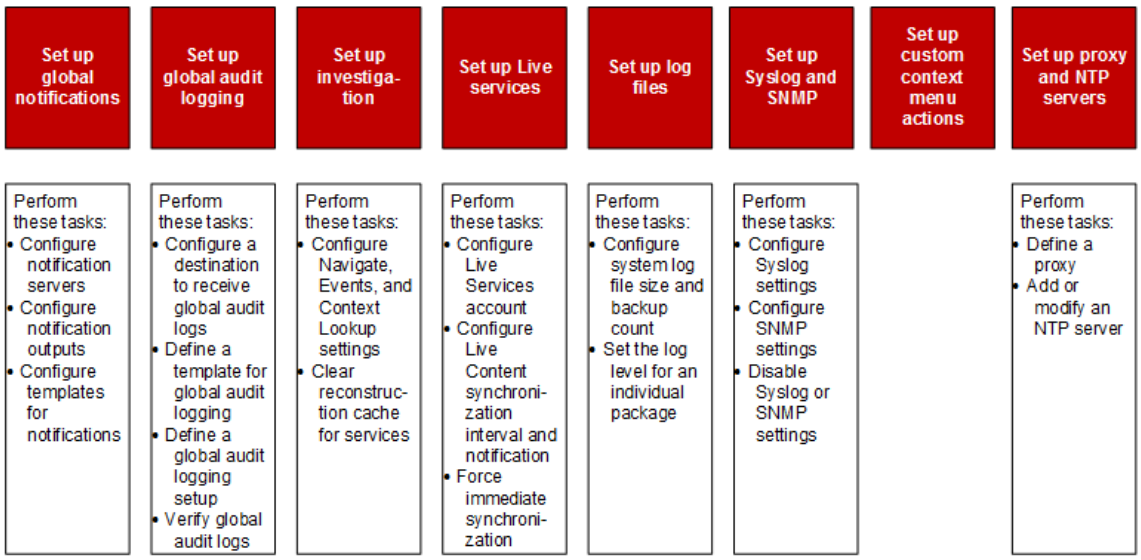
Global Audit Logging Configurations Panel 98
Add New Configuration Dialog 103
Supported CEF Meta Keys 106
Supported Global Audit Logging Meta Key Variables 113
Global Audit Logging Operation Reference 116
Local Audit Log Locations 141
Global Notifications Panel 143
WorkFlow 143
What do you want to do? 143
Related Topics 143
Quick Look 144
Toolbar and Features 144

Global Notifications Panel Toolbar 146
Define Notification Server Dialogs 148
Define Notification Output Dialogs 159
Email 159
SNMP 161
Syslog 162
Script 164
Define Notification Template Dialog 165
Output Tab 168
Servers Tab 172
Templates Tab 175
HTTP Proxy Settings Panel 177
Related topics 177
Quick Look 177
Email Configuration Panel 179
Workflow 179
What do you want to do? 179
Related Topics 180
Quick Look 180
Investigation Configuration Panel 182
Workflow 182
What do you want to do? 182
Related Topics 182
Quick Look 182
Navigate Tab 183
Render Threads Setting 183
Parallel Coordinates Settings 184
Quick Look 185
Quick Look 191
Live Services Configuration Panel 194
New Features Enabled Dialog 194
Workflow 195
What do you want to do? 195
Related Topics 195

Live Services Quick Look 196
About Live Feedback Participation 203
NTP Settings Panel 204
Workflow 204
What you need to do? 204
Related Topics 204
Quick Look 204
Context Menu Actions Panel 207
Workflow 207
What do you want to do? 207
Quick Look 207
Legacy Notifications Configuration Panel 212
Workflow 212
What do you want to do? 212
Related Topics 212
Quick Look 213

System Configuration Overview

In the Administration System view, administrators can configure system settings to receive optimal performance from NetWitness Suite. This diagram show the available configuration options.



In this guide, the standard procedures provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite. Although some of these settings have default values, the administrator needs to view and evaluate all default values.

Additional procedures are not essential for the set up of NetWitness Suite, they include certain customization options that are beyond the usual setup; for example, adding custom context menus or setting up a proxy.

In addition, reference topics and troubleshooting topics supply detailed information about the user interface and suggestions for resolving possible issues.

The following sections describe system configuration:

- Standard Procedures provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite.
- Additional Procedures provide instructions for setting up customization options that are beyond the usual system configuration.

Standard Procedures

The topics in this section provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite. Although some of these settings have default values, the administrator needs to view and evaluate all default values. The procedures can be performed in any sequence and are listed alphabetically.

Access System Settings

Configure Notification Servers

Configure Notification Outputs

Configure Templates for Notifications

Configure the Email Settings as Notification Server

Configure Email Servers and Notification Accounts

Configure Global Audit Logging

Configure Investigation Settings

Configure Live Services Settings

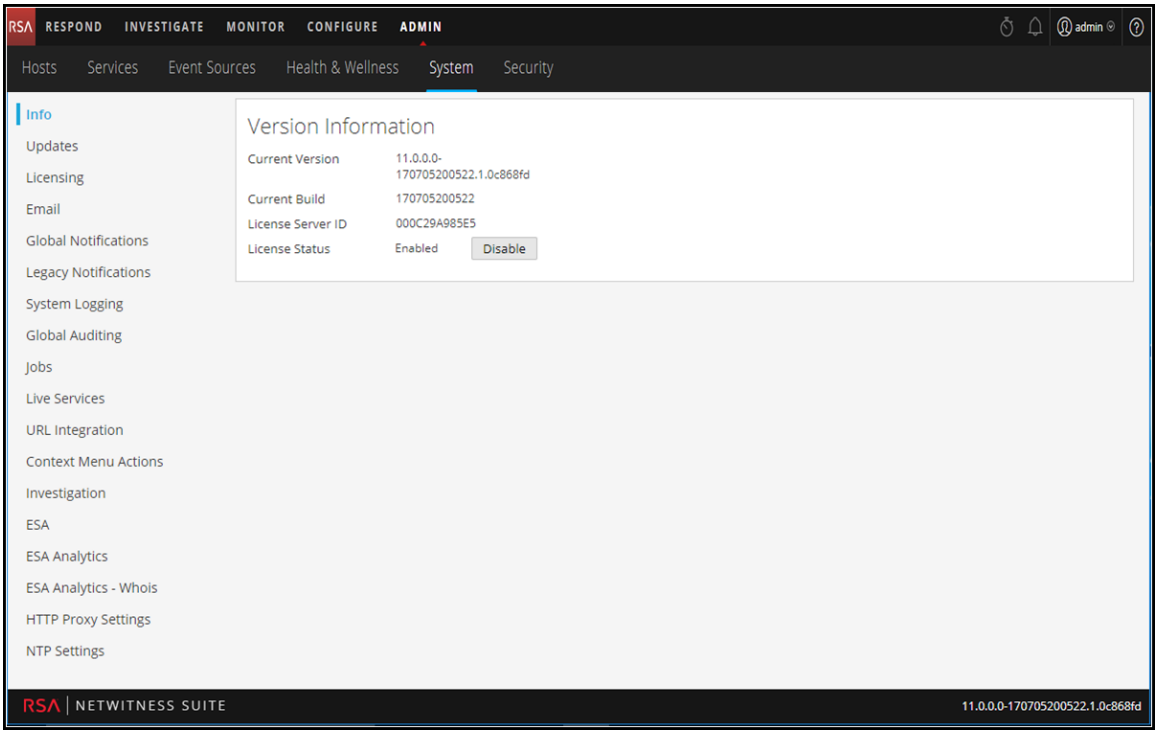
Configure Log File Settings

Access System Settings

This topic introduces system configuration capabilities of NetWitness Suite in the Administration System view. Administrators can configure notifications, email notifications, global audit logging, logging settings, connection to Live Services, and URL integration in NetWitness Suite.

To access the system settings:

Go to **ADMIN > System**.
The Administration System view is displayed.



On the left panel of the Administration System view is an options panel listing all system nodes available for configuration. When you select a node, the associated content is displayed in the right panel.

Configure Notification Servers

This topic provides instructions on how to configure notification servers. For ESA, notification servers are required to define an ESA rule. A notification server is also required to configure global audit logging.

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond. Notification Servers define the servers from which you want to receive notifications from the system. For Global Audit Logging, define Log Decoders as Syslog Notification Servers.

You can define, delete, edit, import, and export a notification server in NetWitness Suite. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide*. You delete, edit, import, and export notification outputs and notification servers in the same way as templates. You cannot disable or delete notification servers associated with global audit logging configurations.

Notification Servers Overview

This topic provides an overview of notification servers. You configure notification servers in the Administration System view (ADMIN > System > Notifications > Servers tab).

Global Notifications are used by a variety of components in NetWitness Suite, such as Event Stream Analysis (ESA), Respond, Health and Wellness, Event Source Management (ESM), and Global Audit Logging. Notification settings are called **Notification Servers**.

Event Stream Analysis sends notifications to users through email, SNMP, or Syslog about various system events. In ESA, these alert notification settings are called Notification Servers. You can configure multiple notification servers and use them while defining an ESA rule, for example, you can configure multiple mail servers or Syslog servers and use the settings while defining an ESA rule.

You can configure the following notification servers:

- Email
- SNMP
- Syslog
- Script

Email notification servers enable you to configure email server settings to send alert notifications. SNMP notification servers enable you to configure SNMP trap host settings as a notification server to send alert notifications.

Syslog notification servers enable you to configure Syslog settings as a notification server to send notifications. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis. For Global Audit Logging, you can only use Syslog Notification Servers.

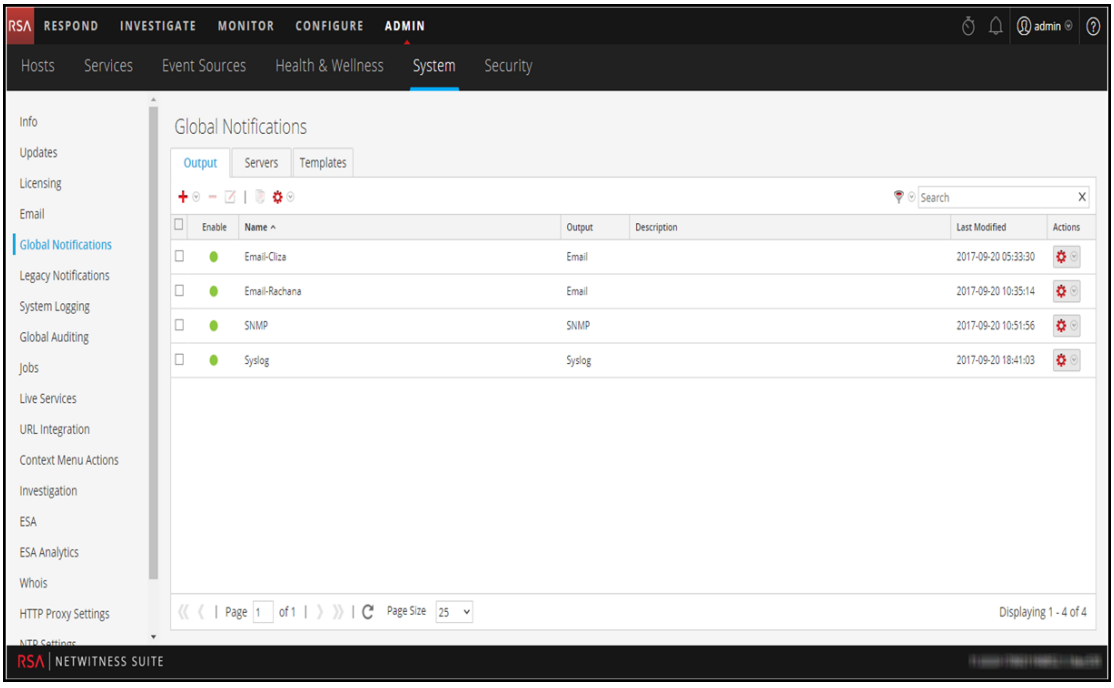
Script notification servers enable you to configure Script as a notification server.

For detailed information on the different notification server configurations, including parameters and descriptions, see Define Notification Server Dialogs.

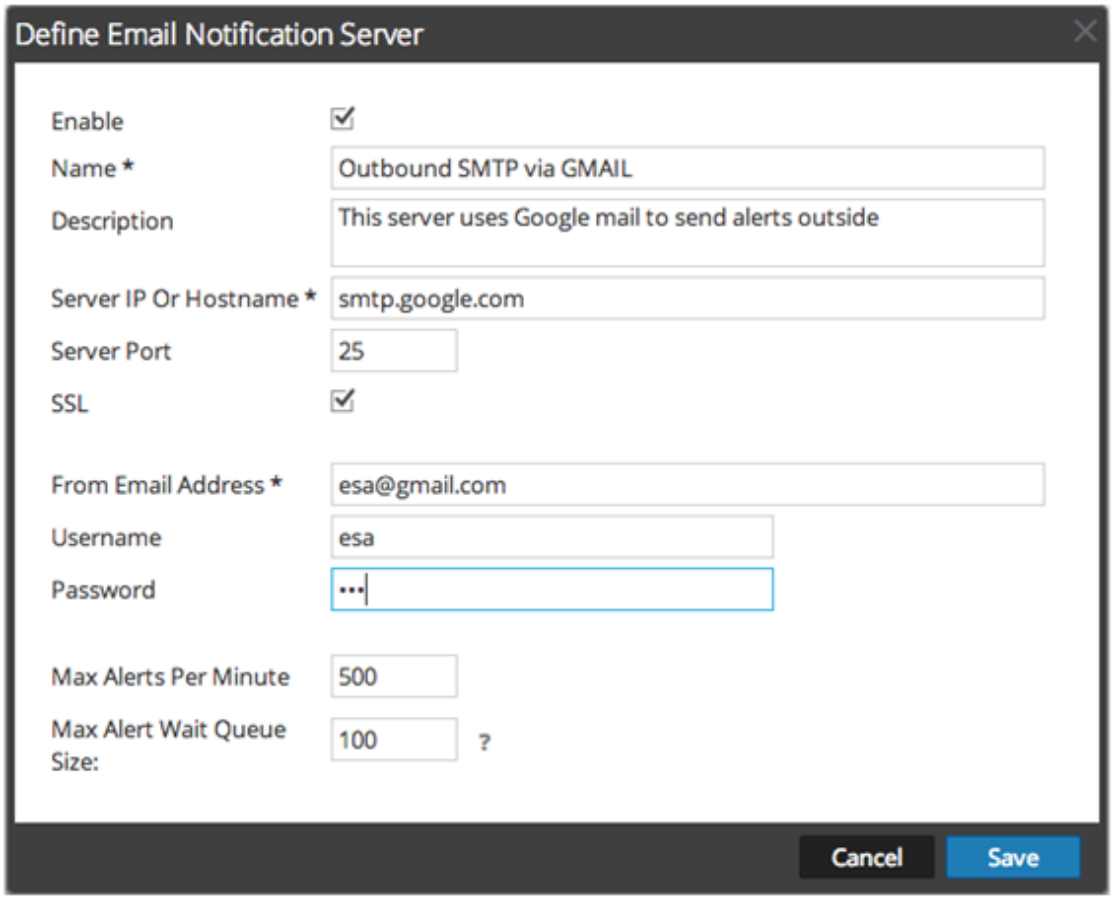
Configure the Email Settings as Notification Server

To configure email server settings as a notification server to send alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
   The **Notifications** configuration panel is displayed with the **Output** tab open.
3. Click the **Servers** tab.



4. From the + drop-down menu, select **Email**.



5. In the **Define Email Notification Server** dialog, provide the required information and click **Save**.

Note: For ESM/SMS and ESA notifications, you must specify only the hostname/FQDN in the Server IP or Hostname field.

For details of the parameters and descriptions, see Define Notification Server Dialogs .

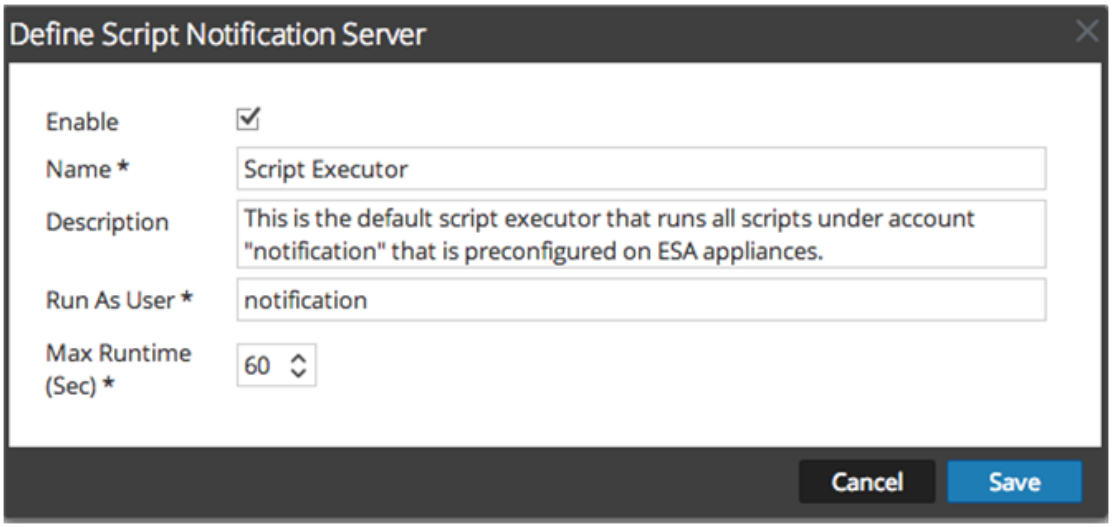
Configure Script as a Notification Server

ESA allows you to run scripts in response to ESA alerts. However, you must first configure the user identity and other details that are required to run the scripts.

To configure Script as a notification server:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

4. From the + drop-down menu, select **Script**.



5. In the **Define Script Notification Server** dialog, provide the required information and click **Save**.

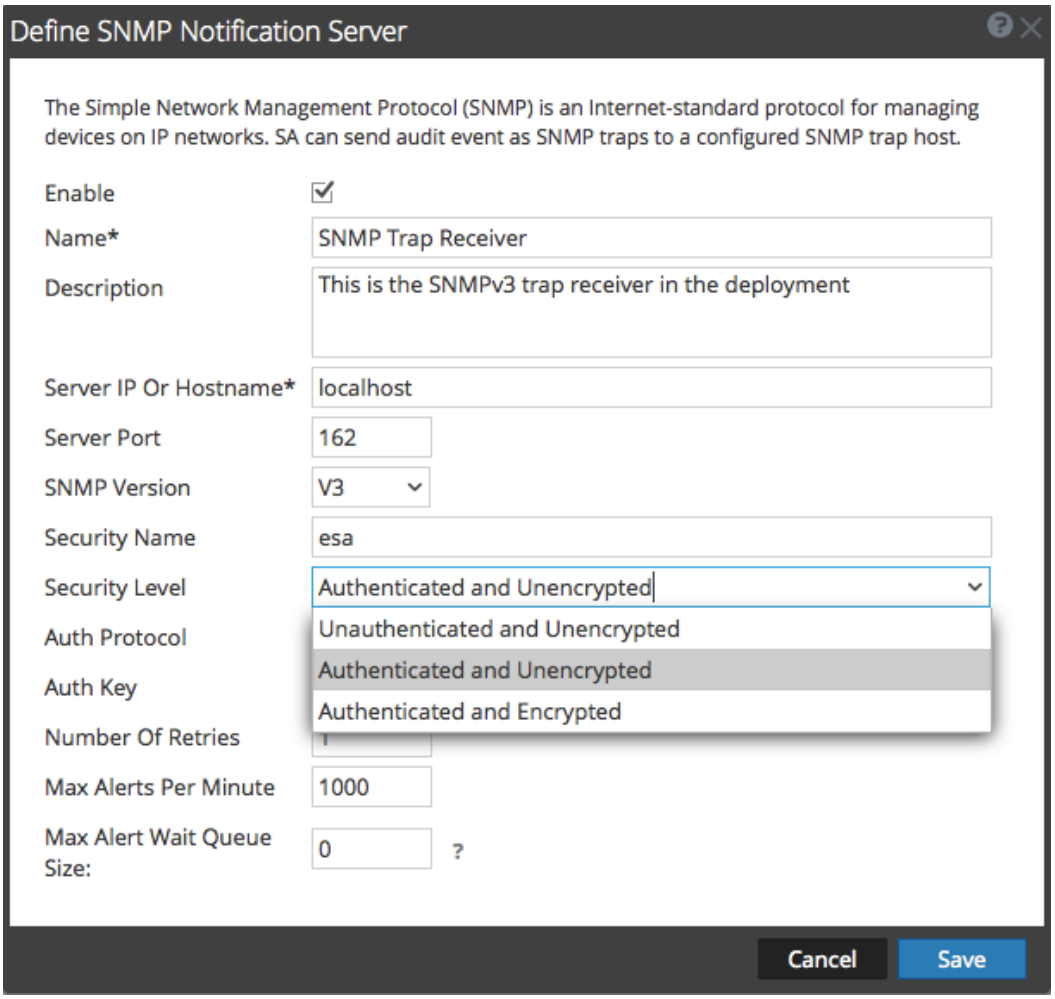
For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure the SNMP Settings as Notification Server

To configure the SNMP trap host settings as a notification server to send alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

4. From the + drop-down menu, select **SNMP**.



5. In the **Define SNMP Notification Server** dialog, provide the required information and click **Save**.

For details of the parameters and descriptions, see Define Notification Server Dialogs.

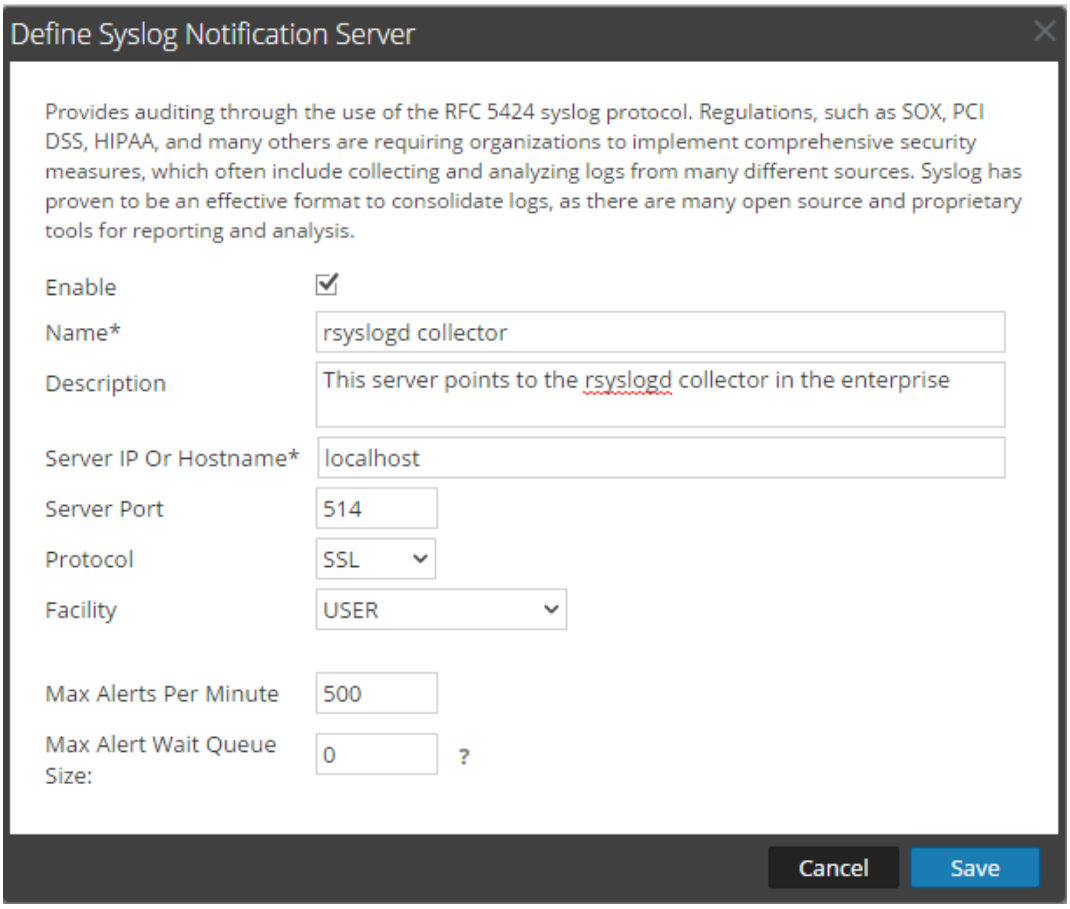
Configure a Syslog Notification Server

This topic provides instructions on how to configure a Syslog notification server. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

To configure Syslog as a notification server:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Servers** tab.
4. From the drop-down menu, select **Syslog**.



5. In the **Define Syslog Notification Server** dialog, provide the required information and click **Save**.

For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure Notification Outputs

This topic provides instructions on how configure notification outputs. These notification outputs are required to define an ESA rule.

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

Note: You do not need to configure the Output tab for Global Audit Logging.

Notification Output configurations define email addresses and subject lines, SNMP trap OID settings, syslog output settings, and script code.

You can define, delete, edit, import, and export notification outputs in NetWitness Suite. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods." You delete, edit, import, and export notification outputs and notification servers in the same way as templates. If you attempt to delete a notification output being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use.

Notification Outputs Overview

This topic provides an overview of notification outputs. These notification outputs are required when defining an ESA rule. You configure notification outputs in the Administration System view (ADMIN > System > Notifications > Outputs tab).

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

Note: You do not need to configure notification outputs (the Output tab) for Global Audit Logging.

Notification outputs are the destinations used for sending notifications. For ESA, notification outputs enable you to define how you want to receive the ESA alerts. The following are the different notification outputs supported by NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

Email notification settings define the destination email address to which you can send the alerts. You can also add a custom description in the subject of the email and define multiple destination email addresses.

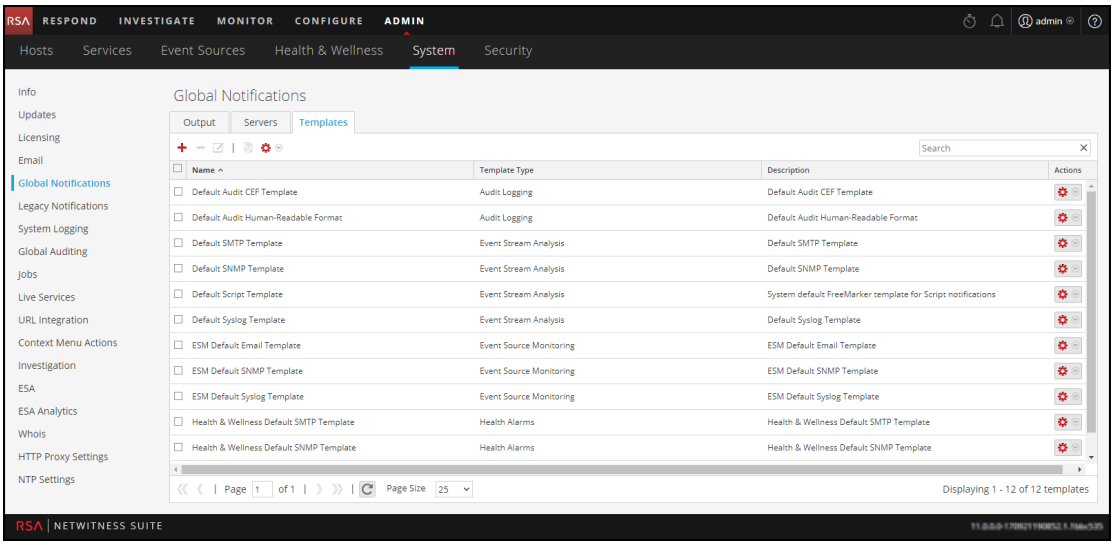
SNMP notification settings enable you to define the SNMP settings to send alert notifications. Syslog notifications enable you to define the Syslog settings used to send alert notifications. Script notifications enable you to define the Script that executes in response to the alert.

For detailed information on the notification configurations, including parameters and descriptions, see Define Notification Server Dialogs.

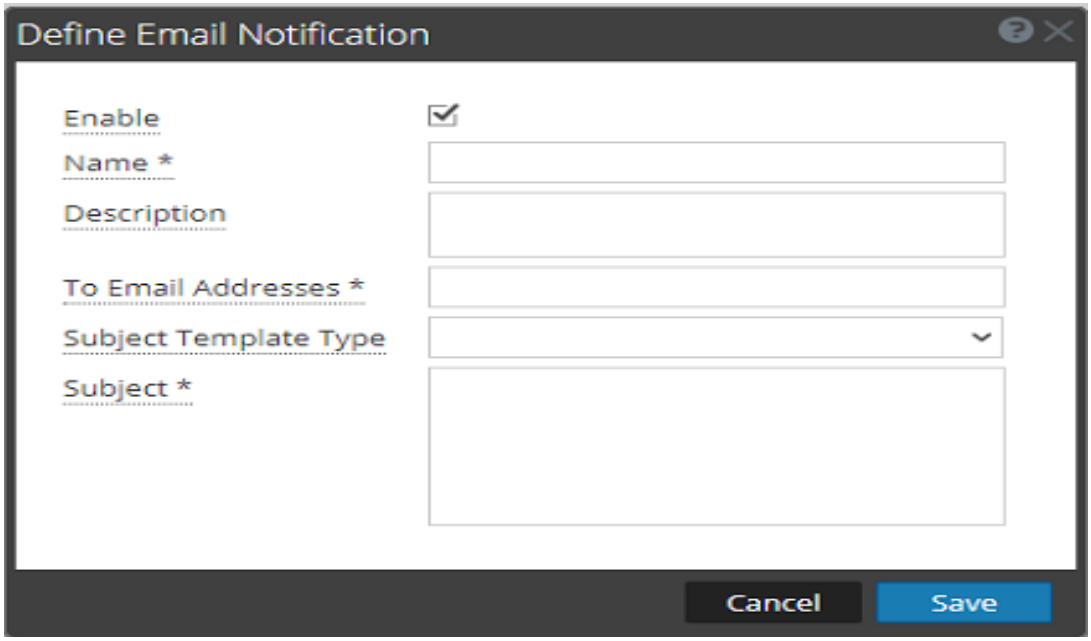
Configure Email as a Notification

To configure Email as a notification:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.



3. On the **Output** tab, from the + drop-down menu, select **Email**.



4. In the **Define Email Notification** dialog, provide the required information and click **Save**.

For details of the parameters and descriptions, see Define Notification Server Dialogs.

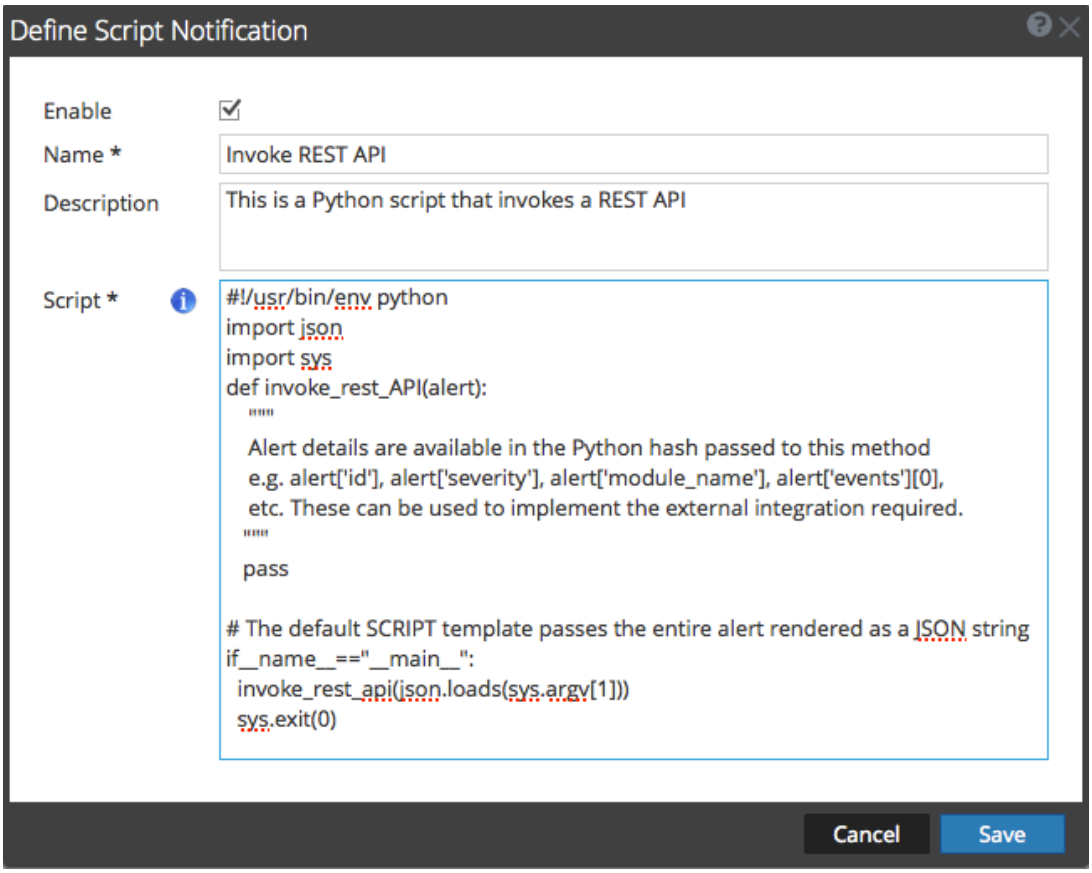
Configure Script as a Notification

This topic provides instructions to define the Script and configure it as a notification output. ESA allows you to run scripts in response to ESA alerts. You need to define the script using the ADMIN > System > Notifications > Output tab. You can use any script for ESA notifications.

To configure the script as a notification:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. On the Output tab, from the + drop-down menu, select **Script**.



4. In the **Define Script Notification** dialog, provide the required information and click **Save**.

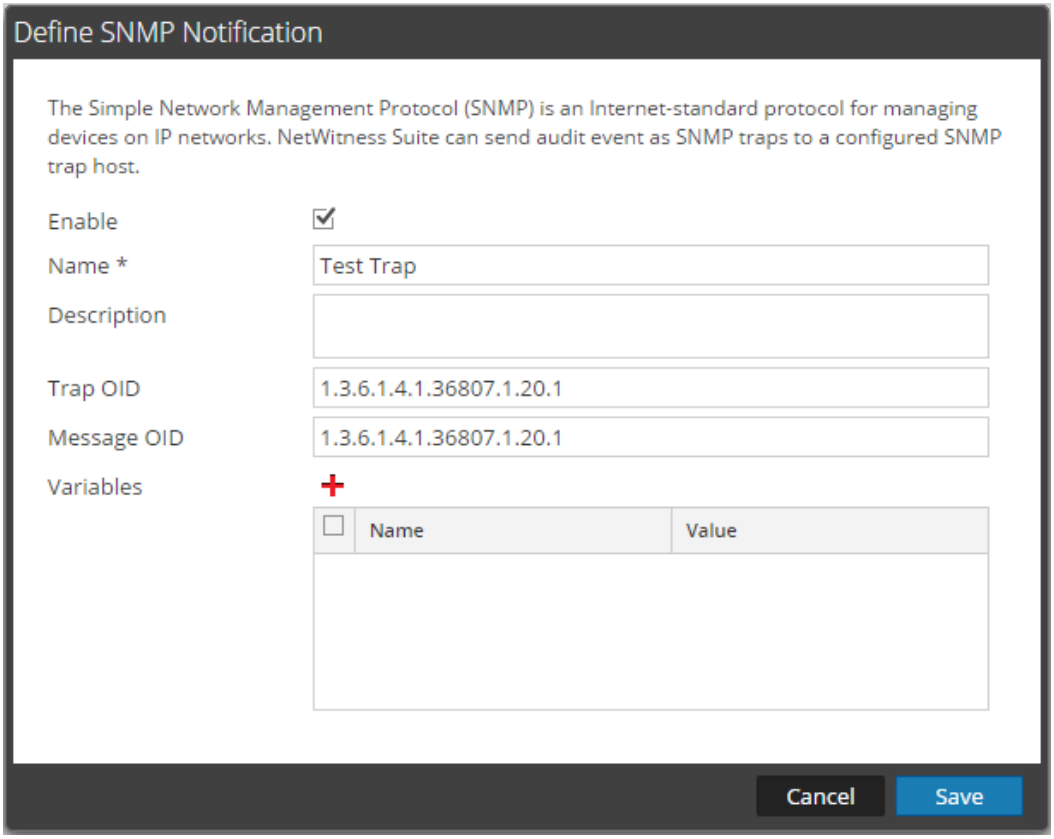
For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure SNMP as a Notification

To configure SNMP as a notification output to send alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. On the Output tab, from the + drop-down menu, select **SNMP**.



4. In the SNMP Notification dialog, provide the required information and click **Save**.

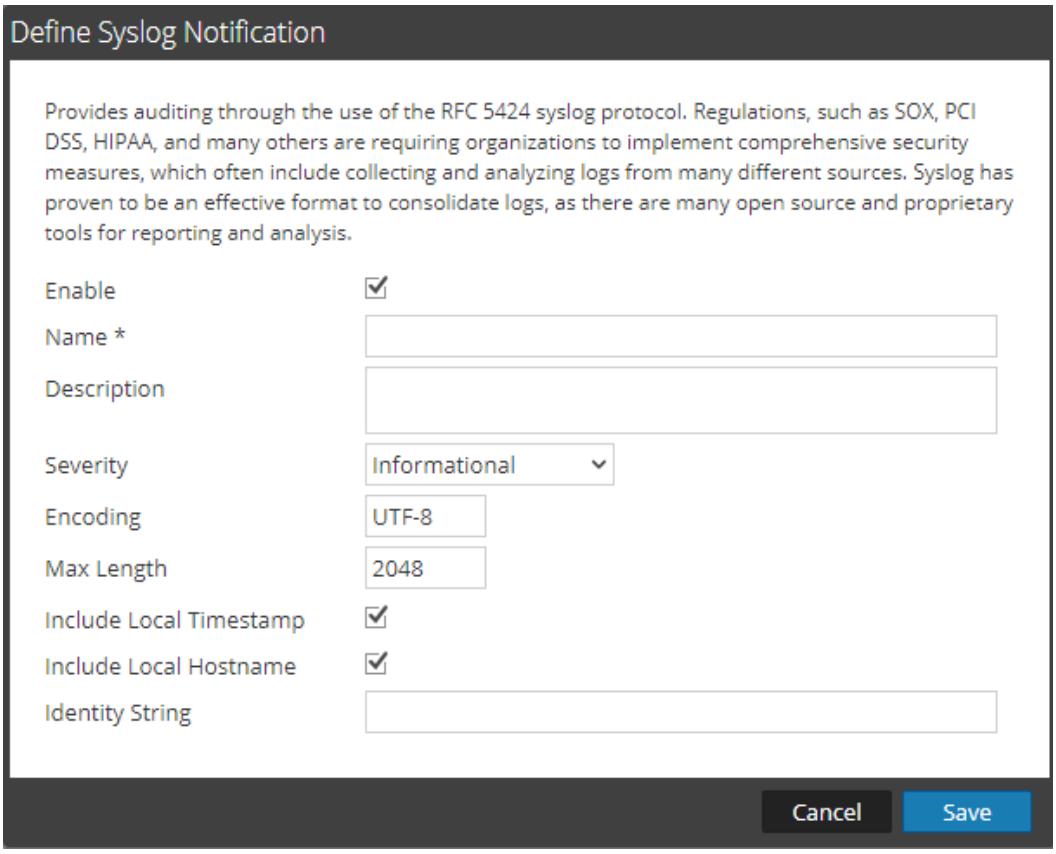
For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure Syslog as a Notification

To configure Syslog as a notification output when sending alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. On the Output tab, from the + drop-down menu, select **Syslog**.



4. In the **Define Syslog Notification** dialog, provide the required information and click **Save**.

For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure Templates for Notifications

You configure notification templates in the Administration System view (ADMIN > System > Notifications > Templates tab). A notification template defines the format and message fields of the notifications. There are different template types for the notifications that you can configure:

- Audit Logging
- Event Stream Analysis
- Event Source Monitoring
- Health Alarms

You can use the available default templates or you can configure your own templates for Email, SNMP, Syslog, and Script, depending on the template type.

Global audit logging sends audit logs in the format specified in the Audit Logging template. You can use the default audit logging templates or you can define your own audit logging template. For more information on how to define an Audit Logging template, see Define a Template for Global Audit Logging.

Event Stream Analysis (ESA) sends notifications in the format specified in the Event Stream Analysis templates. The default Event Stream Analysis templates for email, SNMP, Syslog, and Script are available on installation. You can customize these templates as well as create new templates which you can use for the notifications. For more information on how to define ESA templates, see Define a Template for ESA Alert Notifications.

For more information on ESA alert configuration, see "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide*. You cannot delete templates associated with global audit log configurations.

Note: When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

To learn how to define, delete, edit, duplicate, import, and export a notification template in NetWitness Suite, see:

Configure Global Notifications Templates

Define a Template for ESA Alert Notifications

Import and Export a Global Notifications Template

Configure Global Notifications Templates

This topic provides instructions for adding, editing, duplicating, and deleting global notifications templates.

You can use the available default templates or you can configure your own templates for Email, SNMP, Syslog, and Script, depending on the template type.

Global audit logging sends audit logs in the format specified in the Audit Logging template. You can use the default audit logging templates or you can define your own audit logging template. For more information on how to define an Audit Logging template, see "Define a Template for Global Audit Logging."

Event Stream Analysis (ESA) sends notifications in the format specified in the Event Stream Analysis templates. The default Event Stream Analysis templates for email, SNMP, Syslog, and Script are available on installation. You can customize these templates as well as create new templates which you can use for the notifications. For more information on how to define ESA templates, see Define a Template for ESA Alert Notifications.

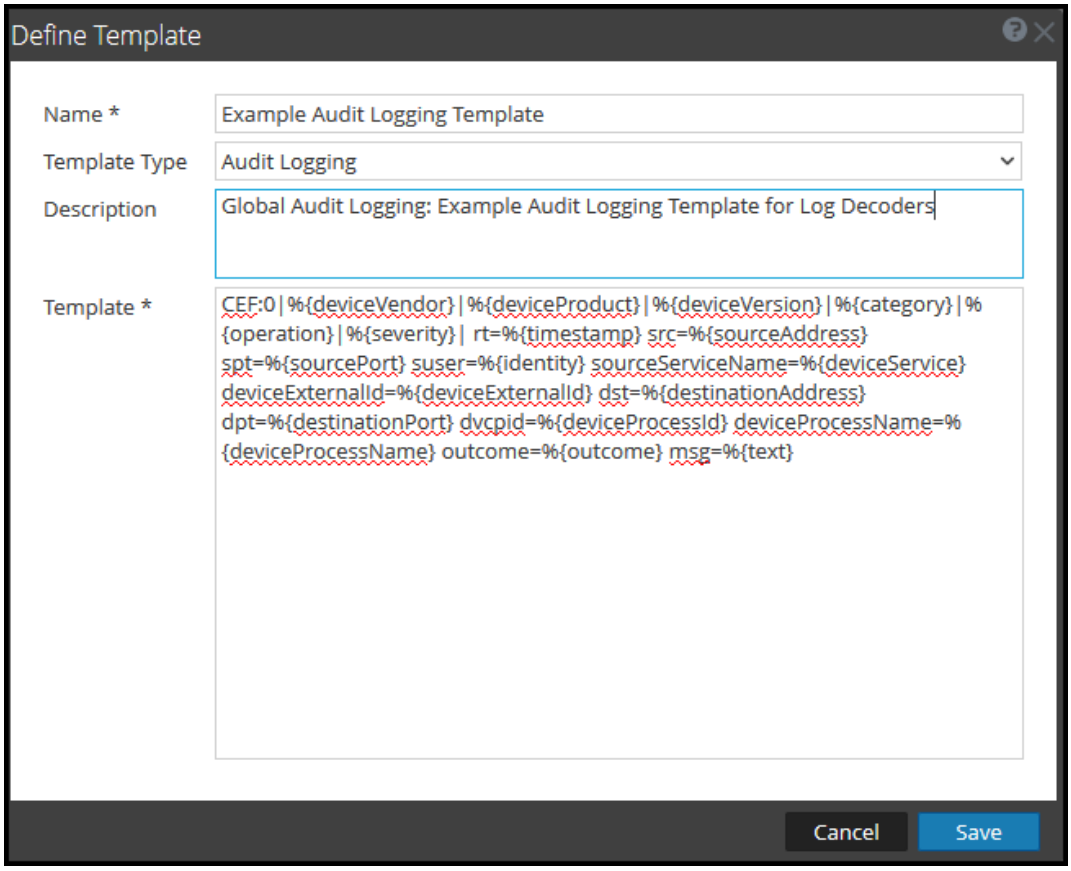
When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

Add a Template

You can use the default templates provided or you can configure your own templates. To configure your own template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Click + to configure a template.
5. In the **Define Template** dialog, provide the following information:
    a. In the **Name** field, type the name for the template.
    b. In the **Template Type** field, select the type of template you want to create. For example, if you are creating a template for global audit logging, select the Audit Logging template type.
    c. In the **Description** field, type a brief description for the template.
    d. In the **Template** field, specify the format for the template.

e. Click **Save** to save the template.



Duplicate a Template

You can make a copy of an existing default or user-defined template. To duplicate a template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select the template that you want to duplicate and click .

   The Duplicate Alert Template dialog is displayed.

5. Type the name for the duplicate template.
6. Click **OK**.

You can modify a default or user-defined template. When you edit a template, the changes are reflected only when the alert is triggered.

Edit a Template

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select a template and click .
5. In the **Define Template** dialog, modify the **Name**, **Template Type**, **Description**, and **Template** fields as required.
6. Click **Save** to save the template.

Delete a Template

You can delete a user-defined template. When you delete a template that is used in an ESA rule, the Event Stream Analysis default template is used for alerts. You cannot delete templates associated with global audit logging configurations.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select one or more templates and click .

   A confirmation dialog is displayed.
5. Click **Yes**.

   The selected template is deleted.

Define a Template for ESA Alert Notifications

This topic describes how you can define a template for alert notifications. Event Stream Analysis (ESA) allows you to define useful templates for alerts. You need to have a good understanding of FreeMarker and the ESA data model to define a template. For more information on FreeMarker, see FreeMarker Template Author's Guide.

ESA Data Model

Consider an ESA alert rule as shown below:

```
@Name('module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert')
@Description('Brute Force Login To Same Destination')
@RSAAlert(oneInSeconds=0, identifiers={"ip_dst"})
SELECT* FROMEvent (ec_activity = 'Logon',ec_theme = 'Authentication',ec
outcome = 'Failure',ip_dst IS NOT NULL)
.std:groupwin(ip_dst)
.win:time_length_batch(60 seconds, 2)
GROUPBYip_dst HAVING COUNT(*) = 2;
```

When a rule like the above is fired, the alert generated will have two constituent events each resembling a NextGen session with multiple meta values. The alert data-object passed to the FreeMarker template evaluator will be as follows:

```
(root)
 |
 +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79"              // Unique identifier for each alert
 |
 +- severity = 1                                  // The severity of the alert
 +- time = 2013-12-31T11:02Z                          // The alert time (needs a ?datetime for proper rendering)
 | +- moduleType = "ootb"                           // The module type
 |
 +- moduleName = "Brute Force Login To Same Destination"        // A description of the module
 |
 +- statement = "module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert" // The name of the EPL statement
 | +- events                                        // The constituent events - as a sequence of event maps
    |  +- [0]                                     // offset 0 (i.e. the first constituent event)
    | |    | |
    |  +- event_cat_name = "User.Activity.Failed Logins"
    |  +- device_class = "Firewall"                    // event meta (accessible as ${events[0].device_class}$)
    | |    |  +- event_source_id = "uttam:50002:1703395"   // Investigation URI to the individual session (used by SA)
    | |
    |  +- ...                                    // Other meta
    | |
    |  +- sessionid = 1703395                          // NextGen sessionid
    | |
    |  +- time = 1388487764                           // event/session time at NextGen source (as a long Unix timestamp)
    | |
    |  +- user_dst = "user5"
    |
    +- [1]                                      // offset 1 (i.e. the second consituent event)
       |
       +- device_class = "Firewall"
       |
       +- event_cat_name = "User.Activity.Failed Logins"
       |
       +- event_source_id = "uttam:50002:1703405"
       |
       +- ...
       |
       +- sessionid = 1703405
       |
       +- time = 1388487766
       |
       +- user_dst = "user5"
```

There are two types of template variables available in the data model:

- **Alert Meta Data:** These hold alert level details like statement name, module name, alert id, alert time, severity, and others. In FreeMarker terminology, these are top level variables associated with the alert instance itself and can be referenced simply by their names like `${moduleName}`. The `time` meta is special because it is of type `Date` and it needs to be suffixed with a `?datetime` to be properly rendered.

- **Constituent Event Meta Data**: These include the session meta fields from individual events that constitute the alert. An alert can have multiple constituent events, so there can be more than one such maps in the same alert. These show up as a sequence of hashes to the FreeMarker template evaluator and must be referenced. For instance, the alert has two constituent events the event_source_id for the first is available as `${events[0].event_source_id}` and the same for the second is accessible as ${events[1].event_source_id.} You also need to be aware of which meta fields are multi-valued because those need be treated as sequences, for example ${events[0].alias_host} will not work because it is a sequence.

Note: The metadata available in the constituent events for a given alert is determined by the EPL SELECT clause. For example, alerts from `SELECT sessionid, time FROM ...` will have only two meta values available (sessionid, time). Constituent events in `SELECT * FROM Event ...` will carry all meta fields from the `Event` type with **non-null** values.

If your template uses meta keys that are not present in all alert output, you should consider using the FreeMarker provisions for default values.

For example, if a template with text Id=${id},ec_outcome=${ec_outcome} is evaluated for an alert which does not include the meta key `ec_outcome` then the template evaluation fails. In such cases, you can use the missing value placeholder `${ec_outcome!"default"}`.

Import and Export a Global Notifications Template

This topic provides instructions on how to import and export a template for notifications.

- You can export default or user-defined templates.
- You can import a template that has been exported from the NetWitness Suite instance. If you import a template with the same name as an existing template, then the existing template will be overwritten.

Import a Template

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Templates** tab.
4. In the toolbar, select **> Import**.

   The **Import** dialog is displayed.
5. In the **Enter File Name** field, type the filename or click **Browse** and select the file to be imported.
6. Click **Import**.

Export a Template

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select the template you want to export.

   Note: You can export all the templates using the **> Export All** option.
5. In the **Actions** column, select **> Export**.

   The **Export** dialog is displayed.
6. In the **Enter File Name** field, type the filename.
7. Click **Save**.

Configure Email Servers and Notification Accounts

This topic provides instructions for configuring email so that users can receive notifications in NetWitness Suite. RSA NetWitness® Suite can send notifications to users via email about various system events. To be able to configure these email notifications, you must first configure the SMTP email server. The Email Configuration panel provides a way to:

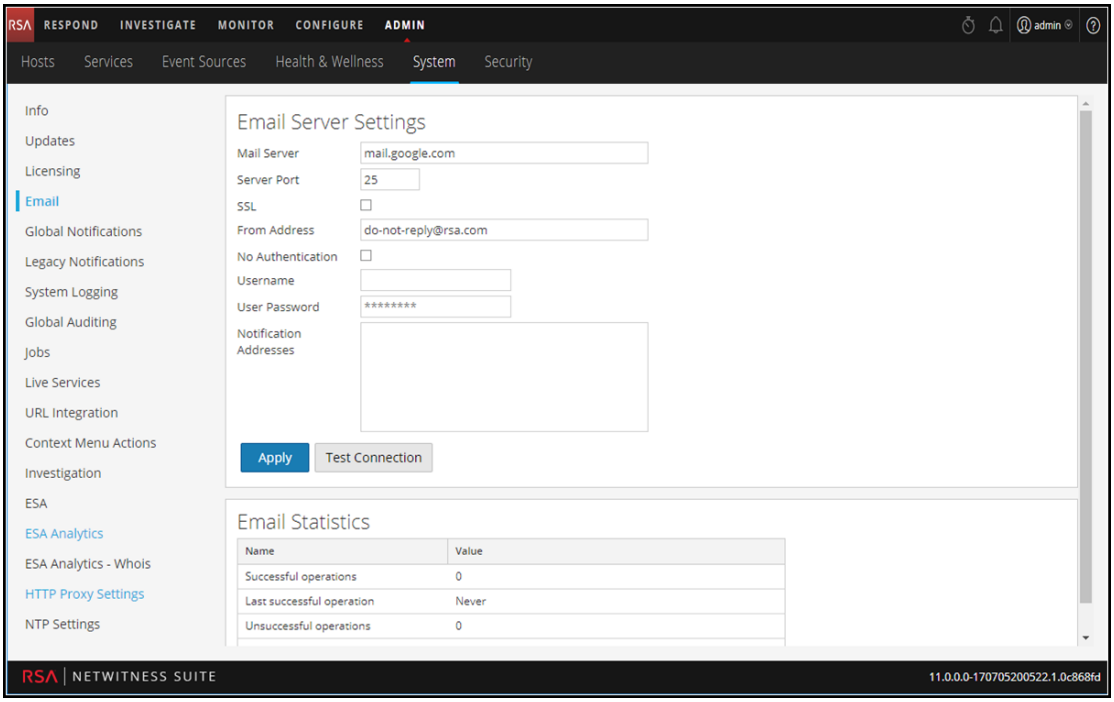
- Configure the email server.
- Set up an email account to receive notifications.
- View statistics on email operations.

NetWitness Suite requires access to an SMTP mail server in order to send reports to users. Each user account can be configured to receive emailed reports. These reports can be generated manually, through the user interface, or automatically, through the auditing system. The following guidelines apply:

- Any SMTP mail host can be used to deliver emails, and each host requires a different configuration. The SMTP provider provides the settings for configuration.
- Some SMTP servers require user authentication in order to relay emails successfully. Typically, this is the login and password for the email account.
- Best practice is to create a new, dedicated email account on the SMTP email server for NetWitness Suite reports.

To configure NetWitness Suite email notifications:

1. Go to **ADMIN > System**.
   The Administration System view is displayed.
2. In options panel, select **Email**.



3. If you want to change the default mail server, specify the **Mail server** name and **Server port**.
4. If the email server communicates with NetWitness Suite using SSL, check the box next to **Use SSL**.
5. In the **From address** field, type the name of the email account sending NetWitness Suite email notifications.
6. If the SMTP server requires user authentication to relay emails successfully, type the **Username** and **User Password** for logging in to the email account.

7. To activate the settings, click **Apply**.

   You can now configure NetWitness Suite modules to receive various notifications by email.

Configure Global Audit Logging

Global Audit Logging provides NetWitness Suite Auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location. This visibility includes audit logs gathered from the NetWitness Suite system and the different services throughout the NetWitness Suite infrastructure.

NetWitness Suite audit logs collect in a centralized system that converts them into the required format and forwards them to an external syslog system. The external syslog system can be a third-party syslog server or a Log Decoder.

You configure global audit logging in the Global Audit Logging Configurations panel. An audit logging template defines the format and message fields of the audit log entries. A Syslog Notification Server configuration defines the destination to send the audit logs. If you want to forward audit logs to a Log Decoder, configure a Syslog type of Notification Server for the Log Decoder.

The following are some of the user actions logged from NetWitness Suite:

- **User logouts**: The NetWitness Server authenticates the logout action and the action is logged in the audit logs file.

  For example:

  ```
  2018-03-13 06:47:02,911 deviceVersion: "11.1.0.0" deviceService: "SA_
  SERVER" category: AUTHENTICATION operation: "Logoff" outcome:
  "Success" identity: "admin" userRole: "Administrators"
  ```

- **All UI pages accessed**: The NetWitness Server logs system entries related to all the accessed UI pages in the audit logs file.

  For example:

  ```
  2018-03-13 07:03:51,234 deviceVersion: "11.1.0.0" deviceService: "SA_
  SERVER" category: SYSTEM operation: "Page Accessed" outcome:
  "Success" key: "[UNF] Dashboard" identity: "admin" userRole:
  "Administrators"

  2018-03-13 07:04:11,153 deviceVersion: "11.1.0.0" deviceService: "SA_
  SERVER" category: SYSTEM operation: "Page Accessed" outcome:
  "Success" key: "[INV] Navigation" identity: "admin" userRole:
  "Administrators"

  2018-03-13 07:04:11,168 deviceVersion: "11.1.0.0" deviceService: "SA_
  SERVER" category: SYSTEM operation: "Page Accessed" outcome:
  "Success" key: "[INV] &amp;quot;NWAPPLIANCE26785 - Broker&amp;quot;
  ```

```
Navigation" identity: "admin" userRole: "Administrators"

2018-03-13 07:04:38,275 deviceVersion: "11.1.0.0" deviceService: "SA_
SERVER" category: SYSTEM operation: "Page Accessed" outcome:
"Success" key: "[INV] Malware Analysis" identity: "admin" userRole:
"Administrators"

2018-03-13 07:04:39,745 deviceVersion: "11.1.0.0" deviceService: "SA_
SERVER" category: DATA_ACCESS operation: "HttpRequest" parameters: "
{referrer=https://10.31.125.48/investigation/malware, method=GET,
userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146
Safari/537.36, queryString=_dc=1520924725291&page=1&start=0&limit=20,
uri=/jobs/jobs, remoteAddress=0:0:0:0:0:0:0:1}" outcome: "Success"
identity: "admin" userRole: "Administrators"
```

- **Committed configuration changes**: The NetWitness Server manages all the configuration changes (including when a user changes their own password) and logs its findings into the audit logs file.
  For example:

```
2018-03-13 08:35:58,094 API{action=/rsa/process/ready, success=true,
identity=admin(unauthenticated), parameters={Arguments=[]}}

2018-03-13 08:36:08,978 DataAccess{action=update, success=true,
identity=admin, parameters={Account=admin}}

2018-03-13 08:36:08,978 API{action=/rsa/security/account/set,
success=true, identity=admin, parameters={Arguments=[Account
(id=admin)]}}
```

- **Queries performed by the user**: The NetWitness Server logs all queries performed by the user in the audit logs file.
  For example:

```
2018-03-13 08:49:17,321 deviceVersion: "11.1.0.0" deviceService: "SA_
SERVER" category: DATA_ACCESS operation: "query" parameters:
"NativeValuesMessage{ deviceId=12, isAppliancePath=false,
timeout=null, collectionName=\'\', appliancePath=false,
sdkPath=\'/sdk\',
callbackChannel=\'/meta/values/12/1520931000851/threat.source;collect
ionName=\',returnValues=false, fieldName=\'threat.source\',
```

```
fieldIdRange=FieldIdRange [ beginId=1, endId=11458684062 ],
threshold=100000, size=20, flags=6401, where=\'time=\"2036-09-22
17:20:00\"-\"2036-09-24 17:19:59\"\', options=InvestigationOptions
{options={date_range=null, total_by=SESSION_COUNT, order_by=TOTAL,
time_range_type=LAST_2_DAYS, sort_order=DESCENDING}, dateRange=null,
orderBy=TOTAL, sortOrder=DESCENDING, timeRangeType=LAST_2_DAYS,
totalBy=SESSION_COUNT}, metaAliases={}, aggregateFunction=\'null\',
aggregateFieldName=\'null\', min=null, max=null}" outcome: "Success"
identity: "admin" userRole: "Administrators"

2018-03-13 08:49:16,909 deviceVersion: "11.1.0.0" deviceService: "SA_
SERVER" category: DATA_ACCESS operation: "HttpRequest" parameters: "
{referrer=https://10.31.125.48/investigation/12/navigate/values,
method=POST, userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146
Safari/537.36, queryString=, uri=/investigation/navigate/meta/load,
remoteAddress=127.0.0.1}" outcome: "Success" identity: "admin"
userRole: "Administrators"
```

- **Data export operations**: The NetWitness Server allows data export operations to be performed and the actions are logged in the audit logs file.
  For example:

```
2018-03-13 08:51:11,004 deviceVersion: "11.1.0.0" deviceService: "SA_
SERVER" category: DATA_ACCESS operation: "Events" outcome: "Success"
value: "ModelAndView: reference to view with name
\'investigation/events/events\'; model is
{i18n=com.rsa.netwitness.carlos.i18n.handler.MessageHandler@431e3472,
globalI18n=com.rsa.netwitness.carlos.i18n.handler.MessageHandler@470b
7db7, timeZone=UTC,
userTimeZone=com.netwitness.platform.server.common.timezone.UserTimeZ
one@6e686ad, browserTimeZoneOffset=0, observesDaylightTime=false,
defaultInvestigateUrl=/investigation/navigate, pageTitle=[INV]
\"NWAPPLIANCE1519 - Concentrator\" Event List, titlePrefix=,
deviceName=NWAPPLIANCE1519 - Concentrator, deviceVersion=11.1.0.0-0,
defaultDevice=12, renderAs=AUTO, activeTab=tab-events, deviceId=34,
endpointId=13ae57e4-2045-46c2-a7a2-42cb17a160f1, collectionName=null,
lastCollectionTime=2105889599999, startCollectionTime=1223917560000,
predicateIds=54, eventsPageForSpeed=true, eventSearchMeta=true,
eventSearchPackets=true, eventSearchCaseInsensitive=true,
eventSearchRegex=false, eventSearchIndexes=true,
```

```
eventsAppendInStore=false, allowFullPacketReconstruction=false,
eventSearchLimit=1000000, eventSearchResultLimit=5000,
exportLogFormat=null, exportMetaFormat=, sessionViewType=LOG_VIEW,
mid1=1, mid2=37258283, timeRange=TimeRange [ beginTime={2008-10-
13T17:06:00 UTC}, endTime={2036-09-24T17:19:59 UTC} ],
timeRangeType=ALL_DATA, responseEndpointId=80b6a199-d74c-45cf-a61b-
2568800cf80d, responseOnline=true}" identity: "admin" userRole:
"Administrators"
```

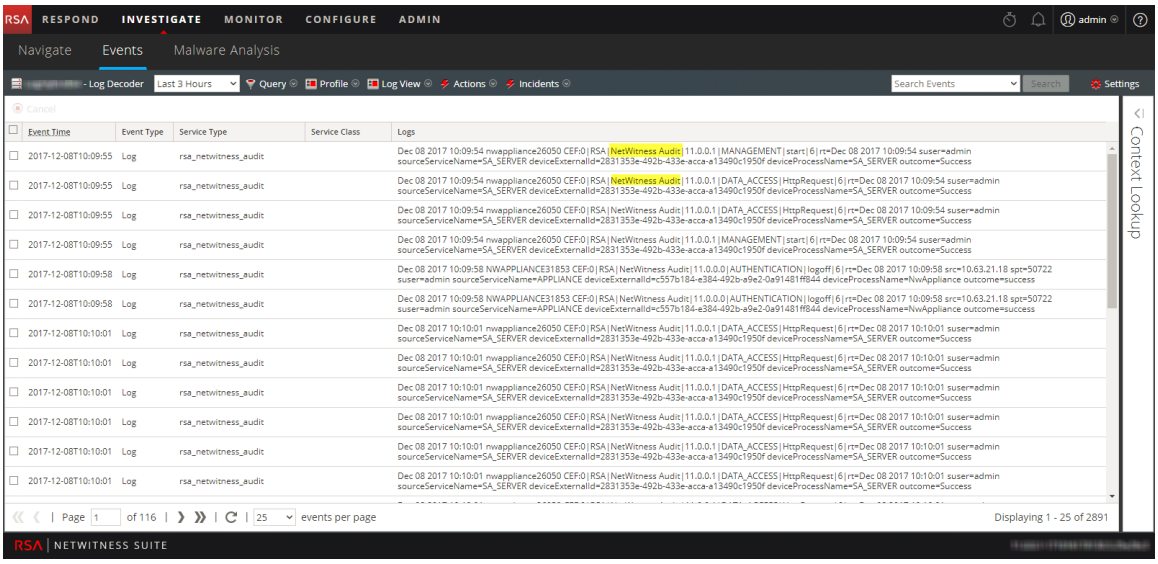
After you create a global audit logging configuration, audit logs containing these user actions automatically go to the external syslog system in the format specified in the selected Audit Logging template. You can create multiple global audit logging configurations for different destinations that use different templates. For example, you can create a global audit logging configuration for an external Syslog server with a template that contains all of the available meta keys and another configuration for a Log Decoder with a template that contains selected meta keys.

For Log Decoders, you use the Default Audit CEF Template. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. Define a Template for Global Audit Logging provides instructions and Supported CEF Meta Keys describes the CEF meta keys available to use in the audit logging templates.

For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). Define a Template for Global Audit Logging provides instructions and Supported Global Audit Logging Meta Key Variables describes the available variables.

Auditors can view the audit logs on the selected Log Decoder or third-party syslog server. If using a Log Decoder, auditors can view the audit logs using NetWitness Suite Investigations or Reports.

The following figure shows global audit logs in Investigation (INVESTIGATE > Events).



For examples of some of the user actions logged, see Add New Configuration Dialog. For a list of message types being logged by the various NetWitness Suite components, see Global Audit Logging Operation Reference.

Global Audit Logging - High-Level Procedure

Global Audit Logging is configured in the Global Audit Logging Configurations panel, which is accessed from ADMIN > System view > Global Auditing. Before you can configure Global Audit Logging, you need to configure a Syslog Notification Server and an Audit Logging template. A Syslog Notification Server defines the destination to send the audit logs. An Audit Logging template defines the format and message fields of the audit log entry.

The Global Audit Logging Configuration panel provides a **view settings** link that takes you to the Global Notifications panel (ADMIN > System view > Global Notifications) where you can configure the Syslog Notification Server and Audit Logging template.

Perform the following procedures in the order shown to configure Global Audit Logging.

Procedures	Reference / Instructions
1. Configure a Syslog Notification Server.	Configure a Syslog Notification Server to use for Global Audit Logging. You can define a third-party syslog server or Log Decoder as a destination to receive the audit logs. Configure a Destination to Receive Global Audit Logs. Global Audit Logging configurations use the Syslog notification server type. If you want to forward audit logs to a Log Decoder, create a Notification Server of the Syslog type.

Procedures	Reference / Instructions
2. Select or configure an Audit Logging template to use.	Select an Audit Logging template for the Syslog notification server. You can use a default Audit Logging template or define your own audit logging template. Global Audit Logging configurations use the Audit Logging template type and a Syslog notification server. Configure Templates for Notifications provides additional information. For Log Decoders, use the **Default Audit CEF Template**. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. Define a Template for Global Audit Logging provides instructions. For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). Define a Template for Global Audit Logging provides instructions and Supported Global Audit Logging Meta Key Variables describes the available variables.
3. (Optional - Only if consuming with a Log Decoder) Deploy the Common Event Format parser to your Log Decoder from Live.	Ensure that you have deployed and enabled the latest Common Event Format parser from Live. Find and Deploy Live Resources and Enable and Disable Log Parsers provide instructions.
4. Define a global audit logging configuration, which defines how the global audit logs are forwarded to external Syslog systems.	Define a Global Audit Logging Configuration provides instructions. After you add a Global Audit Logging configuration, audit logs are forwarded to the selected Notification Server in the configuration.

Procedures	Reference / Instructions
5. Verify that the global audit logs show the audit events.	Test your audit logs to ensure that they show the audit events as defined in your audit logging template. Verify Global Audit Logs provides instructions.

Configure a Destination to Receive Global Audit Logs

In Global Audit Logging, Syslog Notification Servers are the configurations that define the destinations to receive global audit logs. You need to configure a Syslog Notification Server to use Global Audit Logging. You can define a third-party syslog server or a Log Decoder as the destination to receive the audit logs.

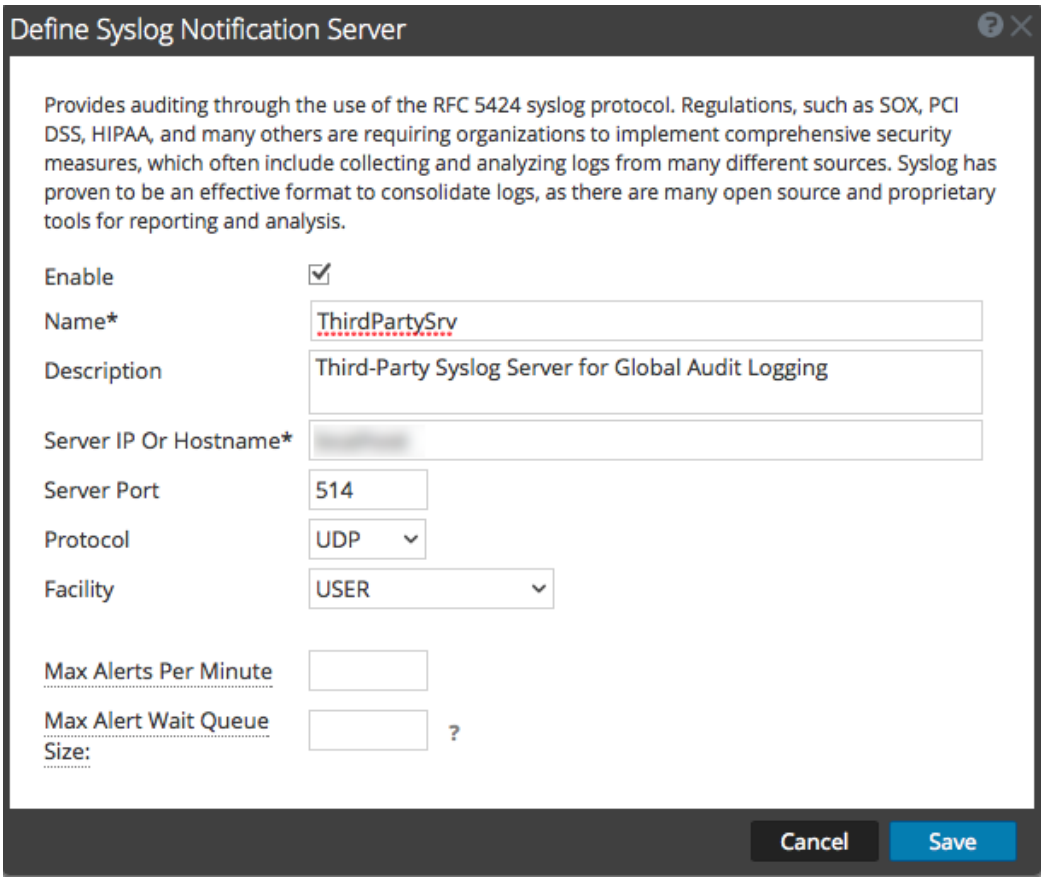
Configure a Syslog Notification Server for a Third-Party Syslog Server

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

   Note: You do not need to configure the Output tab for Global Audit Logging.

4. From the drop-down menu, select **Syslog**.

   The **Define Syslog Notification Server** dialog is displayed.



5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the third-party syslog server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The third-party syslog server hostname or IP address.
Server Port	The port number where the target syslog process is listening.
Protocol	The protocol to be used for transferring formatted audit logs to the third-party syslog server.
Facility	The syslog facility to be used for writing formatted audit logs to the third-party syslog server.

The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

6. Click **Save**.

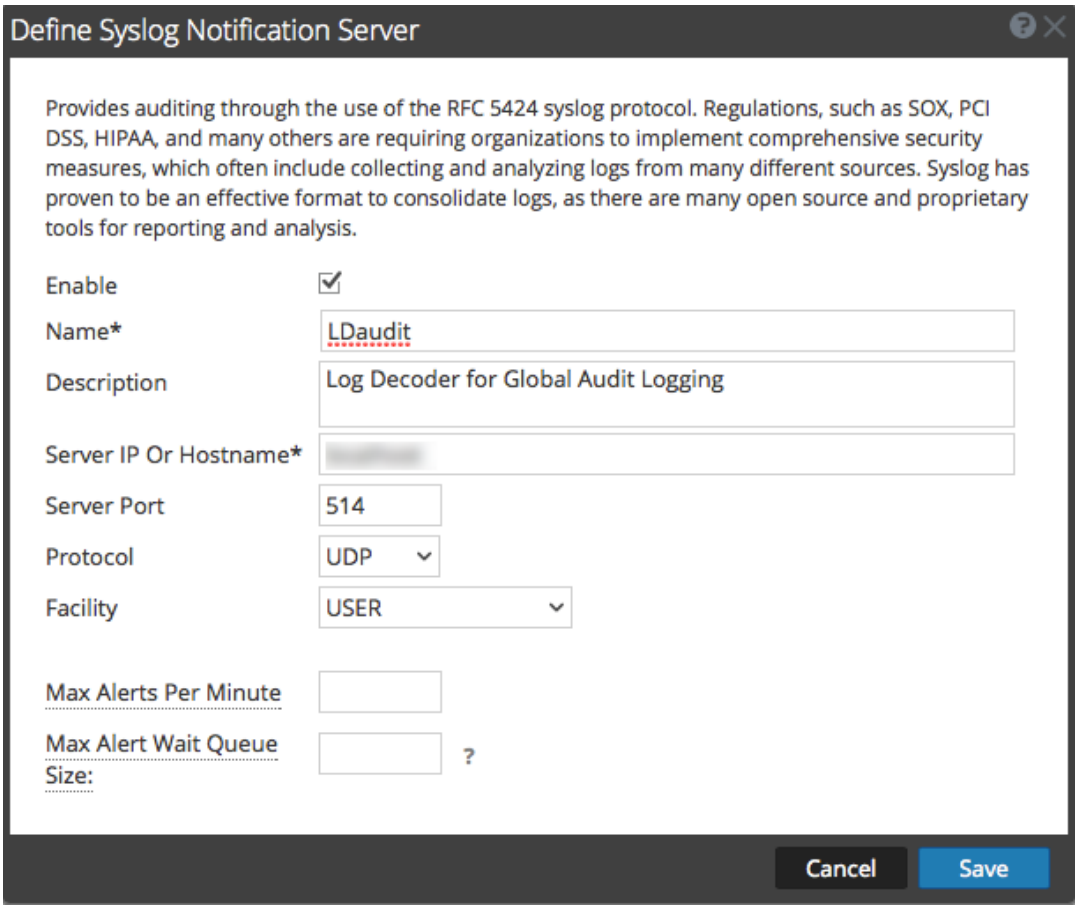
Configure a Syslog Notification Server for a Log Decoder

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

   Note: You do not need to configure the Output tab for Global Audit Logging.

4. From the drop-down menu, select **Syslog**.

   The **Define Syslog Notification Server** dialog is displayed.



5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the Log Decoder syslog notification server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The Log Decoder hostname or IP address.
Server Port	The port number where the target syslog process is listening.
Protocol	The protocol to be used for transferring formatted audit logs to the Log Decoder.
Facility	The Syslog facility to be used for writing formatted audit logs to the Log Decoder.

The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

6. Click **Save**.

Next Steps

Select a default Audit Logging template to use for Global Audit Logging. If necessary, you can define your own custom template. Define a Template for Global Audit Logging provides additional information.

Define a Template for Global Audit Logging

This topic provides instructions on how to define an audit logging template to use for Global Audit Logging. Before you configure Global Audit Logging, configure a Syslog notification server and select an Audit Logging template. You can choose to use a default audit logging template or you can define your own template.

NetWitness Suite includes two default audit logging templates:

- **Default Audit CEF Template**: You can use this template for Log Decoders and third-party syslog servers.
- **Default Audit Human-Readable Format**: You can use this template only for third-party syslog servers. Do not forward messages from this template to a Log Decoder.

The first procedure provides instructions on how to define an audit logging template for a Log Decoder. The audit logging template defines the format and message fields of the audit logs sent to the Log Decoder or third-party syslog server.

Global audit logging templates that you define for a Log Decoder use Common Event Format (CEF) and must meet the following specific standard requirements:

- Include the CEF headers in the template.
- Use only the extensions (Key=Value) listed in the Supported CEF Meta Keys table.
- Ensure that the extensions are in the `key=%{string}<space>key=%{string}` format.

The second procedure provides instructions on how to define a custom global audit logging template in human-readable format for a third-party syslog server. For third-party syslog servers, you can define your own format (CEF or non-CEF).

Define a Global Audit Logging Template for a Log Decoder

You can use the **Default Audit CEF Template** to send global audit logs to a Log Decoder. To define your own template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Templates** tab.
4. Click + to configure a template.
5. In the **Define Template** dialog, provide the following information:
   a. In the **Name** field, type the name for the template.
   b. In the **Template Type** field, select the **Audit Logging** template type.
   c. In the **Description** field, type a brief description for the template.
   d. In the **Template** field, enter the format for the audit logging template.
   The following format is a customized template provided as an example. It differs from the default CEF template.

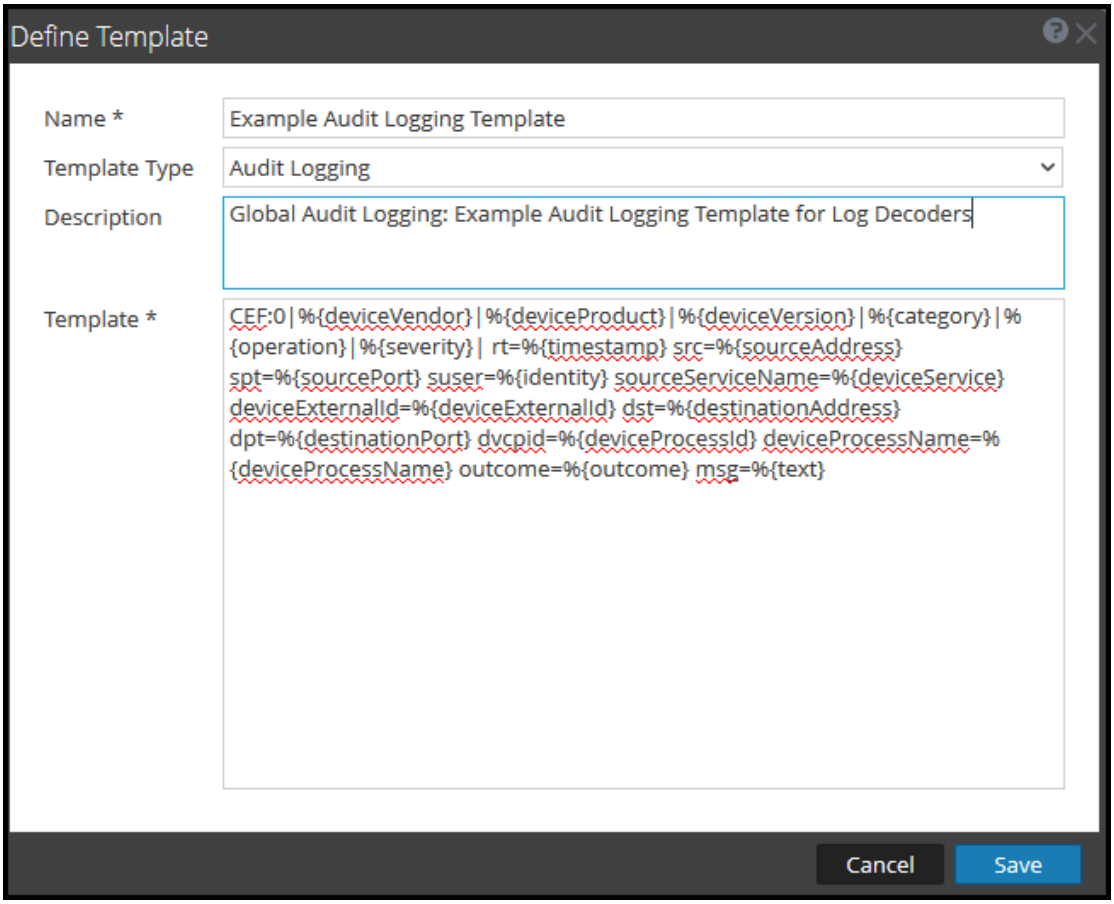
```
CEF:0|%{deviceVendor}|%{deviceProduct}|%{deviceVersion}|%{category}|%{operation}|%{severity}| rt=%{timestamp} src=%{sourceAddress} spt=%{sourcePort}
suser=%{identity} sourceServiceName=%{deviceService}
deviceExternalId=%{deviceExternalId} dst=%{destinationAddress}
dpt=%{destinationPort} dvcpid=%{deviceProcessId}
deviceProcessName=%{deviceProcessName} outcome=%{outcome} msg=%{text}
```

   The highlighed CEF syslog header is required to conform to the CEF standard and is a requirement for the CEF parser in the Log Decoder. The other keys are optional and you can configure them. See all the supported meta keys that are supported by the CEF parser in the Log Decoder in the Supported CEF Meta Keys table.

Note: Use all of the extensions in the following format:
`deviceProcessName=%{deviceProcessName} outcome=%{outcome}`
Include a `<space>` between each key=%{string} pair in the extension keys section.

Note: After you upgrade to 11.1 from earlier versions, then '$' is replaced with '%' automatically

6. Click **Save**.



After you define the CEF audit logging template, ensure that you have deployed and enabled the latest Common Event Format (CEF) parser from Live. "Find and Deploy Live Resources" in the *Live Services Management Guide* provides instructions.

Note: If you need to use a specific meta key for Investigations and Reporting, ensure that the meta keys that you select are indexed in the **table-map-custom.xml** file on the Log Decoder. If they are not indexed, follow the instructions in the "Maintain the Table Map Files" topic in the *Host and Services Configuration Guide*procedure to update the table mappings. Ensure that the meta keys are also indexed in the **index-concentrator-custom.xml** on the Concentrator. See the "Edit a Service Index File" topic in the *Host and Services Configuration Guide* for additional information.

Define a Custom Global Audit Logging Template

For third-party syslog servers, you can define your own template format (CEF or non-CEF). You can use the **Default Audit Human-Readable Format** template to send global audit logs to a third-party syslog server in a format that is easier to read than the CEF format. If you want to define your own template in human-readable format, follow this procedure.

For Log Decoders, you must use a CEF template with some specific requirements. The *Define an Audit Logging Template for a Log Decoder* procedure above provides instructions for creating a template in CEF format.

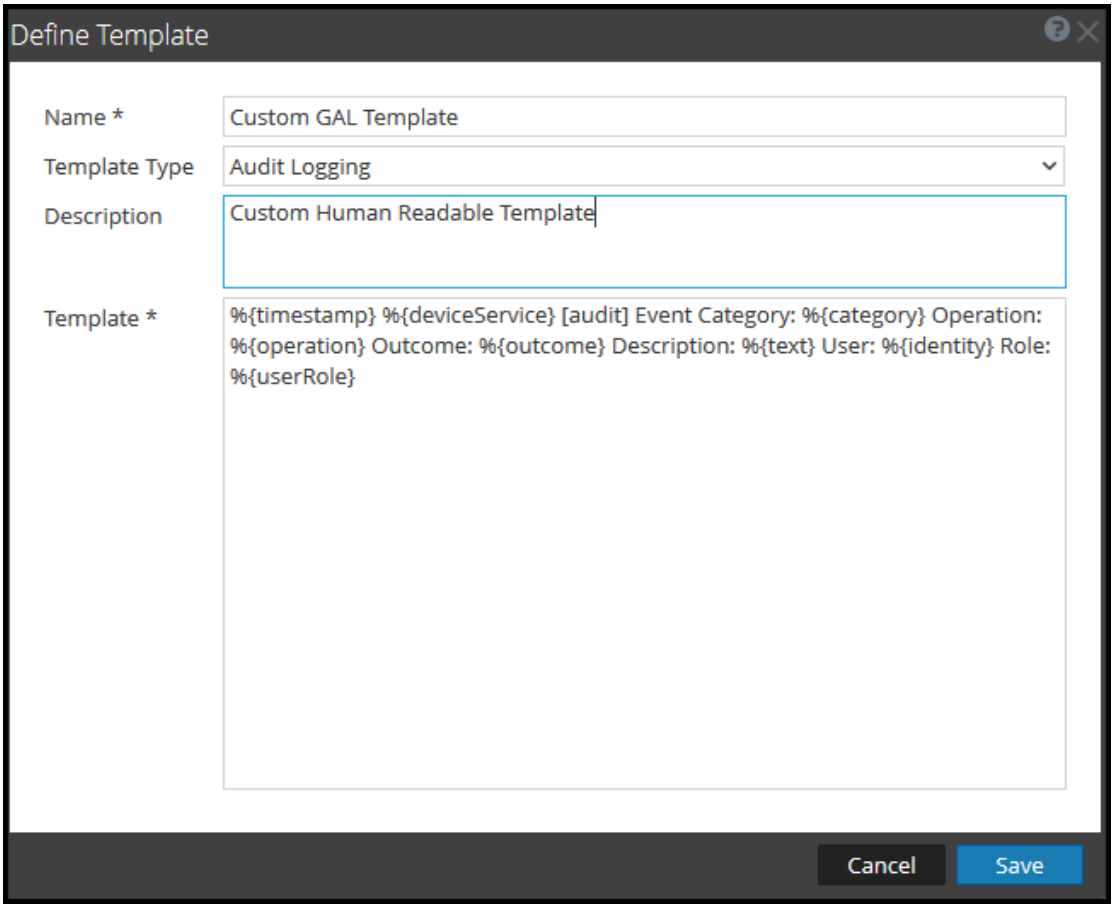
To define a custom global audit logging template in human-readable format:

1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Notifications**.
3. Click the **Templates** tab.
4. Click + to configure a template.
5. In the **Define Template** dialog, provide the following information:
   a. In the **Name** field, type the name for the template.
   b. In the **Template Type** field, select the **Audit Logging** template type.
   c. In the **Description** field, type a brief description for the template.
   d. In the **Template** field, enter the format for the audit logging template. The following example is in human-readable format with selected meta key variables.

```
%{timestamp} %{deviceService} [audit] Event Category: %{category}
Operation: %{operation} Outcome: %{outcome} Description: %{text}
User: %{identity} Role: %{userRole}
```

You can use any of the meta key variables that are supported by global audit logging shown in the Supported Global Audit Logging Meta Key Variables table.

6. Click **Save**.



The following example shows global audit logs in human-readable format for this template:

```
Apr 06 2018 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: Set Outcome: null Description: null User: admin
Role: Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2018 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2018 14:16:04 NW_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

Next Step

Define a Global Audit Logging Configuration provides instructions for defining a global audit logging configuration for NetWitness Suite.

Define a Global Audit Logging Configuration

This topic tells administrators how to define a global audit logging configuration. This procedure is required only if you choose to set up centralized audit logging in your environment. These global audit logging configurations define how the global audit logs are forwarded to external syslog systems or Log Decoders. Audit logs are forwarded to the selected Notification Servers.

Prerequisites

Before starting this procedure, configure the following to use for global audit logging:

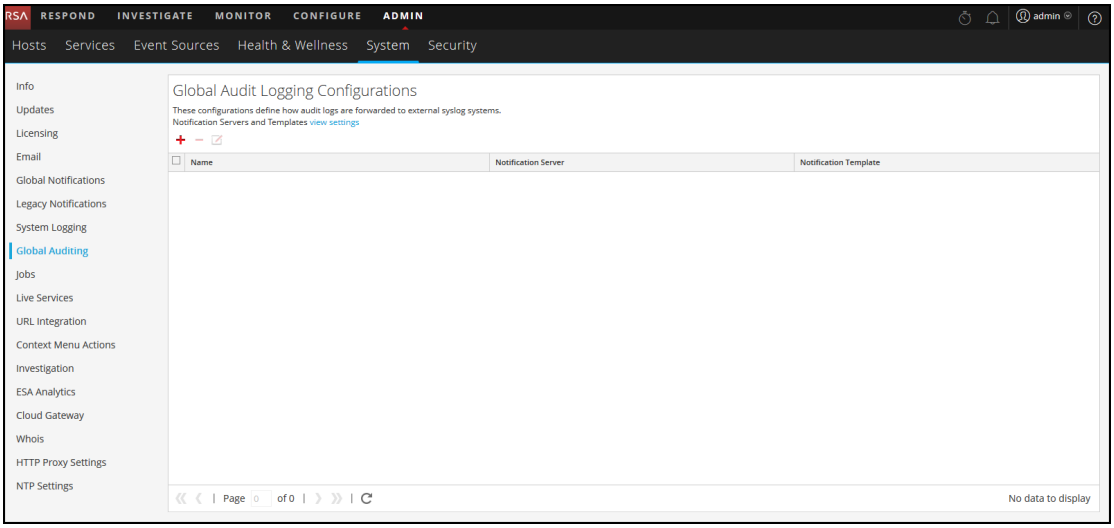
- Syslog Notification Server
- Audit Logging Template

You configure the notification server and template on the Global Notifications panel. You can access the Global Notifications panel by clicking the **view settings** link on the Global Audit Logging Configurations panel. You can only define a Syslog type of Notification Server for global audit logging. For Log Decoders, use a Syslog type of Notification Server and a Common Event Format (CEF) audit logging template. You can use a default audit logging template or define your own template. You can create multiple audit logging templates and Syslog Notification Servers to use for your global audit logging configurations.

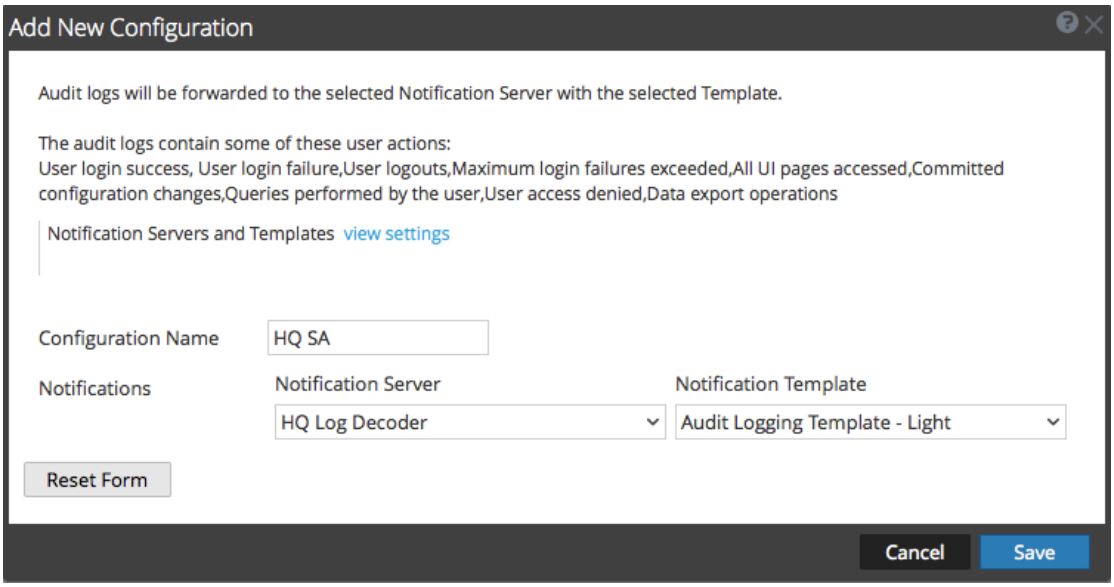
If you are forwarding global audit logs to a Log Decoder, deploy the Common Event Format parser to your Log Decoder from Live.

Add a Global Audit Logging Configuration

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Auditing**.
   The **Global Audit Logging Configurations** panel is displayed.



3. Click + to add a global audit logging configuration.
   The **Add New Configuration** dialog is displayed.



4. In the **Configuration Name** field, type a unique name for the global audit logging configuration. For example, you can create a configuration for a specific type of global audit logging configuration, such as HQ NW for a NetWitness Suite headquarters configuration.

5. In the **Notifications** section, select the syslog **Notification Server** to use for this configuration. The notification server is the destination to send the global audit logs.
6. Select the audit logging **Notification Template** to use for this configuration. The Audit Logging template defines the format and audit log message fields to be sent.
7. Click **Save**.

Add New Configuration Dialog provides additional information and examples of the user actions logged. For a list of message types being logged by the various NetWitness Suite components, see Global Audit Logging Operation Reference.

Edit a Global Audit Logging Configuration

This topic provides instructions on how to edit a global audit logging configuration. You can edit a global audit logging configuration to change the destination of the global audit logs for your user audits by selecting a different Notification Server. You can also change the format and message fields of the global audit log entries by selecting a different Notification Template. You make changes to the Notification Server or Template on the Global Notifications panel. You can access the Global Notifications panel by clicking the **view settings** link on the Global Audit Logging Configurations panel.

You cannot change which NetWitness Suite user actions are logged and sent in the global audit logs.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Auditing**.
3. In the **Global Audit Logging Configurations** panel, select a configuration to edit and click .
4. In the **Add New Configuration** dialog, modify the global audit logging configuration as required. You can modify the **Configuration Name** and select a different **NotificationServer** or **Template**.
5. Click **Save.**

Delete a Global Audit Logging Configuration

Deleting a global audit configuration does not delete the associated notification server and template. After you delete a global audit logging configuration, the forwarding of global audit logs specified in that configuration is discontinued.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Auditing**.

3. In the **Global Audit Logging Configurations** panel, select a configuration to delete and click − .

   A confirmation dialog is displayed.

4. Click **Yes**.

   The selected configuration is deleted.

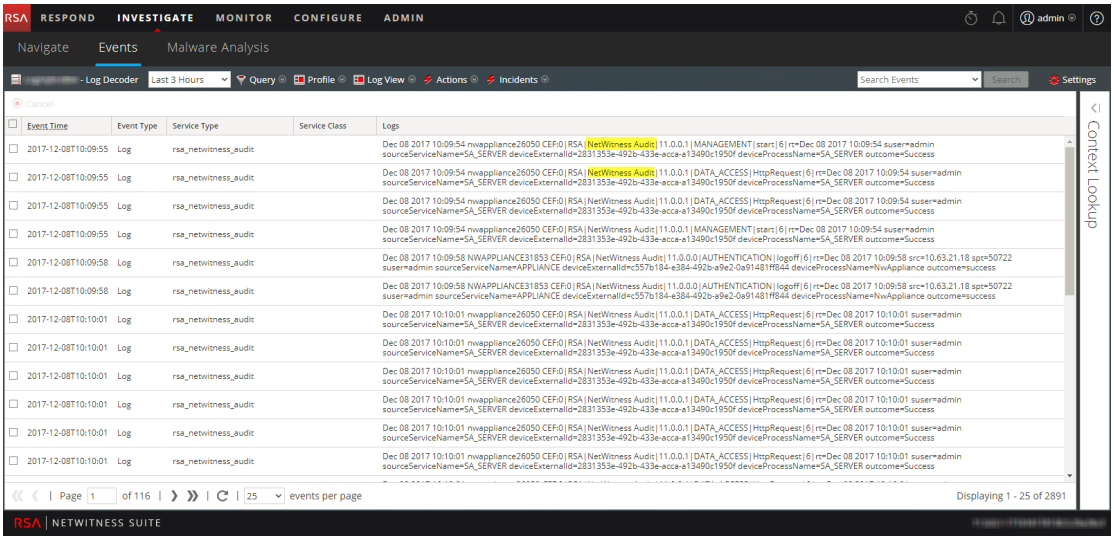
Verify Global Audit Logs

This topic provides instructions on how to verify global audit logs. After you have configured global audit logging, you need to test your global audit logs to ensure that they show the audit events as defined in your global audit logging template.

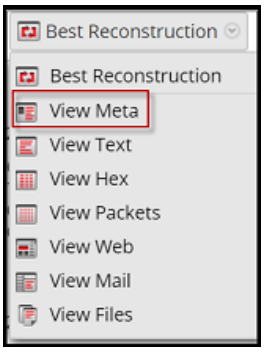
Before starting this task, complete the steps detailed in Configure Global Audit Logging.

To view and verify the global audit logs if you are using a Log Decoder:

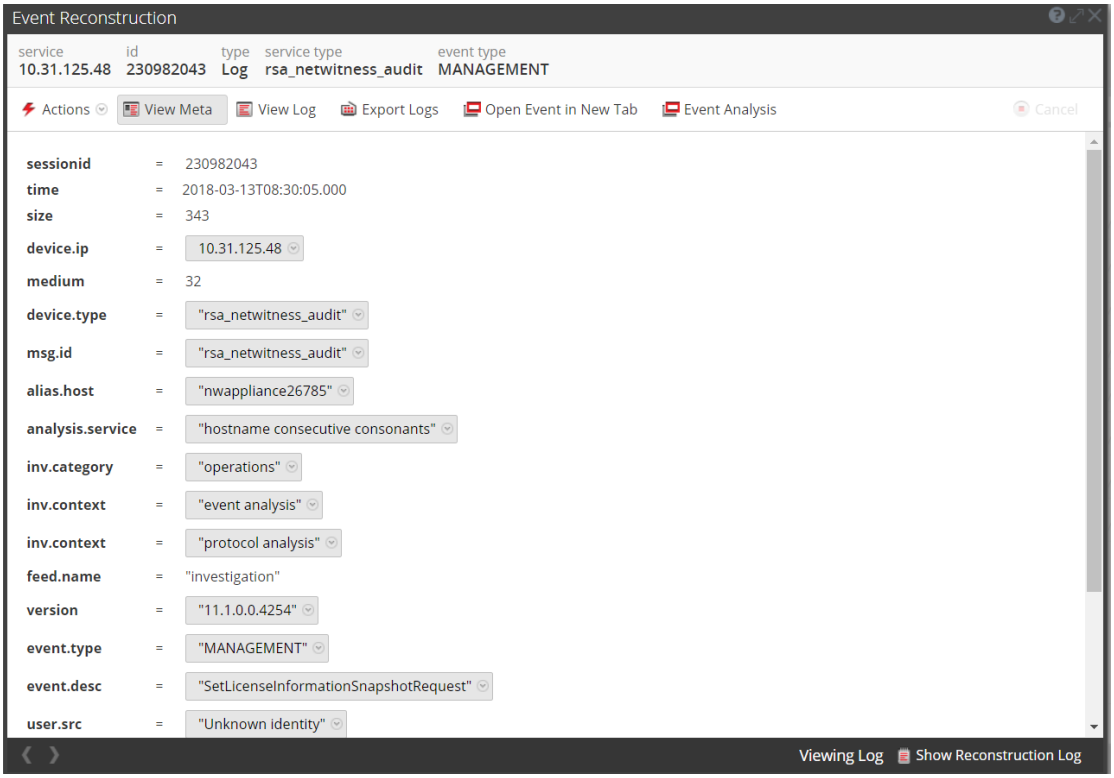
1. Go to **Investigate > Events**.
2. From within the Navigate view, select the Log Decoder, and click **Navigate**.



3. Compare the fields in the global audit logs with the fields defined in the global audit logging template that you used in your global audit logging configuration.
4. Double-click a log and in the Event Reconstruction dialog, select **View Meta**.



5. Verify that the meta that you want to audit is correct.



Example CEF Output

The following example shows global audit logs for an audit logging Common Event Format (CEF) template.

Template:

```
CEF:0|%{deviceVendor}|%{deviceProduct}|%{deviceVersion}|%{category}|%{operation}|%{severity}|

rt=%{timestamp} src=%{sourceAddress} spt=%{sourcePort}

suser=%{identity} sourceServiceName=%{deviceService}

deviceExternalId=%{deviceExternalId} dst=%{destinationAddress}
```

```
dpt=%{destinationPort} dvcpid=%{deviceProcessId}
deviceProcessName=%{deviceProcessName} outcome=%{outcome} msg=%{text}
```

Example logs:

```
CEF:0|RSA|NetWitness Audit|11.1.0.0|AUTHENTICATION|logoff|6|rt=Mar 11
2018 08:58:34 src=10.31.125.48 spt=53392 suser=admin
sourceServiceName=BROKER deviceExternalId=92284373-3cdf-4362-be5b-
426f46410262 deviceProcessName=NwBroker outcome=success
```

```
CEF:0|RSA|NetWitness Audit|11.1.0.0|AUTHENTICATION|logoff|6|rt=Mar 11
2018 09:00:00 src=10.31.125.48 spt=52212 suser=admin
sourceServiceName=CONCENTRATOR deviceExternalId=f17aa153-ac33-4775-ad20-
84962d06ab9e deviceProcessName=NwConcentrator outcome=success
```

```
CEF:0|RSA|NetWitness Audit|11.1.0.0|AUTHENTICATION|logoff|6|rt=Mar 11
2018 08:58:34 src=10.31.125.48 spt=53392 suser=admin
sourceServiceName=BROKER deviceExternalId=92284373-3cdf-4362-be5b-
426f46410262 deviceProcessName=NwBroker outcome=success
```

Configure Investigation Settings

This topic provides instructions for administrators who are configuring the settings that apply to all Investigations on the NetWitness Suiteinstance being configured. The settings for configuring and tuning behavior of NetWitness Suite Investigation are available in the System view > Investigation panel. These settings apply to all investigations and reconstructions on the current instance of NetWitness Suite.

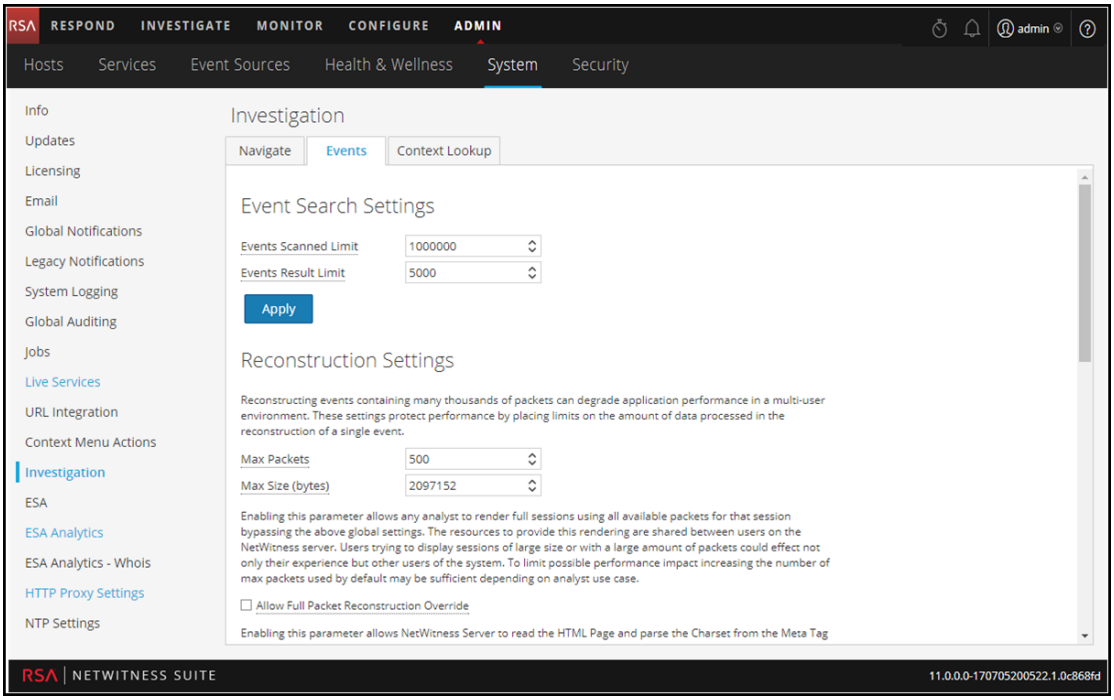
Configure Navigate, Events, and Context Lookup Settings

The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the ADMIN > SYSTEM > Investigations > Context Lookup tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, `ip.address` is a meta key and `ip_address` is not a meta key (it is a field in the MongoDB).

1. Go to **ADMIN > System.**
2. In the options panel, select **Investigation.**

   The Investigation Configuration panel is displayed.



3. In the **Navigate** tab, in the **Render Threads Settings** field, select the maximum number of concurrent meta key values that are loaded by a single user in the navigate view. Click **Apply**.
4. In the **Navigate** tab, in the **Parallel Coordinates Settings** section, set the maximum limits for meta values scanned and meta value results that can be included in a parallel coordinates visualization. For better performance, these are the recommended settings: Meta Values Scan Limit -100000 and Meta Values Result Limit to 1,000-10,000
   Click **Apply**.
5. In the **Events** tab, in the **Event Search Settings** section, set the maximum numbers of events scanned and event results displayed when an analyst is conducting an event search in the Events view. Click **Apply**.
6. In the **Events** tab, in the **Reconstruction Settings** section, set the limits for the amount of data processed in the reconstruction of a single event. The default values are 100 maximum packets and 2097152 bytes. If analysts are seeing slow performance when reconstructing sessions in Investigation, the reconstructing settings may need adjustment. Click **Apply.**

   Caution: Setting a higher value affects the performance of the NetWitness Server by increasing the time and memory taken to create a reconstruction of an event. Setting the value to zero disables any limit and may lead to a NetWitness Server crash.

7. (Optional) In the **Events** tab, in the **Web View Reconstruction Settings** section, enable the use of supporting files in a web view reconstruction, and configure the additional settings to

calibrate web view reconstructions. These include the time range (in seconds) to scan for related events, the maximum number of related events to scan, and overrides to Reconstruction Settings for use with web view reconstructions. Click **Apply**.

8. In the **Context Lookup** tab, manage mapping of Context Hub meta types with meta keys in Investigation. You can add or remove meta keys to the list of meta types supported in Investigation by Context Hub. Procedures associated with this tab are provided in "Manage Meta Type and Meta Key Mapping" in the *Investigation and Malware Analysis Guide*.

Clear Reconstruction Cache for Services

Under Reconstruction Cache Settings, administrators can clear the cache for one or more services. For example, the administrator can clear the cache for a single Broker, a Broker and Decoder, or all connected services. These are a few examples of causes for stale cache being used in a reconstruction.

- The downstream services may have their sessions invalidated or data reset. As an example, if Investigation is browsing a Broker and a downstream Concentrator or Decoder has a data reset, the meta and session data for the investigating service (Broker) does not match the content if the downstream service has reset and repopulated. The reconstruction in Investigation shows content from cache, which does not match the real content. Even if the Decoder is offline, content is still displayed in the Broker reconstruction. Clearing cache on the Broker causes the NetWitness Suite to reach out to the Decoder and an error is returned because the Decoder is offline.
- Another case where cache may be stale is when a service ID for a downstream service changes. This can happen when exporting, importing, deleting, and adding services to NetWitness Suite because NetWitness Suite can reuse service IDs. In this case, clearing the cache on the Broker causes NetWitness Suite to request data from the services.

To clear reconstruction cache, do one of the following:

1. To clear cache for one or more services, select the services and click **Clear Cache for the Selected Services**.
2. To clear the cache for all listed services, click **Clear Cache for All Services.**
   The reconstruction cache for the selected services is cleared. NetWitness Suite sends a request for data to the services.

Configure Live Services Settings

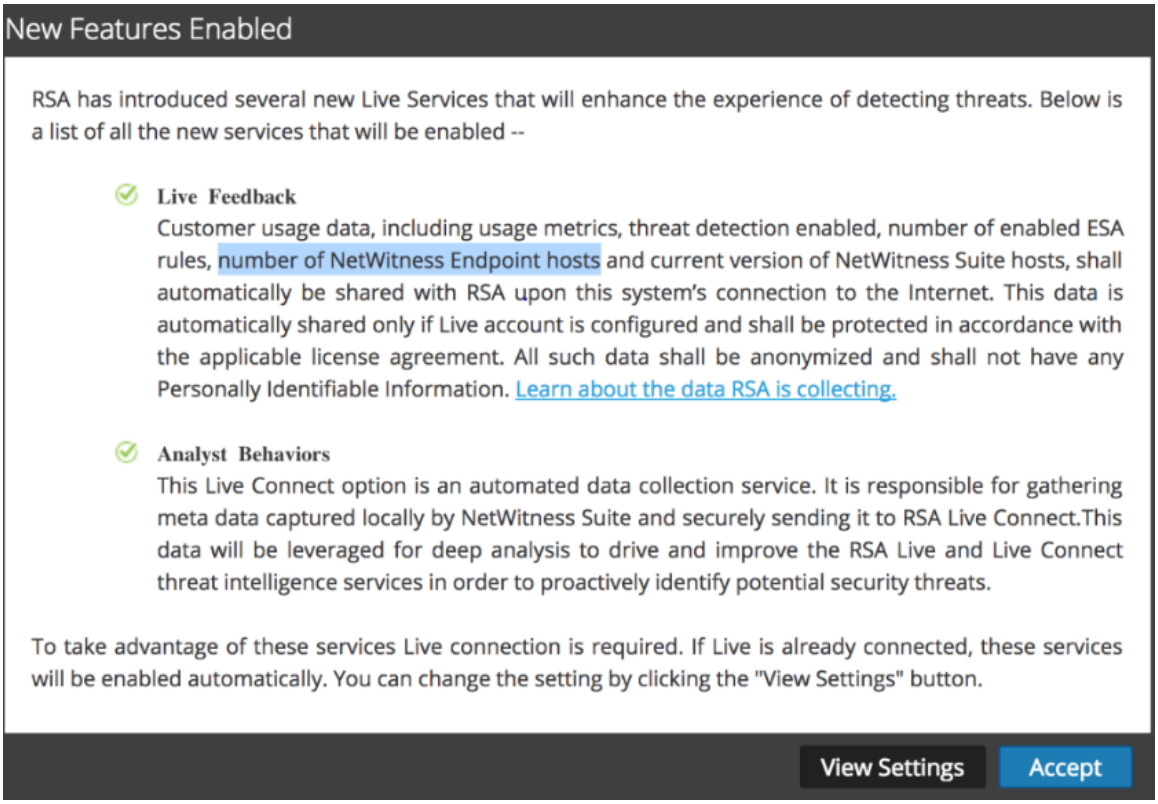
Options for configuring Live Services are in the System view > Live Services Configuration panel. The Live Configuration panel allows you to configure:

- The Live account.
- The Live Content update schedule and preferences for notification of updates.
- Participation in Live Services Feedback.
- Sharing Live Content Usage
- RSA Live Connect (Beta)

Prerequisite

To activate your Live account for NetWitness Suite, please contact RSA Customer Care. When you have a confirmation that your Live account has been set up, you can configure and test the CMS server connection.

When you log on to NetWitness Suite for the first time, you are prompted with **New Features Enabled** dialog.



When you click **Accept**, you automatically agree to the following:

- Participate in Live Feedback.
- Use Live Connect features to receive threat intelligence data.
- Allow NetWitness Suite to send anonymous, technical data about your environment to RSA.

If you click **View Settings**, you are redirected to the Live Services user interface to view the settings for Live Feedback and Live Connect Threat Data Sharing. If you have not configured the Live Account a masked screen is displayed.

For information on Analyst Behaviors and Data Sharing, see "NetWitness Suite Feedback and Data Sharing" topic in the *Live Services Management Guide*.

About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see Live Feedback Overview.

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see Configure Live Services Settings

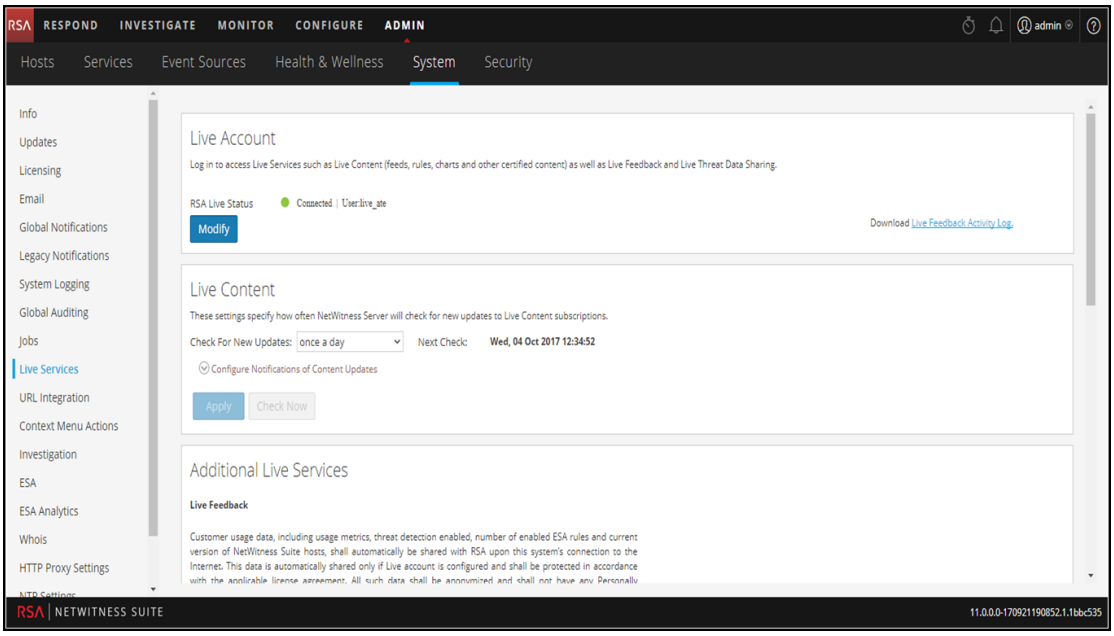
If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see Upload Data to RSA for Live Feedback.

This topic contains the following procedures:

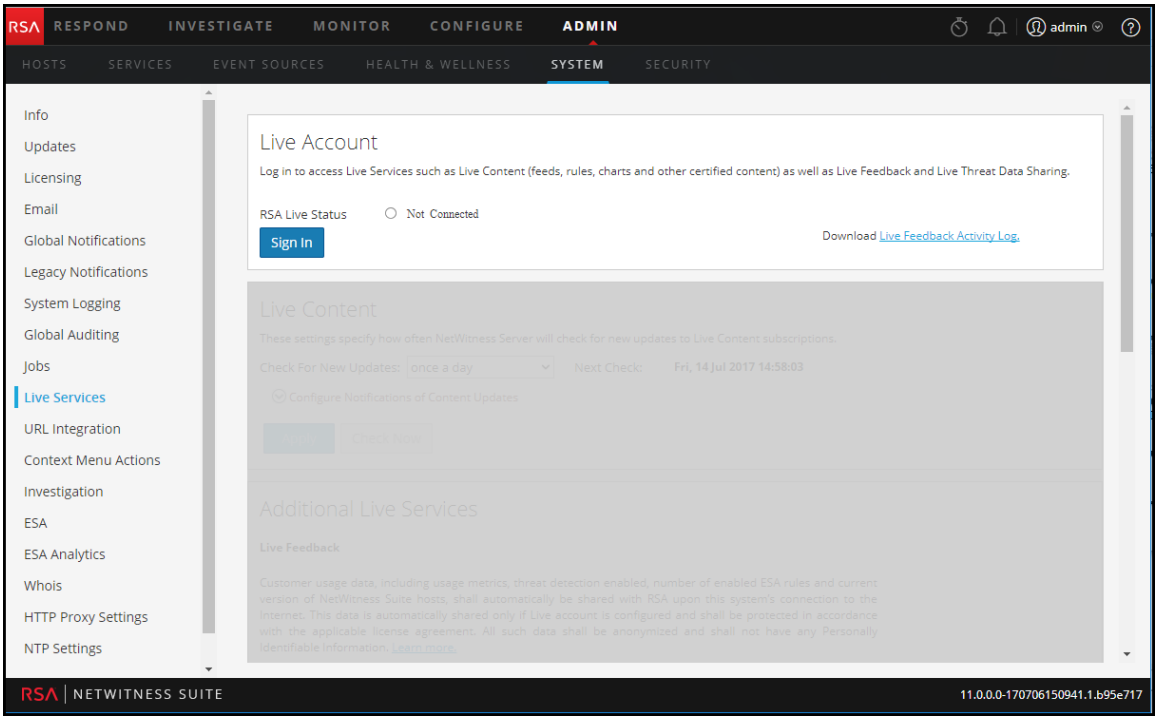
- Access the Live Services Configuration Panel
- Configure Live Account
- Configure the Live Content Synchronization Interval and Notification
- Force Immediate Synchronization
- Using RSA Live Connect

Access the Live Services Configuration Panel

1. Go to **ADMIN** > System.
2. In the options panel, select **Live Services**.



Note: If you are not signed in with your Live Account credentials, a masked screen is displayed.



Configure Live Account

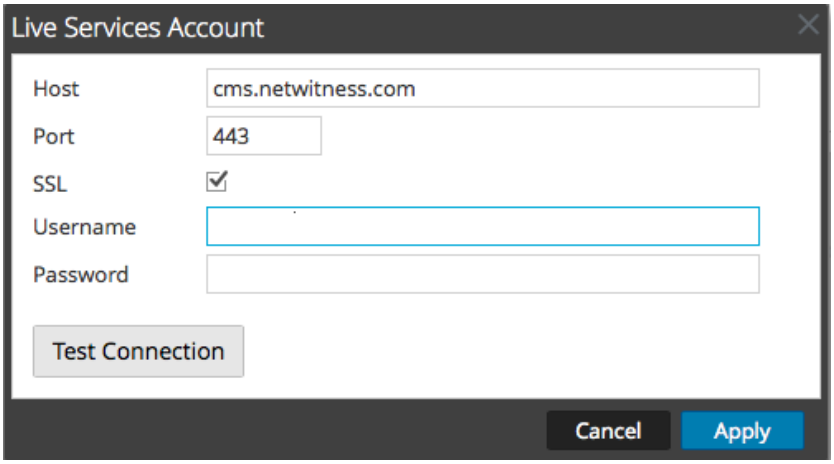
In the **Live Account** section, you must set up the user's Live account. The information needed to set up the user's Live account consists of the Username, Password, and Live URL for the Content Management System. This information is provided by Customer Care.

To configure a Live account:

1. In the **Live Account** section, click **Sign In**.

   Note: The **Modify** button shows that the live account is configured. Click **Modify** to change the user that is accessing Live Services.

2. In the Live Services Account dialog box, enter the Host (typically **cms.netwitness.com**) and type your username and password.

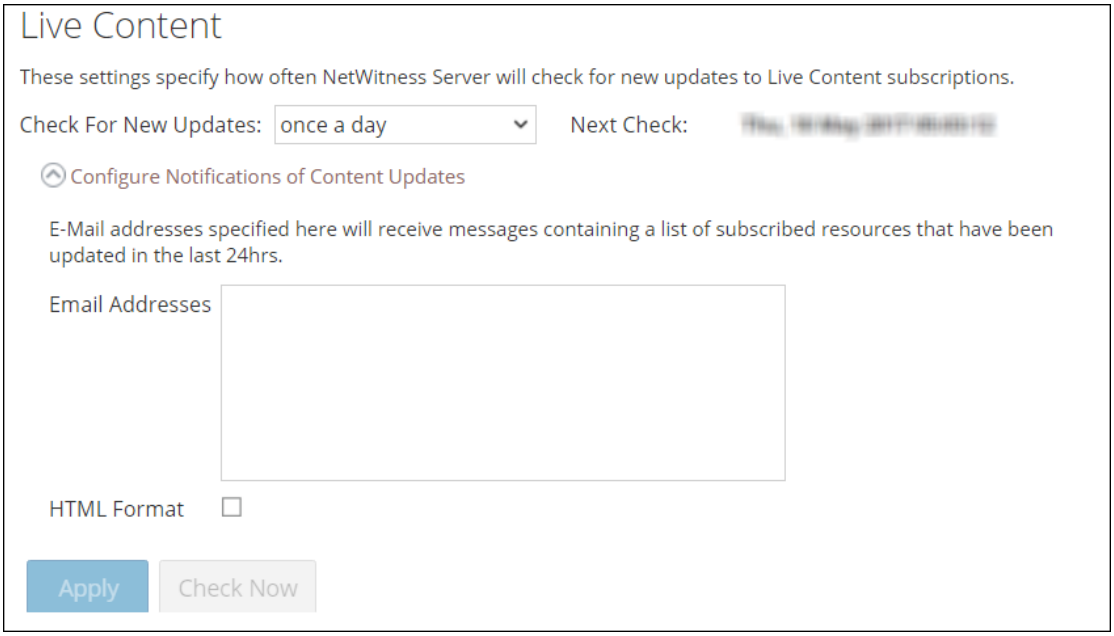


3. (Optional) If you are using a different CMS, type the host URL for the Content Management System. The default points to the CMS at **cms.netwitness.com**.
4. (Optional) If you are using a different CMS, type the communications port for Live to send requests to the Content Management System. The default for this field is **443**, which is the communications port on the Content Management System.
5. (Optional) If you do not want to use SSL, uncheck the **SSL** option. (SSL is enabled by default.)
6. Click **Test connection** to test the connection to CMS.
7. To save and apply the configuration, click **Apply**.

Configure the Live Content Synchronization Interval and Notification

You can change the interval at which NetWitness Suite checks for new updates to Live Content:

1. Use the **Check for New Updates** field to change the interval. Select an interval from the drop-down list. The default value for this setting is **once a day**.



2. To configure Live Services to send update reports to one or more people, in the **Email Addresses** field, type the email addresses as a comma-separated list, for example, **john@company.com,ted@company.com,brian@company.com**
3. (Optional) To receive messages in HTML format rather than plain text, select **HTML Format**.
4. To save and apply, click **Apply**.

   The time and date of the next scheduled Live synchronization based on the configured interval for checking is displayed.

Force Immediate Synchronization

Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite. One use for this is to see the immediate impact of a configuration change. For example, a new service has been added, or new resources have been toggled for automatic deployment. The scheduled synchronization could take place hours later if Live Services is set to synchronize a few times a day.

Caution: Synchronization can cause a parser reload if a FlexParser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.

To force immediate synchronization, click **Check Now**. NetWitness Suite checks for updates in subscribed resources.

Using RSA Live Connect

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA NetWitness® Suite and RSA NetWitness® Endpoint customer community. RSA Live Connect consists of the following features:

- Threat Insights
- Analyst Behaviors

Threat Insights

Threat Insights provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by the analysts during investigation.

By default, **Threat Insights** is enabled in **Additional Live Services** section. If Context Hub service is configured, Live Connect is automatically added as a data source for Context Hub. For more information, see "Configure Live Connect Data Source for Context Hub" topic in the *Context Hub Configuration Guide*.

With Live Connect as a data source for context hub, you can use the Context Lookup option in INVESTIGATE > Navigate view or INVESTIGATE > Events view to fetch contextual information. For instructions, see "View Additional Context for a Data Point" topic in the *Investigation and Malware Analysis Guide*.

Analyst Behaviors

Analyst Behaviors is a feature where analysts participate in sharing data to RSA community. This is an automated data collection service. Its goal is to share potential threat intelligence data to the RSA Live Connect cloud service for analysis. The type of data that could be shared from your network to RSA Live Connect includes various types of meta data captured by NetWitness Suite such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src. For information on Analyst Behaviors and Data Sharing, see "NetWitness Suite Feedback and Data Sharing" topic in the *Live Services Management Guide*.

Live Feedback Overview

This topic provides an introduction to Live Feedback. Live Feedback collects relevant information such as the Licensing usage data for Packet Decoder, Log Decoder and Malware Analysis, Threat Detection Enabled or Disabled status, Number of enabled ESA rules,and version number details of all the services of NetWitness Suite. For more information about the licensing usage data for Packer Decoder, Log Decoder and Malware Analysis, see the **Metered Licenses Tab** topic in the *Licensing Guide*. The information is collected to improve future releases of NetWitness Suite. You will automatically be signed on to live feedback and you cannot disable this option.

In addition to this, information on the Live Content Usage can also be shared with RSA. Live Content usage metrics for resource types from **CONFIGURE > Live Content > Search Criteria** such as total count of RSA Application Rule, RSA Correlation Rule etc. can be shared with RSA. The information collected is used to improve the use of Live Content. For more information about sharing live content configuration, see Live Services Configuration Panel.

About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see Live Feedback Overview.

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see Configure Live Services Settings

If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see Upload Data to RSA for Live Feedback.

Note: Live Feedback is activated only if you have configured your Live account.

The Live Feedback data is in JSON format as mentioned below. When you sign up with your Live Account credentials, a single encrypted JSON file is automatically uploaded to the RSA servers everyday.

JSON File

The JSON file consists of usage data information for a component or a set of components. In case of a set of components with the same license id, the usage data for all the components is aggregated and represented as a component called Entitlement. However, even if there is a single component such as a log decoder or decoder, an Entitlement component will be generated and will display the usage data for a single component. This aggregation is for components namely log decoders, decoders or malware analysis.

Note: The version of Entitlement is always null as it is the aggregate for a license data.

For example, if there are three Decoders with the same license id "xxx" with the following usage data:
Decoder1 = 150 MB
Decoder2 = 250 MB
Decoder3 = 100 MB
The aggregated usage data of 500 MB is displayed.

This JSON file is described in the following sections:

- Components
- Metrics
- Other Product Details
- Sample

Components

Details of each service in your NetWitness Suite deployment. This is represented as Component. For each component the following details are displayed.

Component	Description
Version	Version number of the component in the NetWitness Suite deployment. For example, 11.1.0.0.x.x.x.x.
ID	This is the unique Component ID that represents the host and is used to link to the metrics generated.
Properties	• **Name** - This is the name of the property for that component. For example, malware analysis, ESA, log decoder, etc. • **Value** - This is the unique value to identify the component.

Metrics

Metrics of the components (hosts) such as log decoder, decoder and malware analysis. The license usage data for each host is shared. For Live Content usage metrics, resource types from **CONFIGURE > Live Content > Search Criteria** such as total count of RSA Application Rule, RSA Correlation Rule etc. are shared.

Component	Description
StartTimeUTC	This is the time from when the metrics is collected. (in EPOCH format).

Component	Description
Stats	• **Value** - This is the value generated for the specific component ID for each component. • **Name** - This is the name of the statistics for which the metrics is collected. For example, Capture Total Bytes.
EndTimeUTC	This is the time when the metrics collection is complete (in EPOCH format).
Component ID	This is the ID of the component for which the value is recorded.

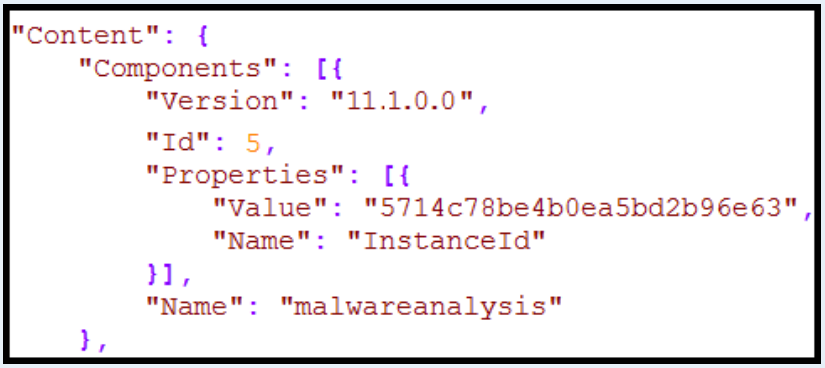
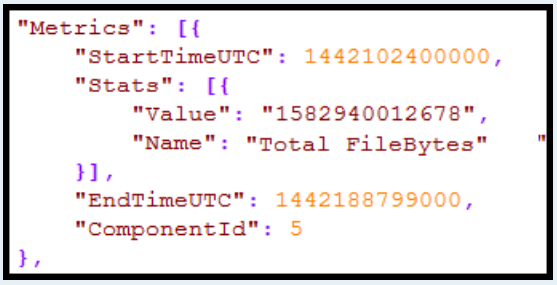
Other Product Details

- **Product Type** - This is the name of the product. In this example, the Product Type is NetWitness Suite.
- **Version** - This is the version of the JSON file which tracks the changes made to the file format.
- **Product Instance** - This is the License Server ID.
- **Checksum** - This is the information which is used for integrity checks.

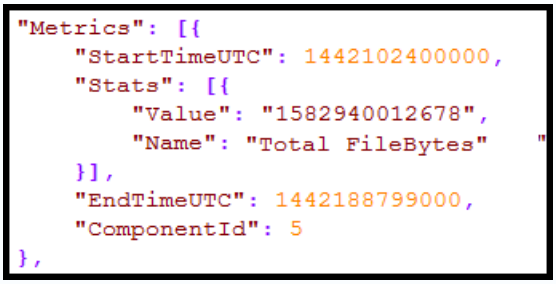
The following table describes details of the JSON file with examples.

Metrics	Description
Content	Displays the content that contains all the Components, Metrics, Product Type and Product Instance data except Checksum.

Metrics	Description

Components	The details of all the services in NetWitness Suite are represented as a Component. The details of the component such as the version number of the component, the name, and the value is displayed as shown below:
	 
	"Content": {
	"Components": [{
	"Version": "11.1.0.0",
	"Id": 5,
	"Properties": [{
	"Value": "5714c78be4b0ea5bd2b96e63",
	"Name": "InstanceId"
	}],
	"Name": "malwareanalysis"
	},
	Version: Displays the version of NetWitness Suite service. For example, 11.1.0.0.
	ID: Displays an unique id which is generated for the NetWitness Suite service and is used to link to the metrics for that particular component. In this example, the ID for Malware Analysis is 5 and the metrics is displayed for ComponentId 5 in bytes, as shown below:
	 
	"Metrics": [{
	"StartTimeUTC": 1442102400000,
	"Stats": [{
	"Value": "1582940012678",
	"Name": "Total FileBytes"
	}],
	"EndTimeUTC": 1442188799000,
	"ComponentId": 5
	},
	Properties: Displays the properties for the component such as name and value as shown in the above figure.
	Value: Displays the value of the property which is an internal UUID for a component as shown in the above figure This is generated by NetWitness Suite.
	For example, For malware analysis the value displayed as
	`"55f7a0b30e502231c42d063f"`
	Name: "InstanceId": Displays the name of the property as shown in the above figure.
	Name": "malwareanalysis": Displays the name of component which is a service name such as LogDecoder, Decoder, or MalwareAnalysis.

Metrics	Description

Metrics	Displays the list of the metrics with the usage data for components namely log decoder, decoder and malware analysis.
	In this example, the metrics is displayed for ComponentId 5 in bytes, as shown below.
	 
	"Metrics": [{
	"StartTimeUTC": 1442102400000,
	"Stats": [{
	"Value": "1582940012678",
	"Name": "Total FileBytes"
	}],
	"EndTimeUTC": 1442188799000,
	"ComponentId": 5
	},

	StartTimeUTC: Displays the time when the metrics is collected, in the EPOCH format.
	Stats: Displays the usage value and usage type statistics of the component.
	Value: Displays the value of the statistics. For example, "Value": "1582940012678" as shown in the above figure.
	Name: Displays the name of the statistics. For example, Capture Total Bytes or Total File bytes.
	EndTimeUTC: Displays the time when the metrics collection is complete, in the EPOCH format.
	ComponentId: Displays the component id for which the metric values are collected. This is the same as the "ID" in the Components section.
Content	Displays the content that contains all the Components, Metrics, Product Type and Product Instance data except Checksum.
ProductType	Displays the product type that generates the file. For example, `"ProductType": "NetWitness Suite"`
ProductInstance	Displays the License server Id and is unique per NetWitness Suite. For example, `"ProductInstance": "00-0C-29-6C-66-E3"`

Metrics	Description
Checksum	Displays the Checksum for the "Content" section in the file. Used by RSA for integrity check. For example, `"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"`

Sample

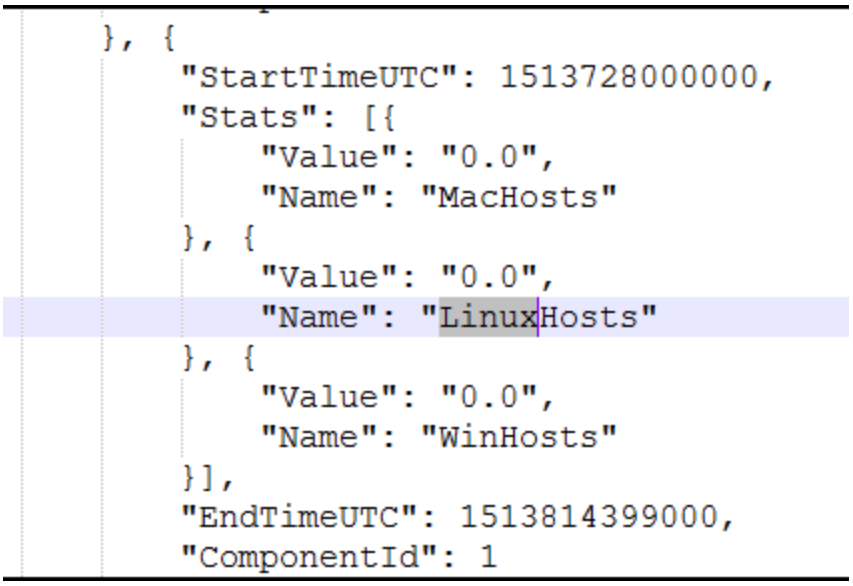
Here is a sample JSON file.


```
{
    "Content": {
        "Components": [{
            "Version": "11.1.0.0",
            "Id": 7,
            "Properties": [{
                "Value": "57470c96e4b0cf62c7bfbd53",
                "Name": "InstanceId"
            }],
            "Name": "esa"
        },
        {
            "Version": "11.1.0.0",
            "Id": 4,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e69",
                "Name": "InstanceId"
            }],
            "Name": "incidentmanagement"
        },
        {
            "Version": "11.1.0.0",
            "Id": 2,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e65",
                "Name": "InstanceId"
            }],
            "Name": "sa"
        },
        {
            "Version": "11.1.0.0",
            "Id": 1,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e63",
                "Name": "InstanceId"
            }],
            "Name": "malwareanalysis"
        },
        {
            "Version": "11.1.0.0",
            "Id": 3,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e67",
                "Name": "InstanceId"
            }],
            "Name": "reportingengine"
        }],
        "Metrics": [{
            "StartTimeUTC": 1464480000000,
            "Stats": [{
                "Value": "Disabled",
                "Name": "Threat Detection"
            },
            {
                "Value": "3.0",
                "Name": "Number Of Enabled ESA Rules"
            }],
            "EndTimeUTC": 1464566399000,
            "ComponentId": 7
        }],
        "EndTime": 1464566399000,
        "Version": "1.0",
        "StartTime": 1464479999000,
        "ProductType": "Security Analytics",
        "ProductInstance": "00-0C-29-A2-57-B4"
    },
    "Checksum": "6445C704D3F9E67D24DBA8F11EB6C003CBCC0B199576342E6E6D2545524F583F"
}
```

The JSON file includes details of all the licenses currently available on the appliance. Here is a sample of the Entitlement information within the JSON file for a service based license for Broker.

```
    }, {
        "Version": "2015.0506",
        "Id": 14,
        "Properties": [{
            "Value": "M133206102",
            "Name": "SerialNumber"
        }, {
            "Value": "Broker",
            "Name": "DeviceType"
        }, {
            "Value": "PERPETUAL",
            "Name": "FeatureType"
        }, {
            "Value": "-1",
            "Name": "Threshold"
        }, {
            "Value": "1000654868",
            "Name": "AccountId"
        }, {
            "Value": "B02E-03A1-08A6-EC3B",
            "Name": "ActivationId"
        }, {
            "Value": "2015-05-05 00:00:00",
            "Name": "LicenseStartDate"
        }, {
            "Value": "permanent",
            "Name": "LicenseEndDate"
        }, {
            "Value": "20t-52osb7",
            "Name": "FeatureId"
        }, {
            "Value": "smcBroker",
            "Name": "Name"
        }, {
            "Value": "20t-52osb7",
            "Name": "InstanceId"
        }],
        "Name": "Entitlement"
    }, {
```

For Endpoint, WinHosts, LinuxHosts and MacHosts metrics are displayed which indicate the number of agents deployed. Here is a sample of the Endpoint metrics within the JSON file.



Upload Data to RSA for Live Feedback

This topic provides instructions for a NetWitness Suite administrator to export the metrics in NetWitness Suite for Live Feedback.

If the Live Account is not configured, you can manually upload the usage data to RSA. For more information, see Live Services Configuration Panel.

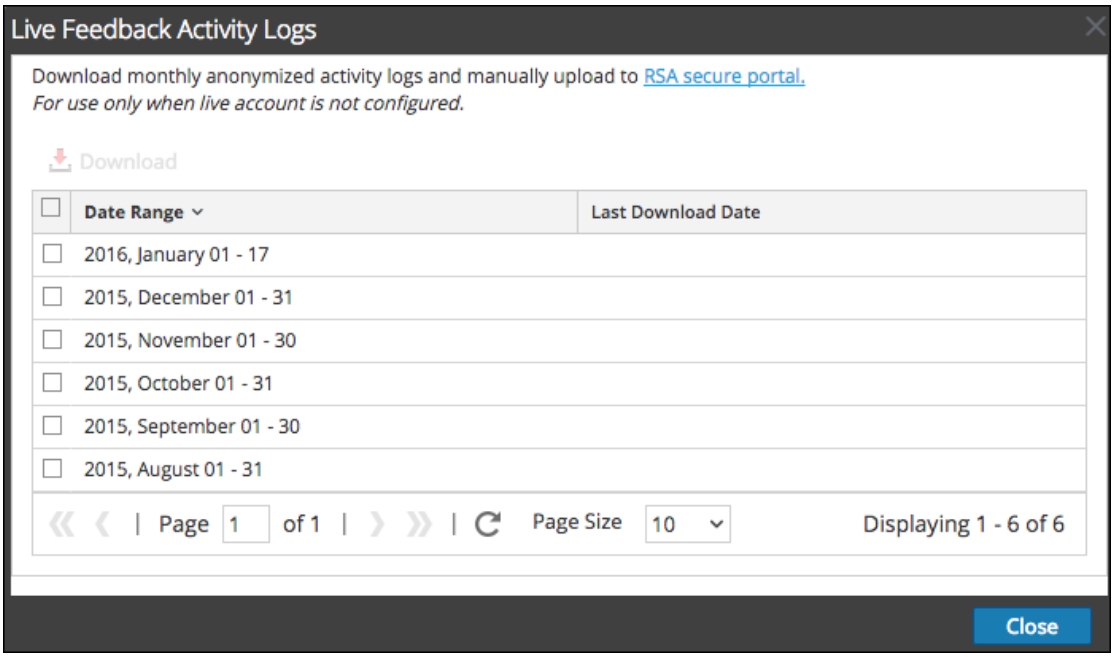
The Live Account section has a Live Feedback Activity Log which enables you to download the usage data required for Live Feedback. This is active regardless of the Live Account configuration.

You can first download the Live Feedback historical data, and then upload it to share with RSA.

Download Live Feedback Historical Data

To download the Live Feedback historical data:

1. Go to **ADMIN** > **System**.
2. In the options panel, select **Live Services**.
   The **Live Account** screen is displayed which consists of the **RSA Live Status** and Download **Live Feedback Activity Log**.
3. Click the **Download Live Feedback Activity Log**.
   The **Download Live Feedback Activity Log** window opens which allows the NetWitness Suite user to download the required Live Feedback historical data.



4. Select one or multiple entries by selecting the checkboxes and click **Download**.

> **Note:** If you select multiple entries in the history table, the downloaded zip file consists of an individual JSON file for each month.

The downloaded Live Feedback data is in JSON format, and is bundled as a .zip file. For more information, see Live Feedback Overview.

Share Data with RSA

After you download the Live Feedback data, you can then upload it using the following procedure.

To share the data to RSA:

1. Click on the **RSA Secure Portal** available on the **Live Feedback Activity Logs** window. The RSA NetWitness® Suite Live Feedback login screen is displayed.
2. Login to the Upload Live Feedback Activity Logs portal using your Live ID credentials.
3. Click **Choose File**, and select the downloaded file.
4. Click **Upload.**

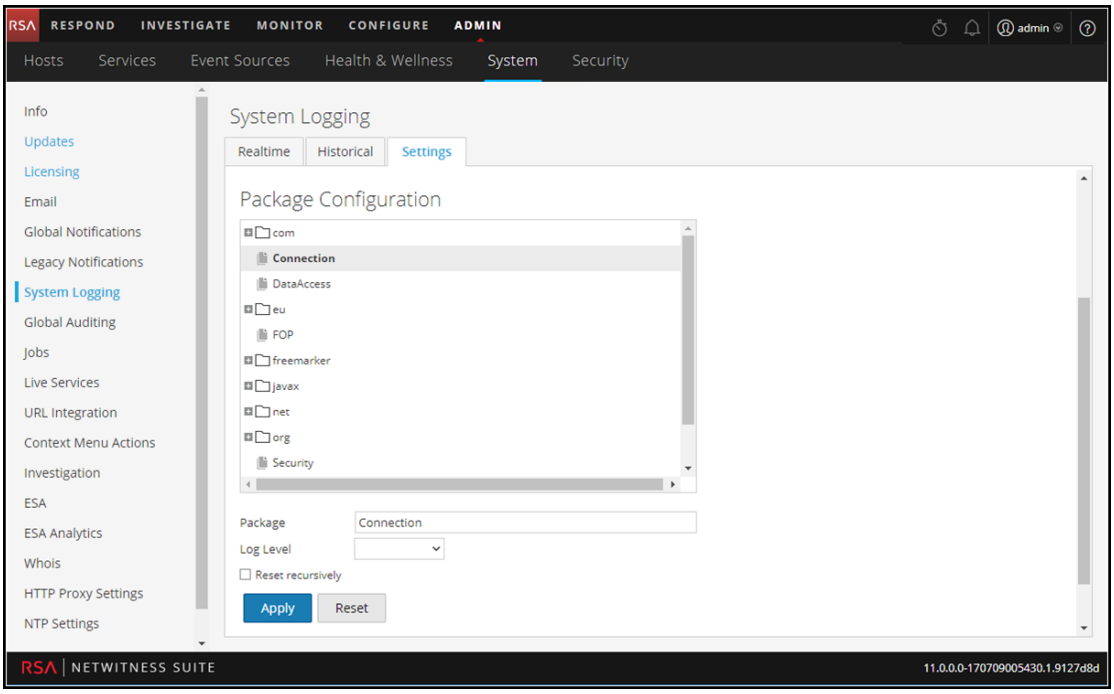
Configure Log File Settings

In RSA NetWitness® Suite, you can configure the size of the log files, the number of backup log files maintained, as well as the default logging levels for the packages within NetWitness Suite.

Configure System Log File Size and Backup Count

The log file size and backup count are configured with default values. If you want to change the default values for the log file size and number of backups:

1. Go to **ADMIN > System.**
2. In options panel, select **System Logging**.
   The System Logging Configuration panel opens to the Realtime tab by default.
3. Click the **Settings** tab.

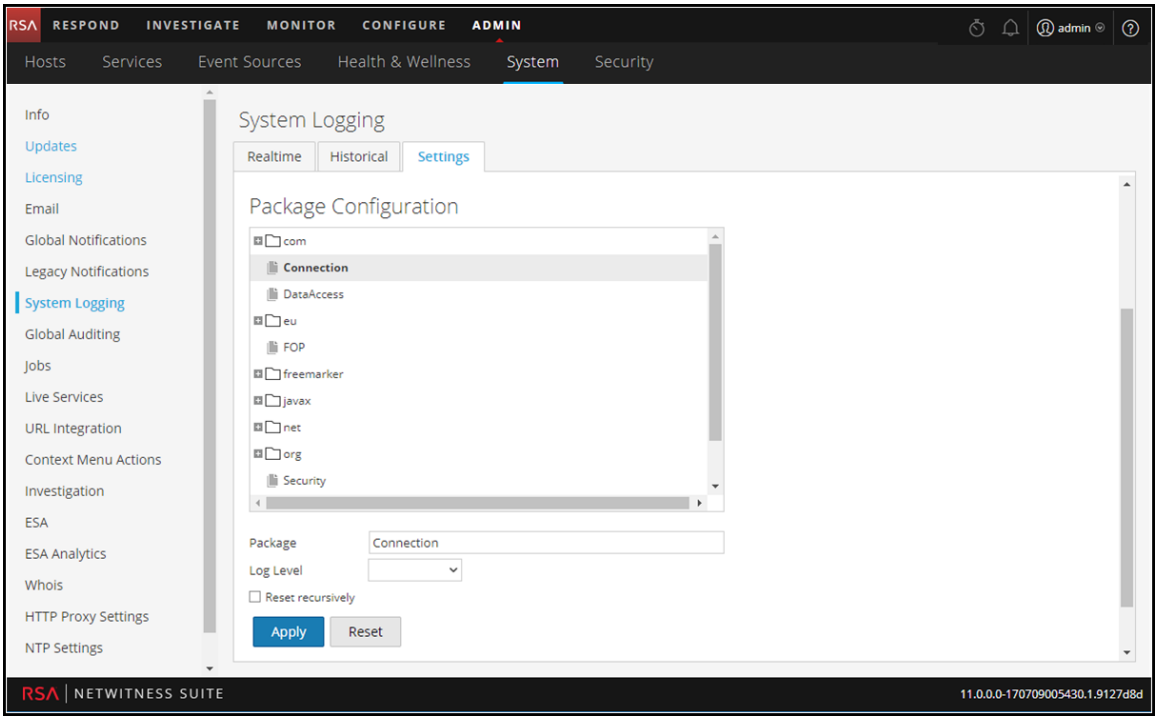


4. In the **Max Log Size** field, type the maximum size in bytes. The minimum value for this setting is **4096**.
5. In the **Max # Backup Files** field, type the maximum number of backup logs to maintain. The minimum value for this setting is **0**. When the maximum number of log files is attained, and a new backup file is made, the oldest backup is discarded.
6. Click **Apply**.
   The changes go into effect immediately.

Set the Log Level for an Individual Package

The Package Configuration section shows the NetWitness Packets in a tree structure. The tree contains all the packages used within NetWitness Suite. You can drill down into the tree to view the log levels of each package. The log level for all packages that are not explicitly set is the same as the **root** log level. To set the log level for a package:

1. Select the package in the **Package** tree.
   The name of the package is displayed in the **Package** field. If a log level is already set for the package, that level is shown.



2. Select the **Log Level** in the drop-down list.
3. Click **Apply**.
   The new log level becomes effective immediately.
4. (Optional) If you want to revert to the default log level specified for **root**, click **Reset**.

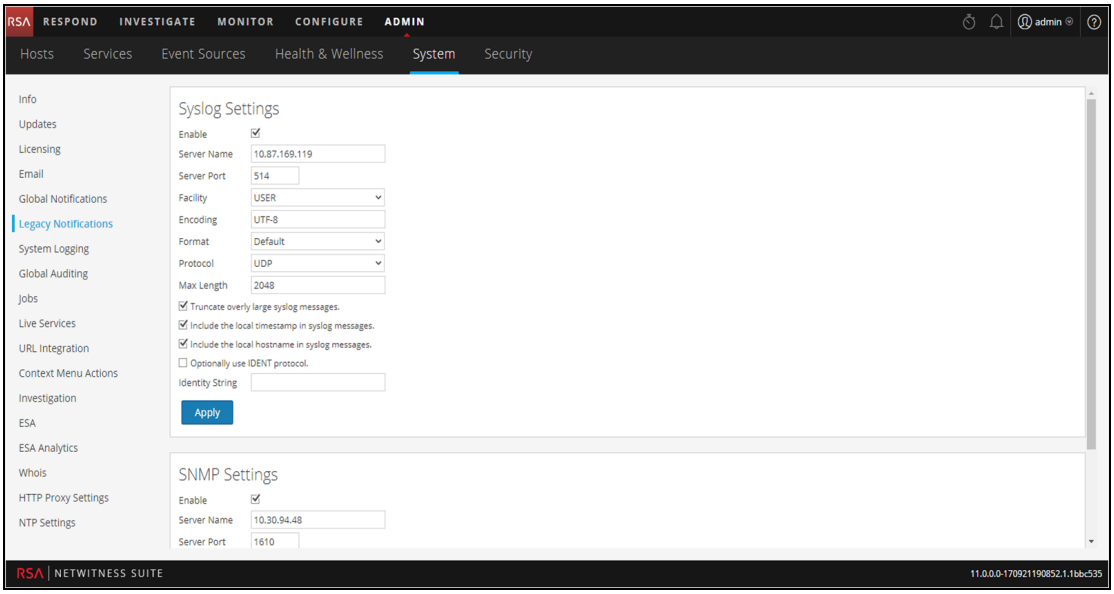
Configure Syslog and SNMP Settings

On the Legacy Notifications panel, you can configure syslog and SNMP notification settings. These configurations are used for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Configure and Enable Syslog Settings

1. Go to **ADMIN > System**.

2. In the options panel, select **Legacy Notifications**.
   The Legacy Notifications Configuration panel is displayed.



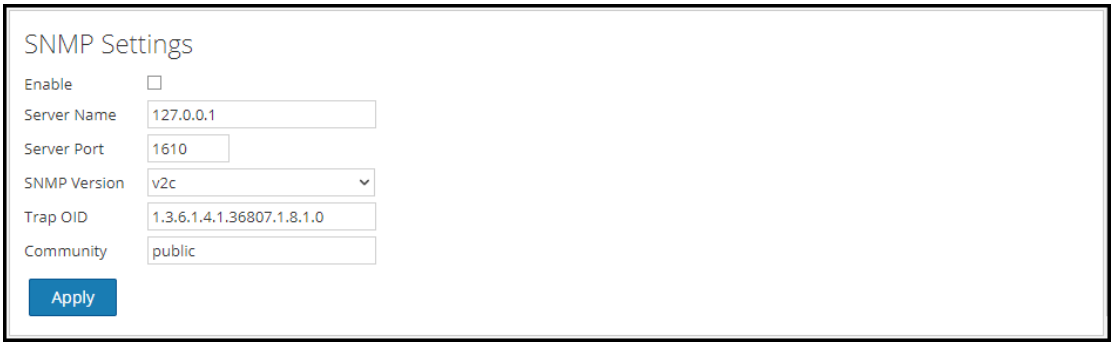
3. In the **Server Name** and **Server Port** fields under **Syslog Settings**, type the host name where the target syslog process is running and the port where the target syslog process is listening.
4. In the **Facility**, **Encoding**, **Format**, and **Max length** fields, specify the syslog facility, message text encoding, message format, and maximum message length.
5. In the **Protocol** field, select either UDP or TCP.
6. (Optional) Select the options for what to include in messages: **Truncate overly large syslog messages**, **Include the local timestamp in syslog messages**, and **Include the local hostname in syslog messages**.
7. (Optional) Configure syslog to prepend an Identity String before each syslog alert.
8. Click the **Enable** checkbox.
9. Click **Apply**.
   Syslog notifications are immediately enabled.

Legacy Notifications Configuration Panel provides detailed information about these settings.

Configure and Enable SNMP Settings

1. Go to **ADMIN > System**.
2. In the options panel, select **Legacy Notifications**.
   The Legacy Notifications Configuration panel is displayed, with SNMP Settings at the

bottom of the panel.



3. In the **Server Name** and **Server Port** fields under **SNMP Settings**, type the host name and listening port of the SNMP trap host.
4. Select the **SNMP version** in the drop-down menu, **v1** or **v2c**.
5. In the **Trap OID** field. specify the object ID for the SNMP trap on the trap host that receives the audit event. The default value is **0.0.0.0.0.1**.
6. In the **Community** field, specify the community string used to authenticate on the SNMP trap host, the default value is **public**.
7. Click the **Enable** checkbox.
8. Click **Apply**.
   SNMP notifications are immediately enabled.

Legacy Notifications Configuration Panel provides detailed information about these settings.

Disable Syslog or SNMP Settings

To disable syslog or SNMP settings on this NetWitness Suite instance:

1. Clear the appropriate **Enable** checkbox.
2. Click **Apply**.
   The selected settings are immediately disabled.

Additional Procedures

Additional procedures are not essential for the set up of NetWitness Suite, they include certain customization options that are beyond the usual setup; for example, adding custom context menus or setting up a proxy.

Add Custom Context Menu Actions

Configure NTP Servers

Configure Proxy for NetWitness Suite

Add New Configuration Dialog

Supported CEF Meta Keys

Supported Global Audit Logging Meta Key Variables

Global Audit Logging Operation Reference

Local Audit Log Locations

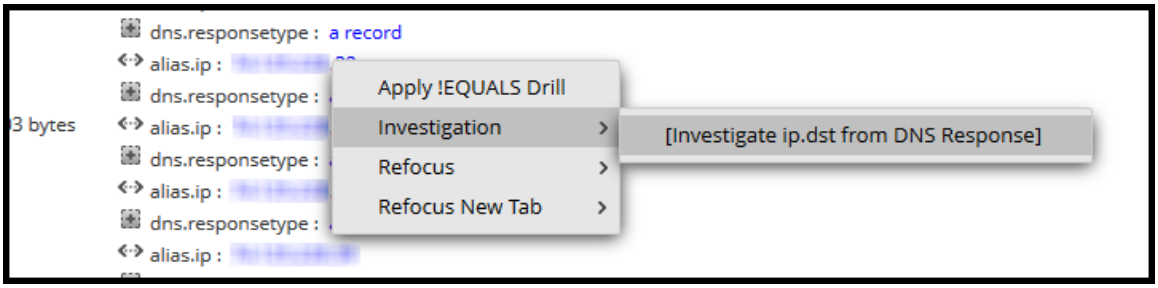
Add Custom Context Menu Actions

In the Context Menu Actions panel, administrators can view, add, and edit context menu actions for the current instance of NetWitness Suite. Each context menu action applies to a specific context in the NetWitness Suite user interface, and appears as an option when you right-click a specific location in the user interface.

Some context menu actions are built into NetWitness Suite; you cannot edit or delete any of the default context menu actions. You can create and edit custom context menu actions. If you want to create a custom variation of a built-in context menu action, you can copy the configuration to a new context menu action and modify the custom context menu action. A context menu action is defined by cascading style sheet (CSS) code that defines:

- The title of the option in the context menu.
- The NetWitness Suite module in which the context menu is available.
- The content to which the action applies.

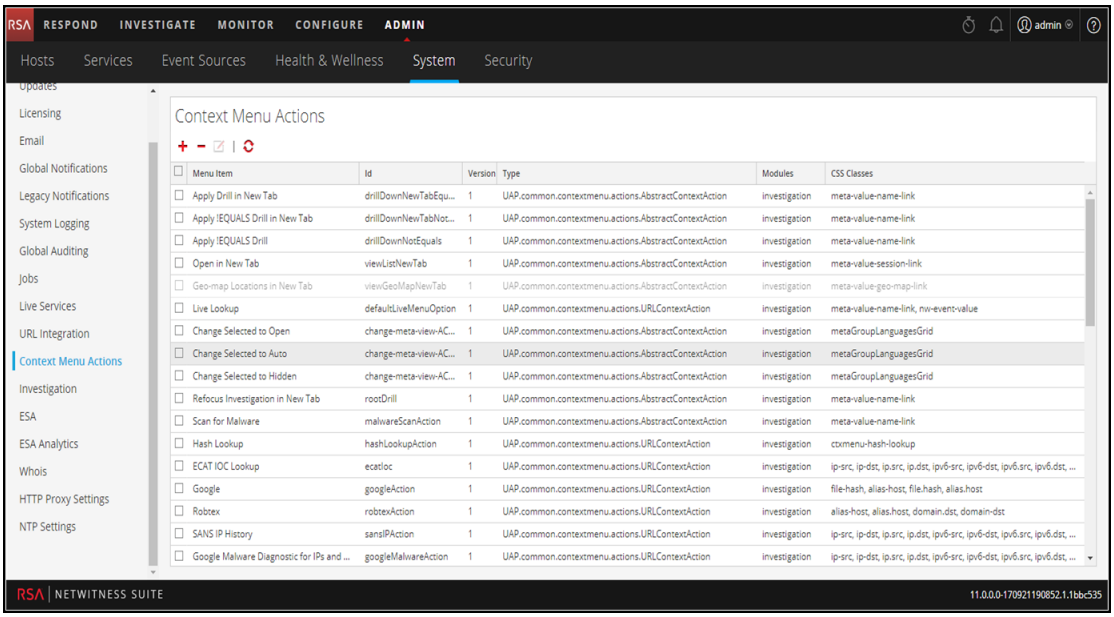
This is an example of a custom context menu action; the steps and CSS code to create this example are provided as an example procedure below.



View Context Menu Actions in NetWitness Suite

To view existing context actions in NetWitness Suite both default and custom:

1. Go to **ADMIN > System.**
2. In the options panel, select **Context Menu Actions**.



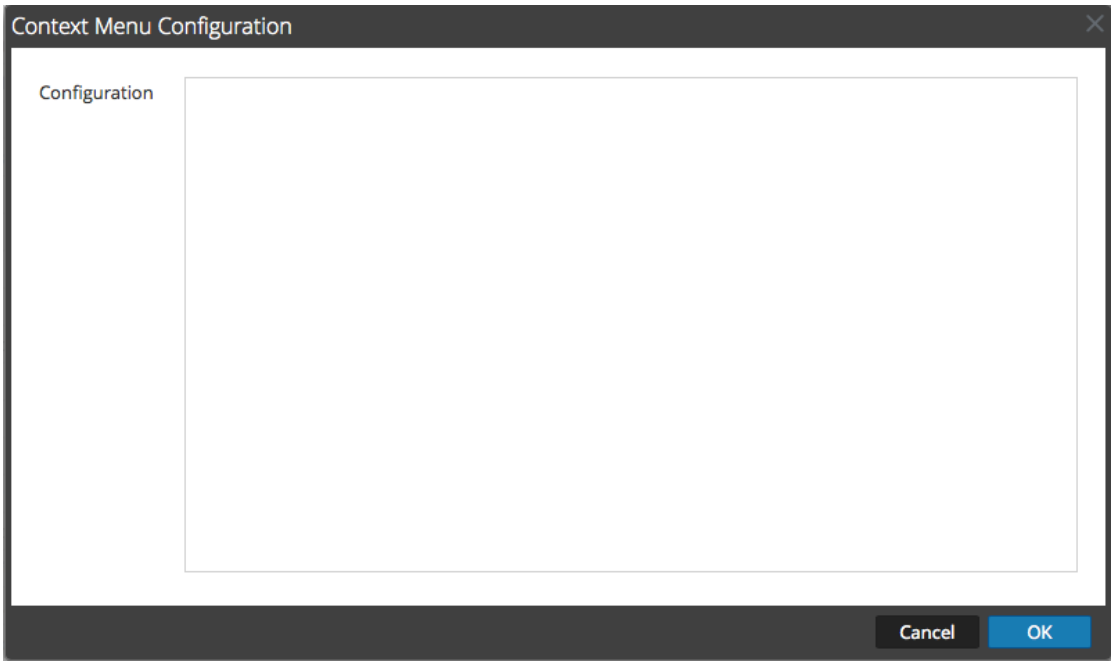
Details of the information in the Context Menu Action panel are provided in Context Menu Actions Panel.

Add a Context Menu Action

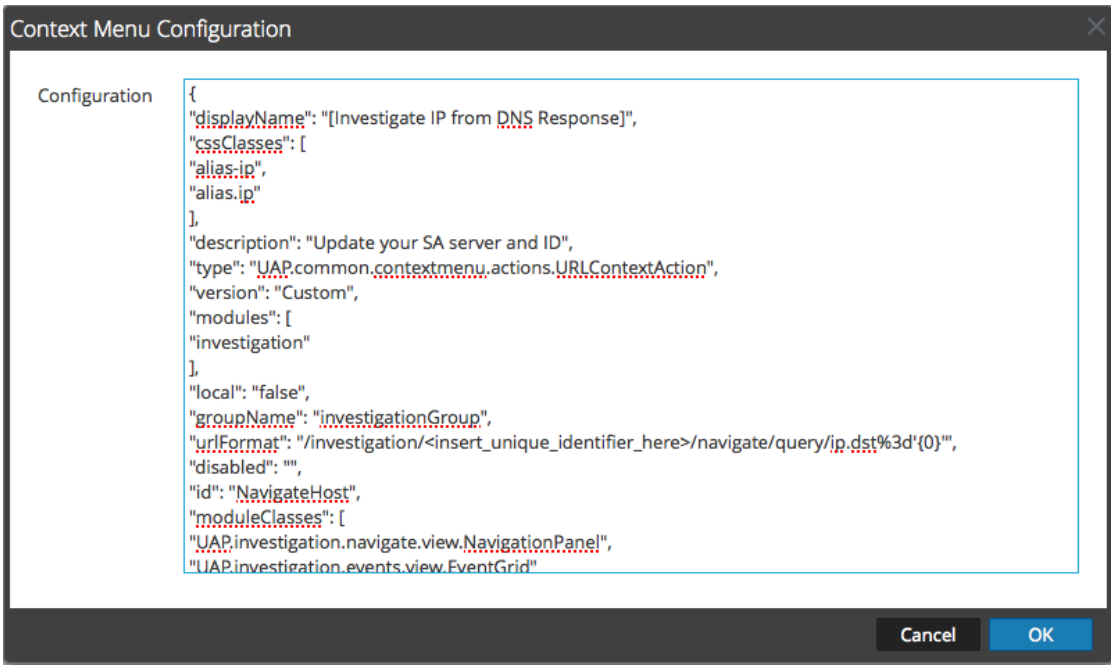
To add a context menu action in NetWitness Suite:

1. In the toolbar, click +.

   The Context Menu Configuration dialog is displayed.



2. Type the CSS code to define the context menu action. The example procedure at the end of this topic provides step-by-step instructions that you can use to create a useful context menu action.



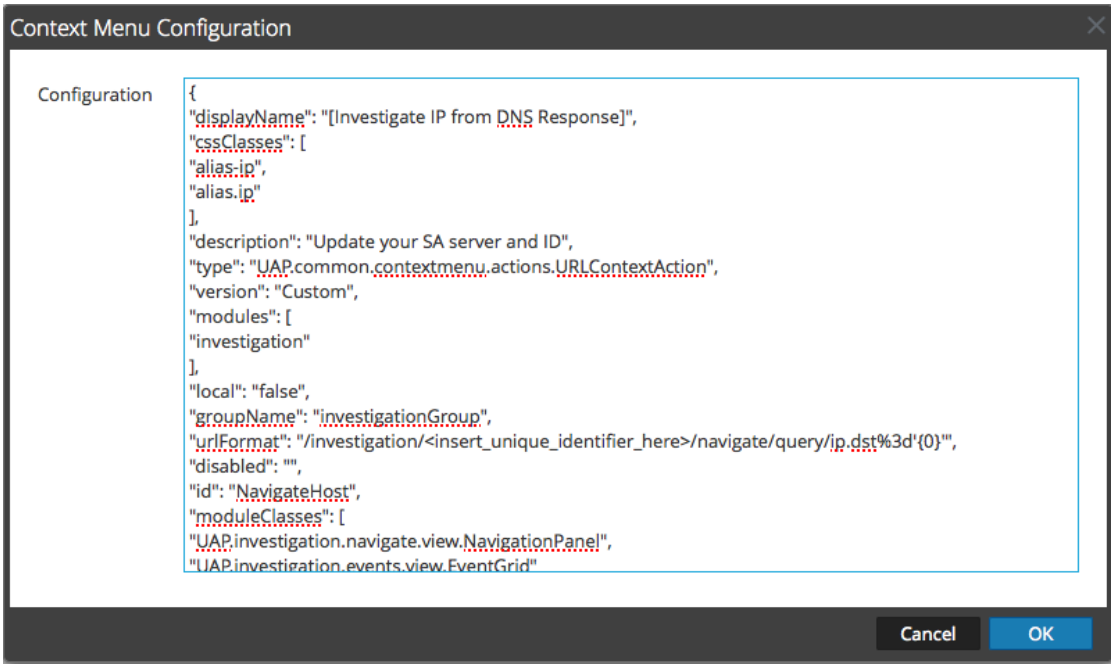
3. Click **OK.**
   The new context menu action is created and added at the end of the list of context menu actions.

4. To activate the new context menu action, restart the browser.
   The context menu action becomes available in the configured location.

Edit a Context Action

To edit a context action:

1. Select the row in the grid and either **double-click** the row or click .
   The **Context Menu Configuration Dialog** is displayed.



2. Edit the **Configuration**.
3. To save the changes, click **OK**.
4. To use the updated action, restart the browser.

Delete a Context Action

To remove a context menu action from NetWitness Suite entirely:

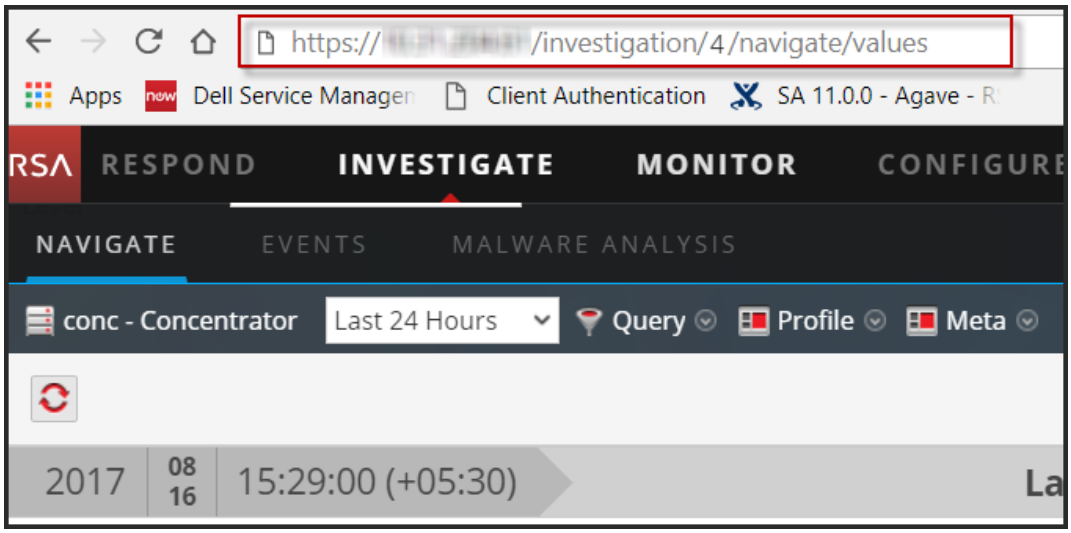
1. Select the action.
2. Click .
   A dialog requests confirmation that you want to delete the context menu action.
3. Click **Yes**.
   The option is removed from the Context Menu Actions panel.
4. Restart the browser to remove the action from the context menus in which it appeared.

Example Procedure: Context Menu Action to Investigate ip.dst from alias.ip

This example adds a context menu action that allows analysts to pivot from the `alias.ip` values (the IP addresses returned from a DNS request) to the `ip.dst` meta key. It helps analysts to locate any detected traffic to the IP address that was returned for a DNS query.

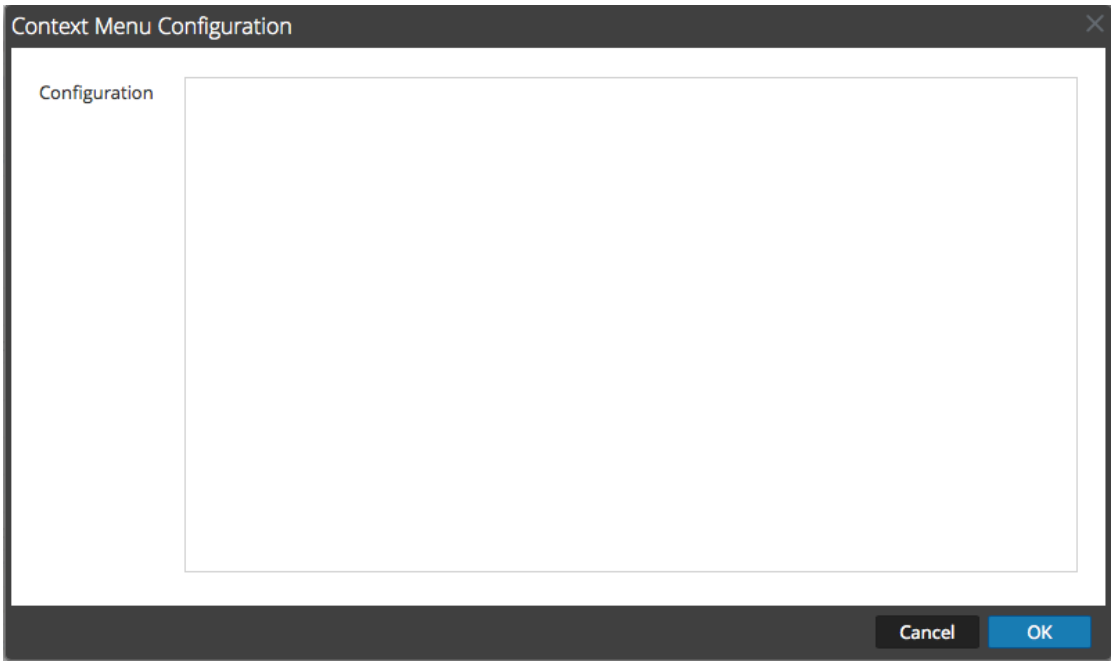
To implement the context menu action:

1. Determine the unique identifier for your NetWitness Server as follows:
   a. Log onto NetWitness Suite, in the main menu, select **INVESTIGATE > Navigate**, choose a service (for example, a Concentrator) to investigate, and wait for the values to load.
   b. Look for the URL and locate the number after `investigation`. In this example, the unique identifier for the action is 4. You need this unique identifier to add to the context menu action.



2. In the toolbar, click +.

   The Context Menu Configuration dialog is displayed.



3. Copy the entire sample code block below and paste it in the window.

```
{
    "displayName": "[Investigate IP from DNS Response]",
    "cssClasses": [
        "alias-ip",
        "alias.ip"
    ],
    "description": "Update your NW server and ID",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "Custom",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "investigationGroup",
    "urlFormat": "/investigation/<insert_unique_identifier_
here>/navigate/query/ip.dst%3d'{0}'",
    "disabled": "",
    "id": "NavigateHost",
    "moduleClasses": [
```

```
            "UAP.investigation.navigate.view.NavigationPanel",
            "UAP.investigation.events.view.EventGrid"
        ],
        "openInNewTab": "true"
    }
```

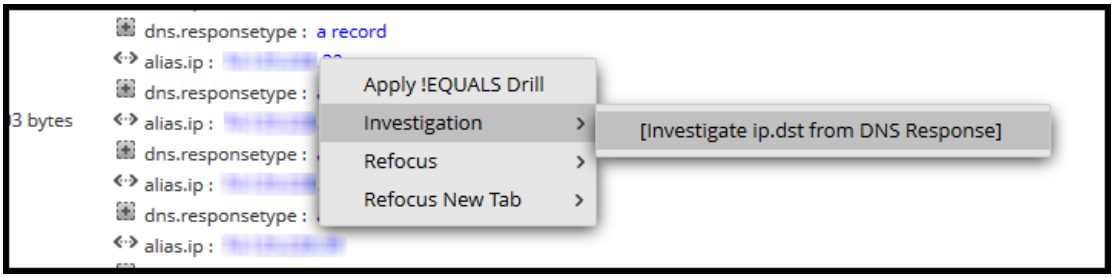
4. In the **urlFormat** line replace **<insert-unique_identifier_here>** with your unique identifier. The URL should look like this:

   `"/investigation/4/navigate/query/ip.dst%3d'{0}'"`

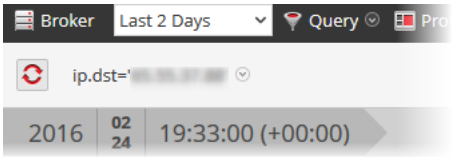
5. Click **OK**, and restart your browser.

6. To test the action, open an investigation in the Navigate view and right-click on the meta key `alias.ip`.

   The context menu with the Investigation option should look like the following figure.



7. Should produce a pivot like this.



8. If you are using this example for DNS traffic investigation, you may want to consider creating a meta group specific to DNS traffic as described in "Manage User-Defined Meta Groups" in the *Investigation and Malware Analysis Guide*.

Configure NTP Servers

This topic provides instructions on how to configure Network Time Protocol (NTP) servers. NTP is a protocol designed to synchronize host machine clocks over a network. For more information on NTP go to their home page (http://www.ntp.org/).

Note: NW Core hosts must be able to communicate with the NW host with UDP port 123 for NTP time synchronization.

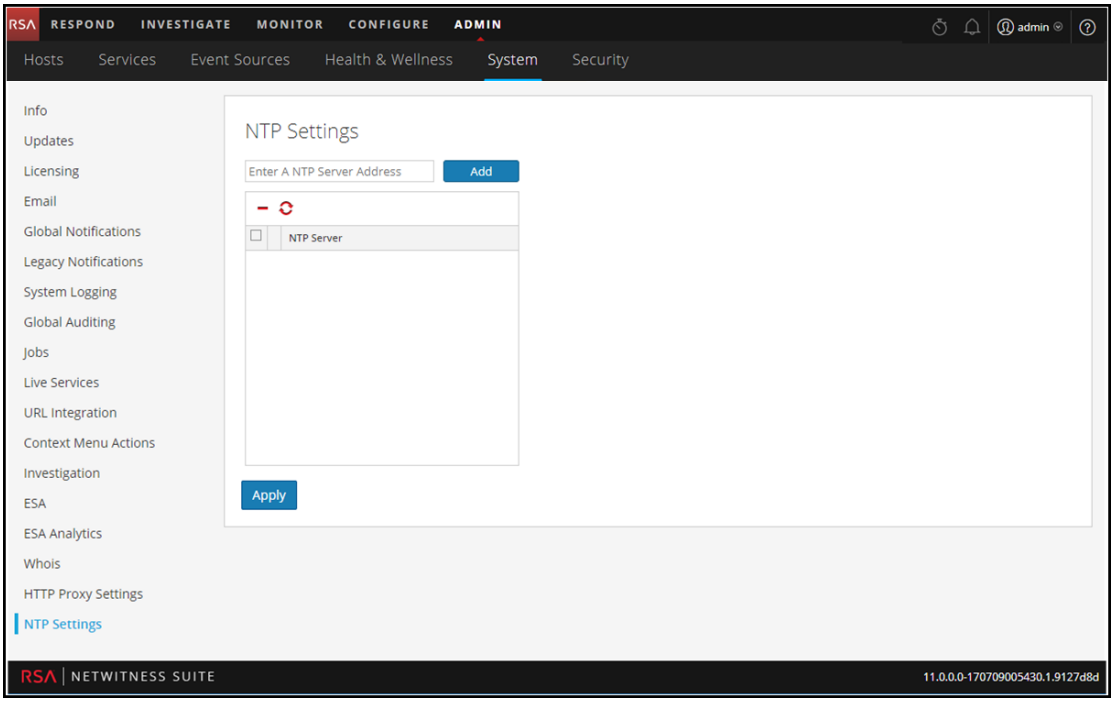
You use the **ADMIN** > **System** > **NTP Settings** view to configure one or more NTP servers. After you configure an NTP server, NetWitness Suite uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes. This topic contains the following procedures:

- Add an NTP Server
- Modify an NTP Server

Add an NTP Server

To add an NTP server:

1. Go to **ADMIN > System**.
2. In the options panel, select **NTP Settings**.
   The NTP Settings panel is displayed prompting you to enter the hostname (that is, the IP Address or FQDN) of an NTP server.



3. Enter the IP address or FQDN for an NTP server.
   If the hostname syntax is invalid, NetWitness Suite disables the **Add** and **Apply** buttons and displays **Entered an invalid hostname**.
4. Click **Add**.
   - If the hostname syntax is valid and NetWitness Suite can reach the server, it displays **Validating**.

- If the hostname syntax is valid and NetWitness Suite cannot reach a server, the following is displayed, where ***hostname*** is the hostname that you attempted to add: **The NTP server *hostname* is unreachable. Please verify the address or check your firewall settings.**

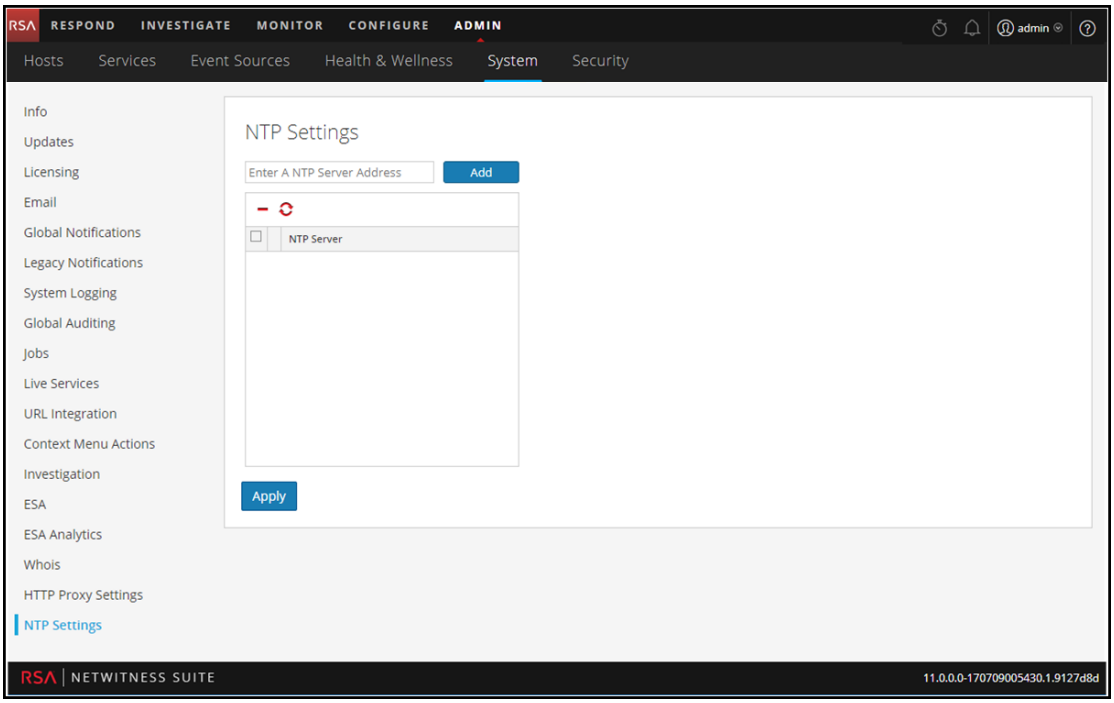
5. Click **Apply**.
   A dialog displays notification that the settings have been saved and requests confirmation that you want to apply the settings now.
6. Click **Yes**.
   The NTP server specified now ensures that your host machine clocks are synchronized. If you decide to configure multiple NTP servers and a server is down, NetWitness Suite will fail over to next server configured.

For details of the parameters and descriptions, see NTP Settings Panel.

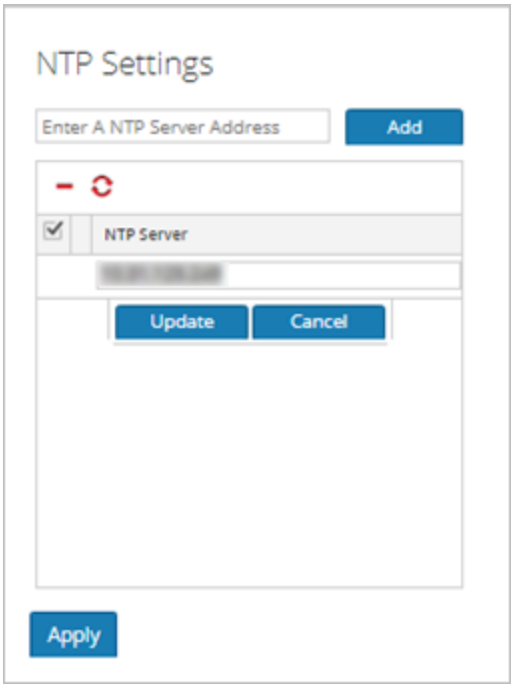
Modify an NTP Server

To modify an existing NTP server:

1. Go to **ADMIN > System**.
2. In the options panel, select **NTP Settings**.
   The NTP Setting panel is displayed.



3. Double-click the **NTP Server** hostname that you want to modify.
   The NTP Server textbox becomes editable and the Update and Cancel buttons are displayed.



4. Edit the hostname, click **Update**, and click **Apply.** (click **Cancel** before you click **Apply** to cancel the edit.)
   NetWitness Suite changes the hostname according to your edits.

Troubleshooting System Configuration

The topics in this section provide troubleshooting information for administrators who are configuring settings that apply across the system in NetWitness Suite.

Troubleshoot Global Audit Logging

Troubleshooting NTP Server Configuration

Troubleshoot Global Audit Logging

This topic provides information about possible issues that NetWitness Suite users may encounter when implementing Global Audit Logging in NetWitness Suite. Look for explanations and solutions in this topic.

After you configure Global Audit Logging, you should test your audit logs to ensure that they show the audit events as defined in your audit logging template. If you cannot view the audit logs on your third-party syslog server or Log Decoder, or the audit logs do not appear as expected, look at the basic troubleshooting suggestions below. If you are still having issues, you can look at the advanced troubleshooting suggestions.

Basic Troubleshooting

If you cannot view audit logs on a third-party syslog server or Log Decoder:

- Verify that RabbitMQ is up and running.
- Verify the syslog notification server configuration and make sure it is enabled. (This configuration is located at ADMIN > System > Global Notifications. Do not select Legacy Notifications.)
- Check the Global Audit Logging configuration.

Configure Global Audit Logging and Verify Global Audit Logs provide instructions. If you are sending audit logs to a Log Decoder:

- Ensure that the Log Decoder is aggregating on the Concentrator on the same host (ADMIN > Services > (Select Concentrator) > > View > Config).
- Verify that the latest CEF parser is deployed and enabled.
- Check the audit logging notification template. You must use a CEF template and all logs feeding into the Log Decoder must use a CEF template.

If you are sending audit logs to a third-party syslog server:

- Ensure that the destination port configured for the third-party syslog server is not blocked by a firewall.

Advanced Troubleshooting

In order to use Global Audit Logging on your network, RabbitMQ must be functioning.

For centralized audit logging, each of the NetWitness Suite services writes audit logs to rsyslog listening on port 50514 using UDP on the local host. The rsyslog plugin provided in the audit logging package adds additional information and uploads these logs to RabbitMQ.
Logstash running on the NetWitness Serverhost aggregates audit logs from all of the NetWitness Suite services, coverts them to the required format, and sends them to a third-party syslog server or Log Decoder for investigation. You configure the format of the global audit logs and the destination used by Logstash through the NetWitness Suite user interface.

Define a Global Audit Logging Configuration provides instructions.

Verify the Packages and Services on the Hosts

NetWitness Suite Host

The following packages or services must be present on the NetWitness Server host:

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-5.6.4
- rsa-audit-plugins
- rabbitmq server

Services on a Host other than the NetWitness Suite Host

The following packages or services must be present on each of the NetWitness Suite hosts other than the NetWitness Server host:

- rsyslog-8.4.1
- rsa-audit-rt
- rabbitmq server

Log Decoder

If you forward global audit logs to a Log Decoder, the following parser should be present and enabled:

- CEF

Possible Issues

What if I perform an action on a service but audit logs do not reach the configured third-party syslog server or Log Decoder?

The possible causes could be one or all of the following:

- A service is not logging to the local syslog server.
- Audit logs are not getting uploaded to RabbitMQ from the local syslog.
- Audit logs are not aggregated on the NetWitness Server host.
- Aggregated logs on the NetWitness Server host are not being forwarded to the configured third-party syslog server or Log Decoder.
- The Log Decoder is not configured to receive global audit logs in CEF format:
  - Log Decoder capture is not turned on
  - CEF Parser is not present
  - CEF Parser is not enabled

Possible Solutions

The following table provides possible solutions for the issues.

Issue	Possible Solutions

A service is not logging to the local syslog server.	• Ensure that rsyslog is up and running.
	You could use the following command:
	`service rsyslog status`
	• Ensure that rsyslog is listening on port 50514 using UDP.
	You could use the following command:
	`netstat -tulnp|grep rsyslog`
	• Ensure the application or component is sending audit logs to port 50514. Run the tcpdump utility on the local interface for port 50514.
	You could use the following command:
	`sudo tcpdump -i lo -A udp and port 50514`
	
	See "Solution Examples" below to view the command outputs.

Issue	Possible Solutions

Audit logs are not getting uploaded to RabbitMQ from the local syslog.	• Ensure that the rsyslog plugin is up and running. You could use the following command:
	`ps -ef|grep rsa_audit_onramp`
	• Ensure the RabbitMQ server is up and running. You could use the following command:
	`service rabbitmq-server status`
	See "Solution Examples" to view the command outputs.

Audit logs are not aggregated on the NetWitness Server host.	• Ensure Logstash is up and running. You could use the following commands:
	`ps -ef|grep logstash`
	`service logstash status`
	• Ensure the RabbitMQ server is up and running. You could use the following command:
	`service rabbitmq-server status`
	• Ensure the RabbitMQ server is listening on port 5672. You could use the following command:
	`netstat -tulnp|grep 5672`
	• Check for any errors generated at the Logstash level. You could use the following command for the location of the log files:
	`ls -l /var/log/logstash/logstash.*`
	See "Solution Examples" to view the command outputs.

Issue	Possible Solutions

Aggregated logs on the NetWitness Server host are not being forwarded to the configured third-party syslog server or Log Decoder.	• Ensure Logstash is up and running.
	You could use the following commands:
	`ps -ef|grep logstash`
	`service logstash status`
	• Check for any errors generated at the Logstash level.
	You could type the following command for the location of the log files:
	`ls -l /var/log/logstash/logstash*`
	See "Solution Examples" below to view the command outputs.
	• Ensure that the destination service is up and running.
	• Ensure that the destination service is listening on the correct port using the correct protocol.
	• Ensure that the configured port on the destination host is not blocked.

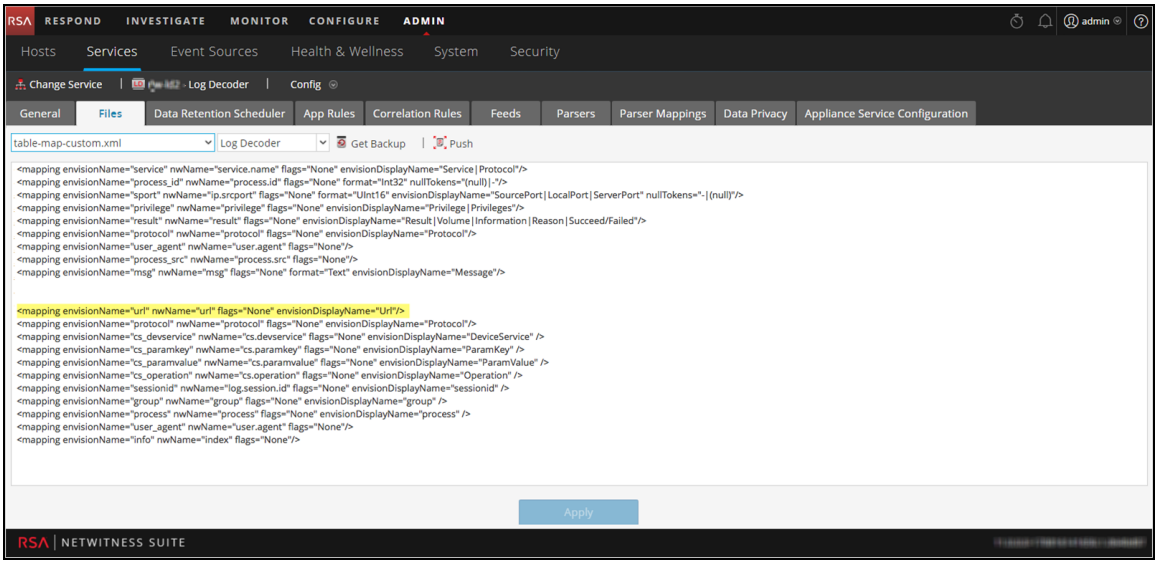
Audit logs forwarded from the Logstash lead to parse failure at the Log Decoder.	• Ensure that you are using an appropriate notification template. Audit Logs parsed by a Log Decoder must be in CEF format. The destination from which audit logs directly or indirectly make their way to the Log Decoder must also use a CEF Template. • The Notification Template must follow the CEF standard. Follow the steps in this guide to either use the default CEF template or create a custom CEF template following strict guidelines. Define a Template for Global Audit Logging provides additional information. • Verify the Logstash configuration.

Why can't we see the custom metadata in Investigation?

Usually, if a meta key is not visible in Investigation, it is not being indexed. If you need to use custom meta keys for Investigations and Reporting, ensure that the meta keys that you select are indexed in the **table-map-custom.xml** file on the Log Decoder. Follow the "Maintain the Table Map Files" procedure to modify the **table-map-custom.xml** file on the Log Decoder.

Ensure that the custom meta keys are also indexed in the **index-concentrator-custom.xml** on the Concentrator. "Edit a Service Index File" provides additional information.

The following figure shows an example **table-map-custom.xml** file in NetWitness Server (ADMIN > Services > (select the Log Decoder) > >View > Config) with a custom meta `url` example highlighted.

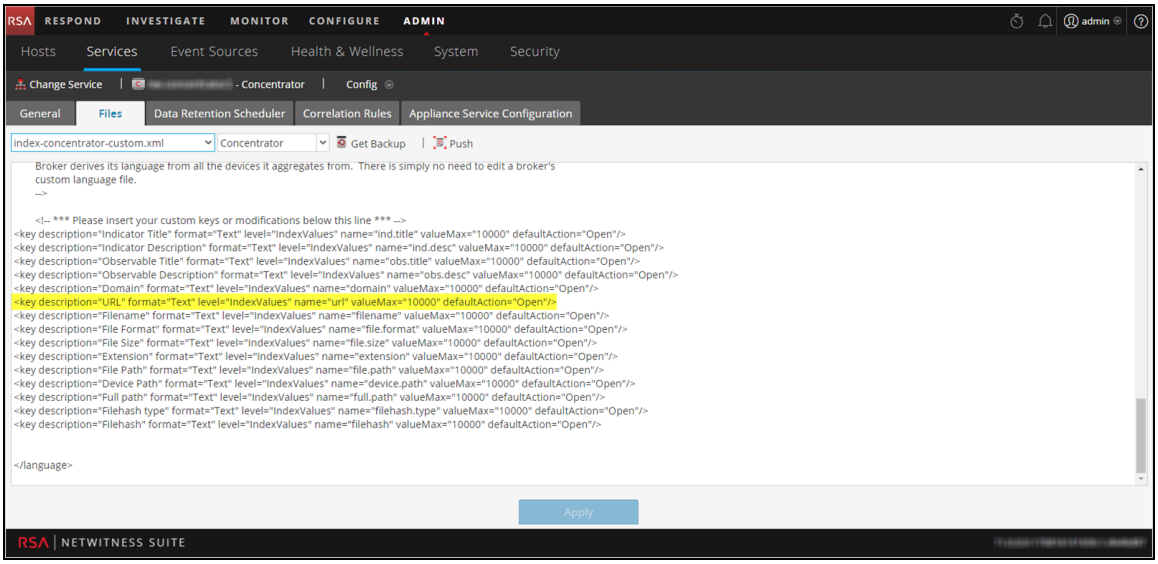


The `url` custom meta example is highlighted in the following code sample from the **table-map-custom.xml** file above:

```
<mapping envisionName="url" nwName="url" flags="None"
envisionDisplayName="Url"/>
<mapping envisionName="protocol" nwName="protocol" flags="None"
envisionDisplayName="Protocol"/><mapping envisionName="cs_devservice"
nwName="cs.devservice" flags="None" envisionDisplayName="DeviceService"
/><mapping envisionName="cs_paramkey" nwName="cs.paramkey" flags="None"
envisionDisplayName="ParamKey" /><mapping envisionName="cs_paramvalue"
nwName="cs.paramvalue" flags="None" envisionDisplayName="ParamValue"
/><mapping envisionName="cs_operation" nwName="cs.operation"
flags="None" envisionDisplayName="Operation" /><mapping
envisionName="sessionid" nwName="log.session.id" flags="None"
envisionDisplayName="sessionid" /><mapping envisionName="group"
```

```
nwName="group" flags="None" envisionDisplayName="group" /><mapping
envisionName="process" nwName="process" flags="None"
envisionDisplayName="process" /><mapping envisionName="user_agent"
nwName="user.agent" flags="None"/><mapping envisionName="info"
nwName="index" flags="None"/>
```

The following figure shows an example **index-concentrator-custom.xml** file in NetWitness Server (ADMIN > Services > (select the Concentrator) > > View > Config) with a custom meta `url` example highlighted.



The `url` custom meta example is highlighted in the following code sample from the **index-concentrator-custom.xml** file above:

```
<key description="Severity" level="IndexValues" name="severity"
valueMax="10000" format="Text"/><key description="Result"
level="IndexValues" name="result" format="Text"/><key
level="IndexValues"  name="ip.srcport" format="UInt16"
description="SourcePort"/><key description="Process" level="IndexValues"
name="process" format="Text"/><key description="Process ID"
level="IndexValues" name="process_id" format="Text"/><key
description="Protocol" level="IndexValues" name="protocol"
format="Text"/><key description="UserAgent" level="IndexValues"
name="user_agent" format="Text"/><key description="DestinationAddress"
level="IndexValues" name="ip.dst" format="IPv4"/><key
description="SourceProcessName" level="IndexValues" name="process.src"
```

```
format="Text"/><key description="Username" level="IndexValues"
name="username"  format="Text"/><key description="Info"
level="IndexValues" name="index"  format="Text"/><key
description="customdevservice" level="IndexValues" name="cs.devservice"
format="Text"/>
<key description="url" level="IndexValues" name="url"  format="Text"/>
<key description="Custom Key" level="IndexValues" name="cs.paramkey"
format="Text"/><key description="Custom Value" level="IndexValues"
name="cs.paramvalue"  format="Text"/><key description="Operation"
level="IndexValues" name="cs.operation"  format="Text"/><key
description="CS Device Service" level="IndexValues" name="cs.device"
format="Text" valueMax="10000" defaultAction="Closed"/>
```

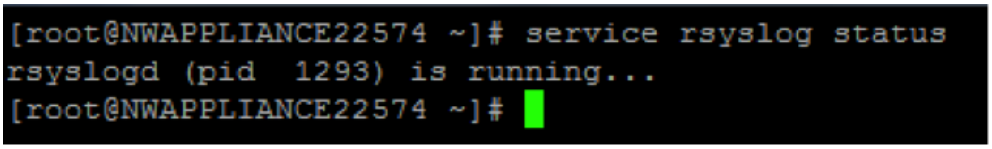
Solution Examples

The following possible solution examples show the outputs of the example commands. See the above table for the complete listing of possible solutions.

Ensure that rsyslog is up and running

You can use the following command:

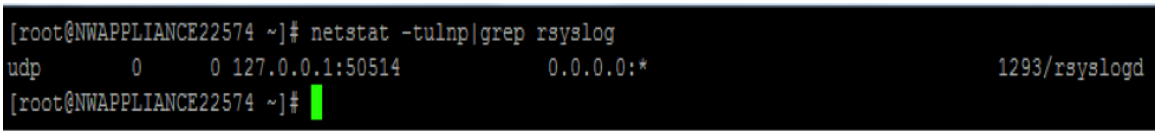
```
service rsyslog status
```



Ensure that rsyslog is listening on port 50514 using UDP

You can use the following command:

```
netstat -tulnp|grep rsyslog
```

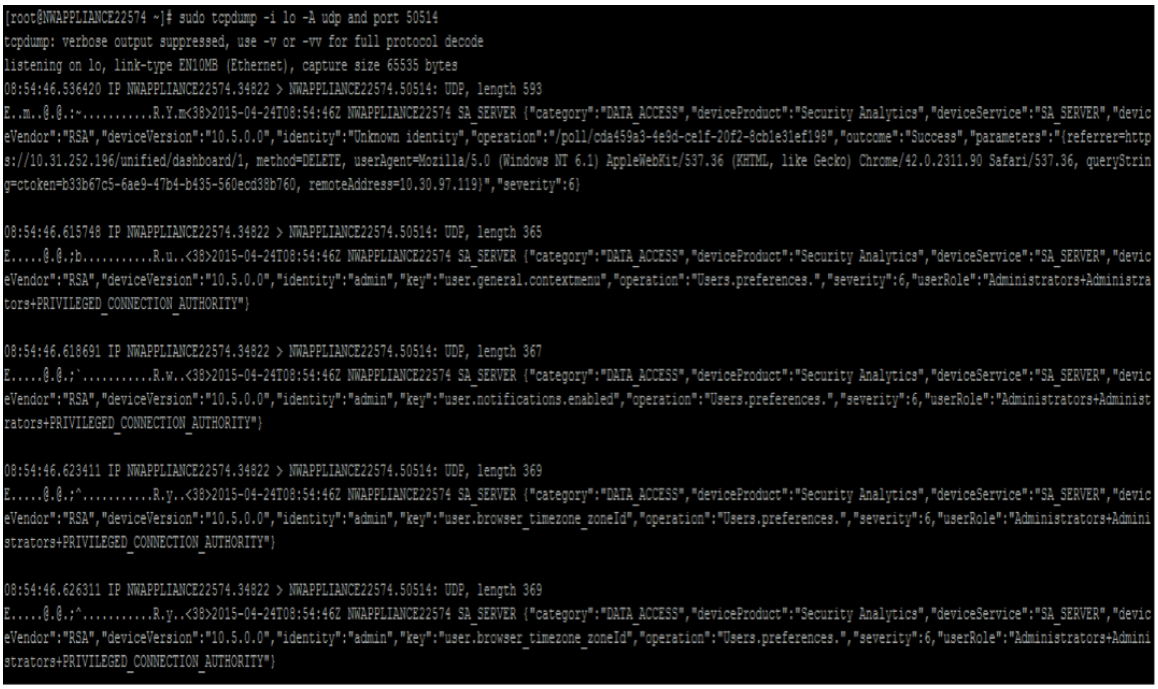


Ensure that the application or component is sending audit logs to port 50514

The following figure shows the output of running the tcpdump utility on the local interface for port 50514.

You can use the following command:

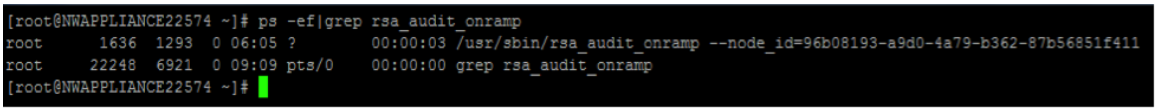
```
sudo tcpdump -i lo -A udp and port 50514
```



Ensure that the rsyslog plugin is up and running

You can use the following command:

```
ps -ef|grep rsa_audit_onramp
```



Ensure the RabbitMQ server is up and running

You can use the following command:

```
service rabbitmq-server status
```

```
[root@NWAPPLIANCE22574 ~]# service rabbitmq-server status
Status of node sa@localhost ...
[{pid,1862},
 {running_applications,
     [{rabbitmq_federation_management,"RabbitMQ Federation Management",
         "3.4.2"},
      {rabbitmq_management,"RabbitMQ Management Console","3.4.2"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.4.2"},
      {webmachine,"webmachine","1.10.3-rmq3.4.2-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.4.2-git680dba8"},
      {rabbitmq_federation,"RabbitMQ Federation","3.4.2"},
      {rabbitmq_stomp,"Embedded Rabbit Stomp Adapter","3.4.2"},
      {rabbitmq_management_agent,"RabbitMQ Management Agent","3.4.2"},
      {rabbit,"RabbitMQ","3.4.2"},
      {ssl,"Erlang/OTP SSL application","5.3.2"},
      {public_key,"Public key infrastructure","0.21"},
      {crypto,"CRYPTO version 2","3.2"},
      {asn1,"The Erlang ASN1 compiler version 2.0.4","2.0.4"},
      {os_mon,"CPO  CXC 138 46","2.2.14"},
      {inets,"INETS  CXC 138 49","5.9.7"},
      {mnesia,"MNESIA  CXC 138 12","4.11"},
      {amqp_client,"RabbitMQ AMQP Client","3.4.2"},
      {rabbitmq_auth_mechanism_ssl,
          "RabbitMQ SSL authentication (SASL EXTERNAL)","3.4.2"},
      {xmerl,"XML parser","1.3.5"},
      {sasl,"SASL  CXC 138 11","2.3.4"},
      {stdlib,"ERTS  CXC 138 10","1.19.4"},
      {kernel,"ERTS  CXC 138 10","2.16.4"}]},
 {os,{unix,linux}},
 {erlang_version,
     "Erlang R16B03 (erts-5.10.4) [source] [64-bit] [smp:2:2] [async-threads:30] [kernel-poll:true]\n"},
 {memory,
```

Ensure logstash is up and running

You can use the following commands:

```
ps -ef|grep logstash
service logstash status
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep logstash
logstash  1583     1  0 06:05 ?       00:01:09 /usr/bin/java -Djava.io.tmpdir=/var/lib/logstash -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Djava.awt.headless=true -XX:C
MSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/jruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
.rb agent --pluginpath /opt/logstash -f /etc/logstash/conf.d -l /var/log/logstash/logstash.log
root      8509  6921  0 09:31 pts/0    00:00:00 grep logstash
[root@NWAPPLIANCE22574 ~]# service logstash status
logstash is running
[root@NWAPPLIANCE22574 ~]#
```

Ensure the RabbitMQ server is listening on port 5672

For example, type the following command:

```
netstat -tulnp|grep 5672
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep 5672
tcp        0      0 127.0.0.1:5672              0.0.0.0:*                   LISTEN      1862/beam.smp
tcp        0      0 0.0.0.0:25672               0.0.0.0:*                   LISTEN      1862/beam.smp
[root@NWAPPLIANCE22574 ~]#
```

Check for any errors generated at the Logstash level

You can type the following command for the location of the log files:

```
ls -l /var/log/logstash/logstash.*
```

```
[root@NWAPPLIANCE22574 ~]# ls -l /var/log/logstash/logstash.*
-rw-r--r--. 1 root     root        0 Apr 24 06:05 /var/log/logstash/logstash.err
-rw-r--r--. 1 logstash logstash 1043 Apr 24 06:04 /var/log/logstash/logstash.log
-rw-r--r--. 1 root     root       57 Apr 24 06:12 /var/log/logstash/logstash.stdout
[root@NWAPPLIANCE22574 ~]#
```

See the Possible Solutions table above for the complete listing of issues and possible solutions.

Troubleshooting NTP Server Configuration

This topic describes NTP server configuration issues that you may encounter and suggests solutions to these problems.

Issues Identified by Messages in the NTP Settings Panel or Log Files

This section provides troubleshooting information for issues identified by messages NetWitness Suite displays in the NTP Settings panel and log files.

Message	User Interface: **Unexpected error occurred. First check the logs then contact Customer Care to resolve error.** **System Log:** **Timestamp Level Message** *yyyy-dd-mmThh:mm:ss:ms* ERROR com.rsa.smc.sa.adm.exception.MCOAgent Exception: No request sent, we did not discover any nodes
Possible Cause	Low level NetWitness Suite configuration is in error or supporting service is not running.
Solution	Contact Customer Care.
Message	User Interface: **Specified an invalid Hostname syntax**.
Possible Cause	Tried to enter NTP server hostname that does not confirm to IP address or FQDN syntax.
Solution	Reenter hostname in using correct syntax.
Message	User Interface: **Specified NTP server that already exists.**
Possible Cause	Tried to enter NTP server hostname that is already defined in NetWitness Suite.
Solution	Enter hostname for an NTP server not configured in NetWitness Suite.
Message	User Interface: **Cannot reach NTP server *hostname***. Please verify the server address and your firewall settings.
Possible Cause	The server address or firewall settings may be in error.

Solution	Verify the server address and your firewall settings and correct them if required.

References

This topic provides reference materials that describe the user interface for configuring system settings in NetWitness Suite and define parameters. Administrators use options in the Administration System view to configure system settings. Each panel is described in a separate topic.

- Global Audit Logging Configurations Panel
- Global Notifications Panel
  - Define Notification Server Dialogs
  - Define Notification Output Dialogs
  - Define Notification Template Dialog
  - Output Tab
  - Servers Tab
  - Templates Tab
- HTTP Proxy Settings Panel
- Email Configuration Panel
- Investigation Configuration Panel
- Live Services Configuration Panel
- NTP Settings Panel
- Context Menu Actions Panel
- Legacy Notifications Configuration Panel

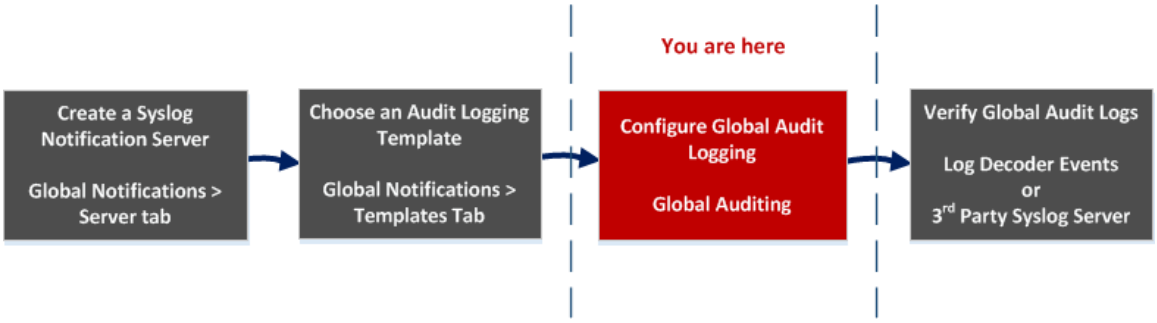
Global Audit Logging Configurations Panel

In the **Global Audit Logging Configurations** panel (ADMIN > System > Global Auditing), you configure global audit logging by adding configurations that define how global audit logs are forwarded to external syslog systems. Global audit logs are forwarded to the selected Notification Server in your global audit logging configuration using the selected Notification Template.

Global Audit Logging provides auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location.

Workflow

This workflow shows the necessary procedures to configure and verify Global Audit Logging.



Before you can define a Global Audit Logging configuration, you need to create a Syslog Notification Server on the Global Notifications > Server tab. The Syslog Notification Server is the destination that receives the global audit logs. Next, you need to select or define an Audit Logging template on the Global Notifications > Templates tab. The Audit Logging template defines the format and message fields of the audit logs sent to the Log Decoder or third-party syslog server. If you are consuming with a Log Decoder, deploy the Common Event Format parser to your Log Decoder from Live.

Note: You do not need to configure the Global Notifications > Output tab for Global Audit Logging.

After you add a Global Audit Logging configuration here, audit logs are forwarded to the selected Notification Server in the configuration. Verify your audit logs to ensure that they show the audit events as defined in your audit logging template.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Create a Syslog Notification Server.	Configure a Destination to Receive Global Audit Logs

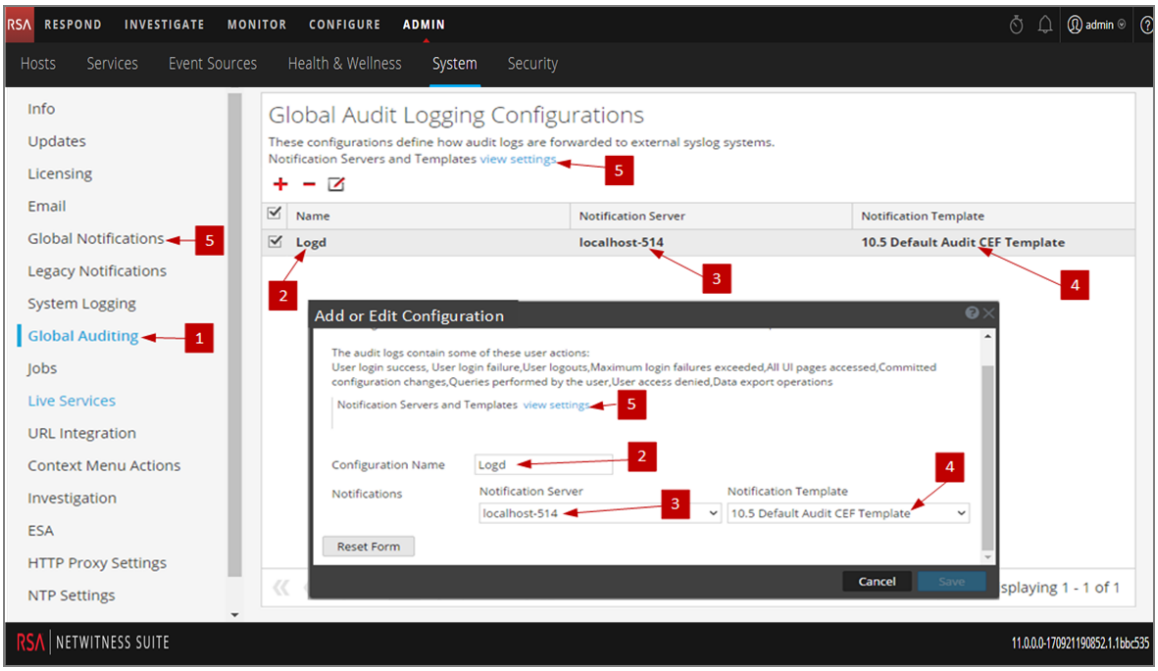
Role	I want to ...	Show me how
Administrator	Choose an Audit Logging template.	Define a Template for Global Audit Logging
Administrator	Configure Global Audit Logging	Define a Global Audit Logging Configuration For the complete procedure, see "Global Audit Logging - High-Level Procedure" in Configure Global Audit Logging.
Administrator	Verify Global Audit logs	Verify Global Audit Logs

Related Topics

- Troubleshoot Global Audit Logging
- Add New Configuration Dialog
- Supported CEF Meta Keys
- Supported Global Audit Logging Meta Key Variables
- Global Audit Logging Operation Reference
- Local Audit Log Locations

Quick Look

The following example illustrates a Global Audit Logging configuration. The configuration defines how NetWitness Suite forwards global audit logs to external syslog systems.



1. Displays the Global Audit Logging Configurations panel.
2. Name that identifies the Global Audit Logging configuration.
3. Notification Server assigned to the Global Audit Logging configuration.
4. Notification Template assigned to the Global Audit Logging configuration.
5. Displays the Global Notifications panel where you set up Servers and Templates required to configure a Global Audit Logging configuration.

Toolbar

The following table describes the toolbar actions

Icon	Description
+	Adds a global audit logging configuration.
−	Deletes a global audit logging configuration. Deleting a global audit configuration does not delete the associated notification server and template. After you delete a global audit logging configuration, the forwarding of global audit logs specified in that configuration is discontinued.

Icon	Description
	Edits a global audit logging configuration. You can change the destination of the global audit logs for your user audits by selecting a different Notification Server. You can also change the format and message fields of the global audit log entries by selecting a different Notification Template. You cannot change which NetWitness Suite user actions are logged and sent in the global audit logs.

Configurations

The following table describes the listed configurations.

Title	Description
	To select an individual configuration, select the checkbox next to the configuration. To select all configurations, select the checkbox in the title bar of the table.
Name	Displays the name of the global auditing configuration. For example, you can name the configurations based on the destination of the global audit logs, such as HQ SA and My Syslog Server.
Notification Server	Displays the Syslog Notification Server selected as the destination for the global audit logs. If you want to forward global audit logs to a Log Decoder, create a Syslog type of Notification Server. Configure a Destination to Receive Global Audit Logs provides instructions on how to create a Syslog Notification Server for global audit logging.

Title	Description
Notification Template	Displays the Audit Logging Notification Template selected for the configuration. It defines the format and message fields of the audit log entries. For Log Decoders, use the **Default Audit CEF Template**. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. Define a Template for Global Audit Logging provides instructions and Supported CEF Meta Keys describes the available CEF meta keys. For, third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). Define a Template for Global Audit Logging provides instructions and Supported Global Audit Logging Meta Key Variables describes the available meta key variables.

Add New Configuration Dialog

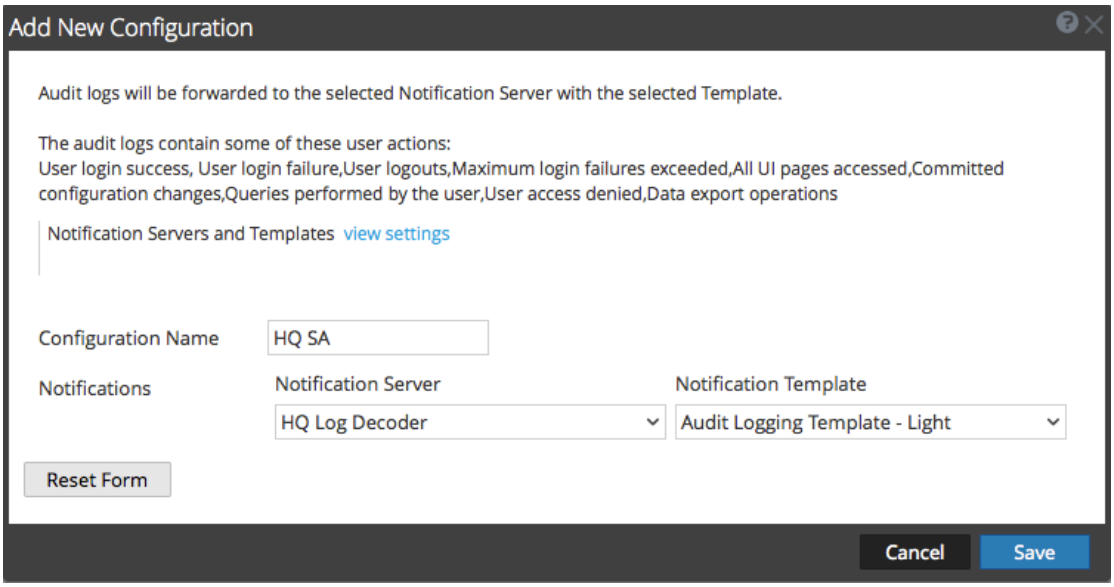
In the RSA NetWitness® Suite Administration System view Global Audit Logging Configurations panel, you can create multiple global audit logging configurations. These configurations are used to forward global audit logs to a central location to perform user audits.

Procedures related to global audit logging are described in Configure Global Audit Logging.

To access the **Add New Configuration** dialog:

1. In the main menu, select **ADMIN > System**.
2. In the options panel, select **Global Auditing**.
3. In the **Global Audit Logging Configurations** panel, click +.

   The **Add New Configuration** dialog is displayed.



The Notifications section enables you to select a syslog notification server for the global audit logging configuration and a template to use for the global audit logs. The template defines the details of the global audit log entries.

Features

The following table describes the features in the Add New Configuration and Edit Configuration dialogs.

Feature	Description
Notifications Servers and Templates **view settings** link	Takes you to the Global Notifications panel where you can view or configure the notification server and template settings. A syslog notification server and an audit logging template are required before you can create a global audit configuration.
Configuration Name	Specifies the unique name used to identify the global audit logging configuration.
Notification Server	Specifies the syslog notification server to send the selected audit log information. Configure a Destination to Receive Global Audit Logs provides instructions on how to create a Syslog Notification Server for global audit logging.
Notification Template	Specifies the template to use for the global audit logging configuration. The template should be an Audit Logging template. For Log Decoders, use the **Default Audit CEF Template**. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. Define a Template for Global Audit Logging provides instructions. For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). Define a Template for Global Audit Logging provides instructions and Supported Global Audit Logging Meta Key Variables describes the available variables.
Reset Form button	Clears the configuration settings in the dialog.

User Actions Logged

The following table provides examples of some of the user actions logged from NetWitness Suite. These actions are the minimum user actions logged when applicable.

User Action	Example
User login success	A user logs on with valid credentials.
User login failure	A user tries to log on using invalid credentials.
User logouts	A user logs out from NetWitness Suite (Administration > Sign Out) or a user logs out due to a session timeout.
Max login failures exceeded	A user tries to log on using invalid credentials five times. Five (5) is the number of Max Login Failures defined in Administration Security view > Settings tab (Administration > Security > Settings tab).
All UI pages accessed	When a user accesses the Reporting module (Administration > Reports), it logs as `[REP] Reports`. When a user accesses the Administration System view (Administration > System), it logs as `[ADM] System`.
Committed configuration changes	A user changes his or her password and or any security setting (Administration > Security > Settings tab).
Queries performed by the user	A user performs an investigation query.
User access denied	A user tries to access a module and does not have permissions to access it.
Data export operations	A user exports data from the Events view (Investigation > Events > Actions > Export).

For lists of message type being logged by the various NetWitness Suite components, see Global Audit Logging Operation Reference.

Supported CEF Meta Keys

This topic describes the Common Event Format (CEF) meta keys that NetWitness Suite global audit logging supports.

Global audit logging templates that you define for a Log Decoder use Common Event Format (CEF) and must meet the following specific standard requirements:

- Include the CEF headers in the template.
- Use only the extensions and custom extensions in a (Key=Value) format from the meta key table below.
- Ensure that the extensions and custom extensions are in the `key=%{string}<space>key=%{string}` format.

For third-party syslog servers, you can define your own format (CEF or non-CEF).

Procedures related to this table are described in Define a Template for Global Audit Logging and Configure Global Audit Logging.

Supported Common Event Format (CEF) Meta Keys

The following table describes the CEF Syslog meta keys that NetWitness Suite global audit logging supports. The Datetime and Hostname fields in the Syslog Prefix are not configurable and not included in the template, but they are prepended to every log message by default. The CEF Header is required to conform to the CEF standard and for any CEF parser. The Extensions and Custom Extensions are optional. The Default Audit CEF Template contains many of the fields in this table. You can add any of the Extensions and Custom Extensions listed to the global audit logging template that you define.

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
Syslog Prefix				
Datetime	Not Configurable	Syslog Header date time	event.time.str	Transient
Hostname	Not Configurable	Syslog Header hostname	alias.host	None

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
CEF Header		The CEF Header fields are required to conform to the CEF standard and for any CEF parser.		
CEF:Version	CEF:0	CEF Header	--STATIC--	N/A
DeviceVendor	%{deviceVendor}	The product vendor, RSA	-	N/A
DeviceProduct	%{deviceProduct}	The product family. This is always NetWitness Suite Audit.	product	Transient
DeviceVersion	%{deviceVersion}	Host/Service version	version	Transient
Signature ID	%{category}	Identifier of the audit event. It specifies the the category of the audit event.	event.type	None
Name	%{operation}	Description of the event	event.desc	None
Severity	%{severity}	Severity of the audit event	severity	Transient
Extensions				

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
deviceExternalId	%{deviceExternalId}	Unique ID of the host or service generating the audit event	hardware.id	Transient
deviceFacility	%{deviceFacility}	Syslog facility used when writing the event to syslog daemon. For example, authpriv.	cs.devfacility	Custom
deviceProcessName	%{deviceProcessName}	Name of the executable corresponding to dvcpid	process	None
dpt	%{destinationPort}	Destination Port	ip.dstport	None
dst	%{destinationAddress}	Destination IP Address	ip.dst	None
dvcpid	%{deviceProcessId}	ID of the process generating the event, which is the process ID of the NetWitness Suite service	process.id	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
msg	%{text}	Free text, extra information, or actual description for the event	msg	Transient
outcome	%{outcome}	Outcome of the operation performed corresponding to the audit event	result	Transient
proto	%{transportProtocol}	Network protocol used	protocol	Transient
requestClientApplication	%{userAgent}	Browser detail of the user accessing the page	user.agent	Transient
rt	%{timestamp}	Time at which the event is reported	event.time	None
sourceServiceName	%{sourceService}	The service that is responsible for generating this event	service.name	Transient
spt	%{sourcePort}	Source Port	ip.srcport	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
spriv	%{userRole}	User role permissions assignment. For example: admin.owner, appliance.manage, connections.manage, everyone, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	privilege	Transient
src	%{sourceAddress}	Source IP Address	ip.src	None
suser	%{identity}	Identity of the logged on user responsible for generating the audit event	user.dst	None
Custom Extensions				
deviceService	%{deviceService}	Service responsible for generating the event	cs.devservice	Custom

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
parameters	%{parameters}	API and Operation parameters, which capture specific parameters about a query	index	Transient
paramKey	%{key}	A configuration item key. It is the config param for which the audit event is captured. For example: /sys/config/stat.interval	cs.key	Custom
paramValue	%{value}	A configuration value. It is the value captured during the update.	cs.value	Custom

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
userGroup	%{userGroup}	Role assignment. For example: Administrators, Analysts, MalwareAnalysts, Malware_Analysts, Operators, PRIVILEGED_CONNECTION_AUTHORITY, SOC_Managers	group	None
referrerURL	%{referrerUrl}	The parent URL that refers to the current URL	url	Transient
sessionId	%{sessionId}	Session or connection identifier	log.session.id	Transient

Note: Use all of the extensions in the following format:
`deviceProcessName=%{deviceProcessName} outcome=%{outcome}`
Include a `<space>` between a value and a tagname.

By default, all meta keys are not indexed. In the above table, the **Index in Log Decoder** column shows the state of the `flags` keyword (Transient, None, and Custom). If a key is set to `Transient`, it is parsed but not stored in the database. If it is set to `None`, it is indexed and stored in the database. A key listed as "Custom" does not exist in the table-map.xml file and, therefore, it is not stored or parsed at all.

"Maintain the Table Map Files" provides instructions for verifying and updating the table mappings. "Edit a Service Index File" provides information on updating the custom index file on the Concentrator.

Supported Global Audit Logging Meta Key Variables

This topic describes the meta key variables that NetWitness Suite global audit logging supports.

NetWitness Suite provides predefined global audit logging templates that you can use for your global audit logging configurations. For third-party syslog servers, you can define your own template format (CEF or non-CEF) using supported meta key variables.

Procedures related to this table are described in Define a Template for Global Audit Logging and Configure Global Audit Logging.

Supported Global Audit Logging Meta Key Variables

The following table describes the meta key variables that NetWitness Suite global audit logging supports. Use these values to create a custom audit logging template for a third-party syslog server.

Variable	Description
%{category}	Identifier of the audit event. It specifies the the category of the audit event.
%{destinationAddress}	Destination IP Address
%{destinationPort}	Destination Port
%{deviceExternalId}	Unique ID of the service generating the audit event
%{deviceFacility}	Syslog facility used when writing the event to syslog daemon. For example, authpriv.
%{deviceProcessId}	ID of the process generating the event, which is the process ID of the NetWitness Suite service
%{deviceProcessName}	Name of the executable corresponding to dvcpid

Variable	Description
%{deviceProduct}	The product family. This is always NetWitness Suite Audit.
%{deviceService}	Service responsible for generating the event
%{deviceVendor}	The product vendor, RSA
%{deviceVersion}	Host/Service version
%{identity}	Identity of the logged on user responsible for generating the audit event
%{key}	A configuration item key. It is the config param for which the audit event is captured.
%{operation}	Description of the event
%{outcome}	Outcome of the operation performed corresponding to the audit event
%{parameters}	API and Operation parameters, which capture specific parameters about a query
%{referrerUrl}	The parent URL that refers to the current URL
%{sessionId}	Session or connection identifier
%{severity}	Severity of the audit event
%{sourceAddress}	Source IP Address

Variable	Description
%{sourcePort}	Source Port
%{sourceService}	The service that is responsible for generating this event
%{text}	Free text, extra information, or actual description for the event
%{timestamp}	Time at which the event is reported
%{transportProtocol}	Network protocol used
%{userAgent}	Browser detail of the user accessing the page
%{userGroup}	Role assignment
%{userRole}	User role permissions assignment
%{value}	A configuration value. It is the value captured during the update

Global Audit Logging Operation Reference

This topic lists message types being logged by the various NetWitness Suite components. Most messages plainly state the operation being logged; when necessary the meaning of the message is explained.

After you create a global audit logging configuration, audit logs automatically go to the external syslog system in the format specified in the selected audit logging template. The message types being logged by the various NetWitness Suite components are shown in the following tables.

CARLOS

The following table lists the operations logged by CARLOS.

Serial #	Operation Name	Meaning
1	SetProviderConfiguration	A new notification server (for example, SMTP server) was added or updated
2	SetInstanceConfiguration	A new notification type (for example, email destination) was added or updated
3	SetTemplateDefinition	A new template was added or updated
4	RemoveProviderConfiguration	A notification server was removed
5	RemoveInstanceConfiguration	A notification type was removed
6	RemoveTemplateDefinition	A template definition was removed
7	Commit	A configuration bean change was committed
8	Set	A JMX property value was set via NetWitness Suite Explore view

ESA

The following table lists the operations logged by the Event Stream Analysis (ESA).

Serial #	Operation Name	Meaning
9	SetSourceRequest	A concentrator was added or updated to ESA as source
10	RemoveSourceRequest	A concentrator was removed from ESA as source
11	SetEplModule	An EPL module was deployed or updated to ESA
12	RemoveEplModule	An EPL module was removed from ESA
13	SetEnrichmentSourceRequest	An ESA enrichment source was added/updated
14	RemoveEnrichmentSourceRequest	An ESA enrichment source was removed
15	SetDatabaseReference	An enrichment database reference was made to ESA
16	UpdateEnrichmentData	Data rows added to an ESA enrichment source
17	SetEnrichmentConnection	A connection was made between an EPL module and an enrichment source
18	RemoveEnrichmentConnection	A connection between an EPL module and an enrichment source was removed
19	DisableTrialModule	ESA Trial rules were disabled

Investigation

The following table lists the operations logged by Investigations.

Serial #	Operation Name	Meaning
1	VisualizePreferences	Operations related to Informer Visualization Request.
2	ParallelCoordinates	Operations related to Loading of Co-Ordinate View Navigation.
3	TimeLine	Operations related to Loading of Timeline View Navigation.
4	ExteralQuery	Operation when a Direct Query is fired via URL.
5	PrintView	Operations to open Investigation in Print View.
6	submitExtractFiles	Operation to submit a Request to Extract files from Sessions.
7	submitExtractLogs	Operation to submit a Request to Extract Logs from Sessions.
8	submitExtractPcap	Operation to submit a Request to Extract Sessions from Sessions.
9	DataScienceDrill	Operation to investigate from Data Science Report.
10	breadCrumbs	Operation to access the Query Breadcumbs.
11	Create	Operation when a new Investigation Query is being saved as a predicate to be used for URL Integration.

Serial #	Operation Name	Meaning
12	userPredicates	Operation to access Recent Queries of a user.
13	chartDefaultMetas	Operation to access last used Meta for generating Coordinate Chart.
14	defaultDevice	Operation to access the Default Investigation Device.
15	deleteDefaultDevice	Operation to delete the Default Investigation Device.
16	chartPreferences	Operation to edit an Investigation Navigation Chart Parameters such as Height.
17	devicePreferences	Operation to save the preferences about the Investigation Device such asTime Range, Profile, Meta Groups etc.
18	topValues	Operation to get the Top Values for Metas. Normally called from Top Values Dashlet.
19	MetaLanguages	Operation to read the Meta Languages from a Device.
20	MetaGroups	Operations related to Investigation Meta Groups.
21	DefaultMetaKeys	Operations related to Investigation Default Meta Keys.
22	UpdateDefaultMetaKeys	Operations to update Investigation Default Meta Keys.

Serial #	Operation Name	Meaning
23	UpdateMetaGroup	Operations to update Investigation Meta Groups.
24	ApplyMetaGroup	Operations to use Investigation Meta Groups.
25	DeactivateMetaGroup	Operations to reset Investigation Meta Groups in UI.
26	DeleteMetaGroup	Operations to remove Investigation Meta Group.
27	DeleteMetaGroups	Operations to remove multiple Investigation Meta Groups.
28	ImportMetaGroups	Operations to import Investigation Meta Groups.
29	ExportMetaGroup	Operations to export multiple Investigation Meta Groups.
30	GeoMap	Operation to access the Geo Map View of Investigation.
31	deleteEndpointCache	Operation to clear Reconstruction Cache of a Device.
32	delete	Operation to delete Alert Templates.
33	CustomColumnGroup	Operation to apply or read Custom Column Group.
34	Import	Operations related to Import of Column Group or Profiles.
35	Export	Operations related to Export of Column Group or Profiles.

Serial #	Operation Name	Meaning
36	SaveProfile	Operation to save an Investigation Profile.
37	ApplyProfile	Operation to apply an Investigation Profile.
38	DeactivateProfile	Operation to deactivate an Investigation Profile.
39	DeleteProfile	Operation to delete an Investigation Profile.
40	DeleteProfiles	Operation to delete multiple Investigation Profiles.

Reporting Engine

The following table lists the operations logged by the Reporting Engine.

Serial #	Operation Name	Meaning
1	TEMPLATE	For all operations related to template
2	CHART	For all operations related to chart
3	REPORT	For all operations related to report
4	RULE	For all operations related to rule
5	IMAGE	For all operations related to Logo Images used in Reports.
6	LIST	For all operations related to list
7	ALERT	For all operations related to alert
8	CONFIG	For all operations related to configuration change

Serial #	Operation Name	Meaning
9	SCHEDULE	For all operations related to schedule
10	ROLE	For all operations related to role/authorization
11	BATCH_JOB	For all operations related to batch jobs
12	SCHEDULER	For all operations related to scheduler
13	QUERYPROCESSOR	For all operations related to queryprocessor
14	FORMATTER	For all operations related to formatter
15	OUTPUTACTION	For all operations related to outputaction
16	STATUSMANAGER	For all operations related to statusmanager
17	BATCH_RUNDEF	For all operations related to batch rundef
18	CHARTGROUP	For all operations related to chart group
19	REPORTGROUP	For all operations related to report group
20	RULEGROUP	For all operations related to rule group
21	LISTGROUP	For all operations related to list group
22	DISKSPACE	For all operations related to disk space

Warehouse Connector

The following table lists the operations logged by the Warehouse Connector.

Serial #	Operation Name	Meaning
1	LockBox Password Create	Operation to create LockBox Password.
2	LockBox Password Update	Operation to update LockBox Password.
3	LockBox Password Refresh	Operation to refresh LockBox Password.
4	Adding Stream	Operation to add a Stream.
5	Adding Source	Operation to add a Source.
6	Adding Destination	Operation to add a Destination.
7	Removing	Operation to remove a Source, Stream, or Destination.
8	Changing Password	Operation to change the Password.
9	Updating Source	Operation to update a Source.
10	Adding Source to Stream	Operation to add a Source to a Stream.
11	Deleting Source from Stream	Operation to delete a Source from a Stream.
12	Setting Destination to Stream	Operation to set a Destination to a Stream.
13	Finalizing Stream	Operation to finalize a Stream and initiate the aggregation.
14	Stopping Stream	Operation to stop a Stream.

Serial #	Operation Name	Meaning
15	Starting Stream	Operation to start a Stream.
16	Reloading Stream	Operation to reload a Stream.

Health & Wellness

The following table lists the operations logged by Health & Wellness.

Serial #	Operation Name	Meaning
1	SavePolicyRequest	Operation while adding or modifying a Policy.
2	RemovePolicyRequest	Operation while removing a Policy.

NetWitness Suite Core Services

The following table lists the operations logged by NetWitness Suite Core Services.

Serial #	Operation Name	Meaning
1	FILE-Command	Operation to list, retrieve and delete files from approved directories on this device.
2	SERVICE-Start	Service started
3	SERVICE-Stop	Service stopped
4	REDIRECT-Syslog	Operation for syslog forwarding.
5	ADD-Monitor	Issuing a filesystem monitor operation
6	DELETE-Monitor	Issuing a filesystem monitor deletion operation
7	SHUTDOWN-Service/shutdown.service	Shutting down appliance service
8	REBOOT-Service	Restarting appliance service

Serial #	Operation Name	Meaning
9	CONFIGURE-Network	Issuing Network Configuration change
10	SET-NTP	Issuing NTP set operation
11	STOP-NTP	Issuing NTP stop operation
12	NTP-Timesync	Issuing NTP time sync operation
13	SET-SNMP	Issuing SNMP set
14	UPGRADE/upgrade	Issuing upgrade operation
15	create.collection	Operation to create an empty collection.
16	restore	Issuing restore
17	session.aggregation	Issuing aggregation start/stop
18	add.device	Adding a device for aggregation
19	edit.device	Editing a device used for aggregation
20	delete.device	Deleting a device used for aggregation
21	capture.start	Starting capture operation
22	capture.stop	Stopping capture operation
23	select.interface	Selecting capture interface
24	export	Operation to export packets or sessions.
25	reload	Issuing a parser reload
26	schema	Issuing a schema request for loaded parsers
27	upload/file.upload	Issuing file upload

Serial #	Operation Name	Meaning
28	notify	Issuing feed notify
29	delete	Issuing file deletion
30	edit.config	Configuration change operation
31	parsers.transforms	Perform a language key transformation
32	data.reset	Data reset operation
33	timeout	REST request timeout
34	cancel	Cancel a running query
35	timeroll	Operation to delete the database files that exceed a given limit.
36	dump	Operation to dump information out of the database in nwd formatted files.
37	session.wipe	Issuing a session wipe operation
38	REPLACE-Rule	Issuing a rule replace operation
39	MERGE-Rule	Issuing a rule merge operation
40	ERASE-Rule	Issuing deletion of a set of all rules
41	ADD-Rule	Issuing a rule addition operation
42	DELETE-Rule	Issuing deletion of a set of rules
43	sdk.info	Issuing SDK summary info.
44	sdk.session	Issuing SDK session info.
45	sdk.language	Issuing SDK language
46	sdk.aliases	Issuing SDK alias request

Serial #	Operation Name	Meaning
47	sdk.transform	Issuing SDK transformation request
48	sdk.search	Issuing session content search request
49	sdk.cache	Operation related to session content cache
50	sdk.content	Issuing session content request
51	check.authorization	Operation to check user roles for permissions to execute an operation.
52	close.connection	Issuing a connection close operation
53	handshake	Issuing an SSL handshake
54	logon/login	Operation to login from NW to the other services, mostly to privileged users.
55	STOREDPROCOP	Issuing file upload cancel/start
56	ADD-Task	Added scheduled task
57	DELETE-Task	Deleted scheduled task
58	logoff	Issuing logout operation
59	list.cacerts	Issuing list trusted CA certificate operation
60	delete.cacerts	Issuing delete trusted CA certificate operation
61	add.cacerts	Issuing addition of trusted CA certificate operation
62	restart.command	Issuing restart command line option

Serial #	Operation Name	Meaning
63	delete.file/file.delete	Operation to delete system configuration files.
64	update.file/file.update	Operation to update system configuration file.
65	create.file	Issuing file creation operation
66	query	Issue a database query
67	unlock	Issuing unlock user account operation
68	user.add	Operation to create user accounts on individual devices.
69	user.delete	Operation to delete a user on individual devices.
70	group.create	Operation to add a new group to the system.
71	user.remove	Remove a user account from a group
72	group.delete	Delete a group from the /users/groups tree
73	add.user	Issuing add user command to collection
74	delete.user	Issuing delete user command to collection
75	remove.user	Removing an user from collection
76	collection.open	Issuing an open command for a collection

Serial #	Operation Name	Meaning
77	collection.close	Issuing a close command for a collection
78	collection.delete	Issuing collection deletion command
79	reingest.start	Operation to start reingesting of packet data in collection.
80	feed.notify	Issuing a feed notify command
81	collect	Issuing a collect command
82	collect.start	Issuing a data collection start
83	collection.global	Issuing import parser command
84	parser.reload	Issuing parser reload command
85	reingest	Operation to reingest packet data in collection.
86	collection.create	Issuing a create collection command
87	collection.restore	Issuing a restore collection command
88	collection.clone	Issuing a clone collection command
89	parser.reload	Issuing parser reload command
90	sdk.query	Performs a query against the meta database
91	sdk.msearch	Search for pattern matches in many sessions or packets
92	sdk.values	Performs a value count query and returns the matching values for a report

Serial #	Operation Name	Meaning
93	sdk.timeline	Returns the count of sessions/size/packets in discrete time intervals

Malware Analysis

The following table lists the operations logged by the Malware Analysis (MA) component.

Serial #	Operation Name	Meaning
1	GetDashBoardSummaryRequest	Get dashboard analysis statistics
2	GetFileScoreSummaryRequest	Get aggregated file scores by score type and risk level
3	CountEventsAndFilesRequest	Get count of events and files over a time frame
4	GetAvVendorDetectionRequest	Get AV vendor analysis results
5	GetAVVendorsRequest	Get list of AV Vendors supported
6	SetInstalledAVVendors	Request Update list of installed AV Vendors in config
7	CountEventByCriteriaRequest	Count events by criteria
8	FindEventByIdRequest	Get event by id
9	FindEventByCriteriaRequest	Get event by criteria
10	DeleteEventRequest	Delete event
11	CommentOnEventRequest	Add comment to event
12	ReSubmitEventRequest	Resubmit event for analysis
13	FindEventScoreByIdRequest	Get event score by event id

Serial #	Operation Name	Meaning
14	FindEventScoreByCriteriaRequest	Get event score by criteria
15	FindMetaByIdRequest	Get meta by id
16	FindMetaByCriteriaRequest	Get meta by criteria
17	FindMetaValueByCriteriaRequest	Get meta value by criteria
18	CountByDistinctMetaValueRequest	Count distinct meta values
19	CountByMetaNameAndValueWithDate RangeIntervalRequest	Count meta and values with interval for charting
20	CountByValueAndAverageOverallScore Request	Count meta and map to overall scores for events
21	CountByValueAndAverageGroupScore Request	Count meta and map to group scores for events
22	CountFileEntryByCriteriaRequest	Count files by criteria
23	FindFileEntryByIdRequest	Get file by id
24	FindFileEntryByCriteriaRequest	Get file by criteria
25	ReSubmitFileEntryRequest	Resubmit file for analysis
26	FileDownloadRequest	Download file from repository
27	FileUploadRequest	Upload file for analysis
28	FindFileScoreByIdRequest	Get file score by id
29	FindFileScoreByCriteriaRequest	Get file score by criteria
30	FindHashValueByIdRequest	Get whitelist/blacklist Hash value by id
31	FindHashValueByCriteriaRequest	Get whitelist/blacklist Hash value by criteria
32	AddHashValueRequest	Add whitelist/blacklist Hash value

Serial #	Operation Name	Meaning
33	UpdateHashValueRequest	Update whitelist/blacklist Hash value
34	DeleteHashValueRequest	Delete whitelist/blacklist Hash value
35	FindHashValueByMd5Request	Find whitelist/blacklist Hash value by md5
36	AddHashValueInFileRequest	Add File to repository as well as hash value
37	GetDefaultRulesRequest	Get default IOC Rules configuration
38	ResetToDefaultRulesRequest	Reset IOC Rules configuration to default
39	GetAllOverrideRulesRequest	Get IOC Rules user created override configuration
40	FindOverrideRuleByIdRequest	Find IOC override rule by id
41	AddOverrideRuleRequest	Add IOC override rule
42	UpdateOverrideRuleRequest	Update IOC override rule
43	DeleteOverrideRuleRequest	Delete IOC override rule
44	SubmitOnDemandNextGenRequest	Submit new ondemand nextgen scan
45	FindOnDemandJobEntryByIdRequest	Get ondemand job entity by id
46	FindOnDemandJobEntryByCriteria Request	Get ondemand job entity by criteria
47	GetOnDemandJobInfoRequest	Get ondemand job reference entity by id
48	GetOnDemandDefaultConfiguration	Request Get ondemand default configuration

Serial #	Operation Name	Meaning
49	CancelOnDemandJobRequest	Cancel ondemand job in progress
50	DeleteOnDemandJobRequest	Delete ondemand job
51	ReSubmitOnDemandJobRequest	Resubmit ondemand job
52	SubscriptionRequest	Subscribe to MA Cloud communication
53	UnSubscribeRequest	Unsubscribe from MA Cloud communication
54	GetTopEventInfluencesRequest	Get Top N event influences
55	GetServerInfoRequest	Get server info, such as server time
56	DataResetRequest	Reset database
57	OnDemandJobStatusNotification	Report ondemandjob progress to subscribers
58	LicenseStatusNotification	Report license status - num samples analyzed
59	DataResetNotification	Report that data was reset
60	GetIocSummaryRequest	Get IOC rules aggregated by event/file scores
61	FindAlertTemplatesByCriteriaRequest	Get rabbitmq alert templates by criteria
62	SaveAlertTemplateRequest	Update alert template
63	DeleteAlertTemplateRequest	Delete alert template
64	GetJobStatusRequest	Get in progress job analysis thread status
65	GetEventTypeCountSummaryRequest	Get event analysis counts by date chart

Serial #	Operation Name	Meaning
66	Logon	Logon to the MA Service
67	Modified	Modifying config changes
68	GetNextGenSummaryRequest	Get nextgen dashboard summary statistics

NetWitness Suite User Interface

The following table lists the operations logged by the NetWitness Suite User Interface component.

Serial #	Operation Name	Meaning
1	uploadTrialLicense	Upload Trial License
2	LicenseEntitle	Entitle License
3	LicenseDeactivation	Deactivate License
4	ExpiredLicense	License Expired
5	LicenseOutOfComplianceAcknowledgement	EULA Acknowledgement
6	resetLicense	Reset License
7	usageDateExport	License data usage - csv/pdf
8	refreshLicense	Refresh LLS license
9	LicenseOutOfCompliance	Out of Compliance
10	OOTBEntitlementOutOfCompliance	OOTB Trial license Out of Compliance
11	OOTBEntitlementFirstLoginTimeModified	OOTB time modified
12	OOTBEntitlementFileDeleted	OOTB File deleted
13	OOTBEntitlementDataTampering	OOTB data tampering

Serial #	Operation Name	Meaning
14	uploadOfflineResponse	Upload offline response
15	offlineDownloadCapRequest	Download offline request
16	movePerpetualToMetered	Move Service-based license to Metered
17	moveMeteredToPerpetual	Mover Metered to Service-based license
18	mapServiceLicense	Map Service to Real license
19	delete	Operation to delete Alert Templates.
20	HttpRequest	Operation for Audit Logging of the accessed URL.
21	Page Accessed	Operation for Audit Logging of the accessed page.
22	Navigate	Operation to navigate to the accessed page.
23	Events	Operation to view the accessed event page.
24	Recon	Operation for Event Reconstruction requested.
25	Services	Operation while reading the list of available devices for investigation.
26	Service	Operation for a List of devices requested to be investigated.

Serial #	Operation Name	Meaning
27	Collections	Operation to view the list of collections requested.
28	Profiles	Operation to apply a Profile.
29	ColumnGroups	Operation to apply or read Column Group.
30	ParallelCoordinates	Operations related to Loading of co-ordinate view navigation.
31	Timeline	Operations related to loading of timeline view navigation.
32	PrintView	Operations to open investigation in print view.
33	Preferences	Operations related to Informer Request.
34	import	Operations related to Import of Column Group or Profiles.
35	export	Operations related to Export of Column Group or Profiles.
36	Predicate	Operations related to Queries (Predicates) used for Investigation.
37	Languages	Operation for Language requested from a Device.
38	CancelLanguageLoad	Operation for Language Load Canceled from Navigate Page.

Serial #	Operation Name	Meaning
39	summary	Operation for a summary requested from a Device.
40	languages	Operation for a language requested from a device.
41	aliases	Operation for meta aliases requested from a device.
42	query	Operation for SDK Query requested from a device.
43	msearch	Operation for a meta search requested from a device.
44	nodeListing	Node Listing for a node requested from a Device.
45	content	SDK Content call requested from a Device for downloading a PCAP or Log.
46	Export Files	File Listing Requested for a Session in File View or Extraction jobs.
47	packets	Packets requested for sessions in Packet View or Extraction Jobs.
48	deleteEndpointCache	Operation to clear reconstruction cache of a device.

Serial #	Operation Name	Meaning
49	Logon	Operation for user to sign in to NetWitness Suite User Interface.
50	Logoff	Operation for user to sign out of NetWitness Suite User Interface.
51	defaultDevice	Operation to access the Default SA UI Device.
52	deleteDefaultDevice	Operation to delete the Default investigation device.
53	submitExtractFiles	Operation to submit a request to Extract files from Sessions.
54	submitExtractLogs	Operation to submit a Request to Extract Logs from Sessions.
55	submitExtractPcap	Operation to submit a Request to Extract Sessions from Sessions.
56	MetaGroup	Operations related to SA UI Meta Groups.
57	ExternalQuery	Operation when a Direct Query is fired via URL.
58	GeoMap	Operation to access the Geo Map View of Investigation.
59	SaveProfile	Operation to save an Investigation Profile.

Serial #	Operation Name	Meaning
60	ApplyProfile	Operation to apply an Investigation Profile.
61	DeleteProfile	Operation to apply an Investigation Profile.
62	DeactivateProfile	Operation to apply an Investigation Profile.
63	VisualizePreferences	Operations related to Informer Visualization Request.
64	ExportMetaGroup	Operations to export multiple SA UI Meta Groups.
65	userPredicates	Operations to export multiple SA UI Meta Groups.
66	FileView	Operation for reconstruction request for File View.
67	resource.update	Operation when Live Subscription State changes.

Respond

The following table lists the operations logged by the RESPOND component.

Serial #	Operation Name	Meaning
1	update	Update notification setting
2	update	Update integration settings configuration
3	delete	Delete Alerts
4	create	Create new incident

Serial #	Operation Name	Meaning
5	update	Update incident details
6	read	Read incident details
7	delete	Delete incidents
8	read	Read remediation tasks
9	delete	Delete Remediation tasks
10	update	Update remediation tasks
11	create	Create new rule
12	update	Update existing alert rule
13	reorder	Reorder priority of alert rules

Security Server

The following table lists the events logged by the Security Server.

Log Category	Description
Authentication:	Logs events pertaining to user logins and logouts.
Authorization:	Logs events pertaining to user access checks and RBAC management.
UserAccount	Logs events pertaining to NetWitness Suite domain account management.
ExternalProvider:	Tracks events pertaining with external account providers (for example, Active Directory).

The following example shows an event logged by the Security Server:

```
2018-03-13 16:25:02,938 UserAccount{action=ExpirePassword, success=true,
identity=admin, parameters={id=Justin}}
```

Local Audit Log Locations

NetWitness Suite has global audit logging capabilities. When you configure global audit logging, audit logs from all NetWitness Suite components collect in a centralized system, which converts them into the required format and forwards them to a third-party syslog server or a Log Decoder.

To view audit logs from the individual services, you can look at the local audit log locations.The following table shows the local directory paths of the audit logs for the NetWitness Suite user interface and the various NetWitness Suite services.

Service/Module	Audit Log Location
NetWitness Suite User Interface (NetWitness Suite Web Server)	The NetWitness Suite user interface sends audit logs to the following locations: • `/var/lib/netwitness/uax/logs/audit/audit.log` (human-readable format) • Syslog running on the local host (JSON format) The NetWitness Suite user interface uses the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (`/var/lib/netwitness/uax/logs/audit/audit.log`).
Core Services (Decoder, Log Decoder, Concentrator, Broker, and Archiver), Log Collector, Warehouse Connector, and Workbench	The Core services and similar services send audit logs to Syslog running on the local host. Path: `/var/log/secure` (JSON format) The Core services use the AUTHPRIV facility of syslog to write audit logs to syslog.

Service/Module	Audit Log Location

Reporting Engine, Malware Analysis, Respond, and Event Stream Analysis (ESA)	These services send audit logs to the following locations:
	• `<application-home-directory>/logs/audit/audit.log` (human-readable format)
	• Syslog running on the local host (JSON format)
	
	The following are the audit log locations of these services:
	Reporting Engine:
	`/var/netwitness/re-server/rsa/soc/reporting-engine/logs/audit/audit.log`
	Respond Server:
	`/var/log/netwitness/respond-server/respond-server.audit.log`
	Malware Analysis:
	`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`
	Event Stream Analysis:
	`/opt/rsa/esa/logs/audit/audit.log`
	These services use the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (`<application-home-directory>/logs/audit/audit.log`).

Health & Wellness, Event Source Management (ESM), and Appliance and Service Grouping (ASG)	These Services send audit logs to the following locations: • `/opt/rsa/sms/logs/audit/audit.log` (human-readable format) • Syslog running on the local host (JSON format) These services use the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (`/opt/rsa/sms/logs/audit/audit.log`).

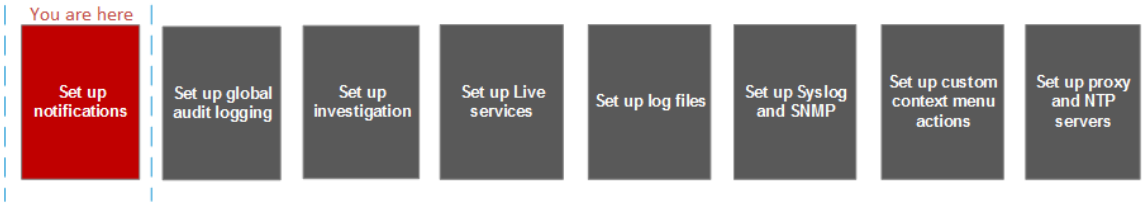
Global Notifications Panel

Global Notifications panel introduces the features for configuring notification settings. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

In the Global Notifications panel, you can configure the following global notification settings:

- Notification Outputs
- Notification Servers
- Templates

WorkFlow



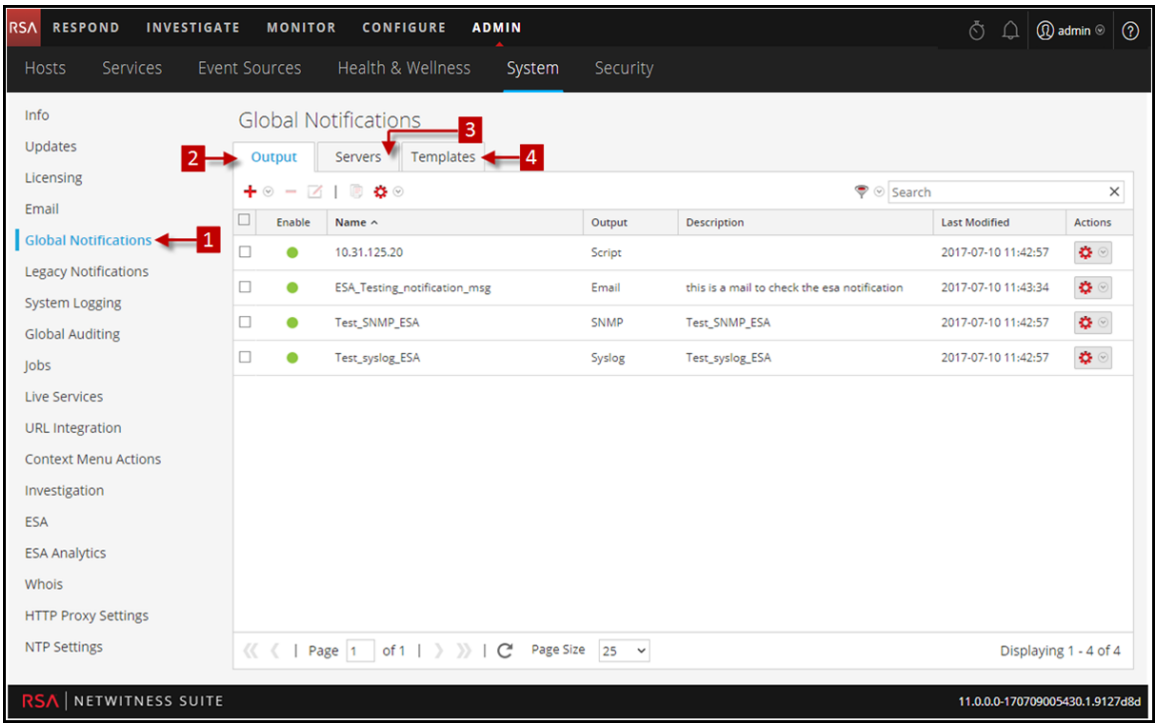
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Notification Servers	Servers Tab
Administrator	Configure Notification Outputs	Output Tab
Administrator	Configure Notification Templates	Templates Tab

Related Topics

- Configure a Syslog Notification Server
- Configure Script as a Notification Server

Quick Look



1 Displays the Global Notification Panel.

2 Displays the Output Tab

3 Displays the Servers Tab

4 Displays the Templates Tab

Toolbar and Features

The Global Notifications panel has three tabs: Output, Servers, and Templates.

Feature	Description
Output tab	This tab enables you to configure notification outputs. See Output Tab for more information.
Servers tab	This tab enables you to configure notification servers. See Servers Tab for more information.
Templates tab	This tab enables you to configure notification templates. See Templates Tab for more information.

This table describes the columns in the grid for Notification Outputs and Notification Servers.

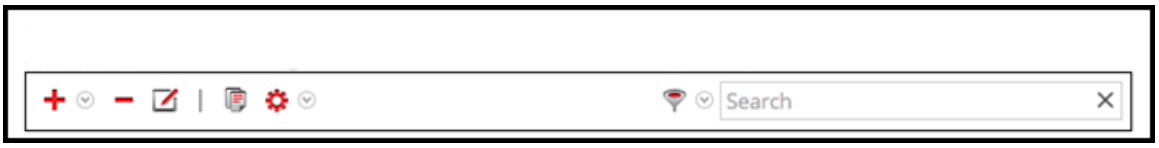
Column	Description
	Selects a row for an action in the toolbar. Clicking the checkbox in the column title selects or deselects all rows in the grid.
Enable	Indicates whether the configuration is enabled. A solid colored green circle indicates that a configuration is enabled. A blank white circle indicates that a configuration is not enabled.
Name	A name that identifies or labels the configuration.
Output	The configuration output. The outputs are Email, SNMP, Syslog, and Script.
Description	A brief description about the configuration.
Last Modified	Shows the date and time of the last configuration change.
Actions	Provides an Actions menu for the selected configuration with actions that can be taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

This table describes the columns in the grid for Notification Templates.

Column	Description
	Selects a row for an action in the toolbar. Clicking the checkbox in the column title selects or deselects all rows in the grid.
Name	A name that identifies or labels the template.
Template Type	The type of template. The types are Audit Logging, Event Stream Analysis, Event Source Monitoring, and Health Alarms.
Description	A brief description about the template.
Actions	Provides an Actions menu for the selected configuration with actions that can be taken on the template. The Actions menu enables you to delete, edit, duplicate, and export the template.

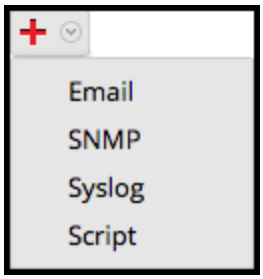
Global Notifications Panel Toolbar

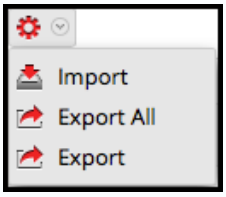
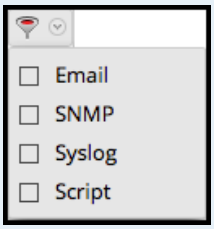
The Global Notifications panel toolbar is at the top of the Output, Servers, and Templates tabs. The following figure shows the toolbar on the Output and Servers tabs.



The following figure shows the toolbar on the Templates tab.

The following table describes the features of the Global Notifications panel toolbar.

Feature	Description
	Adds a notification server on the Servers tab, adds a notification output (notification) on the Output tab, and adds a notification template on the Templates tab. On the Servers and Output tabs, you can select to configure Email, SNMP, Syslog, and Script notification settings.
	Removes a selected notification configuration. You cannot delete notification servers and notification types that are associated with global audit log configurations. If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use. You can also delete a configuration by selecting a configuration and then in the Actions column, selecting > Delete.

Feature	Description
	Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting > Edit.
	Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting > Duplicate.
	Displays the following options: • **Import**: Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration. • **Export All**: Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations. • **Export**: Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting > Export.
	Filters by Email, SNMP, Syslog, or Script.
	Searches configurations in the grid.

Define Notification Server Dialogs

This topic describes the Define Notification Server dialogs used to configure the settings of the various types of notification servers. You configure notification servers in the ADMIN > System > Notifications > Servers tab.

Notifications are used by a variety of components in NetWitness Suite, such as Event Stream Analysis (ESA), Respond, and Global Audit Logging. Notification settings are called Notification Servers. In the Servers tab of the Administration System view Notifications panel, you can create multiple Notification Server configurations.

You can configure the following types of notification server settings in NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

For Global Audit Logging, you can only use Syslog Notification Servers.

Procedures related to notification servers are described in Configure Notification Servers.

To access the Define Notification Server dialogs:

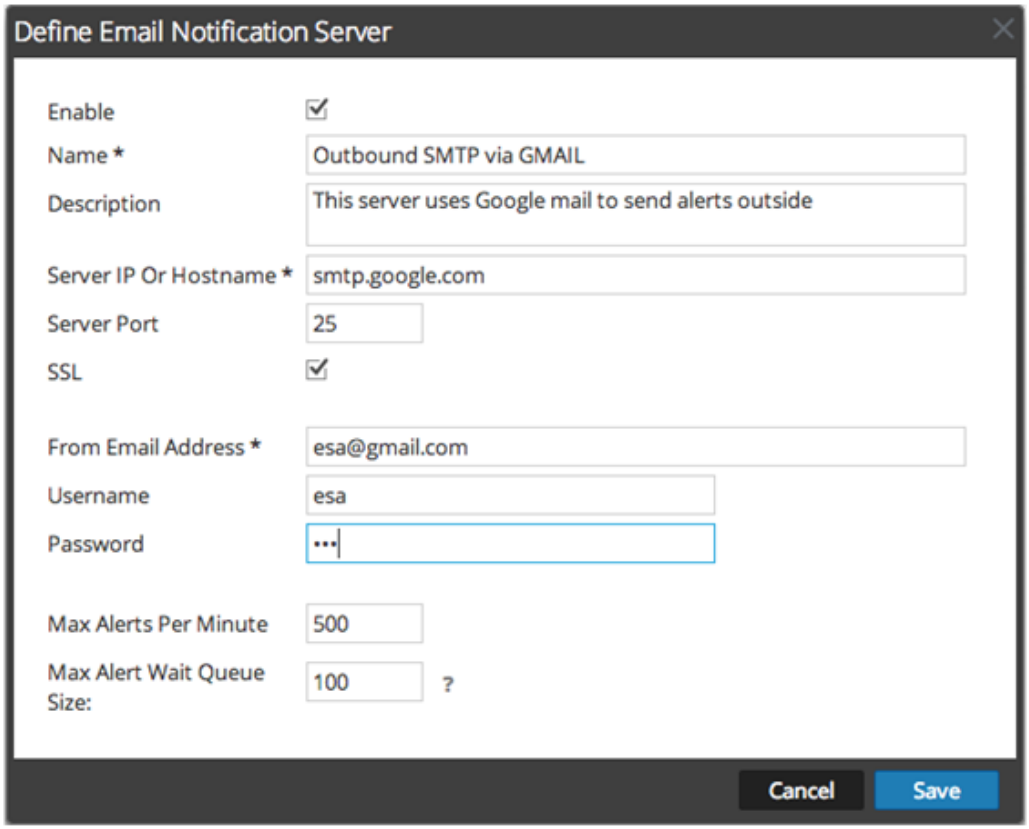
1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Global Notifications**.
3. In the **Notifications Servers** panel, click + and then select a type of notification server (Email, SNMP, Syslog, or Script)
   The Define Notification Server dialog is displayed for your selection.

There are four notification server dialogs, which allow you to configure notification servers.

Email

Email notification servers enable you to configure email server settings to send alert notifications.

The following figure shows the Define Email Notification Server dialog.



The following table lists the various parameters that you need to define for the email notification servers.

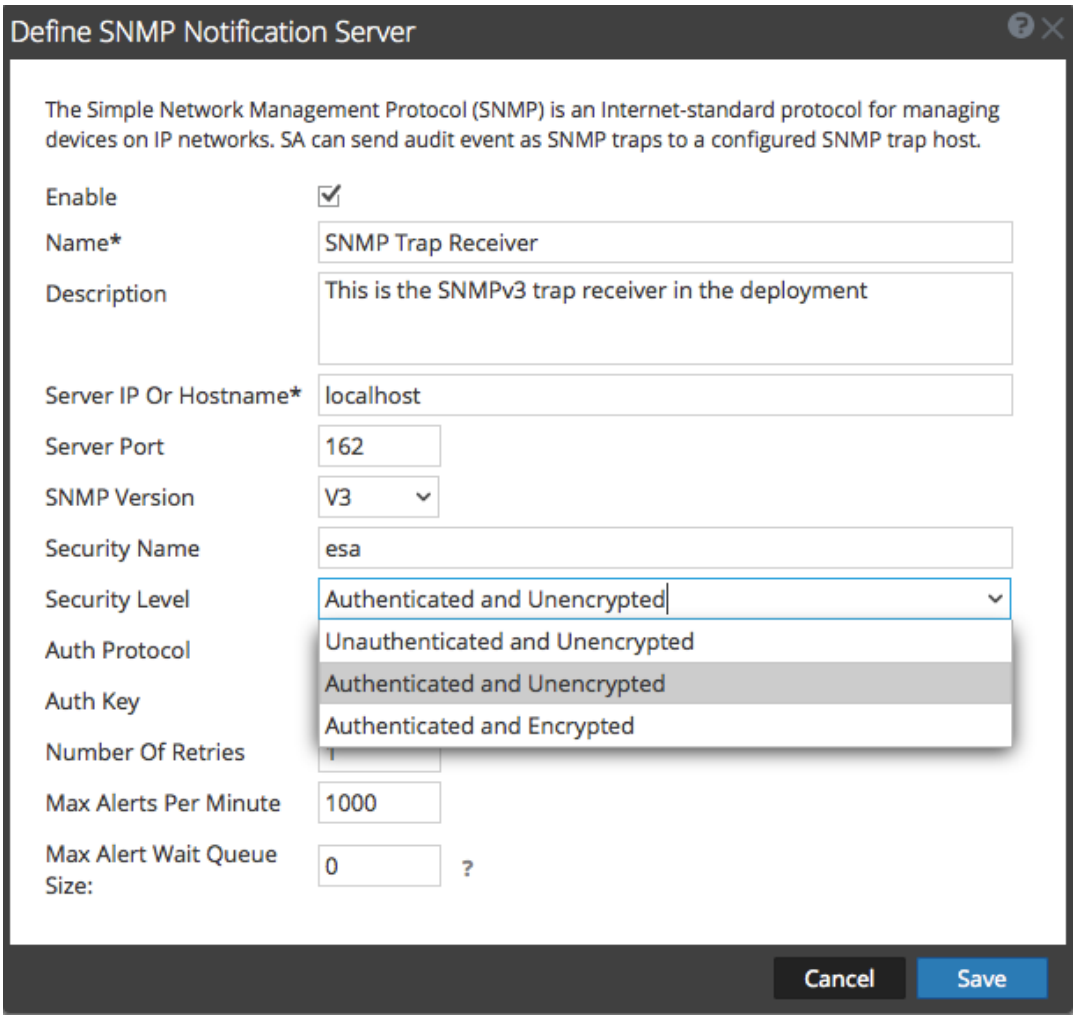
Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	Hostname of the email server. For ESM/SMS and ESA notifications, you must specify only the hostname/FQDN.
Server Port	The server port.

Parameters	Description
SSL	Select the option if you want the communication to happen through SSL.
From EMail Address	Email account from which you want to send email notifications.
Username	Username for logging into the email account if the SMTP server requires user authentication to relay emails successfully.
Password	User password for logging into the email account if the SMTP server requires user authentication to relay emails successfully.
Max Alerts Per Minute	Describes the maximum number of alerts per minute.
Max Alert Wait Queue Size	Describes the maximum number of alerts to be queued before they are dropped.

SNMP

SNMP notification servers enable you to configure SNMP trap host settings as a notification server to send alert notifications.

The following figure shows the Define SNMP Notification Server dialog.



The following table lists the various parameters that you need to define for the SNMP notification servers.

Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	SNMP trap host IP address or hostname.

Parameters	Description
Server Port	Listening port number on the SNMP trap host.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>SNMP Version</td><td>SNMP version. The following are the options:
V1
V2C
V3
If you select SNMP Version 3 (v3), the following parameters are displayed:

<table><tr><th>Parameters</th><th>Description</th></tr><tr><td>Notification Type</td><td>Based on the notification type a SNMP messages are sent each time an alert is generated.
The following notification types are supported:
Inform - Inform is acknowledged trap. The sender gets an acknowledgement from the receiver.
Trap - Trap is unacknowledged notification</td></tr><tr><td>Authoritative Engine ID (This optioin is availabe only for notification type TRAP)</td><td>An identifier which is used to identify the agents. Authoritative engine ID along with the username is used to uniquely identify the agent.</td></tr><tr><td>Security Level</td><td>Define the security level. The following are the options:
Unauthenticated and Unencrypted
Authenticated and Unencrypted
Authenticated and Encrypted</td></tr></table></td></tr>
</table>

Parameters	Description	
	Auth Protocol (This option is available only for security level Authenticated and Unencrypted and Authenticated and Encrypted)	Authentication protocol which is used to validate a user before providing an access to the server. The options are: • SHA • MD5
	Auth Key (This option is available only for security level Authenticated and Unencrypted and Authenticated and Encrypted)	A password that you want to use for authentication.
	Privacy Protocol (This option is available only for security level Authenticated and Encrypted)	Privacy protocol is an encryption technique for data communication.
	Private Key (This option is avaliable only for security level Authenticated and Encrypted)	A password that you want to use for encryption.
Community	Community string used to authenticate on the SNMP trap host. The default value is **public**.	

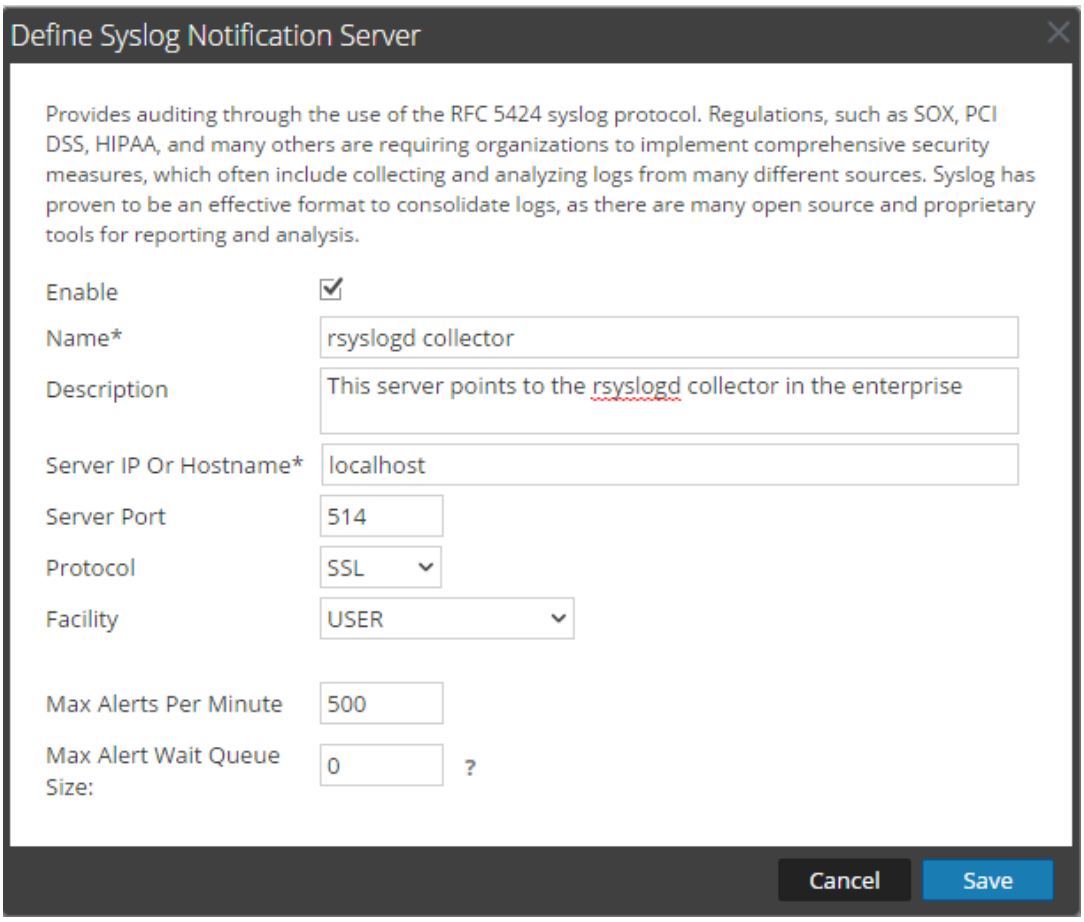
Parameters	Description
Number of Retries	Number of retries for the trap.
Max Alerts Per Minute	Maximum number of alerts per minute.
Max Alert Wait Queue Size	Maximum number of alerts to be queued before they are dropped.

Syslog

Syslog notification servers allow you to configure Syslog settings as a notification server to send notifications. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

You cannot disable notification servers associated with global audit logging configurations.

The following figure shows the Define Syslog Notification Server dialog.



The following table lists the various parameters that you need to define for the Syslog notification servers.

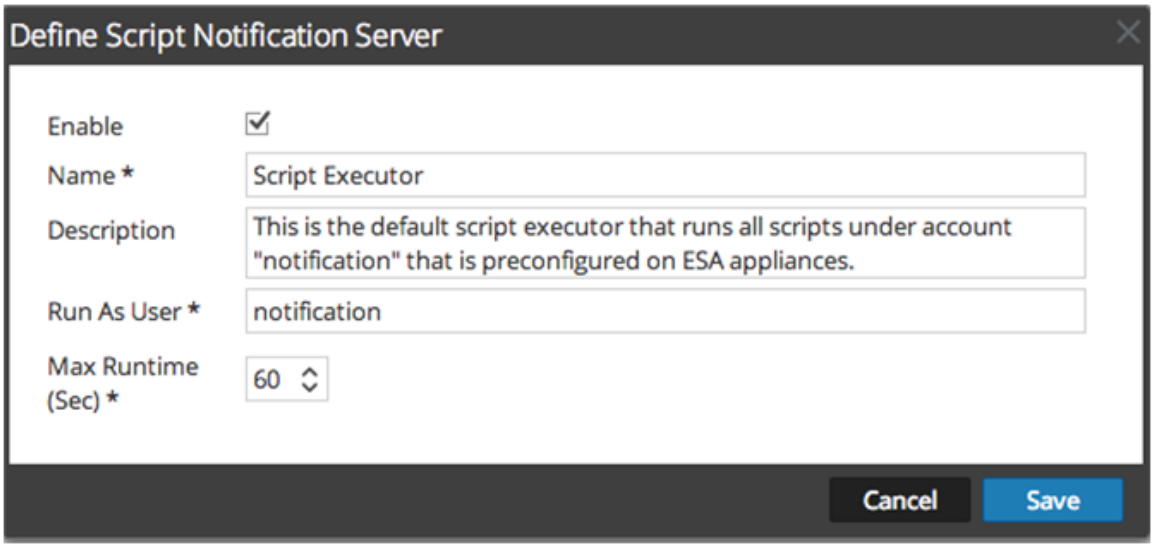
Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	The hostname of the host where the target Syslog process is running.
Server Port	The port number where the target Syslog process is listening.
Protocol	The protocol to be used to transfer the Syslog files.

Parameters	Description
Facility	The designated Syslog facility to use for all outgoing messages. It is used to specify what type of program is logging the message. Some possible values are KERN, USER, MAIL, and DAEMON. This lets the configuration file specify that messages from different facilities will be handled differently.
Max Alerts Per Minute	Maximum number of alerts per minute. This field is not used for Global Audit Logging.
Max Alert Wait Queue Size	Maximum number of alerts to be queued before they are dropped. This field is not used for Global Audit Logging.

Script

Script notification servers enable you to configure Script as a Notification Server.

The following figure shows the Define Script Notification Server dialog.



The following table lists the various parameters that you need to define for the Script notification servers.

Parameters	Description
Enable	Select to enable the notification server.

Parameters	Description
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Run As User	Name of the user identity under which the script is executed. The default user identity is **notification**. For ESA, you cannot set this to anything else unless you have created the account on the ESA host.
Max Runtime (Sec)	The maximum time (in seconds) the script is allowed to run.

Define Notification Output Dialogs

This topic provides descriptions of the various notification output dialogs. You configure notification outputs in the ADMIN > System > Notifications > Output tab. Notifications are basically the destinations used for sending notifications. For ESA, notifications enable you to define how you want to receive the ESA alerts. The following are the different notifications supported by NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

Procedures related to notifications are described in Configure Notification Outputs.

To access the Define Notification dialogs:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. On the **Output** tab, click + and then select a notification output (Email, SNMP, Syslog, or Script)
   The Define Notification dialog is displayed for your selection.

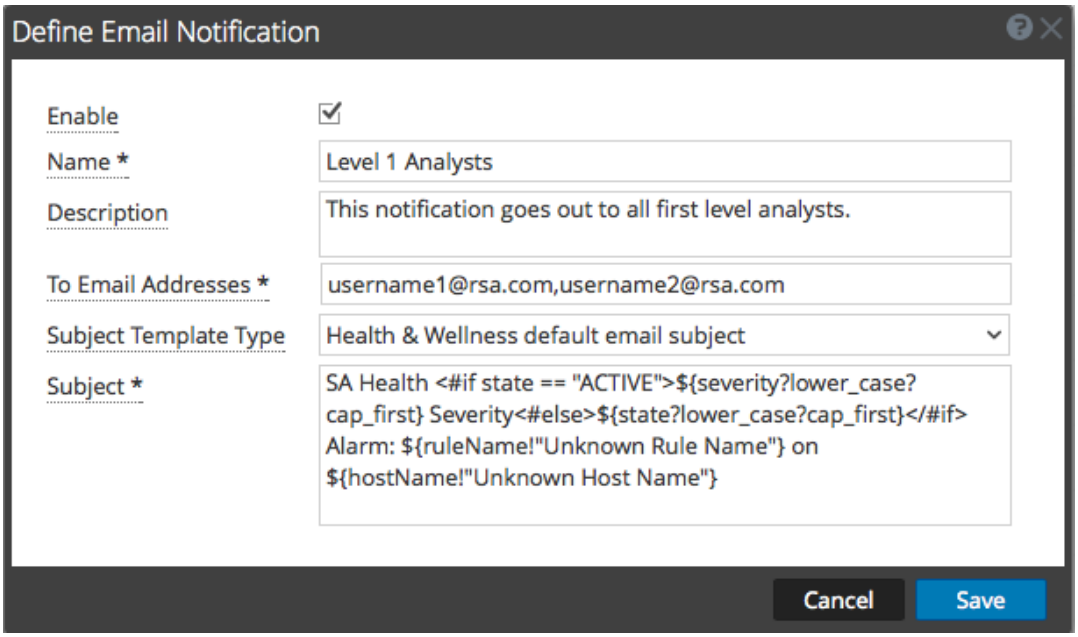
Features

There are four notification dialogs, which allow you to configure notification outputs.

Email

Email notifications enable you to define the destination email address to which you can send the alerts. It also enables you to add a custom description in the subject of the email and also to define multiple destination email addresses.

The following figure shows the Define Email Notification dialog.



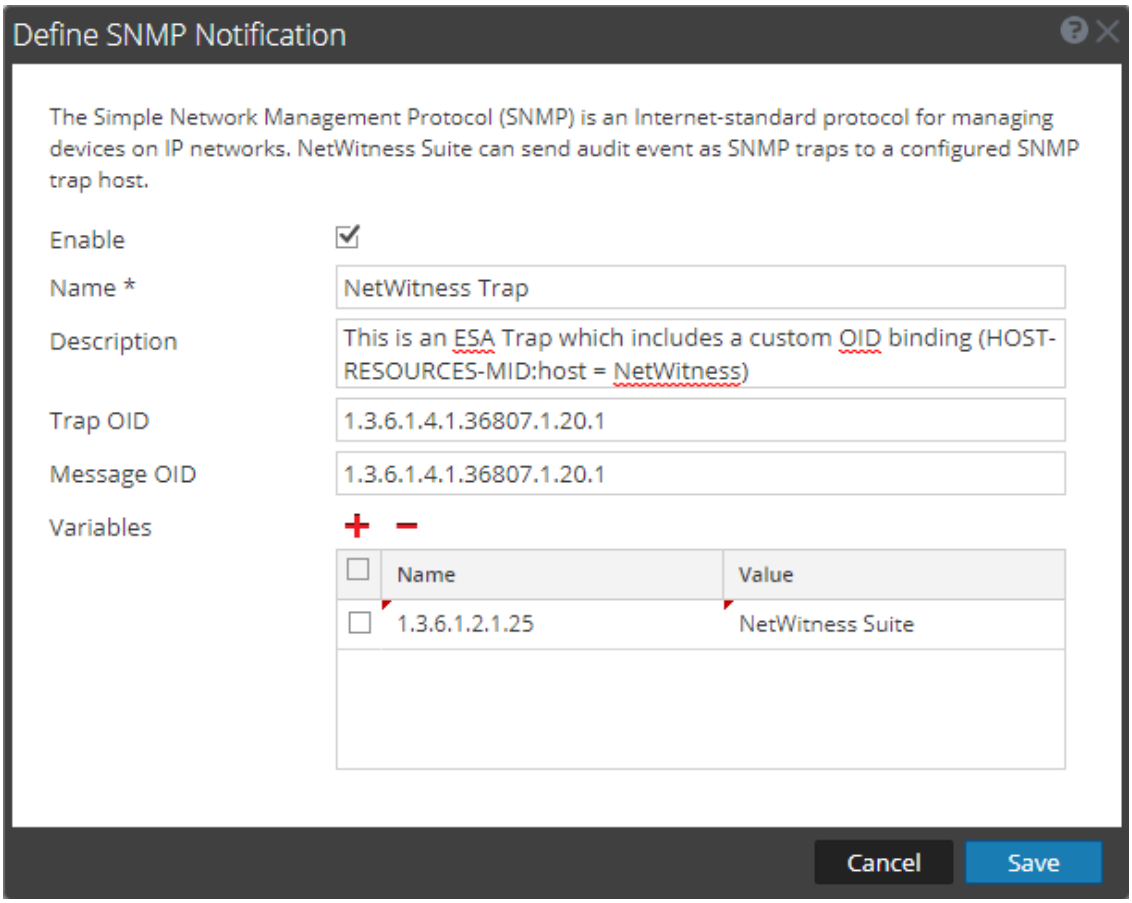
The following table lists the various parameters that you need to define for the email notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
To Email Addresses	Describes the destination email address to which the alert needs to be sent. **Note:** You can define multiple email addresses.
Subject Template Type	Lists available templates for creating a subject. When you choose a template, the Subject field is automatically filled in with the code for your chosen template.
Subject	Custom description about the triggered alert. This information is automatically filled in if you choose one of the predefined templates from the Subject Template Type drop-down menu. **Note:** To provide a custom subject, please refer to "Include the Default Email Subject Line" topic in the *System Maintenance Guide*.

SNMP

SNMP notifications enable you to define the SNMP settings to send alert notifications.

The following figure shows the Define SNMP Notification dialog.



The following table lists the various parameters that you need to define for the SNMP notifications.

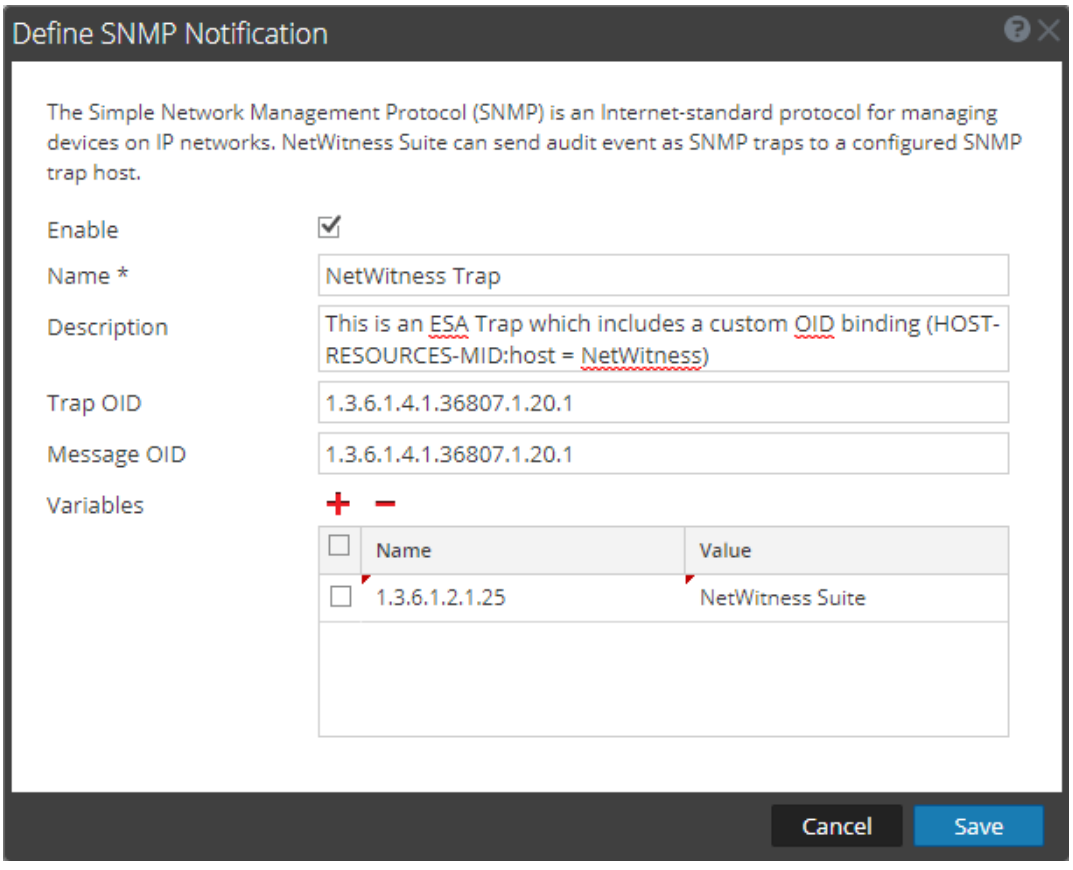
Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.

Parameter	Description
Trap OID	The object ID for the SNMP trap on the trap host that receives the event. The default value is **1.3.6.1.4.1.36807.1.20.1**. This value is a hierarchical name that represents the system that generates the trap. 1.3.6.1.4.1 is the common prefix for all enterprises and 36807.1.20.1 identifies NetWitness Suite.
Message OID	The message object identifier for the SNMP trap.
Variables	Additional information that should be included within the trap. It is a variable that is a name value pair.

Syslog

Syslog notifications enable you to define the Syslog settings to send alert notifications.

The following figure shows the Define Syslog Notification dialog.



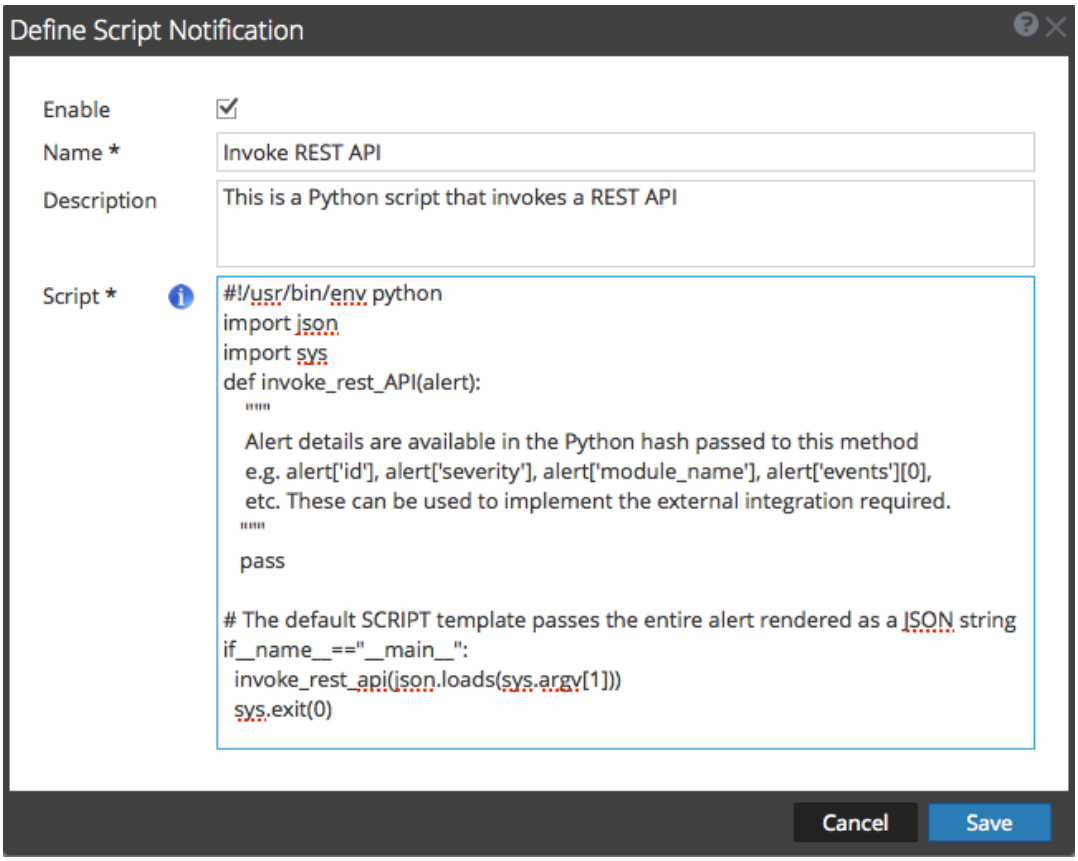
The following table lists the various parameters that you need to define for the Syslog notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Severity	Defines the severity of the alert.
Encoding	Defines the encoding format. In some environments where no regular character sets are used (for example, Japanese characters), this field will help selecting the right encoding of the characters.
Max Length	The maximum length of a Syslog message in bytes. The default value is **2048**. Messages that exceed the maximum length are truncated when the **Truncate overly large syslog messages** checkbox is selected, which is found in Administration > System > Legacy Notifications. Legacy Notifications Configuration Panel provides additional information.
Include Local Timestamp	Select to include the local timestamp in messages.
Include Local Hostname	Select to include the local hostname in Syslog messages.
Identity String	An identity string to be prefixed to each Syslog alert. If the string is blank, no identity string is prefixed to the outgoing Syslog alerts. You can use this to identify the alerts from ESA.

Script

Script notifications enable you to define the Script that executes in response to the alert. You can use any script for ESA notifications.

The following figure shows the Define Script Notification dialog.



The following table lists the various parameters that you need to define for the Script notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Script	Defines the script.

Define Notification Template Dialog

In the Global Notifications panel, you can configure global notification settings for Notification Servers, Notification Outputs, and Notification Templates. On the Templates tab, you configure the templates for various notifications. The notification template defines the format and message fields of the notifications. You can select a default template or you can use the Define Template dialog to configure and edit templates.

You can define the following template types:

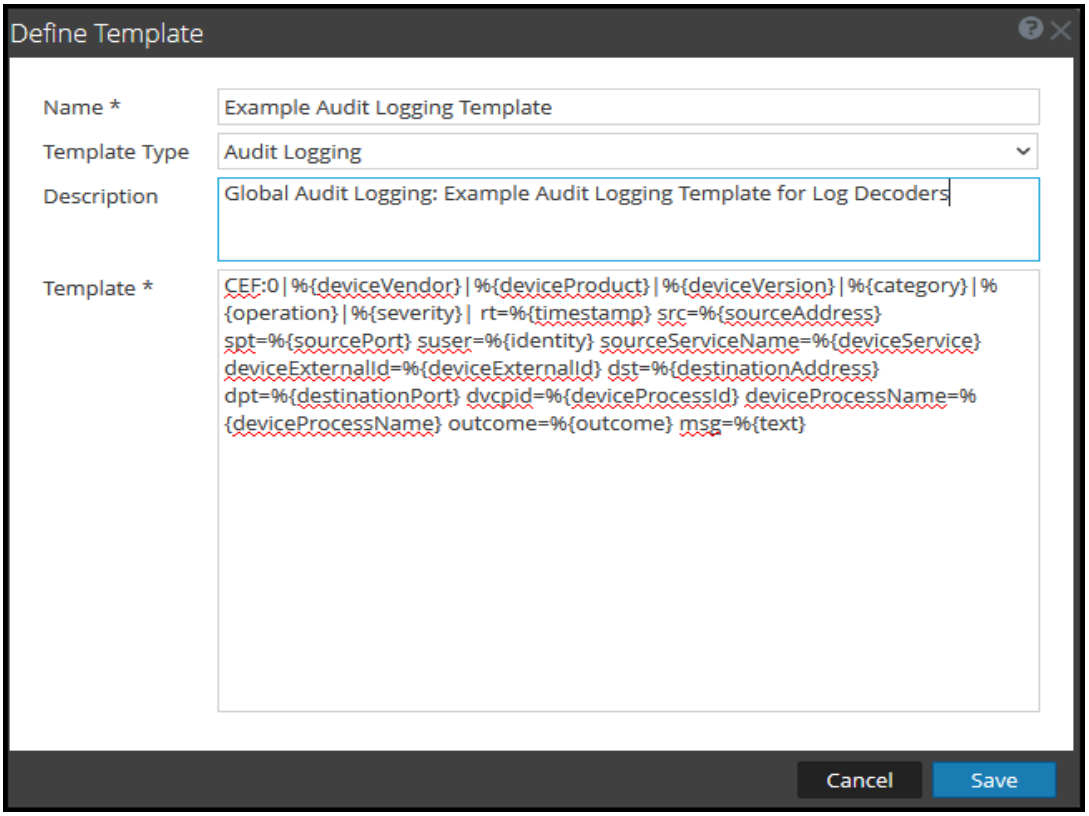
- Audit Logging
- Event Stream Analysis
- Event Source Monitoring
- Health Alarms

Procedures related to notification templates are described in Configure Templates for Notifications.

To access the Define Template dialog:

1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Global Notifications > Template Tab**.
3. In the **Notifications Configurations** panel, click , or select a configuration and click .

The **Define Template** dialog is displayed.



The following table describes the features in the Define Template dialog.

Field	Description
Name	Type a unique name for the notification template.
Template Type	Select the type of template that you want to create: • **Audit Logging**: Use this template for Global Audit Logging. • **Event Stream Analysis**: Use this template type for ESA alert notifications. • **Event Source Monitoring**: Use this template type for ESM notifications. • **Health Alarms**: Use this template type for Health and Wellness notifications.
Description	Add a description for the template. For example, if you create a notification template for Log Decoders to use for Global Audit Logging, you could mention that information in the description.

Field	Description
Template	Specify the format for the template. Define a Template for Global Audit Logging provides instructions on how to define an audit logging template to use for Global Audit Logging. To define a template for Event Stream Analysis (ESA), see Define a Template for ESA Alert Notifications.

Output Tab

In the **Global Notifications** panel, in the **Output** tab (ADMIN > System > Notifications > Output), you configure notification outputs. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

Notification Output configurations define email addresses and subject lines, SNMP trap OID settings, syslog output settings, and script code.

Notifications are the destinations configured for the alert notifications that are sent by ESA service. You can configure the following as destinations using the Output tab:

- Email
- SNMP
- Syslog
- Script

Note: You do not need to configure the Output tab for Global Audit Logging. For detailed steps, see Configure Global Audit Logging.

Workflow

This workflow shows the necessary procedures to configure and verify the output for Global Notifications. You can perform the following:

- Configure the Email settings as notification.
- Configure SNMP settings as notification.
- Configure Syslog settings as notification.
- Configure a Script as notification.

What do you want to do?

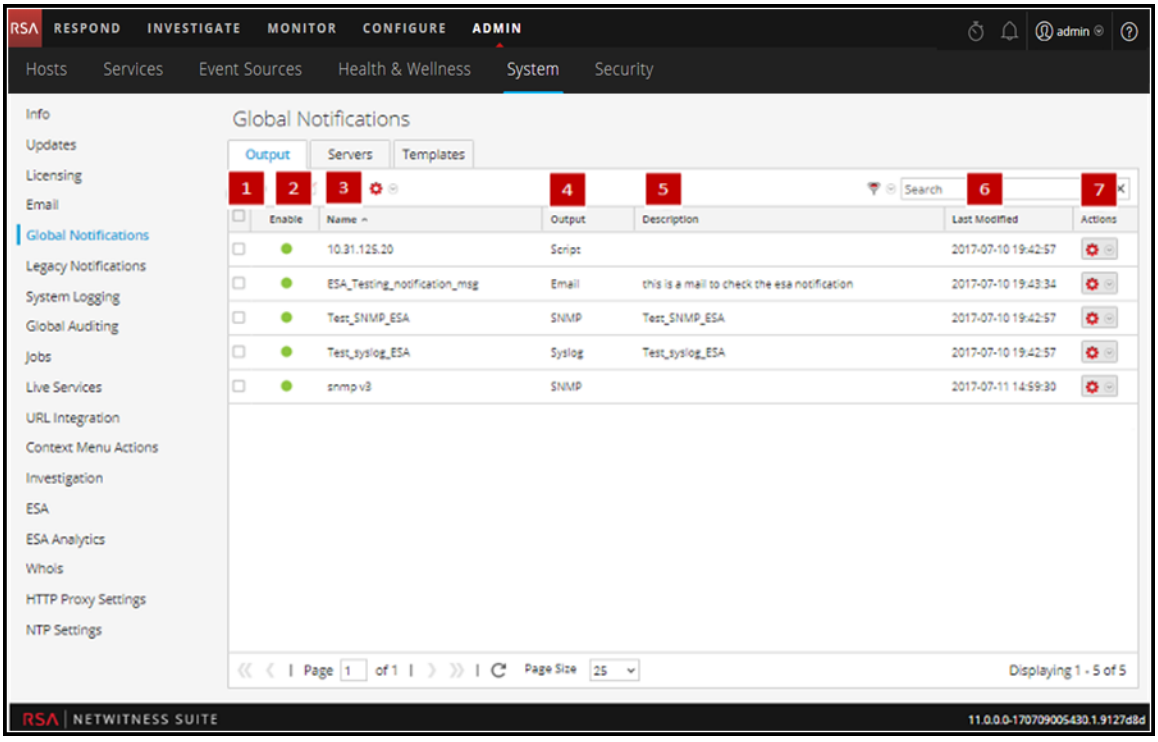
Role	I want to ...	Show me how
Administrator	Define notification outputs.	Configure Notification Outputs

Related Topics

- Notification Outputs Overview
- Configure Email as a Notification
- Configure Script as a Notification
- Configure SNMP as a Notification
- Configure Syslog as a Notification

Quick Look

The following example illustrates Global Notification Outputs configuration.

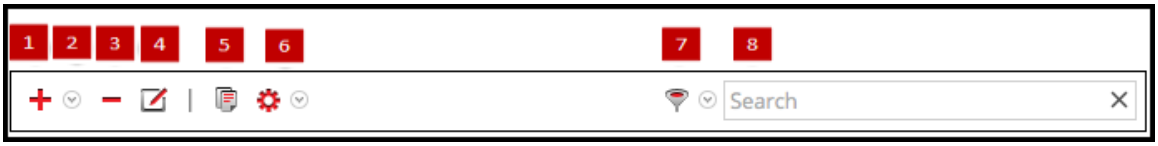


1 Selects a row for an action in the toolbar. Selecting the check box in the column title selects or deselects all rows in the grid.

2 Indicates whether the configuration is enabled. A solid colored green circle indicates that a

	configuration is enabled. A blank white circle indicates that a configuration is not enabled.
3	Identifies or labels the configuration.
4	Identifies the configuration output. The outputs are Email, SNMP, Syslog, and Script.
5	Describes the configuration.
6	Shows the date and time of the last configuration change.
7	Provides an Actions menu for the selected configuration with actions that can be taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

The Global Notifications panel toolbar is at the top of the Output tag and provides the following options:



1	Adds a notification output
2	Configures Email, SNMP, Syslog, and Script notification settings.
3	Removes a selected notification configuration. You cannot delete notification servers and notification types that are associated with global audit log configurations. If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use. You can also delete a configuration by selecting a configuration and then in the Actions column, selecting > Delete.
4	Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting > Edit.
5	Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting > Duplicate.
6	Displays the following options: • **Import**: Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration. • **Export All**: Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations.

- **Export**: Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting > Export.

7 Filters by Email, SNMP, Syslog, or Script.

8 Searches configurations in the grid.

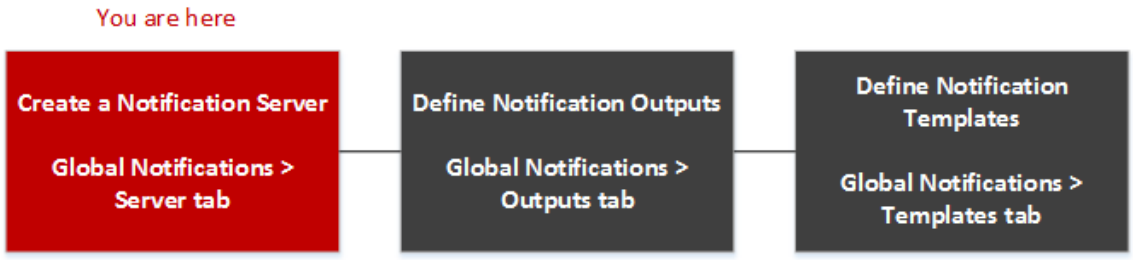
Servers Tab

Servers Tab describes the components of the Global Notifications > Servers tab. This tab enables to configure notification servers. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

Configure **Notification Servers** in the Servers tab. On the Servers tab, add the servers from which you want to receive notifications from the system. For Global Audit Logging, define Log Decoders as Syslog Notification Servers.

Event Stream Analysis can send notifications to users through email, SNMP, or Syslog when an alert is triggered on the ESA service. These alert notification senders are called Notification Servers. You can configure multiple notification settings and use them while defining an ESA rule, for example, you can configure multiple mail servers or Syslog servers and use the settings while defining an ESA rule.

Workflow



The workflow shows the necessary procedures to configure and verify the Servers for Global Notifications. You can perform the following:

- Configure the Email settings as a notification server.
- Configure SNMP settings as a notification server.
- Configure Syslog settings as a notification server.
- Configure a Script as a notification server.

What do you want to do?

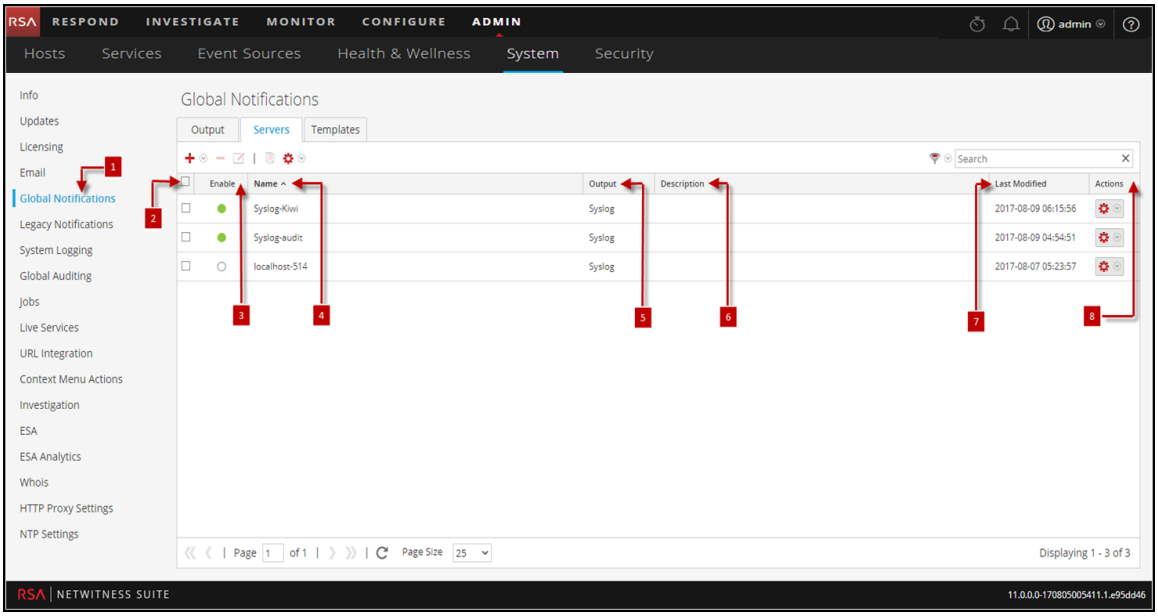
Role	I want to ...	Show me how
Administrator	Define notification Servers	Configure Notification Servers

Related Topics

- Notification Servers Overview
- Configure the Email Settings as Notification Server
- Configure Script as a Notification Server
- Configure the SNMP Settings as Notification Server
- Configure a Syslog Notification Server

Quick Look

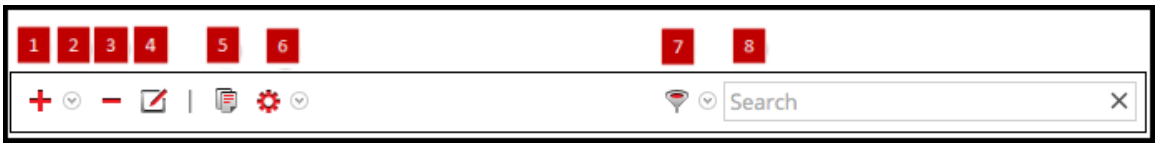
The following example illustrates Global Notification Servers configuration.



1	Displays the Server Tab Panel.
2	Selects a row for an action in the toolbar. Selecting the checkbox in the column title selects or deselects all rows in the grid.
3	Indicates whether the configuration is enabled. A solid colored green circle indicates that a configuration is enabled. A blank white circle indicates that a configuration is not enabled.
4	Identifies or labels the configuration.
5	Identifies the configuration output. The outputs are Email, SNMP, Syslog, and Script.
6	Describes the configuration.
7	Shows the date and time of the last configuration change.
8	Provides an Actions menu for the selected configuration with actions that can be

taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

The Global Notifications panel toolbar is at the top of the Output tag and provides the following options:



1. Adds a notification output
2. Configures Email, SNMP, Syslog, and Script notification settings.
3. Removes a selected notification configuration. You cannot delete notification servers and notification types that are associated with global audit log configurations. If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use. You can also delete a configuration by selecting a configuration and then in the Actions column, selecting > Delete.
4. Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting > Edit.
5. Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting > Duplicate.
6. Displays the following options:
   - **Import**: Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration.
   - **Export All**: Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations.
   - **Export**: Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting > Export.
7. Filters by Email, SNMP, Syslog, or Script.
8. Searches configurations in the grid.

Templates Tab

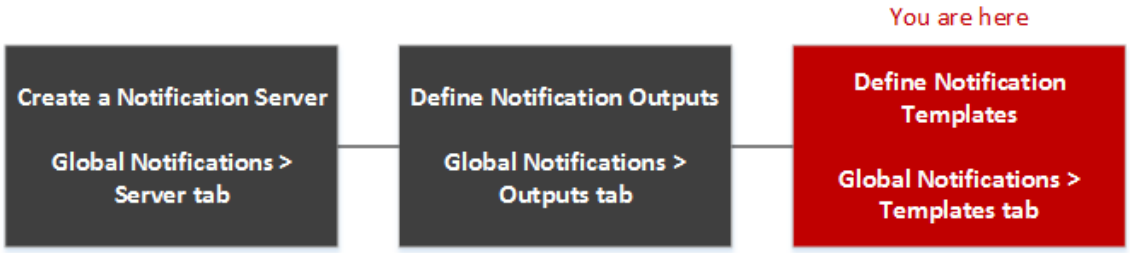
The Notification Templates tab enables to configure notification templates. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond. Notification templates define the format and message fields of the notifications.

Select a default template or configure templates for Email, SNMP, Syslog, and Script, depending on the template type. For Event Stream Analysis (ESA) templates, configure Email, SNMP, Syslog, and Script. For Audit Logging templates, configure Syslog.

Event Stream Analysis templates are not specific to any type of alert notifications, that is, the same template can be used for all types of notifications.

When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Define notification Templates	Configure Templates for Notifications

Related Topics

Configure Global Notifications Templates

Configure a Template

Define a Template for ESA Alert Notifications

Delete a Template

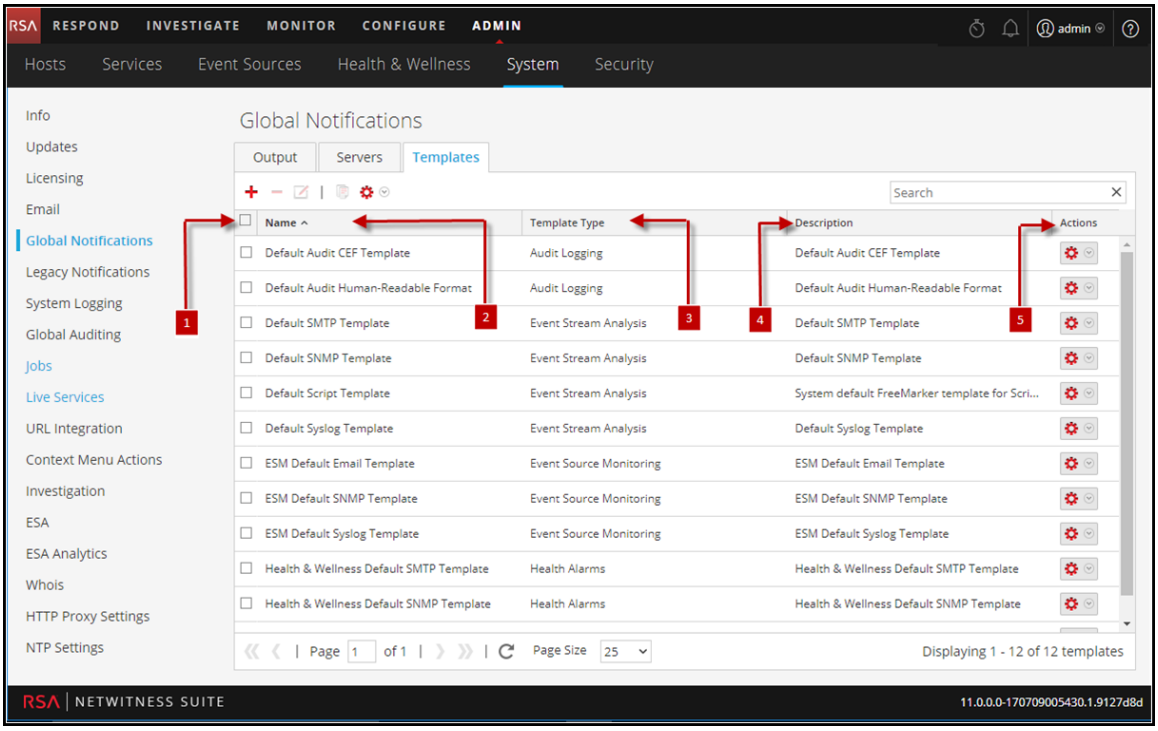
Duplicate a Template

Edit a Template

Import and Export a Global Notifications Template

Quick look

The following example illustrates Global Notification Templates Tab.



1. Selects a row for an action in the toolbar. Selecting the check box in the column title selects or deselects all rows in the grid.
2. Identifies or labels the templates
3. Choose a Template Type
4. Describes the templates
5. Provides an Actions menu for the selected templates with actions that can be taken on the Templates. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

HTTP Proxy Settings Panel

HTTP Proxy Settings Panel introduces the proxy support features of the Administration System view > HTTP Proxy Settings panel.

Note: Proxy support is only for HTTP and HTTPS proxies and not SOCKS5.

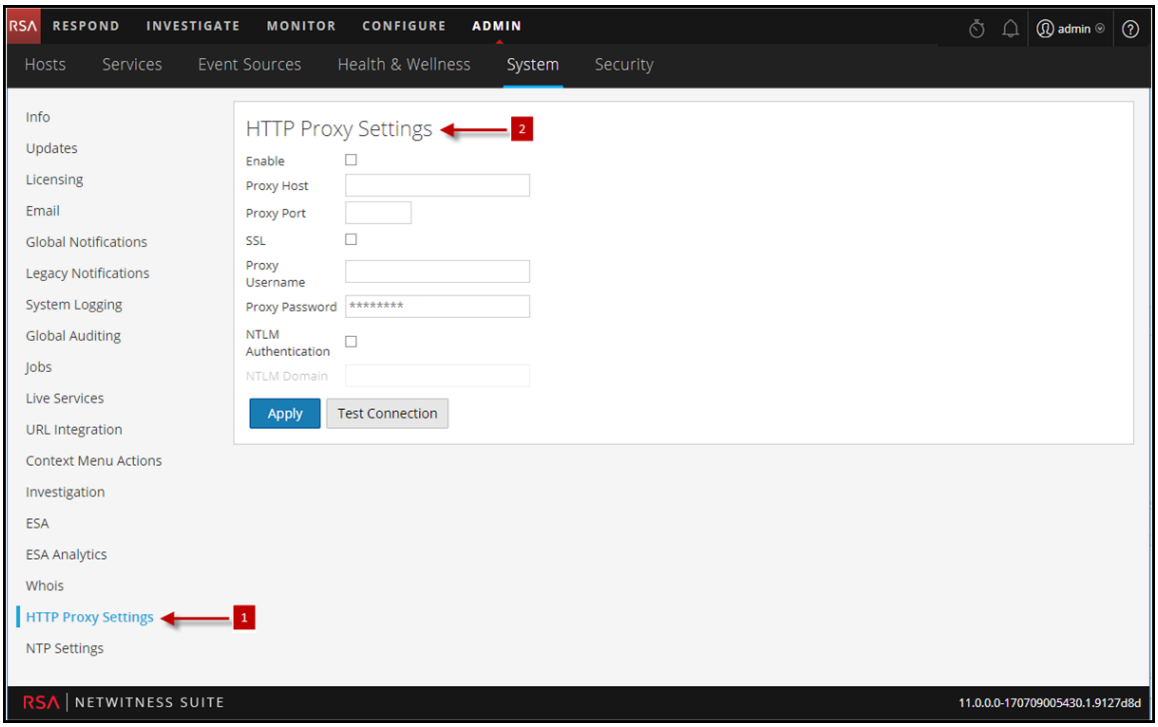
The HTTP Proxy Settings panel provides a user interface for configuring a proxy for use across NetWitness Suite modules and services. The Proxy Settings set up a proxy to be used wherever a proxy is needed in NetWitness Suite. The settings in this panel override any proxy settings configured for an individual service such as Malware Analysis or Live.

Related topics

"Configure Proxy for NetWitness Suite" in Additional Procedures

Quick Look

The following example illustrates an HTTP Proxy Settings Panel.



1 Displays the HTTP Proxy Settings Panel.

2 Allows the user to configure HTTP Proxy Sittings.

This table describes the features in the HTTP Proxy Settings section.

Feature	Description
Enable	Enable the system proxy configuration for use in NetWitness Suite.
Proxy Host	The hostname for the proxy host.
Proxy Port	The port used for communication on the proxy host.
SSL	(Optional) Enable communication using SSL.
Proxy Username	(Optional) The user name used to log on to the proxy host if the proxy requires authentication.
Proxy Password	(Optional) The user password used to log on to the proxy host if the proxy requires authentication.
NTLM Authentication	Use NT LAN Manager authentication and session security protocols.
NTLM Domain	The name of NTLM domain.
Apply	Applies any changes made, and they become effective immediately.

Email Configuration Panel

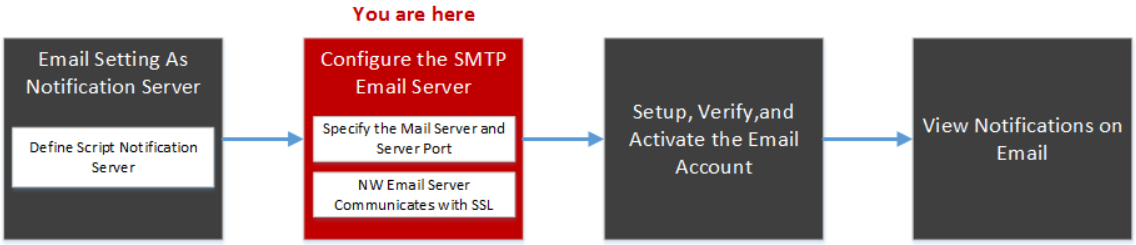
The Email Configuration Panel provides information about email configuration settings in the System View > Email Configuration panel. RSA NetWitness® Suitesends notifications to users via email about various system events. To be able to configure these email notifications, first configure the SMTP email server (See Configure Email Servers and Notification Accounts).

The Email Configuration panel provides a way to:

- Configure the email server.
- Set up an email account to receive notifications.
- View statistics on email operations.

Workflow

This workflow shows the necessary procedures to configure and verify Email Panel.



What do you want to do?

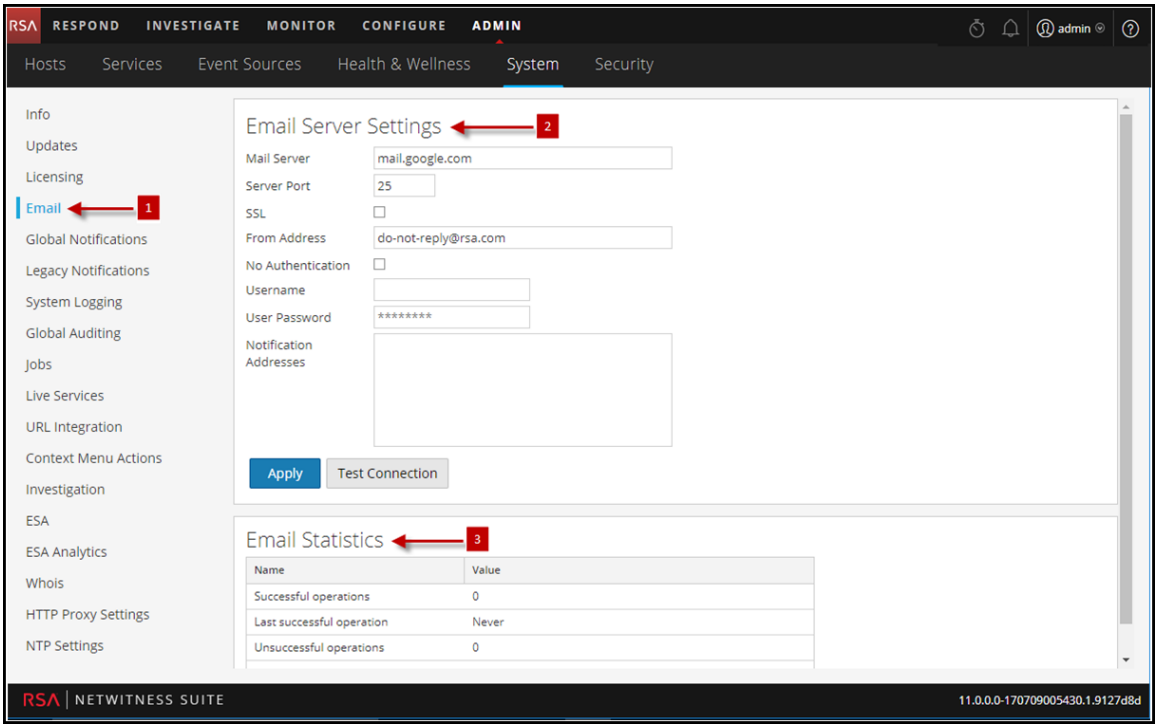
Role	I want to ...	Show me how
Administrator	Configure the SMTP Email Server	Configure Email Servers and Notification Accounts
Administrator	Email Setting as Notification Server	Configure the Email Settings as Notification Server
Administrator	Setup, Verify and Activate the Email Account	Receive Notification on Email

Related Topics

- Configure the Email Settings as Notification Server
- Configure Email as a Notification
- Configure Email Servers and Notification Accounts

Quick Look

The following example illustrates an Email configuration. The configuration defines how events are notified on Email.



1	Displays the Email Configuration Panel.
2	Allows the user to configure Email Server sittings.
3	Provides feedback on Email operations.

The **Email Configuration** panel has two sections: **Email Server Settings** and **Email Statistics**.

Email Server Settings

In the **Email Server Settings** section, you configure the following parameters.

Feature	Description
Mail server	The email server name. The default value is **mail.google.com**.
Server port	The server port used to send and receive emails. The default value is **25**.
Use SSL	The preference for SSL use in communications between the email server and NetWitness Suite. The default value is to not use SSL (unchecked).
From address	The address that appears in all emails from NetWitness Suite. The default from address for emails is **do-not-reply@rsa.com**.
Username	The username to access the email server. The default value is **blank**.
User password	The user password to access the email server. The default value is **blank**.
Test connection	Tests the connection to the email server.
Apply	Applies the email configuration to this instance of NetWitness Suite.

Email Statistics

The Email Statistics section provides feedback on the number of successful and failed email operations as well as the time of the last successful and unsuccessful email operation. For each statistic the name of the statistic and the value is displayed.

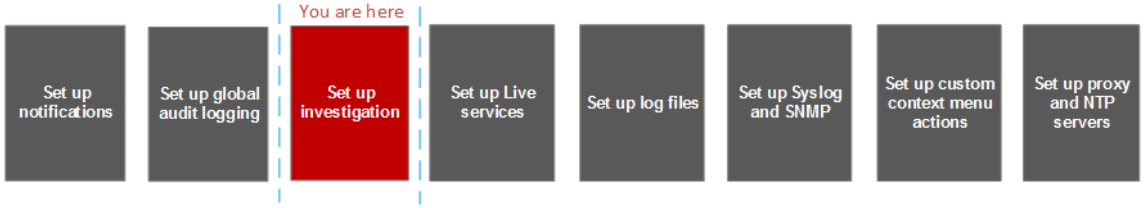
Investigation Configuration Panel

The System view > Investigation Configuration panel, which provides the user interface for Administrators to configure the system-wide settings that NetWitness Suite Investigation uses when analyzing data and reconstructing an event.

The Investigation Configuration settings allow an administrator to manage application performance for Investigation. As analysts analyze and reconstruct sessions that they are investigating, performance can be affected by operations that involve loading, searching, visualizing, and reconstructing large amounts of data.

Note: Analysts can also set individual preferences for Investigation in the Profiles view and in the Navigation view.

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure navigate, events and context lookup settings	Configure Investigation Settings
Administrator	Clear reconstruction cache for services	Configure Investigation Settings

Related Topics

- Standard Procedures

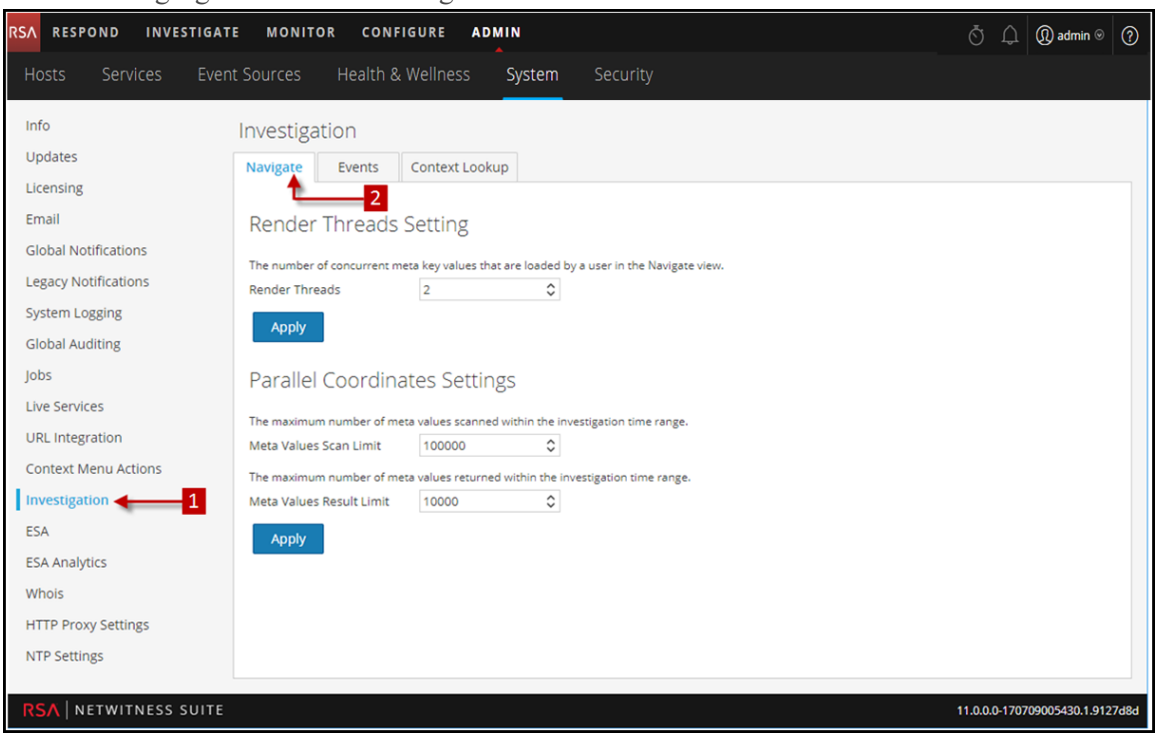
Quick Look

The Investigation Configuration panel has three tabs: Navigate, Events, and Context Lookup.

Though most fields in the tabs have a selection list with specific increments through the range of possible values, you can enter a value within the allowed range manually. An invalid entry is signaled by the field highlighted in red. When valid values are selected, clicking Apply in a given section puts the changes into effect immediately.

Navigate Tab

The following figure shows the Navigate tab.



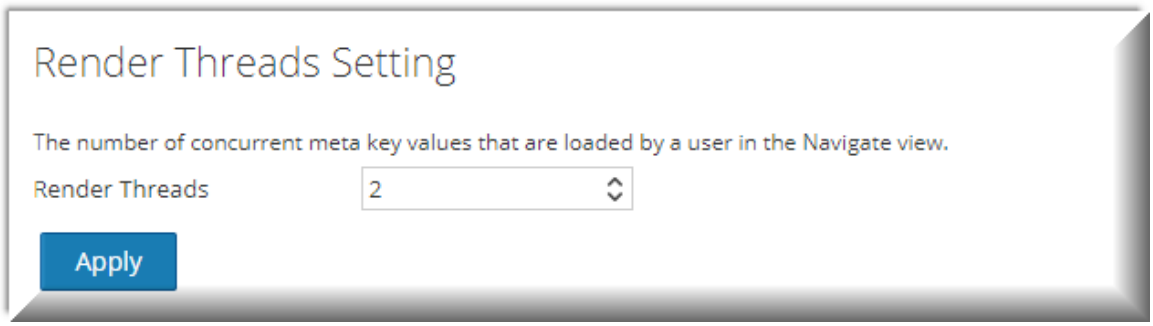
1 Displays the Investigation Configuration Panel.

2 Displays the Navigate Tab.

The Navigate tab has two sections: Render Threads Setting and Parallel Coordinates Settings.

Render Threads Setting

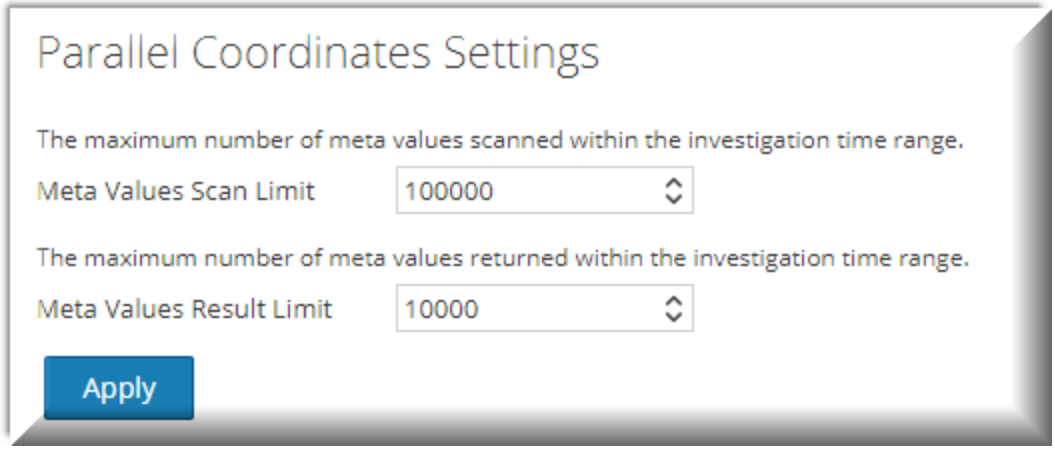
The Render Threads Setting is a selectable value between 1 and 20, which defines the number of concurrent (Values) loads in the Navigate view. The default value is 1.



Parallel Coordinates Settings

The Parallel Coordinates Settings apply to the Parallel Coordinates visualization in the Navigate view. There is a fixed limit on the amount of data that can be rendered as a parallel coordinates chart. In NetWitness Suite the administrator can configure parallel coordinates limits here.

Note: For better performance, recommended settings are **Meta Values Scan Limit: 100000** and **Meta Values Result Limit: 1000-10000**.



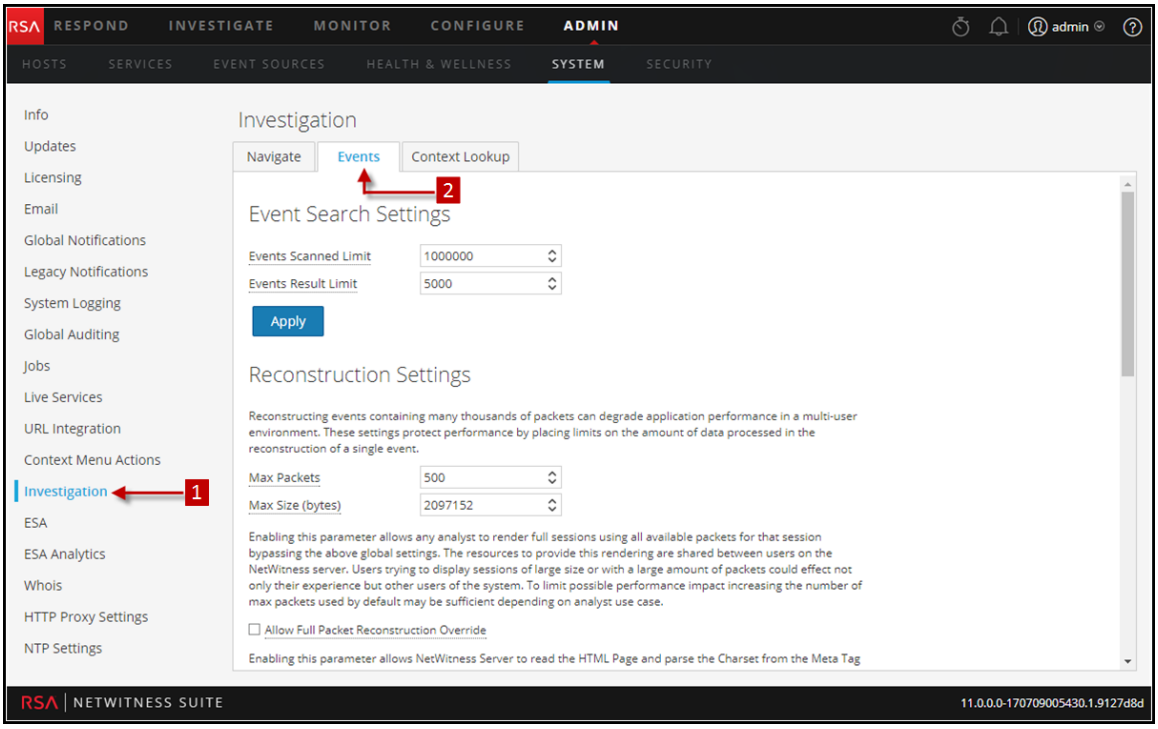
The following table describes the Parallel Coordinates Settings.

Parameter	Description
Meta Values Scan Limit	The maximum number of meta values scanned within the Investigation time range the analyst has selected in the Navigate view. Possible values are in the range of 1,000 to 10,000,000. The default value is 100,000.
Meta Values Result Limit	The maximum number of meta values returned within the Investigation time range the analyst has selected in the Navigate view. Possible values are in the range of 100 to 1,000,000,000. The default value is 10,000.

Quick Look

Events Tab

The following figure shows the Events tab.



Procedures associated with this panel are provided in Standard Procedures.

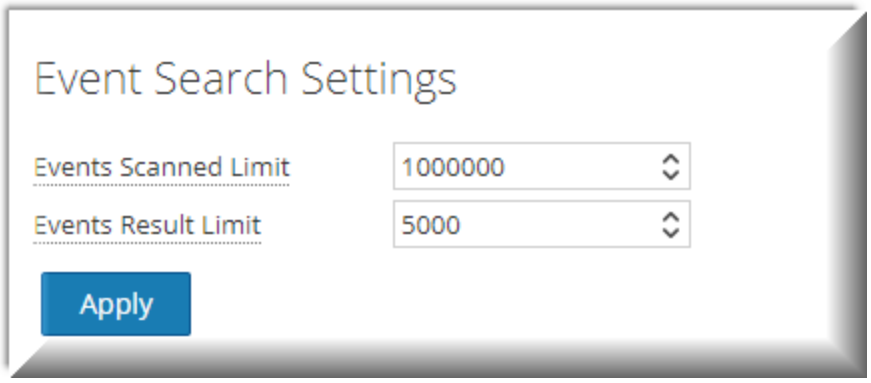
1 Displays the Investigation Configuration Panel.

2 Displays the Events Tab.

The Events tab provides configurable settings that affect the investigation of events. This tab has four sections: Event Search Settings, Reconstruction Settings, Web View Reconstruction Settings, and Reconstruction Cache Settings.

Event Search Settings

The Event Search Settings help to limit the number of events scanned when searching in the Events view.



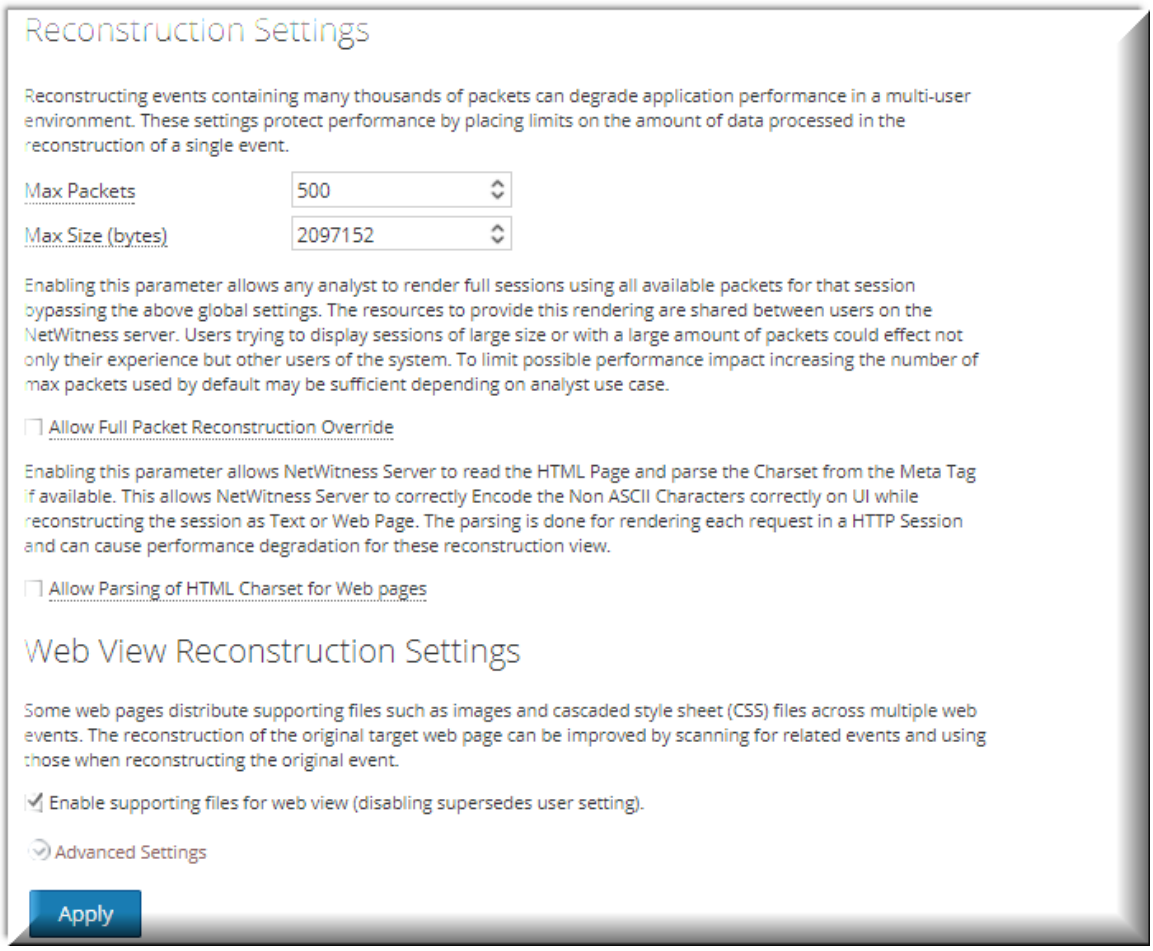
The following table describes the Event Search Settings.

Parameter	Description
Events Scanned Limit	The maximum number of events to scan when searching in the Events view.
Events Result Limit	The maximum number of results to return when searching in the Events view.

Reconstruction Settings

As analysts reconstruct sessions that they are investigating, some events can be very large and contain many thousands of source packets. Reconstructing these sessions, especially in a multi-user environment, can degrade application performance. The Reconstruction Settings allow an administrator to limit the number of packets and the size of a single event during reconstruction.

Note: An override to the Reconstruction Settings section is configurable for web views (under Web View Reconstruction Settings).



The following table describes the Reconstruction Settings features.

Parameter	Description
Maximum number of packets for a single event	This setting protects performance by placing a limit on the number of packets processed for a single event reconstruction. Possible values are in the range from 100 to 10,000 packets, using manual entry or increments of 100 from the selection list. The default value is 100 packets.

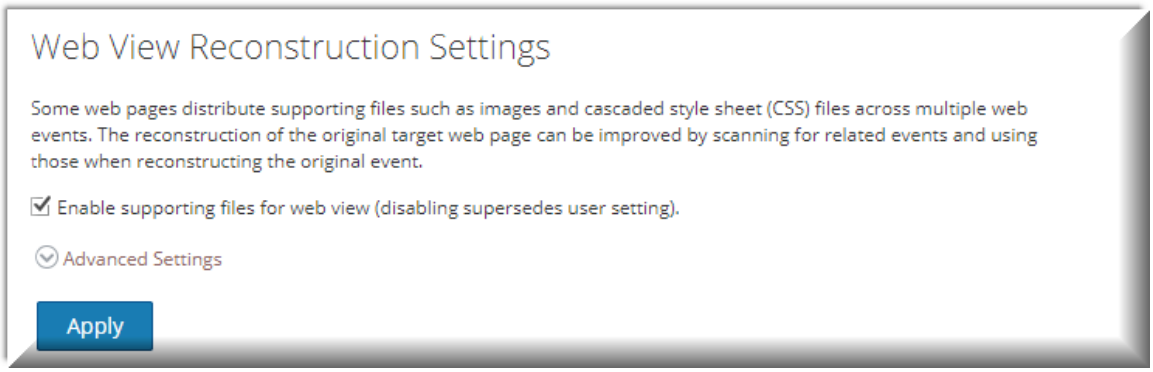
Parameter	Description
Maximum size, in bytes of a single event	This setting protects performance by placing a limit on the maximum size, in bytes, of a single event reconstruction. Possible values are in the range from 102,400 to 104,857,600 bytes, using manual entry or increments of 10,240 from the selection list. The default value is 2,097,152 bytes.
Allow Full Packet Reconstruction Override	When this checkbox is selected, the analysts is provided with a Use More Packets button in the Reconstruction Panel. This enables the NW Server to regenerate events using all the packets available in the Event.
Allow Parsing of HTML Charset for Web pages	This option allows the NetWitness Server to identify the web page encoding defined in the HTML meta tag instead of the HTTP header. The default setting is disabled.

Web View Reconstruction Settings

The Web View Reconstruction Settings allow an administrator to configure settings that improve the reconstruction of a web view by scanning and reconstructing related events that contain the same supporting files. When NetWitness Suite is reconstructing a web view that spans multiple events, it is possible to improve the reconstruction of the target event by scanning and reconstructing related events that contain the same supporting files, such as images and cascaded style sheet (CSS) files.

- The only related events scanned are HTTP service type events with the same source address as the target event, and a time stamp within a specified time range before and after the target event.
- The maximum number of related events to scan is configurable.

Clicking on the Advanced Settings option displays all configurable settings in this section.



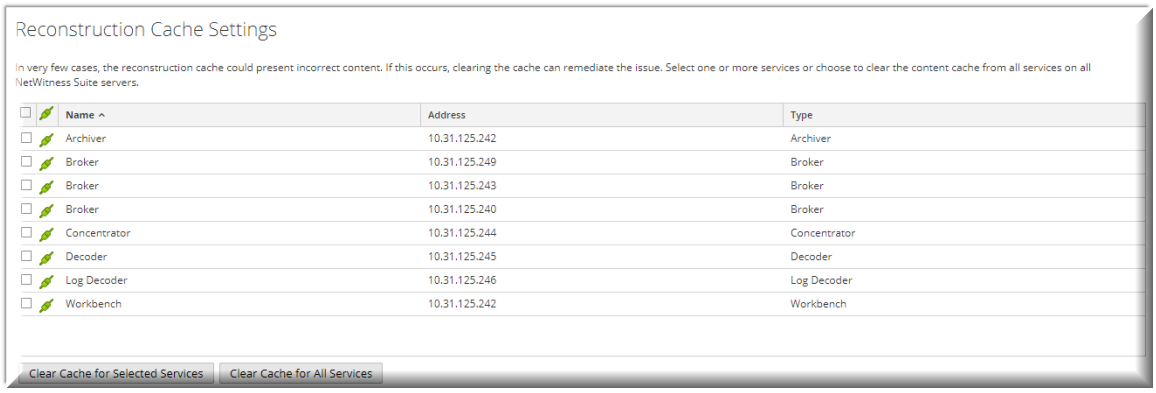
The following table describes the Web View Reconstruction Settings.

Parameter	Description
Enable supporting files for web view	This option determines how web views that have related data in other sessions are reconstructed. The default setting is enabled. When enabled, supporting files from related events can be used in the reconstruction of web views. Additional settings for calibrating the performance are enabled in this section, and Analysts have the option to enable CSS use in reconstructions. When disabled, supporting files from related events are not used and the setting for analysts to enable CSS use in reconstructions is disabled.
Time Range to Scan Related Events	Available when **Enable supporting files for web view** is checked. Configures the time range within which NetWitness Suite scans related events that are of the service type HTTP and have the same source address as the target event. This is a value between 0 and 60. • Seconds Before Target Event • Seconds After Target Event

Parameter	Description
Limit the number of related events processed	Allows configuration of the maximum number of related events that NetWitness Suite scans within the specified time range to discover supporting files for the target event. By default, this is disabled. When enabled, the Maximum Related Events field becomes active.
Max Related Events	When **Limit the number of events processed** is enabled, this field specifies the maximum number of related events that NetWitness Suite scans within the specified time range to discover supporting files for the target event. This is a selectable value between 10 and 1,000, using an increment of 100. The default value is 100.
Limit the number of packets and size of each related event	Overrides the general settings for the maximum number of packets and maximum size (in bytes) for individual related events.
Maximum Number of Packets for a Single Related Event	Possible values are in the range from 100 to 10,000 packets, using increments of 100 from the selection list. The default value is 100 packets.
Maximum Size, in Bytes, of a Single Related Event	Possible values are in the range from 102,400 to 104,857,600 bytes, using increments of 10,240 from the selection list. The default value is 524,288 bytes.

Reconstruction Cache Settings

In some cases, the reconstruction cache can present incorrect content; for this reason NetWitness Suite removes reconstructions that are older than a day from the cache. The cache is cleaned every day at midnight. Between the daily cache cleanings, certain actions may result in stale cache being used for a reconstruction, and if the need arises, administrators can manually clear cache for one or more services that are connected to the current NetWitness Server.



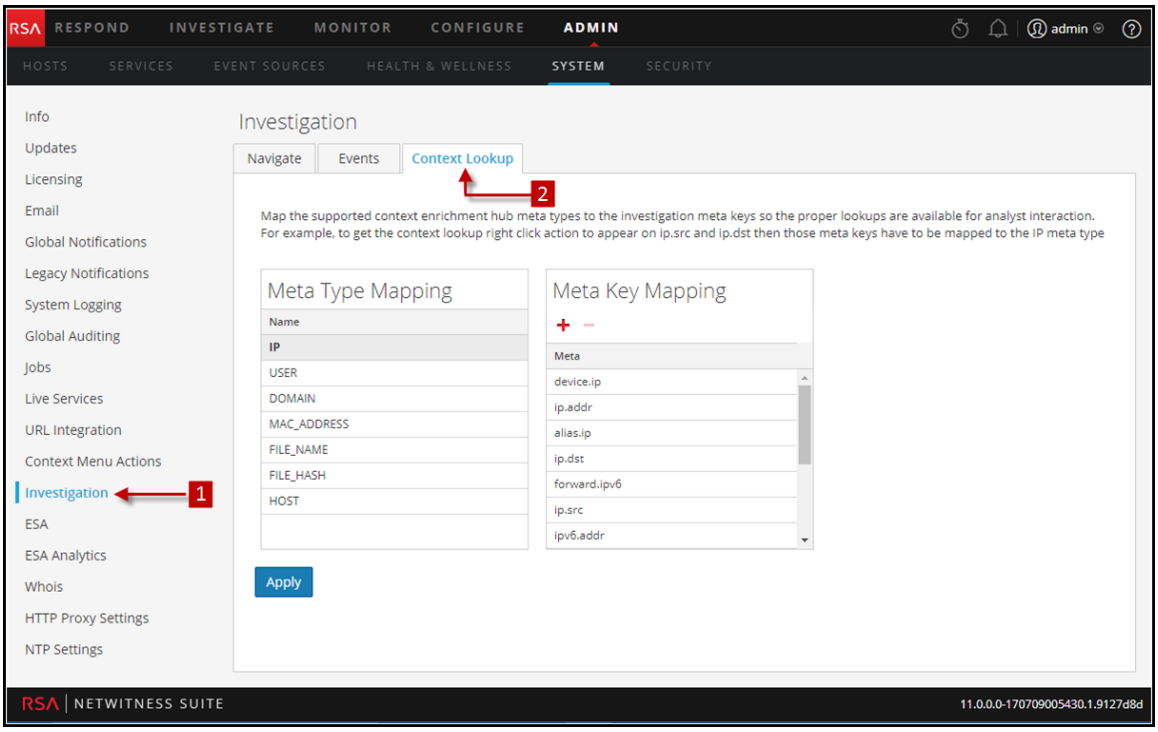
The following table describes the Reconstruction Cache Settings features.

Feature	Description
Selection box	Selection box in individual rows and in the title bar allow selection of one or more, or all services that need to have cache cleared manually.
Clear Cache for Selected Services	Clears the reconstruction cache for each selected service.
Clear Cache for All Services	Clears the reconstruction cache for all services.

Quick Look

Context Lookup Tab

The following figure shows the Context Lookup tab.



Procedures associated with this panel are provided in "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.

1 Displays the Investigation Configuration Panel.

2 Displays the Context Lookup Tab.

The Context Lookup tab enables the administrator to configure the Investigation meta keys and meta type mapping. The administrator can add or remove meta keys found in Investigation to the list of meta types supported by Context Hub service. NetWitness Respond and Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the ADMIN > SYSTEM > Investigations > Context Lookup tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, `ip.address` is a meta key and `ip_address` is not a meta key (it is a field in the MongoDB).

The following table describes the features of the Context Lookup tab.

Feature	Description

Feature	Description
+	Adds an meta key to the selected meta type supported by Context Hub.
−	Deletes the meta key from the selected meta type.
Apply	Saves the changes made to the Context Lookup tab.

Live Services Configuration Panel

Live Services Configuration Panel introduces the features for setting up your Live account and the CMS server connection.

Live Account consists of two sections, namely RSA Live Status and Download Live Feedback Activity Log. **Sign In** by entering your Live Account credentials to access the Live Services. To activate your Live account for NetWitness Suite, please contact RSA Customer Care. When you have confirmation that your Live account has been set up, you can configure the CMS server connection as described in Configure Live Services Settings

The Live Services panel provides the user interface for:

- The Live account
- The Live Content update schedule and preferences for notification of updates
- Participation in Live Feedback
- Sharing Live Content Usage Details
- RSA Live Connect (Beta)

New Features Enabled Dialog

When you log onto NetWitness Suite for the first time, you will be prompted with **New Features Enabled** dialog.

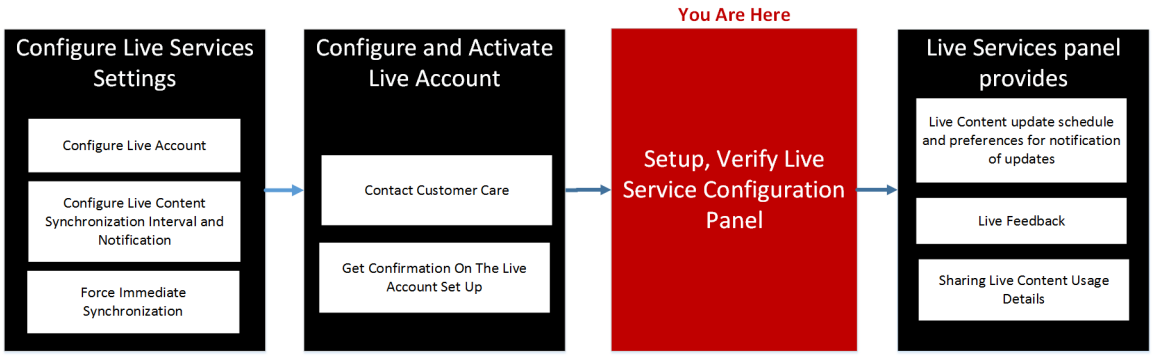
Feature	Description
Accept	Clicking Accept indicates that you agree to the following: • Participate in Live Feedback • Allow NetWitness Suite to send RSA the usage metrics and version of NW hosts about your environment to RSA, provided a Live Account is configured. • Receive threat intelligence data from Live Connect.
View Settings	Clicking **View Settings** redirects you to the Live Services UI to view the settings. If you have not configured the Live Account, a masked screen is displayed.

For information on Live Feedback, see Live Feedback Overview

For information on Analyst Behaviors and Data Sharing, see the "NetWitness Suite Feedback and Data Sharing topic in the *Live Services Management Guide*.

For information on Live Connect Threat Insights, see Configure Live Services Settings

Workflow



What do you want to do?

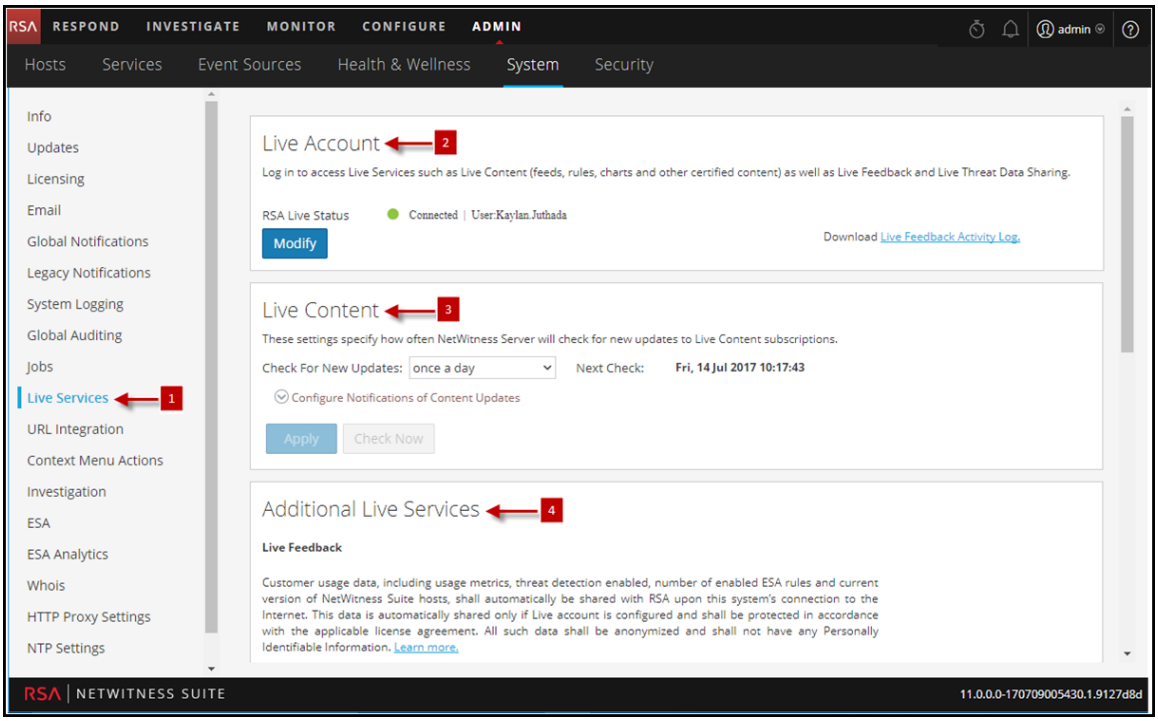
Role	I want to ...	Show me how
Administrator	Configure Live Account, CMS Server Connection	Configure the Email Settings as Notification Server
Administrator	Upload Data to RSA for Live Feedback	Upload Data to RSA for Live Feedback
Administrator	Setup, Verify Live Service Configuration Panel	Live Services Configuration Panel
Administrator	Overview On Live Feedback	Live Feedback Overview

Related Topics

- Live Feedback Overview
- Configure Live Services Settings
- Upload Data to RSA for Live Feedback
- Live Services Management Guide

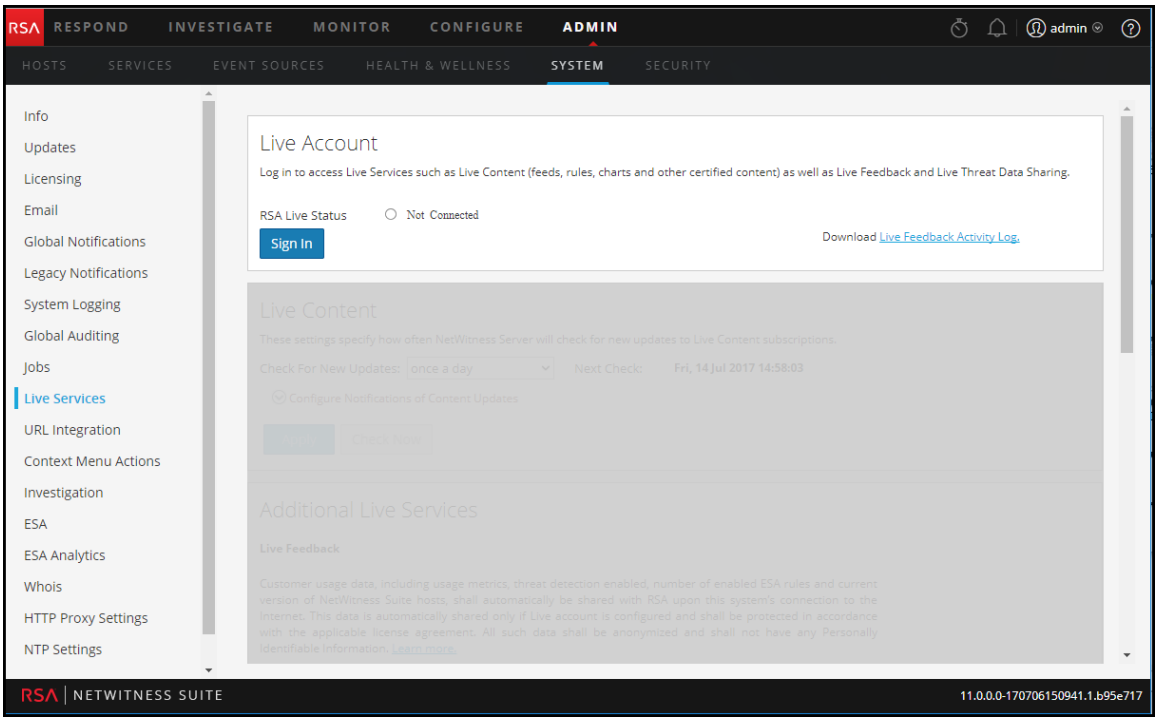
Live Services Quick Look

You access this view in the **ADMIN > System > Live Services**.



1	Displays the Live Services Configuration Panel.
2	Enter Live Account Credentials with the help of Customer Care.
3	Provides updates on Live Content.
4	Additional Live Services provide Live feedback.

Note: If you are not signed in with your Live Account credentials, a masked screen is displayed as shown here.



The Live Configuration panel has three sections: Live Account, Live Content, and Additional Live Services.

Live Account Section

In the **Live Account** section, you must enter the Live credentials. The information needed to set up the user's Live account consists of the Username, Password, and Live URL for the RSA Content Management System. This information is provided by Customer Care.

The following table describes the Live Account section features.

Feature	Description
Host	The Live URL for the Content Management System. The default value points to the RSA CMS at **cms.netwitness.com**.
Port	The communications port for Live to send requests to the Content Management System. The default value for this field is **443**, which is the communications port on the Content Management System.
SSL	Allows the user to communicate via SSL.
Username	The Live account user name as provided by RSA Customer Care.
Password	The Live account user password as provided by RSA Customer Care.

Feature	Description
Test connection	Tests if the connection is successful or not.
Apply	Saves and applies the configuration.

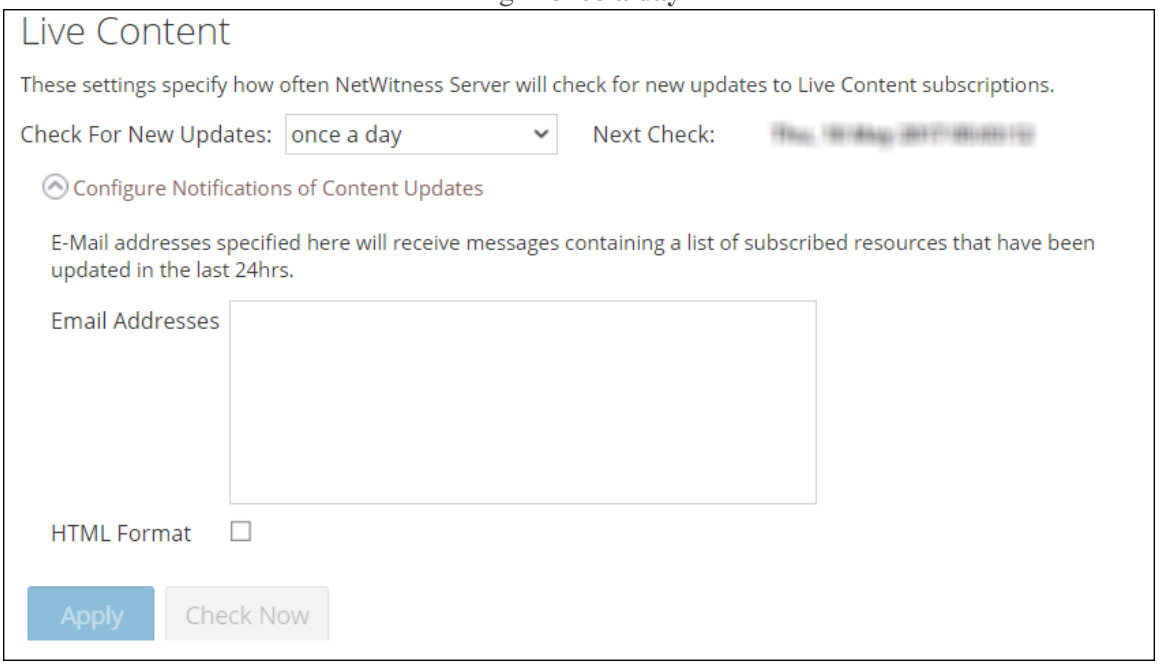
The Live Account section provides an option to download and share the Live Feedback historical data by clicking Live Feedback Activity Log.

For more information about how to download historical data, see Upload Data to RSA for Live Feedback

Live Content Section

You can configure the Live Content Synchronization interval and notification at which NetWitness Suite checks for new updates to Live Content:

Use the **Check for New Updates** field to change the interval. Select an interval from the drop-down list. The default value for this setting is **once a day**.



The following table describes the Live Content features.

Feature	Description
Check for new updates	This setting dictates how often NetWitness Suite checks for new updates to Live Subscriptions and synchronizes subscribed resources and tags: • once a day • twice a day • four times a day • every hour • every other hour • every half hour The default value for this setting is once a day.
Next Check	Displays the time and date of the next scheduled Live synchronization based on the configured interval for checking.
Email Addresses	Email addresses specified here receive messages containing a list of subscribed resources that have been updated in the last 24 hours.
HTML format	Specifies the format of email messages. • Checked = HTML • Not checked = text
Check Now	Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite. **Caution:** Use this feature with caution because synchronization can cause a parser reload if a Lua Parser or Flex Parser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.
Apply	Applies the changed configuration to the subscription synchronization behavior. The changes become effective immediately. The **Next Live synchronization is scheduled for** field is updated if the time changed.

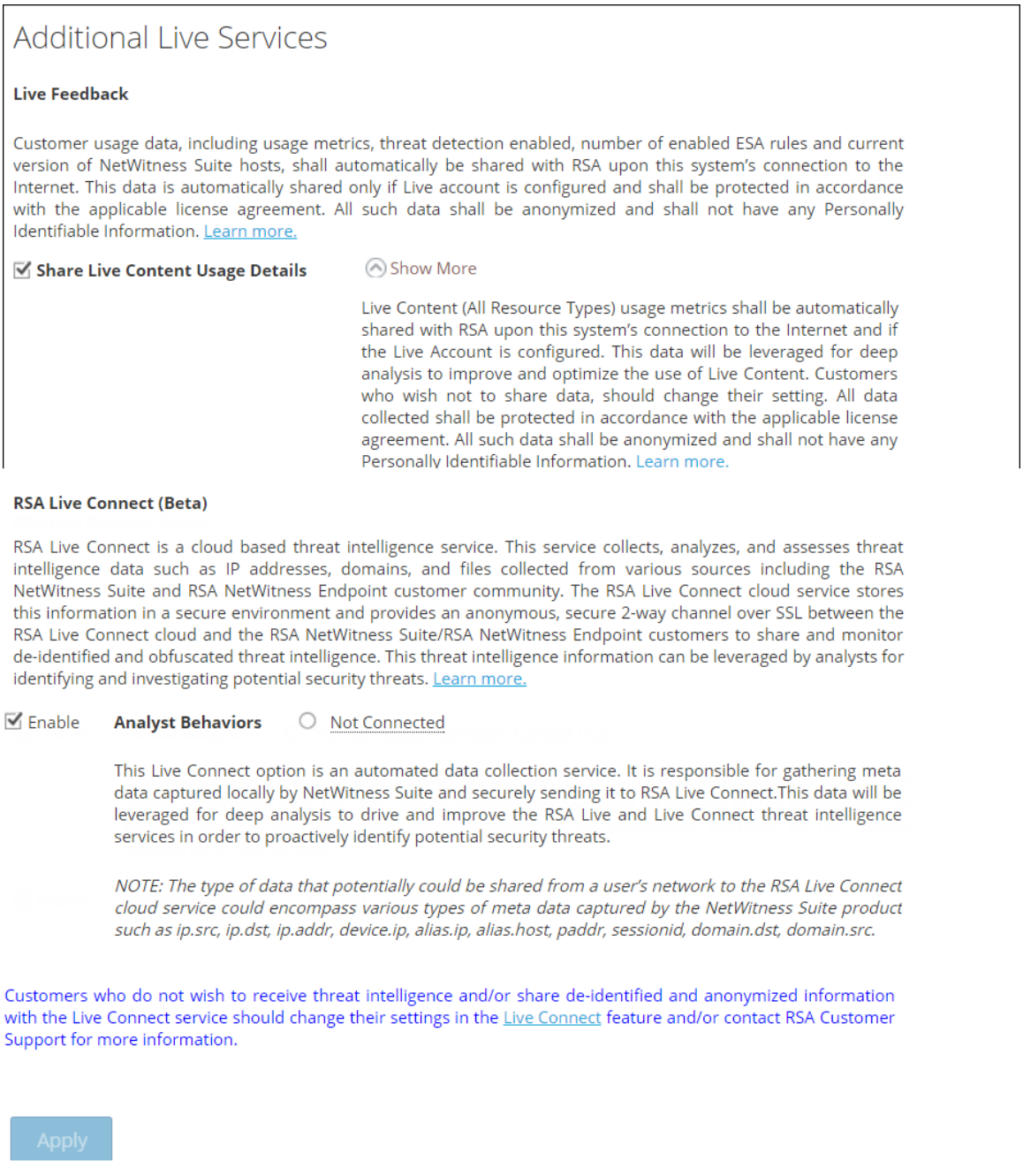
Force Immediate Synchronization

To force immediate synchronization, click **Check Now**. NetWitness Suite checks for updates in subscribed resources.

Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite. One use for this is to see the immediate impact of a configuration change. For example, a new service has been added, or new resources have been toggled for automatic deployment. The scheduled synchronization could take place hours later if Live Services is set to synchronize a few times a day.

Caution: Synchronization can cause a parser reload if a Flex Parser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.

Additional Live Services



Note: Click on Learn more to know more about the data RSA is collecting. For more information, see Live Feedback Overview

The following tables describes the Additional Live Services features.

Feature	Description

Live Feedback	Lists the types of data RSA is collecting:
	• Product Name
	• Product Version
	• Product Instance
	• Activation Key
	• Details of each Component such as:
	  • ID
	  • Name
	  • Version
	  • Instance ID
	• Metrics for each component

Share Live Content Usage Details)	Enables NetWitness Suite to send anonymous, technical data about the content usage metrics to RSA. This option is enabled by default.
RSA Live Connect	Provides more information about Live Connect service and configuring Live Services.
Enable (Threat Insights)	Enables Threat Insights feature where Live Connect is added as a data source for Context Hub service and the analyst can pull threat intel data during investigation. Ensure that context hub is already configured before enabling this feature. This option is enabled by default (checked).
Enable (Analyst Behaviors)	Enables NetWitness Suite to send anonymous, technical data about your environment to RSA. This option is enabled by default (checked).

Feature	Description
Apply	Applies the configured changes. The changes become effective immediately. **Note:** This option is applicable only for Threat Insights and Analyst Behaviors.

About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see Live Feedback Overview.

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see Configure Live Services Settings

If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see Upload Data to RSA for Live Feedback.

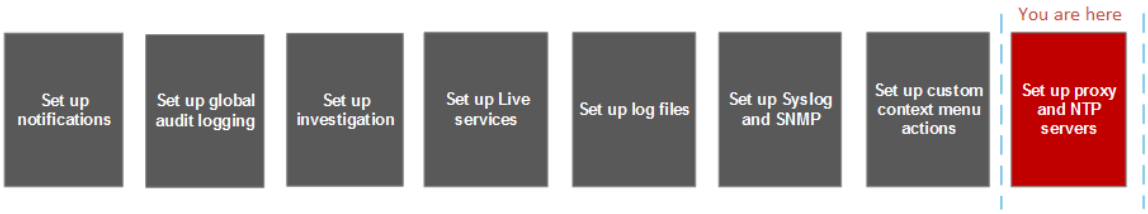
NTP Settings Panel

NTP setting panel is a protocol designed to synchronize the host machine clocks over a network. For more information on NTP see their home page (http://www.ntp.org/).

Note: NetWitness Suite core hosts must be able to communicate with the NW host with UDP port 123 for NTP time synchronization.

You use the**ADMIN** > **System** > **NTP Settings** view to configure one or more NTP servers. After you configure an NTP server, NetWitness Suite uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes.

Workflow



What you need to do?

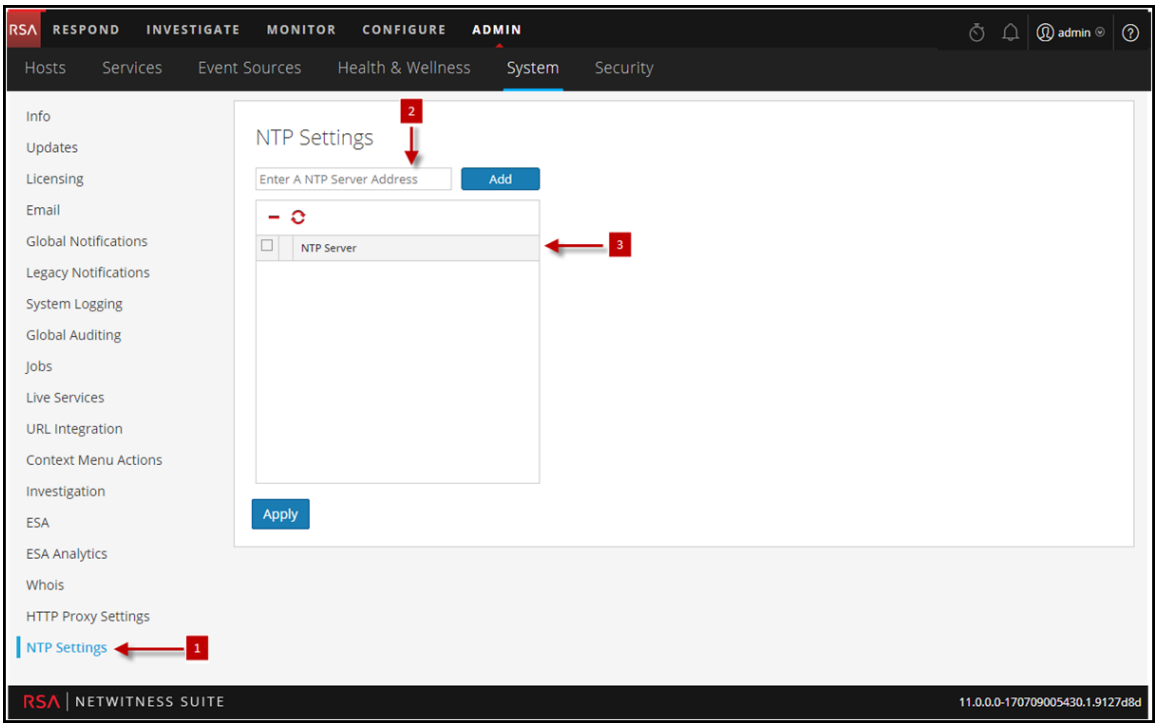
Role	I want to ...	Show me how
Administrator	Add or Modify an NTP Server	Configure NTP Servers

Related Topics

- Configure NTP Servers
- Troubleshooting NTP Server Configuration

Quick Look

The following example illustrates an NTP setting panel. The panel defines how to add NTP server to NTP setting panel.



1. Displays the NTP setting panel.
2. Enter the NTP Server IP Address or hostname.
3. Click on an existing hostname.

The following table describes the settings in the NTP Settings panel.

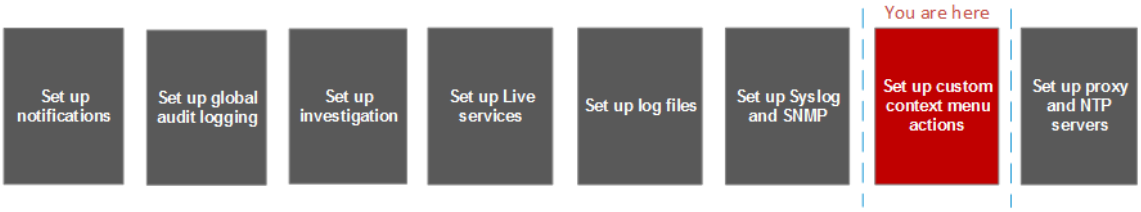
Setting	Description
Add	Enter the NTP Server IP Address or hostname to add the NTP server to NetWitness Suite.
	Delete the selected NTP server.
	Synchronizes the selected NTP server.
	Selects the NTP server that you want to delete or synchronize.

Setting	Description
NTP Server	NTP Server IP Address or hostname. If you click on an existing hostname, NetWitness Suite makes the hostname editable and displays the following command buttons: • **Update** - Applies your edits. • **Cancel** - Cancels your edits.
Apply	Applies the NTP server settings and synchronizes host machine clocks to NTP.

Context Menu Actions Panel

In the Context Menu Actions panel, Administrators can view built-in context menu actions, and add, edit, or delete custom context menu actions that appear as options in a context menu.

Workflow

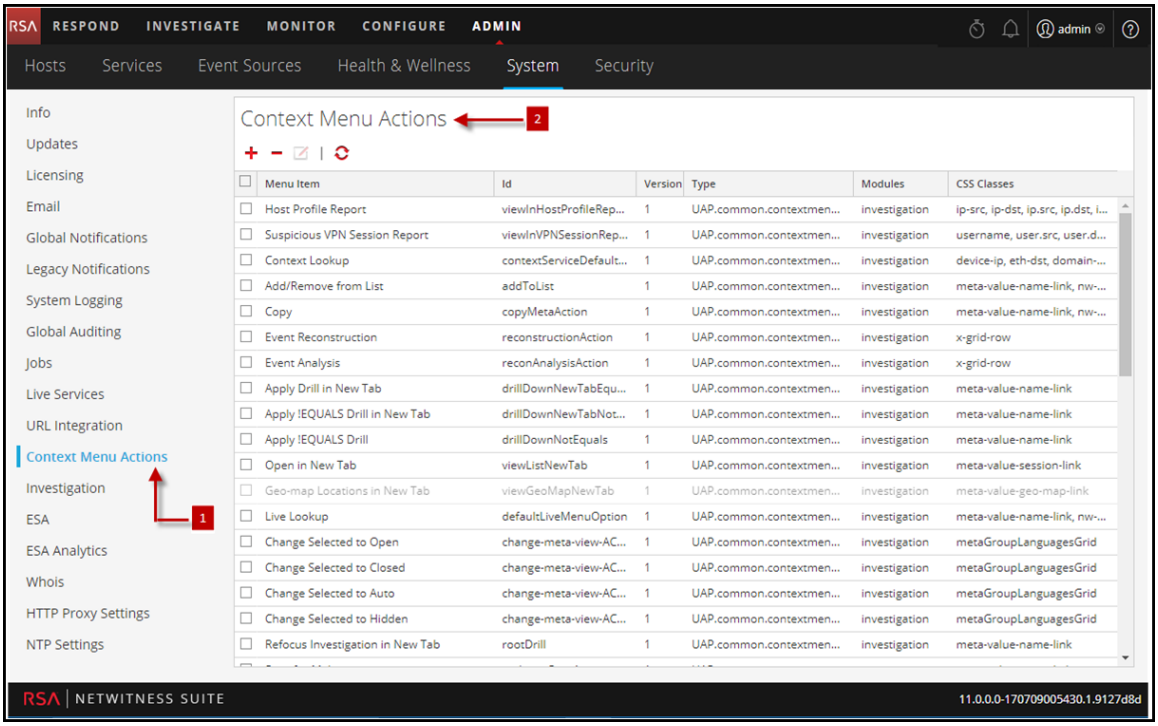


What do you want to do?

Role	I want to ...	Show me how
Administrator	Custom Context Menu Actions panel	Add Custom Context Menu Actions.

Quick Look

The following figure is an example of the Context Menu Actions panel.



1 Displays the Context Menu Actions Panel.

2 Toolbar allows you to Add, Edit, Delete Context Menu Actions.

The Context Menu Actions panel has a list and a toolbar. The following table describes the toolbar options and grid features.

Features	Description
	Displays the Context Menu Configuration dialog, in which you can create a new context action.
	Refreshes the list.
	Deletes the selected context actions. NetWitness Suite does not request confirmation that you want to delete the action. The selected actions are immediately deleted with no opportunity to cancel.
	Displays the Edit Context Action dialog, in which you can edit an existing context action.
Menu Item	The menu item as it appears in the context menu. When creating a context menu action, the parameter is `displayName`. Here is a line of sample code: `"displayName": "User Agent String Lookup”`
ID	The unique ID for the context action. When creating a context menu action, the parameter is `id`. Here is a line of sample code: `"id": "UserAgentStringAction"`
Version	The version number of the context action. When creating a context menu action, the parameter is `version`. Here is a line of sample code: `"version": "1"`

Features	Description
Type	The type of context action. When creating a context menu action, the parameter is `type`. All NetWitness Suite context action types begin with this string: `UAP.common.contextmenu.actions`. The last part of the string identifies the menu within NetWitness Suite, for example, `URLContextAction` or `LivePostContextAction`. Here is a line of sample code: `"type": "UAP.common.contextmenu.actions.URLContextAction"`

Modules	The names of the modules in which the context action is available. Currently all built-in context menu actions are for the Investigation module.
	When creating a context menu action, the parameter is `modules`.
	Here is a line of sample code:
	`"modules": [`
	`"investigation"`
	`],`

Module Classes	The CSS classes that identify the names of the module views in which the context action is available. Currently all built-in context menu actions are for the Investigation module and the non-meta key module classes are described in detail below.
	Here are a few lines of sample code:
	`"moduleClasses": [`
	`"UAP.investigation.navigate.view.NavigationPanel”,`
	`<-- Enabled in Navigate pane-->`
	`“UAP.investigation.events.view.EventGrid”`
	`],`

Features	Description

CSS Classes	The CSS classes to which the context menu action applies. The CSS classes define where the context menu shows up inside investigation when you right-click. When creating a context menu action, the parameter is `cssClasses`.
	Here is a line of sample code:
	`"cssClasses": [`
	`"client"`
	`]`
	Most of the CSS Classes that you can add are meta keys. You can also add certain non-meta key CSS classes. See additional details and examples below.

CSS Classes and Examples

CSS classes can be meta keys and non-meta keys.

Meta Key CSS Classes

One type of CSS class that you can add is meta keys. For meta keys that have a period, change the period to a dash when defining a CSS class. For example, the meta key `alias.host` becomes the CSS class `alias-host`. The meta key `ip.src` becomes the CSS class `ip-src`.

Non-Meta Key CSS Classes

Built-in non-meta key CSS Classes are also available. The classes in the following table define actions and the part of the user interface where the action is available.

CSS Class	Type	Description
`meta-value-session-link`	Action	Open on meta session count number
`meta-value-name-link`	Action	Open on meta value name
`nw-event-value`	Action	Use for reconstruction context actions on meta value
`UAP.investigation.navigate.view.NavigationPanel`	User interface	Applies to Navigate view

CSS Class	Type	Description
`UAP.investigation.events.view.EventGrid`	User interface	Applies to Event View
`UAP.investigation.reconstruction.view.content.ReconstructedEventDataGrid`	User interface	Applies to Event Reconstruction View

Example

This is a commented example of a context menu action to validate the user agent from the Client Application (client) meta key. The comments are removed automatically once applied in the Administration System view. The new menu item is displayed after restarting the browser.

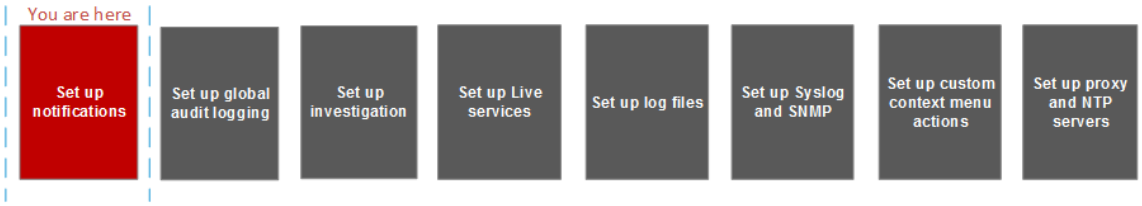
```
{
     "displayName": "User Agent String Lookup”, <!-- What name shows up in NW UI -->
     "cssClasses": [
         “client”  <!-- What meta key to launch from -->
     ],
     "description": "",
     "type": "UAP.common.contextmenu.actions.URLContextAction",
     "version": "1",
     "modules": [
         "investigation"
     ],
     "local": "false",
     "groupName": "externalLookupGroup”, <!-- What group to show link in. Remove line to show in main list -->
     "urlFormat": "http://www.useragentstring.com/?uas={0}&getText=all”, <!-- The {0} gets replaced with whatever was right clicked on -->
     "disabled": "",
     "id": "UserAgentStringAction",
    "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel”, <-- Enabled in Navigate pane-->
        “UAP.investigation.events.view.EventGrid” <-- Enabled in Event View pane -->
     ],
     "openInNewTab": "true",
     "order": "15"
 }
```

Legacy Notifications Configuration Panel

The Legacy Notifications Configuration panel provides the ability to configure syslog and SNMP notification settings. These configurations are used for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Procedures related to these settings are described in Configure Syslog and SNMP Settings.

Workflow



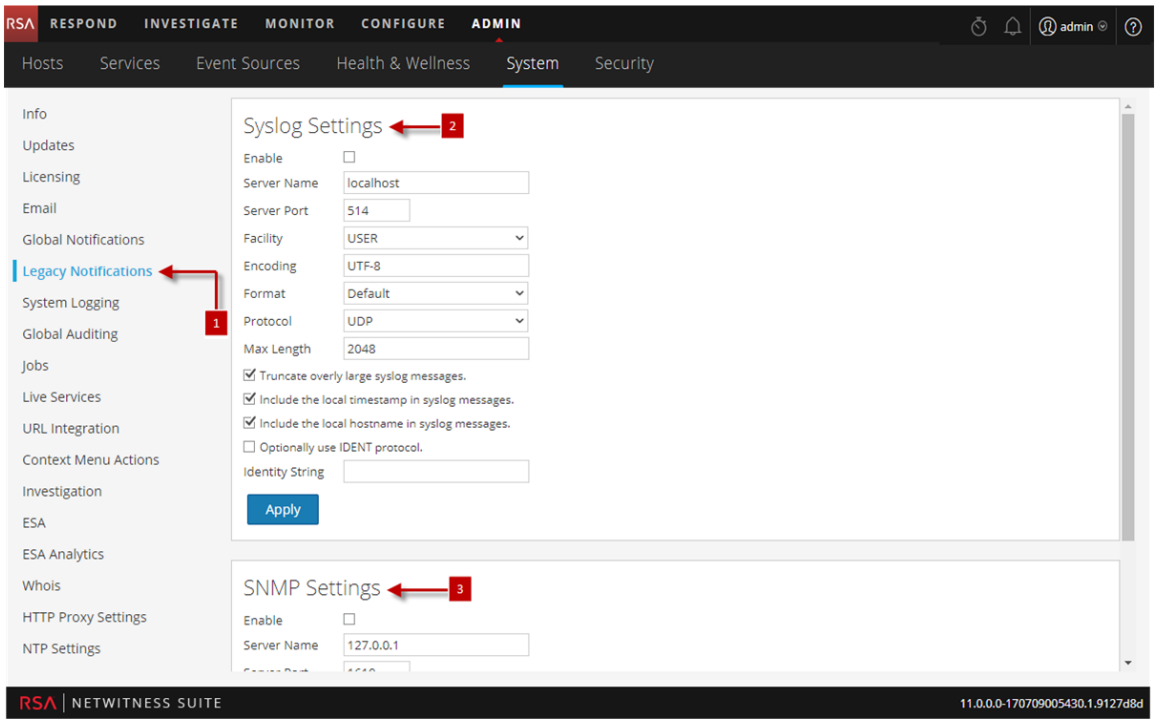
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Syslog Settings	Configure Syslog and SNMP Settings
Administrator	Configure SNMP Settings	Configure Syslog and SNMP Settings

Related Topics

- Configure Syslog and SNMP Settings

Quick Look



1	Displays the Legacy Notification Configuration Panel.
2	Allows the user to configure syslog notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.
3	Allows the user to configure SNMP notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

The Legacy Notifications Configuration Panel consists of two sections: Syslog Settings and SNMP Settings.

Syslog Settings

The following table describes the available options for configuring syslog notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Feature	Description
Enable	Enables the syslog settings configured here.

Feature	Description
Server Name	Specifies the host where the target syslog process is running.
Server port	Specifies the port where the target syslog process is listening.
Facility	Specifies the designated syslog facility to use for all outgoing messages. Possible values are KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL1 through LOCAL7.
Encoding	Specifies the encoding to use for text in syslog messages, for example, UTF-8.
Format	Specifies the message format. Possible values are: Default, PCI DSS, or SEC.
Protocol	Specifies the communications protocol used when sending syslogs: UDP or TCP. By default, the UDP protocol is selected.
Max length	Specifies the maximum length in bytes of any syslog message. The default value is **2048**. Messages that exceed the maximum length are truncated when the **Truncate overly large syslog messages** checkbox is selected.
Truncate overly large syslog messages	When checked, any messages exceeding the maximum length are truncated.
Include the local timestamp in syslog messages	When checked, NetWitness Suite includes the local timestamp in messages.
Include the local hostname in syslog messages	When checked, NetWitness Suite includes the local hostname in syslog messages.
Optionally use IDENT protocol	When checked, NetWitness Suite prepends the identity string to outgoing syslog alerts.

Feature	Description
Identity string	This is an identity string to be prepended to each syslog alert. If the string is blank, no identity string is prepended to the outgoing syslog alerts. You can use this to identify the source of the alert. Users conventionally set it to the name of the program that sends the syslog message.
Apply	Applies the syslog configuration settings.

SNMP Settings

The following table describes the available options for configuring SNMP notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Feature	Description
Enable	Enables the SNMP settings configured here.
Server Name	Specifies the SNMP trap host.
Server port	Specifies the listening port on the SNMP trap host
SNMP version	Specifies the SNMP version, **v1** or **v2c**.
Trap OID	Specifies the object ID for the SNMP trap on the trap host that receives the audit event. The default value is **0.0.0.0.0.1**.
Community	Specifies the community string used to authenticate on the SNMP trap host, the default value is **public**.
Enable	Enables SNMP notifications as configured here.
Apply	Applies the SNMP configuration settings.

RSA NETWITNESS® SUITE

System Maintenance Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2018

Contents

NetWitness Suite System Maintenance **7**

Best Practices **8**

Safeguarding Assets with RSA Supplied Policies 8

Safeguarding Assets with Policies Based on Your Environment 8

Creating Rules and Notifications Judiciously 8

Troubleshooting Issues 8

Monitoring Health and Wellness of NetWitness Suite **9**

Manage Policies 10

Add a Policy 10

Add Policy Example 13

Edit a Policy 15

Duplicate a Policy 16

Assign Services or Groups 17

Remove Services or Groups 19

Add or Edit a Rule 20

Hide or Show Rule Conditions Columns 20

Delete a Rule 21

Suppress a Rule 22

Suppress a Policy 22

Add an Email Notification 22

Delete an Email Notification 23

Include the Default Email Subject Line 23

Monitor System Statistics 25

Filter System Statistics 26

View Historical Graph of System Statistics 29

Monitor Service Statistics 31

Add Statistics to a Gauge or Chart 31

Edit Properties of Statistics Gauges 34

Edit Properties of Timeline Charts 35

Monitor Hosts and Services 36

Filter Hosts and Services in the Monitoring View 37

Monitor Host Details 39
Monitor Service Details 40
Monitor Event Sources 43
Configure Event Source Monitoring 43
Filter Event Sources 45
View Historical Graph of Events Collected for an Event Source 46
Monitor Alarms 48
Monitor Health and Wellness Using SNMP Alerts 49
Troubleshooting Health & Wellness 52
Issues Common to All Hosts and Services 52
Issues Identified by Messages in the Interface or Log Files 52
Issues Not Identified by the User Interface or Logs 58

Managing NetWitness Suite Updates 61

Displaying System and Service Logs 62

View System Logs 62
Display Service Logs 62
Filter Log Entries 63
Show Details of a Log Entry 63
Access Reporting Engine Log File 64
All Log Files 64
Upstart Logs 64
Search and Export Historical Logs 65
Display the Historical System Log 65
Display a Historical Service Log 66
Search Log Entries 66
Show Details of a Log Entry 67
Page Through Log Entries 67
Export a Log File 67

Maintaining Queries Using URL Integration 68

Edit a Query 68
Delete a Query 69
Clear All Queries 70
Use a Query in a URI 70

FIPS Support **72**
FIPS support for Log Collectors 72
FIPS support for Log Decoders and Decoders 73
Troubleshoot NetWitness Suite **74**
Debugging Information 74
NetWitness Suite Log Files 74
Files of Interest 75
Error Notification 77
Miscellaneous Tips 78
Audit Log Messages 78
NwConsole for Health & Wellness 79
Thick Client Error: remote content device entry not found 79
View Example Parsers 79
Configure WinRM Event Sources 79
NwLogPlayer 79
Usage 79
Troubleshoot Feeds 81
Overview 81
Details 81
How it Works 81
Feed File 82
Troubleshooting 82
References **88**
Health and Wellness View 89
Health and Wellness View - Alarms View 90
Event Source Monitoring View 94
Health and Wellness Historical Graphs 98
Health and Wellness Settings View - Archiver 103
Health and Wellness Settings View - Event Sources 106
Health and Wellness Settings View - Warehouse Connector 112
Monitoring View 115
Monitor tab 126
ESA Analytics Details 128
Health Status 128

Collection Tab 132
Event Processing Tab 132
Policies View 138
Health & Wellness Default SMTP Template 145
Alarms Template 146
System Stats Browser View 157
System View - System Info Panel 161
System Updates Panel - Settings Tab 164
What do you want to do? 164
Related Topics 164
Quick Look 164
Features 165
System Logging - Settings View 166
What do you want to do? 166
Related Topics 166
Quick Look 167
Features 167
System Logging - Realtime Tab 169
What do you want to do? 169
Related Topics 169
Quick Look 170
Features 171
System Logging - Historical Tab 172
What do you want to do? 172
Related Topics 172
Quick Look 173
Features 174
Search Log Entries 175
Show Details of a Log Entry 175

NetWitness Suite System Maintenance

This guide encompasses the tasks that administrators perform after initial network setup to allow NetWitness Suite to manage hosts and services in the network, maintain and monitor the network, manage jobs, and tune performance.

The following diagram shows the different system maintenance tasks available to you.

The following topics describe these tasks:

- Best Practices
- Monitoring Health and Wellness of NetWitness Suite
- Displaying System and Service Logs
- Maintaining Queries Using URL Integration
- Managing NetWitness Suite Updates
- FIPS Support
- Troubleshoot NetWitness Suite

Best Practices

Safeguarding Assets with RSA Supplied Policies

The purpose of the RSA Core Policies delivered with NetWitness Suite is to help you safeguarding your NetWitness Suite Domain assets immediately (before you configure rules specific to your environment and your Security Policy).

RSA recommends that you set up email notifications to the appropriate asset owners for these policies as soon as possible. This will notify them when performance and capacity thresholds are crossed so they can take action immediately.

RSA also recommends that you evaluate the Core policies and disable a policy or change its service/group assignments according to your specific monitoring requirements.

Safeguarding Assets with Policies Based on Your Environment

RSA Core Policies are generic and may not provide sufficient monitoring coverage for your environment. RSA recommends that you gather issues over a period of time, not identified by the RSA Core Policies, and configure rules to help you prevent these issues.

Creating Rules and Notifications Judiciously

RSA recommends that you make sure that each rule and policy is necessary before you implement it, if possible. RSA also recommends that you review implemented policies or a regular basis for their validity. Invalid alarms and email notifications can adversely affect the focus of the asset owners.

Troubleshooting Issues

RSA recommends that you review Troubleshooting Health & Wellness and Troubleshoot NetWitness Suite when you receive error messages in the user interface and log files from hosts and services.

Monitoring Health and Wellness of NetWitness Suite

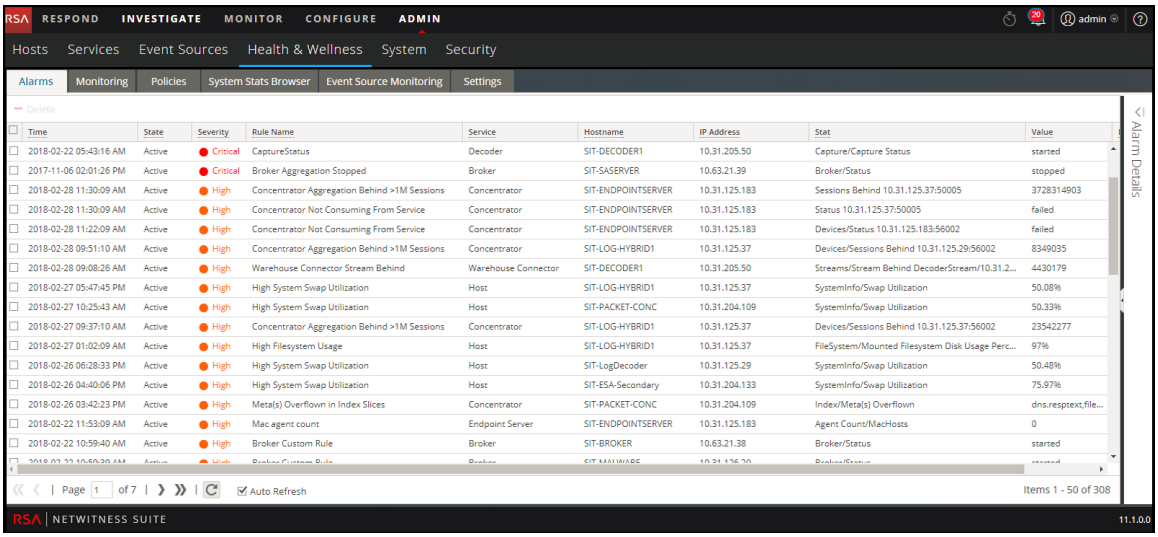
The Health & Wellness module of NetWitness Suite provides the ability to:

- View the current health of all the hosts, services running on the hosts, and various aspects of the hosts' health.
- Monitor the hosts and services in your network environment.
- View details of various event sources configured with NetWitness Suite.
- View system stats for the selected hosts by filtering the views as required.

In addition, you can configure Archiver monitoring and Warehouse Connector monitoring, use the procedures on monitoring host statistics, and work with system logs to monitor NetWitness Suite.

Note: All users have permission to view the entire Health and Wellness interface by default. The Administrator and the Operator roles are the only roles that can manage the Policies view by default. Please refer to the "Role Permissions" topic in the *Security User Management Guide* for a complete list of the default permissions for the NetWitness Suite Interface.

The figure displays the Health & Wellness module of the NetWitness Suite user interface and various sections in the Health & Wellness module.



Manage Policies

Policies are either user-defined or supplied by RSA. A policy defines:

- Services and hosts to which the policy applies.
- Rules that specify statistical thresholds that govern alarms.
- When to suppress the policy.
- Who to notify when an alarm triggers and when to notify them.

For the related reference topics, see NetWitness Suite Out-of-the-Box Policies

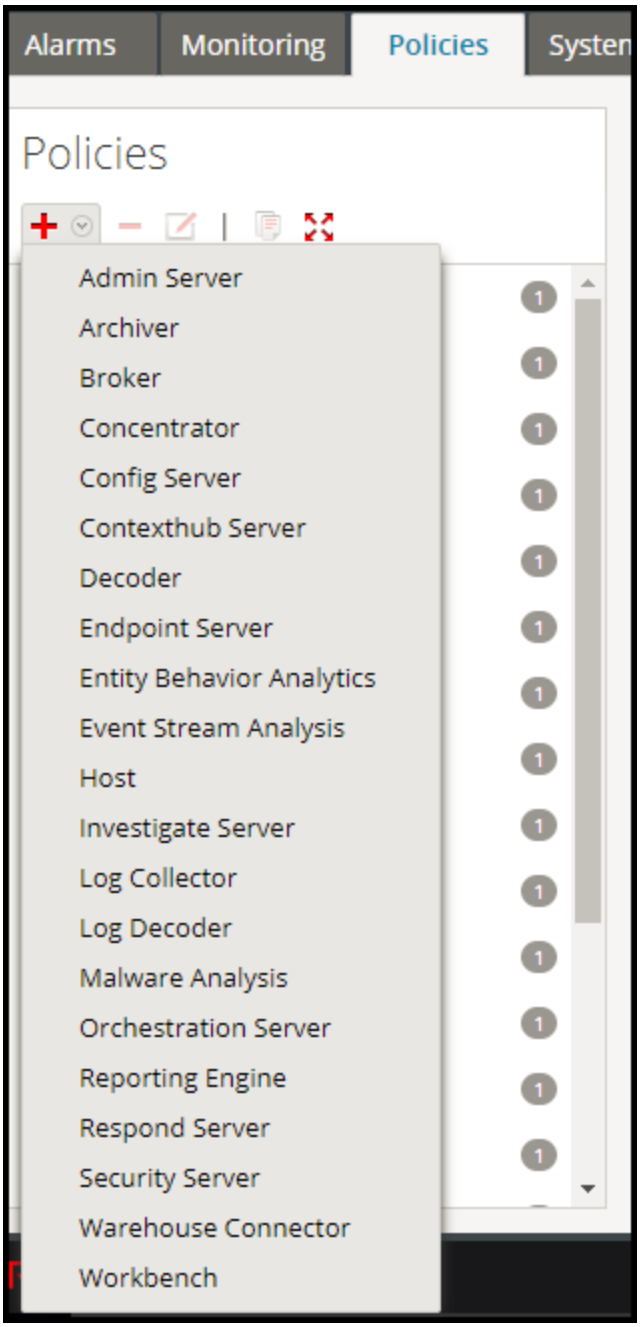
Note: You can now configure a policy to notify Public Key Infrastructure (PKI) certificate expiration status.

Add a Policy

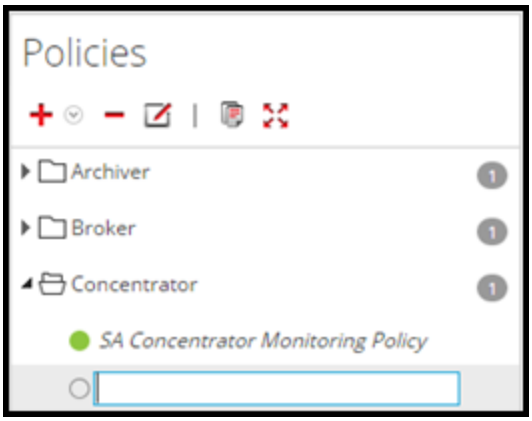
1. Go to **ADMIN > Health & Wellness.**
2. Click **Policies** tab.

   The Policies view is displayed.
3. Click in the **Policies** panel.

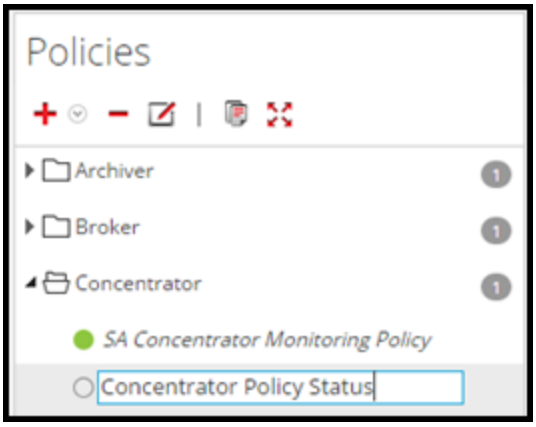
   A list of your hosts and services displays for which you can create health policies.



4. Select a host or service (for example, **Concentrator**).
   For PKI policy, you must select a host (for example, Host).
   The host or service is displayed in the Policies panel with a blank Policy Detail panel.



5. Enter a name for the Policy (for example, **Concentrator Policy Status**) in the **Policies** panel.



The name (for example, **Concentrator Policy Status**) is now displayed as the policy name in Policy Detail panel.

6. Create a Policy in the Policy Detail panel:

   a. Select the **Enable** checkbox.

   b. Add relevant services (in this example, any relevant Concentrator services) that you want to monitor for health statistics.
   For PKI policy, you must select the LOCALHOST to monitor for health statistics.

   c. Add relevant rule conditions you want to configure for the policy.

   d. Suppress enforcement of the policy for the time periods you want.

   e. Add any email notifications you want for the policy.

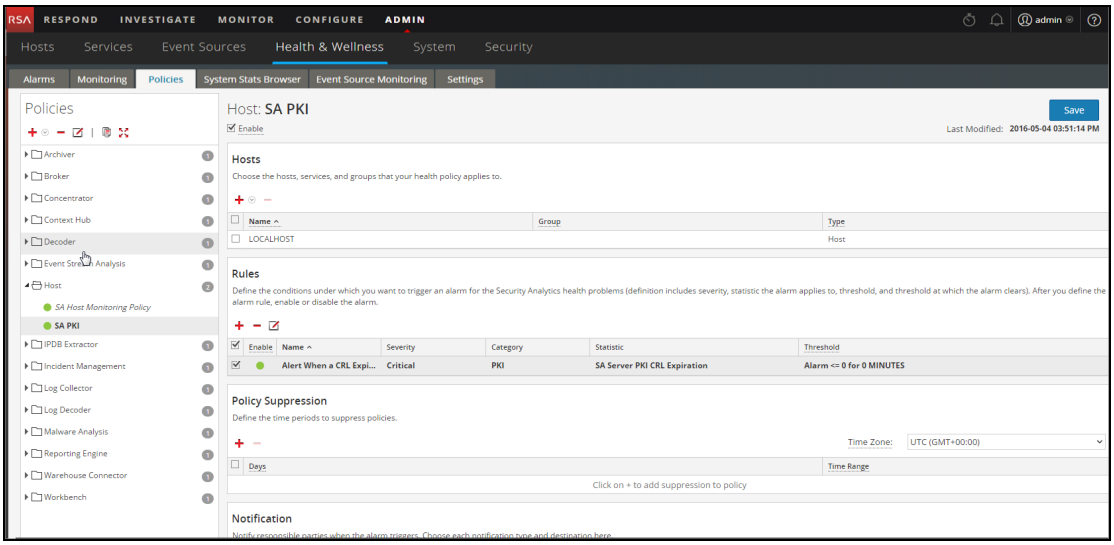
   f. Click **Save** in the Policy Detail panel.

   The Policy is added.

Add Policy Example

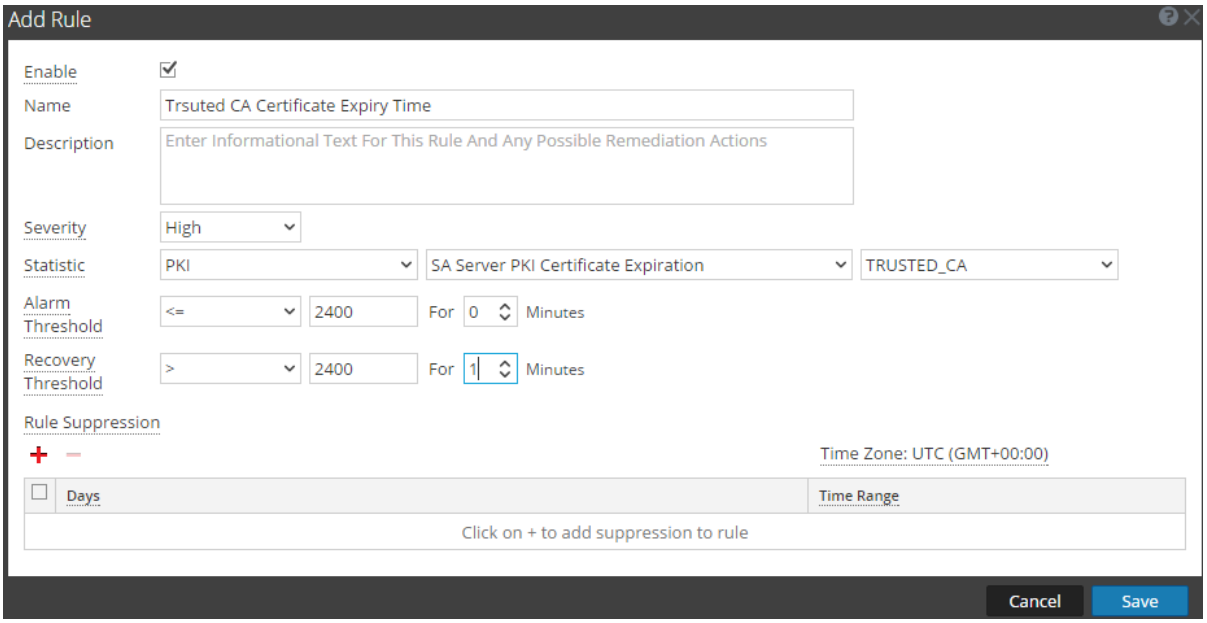
Below is the high-level example for configuring PKI policy:

1. Add a new PKI policy.

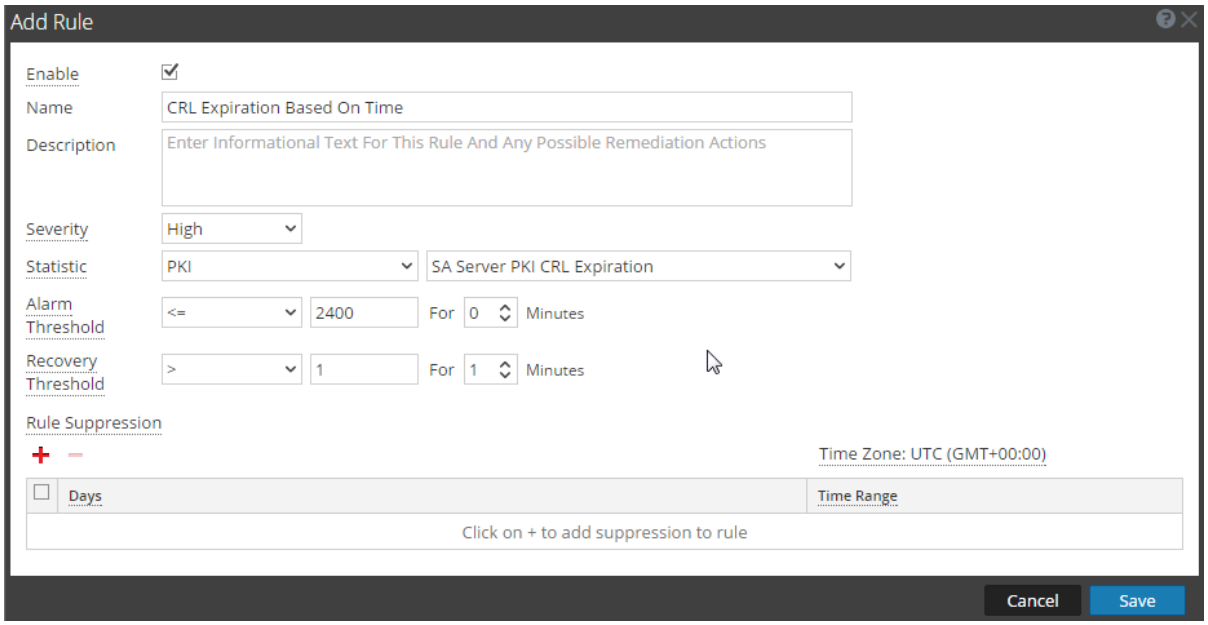


2. Add a Rule with Statistics:

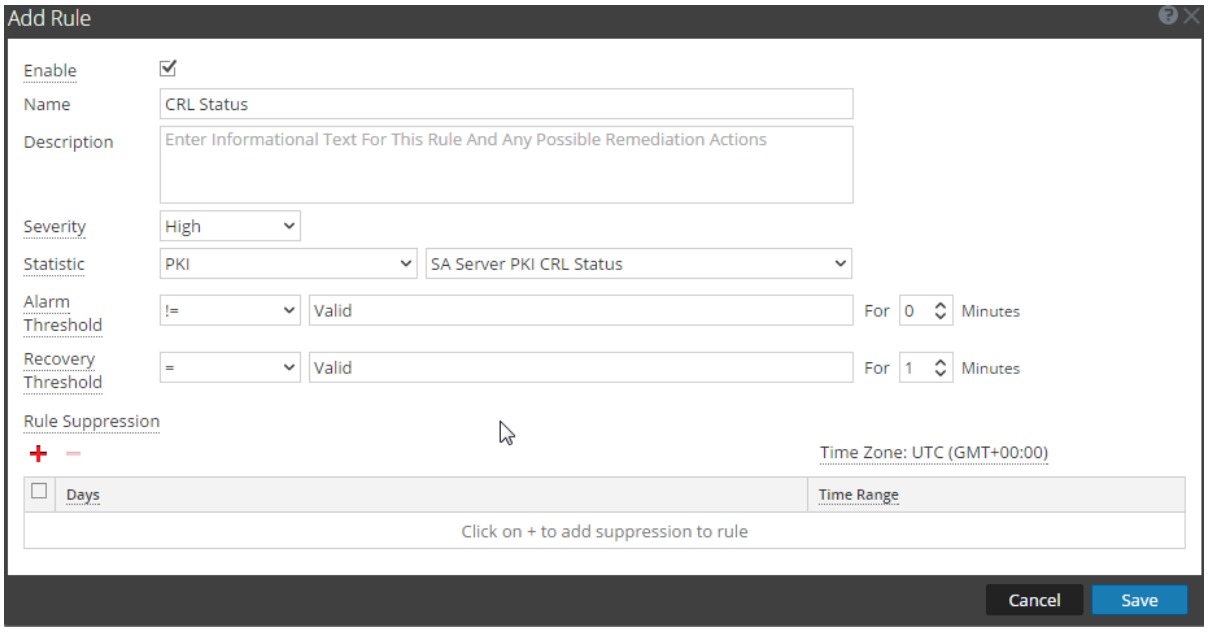
   - For CA Expiration



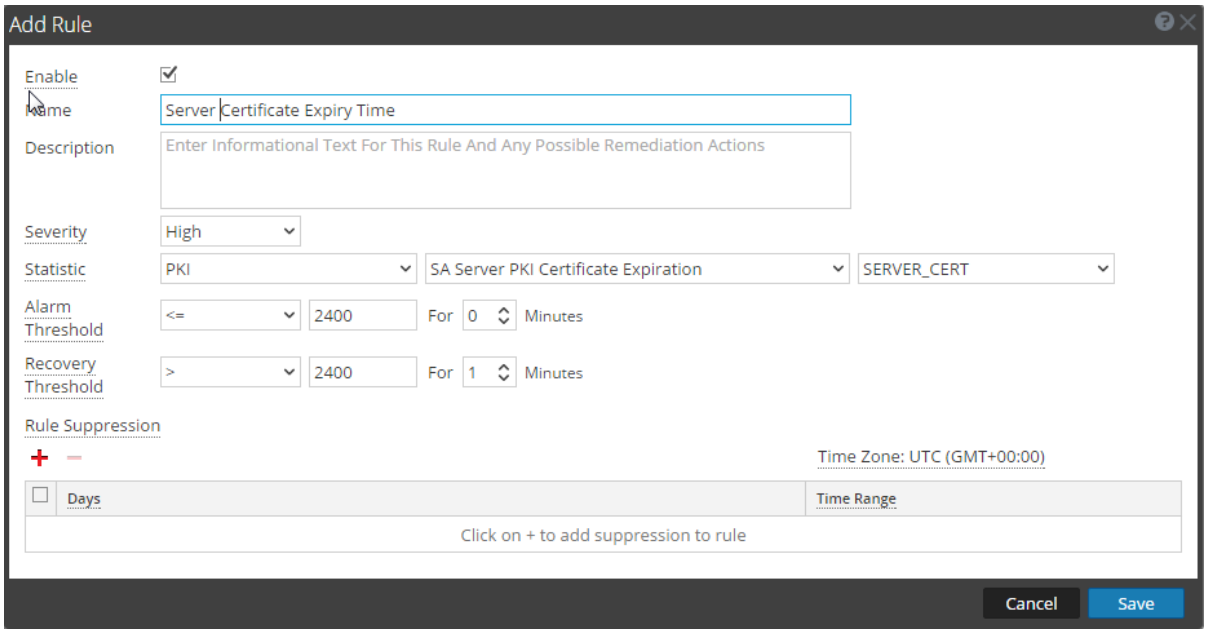
   - For CRL Expiration



- For CRL Status



- For Server Certificate Expiration



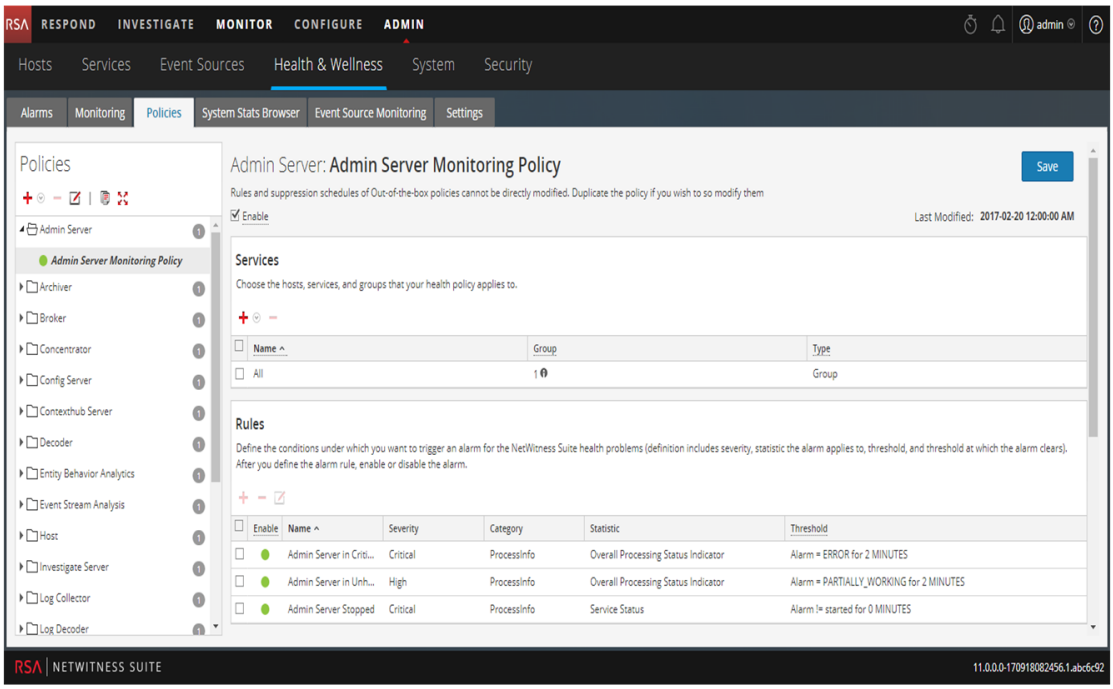
Edit a Policy

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.
3. Select a policy (for example, **Concentrator Policy Status**) under a host or service.

   The Policy Detail is displayed.
4. Click .

   The policy name (for example, **Admin Server Monitoring Policy**) and policy detail panel become editable.

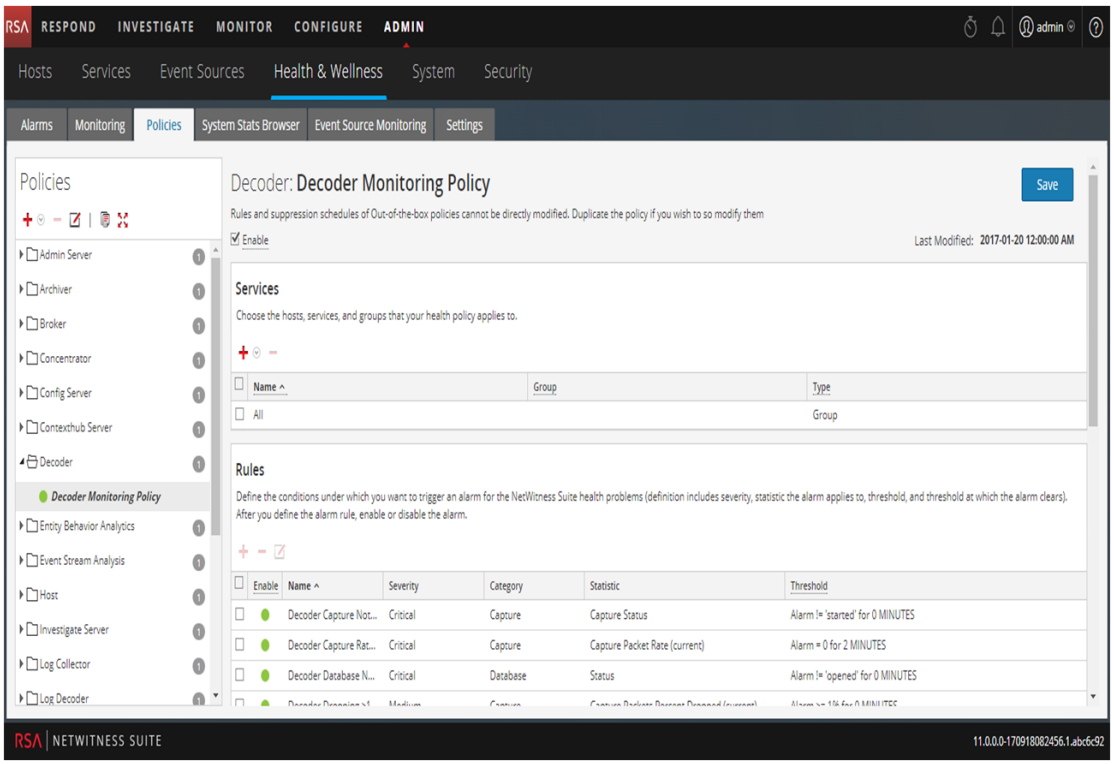


5. Make the required changes and click **Save** in the Policy Detail panel. You can:
   - Edit the Policy name.
   - Enable or disable the policy.
   - Add or delete hosts and services in the policy.
   - Add, delete or modify rules in the policy.
   - Add/Edit/Delete suppressions in the policy.
   - Add/Edit/Delete notifications in the policy.

Note: Save applies the policy rules based on the selection of enable/disable. It also resets the rule condition timers for changed rules, and the entire Policy.

Duplicate a Policy

1. Go to **ADMIN > Health & Wellness**.
2. Click the **Policies** tab.
3. Select a policy (for example, **Concentrator Policy Status**) under a host or service.
4. Click .NetWitness Suite copies the policy and lists it with **(1)** appended to the original policy's name.



5. Click and rename the Policy [for example, rename **Decoder Monitoring Policy(1)** to **New Concentrator Policy Status**.

> **Note:** A duplicated policy is disabled by default and the host and service assignments are not duplicated. Assign any relevant hosts and services to the duplicated policy before you use it to monitor health and wellness of the NetWitness Suite infrastructure.

Assign Services or Groups

To assign hosts or services to a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

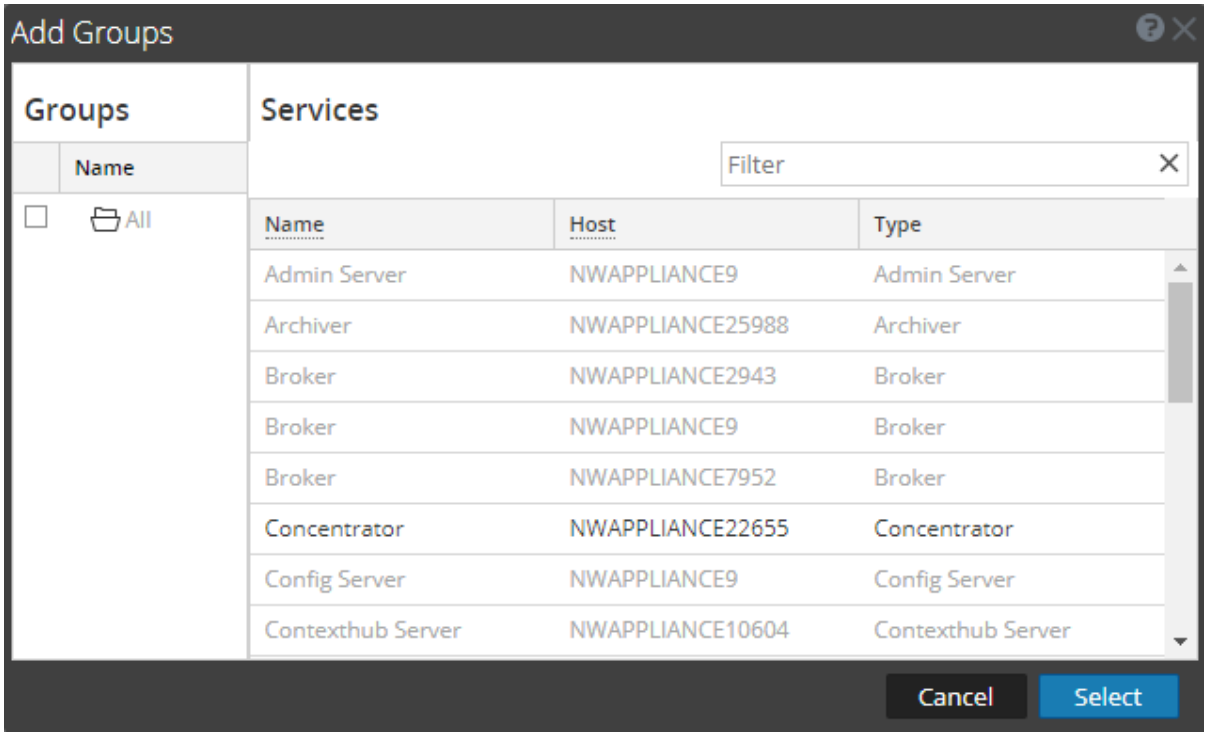
   The Policies view is displayed.
3. Select a policy (for example, **First Policy**) under a host or service.

   The Policy Detail is displayed.
4. Click in the Services and Groups list toolbar.
5. Choose one of the following actions:

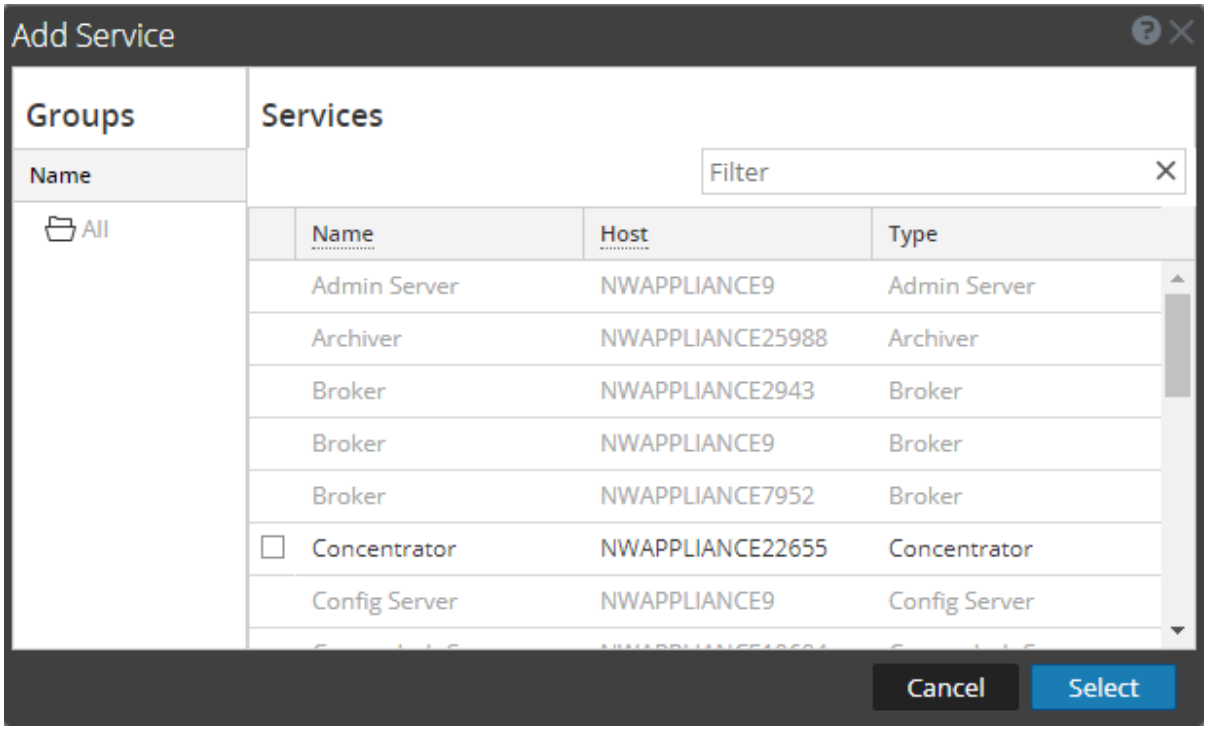
- For Hosts, select **Groups** or **Hosts** from the selection menu.
- For Services, select **Groups** or **Services** from the selection menu.

6. Depending on whether you are assigning services or groups, perform one of the following actions:

- **Groups**, the **Groups** dialog is displayed from which you can select predefined groups of hosts or services.



- **Services**, the **Services** dialog is displayed from which you can select individual services.



7. Select the checkbox next to the groups or services you want to assign to the policy, click **Select** in the dialog, and click **Save** in the Policy Detail panel.

Note: Services are filtered for selection based on the type of policies. For example, you can only select concentrator services for a concentrator type policy.

Remove Services or Groups

To remove a host or service from a policy:

1. Go to **ADMIN > Health & Wellness**.
2. Click **Policies** tab.

   The Policies view is displayed.
3. Select a policy under a service.

   The Policy Detail is displayed.
4. Select a host or service.
5. Click − .

   The host or service is removed from the policy.

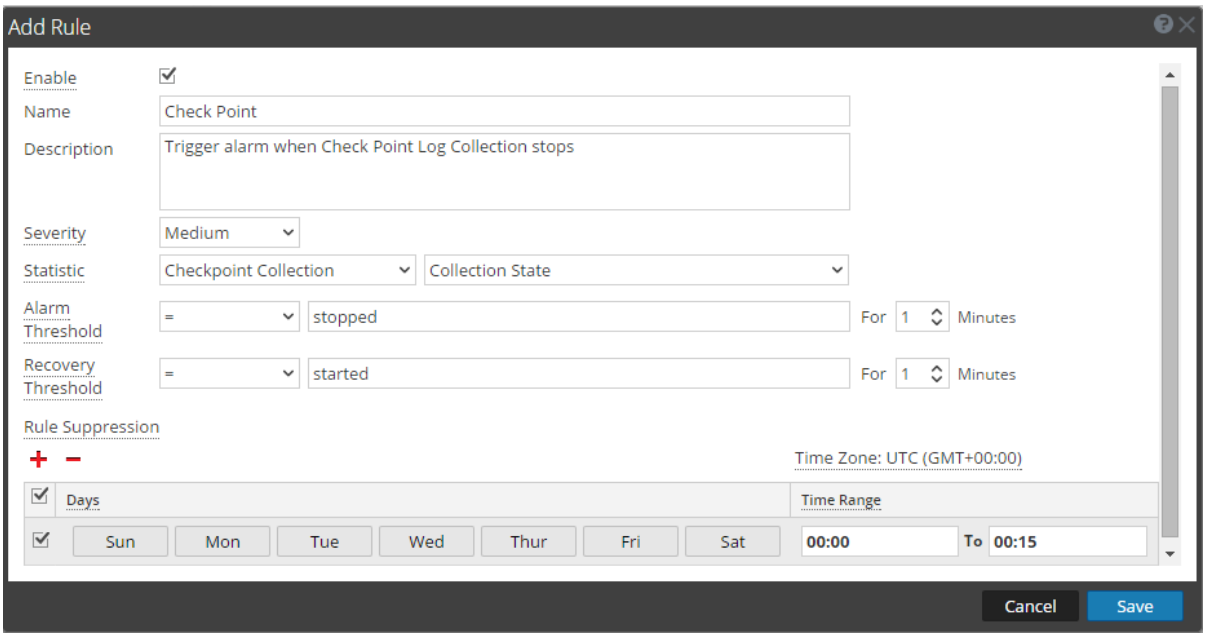
Add or Edit a Rule

To add a rule to a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.
3. Select a policy (for example, **Checkpoint**) under a host or service.

   The Policy Detail is displayed.
4. Depending on whether you are adding an existing rule or adding a rule, do the following:
   - To add: click + in the Rules list toolbar.
   - To edit: select a rule from the Rules list and click .
5. Complete the dialog to define or update the rule.
6. Add the **Description** field as shown in the following example.



7. Click **OK**.

   The rule is added (or updated) to the policy.

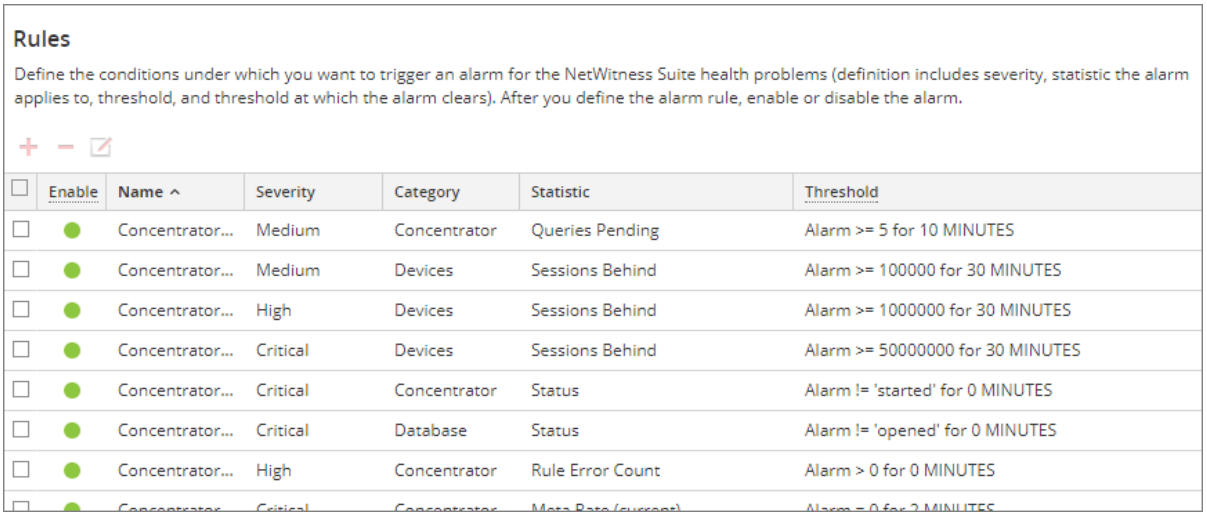
Hide or Show Rule Conditions Columns

To hide or show rule conditions columns in the Rules panel:

1. Go to **ADMIN > Health & Wellness.**
2. Click **Policies** tab.

   The Policies view is displayed.
3. Select a policy under a service.

   The Policy Detail is displayed.
4. Go to the **Rules** panel.



5. Click **v** to the right of **Category** , select **Columns**, and uncheck the **Static** and **Threshold** rule conditions.

   You can check or uncheck any Rules column to show or hide it.
   The **Rules** panel displays without the rule conditions.

Delete a Rule

To remove a host or service from a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.
3. Select a policy under a service.

   The Policy Detail is displayed.
4. Select a rule from the **Rules** list (for example, **Checkpoint**).
5. Click .

   The rule is removed from the policy.

Suppress a Rule

1. Click the **Policies** tab.
   The Policies view is displayed.
2. Select a policy under a service.
   The Policy Detail is displayed. You can specify rule suppressions time ranges when you initially add it or you can edit the rule and specify suppression time ranges.
3. Add or edit a rule.
4. In the **Rules Suppression** panel of the **Add** or **Edit Rule** dialog, specify the days and time ranges during which you want the rule suppressed.

Suppress a Policy

1. Add or edit a policy.
   The Policies view is displayed.
2. In the **Policy Suppression** panel:
   a. Select a time zone from the **Time Zone** drop-down list.
      This time zone applies to the entire policy (both policy suppression and rule suppression).
   b. Click + in the toolbar.
   c. Specify the days and time ranges during which you want the policy suppressed.

Add an Email Notification

To add an email notification to a policy:

1. Add or edit a policy.
   The Policies view is displayed.
2. In the **Notification** panel:
   a. Click + in the toolbar.
      A blank EMAIL notification row is displayed.
   b. Select the email:
      - Notification types in the Recipient column (see "Configure Notification Outputs" in the *NetWitness Suite System Configuration Guide* for the source of the values in this drop-down list).

- Notification server in the Notification Server column (see 'Configure Notification Servers" in the *NetWitness Suite System Configuration Guide* for the source of the values in this drop-down list).
- Template server in the Template column (see "Configure Notification Templates" in the *NetWitness Suite System Configuration Guide*for the source of the values in this drop-down list).

> **Note:** Refer to **Include the Default Email Subject Line** if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Delete an Email Notification

To add an email notification to a policy:

1. Add or edit a policy.
   The Policies view is displayed.
2. In the **Notification** panel:
   a. Select an email notification.
   b. Click .
   The notification is removed.

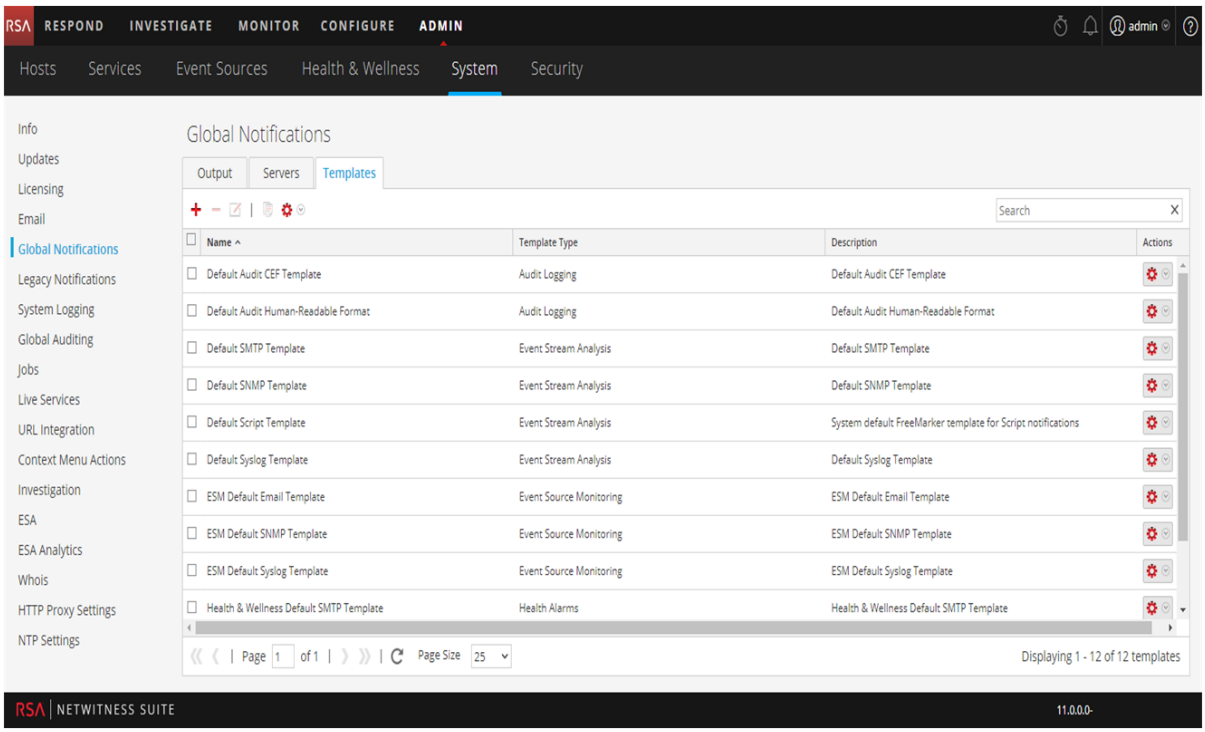
Include the Default Email Subject Line

The emails generated by the notifications you set up for policies do not include the subject line from the Health & Wellness Default Email Notification templates. You need to specify the subject line in the do not include subject lines. This procedure shows you how to insert a subject line into the templates.

For related reference topics, see Policies View and NetWitness Suite Out-of-the-Box Policies.

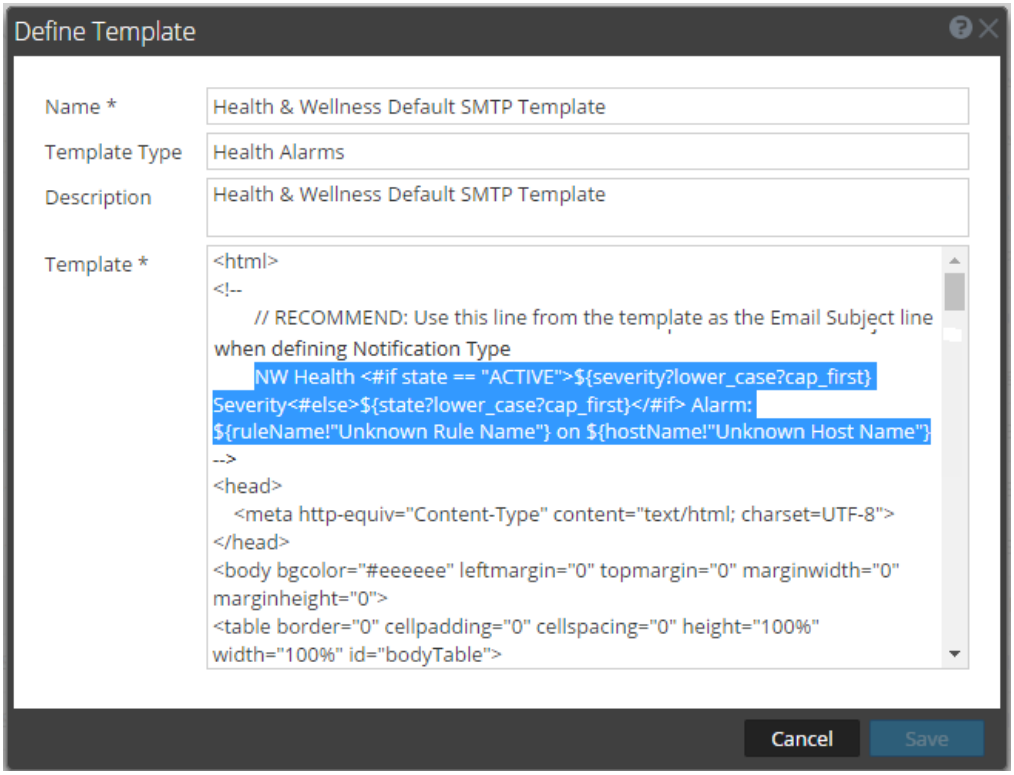
To include the subject line from a Health & Wellness email template in your email notification:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Select a Health & Wellness Email Template (for example, **Health & Wellness Default SMTP Template**).



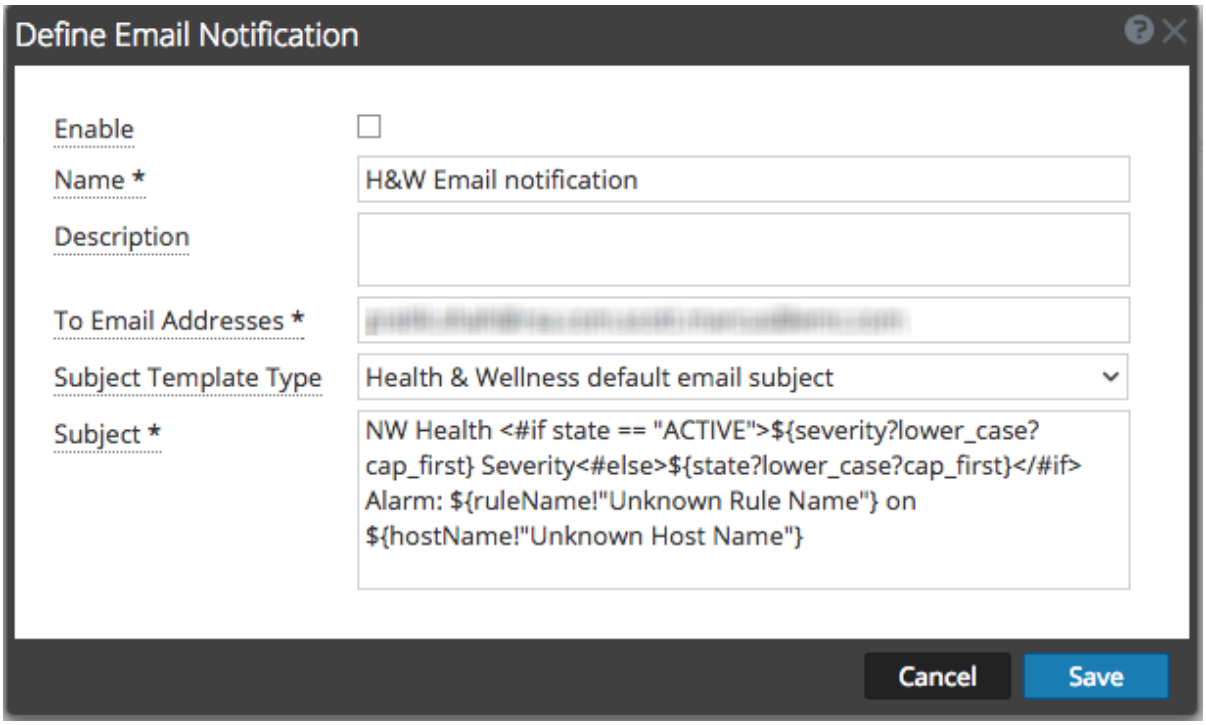
The Define Template dialog is displayed.

4. Click , then in the **Template** field, copy the Subject Line (Highlight the subject line and press Ctrl-C) into the buffer.



5. Click **Cancel** to close the Template.
6. Click the **Output** tab and select a notification (for example **Health & Wellness**).
7. Click .

   The **Define Email Notification** dialog is displayed.
8. Replace the value in **Subject** field text box with the subject line that you have in the buffer (highlight the existing text and press Ctl-V).



9. Click **Save**.

Monitor System Statistics

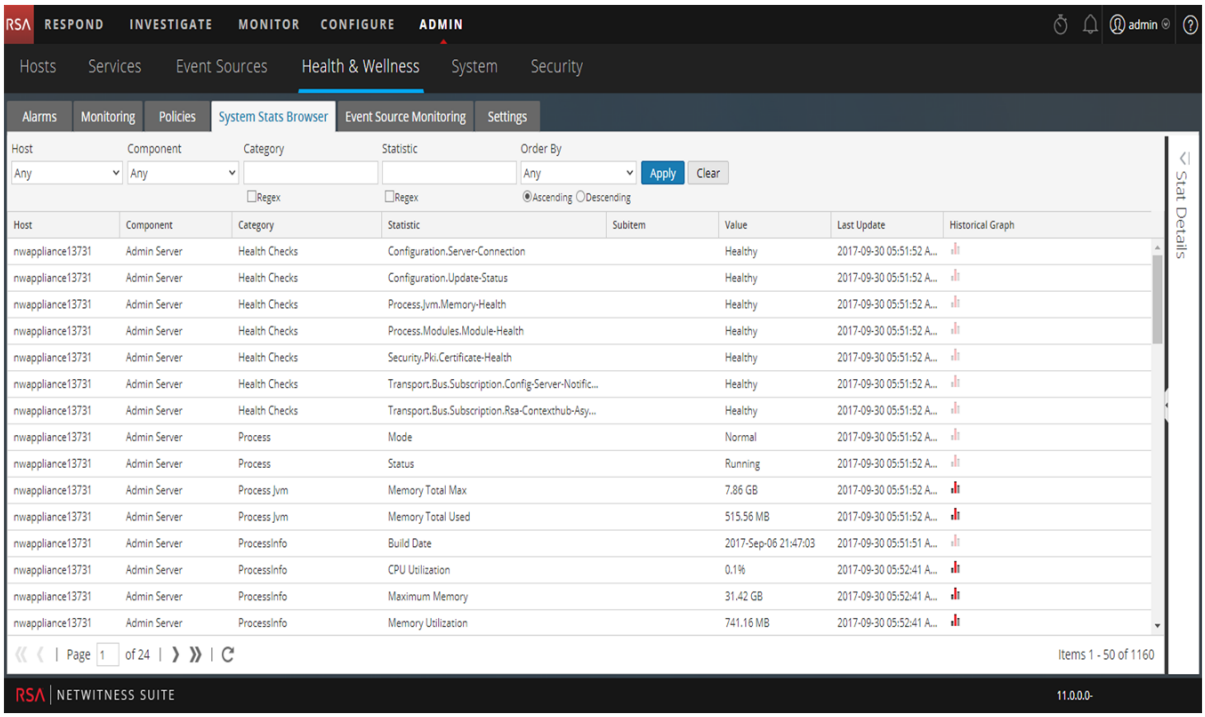
The System Stats Browser filters statistics by the selected host, component running on the host, statistical category, individual statistic, or any combination of host, component, category, and statistic. You can also choose the order in which to display this information.

To access the System Stats browser:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.
2. Click the **System Stats Browser** tab.

The System Stats Browser tab is displayed.



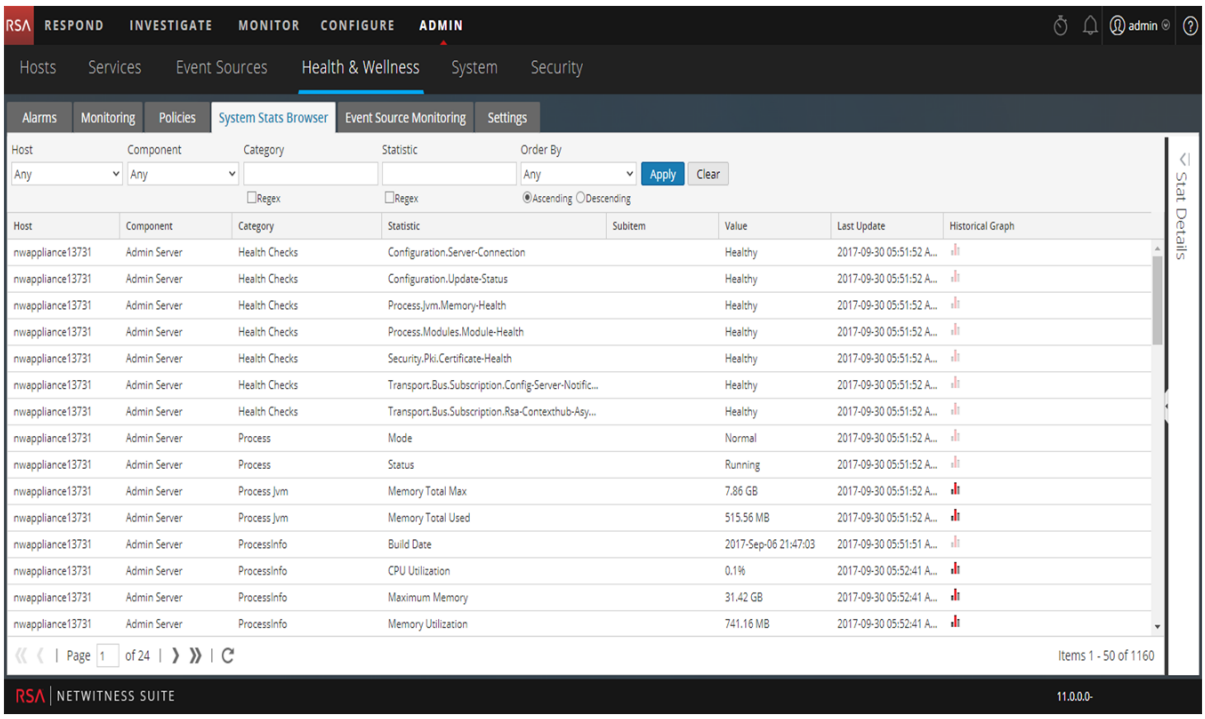
Filter System Statistics

You can filter the System Statistics in one of the following ways to monitor:

- Statistics collected for a particular host
- Statistics collected for a particular component
- Statistics collected of a particular type or that belongs to a certain category
- Statistics listed in an ordered way as per the selection chosen

To filter the list of system statistics:

1. Go to **ADMIN > Health & Wellness**.
   The Health & Wellness view is displayed with the Alarms tab open.
2. Click **System Stats Browser**.
   The System Stats Browser tab is displayed.

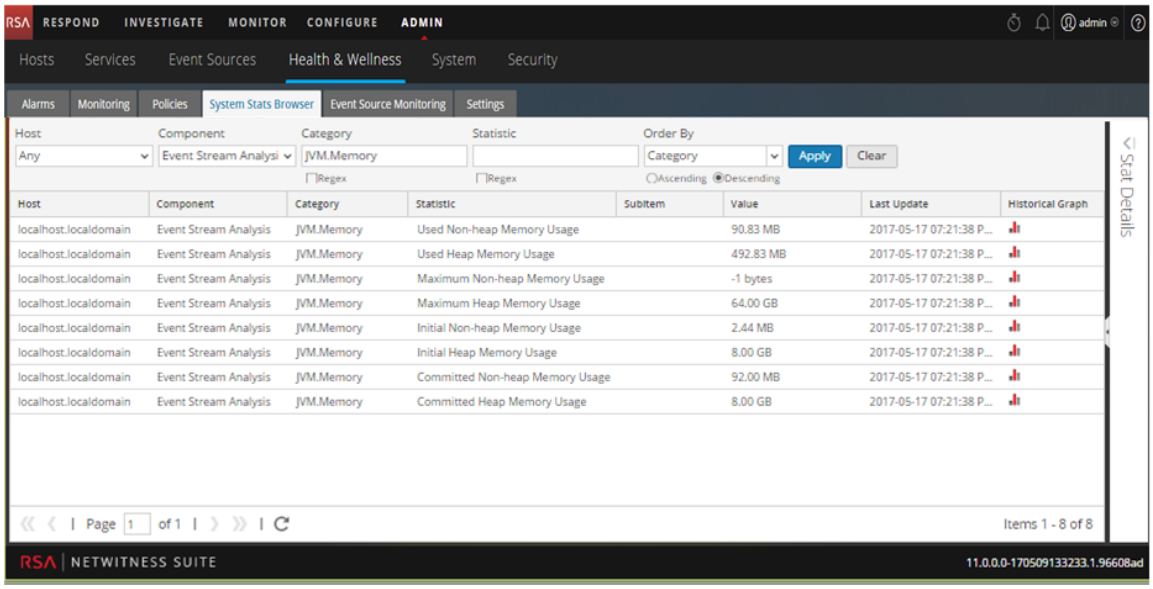


Filter the list of System Statistics in one of the following ways:

- To view System Stats of a particular host, select the host in the **Host** drop-down list.
  The System Stats for the selected host is displayed.
- To view System Stats of a particular component, select the component in the **Component** drop-down list.
  The System Stats for the selected component is displayed.
- To view System Stats of a particular category, type the category name in the **Category** field.
  Select **Regex** to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
  The System Stats for the selected category is displayed.
- To order the list of statistics in a preferred order you can set the order in the **OrderBy** column
- To view a particular statistic across hosts, type the statistic name in the **Statistic** field.
  Select **Regex** to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
  The System Stats for the selected statistics is displayed.

  The following figure shows the System Stats Browser filtered by the

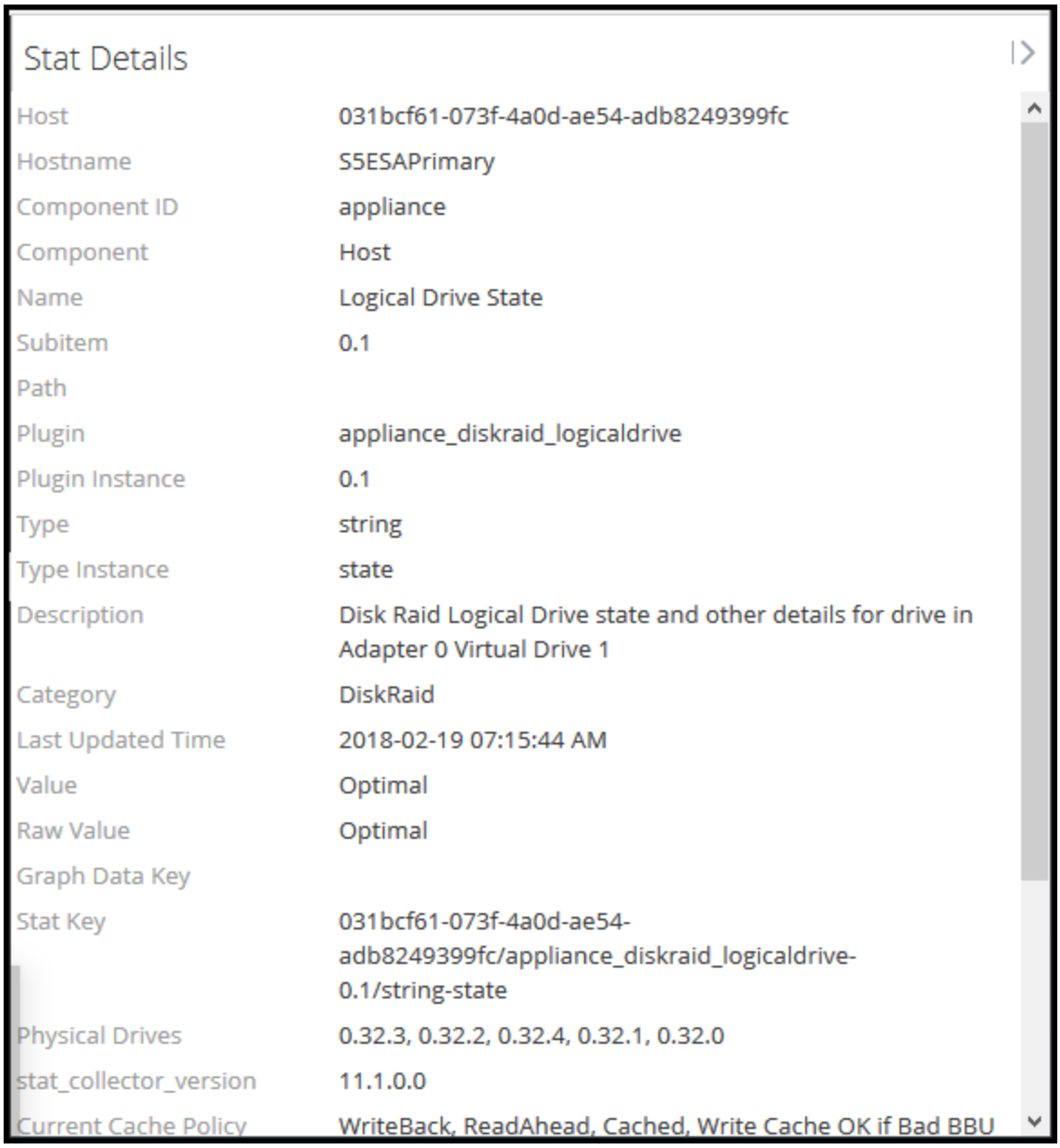
NWAPPLIANCE10604 host listed in descending statistical category order.



4. To view the details for an individual statistic:

   a. Select a row to select a statistic.

   b. Click <|.
   The Stat Details is displayed.



For details on various parameters in the **ADMIN** > **Health & Wellness** > **System Stats Browser** view, see System Stats Browser View

View Historical Graph of System Statistics

The historical graph of the collected system stats gives you information about the variation of the stats over a time frame selected.

To view a historical graph:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

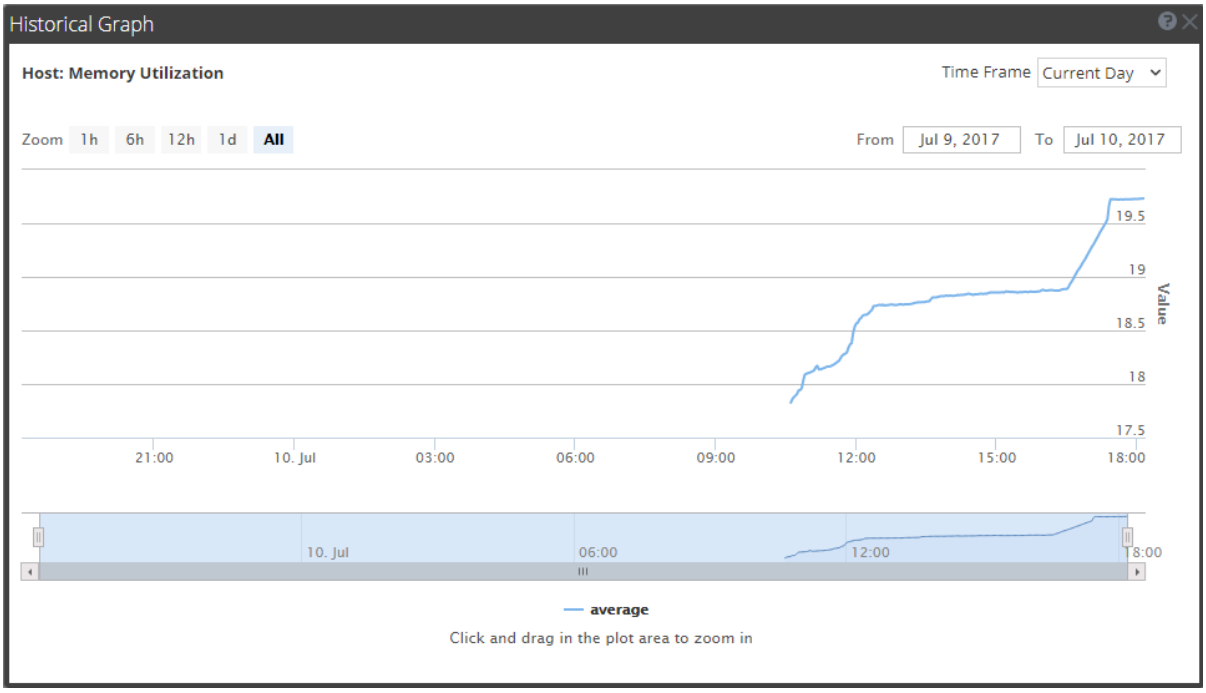
2. Click the **System Stats Browser** tab.

3. In the System Stats Browser tab, specify the filter criteria to display the statistics you want.

4. In the **Historical Graph** column, select .

   The Historical graph for the selected statistic is displayed.

   The figure below gives an example of the historical graph for Memory Utilization statistic for a host.



   The graphical view is customized to display the statistics collected for the current day and the values are zoomed in for an interval of an hour (10.15 - 11.15 hrs). Hover over the graph to view the details at a particular instant. For example, in the figure it displays the memory utilization at 11.00 hrs.

Note: You can customize the graph view by selecting the Time Frame and Date range. You can zoom in using the zoom in value, time window, or by just a click and a drag in the plot area. For details on the parameters to customize and zoom in functions, see Historical Graph for System Stats. Any break or gap in chart line indicates that the service or host was down during that time.

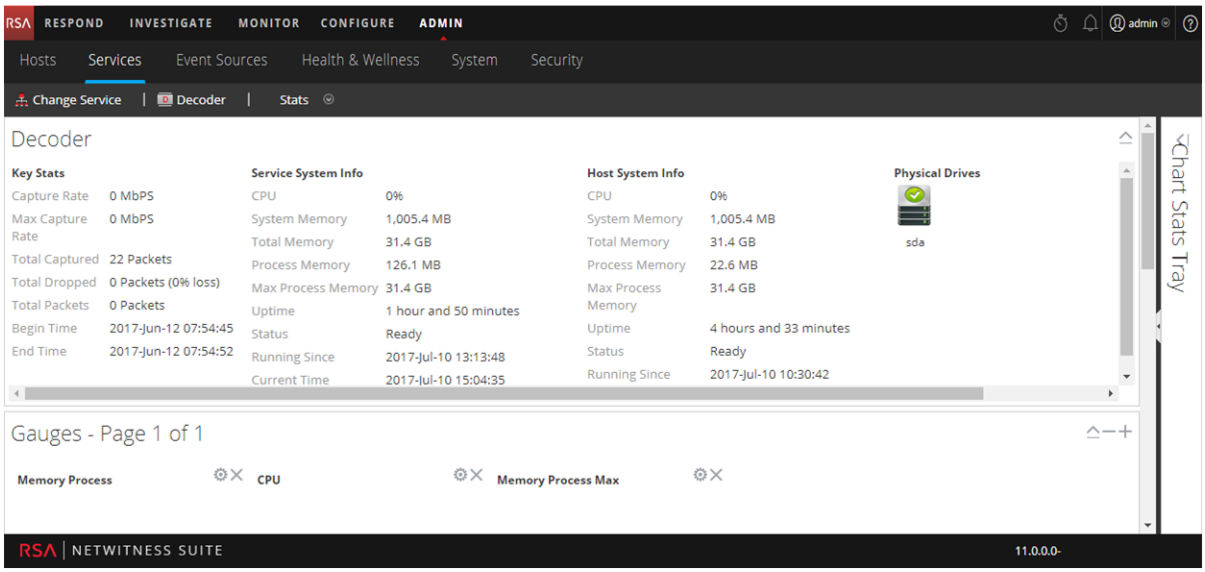
Monitor Service Statistics

NetWitness Suite provides a way to monitor the status and operations of a service. The Service Stats view displays key statistics, service system information, and host system information for a device. In addition more than 80 statistics are available for viewing as gauges, and in timeline charts. Only statistics for session size, sessions, and packets are viewable in historical timeline charts.

Although different statistics are available for different types of services, certain elements are common for any Core device.

To monitor service statistics in NetWitness Suite:

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. Select a service, and select **View > Stats** in the Actions column.



3. To customize the view: Collapse or expand charts, for example expand the Chart Stats Tray to see available charts. Drag a section up or down to change the sequence. For example, drag the Gauges section to the top so that it is above the Summary Stats section.

Add Statistics to a Gauge or Chart

In the Services Stats view, you can customize the monitored statistics for individual services. The Chart Stats Tray lists all available statistics for the service. The number of statistics varies according to the type of service being monitored. Any statistic in the Chart Stats Tray can be displayed in a gauge or a timeline chart. Only statistics for session size, sessions, and packets are viewable in historical timeline charts.

Create a Gauge for a Statistic

To create a gauge for a statistic in the Services Stats view:

1. Go to **ADMIN > Services**.

   The Admin Services View is displayed.

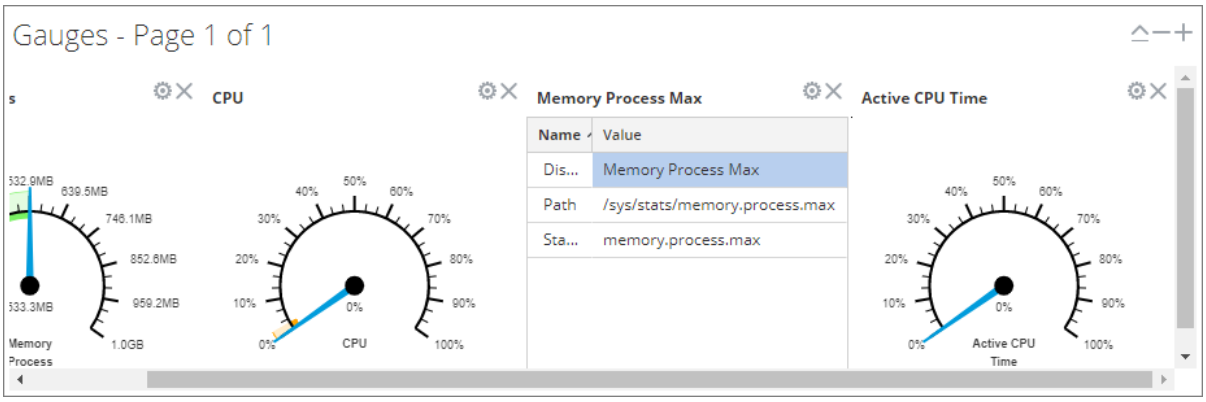
2. Select a service and select **View > Stats** in the Actions column.

   The Chart Stats Tray is displayed on the right side.

3. If the tray is collapsed, click <| to view the list of available statistics.

4. From the **Chart Stats Tray**, click on any statistic and drag it into the **Gauges** section.

   A gauge is created for the statistic. If there is no space for the gauge, a new page is created on the Gauges section and the gauge is added to the new page. In the example, the Active CPU Time chart was added to the Gauges section by dragging it from the Chart Stats Tray.

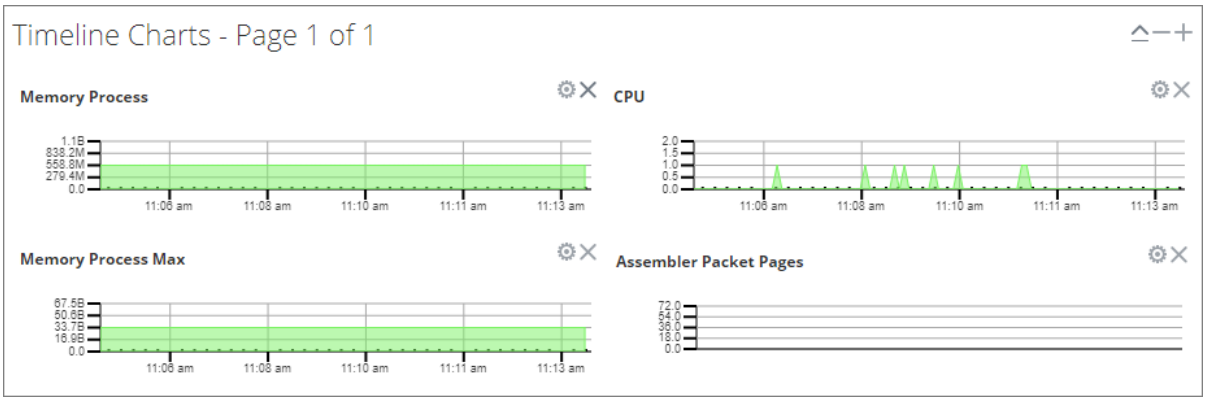


Create a Timeline Chart for a Statistic

To create a timeline for a statistic:

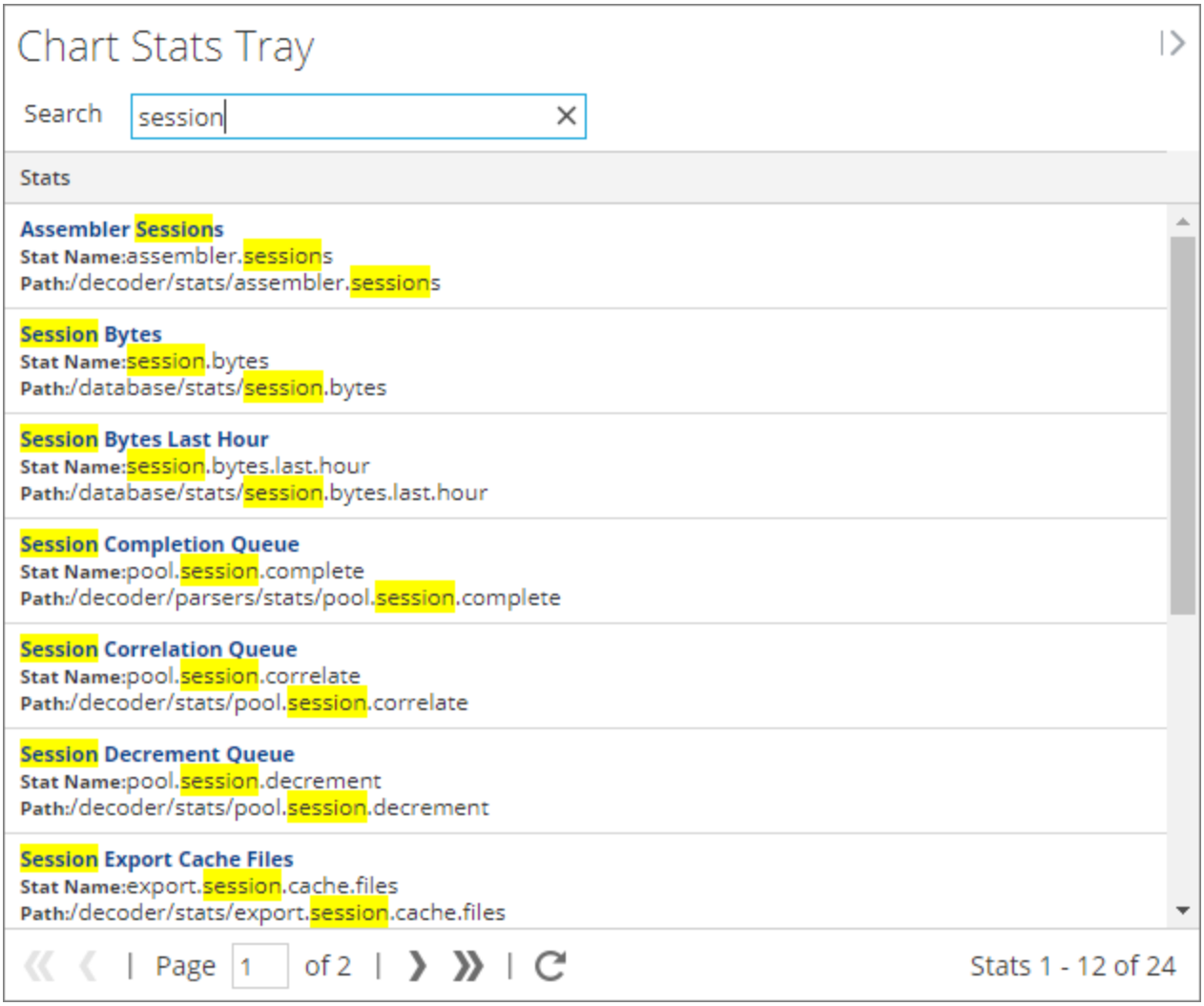
From the **Chart Stats Tray**, click on a statistic and drag it into the **Timeline Charts** or the **Historical Timeline Charts** section.

A timeline chart is created for the statistic. If there is no space for the chart, a new page is created on the Timeline Chart section and the chart is added to the new page. In the example, the Assembler Packet Pages chart was added to the Timeline Charts section by dragging it from the Chart Stats Tray.



Search for a Statistic in the Chart Stats Tray

To search for a statistic, type a search term; for example, **session**, in the Search field and press **RETURN**. Statistics that match are displayed with the matching word highlighted.

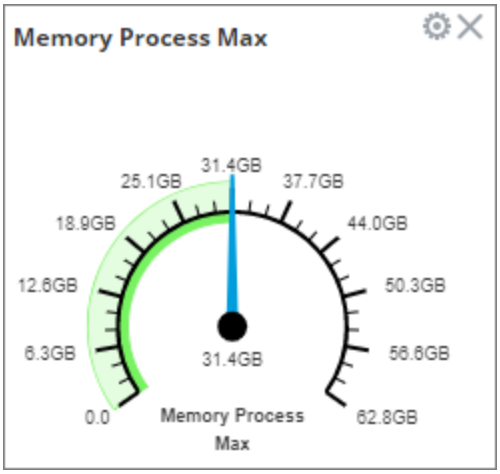


Edit Properties of Statistics Gauges

The Gauges section of the Service Stats view presents statistics in the form of an analog gauge. The properties of each individual gauge are editable; all gauges have an editable title and some have additional editable properties.

Edit Properties of a Gauge

1. Go to **ADMIN > Services**
   The Admin Services view is displayed.
2. Select a service and select **View > Stats** in the Actions column.
   The Service Stats view includes the Gauges section.
3. Go to the gauge for which you want to edit properties (for example, **Memory Process**).



4. Click the Properties icon ( ) to display the parameter names and values.
5. To highlight the value of the **Display Name** field, double-click on the value; for example, **Memory Process**.

   Note: Clicking the other two values does nothing because the properties are not editable in the gauge.

5. Type a new value for the Display Name and click the **Properties** icon ( ).
   The new title replaces **Memory Process**.

Add Stats to the Gauges Section

You can add more gauges by dragging a statistic from the **Chart Stats Tray** into the **Gauges** section.

1. To expand the Chart Stats Tray, click <|.
2. Scroll down and select a statistic, for example, **Session Rate (maximum)**.
3. Drag the statistic to the **Gauges** section.
   The new gauge is displayed in the Gauges section.

Edit Properties of Timeline Charts

Timeline charts display statistics in a running timeline. The Service Stats view includes two types of timelines: current time and historical. You can drag any statistic available in the Chart Stats Tray to the Timeline Charts section. Only statistics for session size, sessions, and packets are viewable in historical timeline charts. The properties of an individual timeline chart are editable; all timeline charts have an editable title and some have additional editable properties.

To access the charts:

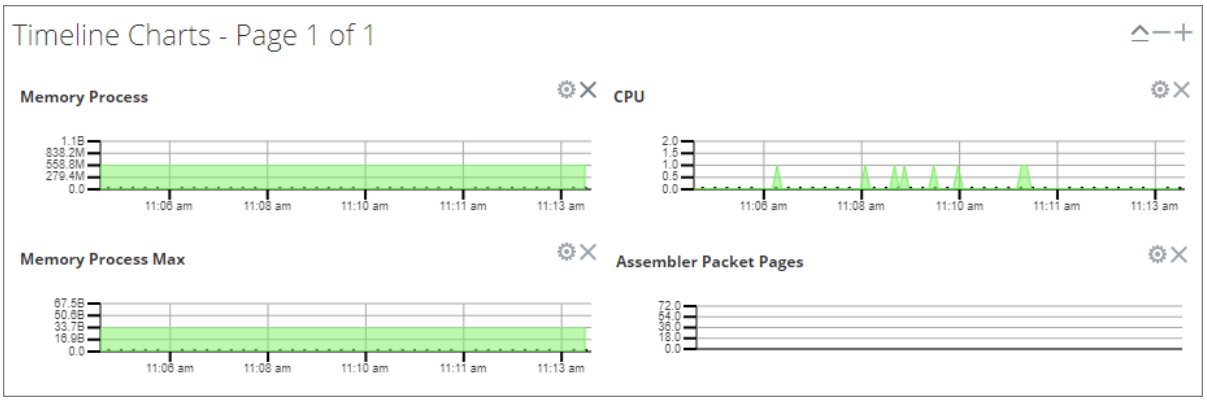
1. Go to **ADMIN > Services**.
2. Select a service and click **Stats**.

   The Services Stats view is displayed. The charts are in this view.

Edit Properties of a Timeline

To edit properties of a timeline chart:

1. Go to the timeline chart for which you want to edit properties (for example, **Memory Process**).



2. Click the **Properties** icon ( ) to display the parameter names and values.
3. Double-click on a value (for example, the **Display Name** field) to make the value editable.

   Note: Clicking the other two values does nothing because the properties are not editable in the chart.

4. Type a new value and click the **Properties** icon.

   The timeline chart is displayed with new values.

Edit Properties of a Historical Timeline

To edit properties of a historical timeline chart:

1. Go to Historical Timeline Charts.
2. Click the **Properties** icon ( ) to display the parameter names and values.
3. Click on a value (for example, **01/27/2015** for the **Begin Date** field) to make the value editable.
4. Type a new value.
5. Edit the **End Date** and **Display Name** if required.
6. Click the **Properties** icon ( ).

   The historical timeline is displayed with new values.

Note: To return the properties of the historical timeline chart back to the default so that the values dynamically update, remove the Begin Date and the End Date, place your cursor in the Begin Date field, and refresh your browser.

Add Stats to Timeline Charts

You can add timeline charts by dragging a statistic from the Chart Stats Tray into the Timelines section.

1. To expand the Chart Stats Tray, click .
2. Scroll down and select a statistic; for example, **Session Rate (maximum)**.
3. Drag the statistic to the **Timelines Section**.

   The new timeline is displayed in the Timelines section.

Monitor Hosts and Services

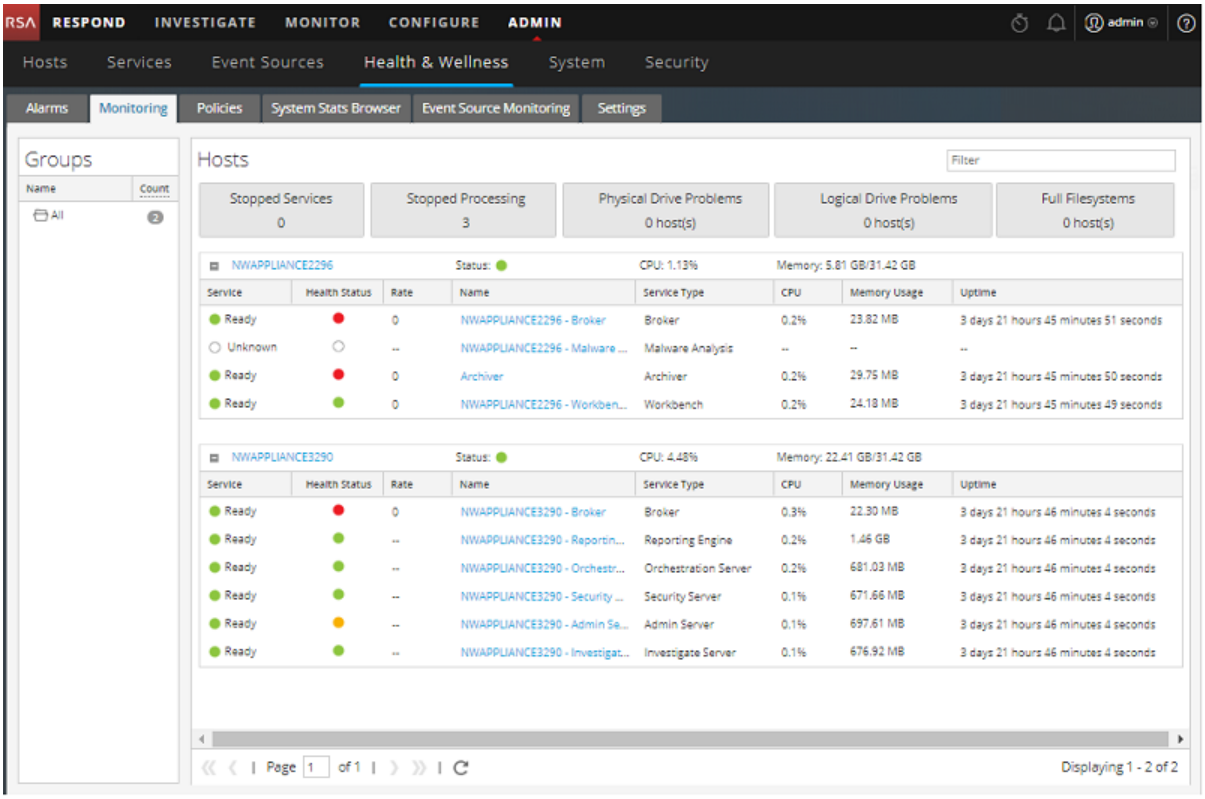
NetWitness Suite provides a way to monitor the status of hosts and services installed. You can view the current health of all the hosts, services running on the hosts, their CPU usage and memory consumption and the host details and service details.

To monitor hosts and services in NetWitness Suite:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Select the **Monitoring** tab.
   A list of all hosts and their associated services that belong to the group **All** is displayed by default.
   The operational status, CPU usage, and memory usage for each host is displayed.



   Click ⊞ to the left of a host (⊞ is visible if there are services installed on a host)

3. A list of services installed on the selected host is displayed.
   The name, operating status, CPU usage, memory usage, and the time operating for each service is displayed.

Filter Hosts and Services in the Monitoring View

You can filter hosts and services in the monitoring view in one of the following ways:

- Hosts belonging to a particular group
- Specific host and its associated services
- Hosts whose services are stopped
- Hosts whose services have stopped processing or processing has been turned off

- Hosts that have Physical drive problems
- Hosts that have Logical drive problems
- Hosts that have Full File systems

For the related reference topic, see Monitoring View.

To filter hosts and services:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open by default.

2. Select the **Monitoring** tab.
3. Filter the hosts and services in one of the following ways:
   - To view a list of hosts and their associated services belonging to a particular group, select the group in the Groups panel.

     All hosts and their associated services belonging to the specified group are displayed in the Hosts panel.

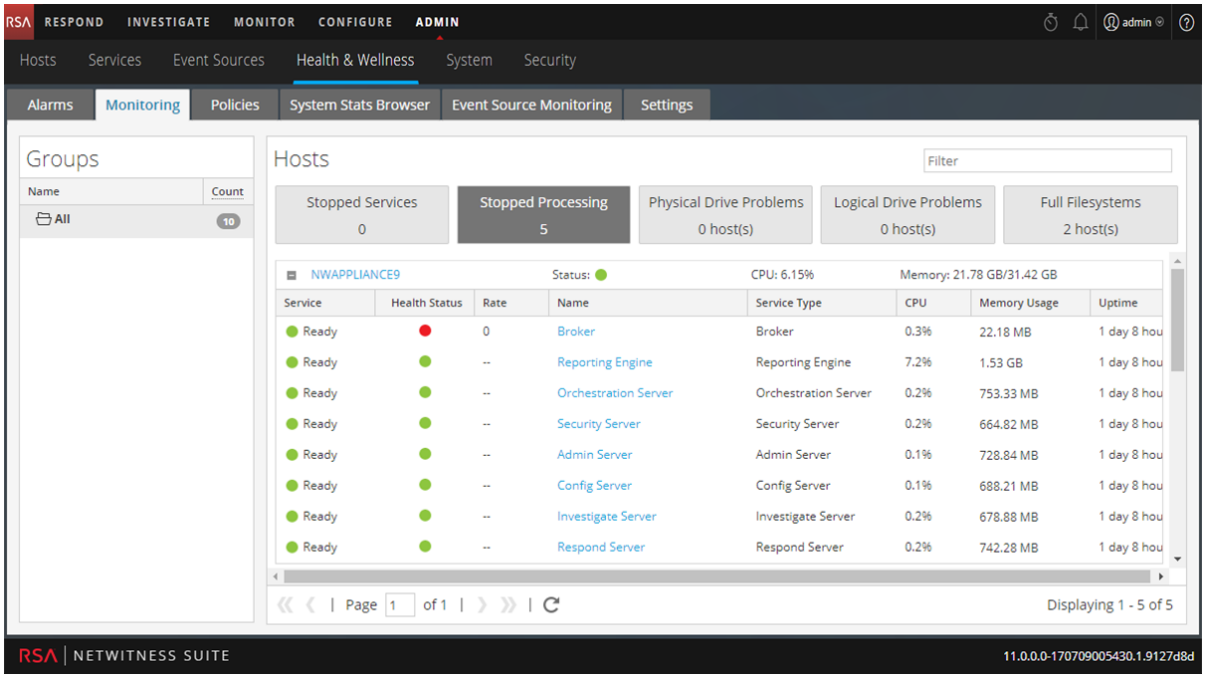
     Note: The grouping of hosts is derived from the groups created in the Administration page. All groups created in the Administration page are displayed here.

     For example, if you select the group **LC_Group** in the Groups panel, a list of all hosts that are part of the group are displayed.

   - To view a list of all services that have stopped processing, click **Stopped Processing** in the Hosts panel.

     A list of all the hosts that have at least one service with the status as stopped processing is displayed.

     Note: The buttons on the top display the System Statistics for all the hosts configured in NetWitness Suite and does not change with application of filters on groups.



Note: In a similar way you can filter the list of hosts and the associated services by choosing the right filter
- Click Stopped Services to display a list of all stopped services.
- Click Physical Drive Problems to display a list of host with Physical Drive Problems.
- Type the host name in the Filter box to display only the required host and the services running on the host.

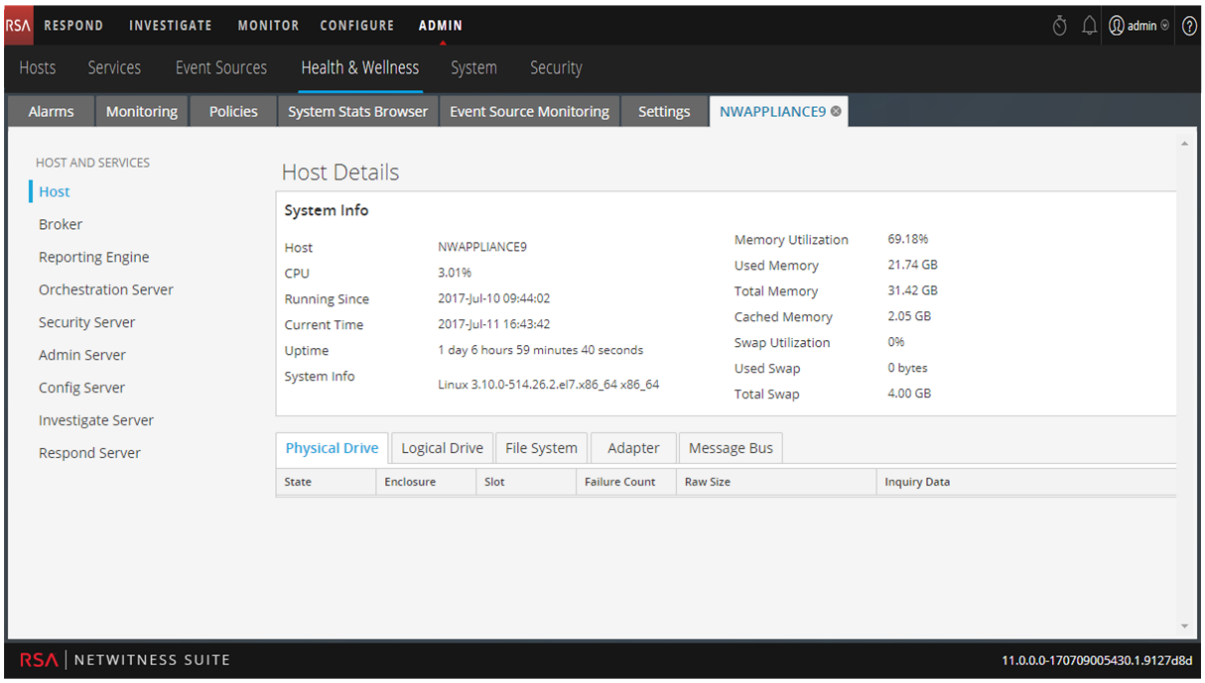
Monitor Host Details

You can view the details of the host, its memory and CPU usage, system information, the physical drive, logical drive and file system details to further investigate if you encounter some problem with the host.

To view host details:

1. Go to **ADMIN > Health & Wellness**.
   The Health & Wellness view is displayed with the Alarms tab open.
2. Select the **Monitoring** tab.
3. Click a host in the **Hosts** panel.

The Host Details view is displayed as a new page.



Monitor Service Details

You can view the details of a service, its memory and CPU usage, system information, and various details depending on the service selected.

To view service details:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

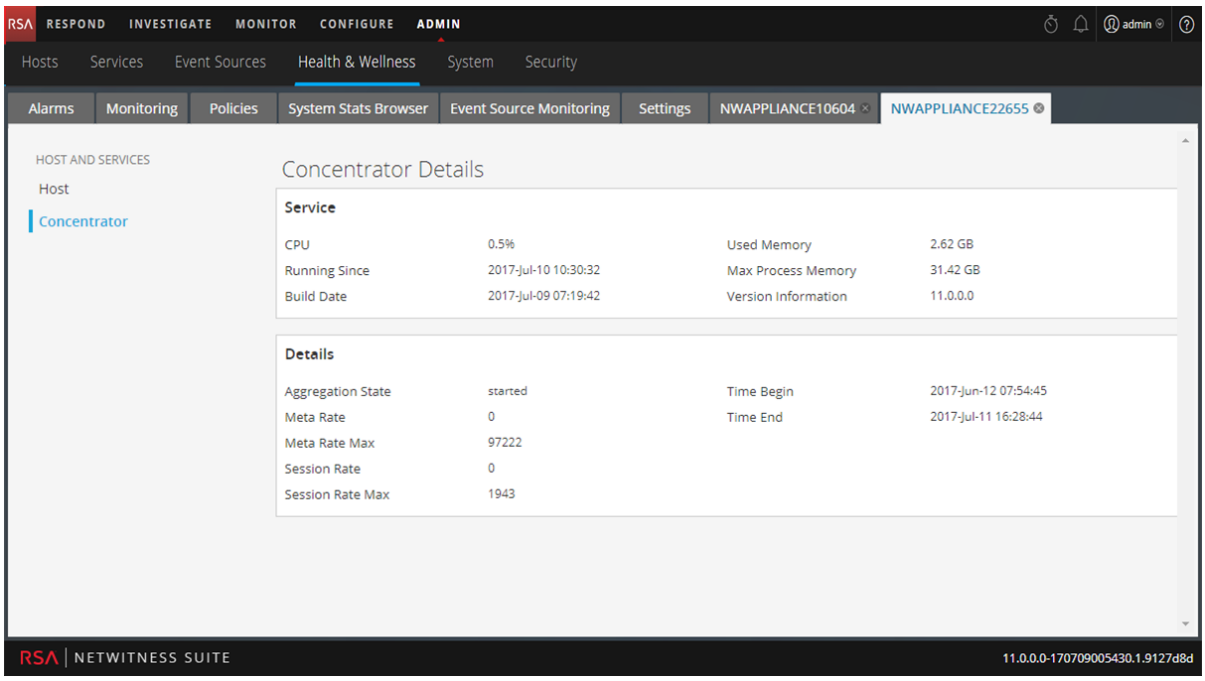
2. Select the **Monitoring** tab.

3. Click ⊞ for a host in the Hosts panel.

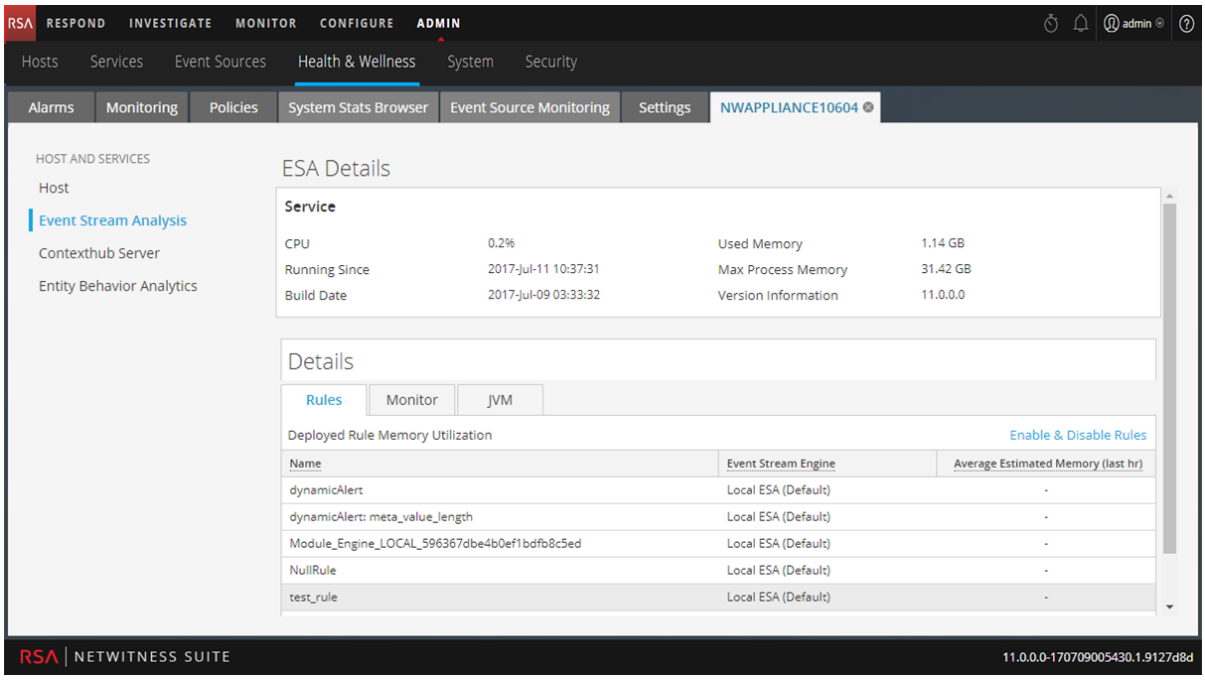
   A list of services running on the host is displayed.

4. Click on any service.

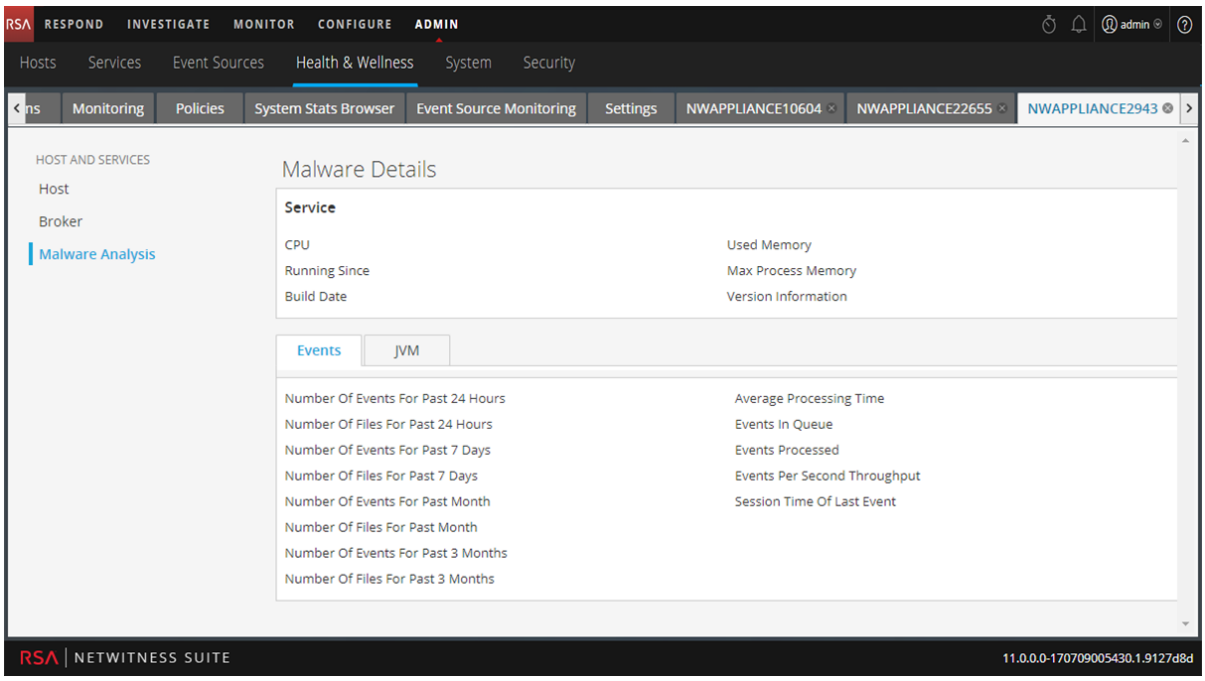
   The service details view is displayed as a new page. The Archiver, Broker, Concentrator, and Decoder service details views have the **Service** and **Details** panels.



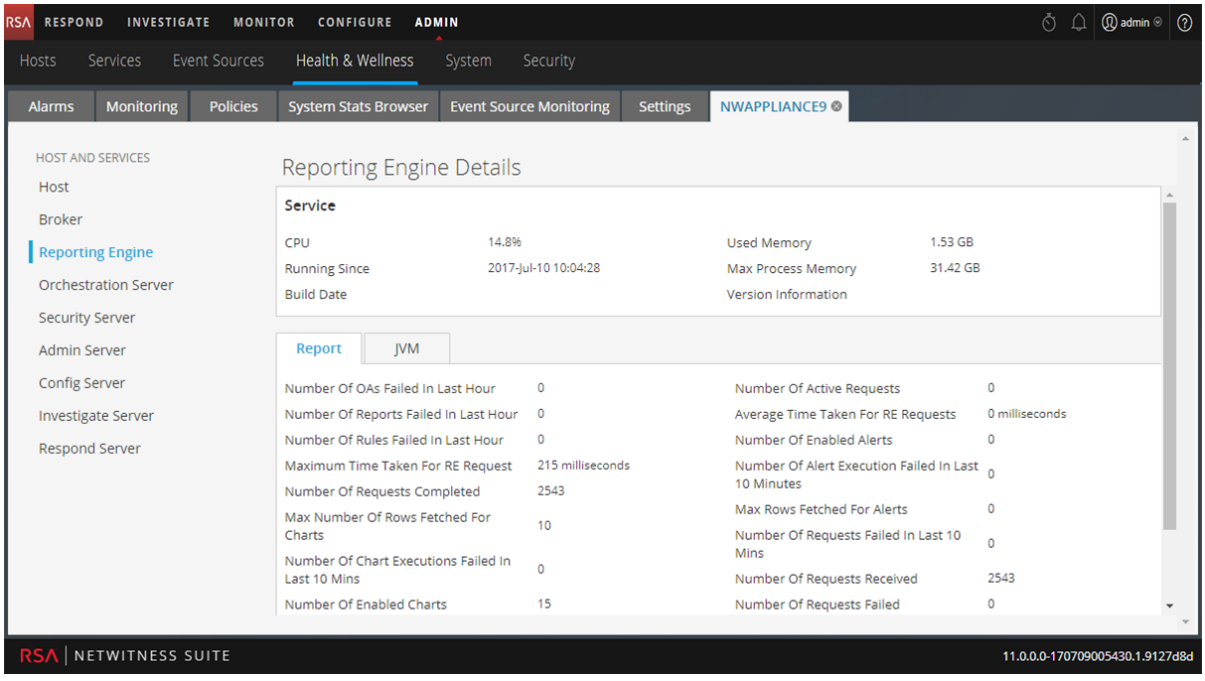
The Event Stream Analysis (ESA) service details view has the **Service**and **Details** panels, plus the **Monitor** and **JVM** tabs that show additional statistics.



The Malware Analysis service details view has the **Service** panel plus the **Rules, Events,** and **JVM** tabs that show additional statistics.



The Reporting Engine service details view has the **Service** panel plus the **Report** and **JVM** tabs that show additional statistics.



Note: Alternatively, you can access the service details page by clicking the services listed in the options panel in the Host Details view.

Refer to Monitoring View for a detailed description of the Details view for each service.

Monitor Event Sources

The event source monitoring feature of NetWitness Suite provides the following functionalities:

- Support for failover
- Provides a consolidated list of event sources and their associated collector and log decoder devices
- Regex support for rules
- Decommission
- Filtering capabilities
- Historical graph

In addition, you can monitor event sources, check the number of events generated from a source type and view the historical graph of the events collected. To monitor event sources you have to configure the event sources so that they generate and send out notifications when required.

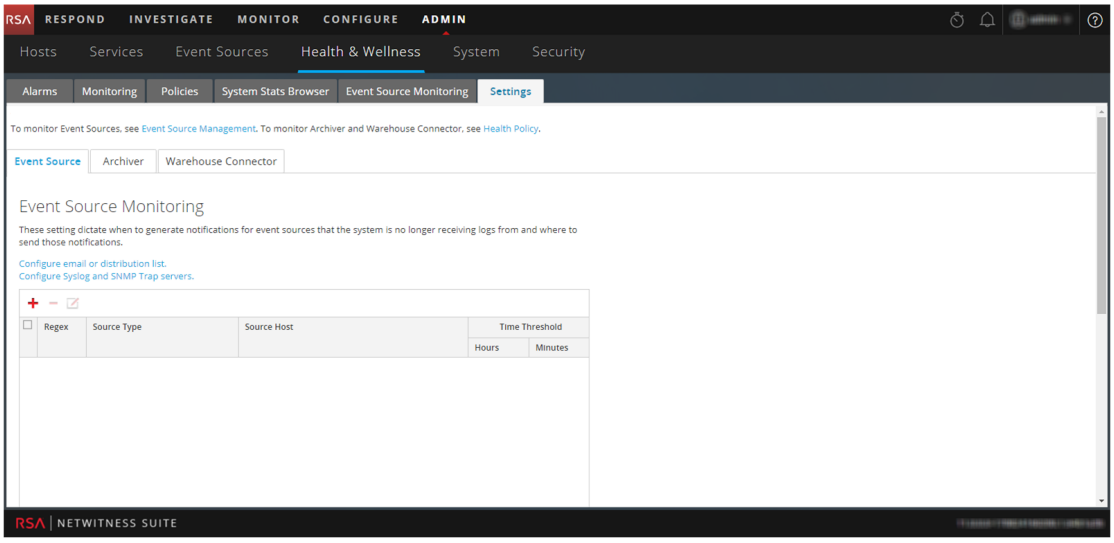
Configure Event Source Monitoring

To monitor event sources you have to configure the event sources so that they generate and send out notifications when required. For the related reference topic, see Health and Wellness Settings View - Event Sources.

To configure and enable event monitoring in NetWitness Suite:

1. Go to **ADMIN** > **Health & Wellness**.
2. Select **Settings** > **Event Source**.

   The Event Source tab is displayed.

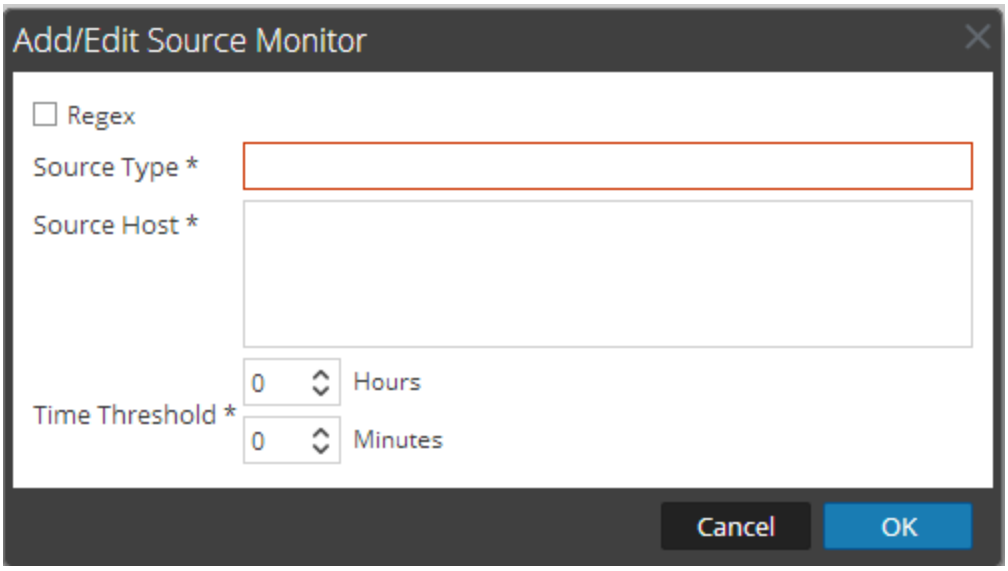


3. Under **Event Source Monitoring**, click +.

   The Add/Edit Source Monitor dialog is displayed.

4. Define the **Source Type**, **Source Host**, and **Time Threshold** for the source of the event source that you want to monitor to detect when NetWitness Suite stops receiving logs from it. If you do not specify a **Time Threshold**, NetWitness Suite monitors the event source until you set a threshold.

   Note: For **Source Type** and **Source Host**, you must specify the values that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view. You add or modify the the event sources that you want to monitor. The two parameters that identify an event source are **Source Type** and **Source Host**. You can use **globbing** (pattern matching and wildcard characters) to specify the **Source Type** and **Source Host** of event sources



5. Click **OK**.

   The event source is displayed in the panel.

6. Configure the method of notification, by doing one of the following:

   - Select **Configure email or distribution list**.

     The AMIN > System > Email Configuration Panel is displayed so that you can specify to whom the notifications are sent.

   - Select **Configure Syslog and SNMP Trap servers**.

     The Administration > System Auditing Configuration panel is displayed so that you can configure the Syslog and SNMP Traps to which the notifications are sent.

7. Click **Apply**.

   NetWitness Suite begins sending notifications when it stops receiving events from this event source after the time threshold has elapsed.

For details on parameters in the Event Source Monitoring settings view, see Event Source Monitoring View.

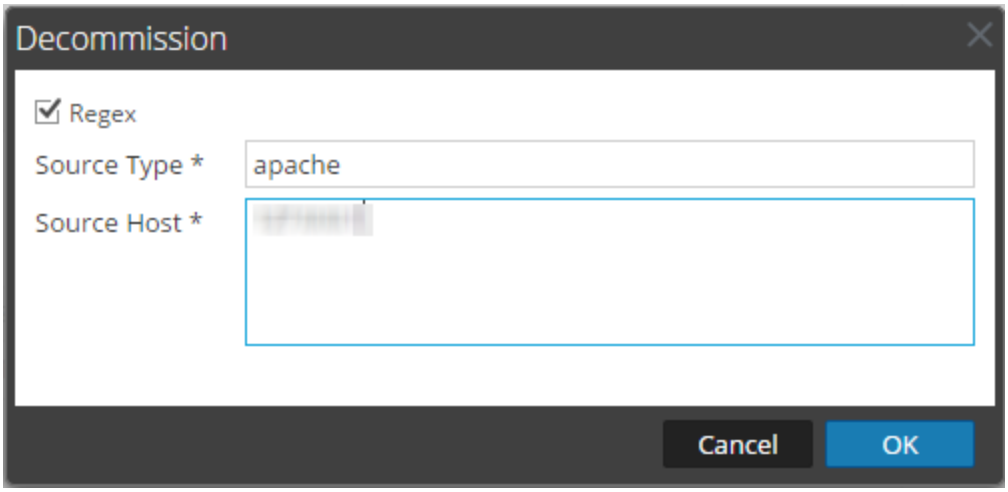
Decommission Event Source Monitoring

If a Log Collector service (Local Collector or Remote Collector) for which you set up Event Source monitoring becomes inoperable, NetWitness Suite continues to notify that you it is not receiving events from it until you decommission the Collector.

Caution: If you configured a failover Local Collector for a Remote Collector and the Local Collector fails over to a standby Log Decoder, you must decommission the Local Collector to stop the notifications.

To decommission event source monitoring for an event source:

1. Go to **ADMIN**> **Health & Wellness**.
2. Select **Settings** > **Event Source**.
   The **Event Source** tab is displayed.
3. Under **Decommission**, click +.
   The **Decommission** dialog displays.
4. Define the **Source Type** and the **Source Host** for the source for which you want to decommission event monitoring notifications.



Filter Event Sources

You can choose a filter to display:

- Events belonging to a particular event source
- Events belonging to particular event source types
- Events collected from a particular log Collector
- Events list arranged in a order based on the Event Source Type, Log Collector, Log Decoder or Last Event Time.

To filter the list of event sources:

1. Go to **ADMIN > Health & Wellness**.
2. Select **Event Source Monitoring**.
3. Filter the list in one of the following ways:

- To view the events generated by a particular event source, type the required event source in the **Event Source** field. Select **Regex** to enable Regex filter and click **Apply**. It performs a regular expression search against text and lists out the specified category. This field also supports globbing pattern matching.
  All events generated by the Event Source specified are displayed.
- To view events collected from a particular Log Collector, select a Log Collector from the drop-down list and click **Apply**.
  A list of all events being collected from the specified Log Collector from various event sources is displayed.

Note: Similarly, you can also choose the following filters:
- To view events belonging to an event source type, select the event source type and click **Apply**.
- To view events received in a specified time frame, select the required time frame and click **Apply**. You can further filter the query results to contain only event sources that logs have been received from within the selected time or the query results to contain only event sources that logs have not been received from within the selected time.

For details on various parameters and description, see Event Source Monitoring View.

View Historical Graph of Events Collected for an Event Source

The historical graph of the events collected from an event source gives you information about the variation of the collection over a time frame selected.

To view a historical graph:

1. Go to **ADMIN > Health & Wellness**.
   The Health & Wellness view is displayed with the Alarms tab open.

2. Click **Event Source Monitoring**.
   The Event Source Monitoring view is displayed.

3. In the **Historical Graph** column, select .
   The Historical graph for the selected event source is displayed.
   The figure below gives an example of the historical graph for the event source type **winevent_snare**.

   The graphical view is customized to display the events collected for the current day and the values are zoomed in for an interval of an hour (09.05 - 105.05 hrs). Hover over the graph to view the details at a particular instant. For example, in the figure it displays the average rate of collection at 09.30 hrs.

Note: You can customize the graph view by selecting the Time Frame and Date range. You can zoom in using the zoom in value, time window, or by just a click and a drag in the plot area. For details on the parameters to customize and zoom in functions see Health and Wellness Historical Graphs collected from an event source.
If there is no data displayed on the chart it may be due to one of the following reasons:
- event source is down.
- event source is not processing anything right now.

Monitor Alarms

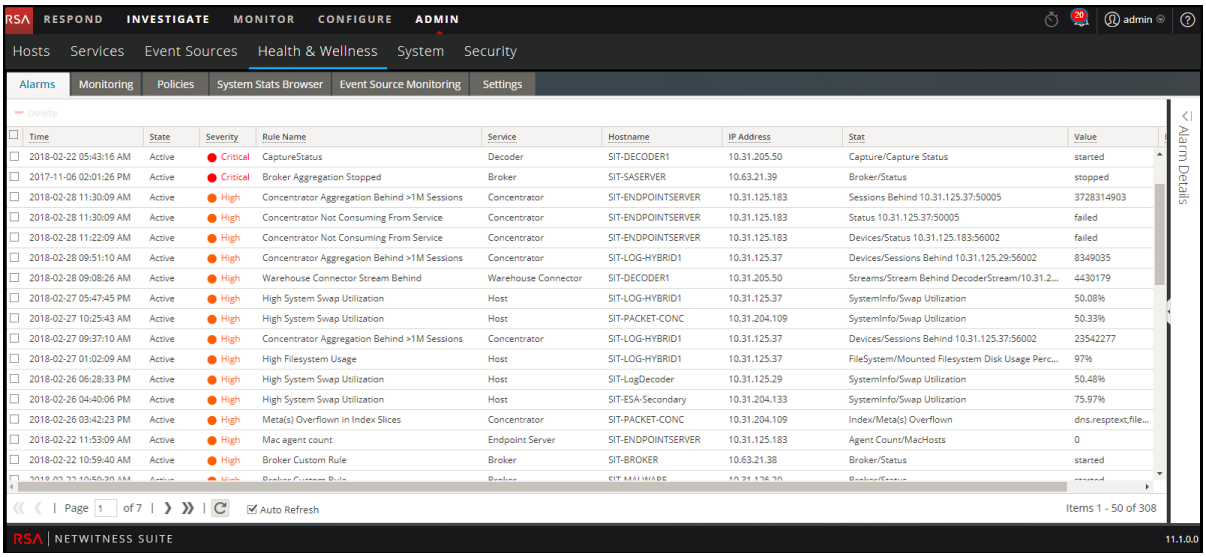
You can set up alarms and monitor them in the Health and Wellness interface for the hosts and services in your NetWitness Suite domain. Alarms display in the view as **Active** when the Policy-rule-defined statistical thresholds for hosts and services have been crossed. Alarms are grayed out and change to the **Cleared** status when the clearing threshold has been crossed.

You set up the parameters for alarms in Manage PoliciesManage Policies For the related reference topic, see Health and Wellness View - Alarms View.

To monitor the alarms set up in NetWitness Suite:

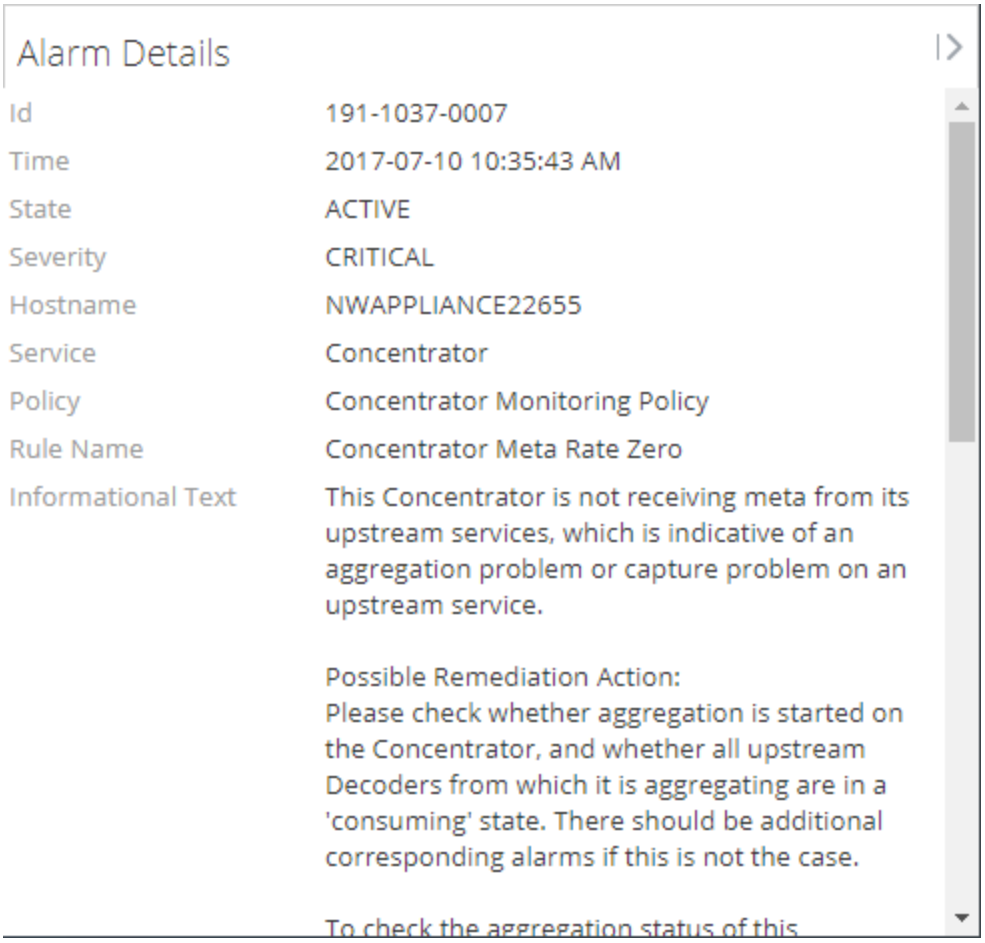
1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open by default.



2. Click on the alarm for which you want to display details in the Details Panel.

3. Click (expand) to view the details for the alarm you selected.



Monitor Health and Wellness Using SNMP Alerts

You can monitor an NetWitness Server component to proactively alert using Simple Network Management Protocol (SNMP) based on the thresholds or system failures.

You can monitor the following for NetWitness Suite components:

- CPU utilization that reaches a defined threshold.
- Memory utilization that reaches a defined threshold.
- Disk utilization that reaches a defined threshold.

SNMP Configuration

The NetWitness Servers can be configured to send out SNMPv3 Threshold Traps and Monitor Traps. Threshold traps are sent in conjunction with configured node thresholds by the NetWitness Suite Core applications themselves. Monitor traps are sent by the SNMP daemon itself for the items indicated in its configuration file. The customer must set up the SNMP daemon on another service to receive SNMP traps from NetWitness Suite. You can set up SNMP on NetWitness Suite in the configuration setting for the NetWitness Server. For more information, see "Service Configuration Settings" in the *NetWitness Suite Host and Services Getting Started Guide* for the specific host.

Thresholds

Thresholds can be set on any service statistics that can accept the setLimit message. You can retrieve the current thresholds using the getLimit message. To set a limit, you can pass a low and high threshold value.

When the value of the stat crosses either the low or high threshold, a SNMP trap is triggered indicating the threshold is crossed. The trap will not be triggered if the value is below the low and above the high value, but another trap is triggered if it crosses back into the normal range (above the low and below the high).

You must set the threshold for the service using the Service Explorer view or the REST API.

Following is a sample threshold for monitoring CPU usage (below 10% or above 90%):

```
/sys/stats/cpu setLimit low=10 high=90
```

Following is an example of how the threshold is set using REST API:

```
http://<log decoder>:50102/sys/stats/cpu?msg=setLimit&low=10&high=90
```

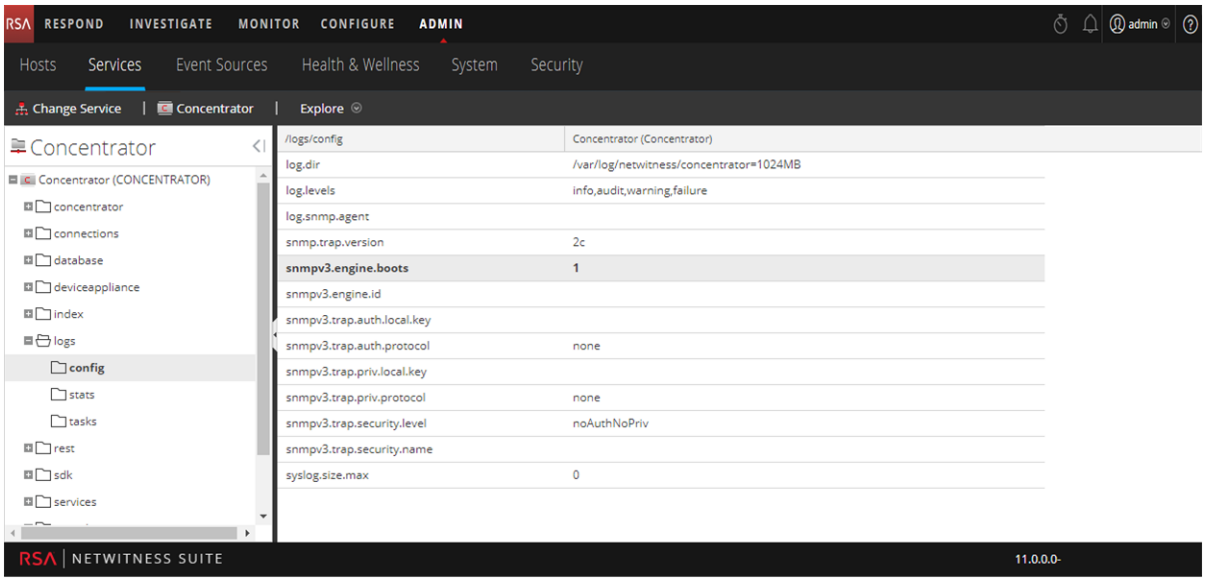
If the CPU usage spikes to 90% or higher, a SNMP trap will be generated:

```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu
old=77% new=91
```

Configure SNMPv3 for a Host

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. Select the service.
3. In the Actions column, select **View > Explore**.
4. In the nodes list, expand the list and select a config folder. For example, logs > config

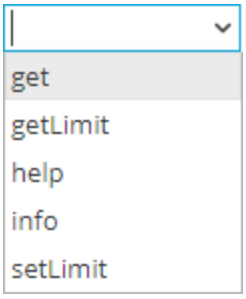
5. Set the SNMPv3 configuration.



Set the Threshold for a Service

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. Select the service.
3. In the Actions column, select **View > Explore**.
4. In the nodes list, expand the list and select a stat folder.
5. Select a stat, for example, cpu, and right-click.
6. From the drop-down menu, select **Properties.**

   The Properties panel is displayed. The Properties panel has a drop-down list of available messages for the parameter.



7. Select setLimit.
8. Specify the low and high values.

Troubleshooting Health & Wellness

Issues Common to All Hosts and Services

You may see the wrong statistics in the Health & Wellness interface if:

- Some or all the hosts and services are not provisioned and enabled correctly.
- You have a mixed-version deployment (that is, hosts updated to different NetWitness Suite versions).
- Supporting services are not running.

Issues Identified by Messages in the Interface or Log Files

This section provides troubleshooting information for issues identified by messages NetWitness Suite displays in the Health & Wellness Interface or includes in the Health & Wellness log files.

Message	User Interface: **Cannot connect to System Management Service** System Management Service (SMS) logs: `Caught an exception during connection recovery! java.io.IOException at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:106) at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:102) at com.rabbitmq.client.impl.AMQConnection.start(AMQConnection.java:346) at com.rabbitmq.client.impl.recovery. RecoveryAwareAMQConnectionFactory. newConnection (RecoveryAwareAMQConnectionFactory.java:36) at com.rabbitmq.client.impl.recovery. AutorecoveringConnection. recoverConnection(AutorecoveringConnection.java:388) at com.rabbitmq.client.impl.recovery. AutorecoveringConnection.beginAutomaticRecovery (AutorecoveringConnection.java:360) at com.rabbitmq.client.impl.recovery.AutorecoveringConnection. access$000(AutorecoveringConnection.java:48) at com.rabbitmq.client.impl.recovery.`

	AutorecoveringConnection$1.shutdownCompleted (AutorecoveringConnection.java:345) at com.rabbitmq.client.impl.ShutdownNotifierComponent. notifyListeners(ShutdownNotifierComponent.java:75) at com.rabbitmq.client.impl.AMQConnection$MainLoop.run (AMQConnection.java:572) at java.lang.Thread.run(Thread.java:745) Caused by: com.rabbitmq.client.ShutdownSignalException: connection error at com.rabbitmq.utility.ValueOrException.getValue (ValueOrException.java:67) at com.rabbitmq.utility.BlockingValueOrException. uninterruptibleGetValueBlockingValueOrException.java:33) at com.rabbitmq.client.impl.AMQChannel$BlockingRpcContinuation. getReply (AMQChannel.java:343) at com.rabbitmq.client.impl.AMQConnection.start (AMQConnection.java:292) ... 8 more Caused by: java.net.SocketException: Connection reset at java.net.SocketInputStream.read (SocketInputStream.java:189) at java.net.SocketInputStream.read (SocketInputStream.java:121) at java.io.BufferedInputStream.fill (BufferedInputStream.java:246) at java.io.BufferedInputStream.read (BufferedInputStream.java:265) at java.io.DataInputStream.readUnsignedByte (DataInputStream.java:288) at com.rabbitmq.client.impl.Frame.readFrom(Frame.java:95) at com.rabbitmq.client.impl.SocketFrameHandler.readFrame (SocketFrameHandler.java:139) at com.rabbitmq.client.impl.AMQConnection$MainLoop.run (AMQConnection.java:532)
Possible Cause	RabbitMQ service not running on the NetWitness Server.

Solution	Restart the RabbitMQ, SMS, and NetWitness Suite services using the following commands.
	`systemctl restart rabbitmq-server`
	`systemctl restart rsa-sms`

	`systemctl restart jetty`

Message/ Problem	User Interface: **Cannot connect to System Management Service**
Cause	The System Management Service, RabbitMQ, or Mongo service is not running.

Solution	Run the following commands on NetWitness Server to make sure all these services are running.
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is not running.`
	`[root@nwserver ~]# systemctl start rsa-sms`
	`Starting RSA NetWitness SMS :: Server...`
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is running (5687).`
	`[root@nwserver ~]# systemctl status mongod`
	`mongod (pid 2779) is running...`
	`systemctl status rabbitmq-server`
	`Status of node nw@localhost ...`
	`[{pid,2501},`
	`{running_applications,`
	`[{rabbitmq_federation_management,"RabbitMQ Federation Management",`
	`"3.3.4"},`

Message/ Problem	User Interface: **Cannot connect to System Management Service**
Possible Cause	`/var/lib/rabbitmq` partition usage is 70% or greater.
Solution	Contact Customer Care.

Message/ Problem	User Interface: **Host migration failed.**
Possible Cause	One or more NetWitness Suite services may be in a **stopped** state.
Solution	Make sure that the following services are running then restart the NetWitness Server: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problem	User Interface: **Server Unavailable.**
Possible Cause	One or more NetWitness Suite services may be in a **stopped** state.
Solution	Make sure that the following services are running then restart the NetWitness Server: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problem	User Interface: **Server Unavailable**
Possible Cause	System Management Service (SMS), RabbitMQ, or Mongo service is not running.

Solution 1	Run the following commands on NetWitness Server to make sure all these services are running.
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is not running.`

	[root@nwserver ~]# systemctl start rsa-sms Starting RSA NetWitness SMS :: Server... [root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is running (5687). [root@nwserver ~]# systemctl status mongod mongod (pid 2779) is running... systemctl status rabbitmq-server Status of node nw@localhost ... [{pid,2501}, {running_applications, [{rabbitmq_federation_management,"RabbitMQ Federation Management", "3.3.4"},
Solution 2	Make sure `/var/lib/rabbitmq` partition is less than 75% full
Solution 3	Check NetWitness Server log files (`var/lib/netwitness/uax/logs/nw.log`) for any errors.

Message/ Problem	ContextHub stops and does not allow you to add or edit data sources and lists.
Possible Cause	The storage is full by 95% or above.
Solution 1	Increase the storage by updating the YML file, located at /etc/netwitness/contexthub-server/ contexthub-server.yml. For example, to increase storage from 120 to 150 GB, enter a value (in bytes) by editing the relevant parameter: `rsa.contexthub.data.disk-size: 161061273600`
Solution 2	Delete unwanted or unused large list.
Solution 3	Configure the TTL index for the list to automatically delete STIX and TAXI data and to clean up storage space.

Message/ Problem	Context Hub runs on a fixed memory and 50% is reserved for cache. When cache is 100% full, the cache response stops. For all new lookups the response will be slow.
Possible Cause	The cache is full by 50% or above.
Solution 1	By default, Context Hub cleans the cache every 30 minutes. Reduce the cache expiration time of data sources.
Solution 2	Disable cache for data sources.
Solution 3	Increase the RAM of the CH Java process by editing the `-Xmx` option available in the /etc/netwitness/contexthub-server/contexthub-server.conf file. In `JAVA_OPTS`, search for the `-Xmx` option. For example, edit the entry as follows: `-Xmx8G` where `8G` represents 8GB space. Then restart the ContextHub service. **Note:** The memory is less than the available system memory. Be aware that there are many other services running on the host.

Message/ Problem	List Data Source displays an unhealthy stats or status.
Possible Cause 1	Unable to: • access the data source • parse or read a CSV file • schema mismatched CSV
Possible Cause 2	Unable to authenticate when accessing the data source.
Solution 1	Make sure to save the csv file at correct location i.e/var/lib/netwitness/contexthub-server/data/ and verify the required read permissions.

Solution 2	Make sure the csv file schema specified while configuring the data source matches. If not, then either create a new data source with the new schema or edit the csv file to match the schema. For example, if you configure a List Data Source with a schema with column1, column2, and column3. And next time you update the csv file where the number of column increase or decrease or the order of the columns are changed. In this case there is a schema mismatch and the configured list data source will show “Unhealthy” in Health and Wellness stats.
Solution 3	Make sure the password is correct. To confirm edit the data source, enter the password and click test connection. For more information related the above solutions, see "Configure Lists as a Data Source" topic in the *Context Hub Configuration Guide*.

Issues Not Identified by the User Interface or Logs

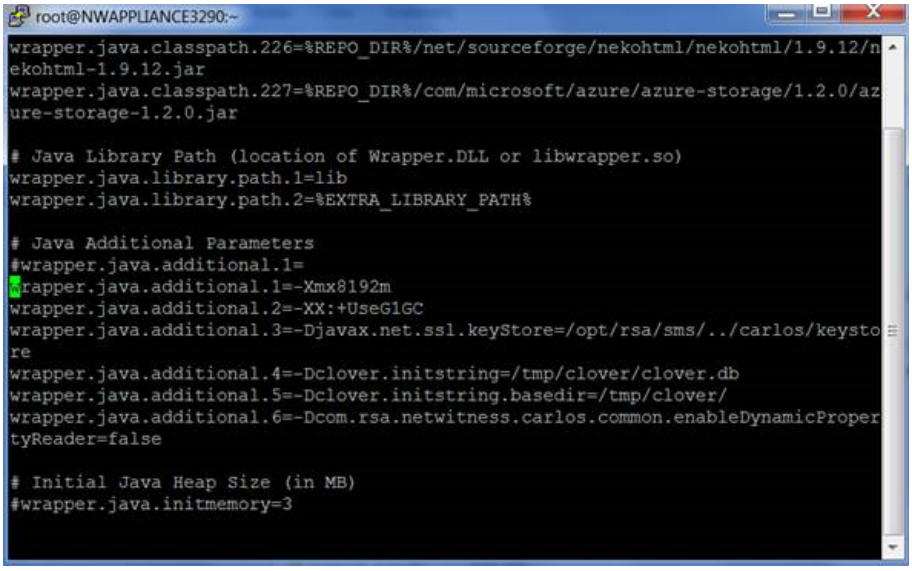
This section provides troubleshooting information for issues that are not identified by messages NetWitness Suite displays in the Health & Wellness Interface or includes in the Health & Wellness log files. For example, you may see incorrect statistical information in the Interface.

Problem	Incorrect statistics displayed in Health and Wellness interface.
Possible Cause	SMS service is not running. SMS service must be running on the NetWitness Server.
Solution	Restart SMS service.

Problem	NetWitness Suite does not show the version to which you upgraded until you restart jettysrv (jeTTy server).
Possible Cause	When NetWitness Suite checks a connection, it polls a service every 30 seconds to see if it is active. During that 30 seconds, if the service comes back up, it will not get the new version.
Solution	1. Manually stop the service.

	2. Wait until you see that it is it offline. 3. Restart the service. NetWitness Suite displays the correct version.

Problem	NetWitness Server does not display the **Service Unavailable** page.
Possible Cause	After you upgrade to NetWitness Suite version 10.5, JDK 1.8 is not default version and this causes the jettysrv (jeTTy server) to fail to start. Without the jeTTy server, the NetWitness Suite server cannot display the **Service Unavailable** page.
Solution	Restart jettysrv.

Problem	The SMS service is stopped and the following error is displayed in the log file: `java.lang.OutOfMemoryError: Java heap space`
Solution	You can use the following solution to increase the memory according to your needs. 1. Open /opt/rsa/sms/conf/wrapper.conf  2. Replace `wrapper.java.additional.1=-Xmx8192m` with: `wrapper.java.additional.1=-Xmx16g`

3. Restart the SMS service:

```
systemctl start rsa-sms
```

Managing NetWitness Suite Updates

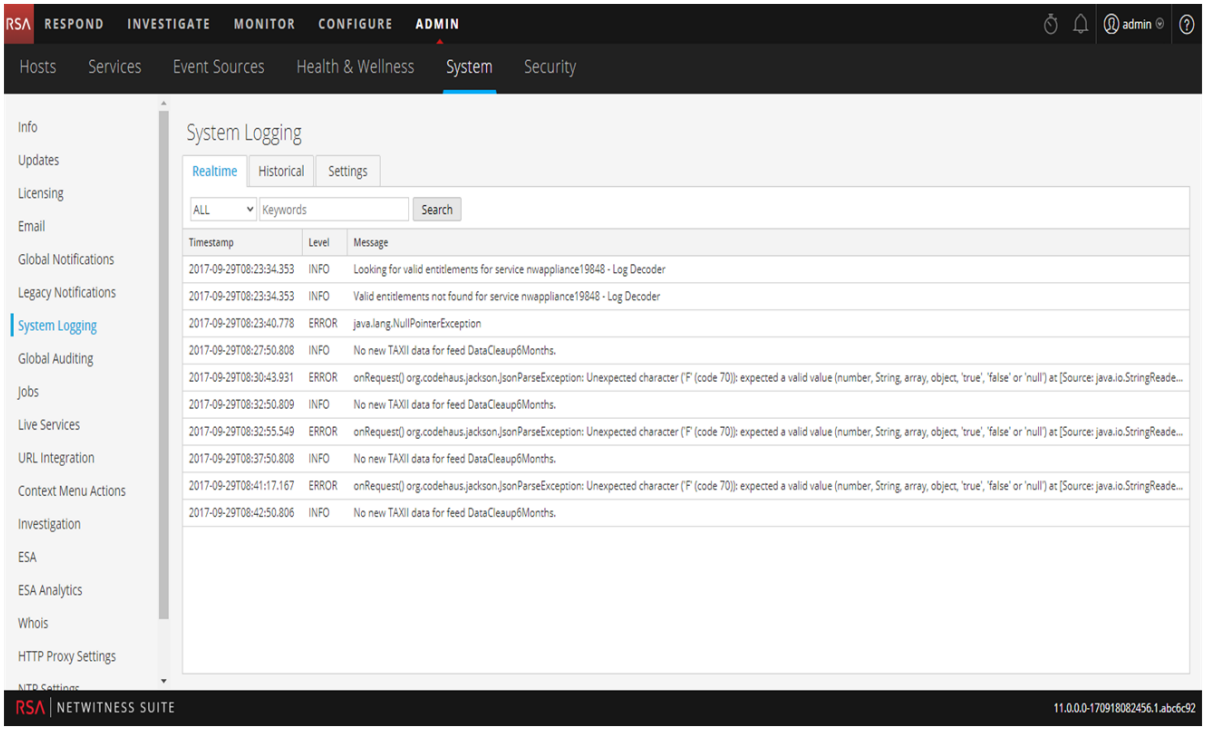
RSA issues NetWitness Suite software version updates on a regular basis as it strives to continually improve the product. A software version update consists of a release, service pack, or patch (including security patch) and ancillary software on which the release, service pack, or patch depends. User guides are provided for each software version update release, which include detailed steps for installing the update. It is important that you download the update guide for the release from RSA Link (https://community.rsa.com/community/products/netwitness) and follow the steps described there. Additional information is available in the "Update Existing Host to New Version" topic in the *Hosts and Services Getting Started Guide* and in System Updates Panel - Settings Tab.

Displaying System and Service Logs

NetWitness Suite provides views into system logs and service logs. When you view service logs, you can also select messages for the service or host.

View System Logs

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.

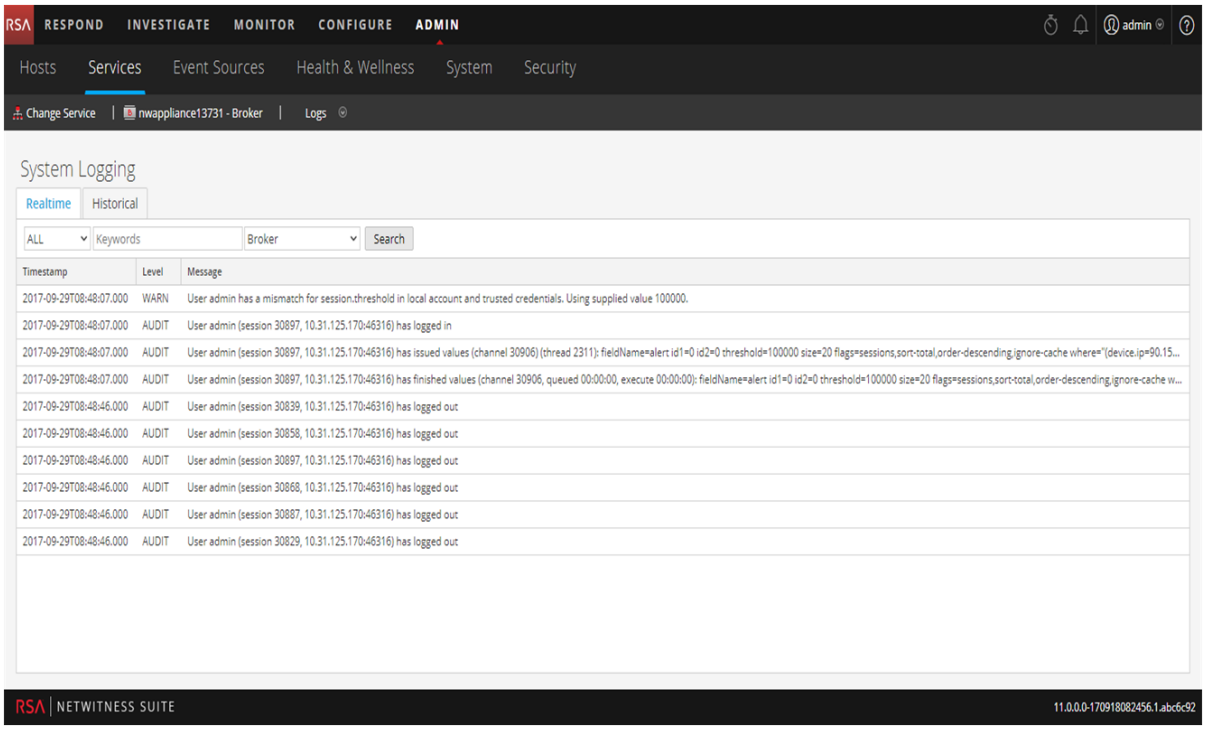


Display Service Logs

To display NetWitness Suite service logs:

1. Go to **ADMIN > Services**.
2. In the **Services** grid, select a service.

3. In the **Actions** column, select **View > Logs**.



Filter Log Entries

To filter the results shown in the Realtime tab:

1. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
2. (Optional) For service logs, select the Service: host or service.
3. Click **Filter**.

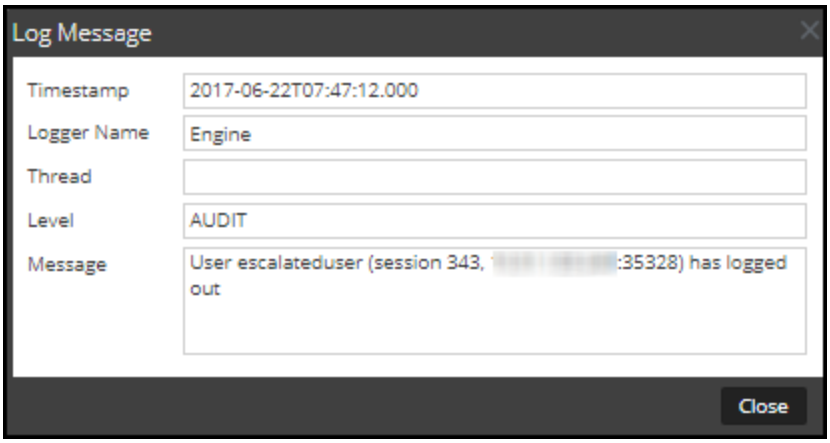
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the Realtime tab Log grid provides the summary information of a log entry. To view complete details:

1. Double-click a log entry.

   The **Log Message** dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



2. After viewing, click **Close**.

Access Reporting Engine Log File

All Log Files

The Reporting Engine stores the following logs in the **rsasoc/rsa/soc/reporting-engine/log** directory:

- Current logs in the **reporting-engine.log** file.
- Backup copies of previous logs in the **reporting-engine.log.*** file.
- All UNIX script logs in the files that have the following syntax: **reporting-engine.sh_*timestamp*.log** (for example, **reporting-engine.sh_20120921.log**).

The Reporting Engine rarely writes command line error messages to the **rsasoc/nohup.out** file.

Upstart Logs

The Reporting Engine appends the log messages and output written by upstart daemon and the commands used to start the reporting-engine to the **/var/log/secure** directory.

An upstart log file is a system log file so only the root user can read it. The Reporting Engine generates log files, retains backup copies of previous log files, stores UNIX script log files, and appends upstart log files to another directory.

Search and Export Historical Logs

NetWitness Suite provides a searchable view of the NetWitness Suite log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the service. You can export logs from the current view.

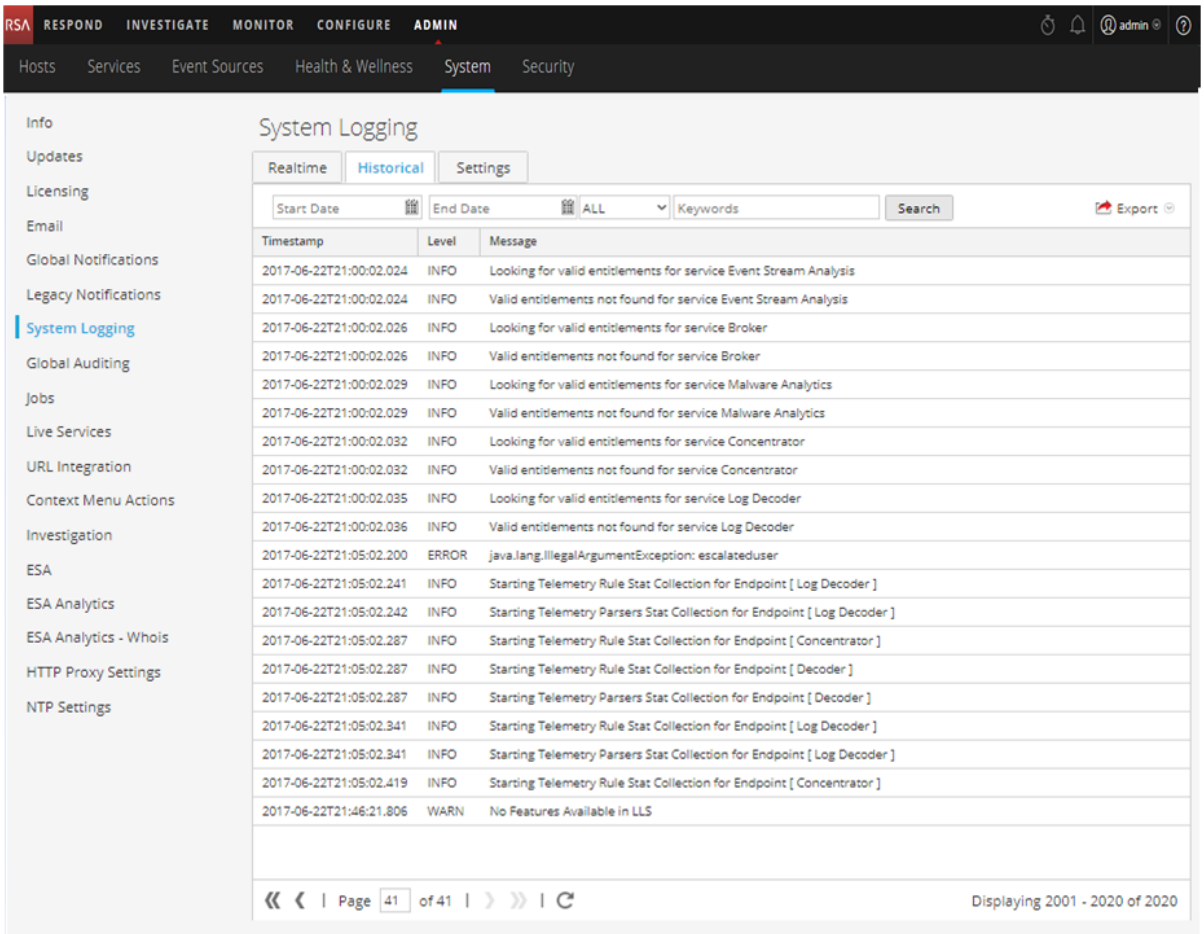
Display the Historical System Log

To display the historical log for the system:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel is opened to the Realtime tab by default.
3. Click the **Historical** tab.

   A list of historical logs for the system is displayed.



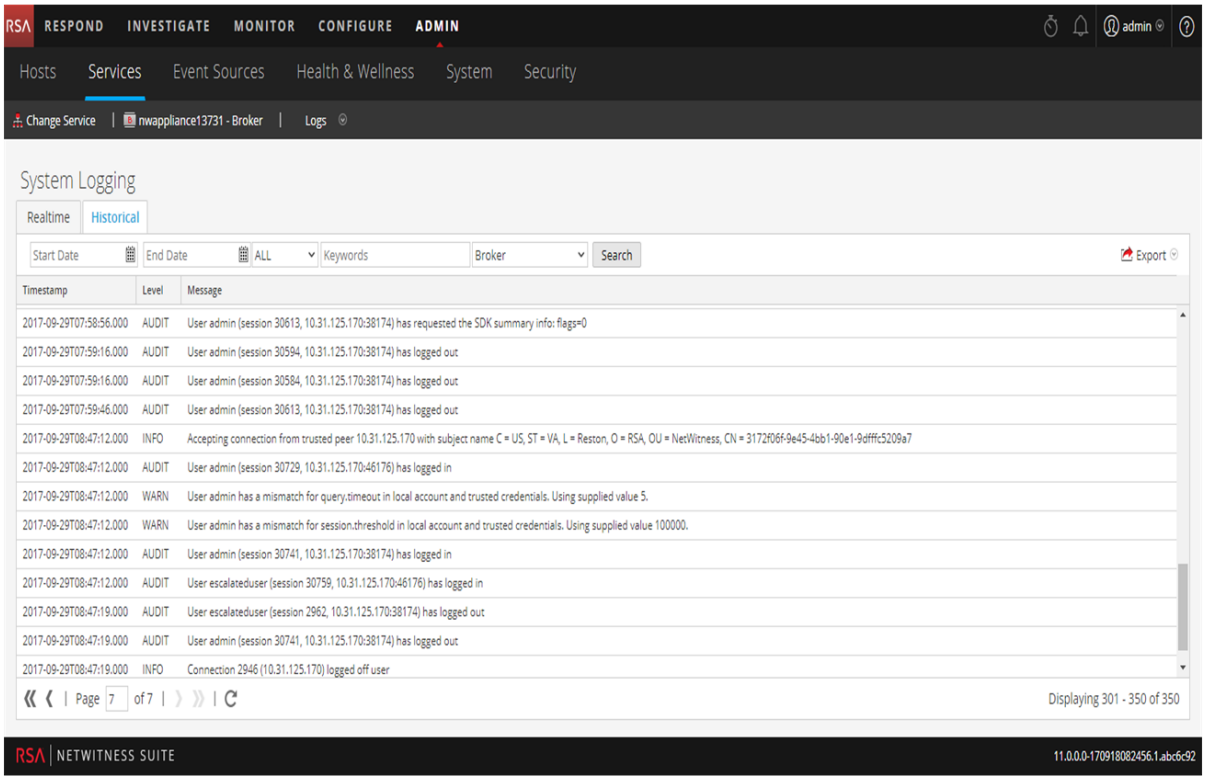
Display a Historical Service Log

To display the historical log for services:

1. Select **ADMIN > Services**.
2. Select a service.
3. In the **Actions** column, select **View > Logs**.

   The service logs view is displayed with the Realtime tab open.
4. Click the **Historical** tab.

   A list of historical logs for the selected service is displayed.



Search Log Entries

To search the results shown in the **Historical** tab:

1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
3. (Optional) For service logs, select the Service: host or service.

4. Click **Search**.

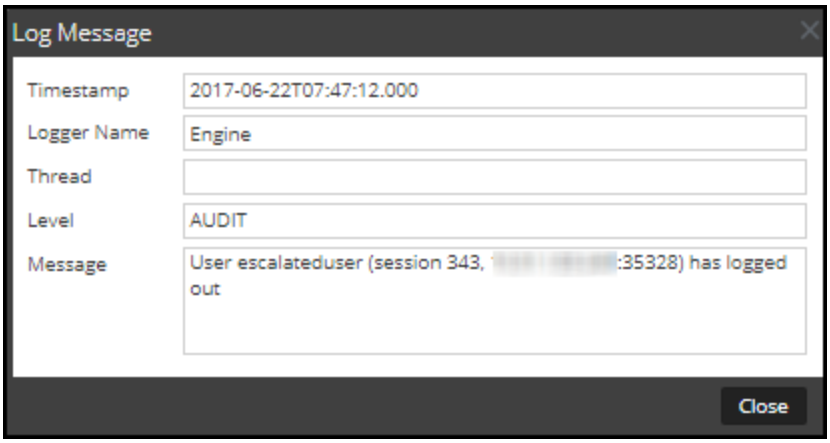
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the **Historical** tab Log grid provides the summary information of a log entry. To display all the details for a log message:

1. Double-click a log entry.

   The **Log Message** dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



2. After viewing, click **Close**.

   The dialog closes.

Page Through Log Entries

To peruse the different pages of the grid, use the paging controls on the bottom of the grid as follows:

- Use the navigation buttons
- Manually type the page number you want to view, and press **ENTER**.

Export a Log File

To export the logs in the current view:

Click **Export**, and select one of the drop-down options: **CSV Format** or **Tab Delimited**.
The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a NetWitness Suite system log exported with comma-separated values is named **UAP_log_export_CSV.txt**, and a host log exported with tab-separated values is named **APPLIANCE_log_export_TAB.txt**.

Maintaining Queries Using URL Integration

A URL integration provides a way to represent the bread crumbs, or query path, you take when actively investigating a service in the Navigate view. You do not need to display and edit these objects often.

A URL integration maps a unique ID that is automatically created each time you click on a navigation link in the Navigation view to drill into data. When the drill-down completes, the URL reflects the query IDs for the current drill point. The Display Name is displayed in the bread crumb in the Navigate view.

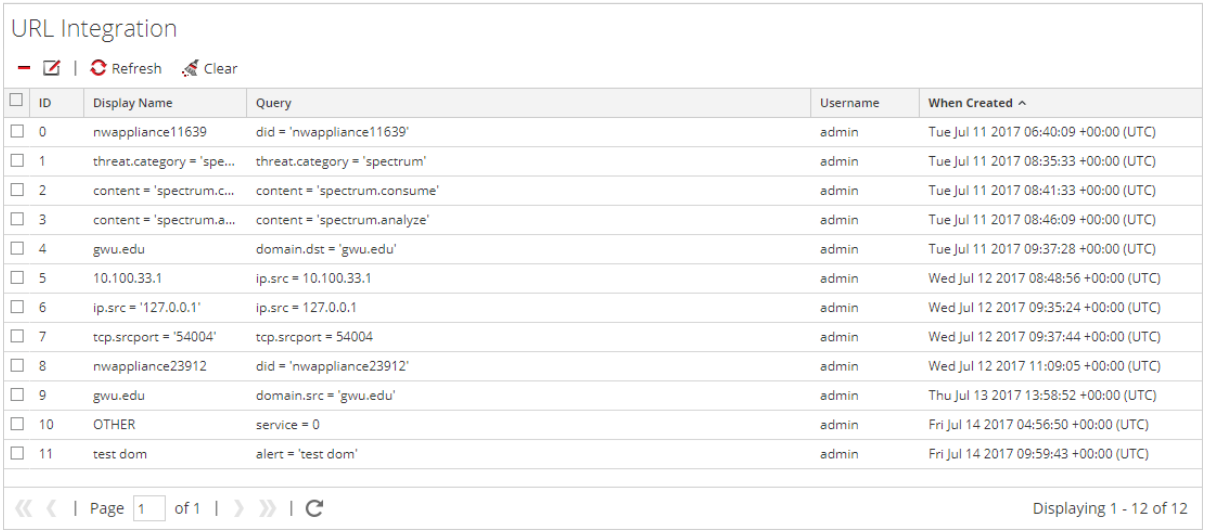
The **URL Integration** panel provides a list of queries and allows users who have the proper permissions to modify this underlying source of data and analyze the query patterns of other users of the NetWitness Suite system. Within the panel, you can:

- Refresh the list.
- Edit a query.
- Delete a query.
- Clear all queries in the list.

Caution: After a query has been removed from the system, any Investigation URLs that included the ID of that query will no longer function.

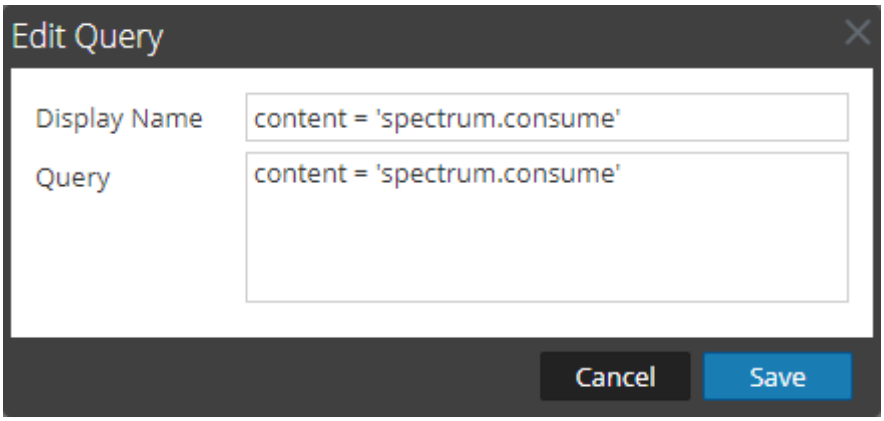
Edit a Query

1. Go to **ADMIN > System**.
2. In the options panel, select **URL Integration**.



3. Select the row in the grid and either double-click the row or click .

   The **Edit Query Dialog** is displayed.



4. Edit the **Display Name** and the **Query**, but do not leave either field blank.
5. To save the changes, click **Save**.

Delete a Query

Caution: After a query has been removed from the system, any Investigation URLs that included the ID of that query will no longer function.

To remove a query from NetWitness Suite entirely:

1. Select the query.
2. Click

A dialog requests confirmation that you want to delete the query.

3. Click **Yes**.

Clear All Queries

To clear all queries from the list:

- Click

The entire list is cleared.

Use a Query in a URI

URL Integration facilitates integrations with third-party products by allowing a search against the NetWitness Suite architecture. By using a query in a URI, you can pivot directly from any product that allows custom links, into a specific drill point in the Investigation view in NetWitness Suite.

The format for entering a URI using a URL-encoded query is:

http://<nw host:port>/investigation/<serviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
where

- **<nw host: port>** is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is only needed if access is configured over a non-standard port through a proxy.
- **<serviceId>** is the internal Service ID in the NetWitness Suite instance for the service to query against. The service ID can be represented only as an integer. You can see the relevant service ID from the url when accessing the investigation view within NetWitness Suite. This value will change based on the service being connected to for analysis.
- **<encoded query>** is the URL-encoded NetWitness Suite query. The length of query is limited by the HTML URL limitations.
- **<start date>** and **<end date>** define the date range for the query. The format is <yyyy-mm-dd>T<hh:mm>. The start and end dates are required. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.

For example:
http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00/2012-10-31T00:00

Examples

These are query examples where the NetWitness Server is 192.168.1.10 and the serviceID is identified as 2.

All activity on 03/12/2013 between 5:00 and 6:00 AM with a hostname registered

- Custom Pivot: alias.host exists
- https://192.168.1.10/investigation/2...13-03-12T06:00

All activity on 3/12/2013 between 5:00 and 5:10 PM with http traffic to and from IP address 10.10.10.3

- Custom Pivot: service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- Encoded Pivot Dissected:
  - service=80 => service&3D80
  - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - https://192.168.1.10/investigation/2...13-03-12T17:10

Additional Notes

Some values may not need to be encoded as part of the query. For example, commonly the IP src and dst is used for this integration point. If leveraging a third-party application for integration of this feature, it is possible to reference those without encoding applied.

FIPS Support

NetWitness Suite 11.0 ships with FIPS-validated 140-2 Cryptographic Modules that support all cryptographic operations within NetWitness Suite. NetWitness Suite leverages two modules that support a level 3 design assurance:

- RSA BSAFE Crypto-J
- OpenSSL with BSAFE (OWB)

Both modules have been certified with an operational environment comparable to the standard NetWitness Suite configuration.

By default, the cryptographic modules enforce the usage of FIPS-certified cipher suites wherever possible. For exceptions, refer to the information below and to the release notes. For additional information about the FIPS modules, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

The RSA BSAFE Crtypo-J FIPS Certificate number is 2468 and the OWB FIPS Certificate is included in the RSA BSAFE Crypto-C Micro Edition with certificate number 2300.

In 11.0.0.0, FIPS is enabled on all services except Log Collector. This includes Log Decoder and Decoder if they were FIPS-enabled in 10.6.4.x. FIPS cannot be disabled on any services except for Log Collector, Log Decoder and Decoder.

Note: For a fresh installation of 11.0.0.0, by default, all core services will be FIPS enforced except Log Collector and Log Decoder. FIPS cannot be disabled on any services except for Log Collector, Log Decoder and Packet Decoder.

Note: For upgrades to 11.0.0.0 from 10.6.4.x, the following conditions apply for the Log Collector, Log Decoder and Decoder services:
- Log Collector is not FIPS enabled after upgrading to 11.0.0.0, even if FIPS was enabled in 10.6.4.x. You must enable FIPS support after upgrading to 11.0.0.0. See the instructions in FIPS support for Log Collectors.
- If FIPS was enabled for the Log Decoder and Packet Decoder services in 10.6.4.x, FIPS will also be enabled in 11.0.0.0. However, if Log Decoder and Packet Decoder were NOT FIPS enabled in 10.6.4.x, they will not be enabled in 11.0.0.0, and you can manually enable FIPS for these services if required. See the instructions in FIPS support for Log Decoders and Decoders.

FIPS support for Log Collectors

To enable FIPS for Log Collectors:

1. Stop the Log Collector service.
2. Open the `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` file.
3. Change the value of the following variable to **off** as described here:
   `Environment="OWB_ALLOW_NON_FIPS=on"`
   to
   `Environment="OWB_ALLOW_NON_FIPS=off"`
4. Reload the system daemon by running the following command:
   `systemctl daemon-reload`
5. Restart the Log Collector service.
6. Set the FIPS mode for the Log Collector service in the UI :

   Note: This step is not required if you are upgrading from 10.6.4 to 11.0.0.0 and FIPS was enabled in 10.6.4.

   a. Go to **ADMIN** > **Services**.
   b. Select the Log Collector service and go to **View** > **Config**.
   c. In SSL FIPS Mode, select the checkbox under Config Value and click **Apply**.

FIPS support for Log Decoders and Decoders

To enable FIPS for Log Decoders and Decoders that did not have FIPS enabled in 10.6.4.x:

1. Go to **ADMIN** > **Services** and select a Log Decoder or Packet Decoder service.
2. Select **View** > **Config**, and in **System Configuration**, enable **SSL FIPS Mode** by selecting the check box in the **Config Value** column.
3. Restart the service.
4. Click **Apply**.

Troubleshoot NetWitness Suite

For information about troubleshooting NetWitness Suite, see the following topics:

- Debugging Information
- Error Notification
- Miscellaneous Tips
- NwLogPlayer
- Troubleshoot Feeds

Debugging Information

NetWitness Suite Log Files

The following files contain NetWitness Suite log information.

Component	File
rabbitmq	/var/log/rabbitmq/nw@localhost.log /var/log/rabbitmq/nw@localhost-sasl.log
collectd	/var/log/messages
nwlogcollector	/var/log/messages
nwlogdecoder	/var/log/messages
sms	/opt/rsa/sms/wrapper.log
sms	/opt/rsa/sms/logs/sms.log
sms	/opt/rsa/sms/logs/audit/audit.log
NetWitness Suite	/var/lib/netwitness/uax/logs/nw.log
NetWitness Suite	/var/lib/netwitness/uax/logs/ audit/audit.log
NetWitness Suite	/opt/rsa/jetty9/logs

Files of Interest

The following files are used in key NetWitness Suite components, and can be useful when trying to track down miscellaneous issues.

Component	File	Description
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQ configuration file. This configuration file partially drives the behavior of RabbitMQ, particularly around network/SSL settings.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQ environment configuration file. This file specifies the RabbitMQ node name and location of the enabled plugins file.
rabbit	/etc/rabbitmq/rsa_enabled_plugins	This file specifies the list of enabled plugins in RabbitMQ. This file is managed by the RabbitMQ server, via the rabbitmq-plugins command. This file overrides the /etc/rabbitmq/enabled_plugins path, in order to work around issues with upgrading the Log Collector from early versions.

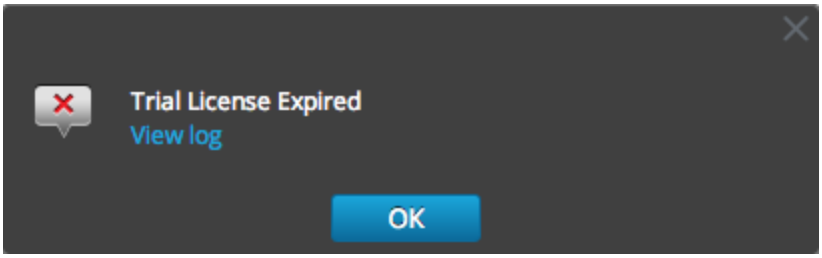
Component	File	Description
rabbit	/etc/rabbitmq/ssl/truststore.pem	The RabbitMQ trust store. This file contains a sequence of PEM-encoded X.509 certificates, represented trust CAs. Any clients that connect to RabbitMQ and present a certificate that is signed by a CA in this list is considered a trusted client.

Component	File	Description
rabbit	/var/log/rabbitmq/mnesia/nw@localhost	The RabbitMQ Mnesia directory. Mnesia is the Erlang/OTP database technology, for storing Erlang objects persistently. RabbitMQ uses this technology for storing information such as the current set of policies, persistent exchanges and queues, and so forth. Importantly, the msg_store_ persistent and msg_store_transient directories are where RabbitMQ stores messages that have been spooled to disk, e.g., if messages are published as persistent messages, or which have paged off to disk due to memory limitations. Keep a close eye on this directory, if the disk or memory alarms have tripped in RabbitMQ. **Caution:** Do not delete these files manually. Use RabbitMQ tools to purge or delete queues. Modifying these files manually may render your RabbitMQ instance inoperable.

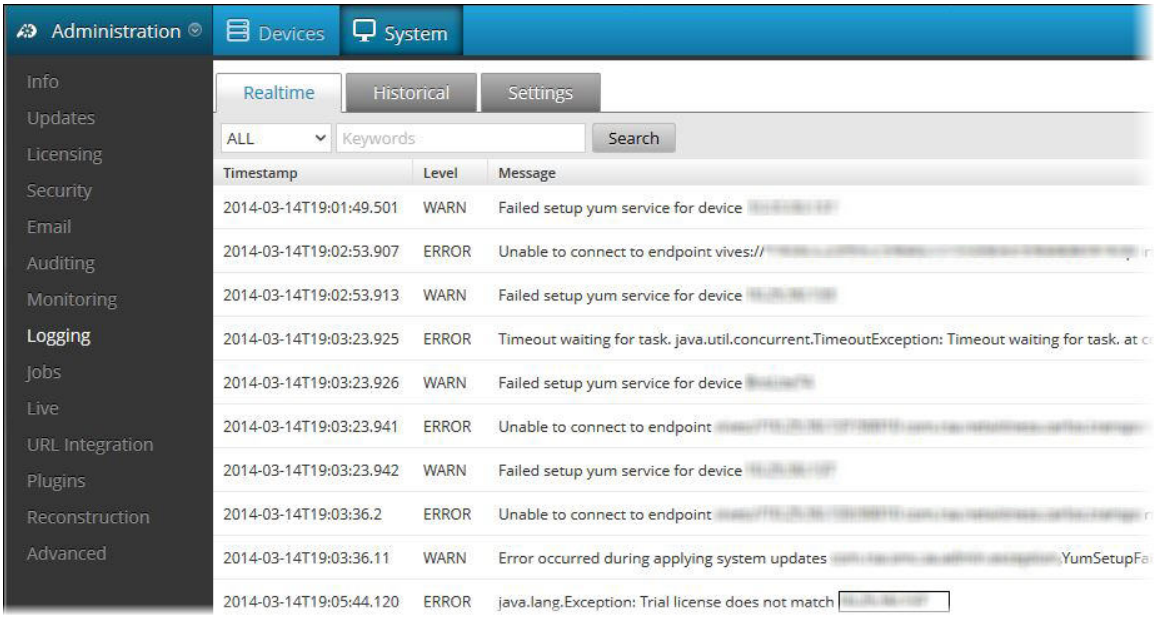
Error Notification

NetWitness Suite has a set of error message types associated with different components and operations. NetWitness Suite displays feedback in the form of a simple error notification and a log entry.

When an error notification dialog is displayed, you have two options: simply acknowledge the message or view the system log for more information.



If you want to view the system log for more information when an error notification is displayed, click **View log**. The log opens in the **Administration** > **System** view with a list of messages. Timestamp and message level are also listed.



Miscellaneous Tips

Audit Log Messages

It can be useful to see which user actions result in which log message types in the **/var/log/**messages file.

The event categories spreadsheet included in the log parser package in the NetWitness Suite Parser v2.0.zip archive lists the event categories and the event parser lines to help with building reports, alerts, and queries.

NwConsole for Health & Wellness

RSA has added a command option called **logParse** in **NwConsole**. This command option supports log parsing, a convenient way to check log parser without setting up the full system to do log parse. For more information about the **logParse** command, at the command line, type `help logParse`.

Thick Client Error: remote content device entry not found

Error: "*The remote content device entry was not found*," generated for a correlation rule applied to a concentrator.

Problem: in Investigation, if you click the `correlation-rule-name` meta value in the Alert meta key, you do not get session information.

Solution: Instead of using correlation rules on decoders and concentrators, use ESA rules. The ESA rules **do** record the correlation sessions that match the ESA rule.

View Example Parsers

Since flex and lua parsers are encrypted when they are delivered by Live, you cannot easily view their contents.

However, some plain text examples are available here: **https://community.emc.com/docs/DOC-41108**.

Configure WinRM Event Sources

The following Inside EMC article has a video that walks through the process of setting up Windows RM (Remote Management) collection: **https://inside.emc.com/docs/DOC-122732**.

Additionally, it contains two scripts that are shortcuts for procedures described in the "Windows Event Source Configuration Guide."

NwLogPlayer

NwLogPlayer is a utility that simulates syslog traffic. In the hosted environment, `NwLogPlayer.exe` is a command line utility located on the RSA NetWitness® Suite Client machine in the following directory:

```
C:\Program Files\NetWitness\NetWitness 9.8
```

NwLogPlayer is also located on the Log Decoder host in `/usr/bin`.

Usage

At the command line, type `nwlogplayer.exe -h` to list the available options, as reproduced here:

`--priority arg`	set log priority level
`-h [ --help ]`	show this message
`-f [ --file ] arg (=stdin)`	input message; defaults to **stdin**
`-d [dir ] arg`	input directory
`-s [ --server ] arg (=localhost)`	remote server; defaults to **localhost**
`-p [ --port ] arg (=514)`	remote port; defaults to **514**
`-r [ --raw ] arg (=0)`	Determines raw mode. • 0 = add priority mark (default) • 1= File contents will be copied line by line to the server. • 3 = auto detect • 4 = enVision stream • 5 = binary object
`-m [ --memory ] arg`	Speed test mode. Read up to 1 Megabyte of messages from the file content and replays.
`--rate arg`	Number of events per second. This argument has no effect if **rate** > eps that the program can achieve in continuous mode.
`--maxcnt arg`	maximum number of messages to be sent
`-c [ --multiconn ]`	multiple connection
`-t [ --time ] arg`	simulate time stamp time; format is `yyyy-m-d-hh:mm:ss`
`-v [ --verbose ]`	If **true**, output is verbose
`--ip arg`	simulate an IP tag
`--ssl`	use SSL to connect

`--certdir arg`	OpenSSL certificate authority directory
`--clientcert arg`	use this PEM-encoded SSL client certificate
`--udp`	send in UDP

Troubleshoot Feeds

Overview

The purpose of the feed generator is to generate a mapping of an event source to the list of groups to which it belongs.

If you have an event source from which you are collecting messages, and yet it is not displayed in the correct event source groups, then this topic provides background and information to help you track down the problem.

Details

The ESM Feed maps multiple keys to single value. It maps the DeviceAddress, Forwarder, and DeviceType attributes to groupName.

The purpose of the ESM feed is to enrich event source Meta with the groupName collected on the Log Decoder.

How it Works

The feed generator is scheduled to update every minute. However, it is triggered only if there are any changes (create, update, or delete) in event sources or groups.

It generates a single feed file with event source to group mapping, and pushes the same feed to all of the Log Decoders that are connected to NetWitness Suite.

Once the feed file is uploaded on the Log Decoders, for any new events, it enriches events Meta data with groupName, and appends this groupName to logstats.

Once the groupName is in logstats, the ESM Aggregator groups information and sends it to ESM. At this point, you should see the **Group Name** column under the **Event Source Monitoring** tab.

The entire process can take some time. Therefore, you may need to wait for several seconds after you add a new group or event source, before the Group name is displayed.

Note: If the event source type attribute changes when the feed is updated, NetWitness Suite adds a new logstats entry, rather than updating the existing one. Thus, there will be two different logstats entries in logdecoder. Previously existing messages would have been listed under the previous type, and all new messages are logged for the new event source type.

Feed File

The format of the feed file is as follows:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

The `DeviceAddress` is either `ipv4, ipv6`, or `hostname`, depending on which of these have been defined for the event source.

The following is a sample of the feed file:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apachegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","Apachegrp"
```

Troubleshooting

You can check the following items to narrow down where the problem is occurring.

Feed File Existence

Verify that the feeds ZIP archive exists in the following location:

```
/opt/rsa/sms/esmfeed.zip
```

Do not modify this file.

Group Meta Populated on LD

Verify that the group meta is populated on the Log Decoder. Navigate to the Log Decoder REST and check logstats:

```
http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain
```

This is a sample logstats file with group information:

```
device=apache  forwarder=NWAPPLIANCE10304  source=1.2.3.4  count=338  lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-04 22:30:19 groups=IP1234Group,apacheGroup
device=apachetomcat  forwarder=NWAPPLIANCE10304  source=5.6.7.8  count=1301  lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-04 22:30:19  groups=AllOtherGroup,ApacheTomcatGroup
```

In the above text, the group information is **bold**.

Device Group Meta on Concentrator

Verify that the **Device Group** meta exists on the Concentrator, and that events have values for the `device.group` field.

SMS Log File

Check the SMS log file in the following location to view informational and error messages: `/opt/rsa/sms/logs/sms.log`

The following are example informational messages:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

The following are example error messages:

```
Error creating CSV File : <reason>Unable to push the ESM Feed: Unable to
create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> : Error: <error>
Unable to push the ESM Feed: CSV file is empty, make sure you have al-
least on group with al-least one eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on LogDecoder-
<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error: The zip
archive "/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not be
opened
Unable to push the ESM Feed: <reason>
```

Verify Logstats data is getting Read & Published by ESMReader & ESMAggregator

These are the steps to verify that logstats are collected by **collectd** and published to Event Source Management.

ESMReader

1. On LogDecoders add **debug "true"** flag in **/etc/collectd.d/NwLogDecoder_ESM.conf**:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>        </stats>    </Module>    <Module
"NgEsmReader" "update">        port      "56002"
```

```
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>        </stats>    </Module></Plugin>
```

2. Run the command:
   `collectd service restart`
3. Run the following command:
   `tail –f /var/log/messages | grep collectd`
   Verify that ESMReader is reading logstats and there are no errors. If there are any read issues, you will see errors similar to the following:

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. On NetWitness Suite, uncomment the verbose flag in **/etc/collectd.d/ESMAggregator.conf**:

```
        # ESMAggregator module collectd.conf configuration file
        #
        # Copyright (c) 2014 RSA The Security Divsion of EMC
        #

        <Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"

        <Module "ESMAggregator">
                verbose 1
                interval "60"
                cache_save_interval "600"
```

```
                persistence_dir "/var/lib/netwitness/collectd"
        </Module>    </Plugin>
```

2. Run the following:
   `collectd service restart.`
3. Run the following command:
   `run "tail -f /var/log/messages | grep ESMA`
   Look for for ESMAggregator data and make sure your logstat entry is available in logs.

Sample output:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
```

```
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Configure JMX Feed Generator Job Interval

Although the feed generation job is scheduled to execute every minute by default, you can change this by using `jconsole`, if necessary.

To change the feed generator job interval:

1. Open **jconsole** for the SMS service.
2. On the MBeans tab, navigate to **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributes**.
3. Modify the value for the property **FeedGeneratorJobIntervalInMinutes**.
4. Go to **Operations** under the same navigation tree, an click **commit()**. This persists the new value in the corresponding json file under **/opt/rsa/sms/conf**, and uses the value if SMS is restarted.

Setting a new value reschedules the feed generator job for the new interval.

References

This section describes the NetWitness Suite user interface views in which you can perform system maintenance tasks. You use this interface to:

- Monitor and maintain services (settings, statistics, command and message syntax, REST API, RSA Console utility, and protocols supported in NetWitness Suite).
- Display the current NetWitness Suite version and license status.
- Manage your Local Update Repository from which you apply software version updates to hosts.

The following topics describe each interface in detail:

- Health and Wellness View
- System View - System Info Panel

Health and Wellness View

The Health and Wellness settings allow you to set and view alarms, monitor events, and view policies and system statistics. For more details on each of these, see the following topics:

- Health and Wellness View - Alarms View
- Event Source Monitoring View
- Health and Wellness Historical Graphs
- Health and Wellness Settings View - Archiver
- Health and Wellness Settings View - Event Sources
- Health and Wellness Settings View - Warehouse Connector
- Monitoring View
- Policies View
- System Stats Browser View

Health and Wellness View - Alarms View

You can monitor hosts and services to determine when user-defined limitations have been reached by viewing all the active alarms. Policy rules, that you define or assign to hosts and services, in the **Policies tab** trigger these alarms. You can:

- View all the alarms that are currently active for all your systems and services
- Select an alarm and view its details

What do you want to do?

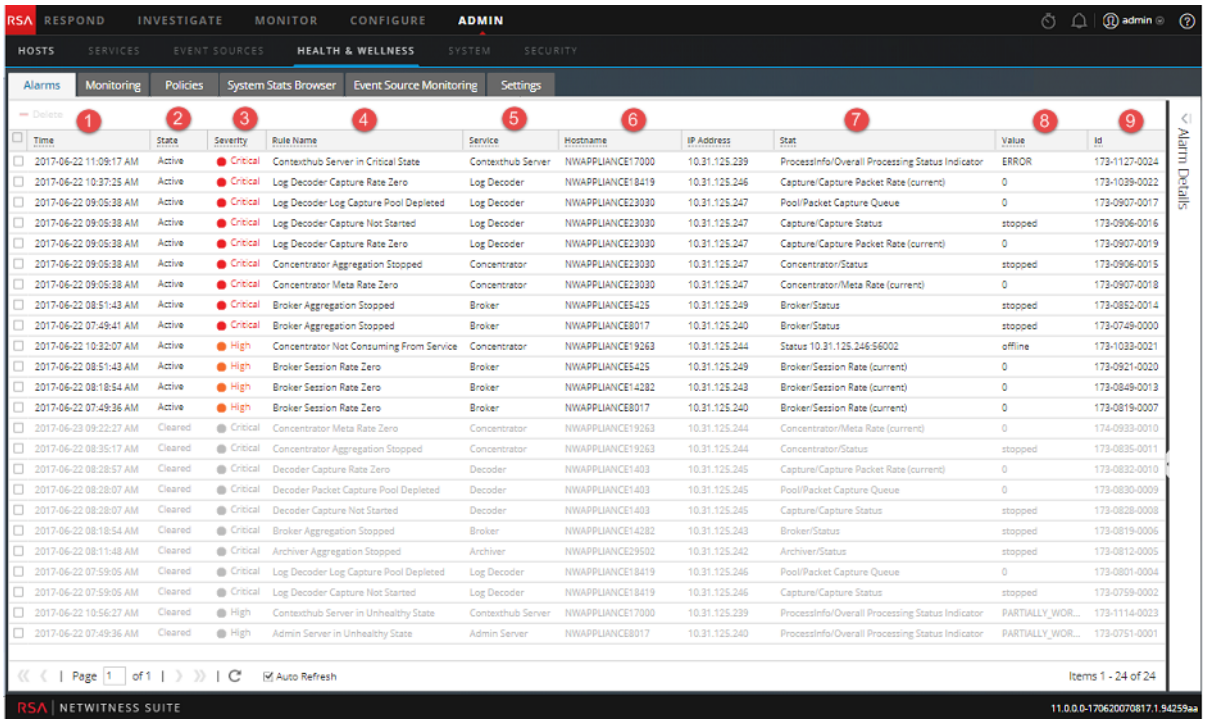
Role	I want to ...	Show me how
Administrator	View the alarm status of NetWitness Servers and services.	Monitor Alarms
Administrator	View detailed information about a specific alarm.	Monitor Alarms

Related Topics

Manage Policies

Quick Look

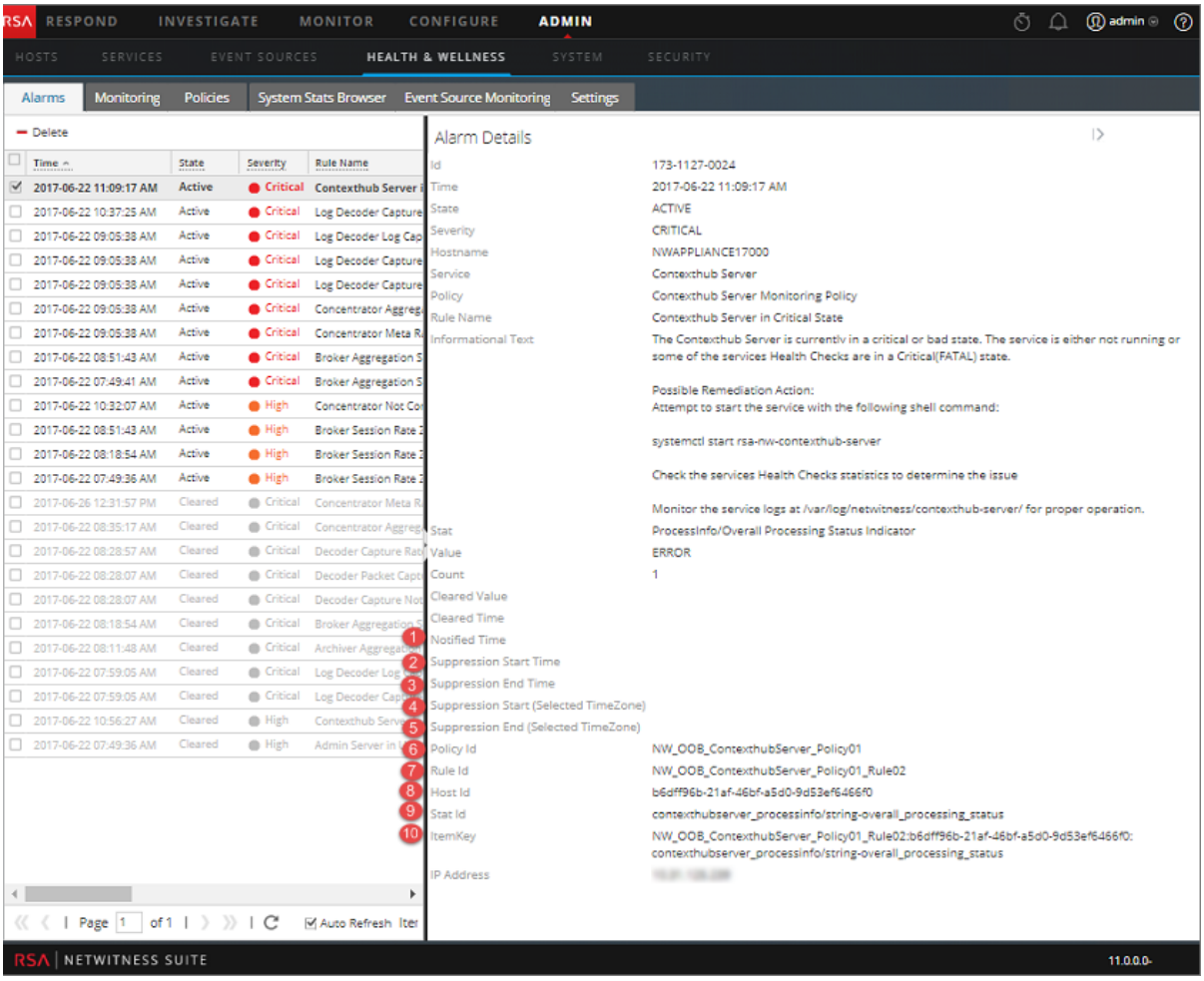
The required permission to access this view is **Manage services**. To access the Alarms view, go to **Admin** > **Health & Wellness**. The Health & Wellness view opens with the Alarms tab displayed. The Alarms tab contains an alarms list and an Alarm Details panel.



1	Time when the alarm was triggered.
2	Status of the alarm: • **Active** - the statistical threshold was crossed triggering the alarm. • **Cleared** - the clearing threshold was crossed and the alarm is no longer active.
3	Severity assigned to this alarm: • **Critical** • **High** • **Medium** • **Low**
4	Name of the rule that triggers the alarm.
5	Service defined in the rule.
6	Host on which the alarm is triggered.
7	Statistic selected in the rule that triggers the alarm.
8	Value of the statistic that triggered the alarm.
9	Identification number of the alarm.

Note: NetWitness Suite sorts the alarms in time order. You can sort the relevant parameters in ascending or descending order.

This figure shows the Alarms tab with the Alarm Details panel expanded.



Alarm Details Panel

The Alarm Details panel displays information for the alarm selected in the Alarms list. It contains all the information in the Alarms list plus the following fields.

1	Alarm Notified time
2	Suppression start time
3	Suppression end time
4	Suppression start (selected time zone)
5	Suppression end (selected time zone)
6	The Policy ID

7 The Rule ID

8 The Host ID

9 The Stat ID

10 Item key

Event Source Monitoring View

Note: To manage Event Sources, see "About Event Source Management" in the *NetWitness Suite Event Source Management Guide*.

NetWitness Suite provides a way to monitor the statistics for various event sources in the User Interface. The information displayed is historical and comes from the Log decoder. You can customize the view depending on the parameter you select to filter the data.

To access the Event Source Monitoring view:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Click **Event Source Monitoring**.

What do you want to do?

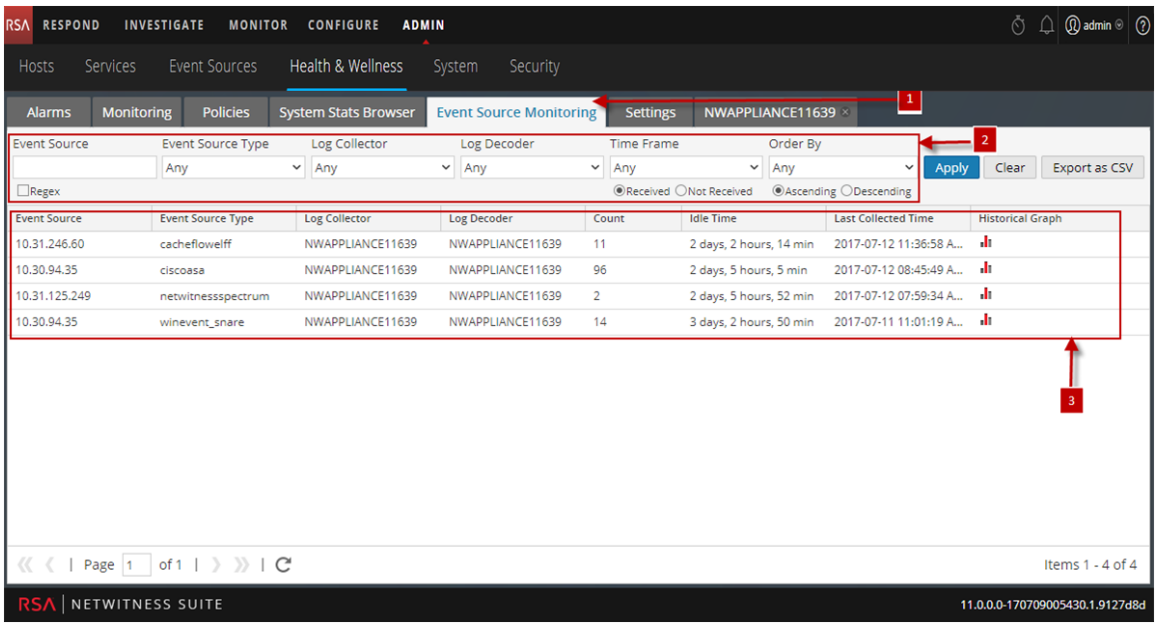
Role	I want to ...	Show me how
Administrator	View the Events Collected from an Event Source	Historical Graph View for Events Collected from an Event Source

Related Topics

- Monitor Event Sources
- Filter Event Sources
- View Historical Graph of Events Collected for an Event Source

Quick Look

The Event Source Monitoring view is displayed.



1 Displays Event Source Monitoring tab.

2 Toolbar used to filter and customize the Event Source Monitoring tab.

3 Displays Event Source Stats panel.

Filters

This table lists the various parameters you can use to filter and customize the event source monitoring view.

Parameter	Description
Event Source	Type the name of an event source you want to monitor. Select Regex to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Event Source Type	Select an event source type for the event source selected.
Log Collector	Select the Log Collector to display the data collected by the specified Log Collector.

Parameter	Description
Log Decoder	Select a Log Decoder to display the data collected by the specified Log Decoder.
Time Frame	Select the time frame for which you want the stats. Select **Received** if you need the query results to contain only event sources that logs have been received from within the selected time. or Select **Not Received** if you need the query results to contain only event sources that logs have not been received from within the selected time
Order By	Select the order in which the list needs to be filtered. Select Ascending to filter it in an ascending order.
Apply	Click to apply the filters chosen and display the list accordingly.
Clear	Click to clear the chosen filters.
Export as CSV	Click to export the information as a csv file.

Event Source Stats View Display

Parameter	Description
Event Source	Displays the name of the event source.
Event Source Type	Displays the event source type.
Log Collector	Displays the Log Collector from where the events were initially captured.
Log Decoder	Displays the Log Decoder where the events are being processed.
Count	Displays the number of events received by Log Decoder since last reset of count value.
Idle Time	Displays the time lapsed after the last stat collection.

Parameter	Description
Last Collected Time	Displays the time at which the Log Decoder last processed an event for the event source
Historical Graph	Click to view the historical graph of the stats collected for the event source.

Health and Wellness Historical Graphs

Configuring the Archiver monitoring enables you to automatically generate notification when critical thresholds concerning Archiver aggregation and storage have been met. The Historical Graph view provides a visualization of historical data.

Note: Historical graphs are not available for non-numeric statistics, and is indicated by a greyed out icon.

See the following topics for more details:

- Historical Graph View for Events Collected from an Event Source
- Historical Graph for System Stats

Historical Graph View for Events Collected from an Event Source

The Historical Graph view for events collected from an event source provides a visualization of historical data. To access this view:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Monitoring tab open.

2. Click **Event Source Monitoring**.

   The Event Source Monitoring view is displayed.

3. In the **Historical Graph** column, select .

   The Historical graph for the selected event source type is displayed in a popup window.

The figure displays the events collected from the event source type **winevent_snare**.

You can customize the graph as required. The table lists the various parameters used to customize the historical graph.

Parameter	Description
Time Frame	Select the Time Frame for which you want to view the historical data. The available options are: Current Day, Current, Week, Current Month.
From <date> To <date>	Select the date range for which you want to view the historical data.

You can zoom in for a detailed view of the data in the Historical graph.

Zoom In Function 1 and 2

You can select one of the values to view the historical data for the selected value. The figure below displays an example for the 6h frame selected for zoom in. The slider bar at the right bottom corner is also changed to a 6h window.

Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.

Zoom In Function 3

You can click and drag in the plot area to zoom in for a required frame of time.

Historical Graph for System Stats

To access the Historical Graph for the System Stats:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

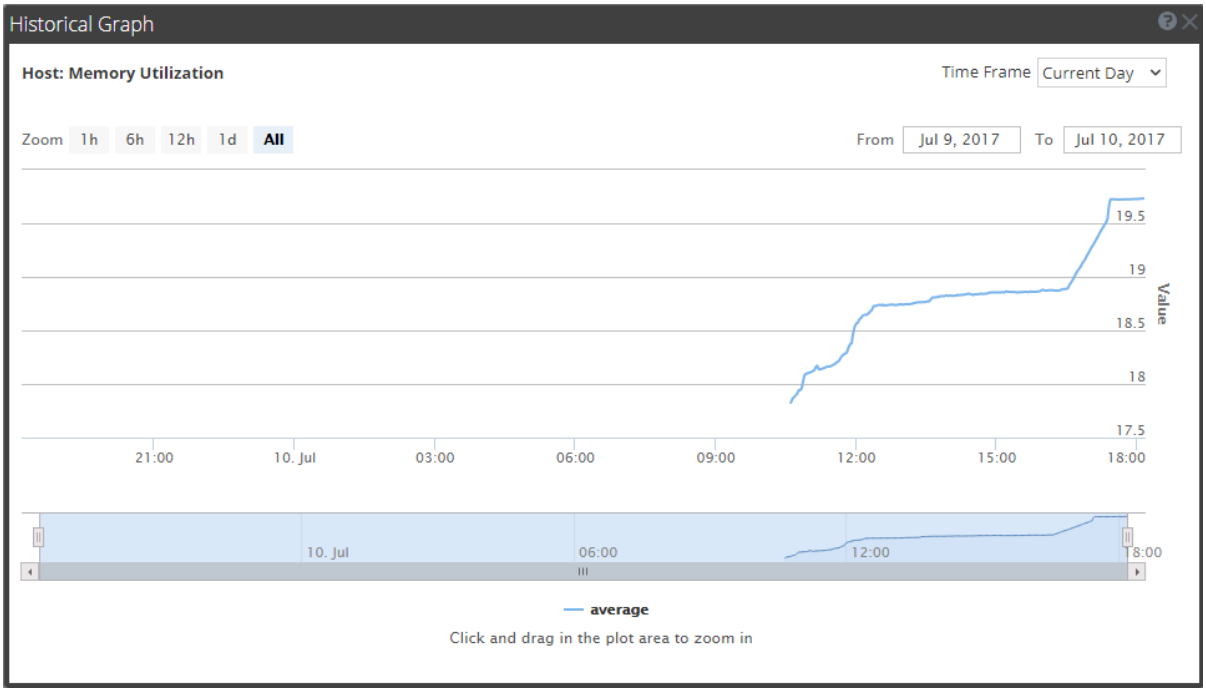
2. Click the **System Stats Browser** tab.

   The System Stats Browser tab is displayed.

3. In the **Historical Graph** column, select .

   The Historical graph for the selected statistic for a host is displayed.

   The figure displays the system stats view for the Memory Utilization statistics.



Parameters

You can customize the graph view as required. The table lists the various parameters used to customize the historical graph view.

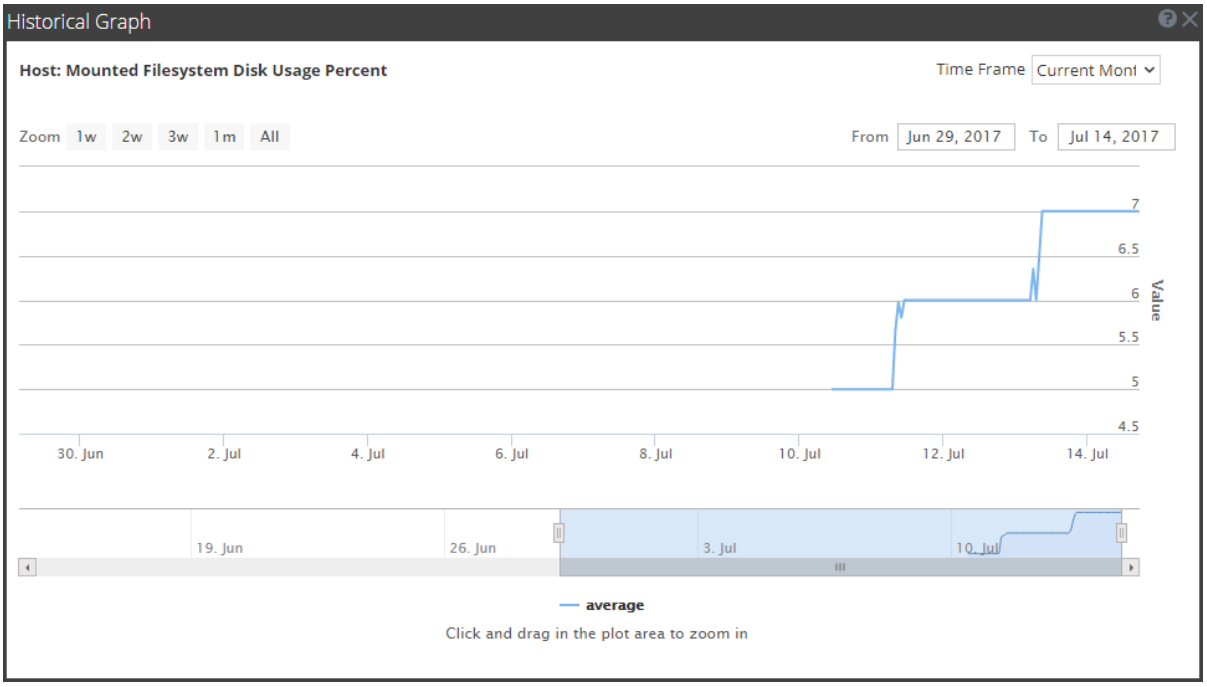
Parameter	Description
Time Frame	Select the time frame for which you want to view the historical data. The available options are: **Current Day**, **Current Week**, **Current Month**, and **Current Year**.
From <date> To <date>	Select the date range for which you want to view the historical data,

You can zoom in for a detailed view of the data in the Historical graph.

Zoom in function 1 and 2:

You can select one of the values to view the historical data for the selected value. The figure below displays an example for the 6h frame selected for zoom in. The slider bar at the right bottom corner is also changed to a 6h window.

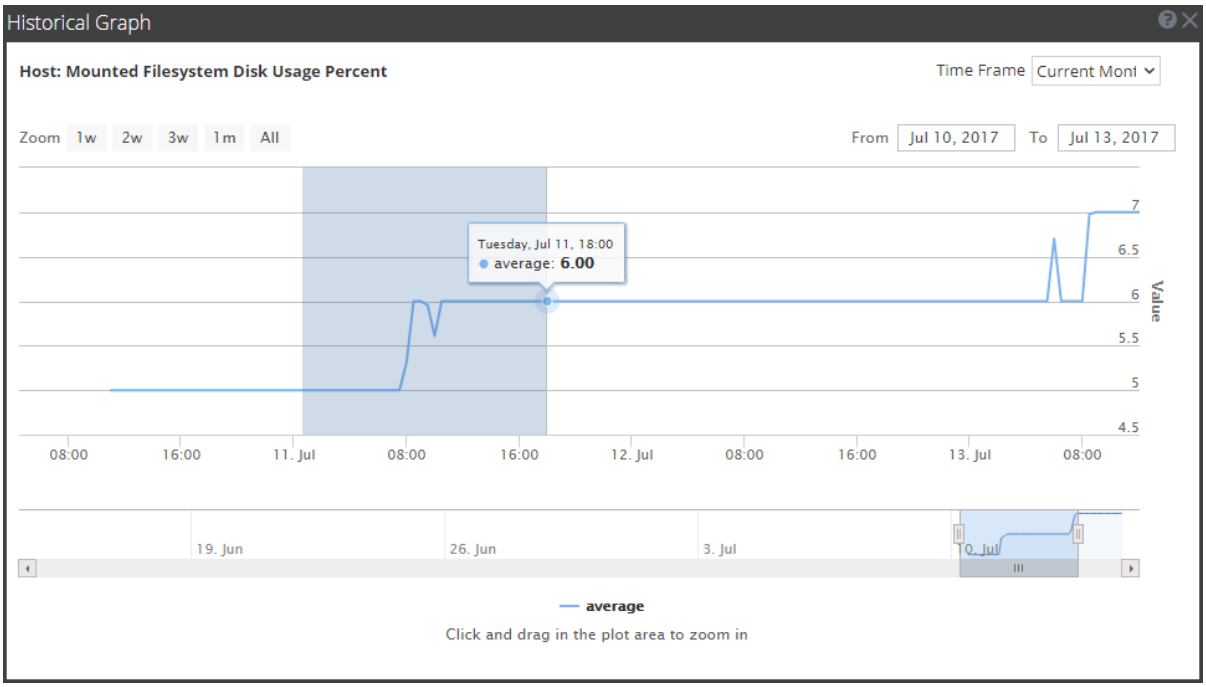
Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.



Zoom in function 3:

You can click and drag in the plot area to zoom in for a required frame of time.

The figure below displays an example of how the graph appears while you click and drag.


Historical Graph
Host: Mounted Filesystem Disk Usage Percent
Time Frame
Current Mont
Zoom
1w
2w
3w
1m
All
From
Jul 10, 2017
To
Jul 13, 2017
Tuesday, Jul 11, 18:00
average: 6.00
7
6.5
6
5.5
5
4.5
Value
08:00
16:00
11. Jul
08:00
16:00
12. Jul
08:00
16:00
13. Jul
08:00
19. Jun
26. Jun
3. Jul
10. Jul
average
Click and drag in the plot area to zoom in

Health and Wellness Settings View - Archiver

Note: To monitor Archiver and Warehouse Connector, see Health Policy.

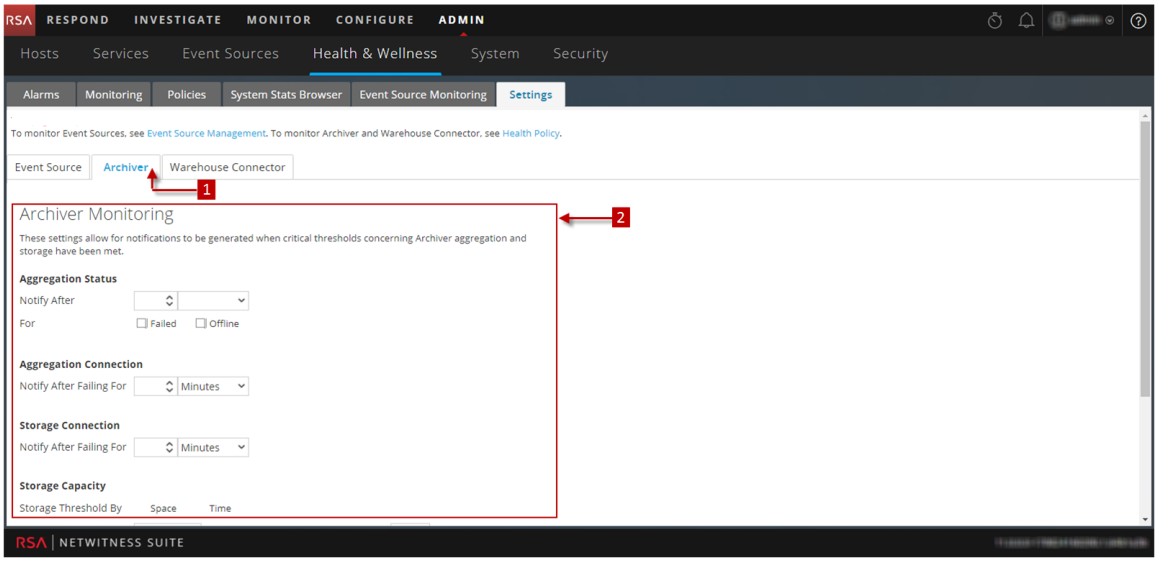
To access the Archiver Monitoring view:

1. Go to **Administration > Health & Wellness**.
2. Select **Settings > Archiver**.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Monitor service details of Archiver	Monitor Service Details

Quick Look



1	Displays Archiver Monitoring Panel
2	Configure Archiver Monitoring Panel to automatically receive notification

Features

The following table lists the parameters required to configure the Archiver to automatically generate notification when critical thresholds are reached.

Parameter	Value	Description
Aggregation Status	Notify After	Number of minutes or hours after which the you will get notified of the Aggregation status
	For	Failed - If enabled, you get notification when the Archiver aggregation status is failed for the defined number of minutes or hours. Offline - If enabled, you get a notification when the Archiver aggregation status is offline for the defined number of minutes or hours
Aggregation Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver aggregation connection fails.
Storage Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver storage connection fails.
Storage Capacity	Storage Threshold By	Select **Space**, if you want to receive a notification when the Archiver storage capacity exceeds the percentage defined in the **When Storage Size Is** field. Select **Time**, if you want to receive a notification when the files stored in the Archiver exceeds the defined number of days in the **When Oldest Storage File Is** field
	When Storage Size Is	Enter what percent full the storage size should be if you want to receive a notification.
	When Warm Storage Size Is	Enter what percent full the warm storage size should be if want to receive a notification.

Parameter	Value	Description
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness Suite.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.
	NW Console, Email, Syslog Notification, SNMP Trap Notification	Enable NW Console to get notifications on the NetWitness Suite UI notification toolbar. Enable Email to get email notifications. Enable Syslog Notification to generate syslog events. Enable SNMP Trap Notification to get audit events as SNMP traps.

Health and Wellness Settings View - Event Sources

Note: To manage Event Sources, see "About Event Source Management" in the *RSA NetWitness Suite Event Source Management Guide*.

The Event Source Monitoring view consists of the Event Source panel, Add/Edit Source Monitor dialog, Decommission panel, and the Decommission dialog. You use the view to configure:

- When to generate notifications for event sources from which the Log Collector is no longer receiving logs.
- Where to send those notifications.
- When to decommission a Log Collector when a Remote Collector and the Local Collector fails over to a standby Log Decoder.

The required role to access this view is **Manage NW Auditing**. To access this view:

1. Go to **Admin > Health & Wellness**.
2. Select **Settings > Event Source**.

What do you want to do?

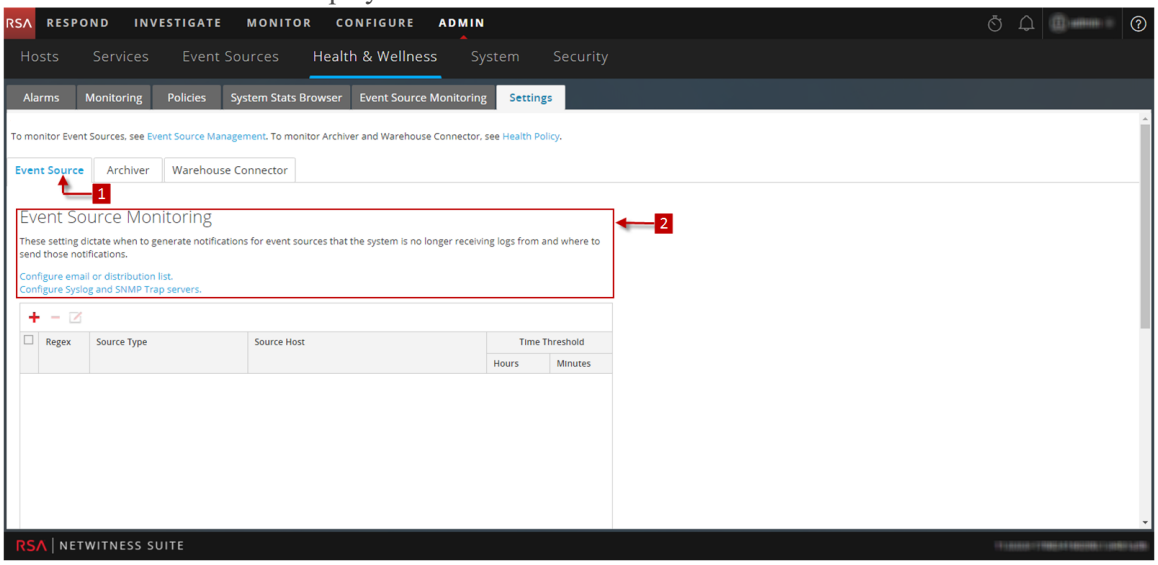
Role	I want to ...	Show me how
Administrator	View the functionality of Event Source Monitoring	Monitor Event Sources

Related Topics

Configure Event Source Monitoring

Quick Look

The Event Source tab is displayed.



1	Displays Event Source Monitoring Panel
2	Configure Event Source Monitoring Panel to receive notification

Event Source Monitoring Panel

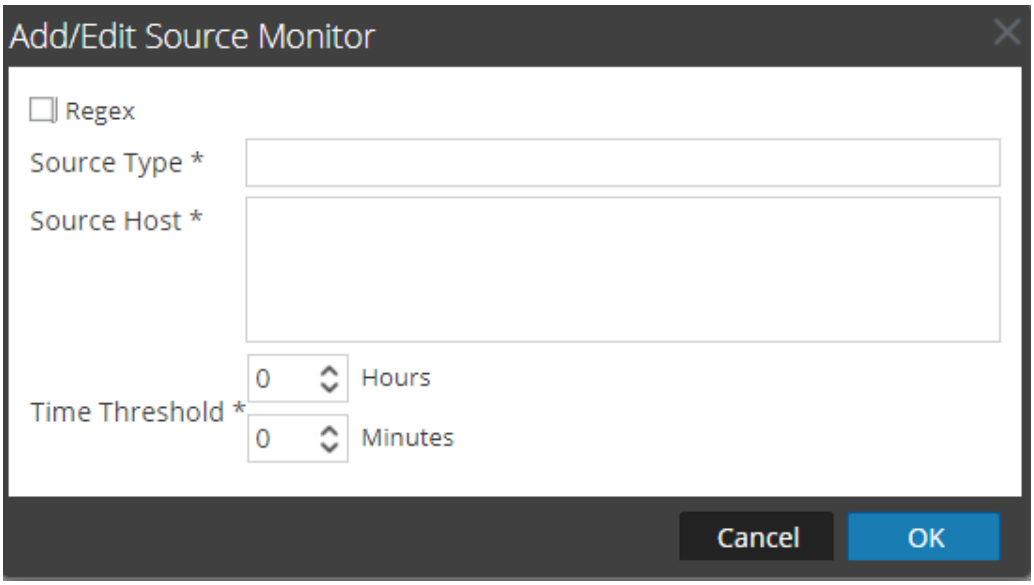
Feature	Description
Configure email or distribution list.	Opens the **Administration** > **System** > **Email view** so you can adjust the email distribution for the Event Source Monitoring output, if necessary.
Configure Syslog and SNMP Trap servers.	Opens the **Administration** > **System** > **Auditing view** so you can adjust the Syslog and SNMP trap distribution for the Event Source Monitoring output, if necessary.
+	Displays the Add/Edit Source Monitor dialog in which you add or modify event sources to monitor.
−	Deletes the selected event sources from monitoring.
☐	Selects an event source.

Feature	Description
Source Type	Displays the source type of the event source.
Source Host	Displays the source host of the event source.
Time Threshold	Displays the time period after which NetWitness Suite stops sending notifications (Time Threshold).
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancels any additions, deletion, or changes.

Decommission Panel

Feature	Description
	Displays the Decommission dialog in which you add or modify event sources to decommission.
	Deletes the selected event sources from decommissioning.
	Selects an event source.
Regex	Displays if you choose to use regular expressions
Source Type	Displays the source type of the decommissioned event source.
Source Host	Displays the source host of the decommissioned event source.
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancels any additions, deletions, or changes.

Add/Edit Source Monitor Dialog



In **Add/Edit Source Monitor** dialog, you add or modify the the event sources that you want to monitor. The two parameters that identify an event source are **Source Type** and **Source Host**. You can use **globbing** (pattern matching and wildcard characters) to specify the Source Type and Source Host of event sources as shown in the following example:

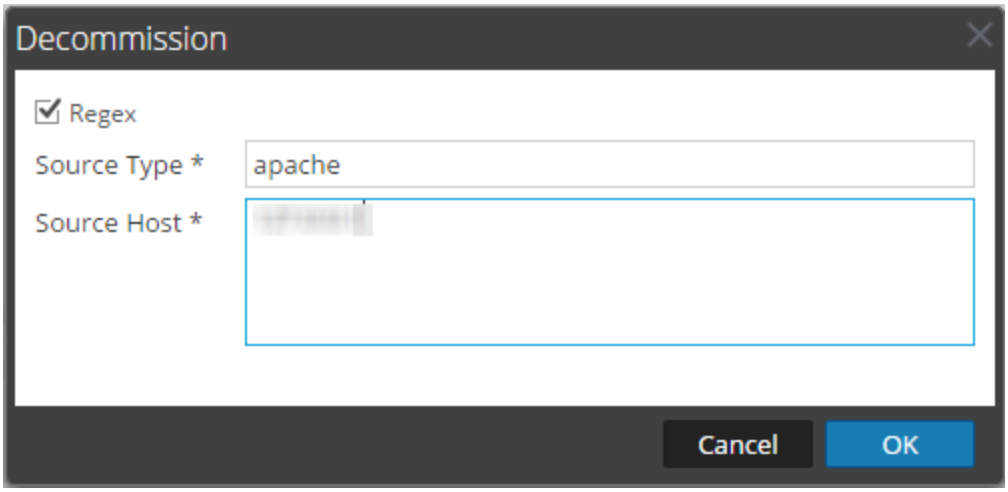
Source Type	Source Host
ciscopix	**1.1.1.1**
*	**1.1.1.1**
*	*
*	**1.1.1.1|1.1.1.2**
*	**1.1.1.[1|2]**
*	**1.1.1.[123]**
*	**1.1.1.[0-9]**
*	**1.1.1.11[0-5]**
*	**1.1.1.1,1.1.1.2**
*	**1.1.1.[0-9]|1.1.1.11[0-5]**

Source Type	Source Host
*	**1.1.1.[0-9]|1.1.1.11[0-5],10.31.204.20**
*	**1.1.1.***
*	**1.1.1.[0-9]{1,3}**

Features

Feature	Description
Regex	Select the checkbox if you want to use regular expressions
Source Type	The source type of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view.
Source Host	Hostname or IP address of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector device > **View** > **Config** view.
Time Threshold	The time period after which NetWitness Suite starts sending notifications.
Cancel	Closes the dialog without adding the event source, or changes to the event source, to the Event Source Monitoring panel.
OK	Adds the event source to the Event Source Monitoring panel.

Decommission Dialog



Feature	Description
Source Type	The source type of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector device > **View** > **Config** view.
Source Host	Hostname or IP address of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view.
Cancel	Closes the dialog without applying any event source additions, deletions, or changes to the Decommissioning panel.
OK	Applies any event source additions, deletions, or changes to the Decommissioning panel.

Health and Wellness Settings View - Warehouse Connector

Note: To monitor Archiver and Warehouse Connector, see "Health Policy".

Configuring the Warehouse Connector monitoring enables you to automatically generate notification when critical thresholds concerning Warehouse Connector and storage have been met.

Access the Warehouse Connector Monitoring view

1. Go to **Admin** > **Health & Wellness**.
2. Select **Settings** > **Warehouse Connector**.

What do you want to do?

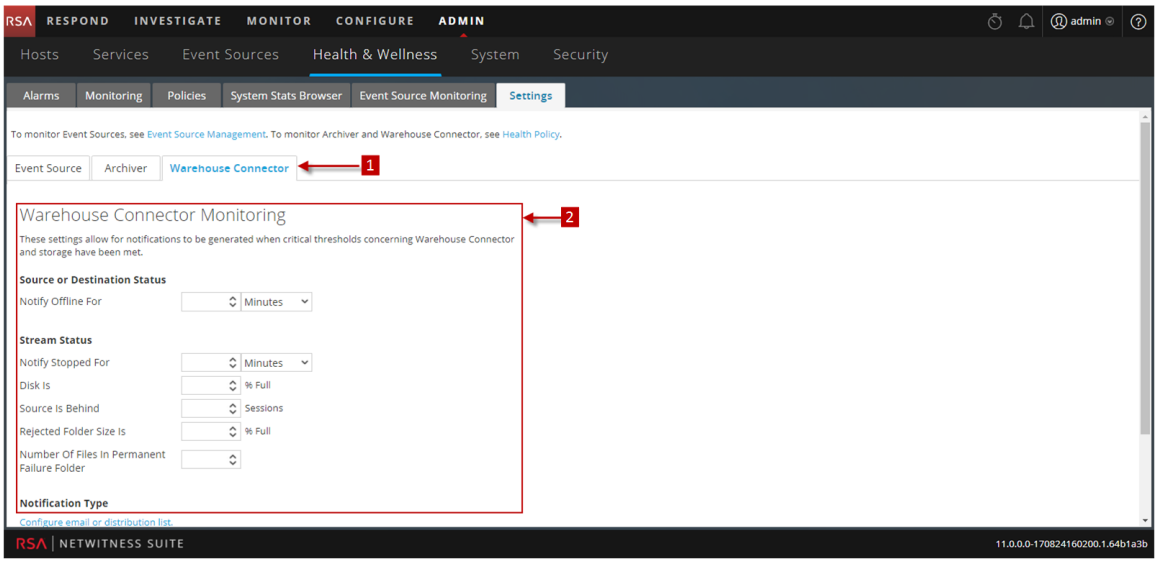
Role	I want to ...	Show me how
Administrator	View the details of Warehouse connector	Warehouse Connector Details View

Related topics

Monitor Service Details

Quick Look

The Warehouse Connector Monitoring view is displayed.



1 Displays Warehouse Connector Monitoring view Panel

2 Allows to configure Warehouse Connector Monitoring parameters

Warehouse Connector Monitoring parameters

The following table lists the parameters required to configure the Warehouse Connector to automatically generate notification when critical thresholds are reached.

Parameter	Value	Description
Source or Destination Status	Notify Offline For	Number of minutes or hours after which the you will receive a notification if the source or destination connection fails.
Stream Status	Notify Stopped For	Number of minutes or hours after which you would like to receive a notification when the Stream goes offline.
	Disk Is	The limit on the percentage of disk usage after which you would like to receive a notification.
	Source Is Behind	Number of sessions after which a notification is raised if the source goes behind the defined number of sessions.
	Rejected Folder Size Is	Limit on the percentage of folder usage after which you would like to receive a notification.
	Number Of Files in Permanent Failure Folder	Limit on the number of files in the permanent failure folder after which you would like to receive a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness Suite.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.

Parameter	Value	Description
	NW Console, Email, Syslog Notification, SNMP Trap Notification	Enable NW Console to get notifications on the NetWitness Suite UI notification toolbar. Enable Email to get email notifications. Enable Syslog Notification to generate syslog events. Enable SNMP Trap Notification to get audit events as SNMP traps.

Monitoring View

NetWitness Suite provides detailed statistics and other information about the host and the individual NetWitness Suite services on Details views. You can view the current health of all the hosts, services running on the hosts, various aspects of the hosts' health, host details and service details in the Monitoring view.

To access this view:

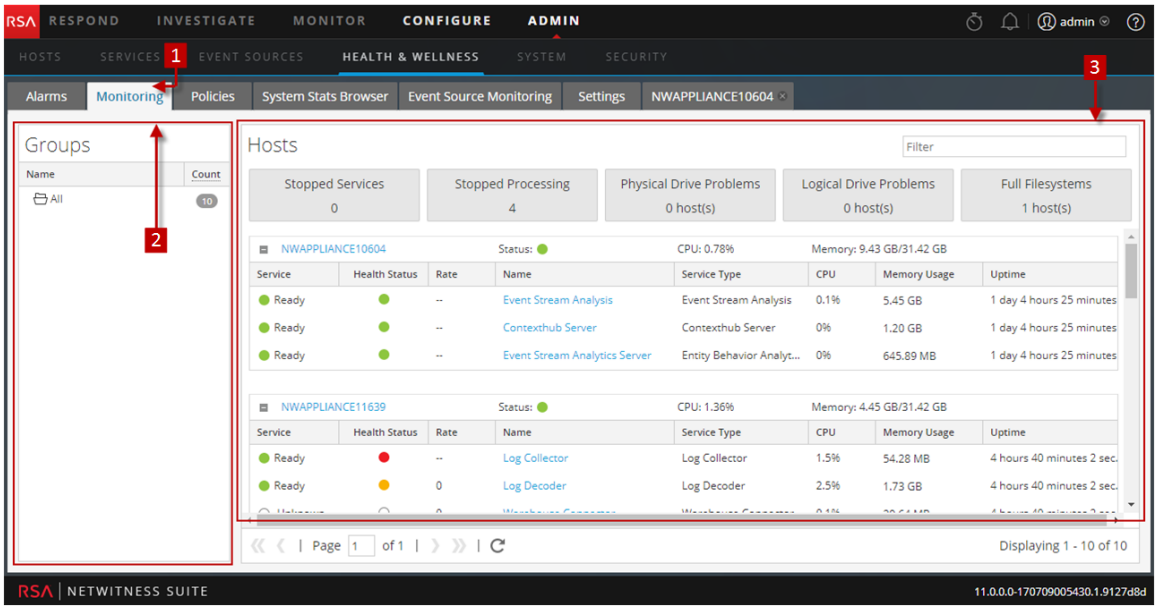
1. Go to **ADMIN > Health & Wellness**.
2. Click the **Monitoring** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View and Perform Procedures	Monitor Hosts and Services

Quick Look

The Monitoring view is displayed.



1	Displays Monitoring tab.
2	Group Panel to select a Group.
3	Hosts panel displays operational statistics.

Groups Panel

The Groups panel lists all the groups of hosts available. When you select a group, the associated content is displayed in the Hosts panel.

Note: If the total host **Count** in the **Groups** panel is lower than the actual number of hosts displayed in the **Hosts** panel, please refer to the Troubleshooting Health & Wellness topic for possible causes of this issue and recommended solutions.

Hosts Panel

The Hosts panel displays operational statistics for hosts and the services running on each host.

Parameter	Description
Filter	Type a host name or a service name in the Filter field to display the corresponding hosts and services in the Host panel.
Stopped Services	Click **Stopped Services** to display a list of all stopped services. It also displays the host on which the service is installed.
Stopped Processing	Click **Stopped Processing** to display a list of all the hosts that have services installed on them that are in the stopped processing status.
Physical drive Problems <#> host(s)	Click to view the hosts that have physical drive problems.
Logical Drive Problems <#> host(s)	Click to view the hosts that have logical drive problems.
Full Filesystems <#> host(s)	Click to view the hosts that have full file systems.

Note: The summary information in the boxes at the top displays the System Statistics for all the hosts configured in NetWitness Suite and does not change with host of filters on groups.

The top panel is followed by a list of hosts, the services installed on them and information regarding the hosts and services.

Parameter	Description
Host Name	Displays the host name. If a host has services installed you will see a ⊞ prefixed to the host name. Click ⊞ to view all the services installed on the host.
Status	Displays the status of the Host. ● - denotes that the host is active and running. ● - denotes that the host is stopped or yet to start processing.
CPU	Displays the current CPU usage of the host.
Memory	Displays the Memory used by the host.

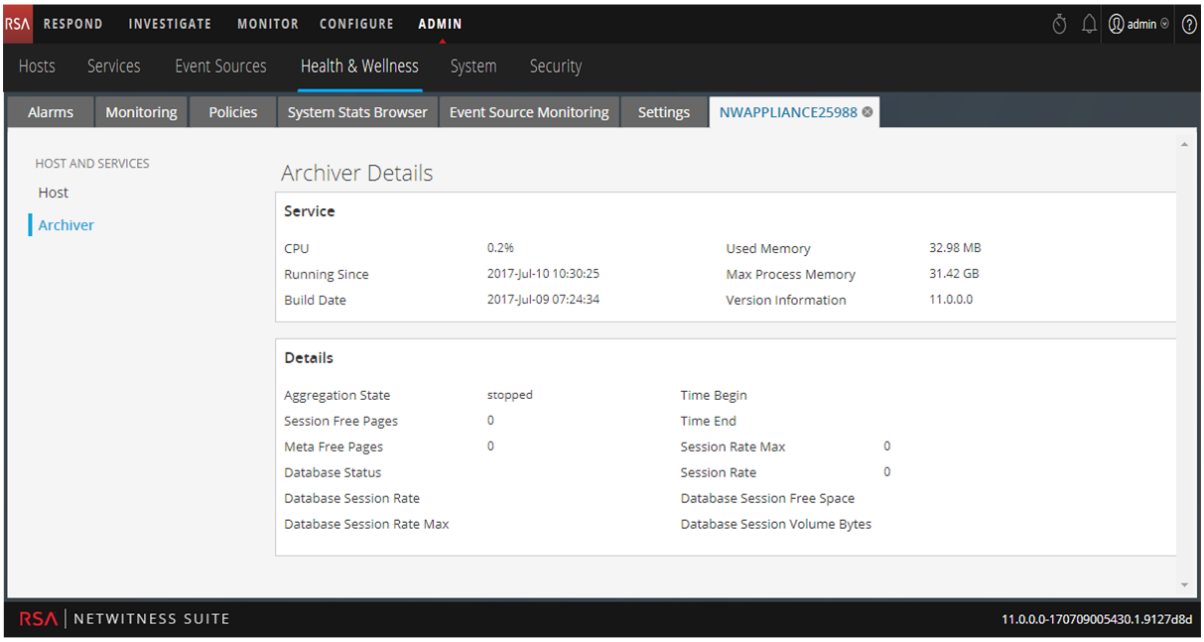
When you click ⊞ prefixed to the host name, a list of all the services installed on the host is displayed. The table below describes various parameters displayed for a service and their description.

Parameter	Description
Service	Displays the status of the service. ● Ready - denotes that the service is active and running. ● Stopped - denotes that the service is stopped or yet to start processing.
Health Status	Displays the processing status of the Service. ● - denotes that the process is running and the data is being processed at a rate greater than zero. ● - denotes that the processing is stopped. ● - denotes that the processing is turned on but the data is not being processed.
Rate	Denotes the rate at which the data is being processed.
Name	Name of the service.

Parameter	Description
Service Type	Name of the type of service.
CPU	Displays the current CPU usage of the service.
Memory Usage	Displays the Memory used by the service.
Uptime	Displays the time for which the service has been running.

Archiver Details View

The Archiver Details view provides information about the Archiver. The following figure depicts the Archiver Details.



For the related procedure, see Monitor Service Details

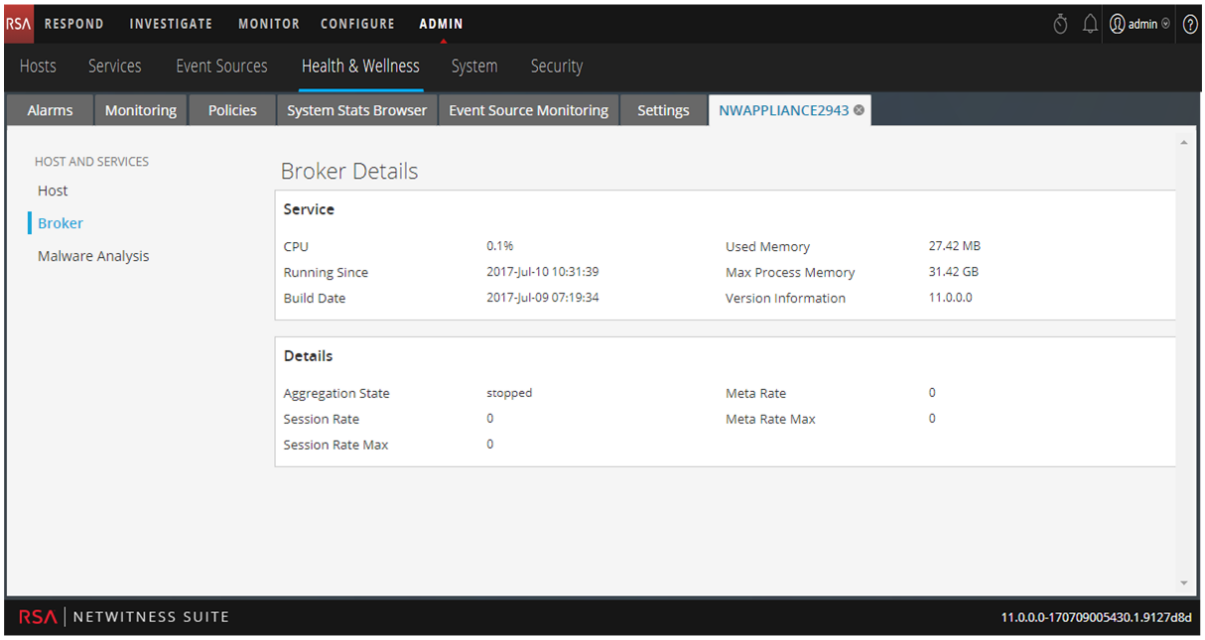
This section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Time Begin	Time (UTC) when the first session was tracked by the index.
Session Free Pages	Session pages available for aggregation.
Time End	Time (UTC) when the last session was tracked by the index.
Meta Free Pages	Pages available for aggregation.
Session Rate Max	Maximum sessions per second rate.

Statistic	Description
Database Status	Status of databases. Valid values are: • **closed** - not available for QUERY and UPDATE (databases are being initialized). This value is seldom seen. • **opened** - available for QUERY and UPDATE. • **failure** - failed to open. This can happen for any number of reasons. You can check this if CAPTURE fails to start or if queries fail to return data. This is normally caused by database corruption.
Session Rate	Sessions per second rate.
Database Session Rate	Per second rate at which the service is writing sessions to the database.
Database Session Free Space	Amount of session free space available for aggregation.
Database Session Rate Max	Maximum per second rate at which the service is writing sessions to the database.
Database Session Volume Bytes	Number of session bytes in the database.

Broker Details View

The Broker Details view provides information for the Broker. The following figure depicts the Broker Details.



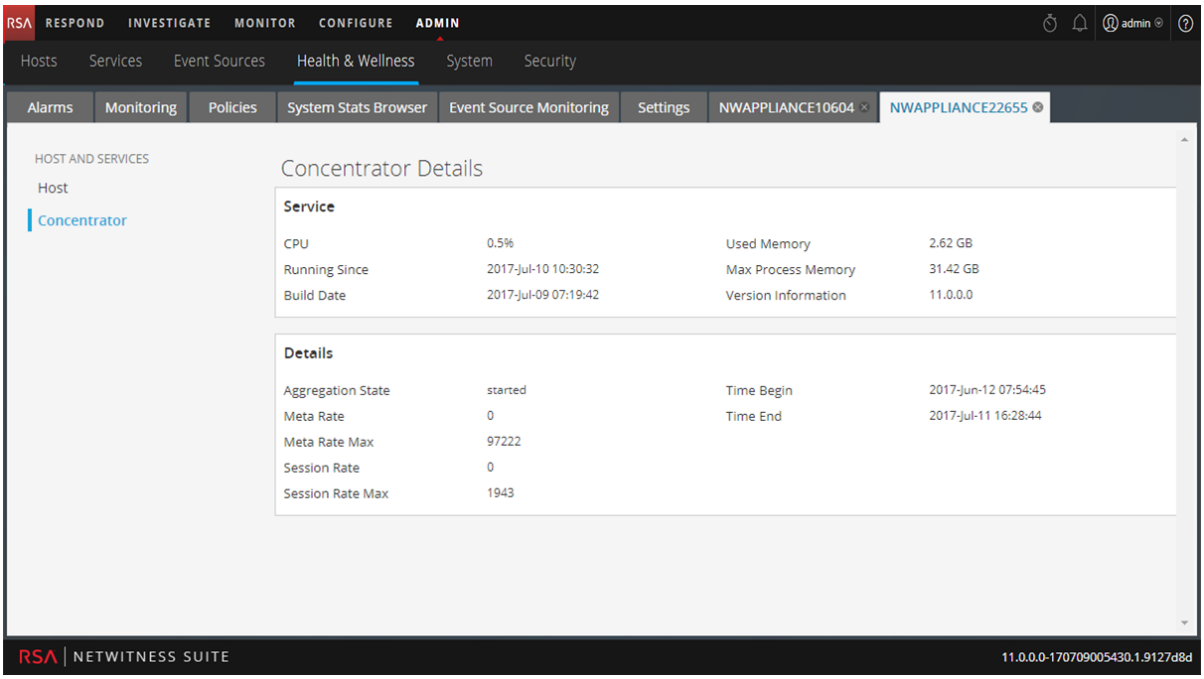
For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Meta Rate	Metadata objects per second rate.
Session Rate	Sessions per second rate.
Meta Rate Max	Maximum metadata objects per second rate.
Session Rate Max	Maximum sessions per second rate.

Concentrator Details View

The Concentrator Details view provides information for the Concentrator. The following figure depicts the Concentrator Details.



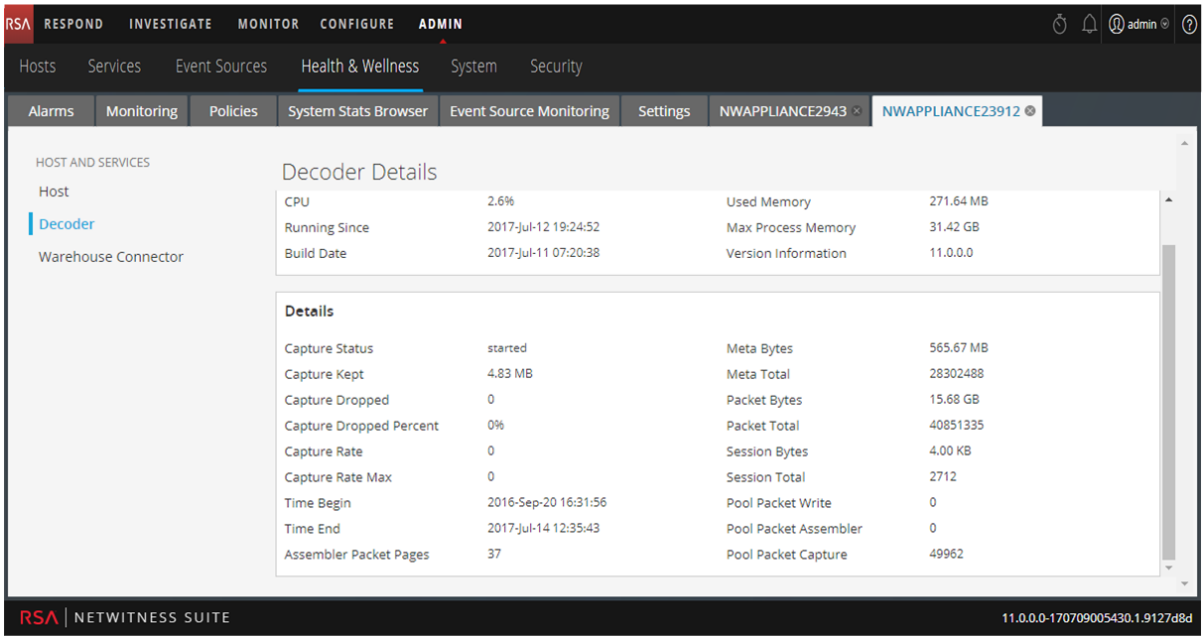
For the related procedure, see Monitor Service Details

The section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Time Begin	Time (UTC) when the first session was tracked by the index.
Meta Rate	Metadata objects per second rate.
Time End	Time (UTC) when the last session was tracked by the index.
Meta Rate Max	Maximum metadata objects per second rate.
Session Rate	Sessions per second rate.
Session Rate Max	Maximum sessions per second rate.

Decoder Details View

The Decoder Details view provides information for the Decoder. The following figure depicts the Decoder Details.



For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

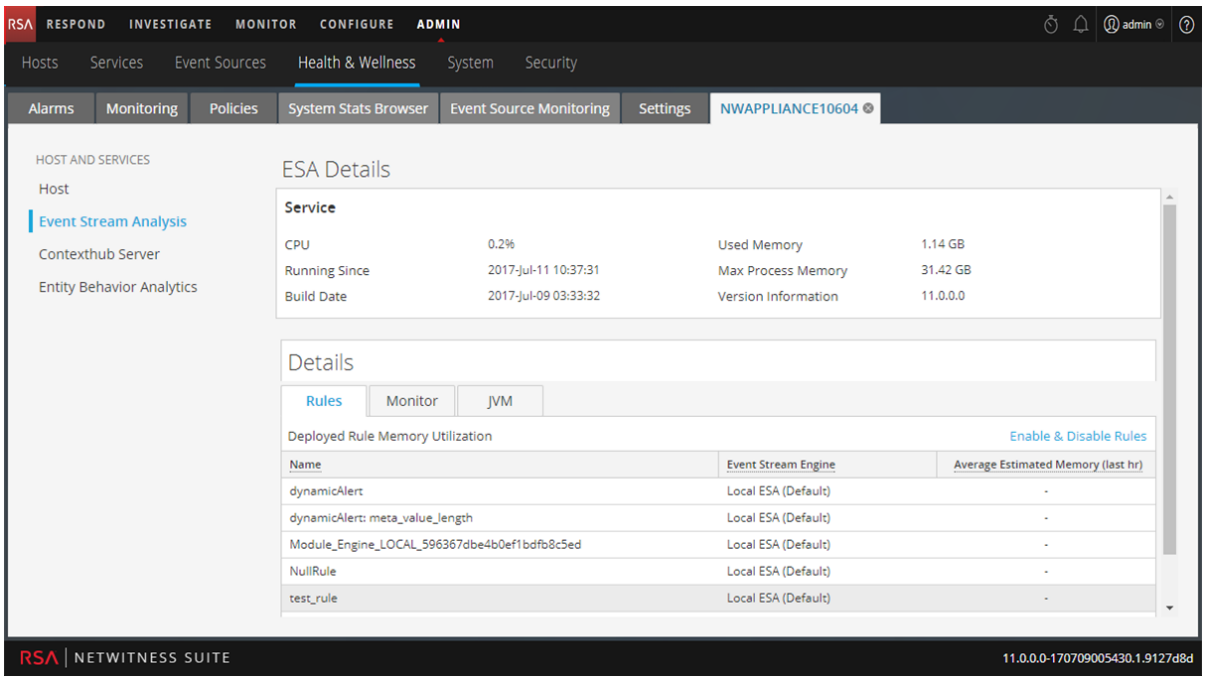
Statistic	Description
Capture Status	Status of data capture. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started**- Capturing data. • **stopping**- Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Decoder service.
Meta Bytes	Number of meta bytes in the database.
Capture Kept	Number of packets kept during capture.

Statistic	Description
Meta Total	Number of metadata in the database.
Capture Dropped	Number of packets reported by the network card as dropped. After the service stops capturing data, rate is reset to zero.
Packet Bytes	Number of packet bytes in the database.
Capture Dropped Percent	Packets reported by the network card as dropped as a percentage.
Packet Total	Number of packet objects held in the packet database. The total decreases when the database rolls files off due to size constraints. After the service stops capturing data, the number is not reset.
Capture Rate	Megabits per second rate at which the service is capturing data. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, rate is reset to zero.
Session Bytes	Number of session bytes in the database.
Capture Rate Max	Maximum megabits per second rate at which the service is capturing data. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate during data capture.
Session Total	Number of sessions held in the session database. This value shrinks when the database rolls files off due to size constraints. After the service stops capturing data, the number is not reset.
Time Begin	Time when first packet was captured (time when the first packet was stored in the packet database). This time increases as packets are rolled out of the packet database.

Statistic	Description
Pool Packet Write	Number of packet pages currently in the PCS pipeline that need to be written to the database.
Time End	Time when the last packet was captured (time when packet was written to the database). The time increases as new packets are captured.
Pool Packet Assembler	Number of packet pages waiting to be assembled.
Assembler Packet Pages	Number of packet pages waiting to be assembled.
Pool Packet Capture	Number of packet pages available for capture.

Event Steam Analysis (ESA) Details View

The Event Stream Analysis Details view provides information for ESA. The following figure depicts the Event Stream Analysis Details.



For the related procedure, see Monitor Service Details.

This section displays the current generic statistics and Rule information for the service. It consists of **Rules**, **Monitor**, and Java Virtual Machine (**JVM**) tabs that show Event Stream Analysis rules and additional statistics.

Monitor tab

Displays the following generic statistical information for the Event Stream Analysis service:

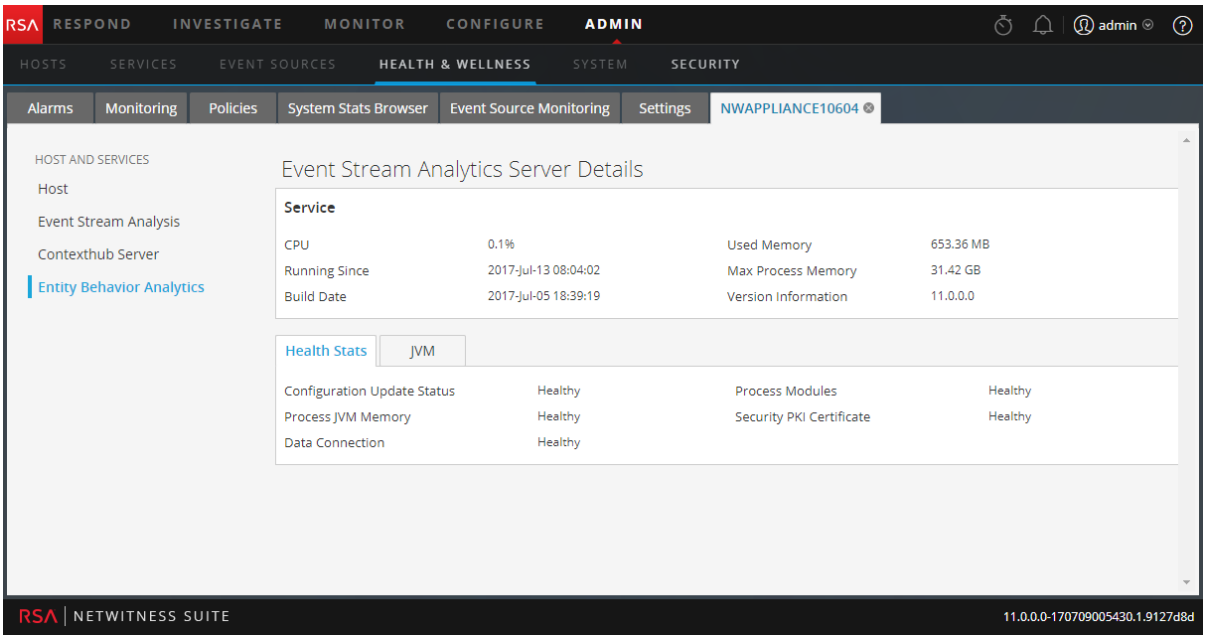
- Average number of bytes received per event message field.
- Average number of bytes received per event message.
- Total number of bytes of bytes received.
- Total number of fields received.
- Number of rules deployed on the ESA Service. The Sum of Enabled rules and Disabled rules should equal to Deployed
- Total number of events matched to all rules on the ESA service.
- Total number of events analyzed by the ESA Service since the last service start.
- Total number of alerts fired based on all the rules on the ESA service.
- Total dropped as late.
- Total fed on time.

- Total exit early.
- Seconds between feeds.
- Time span in window.
- Total events in window.
- Percent window consumed.
- Total source work units.
- Total bus dropped by payload.
- Total bus dropped events.
- Total bus dropped by fields.
- Total number of alerts sent to the message bus.
- Total number of bus events.
- Total number of Bus work units.
- Total endpoints detected.
- Total lost endpoints.
- Total failed client count.
- Total successful client count.
- Total successful server count.
- Minutes since last success.
- Number of times proxy was requested and granted.
- Total successful requests.
- Number of times proxy was requested and not granted.
- Total unsuccessful requests.

ESA Analytics Details View

The ESA Analytics Details view provides health status information about the selected ESA Analytics service. ESA Analytics services process the data for automated threat detection. It is important that you address any checked item that shows a status other than green (healthy), so that data processing is not interrupted and critical events are not missed.

The following figure shows the ESA Analytics Details view.



For the related procedure, see Monitor Service Details.

ESA Analytics Details

This section displays the current generic statistics for the selected ESA Analytics service.

Health Status

The Health Status section shows the health of the following items for the selected ESA Analytics service:

- Mongo
- JVM (Java Virtual Machine)
- Disk Space
- Suspicious Domains Module
- User Behavior Analytics Module

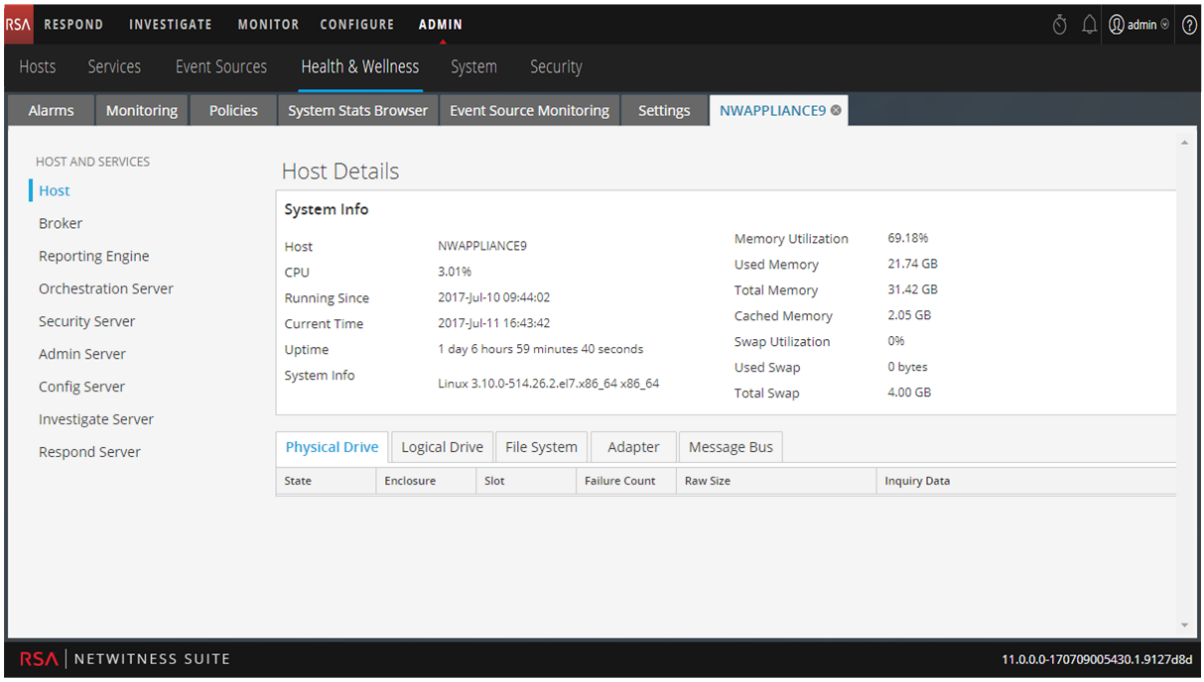
The following table describes the meaning of each health status.

Health Status	Description
Green	Healthy
Yellow	Unhealthy
Red	Critical and it needs immediate attention.

Health Status	Description
- -	Inapplicable

Host Details View

The Host Details view provides information about a host. The following figure depicts the Host Details.



The options panel on the left displays the host and the services installed on the host. You can click on Host any service to view the statistics and other pertinent information for that host or service.

The Details panel displays information that is specific to the host and provides additional information regarding the hardware of the host.

For the related procedure, see .Monitor Service Details

This section displays the current performance, capacity, and historical statistics for the host.

Parameter	Description
Host	Hostname.
CPU	Current CPU usage of the host.
Running Since	Time when the host was started.

Parameter	Description
Current Time	Current time on the host
Uptime	Time for which the host has been active.
System Info	OS version installed on the host.
Memory Utilization	Percentage of memory utilized by the host.
Used Memory	Memory used in GB.
Total Memory	Capacity of the memory installed on the system.
Cached Memory	Memory that is cached to disk in GB.
Swap Utilization	Percentage of system swap in use.
Used Swap	Swap used in GB.
Total Swap	Capacity of the swap installed on the system.

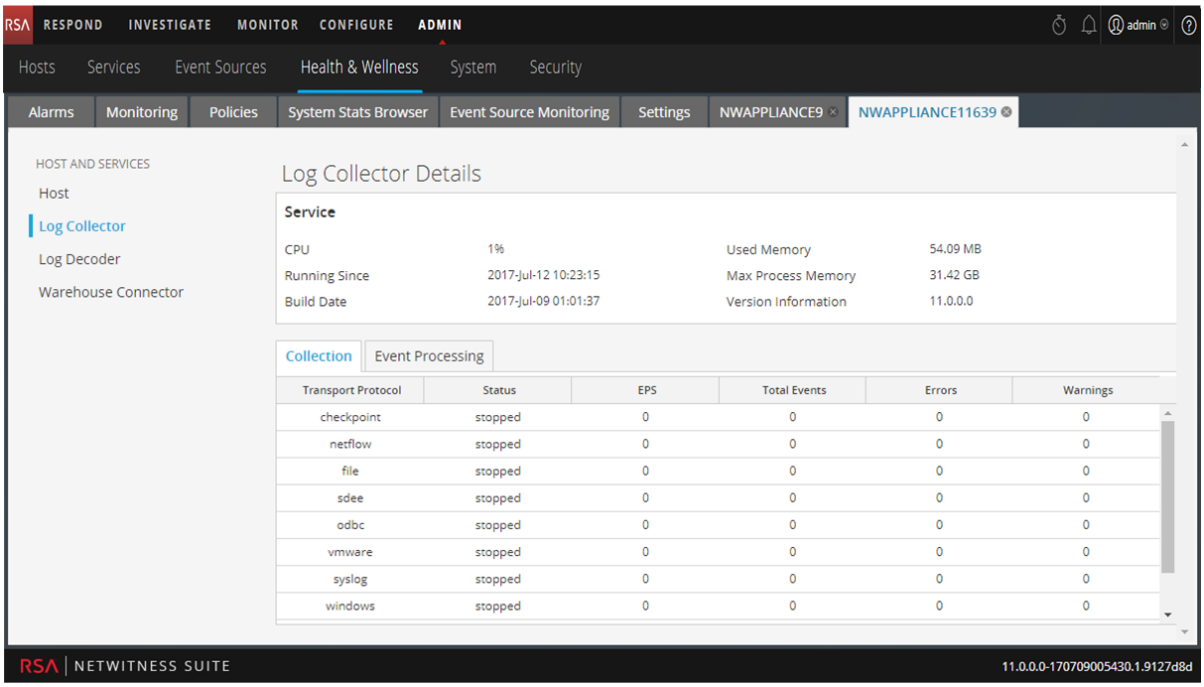
The lower section displays the current generic statistics for the host in the tabs described in the following table.

Tab	Description
Physical Drive	Type of physical drive, its usage and additional information of the physical drive on the host.
Logical Drive	Logical drive on the host.
File System	File system information, the size, current usage and available capacity on the host.
Adapter	Adapter used on the host.

Tab	Description
Message Bus	**Publish In Rate** - rate at which incoming messages are published to the message bus queue. **Total Messages Queued** - number of messages in the message queue. **Memory Used** - amount of memory used by the message bus (in bytes). **Disk Free** - free disk space available for the message bus (in bytes). **Memory Limit** - system memory limit. If the memory usage exceeds this value, this trips the **Memory Alarm** and Security Analytics stops accepting messages. **Disk Free Limit** - limit of free disk space available for the message bus. If the available disk space falls below this value, this trips the **Disk Free Alarm** and Security Analytics stops accepting messages. **Memory Limit Available** - Amount of memory available to this message broker (in bytes) before the **Memory Used Alarm** is tripped. **Disk Limit Available** - Amount of free disk space available to this message broker (in bytes) before the **Disk Free Limit** alarm is tripped. **Disk Free Alarm** - **True** or **False**. **True** indicates that the available disk space is below the value set in **Disk Free Limit** and Security Analytics has stopped accepting messages. **Memory Alarm** - **True** or **False**. **True** indicates that the available memory is below the value set in **Memory Limit** and Security Analytics has stopped accepting messages.

Log Collector Details View

The Log Collector Details view provides information for the Log Collector. The following figure depicts the Log Collector Details.



For the related procedure, see Monitor Service Details.

The lower section consists of the **Collection** and **Event Processing** tabs that display generic statistics for the service.

Collection Tab

Displays the event collection statistics for each Log Collection protocol you have implemented in NetWitness Suite (see "Log Collection Getting Started Guide" in the ***Log Collection Guides***).

Event Processing Tab

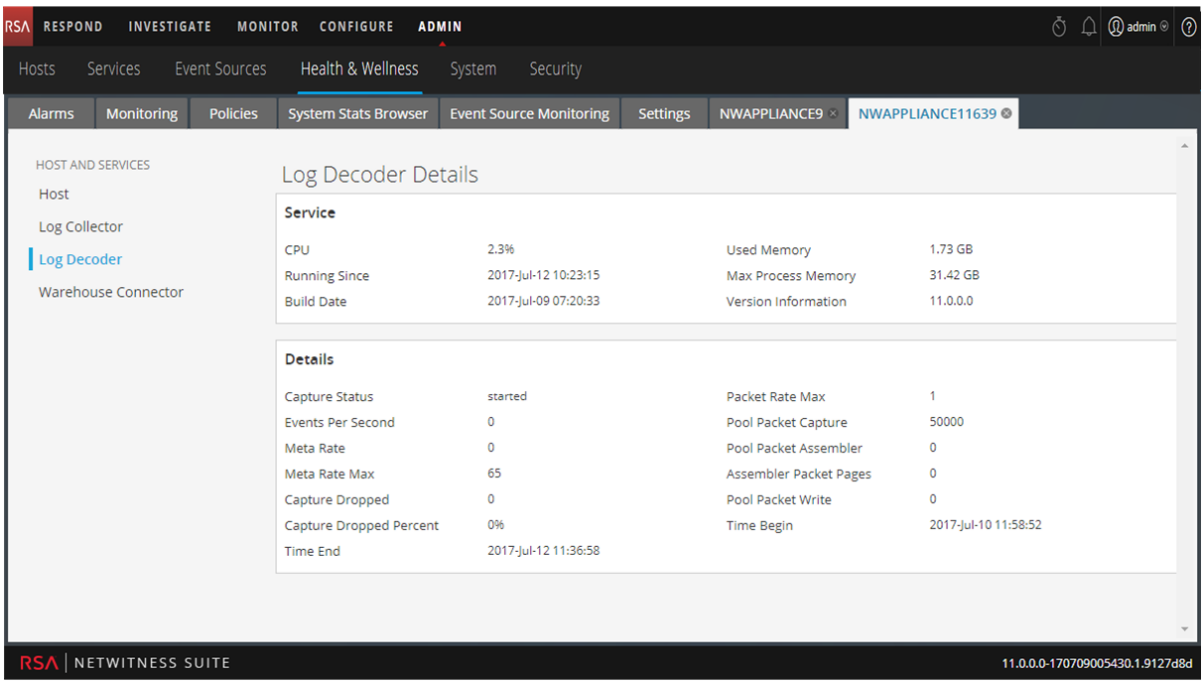
Displays statistics for the NetWitness Suite internal event processing protocol (that is, the Log Decoder) for Log Collection.

Parameter	Description
Transport Protocol	NetWitness Suite protocol use for Log Collections (that is, the Log Decoder).

Parameter	Description
Status	Status of the Log Decoder. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started** - Capturing data. • **stopping**- Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Decoder service.
EPS	Rate (events per second) at which this the Log Decoder is processing events from the Log Collector.
Total Events	Total events processed by the Log Decoder.
Errors	Number of errors encountered.
Warnings	Number of warnings encountered.
Byte Rate	Current throughput in bytes per second.

Log Decoder Details View

The Log Decoder Details view provides information for the Log Decoder. The following figure depicts the Log Decoder Details.



For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

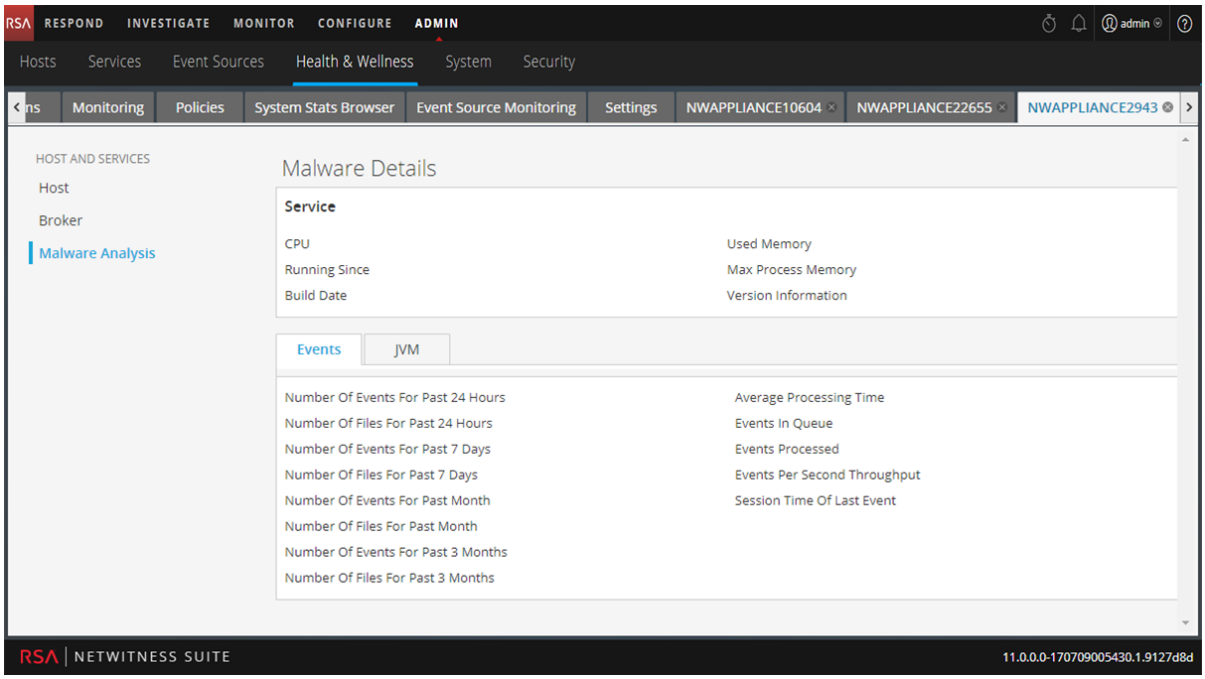
Statistic	Description
Capture Status	Status of data capture. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started** - Capturing data. • **stopping** - Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Log Decoder service.
Packet Rate Max	Maximum per second rate at which the service is writing packets to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate during data capture.
Events Per Second	Rate (events per second) at which the Log Decoder is processing events from the Log Collector.

Statistic	Description
Pool Packet Capture	Number of packet pages available for capture.
Meta Rate	Per second rate at which the service is writing metadata objects to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, rate is reset to zero.
Pool Packet Assembler	Number of packet pages waiting to be assembled.
Meta Rate Max	Maximum per second rate at which the service is writing metadata objects to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate reached during data capture.
Assembler Packet Pages	Number of packet pages waiting to be assembled.
Capture Dropped	Number of packets reported by the network card as dropped. After the service stops capturing data, rate is reset to zero.
Pool Packet Write	Number of packet pages in the PCS pipeline that need to be written to the database.
Capture Dropped Percent	Packets reported by the network card as dropped as a percentage.
Time Begin	Time when first packet was captured (time when the first packet was stored in the packet database). This time increases as packets are rolled out of the packet database.

Statistic	Description
Time End	Time when the last packet was captured (time when packet was written to the database). The time increases as new packets are captured.

Malware Details View

The Malware Details view provides information for Malware Analysis. The following figure depicts the Malware Details.



For the related procedure, see Monitor Service Details.

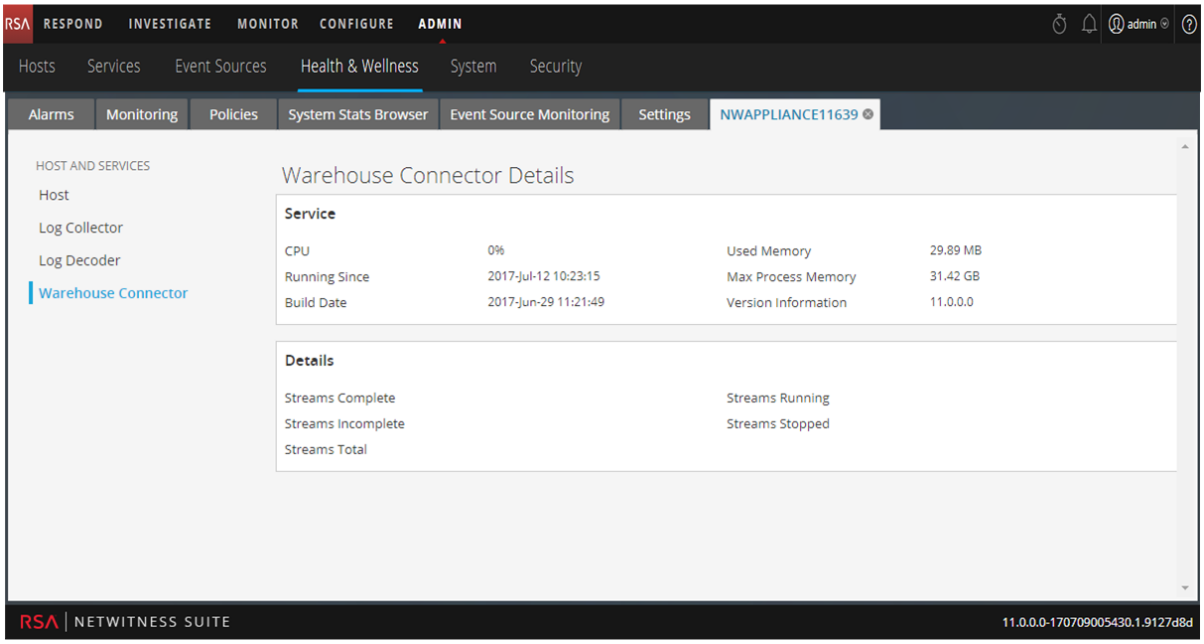
Displays the following event-related statistical information for the Malware Analysis service.

- Number of events for the past 24 hours
- Average processing time
- Number of files for the past 24 hours
- Events in queue
- Number of events for the past 7 days
- Events processed
- Number of events for the past 7 days
- Events per second throughput

- Number of events for the past month
- Session time of the last event
- Number of files for the past month
- Number of events for the past 3 months
- Number of files for the past 3 months

Warehouse Connector Details View

The Warehouse Connector Details tab provides information for the Warehouse Connector, such as the date it was built, CPU, and version information. The following figure depicts the Warehouse Connector Details.



For the related procedure, see Monitor Service Details.

Policies View

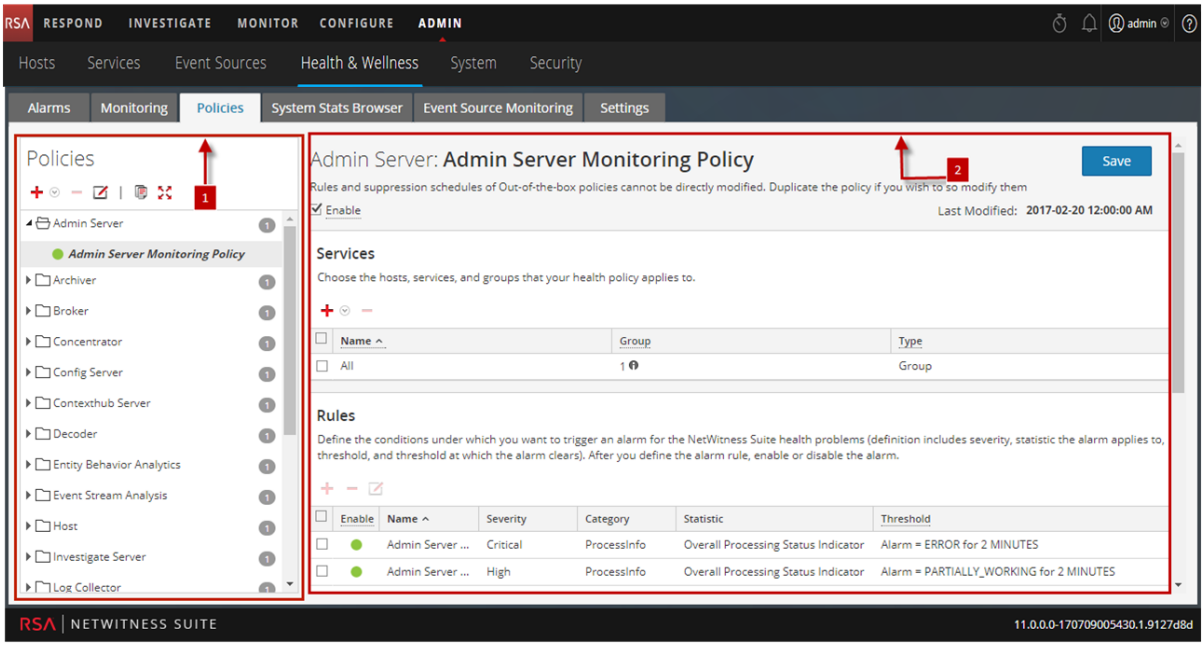
The required permission to access this view is **Manage services**.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the policies NetWitness Server and Services	Manage Policies
Administrator	Add, Edit, Duplicate, and Delete Policies	Manage Policies

Quick Look

The figure depicts the Policies view.



1 Policies Panel

2 Policy Detail Panel

1. Go to **ADMIN > Health & Wellness**.
2. Click the **Policies** tab.

Policies Panel

In the Policies panel, you can add or delete policies for hosts and services in this panel.

Feature	Description
	Displays available service types to create a new policy . Select one so that you can define a policy or policies for it.
	Deletes the selected policy from the Policies panel. You can only delete one policy at a time.
	Allows you to change the name of the policy.
	Creates a copy of the selected policy. For example, if you select **First Policy** and click , NetWitness Suite creates a copy of this policy and names it First Policy (1).
	Expands the list of policies under the services and hosts in the **Policies** panel.
	Contracts the list of policies under the services and hosts in the **Policies** panel.
	List of: • Services and hosts for which you have defined policies. • RSA standard policies that you can apply to hosts and services.

Policy Detail Panel

The **Policy Detail** panel displays the policy selected from the Policies panel.

Feature	Description
Save	Saves any changes you made in this panel.
Policy Type	Displays the type of policy you selected.
Modified Date	Displays the last date this policy was modified.
Enable	Select and deselect this checkbox to enable and disable the policy.
Services	

Feature	Description
	Displays menu in which you select: • **Groups** to display the **Groups** dialog from which you select service groups to this policy. • **Service/Host** to display the **Services/Hosts** dialog from which you select services to add to this policy. If policy type is **Host**, the menu will have **Host** not **Service**. You can select services based on policy type.
	Deletes the selected service or group from this policy.
Rules	
	Displays the Add Rule dialog in which you define a rule for this policy.
	Deletes the selected rule from this policy.
	Displays the Edit Rule dialog for the selected rule.
Policy Suppression	
	Adds a policy suppression timeframe row.
	Deletes the selected policy suppression timeframe row.
Time Zone	Selects the time zone for the Policy from the drop-down list. This time zone applies to both Policy Suppression and Rule Suppression.
	Selects the checkbox to select a policy suppression timeframe row.
Days	Days of the week that you want to suppress the policy according to the time range specified. Click on the day of the week that you want to suppress the policy. You can select any combination of days including all days.
Time Range	Time range during which the policy is suppressed for the days selected.
Notifications	

Feature	Description
+	Adds an EMAIL notification row.
−	Deletes the selected policy suppression timeframe row.
Notification Settings	Opens the Notification Servers view in which you can define the Email notification settings.
☐	Selecting the checkbox selects a policy suppression time frame row.
Output	The type of notification defined on the Global Notifications page. Can be email, SNMP, Syslog, or Script.
Recipient	The name of the person receiving the notification.
Notification Server	Select the EMAIL notification server. See "Configure Notification Servers" in the *System Configuration Guide* for the source of the values in this drop-down list.
Template	Select the Template for this EMAIL notification. RSA provides the Health & Wellness Default SMTP Template and the alarms template. See" Configure Notification Templates"in the *System Configuration Guide* for the source of the other values in this drop-down list. **Note:** Refer to Include the Default Email Subject Line if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Groups dialog

Feature	Description
Groups panel	
Name	Displays the service groups you have defined. You can select: • **All** to display all your services in the **Services** panel. • A group to display the services in comprise that group in the **Services** panel.
Services panel	

Feature	Description
Name	Displays the name of the service.
Host	Displays the host on which the service is running.
Type	Displays the type of service.

Rules Dialog

Feature	Description
☐ Enable	Select and deselect this checkbox to enable and disable the rule for this policy.
Name	Enter the name of the rule.
Description	Enter the description of the rule. RSA suggests that you include the following information in this field. • Informational description - purpose of the rule and what problem it monitors. • Remediation - steps to take to resolve the condition that triggers the alarm for this rule.
Severity	Select the severity of the rule. Valid values are: • Critical • High • Medium • Low

Feature	Description
Statistic	Select the statistics you want to check with this rule. You can select: • Statistical category from the left drop-down list. • Statistic from the right drop-down list. **Note:** For Public Key Infrastructure (PKI) policy, select PKI in the category and statistics as any one of the following: - NetWitness Server PKI Certificate Expiration - Displays the time left before the certificate expires. - NetWitness Server PKI CRL Expiration - Displays the time left before the Certificate Revocation List (CRL) expires. - NetWitness Server PKI CRL Status - Displays the current status of the CRL. Please refer to the System Stats Browser View for examples of the statistics you may want to check with a rule.
Alarm Threshold	Define the threshold of the rule that will trigger the policy alarm: • Amount **Note:** For CRL expiry the supported format is ddddhhmm, for example: - 10000 represent 1 day - 2359 represent 23 hours and 59 minutes - 10023 represent 1 day and 23 minutes - 3650100 represent 365 days and 1 hour • Time in minutes

Recovery	Defines when to clear the threshold of the rule:
	• Operator:
	  • For NetWitness Suite 10.5 (=, !=, <, <=, >, or >=)
	  • For NetWitness Suite 10.5.0.1 and later (See Threshold Operators below)
	• Amount
	• Time in minutes

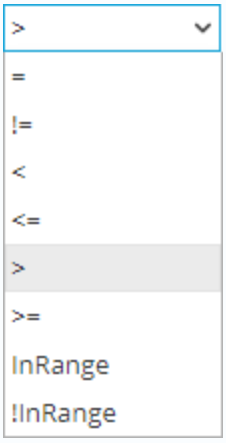
Rule Suppression	
+	Selecting this option allows you to add a rule suppression timeframe row.

Feature	Description
−	Selecting this option allows you to delete the selected rule suppression time frame row.
☐	Selecting the checkbox allows you to select a rule suppression time frame row.
Time Zone: *time-zone*	Displays the Policy time zone. You select the time zone for a policy in the Policy Suppression panel.
Days	Days of the week that you want to suppress the rule according to the time range specified. Click on the day of the week that you want to suppress the rule. You can select any combination of days including all days.
Time Range	Time range during which the rule is suppressed for the days selected.

Threshold Operators

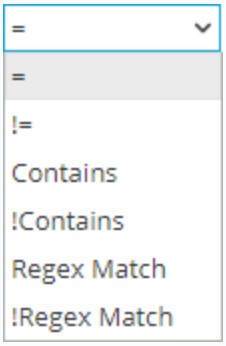
The **Alarm Threshold** and **Recovery Threshold** fields in the **Rules** dialog prompt you for either numeric or string operators based on the statistic criteria you specify.

Numeric operators drop-down menu:



=
!=
<
<=
>
>=
InRange
!InRange

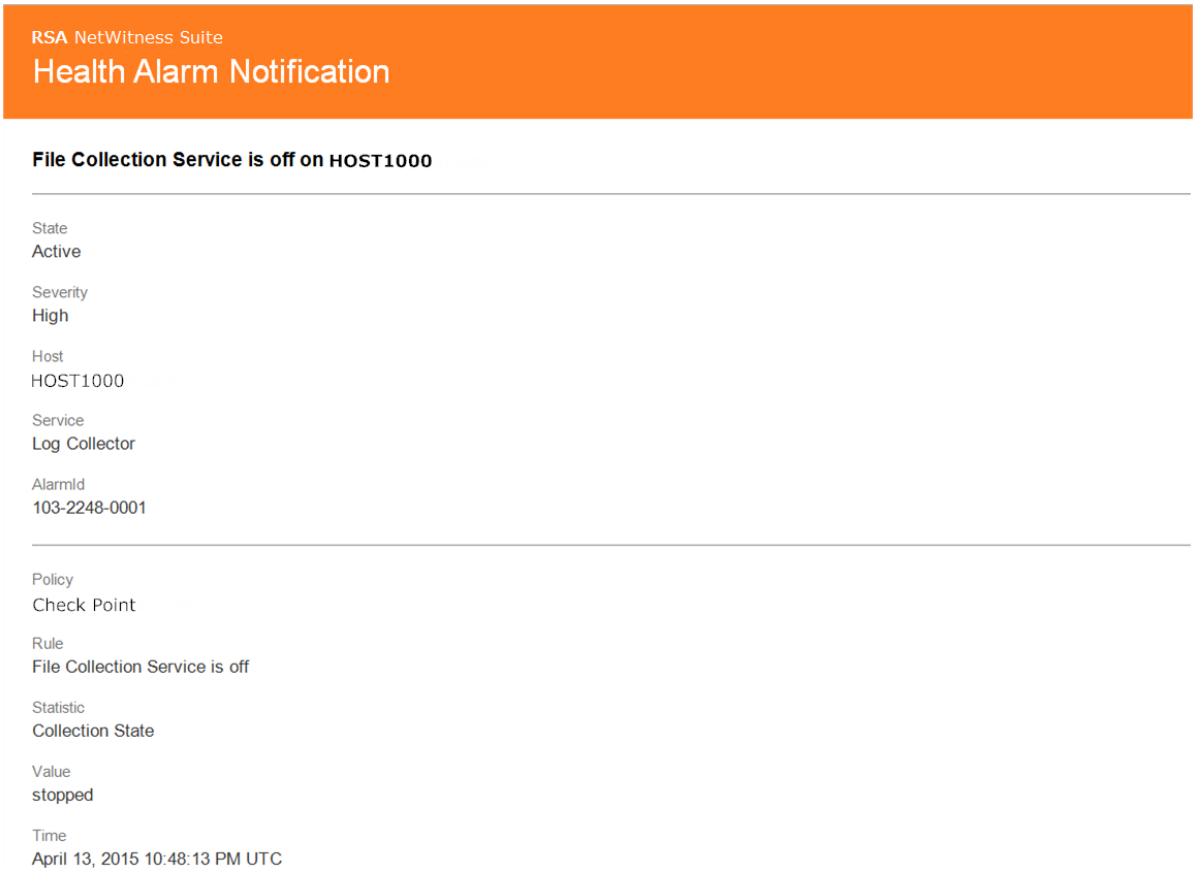
String operators drop-down menu:



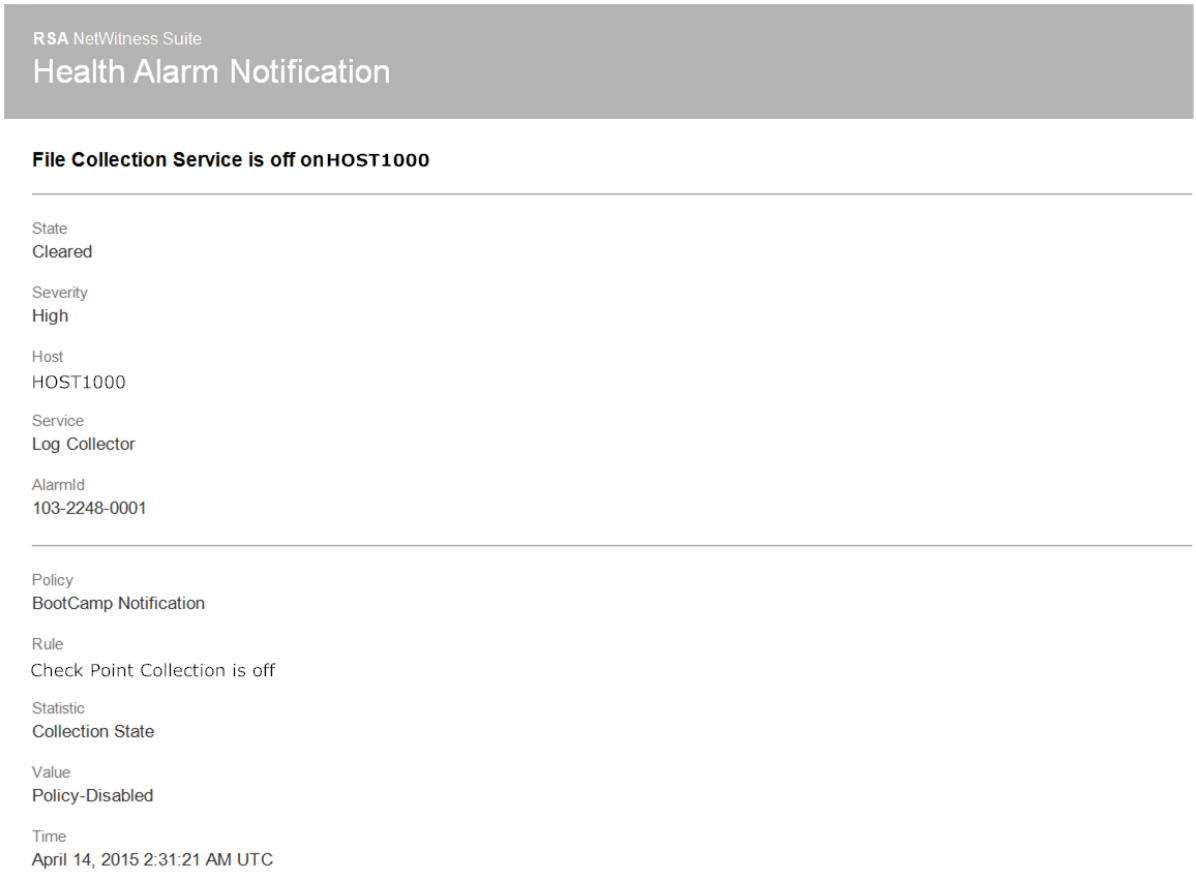
RSA Health & Wellness Email Templates

Note: Please refer to Include the Default Email Subject Line if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Health & Wellness Default SMTP Template



Alarms Template



NetWitness Suite Out-of-the-Box Policies

The following table lists the NetWitness Suite Out-of-the-Box Policies with the rules defined for each policy.

You can perform the following tasks on any of these policies:

- Change service/group assignments.
- Disable/enable them.

You cannot perform the following tasks on any of these policies:

- Delete them.
- Edit Policy names.

Note: Additional information about the Out-of-the-Box Policies can be found in the User Interface under
Health & Wellness – Policies.

Policy Name	Rule Name	Alarm Triggered
	Communication Failure Between Master Security Analytics Host and a Remote Host	Host is down, Network is down, Message Broker is Down, or Invalid or missing security certificates for 10 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Server Monitoring Policy	Critical Usage on Rabbitmq Message Broker Filesystem	For `var/lib/rabbitmq`, Mounted Filesystem Disk Usage goes over 75%.
	Filesystem is Full	Overall Mounted Filesystem Disk Usage reaches 100%.
	High Filesystem Usage	Overall Mounted Filesystem Disk Usage goes over 95%.
	High System Swap Utilization	Swap Utilization goes under 5 % for 5 minutes or more.
	High Usage on Rabbitmq Message Broker Filesystem	Mounted Filesystem Disk Usage for `var/lib/rabbitmq` goes over 60%.
	Host Unreachable	Host down.
	LogCollector Event Processor Exchange Bindings Status	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Bindings	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Consumers	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	Power Supply Failure	Host not receiving power.
	RAID Logical Drive Degraded	For Raid Logical Drive, Drive State equals Degraded or Partially Degraded.

Policy Name	Rule Name	Alarm Triggered
	RAID Logical Drive Failed	For Raid Logical Drive, Logical Drive State equals Offline, Failed, or Unknown.
	RAID Logical Drive Rebuilding	For Raid Logical Drive, Logical Drive State equals Rebuild.
	RAID Physical Drive Failed	For Raid Physical Drive, Physical Drive State does not equal Online, Online Spun Up, or Hotspare.
	RAID Physical Drive Failure Predicted	For Raid Physical Drive, Physical Drive Predictive Failure Count is greater than 1.
	RAID Physical Drive Rebuilding	For Raid Physical Drive, Physical Drive State equals Rebuild.
	RAID Physical Drive Unconfigured	For Raid Physical Drive, Physical Drive State contains Unconfigured(good).
	SD Card Failure	SD Card Status does not equal ok.
NetWitness Suite Archiver Monitoring Policy	Archiver Aggregation Stopped	Archiver Status does not equal started.
	Archiver Database(s) Not Open	Database Status does not equal opened.
	Archiver Not Consuming From Service	Devices Status does not equal consuming.
	Archiver Service in Bad State	Service State does not equal started or ready.
	Archiver Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Broker Monitoring Policy	Broker >5 Pending Queries	Queries Pending greater than or equal to 5 for 10 minutes or more.
	Broker Aggregation Stopped	Broker Status does not equal started.
	Broker Not Consuming From Service	Devices Status does not equal consuming.
	Broker Service in Bad State	Service State does not equal started or ready.
	Broker Service Stopped	Server Status does not equal started.
	Broker Session Rate Zero	Session Rate (current) equals 0 for 2 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Concentrator Monitoring Policy	Concentrator >5 Pending Queries	Queries Pending greater than or equal to 5 for 10 minutes or more.
	Concentrator Aggregation Behind >100K Sessions	Devices Sessions Behind is greater than or equal to 100000 for 1 minute or more.
	Concentrator Aggregation Behind >1M Sessions	Devices Sessions Behind is greater than or equal to 1000000 for 1 minute or more.
	Concentrator Aggregation Behind >50M Sessions	Devices Sessions Behind is greater than or equal to 50000000 for 1 minute or more.
	Concentrator Aggregation Stopped	Broker Status does not equal started.
	Concentrator Database(s) Not Open	Database Status does not equal opened.
	Concentrator Meta Rate Zero	Concentrator Meta Rate (current) equals 0 for 2 minutes or more.
	Concentrator Not Consuming From Service	Devices Status does not equal consuming.
	Concentrator Service in Bad State	Service State does not equal started or ready.
	Concentrator Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Decoder Monitoring Policy	Decoder Capture Not Started	Capture Status does not equal started.
	Decoder Capture Rate Zero	Capture Rate (current) equals 0 for 2 minutes or more.
	Decoder Database Not Open	Database Status does not equal opened.
	Decoder Dropping >1% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 1%.
	Decoder Dropping >10% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 10%.
	Decoder Dropping >5% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 5%.
	Decoder Packet Capture Pool Depleted	Packet Capture Queue equals 0 for 2 minutes or more.
	Decoder Service in Bad State	Service State does not equal started or ready.
	Decoder Service Stopped	Server Status does not equal started.
NetWitness Suite Event Steam Analysis Monitoring Policy	ESA Overall Memory Utilization > 85%	Total ESA Memory Usage % is greater than or equal to 85 %.
	ESA Overall Memory Utilization > 95%	Total ESA Memory Usage % is greater than or equal to 95 %.
	ESA Service Stopped	Server Status does not equal started.
	ESA Trial Rules Disabled	Trial Rules Status does not equal enabled.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite IPDB Extractor Monitoring Policy	IPDB Extractor Service in Bad State	Service State does not equal started or ready.
	IPDB Extractor Service Stopped	Server Status does not equal started.
NetWitness Suite Incident Management Monitoring Policy	Incident Management Service Stopped	Server Status does not equal started.
NetWitness Suite Log Collector Monitoring Policy	Log Collector Service Stopped	Server Status does not equal started.
	Log Decoder Event Queue > 50% Full	Number of events currently in the queue is using 50% or more of the queue.
	Log Decoder Event Queue > 80% Full	Number of events currently in the queue is using 80% or more of the queue.
	Log Collector Service in Bad State	Service State does not equal started or ready.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Log Decoder Monitoring Policy	Decoder Dropping>10% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 10%
	Log Capture Not Started	Capture Status does not equal started.
	Log Decoder Capture Rate Zero	Capture Rate (current) equals 0 for 2 minutes or more.
	Log Decoder Database Not Open	Database Status does not equal opened.
	Log Decoder Dropping >1% of Logs	Capture Packets Percent Dropped (current) is greater than or equal to 1%.
	Log Decoder Dropping >5% of Logs	Capture Packets Percent Dropped (current) is greater than or equal to 5%.
	Log Decoder Packet Capture Pool Depleted	Packet Capture Queue equals 0 for 2 minutes or more.
	Log Decoder Service Stopped	Server Status does not equal started.
	Log Decoder Service in Bad State	Service State does not equal started or ready.
NetWitness Suite Malware Analysis Monitoring Policy	Malware Analysis Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Reporting Engine Monitoring Policy	Reporting Engine Alerts Critical Utilization	Alerts Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Available Disk <10%	Available disk space is less than 10%.
	Reporting Engine Available Disk <5%	Available disk space is less than or equal to 5%.
	Reporting Engine Charts Critical Utilization	Charts Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Rules Critical Utilization	Rules Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Schedule Task Pool Critical Utilization	Schedule Task Pool Utilization is greater than or equal to 10 for 15 minutes or more.
	Reporting Engine Service Stopped	Server Status does not equal started.
	Reporting Engine Shared Task Critical Utilization	Shared Task Pool Utilization is greater than or equal to 10 for 5 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Warehouse Connector Monitoring Policy	Warehouse Connector Service in Bad State	Service State does not equal started or ready.
	Warehouse Connector Service Stopped	Server Status does not equal started.
	Warehouse Connector Stream Behind	Stream Behind is greater than or equal to 2000000.
	Warehouse Connector Stream Disk Utilization > 75%	Stream Disk Usage (Pending Destination Load) is greater than or equal to 75.
	Warehouse Connector Stream in Bad State	Stream Status does not equal consuming or online for 10 minutes r more.
	Warehouse Connector Stream Permanently Rejected Files > 300	Number of files in the permanently rejected files is greater than or equal to 300.
	Warehouse Connector Stream Permanently Rejected Folder > 75% Full	Rejected folder usage is greater than or equal to 75%.
NetWitness Suite Workbench Monitoring Policy	Workbench Service in Bad State	Service State does not equal started or ready.
	Workbench Service Stopped	Server Status does not equal started.

System Stats Browser View

NetWitness Suite provides a way to monitor the status and operations of hosts and services. The System Stats Browser tab displays key statistics, service system information, and host system information for a host or service.

You can customize the stats view depending on the parameter you select to filter the data.

To access the System Stats Browser view:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Click the **System Stats Browser** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the System Stat Historical Graph	Historical Graph for System Stats

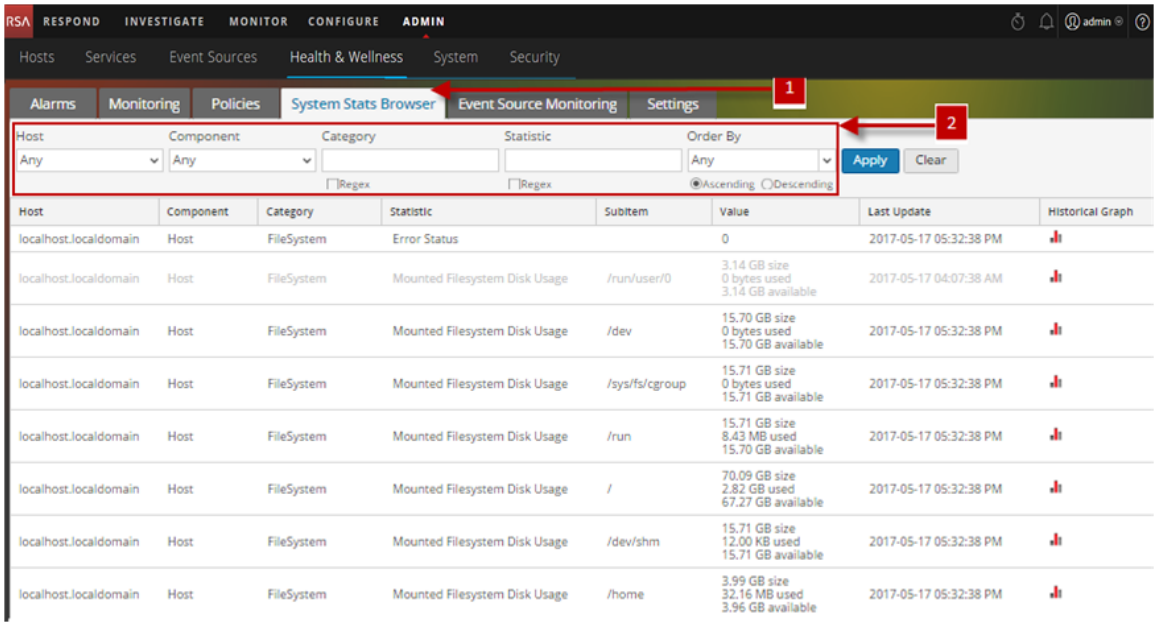
Related Topics

Monitor Service Statistics

Filter System Statistics

Quick Look

The System Stats Browser view is displayed.



1 Displays System Stats Browser View

2 Toolbar used to filter and customize the System Stats Browser View

Note: Historical graphs are enabled, and can be displayed, for statistics with numeric values. However, historical graphs are disabled for statistics with string values, for example, Health checks (Healthy), and are displayed as gray in the UI.

Filters

This table lists the various parameters you can use to filter and customize the System Stats view.

Parameter	Description
Host	Select a host from the drop-down menu to display the stats of the selected host. Select **Any** to list all the available hosts.
Component	Select a component from the drop-down menu to display the stats for the selected component. Select **Any** to list out all the components on a selected host.
Category	Type the category to display the stats for the required category. Select Regex to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Statistic	Type the statistic to display the required statistic on all the hosts or components. Select Regex to enable Regex filter. This performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Order By	Select the order in which the list needs to be filtered. Select Ascending to filter the list it in an ascending order.

Commands

Command	Action
Apply	Click to apply the filters chosen and display the list accordingly.

Command	Action
Clear	Click to clear the chosen filters.

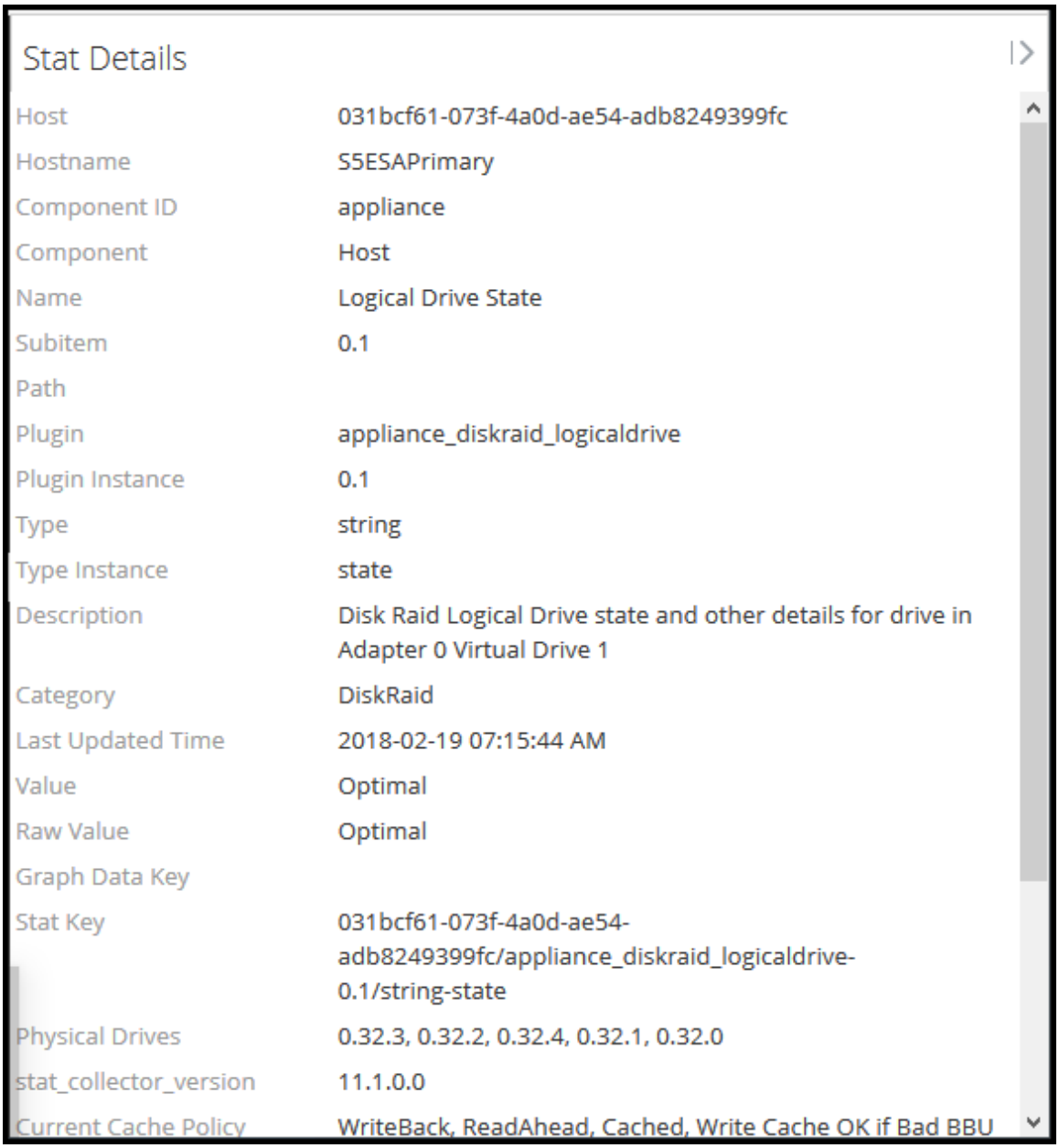
System Stats View Display

Displays statistics, service system information, and host system information for a host or service.

Access Stats Details

Select one of the stats and click **Stats Details** on the right hand side of the panel.

The Stats details panel opens with details of the selected stats.


Stat Details
Host
031bcf61-073f-4a0d-ae54-adb8249399fc
Hostname
S5ESAPrimary
Component ID
appliance
Component
Host
Name
Logical Drive State
Subitem
0.1
Path
Plugin
appliance_diskraid_logicaldrive
Plugin Instance
0.1
Type
string
Type Instance
state
Description
Disk Raid Logical Drive state and other details for drive in Adapter 0 Virtual Drive 1
Category
DiskRaid
Last Updated Time
2018-02-19 07:15:44 AM
Value
Optimal
Raw Value
Optimal
Graph Data Key
Stat Key
031bcf61-073f-4a0d-ae54-adb8249399fc/appliance_diskraid_logicaldrive-0.1/string-state
Physical Drives
0.32.3, 0.32.2, 0.32.4, 0.32.1, 0.32.0
stat_collector_version
11.1.0.0
Current Cache Policy
WriteBack, ReadAhead, Cached, Write Cache OK if Bad BBU

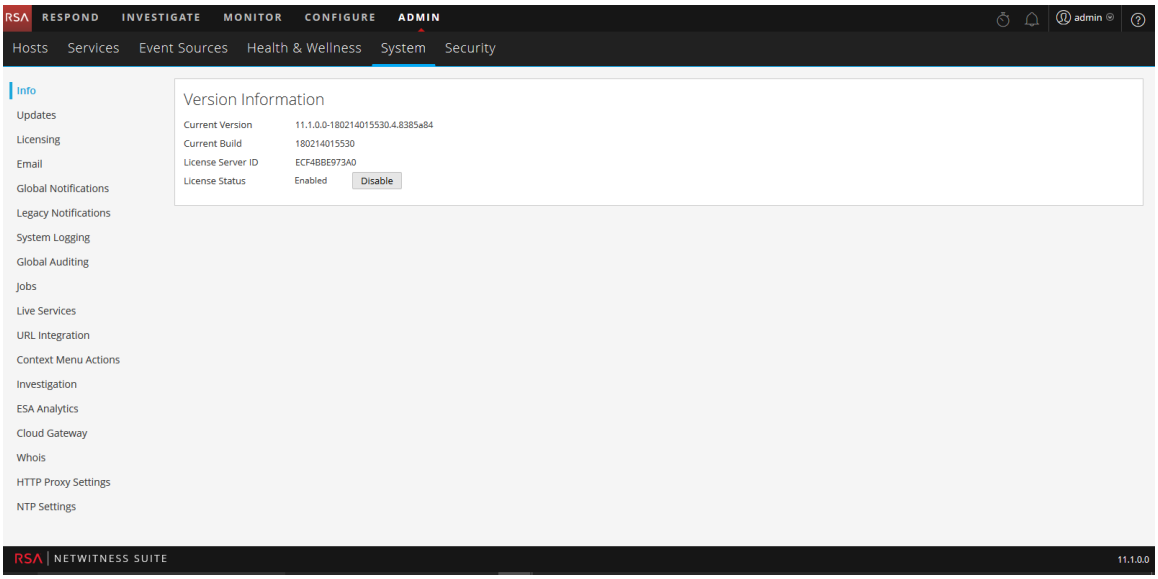
System View - System Info Panel

This topic describes the System Information panel, which displays information about the system version and license status.

The required role to access this view is **Manage System Settings**.

To access this view, do one of the following:

- Go to **ADMIN > System**.
  The System Information panel is displayed by default.
- When you receive a notification that a new version of NetWitness Suite is available in the Notifications tray, click **View**.



The Version Information section displays version information about the version of NetWitness Suite that is currently installed. The following table describes the features of the Version Information section.

Name	Description
Current Version	Displays the version of Security Analytics that is currently running. The format of the version is *major-relase.minor-release.stability-id.build-number*. Possible values for the *stability-id* are: • 1 - Development • 2 - Alpha • 3 - Beta • 4 - RC • 5 - Gold
Current Build	Identifies the current build revision for use in troubleshooting situations.
License Server ID	Each client host is shipped with the Local Licensing Server (LLS) installed to manage host licenses. This field indicates whether the LLS is installed for this instance of Security Analytics. • When the LLS is installed, the Licensing Server ID is displayed. • **Unknown** indicates that the LLS is not installed.
License Status	Indicates whether or not the license is enabled. If the license is: • Enabled, **Enabled** is displayed in this field and there is a **Disable** button to the right so you can disable it. • Disabled, **Disabled** is displayed in this field and there is an **Enable** button to the right so you can enable it.

System Updates Panel - Settings Tab

System Updates Settings tab describes the interface you use to set up a connection to Live Update Repository. These settings ensure that the NetWitness Suite can reach the Live Update Repository and synchronize it with your Local Update Repository.

The required permission to access this view is **Apply System Updates**.

To access this view:

1. Go to **ADMIN > System**.
2. Select **Updates**.

What do you want to do?

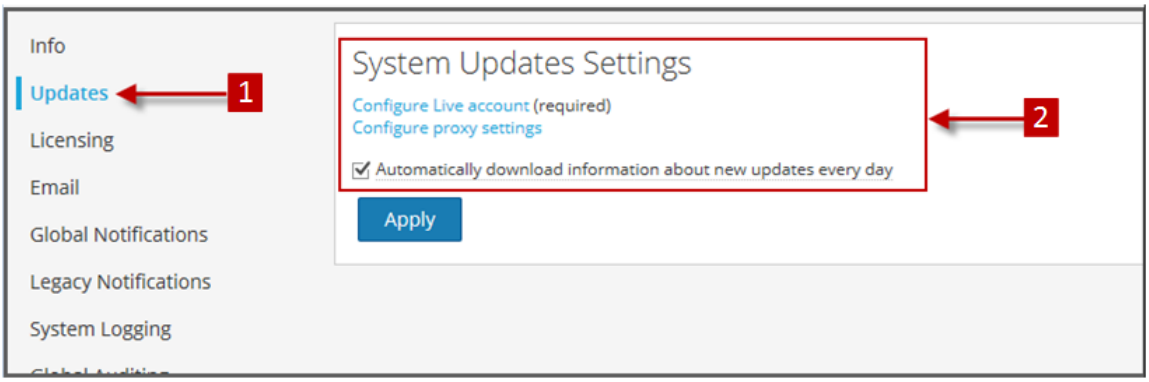
Role	I want to ...	Show me how
Administrator	Automatically download updates	Enable automatic synchronization with the RSA update repository.

Related Topics

Managing NetWitness Suite Updates

Quick Look

The System Updates Settings panel is displayed.



1 Displays System Update Setting Tab

2 Configure Account and Setting for Automatic Updates

Features

This table describes the features in the System Updates Settings panel.

Feature	Description
Configure Live account	Displays the **ADMIN** > **System** > **Live Services** panel in which you can configure your Live Account credentials if they are not configured.
Configure proxy settings	Displays the **ADMIN** > **System** > **HTTP Proxy Settings** panel in which you can configure an HTTP proxy if it is not configured.
Automatically download information about new updates every day	Select to enable automatic synchronization with the RSA update repository. If there are new updates available, information will automatically be displayed in the **ADMIN** > **HOSTS** panel.
Apply	Applies the settings in this tab.

System Logging - Settings View

The RSA NetWitness SuiteSettings view in the System Logging panel configures the size of the log files, the number of backup log files maintained, as well as the default logging levels for the packages within NetWitness Suite. The **Configure Log File Settings** topic in the *System Configuration Guide* provides detailed procedures.

To access the Settings tab:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.
   The System Logging panel opens to the Realtime tab by default.
3. Click the **Settings** tab.

What do you want to do?

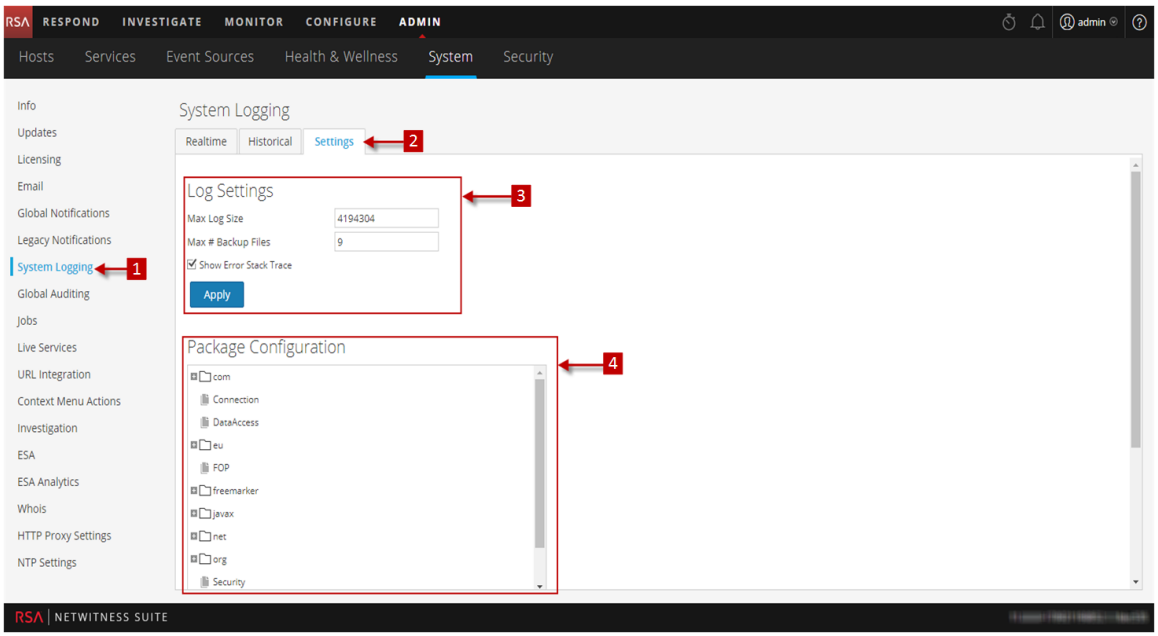
Role	I want to ...	Show me how
Administrator	Configure the size of the Log files	Setup the Log Settings Toolbar

Related Topics

System Logging - Historical Tab

System Logging - Realtime Tab

Quick Look



1	Displays System Logging Panel
2	Displays Settings Tab
3	The section allows the user to configure Log Settings
4	The section allows the user to configure Package

Features

The **Settings** tab has two sections: Log Settings and Package Configuration.

Log Settings

The Log Settings section configures the size of the NetWitness Suite log files and the number of backup logs that NetWitness Suite maintains.

Feature	Description
Max Log Size	Configures the maximum size in bytes of each log file. The minimum value for this setting is **4096**.

Feature	Description
Max # Backup Files	Specifies how many backup log files are maintained. The minimum value for this setting is **0**. When the maximum number of log files is attained, and a new backup file is made, the oldest backup is discarded.
Show Error Stack Trace	Select checkbox to display ERROR, STACK, and TRACE log messages.
Apply	Puts the settings into effect immediately for all future logs.

Package Configuration

The Package Configuration section shows the NetWitness Suite packages in a tree structure.

Feature	Description
Package tree	The tree contains all the packages used within NetWitness Suite. You can drill down into the tree to view the log levels of each package. The **root** logging level represents the default log level for all packages that are not explicitly set. The root level is set to **INFO**
Package field	This field is populated with the name of the selected package when you select a package in the **Package** tree.
Log Level	If the selected package has a log level explicitly set, the value is displayed in the **Log Level** field.
Reset recursively	Select checkbox to reset the log recursively.
Apply	This button puts the settings into effect immediately for all future logs.
Reset	This button resets the selected package to the log level of **root**.

System Logging - Realtime Tab

This topic describes the features of the System Logging > Realtime tab and the Services Logs view > Realtime tab.

The **Realtime** tab is a view of the NetWitness Suitelog or a service log. When it is initially loaded, the view contains the last 10 log entries. As new entries become available, the view is updated with those entries.

To access the Realtime tab:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.
   The System Logging panel opens to the **Realtime** tab by default.

What do you want to do?

Role	I want to ...	Show me how
Administrator	See details of Log entry	Displaying System and Service Logs

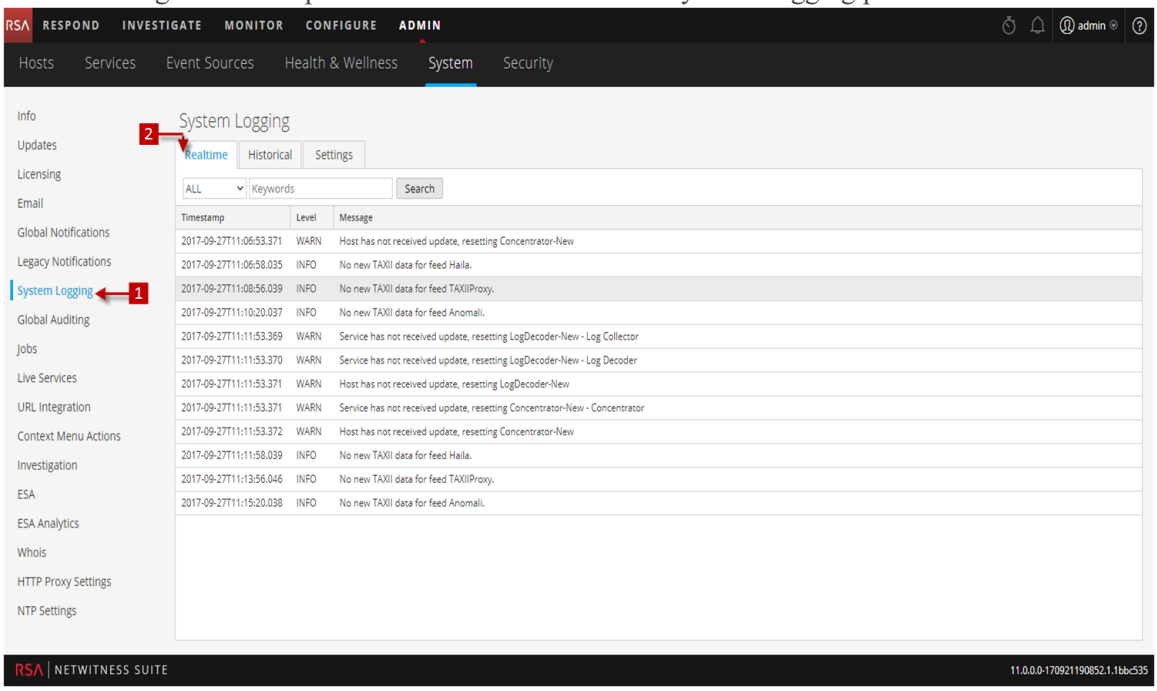
Related Topics

System Logging - Settings View

System Logging - Historical Tab

Quick Look

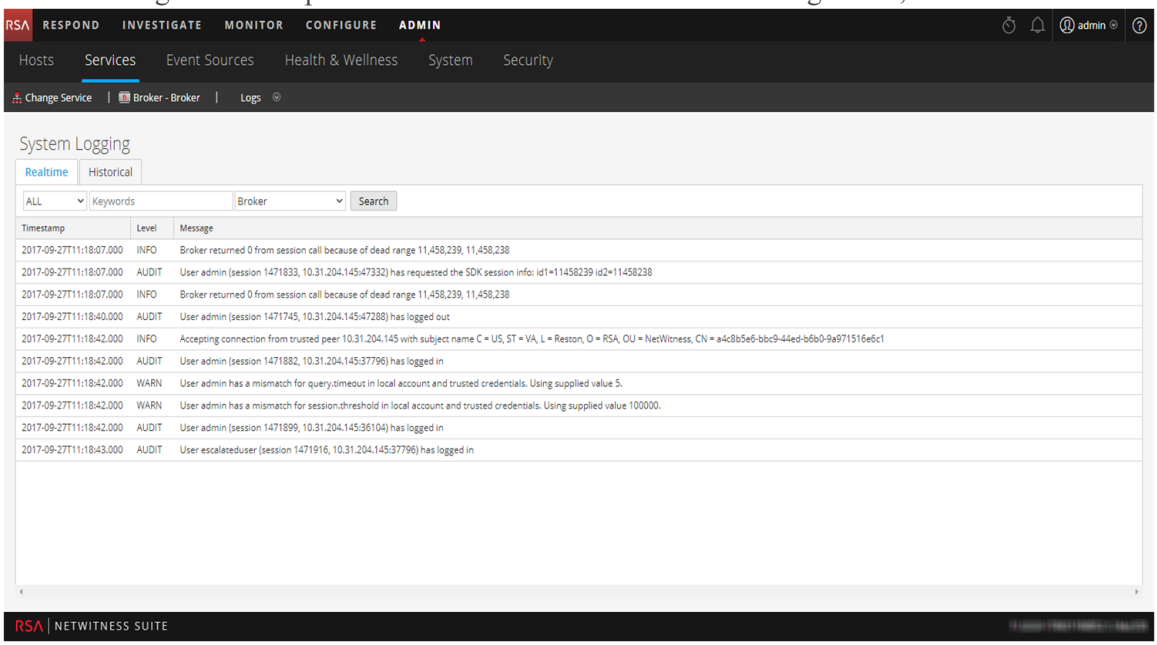
The following is an example of the **Realtime** tab in the System Logging panel.



1 Displays System Logging Panel

2 Displays Realtime Tab

The following is an example of the **Realtime** tab in the Services Logs view, which is similar.



Features

The **Realtime** tab has a toolbar with input fields to allow filtering of the entries, and below the toolbar is a grid containing the log entries.

Toolbar

Feature	Description
Log Level drop-down	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.
Keywords field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Filter button	Click to activate filtering based on the log level, keyword, and service selections.

Log Grid Columns

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

System Logging - Historical Tab

The Historical tab provides a searchable view of the NetWitness Suite log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the system.

To access the Historical tab:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the **Realtime** tab by default.
3. Click the **Historical** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the Historical Graph	Historical Graph for System Stats

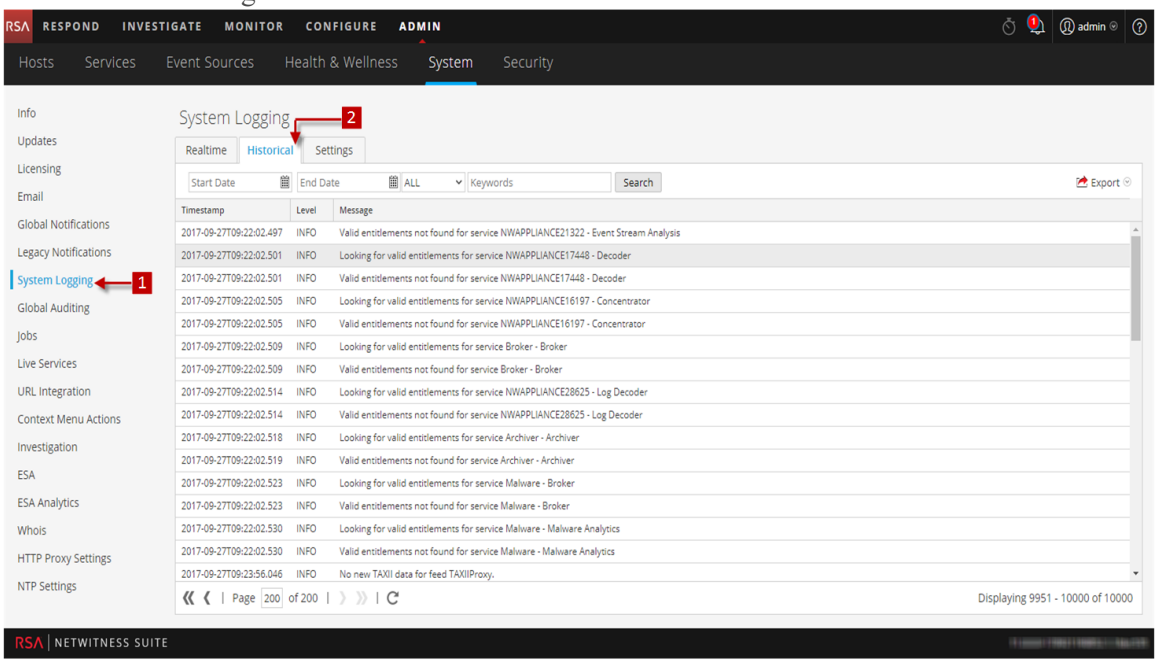
Related Topics

System Logging - Realtime Tab

System Logging - Settings View

Quick Look

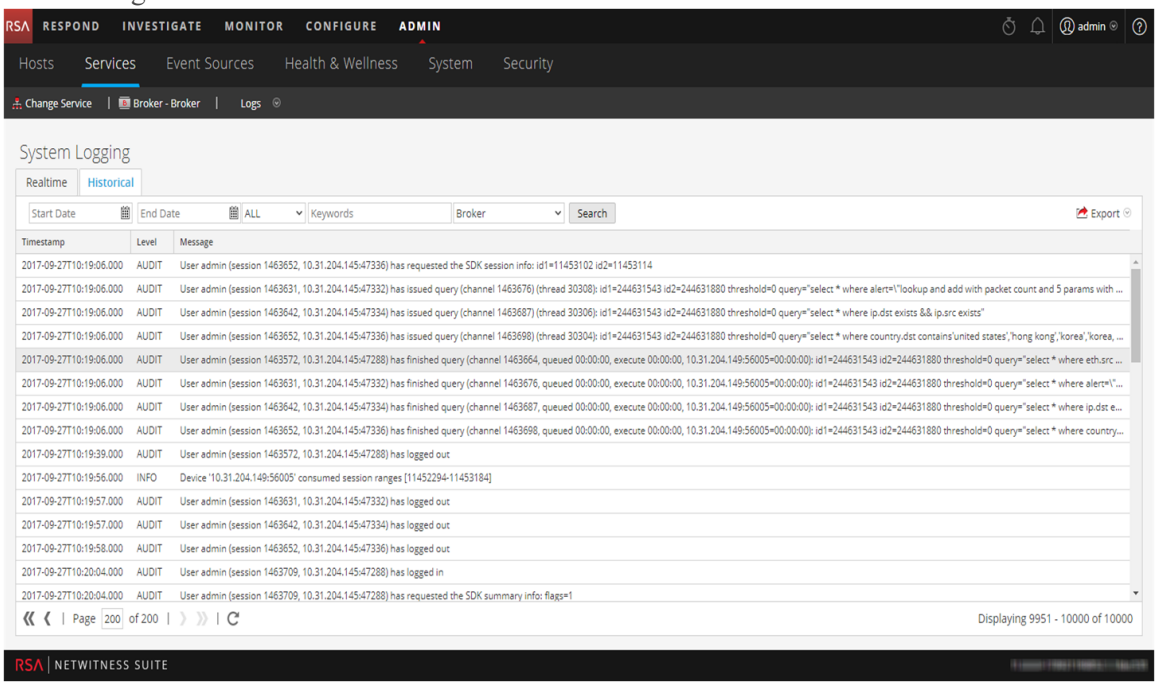
The following is an example of the **Historical** tab in the System Logging panel. It shows the NetWitness Suite logs.



1 Displays System Logging Tab

2 Displays Historical Tab

The following is an example of the **Historical** tab in the Services Logs view. It shows the services logs.



Features

The **Historical** tab has a toolbar with input fields to allow filtering of the entries, a grid containing the log entries, and paging tools.

Feature	Description
Start Date and **End Date**	The **Start Date** and **End Date** range search options limit the log entries to a point in time. When used, you must provide both a start and end date. The times are optional. The date range is validated to assure that the end date is not before the start date.
Log Level drop-down	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.
Keyword field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Search button	Click to activate a search based on the start and end date, log level, keyword, and service selections.
Export	Click to export the currently viewed grid entries to a text file. You can select either comma-separated or tab-separated format for the entries in the file.

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

The paging tools below the grid provide a way to navigate through the pages of log entries.

Search Log Entries

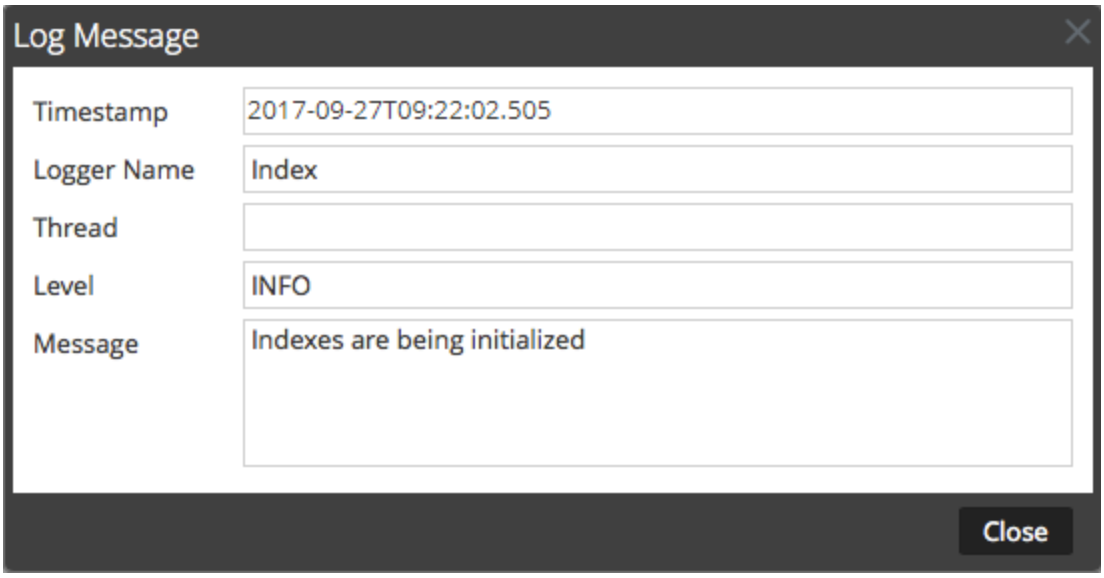
To search the results shown in the **Historical** tab:

1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both.
3. (Optional) For service logs, select the **Service**: host or service.
4. Click **Search**.
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the **Historical** tab Log grid provides the summary information of a log entry. To view complete details:

1. Double-click a log entry.
   The Log Message dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



2. When finished viewing, click **Close**.

Page Through the Entries

To view the different pages of the grid, use the paging controls on the bottom of the grid as follows:

- Use the navigation buttons
- Manually enter the page you want to view, and press **ENTER**.

Export

To export the logs in the current view:

Click **Export**, and select one of the drop-down options, **CSV Format** or **Tab Delimited**.
The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a NetWitness Suite system log exported with comma-separated values is named **UAP_log_export_CSV.txt**, and an appliance log exported with tab-separated values is named **APPLIANCE_log_export_TAB.txt**.

RSA NETWITNESS® SUITE

System Security and User Management Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

System Security and User Management **7**

Set Up System Security **9**

Step 1. Configure Password Complexity 10

Password Strength 10

Configure Password Strength 11

Step 2. Change the Default Admin Passwords 14

Best Practices 14

Change the admin Password for the NetWitness Suite 14

Change the admin Password for Core Services 14

Remove and re-add a Data Source on the Reporting Engine 15

Change the admin Password for a Service Using the REST API 16

Step 3. Configure System-Level Security Settings 17

Configure Security Settings 17

Step 4. (Optional) Configure External Authentication 19

Configure Active Directory 20

Configure Active Directory Authentication 20

Add a New Active Directory Configuration 21

Edit an Active Directory Configuration 22

Test an Active Directory Configuration 23

Delete an Active Directory Configuration 24

Configure PAM Login Capability 25

Prerequisites 26

PAM Kerberos 26

PAM LDAP 28

PAM RADIUS 29

Add a RADIUS Client and Associated Agent 31

PAM Agent for SecurID 32
Choose an NSS Service 37
NSS UNIX 37
NSS LDAP 38
Test NSS Functionality 40

How Role-Based Access Control Works 43

Pre-Configured Roles 43
Trusted Connections Between Server and Service 44
How Trusted Connections Are Established 45
Common Role Names on the Server and Services 45
End-to-End Workflow for User Setup and Service Access 46
Role Permissions 48
Service Permissions Format for New Services 48
Administration 49
Admin-server 50
Alerting 51
Cloud-gateway-server 51
Config-server 52
Contexthub-server 53
Dashboard 55
Endpoint-server 57
Esa-analytics-server 60
Incidents 61
Integration-server 61
Investigate 63
Investigate-server 64
Live 65
Malware 66
Orchestration-server 66
Reports 67
Respond-server 69
Security-server 73

Manage Users with Roles and Permissions **75**
Step 1. Review the Pre-Configured NetWitness Roles 76
Step 2. (Optional) Add a Role and Assign Permissions 77
Add a Role and Assign Permissions 78
Duplicate a Role 79
Change Permissions Assigned to a Role 79
Delete a Role 79
Step 3. Verify Query and Session Attributes per Role 80
Query and Session Attributes 80
How Query-Handling Attribute Settings Apply to Individual Users 81
Set Query Handling Attributes for a User Role 81
Step 4. Set Up a User 83
Add a User and Assign a Role 84
Add a User and Assign a Role 84
Add a User for External Authentication 87
Change User Information or Roles 89
Delete a User 89
Reset a User Password 90
Enable, Unlock, and Delete User Accounts 91
Step 5. (Optional) Map User Roles to External Groups 93
Prerequisites 93
Add Role Mapping for an External Group 94
Edit Role Mapping for a Group 95
Search for External Groups 97
References **99**
Admin Security View 100
What do you want to do? 100
Related topics 100
Users Tab 102
What do you want to do? 102
Related Topics 102
Add or Edit User Dialog 104
What do you want to do? 104

Related Topics 104
User Preferences 104
Add User Dialog 105
Edit User Dialog 105
User Information 106
Roles Tab 107
Roles Tab 108
What do you want to do? 108
Related Topics 108
Add or Edit Role Dialog 110
What do you want to do? 110
Role Info 111
Attributes 111
Permissions 112
External Group Mapping Tab 114
What do you want to do? 114
Related Topics 114
Add Role Mapping Dialog 116
What do you want to do? 116
Group Mapping 117
Mapped Roles 118
Search External Groups Dialog 119
What do you want to do? 119
Settings Tab 121
What do you want to do? 121
Related Topics 121
Admin Security View Settings Tab 121
Password Settings 123
Security Settings 125
PAM Authentication 126
Active Directory Configurations 126

System Security and User Management

This guide provides information about setting up security and controlling user access. The System Administrator needs to understand system-wide settings, user accounts, system roles, permissions, and access to services.

Topics

- Set Up System Security
- How Role-Based Access Control Works
- Manage Users with Roles and Permissions
- References

Set Up System Security

This topic introduces a set of end-to-end procedures for implementing system security. Each step in the following topics explains a system-wide setting. Follow the steps in order to set up security in NetWitness Suite.

Topics

- Step 1. Configure Password Complexity
- Step 2. Change the Default Admin Passwords
- Step 3. Configure System-Level Security Settings
- Step 4. (Optional) Configure External Authentication

Step 1. Configure Password Complexity

This topic provides instructions to set system-wide NetWitness Suite password complexity requirements.

Passwords are an important part of your network security strategy. They provide critical front-line protection for your computer systems and help prevent attacks and unauthorized access to private information.

Password policies, designed to enhance the security of corporate networks, vary depending on the industry, corporate requirements, and regulations. Because of these password policy variations, NetWitness Suite software allows you to configure the password complexity requirements for internal NetWitness Suite users to conform to your corporate password policy guidelines.

Password complexity requirements apply only to internal users and are not enforced for external users. External users rely on their own methods and systems to enforce password complexity.

In addition, you can set a global default user expiration period and determine if and when internal users receive notification that their passwords are about to expire. The password expiration notification consists of a password expiration message when a user logs on to NetWitness Suite.

Password Strength

Strong passwords make it more difficult for attackers to guess user passwords and help prevent unauthorized access to your organization's network. You can define the appropriate level of password strength for your NetWitness Suite users. When you configure the password strength settings, they apply to internal NetWitness Suite users, including the admin user.

You can choose to enforce any combination of the following password strength requirements when a NetWitness Suite user creates or changes their password:

- Minimum password length
- Minimum number of uppercase characters
- Minimum number of lowercase characters
- Minimum number of decimals (0 through 9)
- Minimum number of special characters
- Minimum number of non-Latin alphabetic characters (includes Unicode characters from Asian languages)
- Whether or not the password can contain the username

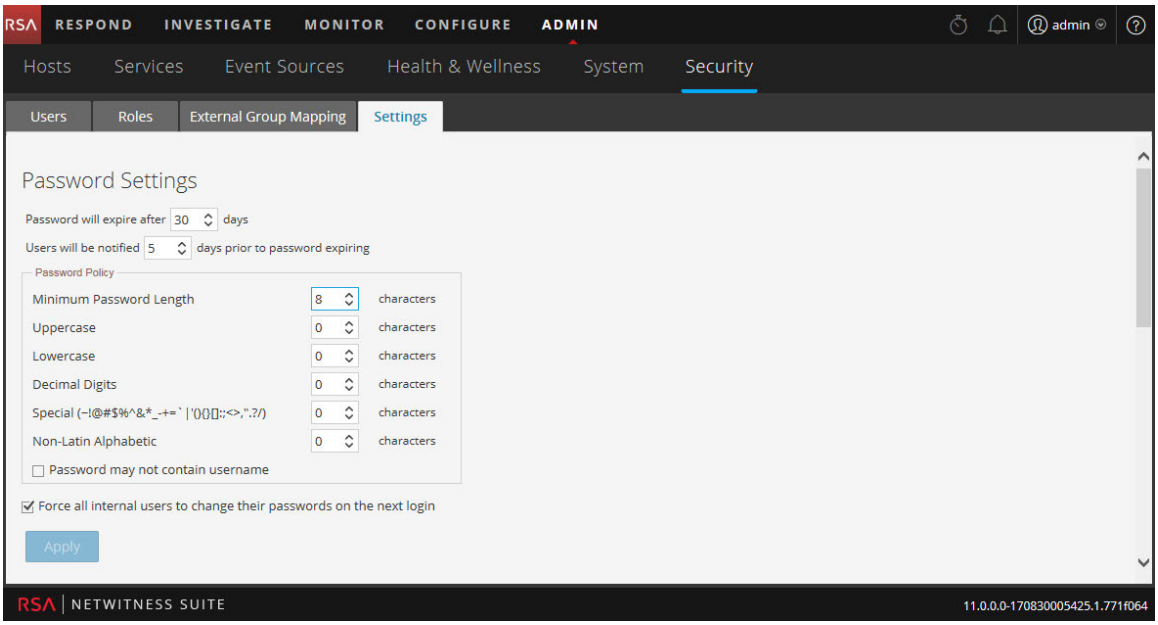
For example, you can create a strong password requirement that has a minimum of 8 characters, cannot contain the username of the user, and contains a mix of uppercase and lowercase letters, numbers, and special characters.

If you choose to enforce a minimum number of non-Latin alphabetic characters, ensure that your users have these characters available to them when setting their passwords.

The topic "STIG Compliant Passwords" in the *System Maintenance Guide* provides an example of a strong password policy.

Configure Password Strength

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.



3. In the **Password Settings** section, select the password complexity requirements to enforce when NetWitness Suite users set their passwords and specify the minimum characters required, if applicable. Set the value to 0 for requirements you do not want to enforce, except for Minimum Password Length, which has a minimum value of 4 characters.

Requirement	Description
Password will expire after <n> days	The default number of days before a password expires for all internal NetWitness Suite users. A value of zero (0) disables password expiration. For new installations, the default value is 30. For upgrades, the previous value will migrate automatically to the upgraded installation.
Users will be notified <n> days prior to password expiring	The number of days before the password expiration date, to notify a user that their password is about to expire. Users see a Password Expiration Message dialog when they log on to NetWitness Suite. The minimum value is 1 day.
Minimum Password Length	Specifies a minimum password length. A minimum password length prevents users from using short passwords that are easy to guess. There is a minimum password length of 4 characters required by default.
Uppercase	Specifies a minimum number of uppercase characters for the password. This includes European language characters A through Z, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic uppercase: Д Ц • Greek uppercase: Π Λ
Lowercase	Specifies a minimum number of lowercase characters for the password. This includes European language characters a through z, sharp-s, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic lowercase: д ц • Greek lowercase: π λ
Decimal Digits	Specifies a minimum number of decimal characters (0 through 9) for the password.
Special (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Specifies a minimum number of special characters for the password: `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`

Requirement	Description
Non-Latin Alphabetic	Specifies a minimum number of Unicode alphabetic characters that are not uppercase or lowercase. This includes Unicode characters from Asian languages. For example: • Kanji (Japanese): 頁 (leaf) 枒 (tree)
Password May Not Contain Username	Specifies that a password cannot contain the case-insensitive username of the user.

4. If you want your password policy changes to take effect at the next login instead of the next password change, select **Force all internal users to change their passwords on the next login**. Note that this setting is checked by default.
5. Click **Apply**.
   The password strength settings take effect when internal users create or change their passwords. If you selected **Force all internal users to change their passwords on the next login**, all internal users must change their password the next time they log on to NetWitness Suite.

Step 2. Change the Default Admin Passwords

This topic provides instructions for changing the admin password for the NetWitness Suite service and for the Core services.

The system administrator's user account is installed with NetWitness Suite. The username is **admin** and the default password is the password that was entered in the Text-based User Interface (TUI) during the NetWitness Suite installation process. The **Administrators** role is assigned to admin. This role has full system privileges to control what a user can do and which services a user can access. The only modification you can make to this account is to change the password. Unlike other NetWitness Suite users, changes to the **admin** user password do not automatically propagate to downstream services. When you configure the password strength settings, they apply to all NetWitness Suite users, including the admin user.

Passwords, an important aspect of computer security, are the front line of protection for your system. The **admin** user is pre-installed in NetWitness Suite and on each Core service. For security, you create the Users and Roles for your organization in NetWitness Suite, and on each Core service.

Best Practices

RSA recommends the following best practices:

- Change the **admin** password of each service from the default.
- Create a different password for the **admin** account on each service.

Change the admin Password for the NetWitness Suite

Change the **admin** password for the NetWitness Suite in the Profile view. See "Change Password" in the *NetWitness Suite Getting Started Guide*. The password of the **admin** user does not propagate to Core services.

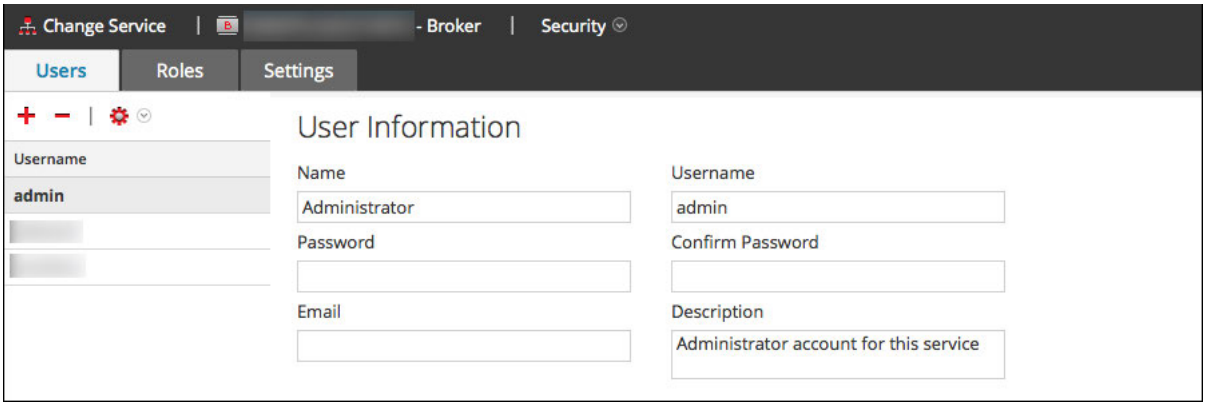
Note: After you change the admin password, you must remove and re-add a Data Source on the Reporting Engine. For more information, see the **Remove and re-add a Data Source on the Reporting Engine** section below.

Change the admin Password for Core Services

To change the admin password for a Core service:

1. In NetWitness Suite, go to **ADMIN > Services.**
2. Select a service, and then select **> View > Security**.

3. On the **Users** tab, select the **admin** user.



4. In the **Password** field, type a new admin password for the selected service.
5. In the **Confirm Password** field, retype the new password.
6. Click **Apply**.

Note: After you change the admin password, you must remove and re-add a Data Source on the Reporting Engine. For more information, see **Remove and re-add a Data Source on the Reporting Engine** below.

Remove and re-add a Data Source on the Reporting Engine

Reporting Engine validates a Data Source using the Data Source username and password. If you change the username or password of a Data Source, you must remove and re-add the Data Source.

To remove and re-add a data source on the Reporting Engine:

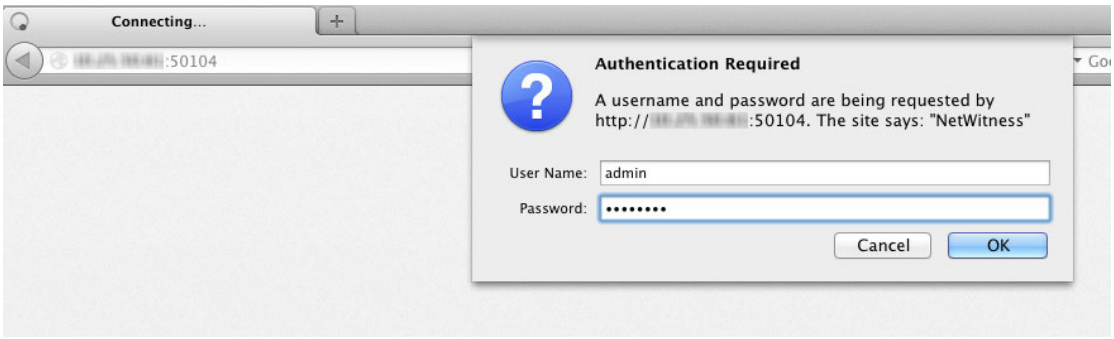
1. In NetWitness Suite, go to **ADMIN > Services**.
2. In the Services view, select Reporting Engine and **View > Config**.
3. Click the **Sources** tab.
4. Select a service to remove and click −
5. Click + and select **Available Services.**
6. Select the service you removed in step 4 and click **OK**.
7. When prompted, enter the new username and password for the service.

Change the admin Password for a Service Using the REST API

In rare circumstances, you may need to change the admin password for a Core service outside of the NetWitness Suite user interface. This is simply another way to perform the Core service password change, and is not the preferred method.

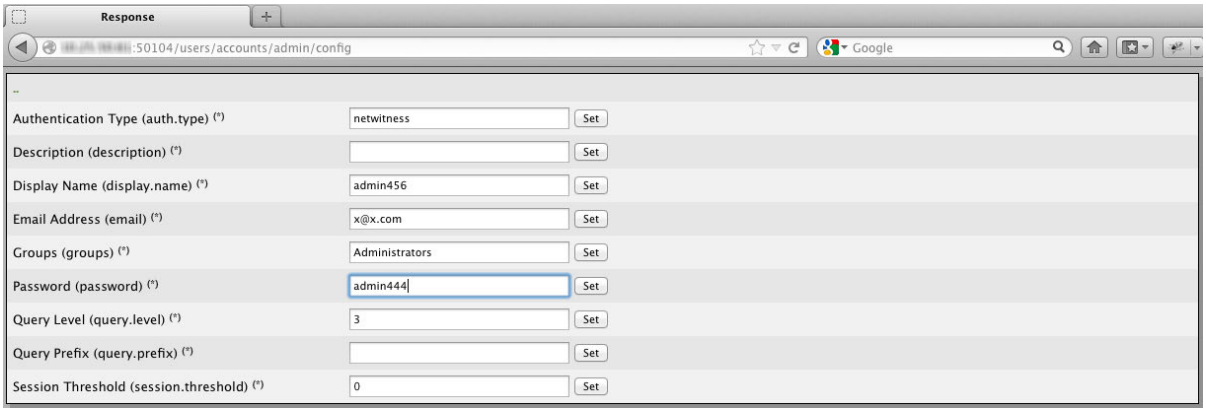
To change the admin password for the service using the REST User Interface:

1. Open a web browser, and go to the following URL:
   <hostname>:<port>
   where the **hostname** is the name of a NetWitness Suite Core service and **port** is the port used for REST communication. Here is an example for a Decoder:
   `http://10.20.30.40:50104`
   The authentication dialog is displayed.



2. In the dialog enter the user name and password used for authentication as admin on the service, and click **OK**. The default user name is **admin** and the default password is **netwitness**.
   The REST window for the service is displayed.

3. Navigate through the node structure to **users/accounts/admin/config**.
   The user configuration fields for admin are displayed in the browser window.



4. In the Password field, type a new admin password and click **Set**.

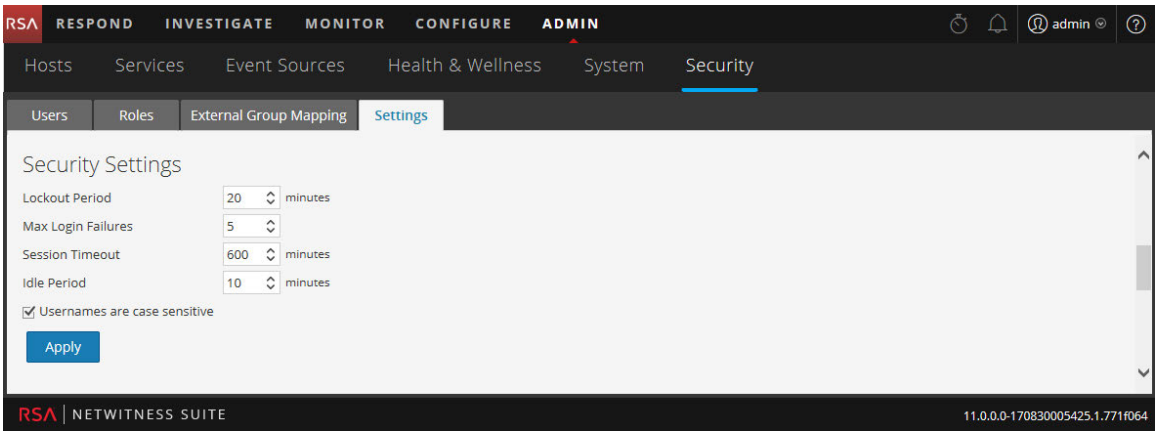
Step 3. Configure System-Level Security Settings

This topic explains how to set system-wide security parameters.

Most global security settings, such as the maximum number of failed login attempts to allow, apply to all NetWitness Suite users and sessions. Settings related to passwords in the Password Strength section, such as password expiration period and the default number of days before user passwords expire, apply to internal NetWitness Suite users, but not external users.

Configure Security Settings

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.



3. In the **Security Settings** section, specify values for the fields as described in the following table.

Field	Description
Lockout Period	Number of minutes to lock a user out of NetWitness Suite after the configured number of failed logins is exceeded. The default value is 20 minutes.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5.

Field	Description
Session Timeout	The maximum duration of a user session before timing out in minutes. The default value is 600. The session times out when the configured time has elapsed, after which the user must log in again. The maximum allowed value is 30,000. **Note:** If you migrated to NetWitness Suite 11.0 from version 10.6.x and previously used a value of 0 for an unlimited session timeout, the value was reset automatically to 30,000 minutes, as a value of 0 is no longer supported.
Idle Period	Number of minutes of inactivity before a session times out. The default value is 10. The maximum allowed value is 30,000. **Note:** If you migrated to NetWitness Suite 11.0 from version 10.6.x and previously used a value of 0 for an unlimited idle period, the value was reset automatically to the default value of 10, as a value of 0 is no longer supported.
Usernames are case sensitive	Select this option if you want the Username field on the NetWitness Suite login screen to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness Suite, but you could not use Admin.

4. Click **Apply**. The Security Settings take effect immediately. If a password expires, the user receives a prompt to change the password when they log on to NetWitness Suite.

Step 4. (Optional) Configure External Authentication

This topic introduces the external authentication methods that NetWitness Suite supports.

When a user logs in, NetWitness Suite first attempts to authenticate locally. If no local user is found, and External Authentication configuration is enabled, an attempt is made to authenticate externally.

External authentication allows users who do not have an internal NetWitness Suite user account to log on to NetWitness Suite and receive role-based permissions.

NetWitness Suite supports two methods of external authentication, Active Directory and Pluggable Authentication Modules (PAM). Topics in this section describe how to configure and test each method.

Topics

- Configure Active Directory
- Configure PAM Login Capability

Configure Active Directory

This topic explains how to configure NetWitness Suite to use Active Directory to authenticate external user logins.

When a user logs in, NetWitness Suite first attempts to authenticate locally. If no local user is found, and Active Directory configuration is enabled, an attempt is made to authenticate with Active Directory Service. You can configure Active Directory settings to enable authentication of external groups in the Admin > Security view > Settings tab.

In an environment with multiple authentication servers, LDAP forwarding allows LDAP referral following for AD group lookups. LDAP forwarding can increase the time required to log on because AD group lookups are extended to connected authentication servers. When your AD instance attempts to contact domain controllers that are blocked by your firewall, users can experience a delay of several minutes in logging on to NetWitness Suite. NetWitness Suite has a configuration option that specifies whether LDAP forwarding occurs; by default, LDAP referrals are disabled. When disabled, your AD instance does not attempt to contact referred domain controllers.

Note: The Settings tab also provides the option to enable PAM configuration, which can be used simultaneously with Active Directory configurations. For information on enabling and configuring PAM authentication, see Configure PAM Login Capability.

Procedures

Configure Active Directory Authentication

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.
   The Active Directory Configurations list is displayed in the panel so that you can add or edit

a configuration.

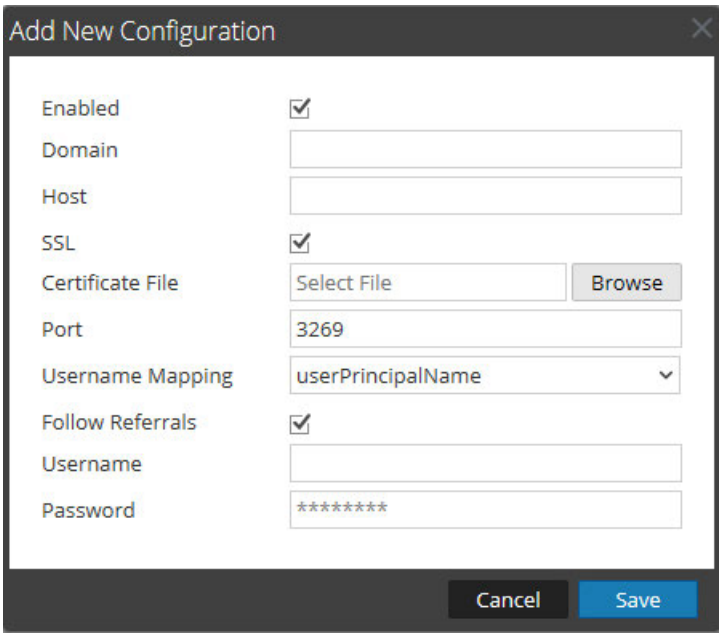
3. Add, edit, or delete domains as necessary, as described in the following sections.
   The domains added to this list are automatically populated in the External Group Mapping tab so that you can map security roles to each group.

Note: To configure security roles used for Active Directory access, see Step 5. (Optional) Map User Roles to External Groups.

Add a New Active Directory Configuration

To add a new active directory configuration in the Active Directory Configurations list:

1. Under Active Directory Configurations, click +.
   The Add New Configuration dialog is displayed.



2. Click the **Enabled** checkbox.
3. Enter **Domain**, **Host** and **Port** information for the Active Directory Service.
4. (Optional) To select SSL for this configuration, check the **SSL** checkbox. You must then enter the Active Directory server certificate file by clicking **Browse** and selecting the desired file to upload.
5. In the **Username Mapping** field, select the Active Directory search field to use for username mapping. You can select userPrincipalName (UPN) or sAMAccountName.
6. For sites that have multiple authentication servers, click **Follow Referrals** to enable or disable LDAP referral following for AD group lookups.
7. To provide credentials to bind to the Active Directory Service while searching Active Directory group, enter the credentials in the **Username** and **Password** fields.

Note: If you selected sAMAccountName in the **Username Mapping** field, you must enter the username in the format "domain\user" to authenticate.

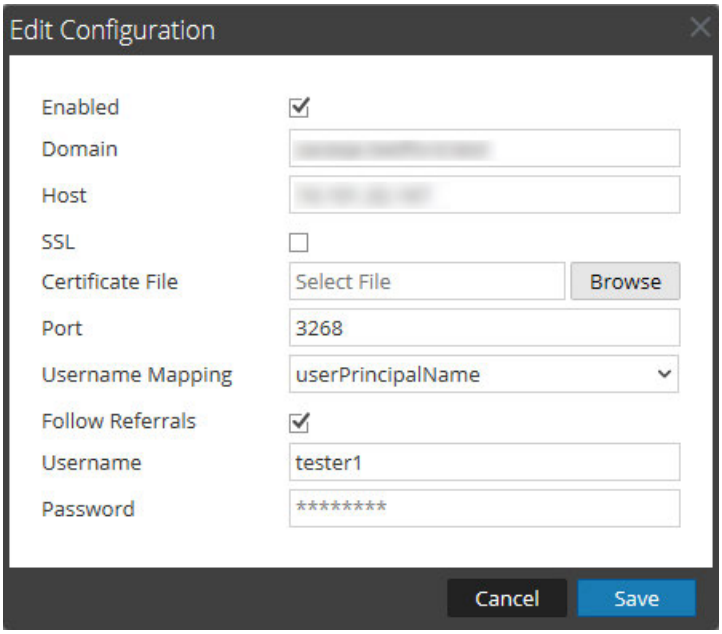
8. Click **Save**.
   The new configuration is listed in the Active Directory Configurations list.

Edit an Active Directory Configuration

To edit an active directory configuration in the Active Directory Configurations list:

1. Under **Active Directory Configurations**, select the configuration you wish to edit and click .

The Edit Configuration dialog is displayed.



2. (Optional) Enter the **Domain**, **Host** and **Port** information for the Active Directory Service.
3. (Optional) To select SSL for this configuration, check the **SSL** checkbox. You must then enter the Active Directory server certificate file by clicking **Browse** and selecting the desired file to upload.
4. (Optional) In the **Username Mapping** field, select the the Active Directory search field to use for username mapping.
5. To specify the Follow LDAP referrals behavior in environments with multiple authentication servers, click the **Follow Referrals** checkbox.
   a. If you want to disable LDAP forwarding, uncheck the box.
   b. If you want to enable LDAP forwarding, check the box.
6. To provide credentials to bind to the Active Directory Service while searching Active Directory group, enter the credentials in the **Username** and **Password** fields.
7. Click **Save**.
   The configuration is listed in the Active Directory Configurations list.

Test an Active Directory Configuration

To test an active directory configuration:

1. Select the configuration to be tested from the Active Directory Configurations list.
2. In the toolbar, click Test.
   A message that the test is successful is displayed.
3. If the test does not succeed, review and edit the configuration.

Delete an Active Directory Configuration

To delete an active directory configuration:

1. Under Active Directory Configurations, select the configuration to be deleted from the Active Directory Configurations list.
2. In the toolbar, click −.
   A message is displayed warning you that all users in the selected Active Directory configuration will not be able to log in to NetWitness Suite if it is deleted.
3. Do one of the following:
   a. To confirm the deletion, click **Yes**.
   b. To cancel the deletion, click **No**.

Configure PAM Login Capability

This topic explains how to configure NetWitness Suite to use Pluggable Authentication Modules (PAM) to authenticate external user logins.

PAM login capability involves two separate components:

- PAM for user authentication
- NSS for group authorization

Together they provide external users the capability to log on to NetWitness Suite without having an internal NetWitness Suite account, and to receive permissions or roles determined by mapping the external group to a NetWitness Suite security role. Both components are required for a login to succeed.

External authentication is a system-level setting. Before configuring PAM, carefully review all of the information here.

Pluggable Authentication Modules

PAM is a Linux-provided library responsible for authenticating users against authentication providers such as RADIUS, Kerberos, or LDAP. For implementation, each authentication provider uses its own module, which is in the form of an operating system (OS) package such as pam_ldap. NetWitness Suite uses the OS-provided PAM library, and the module that the PAM library is configured to use, to authenticate users.

Note: The PAM provides only the ability to authenticate.

Name Service Switch

NSS is a Linux feature that provides databases that the OS and applications use to discover information like hostnames; user attributes like home directory, primary group, and login shell; and to list users that belong to a given group. Similar to PAM, NSS is configurable and uses modules to interact with different types of providers. NetWitness Suite uses OS-provided NSS capabilities to authorize external PAM users by looking up whether a user is known to NSS and then requesting from NSS the groups of which that user is a member. NetWitness Suite compares the results of the request to the NetWitness Suite External Group Mapping and if a matching group is found, the user is granted access to log on to NW with the level of security defined in the External Group Mapping.

Note: NSS does not provide authentication.

PAM and NSS Combination

Both PAM (authentication) and NSS (authorization) must succeed in order for an external user to be allowed to log on to NetWitness Suite. The procedure for configuring and troubleshooting PAM is different than the procedure for configuring and troubleshooting NSS. The PAM examples in this guide include Kerberos, LDAP, and Radius. The NSS examples include LDAP and UNIX. The PAM and NSS module combination used is determined by site needs.

Process Overview

To configure PAM login capability, follow the instructions in this document to complete each step:

1. Configure and test the PAM module.
2. Configure and test the NSS service.
3. Enable PAM in NetWitness Server.
4. Create group mappings in NetWitness Server.

Prerequisites

Before beginning the setup of PAM, review the procedure and gather the external authentication server details depending on the PAM module you want to implement.

Before beginning the setup of NSS, review the procedure, identify the group names that you will use in the External Group mapping, and gather the external authentication server details, depending on the NSS service being used.

Before beginning setup of PAM in NetWitness Suite, identify the group names that you will use in the External Group mapping. When mapping roles, the role in NetWitness Suite must match a group name that exists in the external authentication server.

Configure and Test the PAM Module

Choose one of the following sections to set up and configure the PAM component:

- PAM Kerberos
- PAM LDAP
- PAM RADIUS
- SecurID

PAM Kerberos

Kerberos Communication Ports – TCP 88

To configure PAM authentication using Kerberos:

1. Execute the following command (but first verify that the `krb5-workstation` package is installed in your environment):
   `yum install krb5-workstation pam_krb5`
2. Edit the following lines in the Kerberos configuration file `/etc/krb5.conf`. Replace variables, which are delimited by <angle brackets>, with your values and omitting the angle brackets. Capitalization is required where shown.

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 dns_lookup_kdc = true
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = <DOMAIN.COM>
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 <DOMAIN.COM> = {
 kdc = <SERVER.DOMAIN.COM>
 admin_server = <SERVER.DOMAIN.COM>
 }

 [domain_realm]
 <domain.com> = <DOMAIN.COM>
 <.domain.com> = <DOMAIN.COM>
```

3. Test the Kerberos configuration with the command:
   `kinit <user>@<DOMAIN.COM>`
   No output after entering the password indicates success.

4. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   `auth sufficient pam_krb5.so no_user_check`

This completes the configuration for PAM Kerberos. Now, proceed to the next section, *Configure and Test the NSS Service*.

PAM LDAP

LDAP Communication Ports - TCP 389 or TCP 636

TCP 389 can be used for both unencrypted and in most cases encrypted traffic and is usually sufficient. Most modern LDAP implementations support the `start_tls` command once connected to port 389, which upgrades the connection from an unencrypted to an encrypted state. In this instance, LDAP URIs still begin with `ldap://` even when using `start_tls`.

TCP 636 is used only in instances where the LDAP server does not support the `start_tls` command. In this case, LDAP URIs begin with `ldaps://` and the `start_tls` command is not used.

Note: The PAM LDAP example in this guide has been tested with OpenLDAP server. User should refer to other documentation also if a different directory server is used.

To configure PAM authentication using LDAP:

1. Execute the following command (but first verify that the `openldap-clients` package is installed in your environment):
   `yum install nss-pam-ldapd openldap-clients`
2. Edit the LDAP configuration file `/etc/nslcd.conf` as shown in the following example:

Note: Replace variables, which are delimited by <angle brackets>, with your values and omit the angle brackets. Capitalization is required where shown.

Sample `/etc/nslcd.conf` file entries:

```
uri ldap://<server.domain.com>
 base <dc=domain,dc=com>
 binddn <cn=bineuser,dc=domain,dc=com>
 bindpw <secret>
```

3. After modifying the `/etc/nslcd.conf` file, run the following command:
   `systemctl restart nslcd`
4. (Optional) To enable secure transport for LDAP communication with peer certificate verification (more secure), refer to Linux man page for nslcd for the correct code modification for the `/etc/nslcd.conf` file.

5. (Optional) To enable secure transport for LDAP communication without peer certificate, refer to Linux man page for nslcd for the correct code modification for the `/etc/nslcd.conf` file.
6. To troubleshoot the LDAP configuration, first stop the `nslcd` service by entering the following command:
   ```
   systemctl stop nlscd
   ```
7. To output troubleshooting and status information from the service to the console, run the `nslcd` service in debug mode from the command line:
   ```
   nslcd -d
   ```
8. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   ```
   auth sufficient pam_ldap.so
   ```

This completes the configuration for PAM LDAP. Now, proceed to the next section, *Configure and Test the NSS Service*.

PAM RADIUS

Radius Communication Ports - UDP 1812 or UDP 1813

To configure PAM authentication using Radius you must add the NetWitness Server to your Radius Server's Client list and configure a shared secret. Contact the Radius Server Administrator for this procedure.

To configure PAM authentication using RADIUS:

1. Execute the following command (but first verify that the `pam_radius_auth` package is installed in your environment):
   ```
   yum install pam_radius_auth
   ```
2. Edit the RADIUS configuration file, `/etc/raddb/server` as follows:
   ```
   # server[:port] shared_secret  timeout (s)
   server    secret     3
   ```
3. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   ```
   auth sufficient pam_radius_auth.so
   ```
4. Execute the following command to copy the RADIUS library:
   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

Caution: For PAM RADIUS to work, the `/etc/raddb/server` files must have write permission. The command needed for this is: `chown netwitness:netwitness /etc/raddb/server`.

Caution: You must restart the Jetty server after making the above changes for PAM RADIUS.

The PAM Modules and associated services output information to `/var/log/messages` and `/var/log/secure`. These outputs can be used to assist in troubleshooting configuration problems.

The following procedure is an example of the steps to configure PAM authentication for RADIUS using SecurID:

Note: The examples in these tasks use RSA Authentication Manager as the RADIUS server.

1. Execute the following command (but first verify that the `pam_radius_auth` package is installed in your environment):

   ```
   yum install pam_radius_auth
   ```

2. Edit the RADIUS configuration file, `/etc/raddb/server` and update it with the authentication manager instance hostname, shared secret and timeout value:

   ```
   # server[:port] shared_secret timeout (s)

    111.222.33.44         secret       1

    #other-server        other-secret 3

    192.168.12.200:6369 securid      10
   ```

   Note: You must comment out `127.0.0.1` and `other-server` lines and add the IP address of the authentication manager primary instance with RADIUS port number (for example, `192.168.12.200:1812`), RADIUS shared secret, and a timeout value of 10.

3. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

   ```
   auth sufficient pam_radius_auth.so
   ```

   Note: You can add `debug` to the end of the above line in the `/etc/pam.d/securityanalytics` file to enables PAM debugging (for example, `auth sufficient pam_radius_auth.so debug`)

4. Execute the following command to copy the RADIUS library:

   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

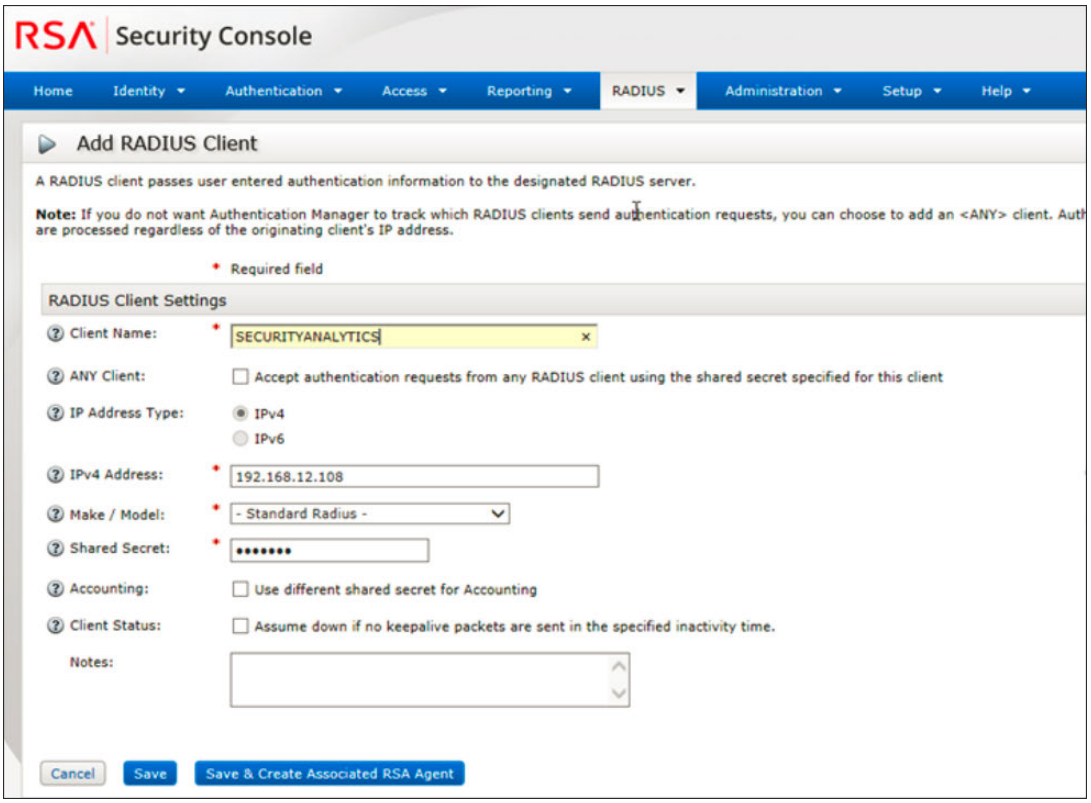
The PAM Modules and associated services output information to `/var/log/messages` and `/var/log/secure`.These outputs can be used to assist in troubleshooting configuration problems.

Add a RADIUS Client and Associated Agent

Note: The examples in these tasks use RSA Authentication Manager as the RADIUS server. You must use administrative account credentials to log on RSA Authentication Manager Security Console.

To add a RADIUS Client and Associated Agent:

1. Log on to RSA Authentication Manager.
   The Security Console is displayed.
2. In the Security Console, Click **RADIUS > RADIUS Client > Add New**.
   The Add RADIUS Client page is displayed.

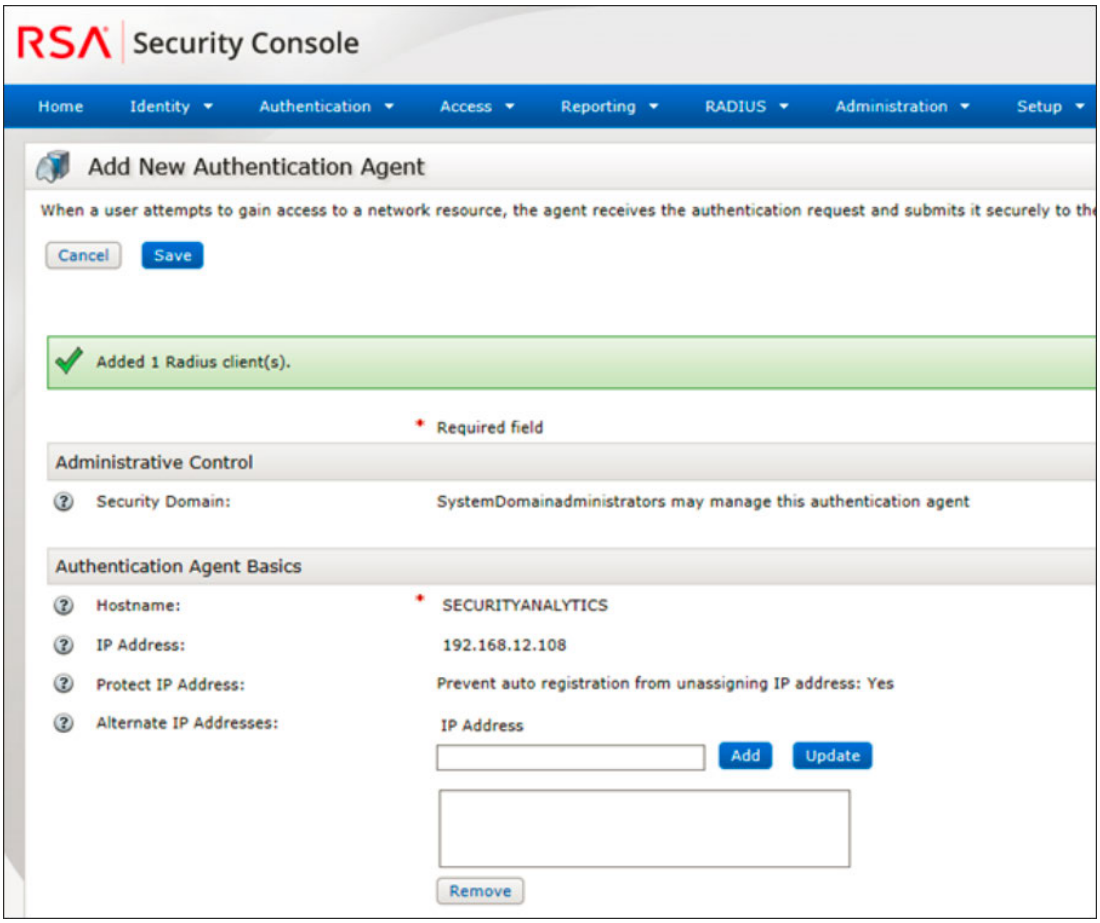


3. In RADIUS Client Settings, provide the following information:
   a. In the **Client Name** field, enter the name of the client, for example, NetWitness Suite.
   b. In the **IPv4 Address** field, enter the IPv4 address of the RADIUS client, for example, 192.168.12.108.

c. In the **Make/Model** drop-down list, select the type of RADIUS client, for example, Fortinet.

d. In the **Shared Secret** field, enter the authentication shared secret.

4. Click **Save & Create Associated RSA Agent**.



5. Click **Save**.

If Authentication Manager Instance is unable to find the authentication agent on the network, A warning page is displayed. Click **Yes, Save Agent**.

For more information, see Add a RADIUS Client topic in *RSA Authentication Manager 8.2 Administrator's Guide*.

This completes the configuration for PAM RADIUS. Now, proceed to the next section, *Configure and Test the NSS Service*.

PAM Agent for SecurID

PAM Communication Port - UDP 5500

Prerequisites

The RSA SecurID PAM module is supported only under the following conditions:

1. Trusted connections must be enabled and functioning between NetWitness Suite and Core services.

Process Overview

The high-level steps to configure the SecurID PAM module are:

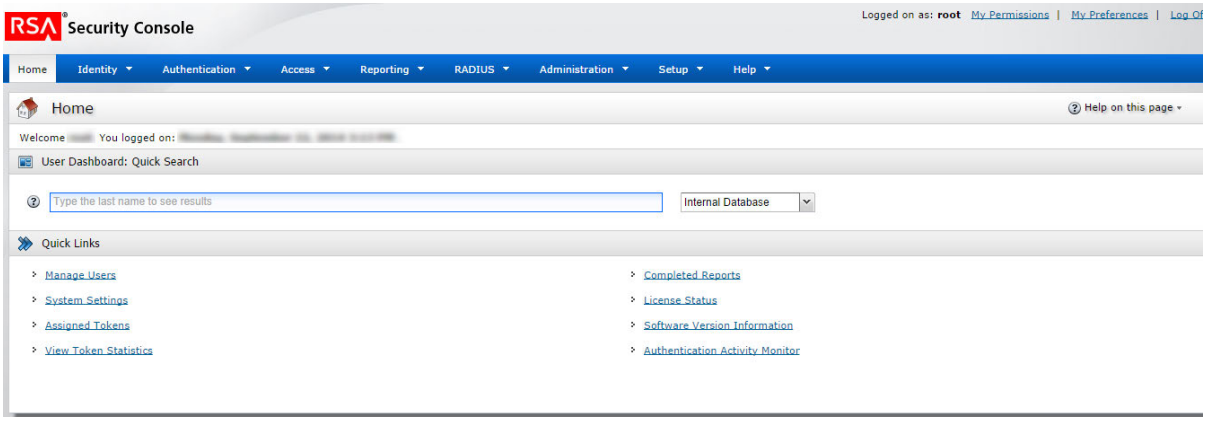
1. Configure **Authentication Manager**:
   a. Add Authentication Agent.
   b. Download configuration file.
2. Configure **NetWitness Server**:
   a. Copy configuration file from Authentication Manager and customize it.
   b. Install the PAM SecurID Module.
3. Test connectivity and authentication.

Then follow the remaining procedures in the sections that follow:

- Configure NSS.
- Enable PAM in NetWitness Server.
- Configure group mappings in NetWitness Server.

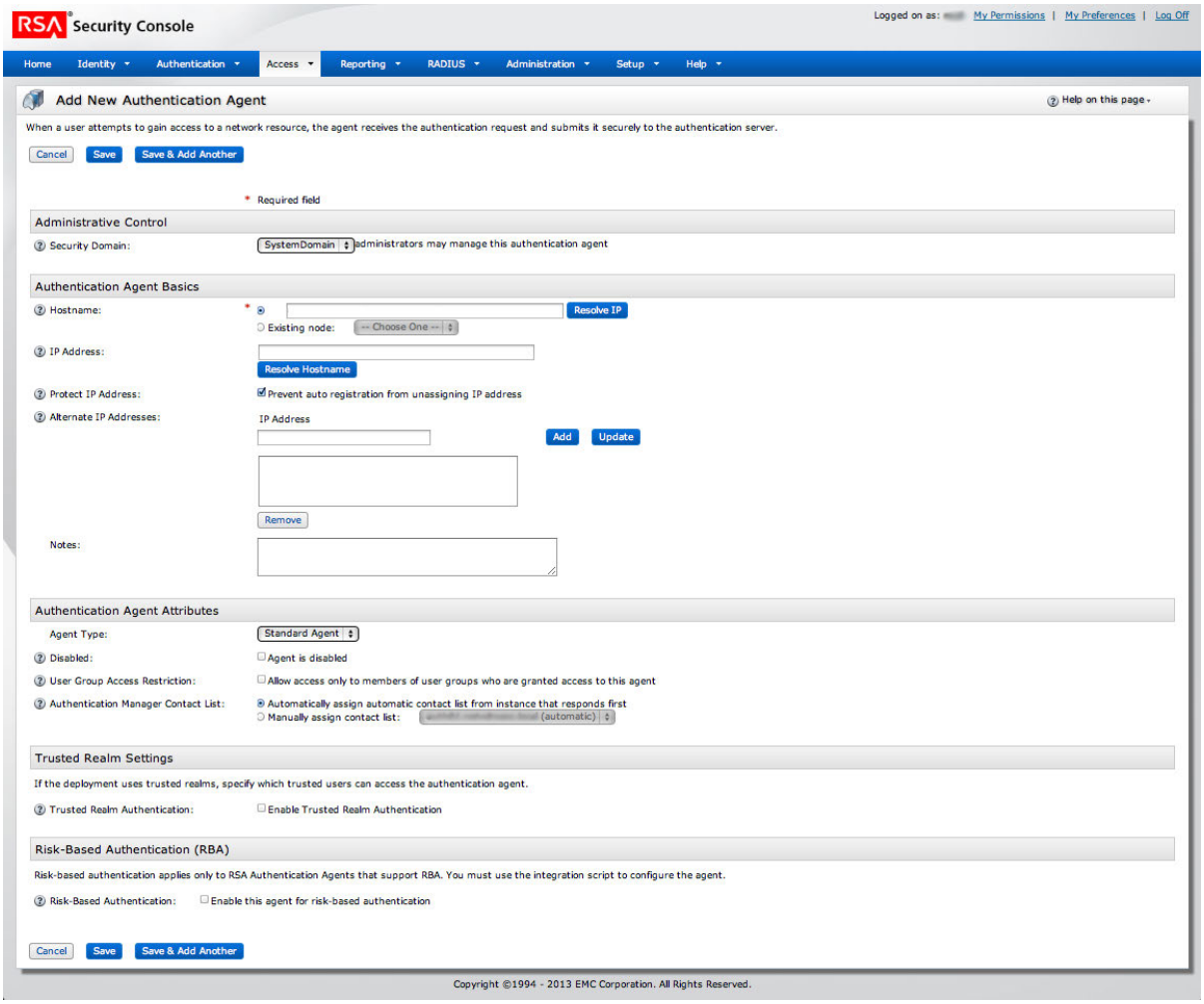
To configure Authentication Manager:

1. Log on to RSA Authentication Manager.
   The Security Console is displayed.

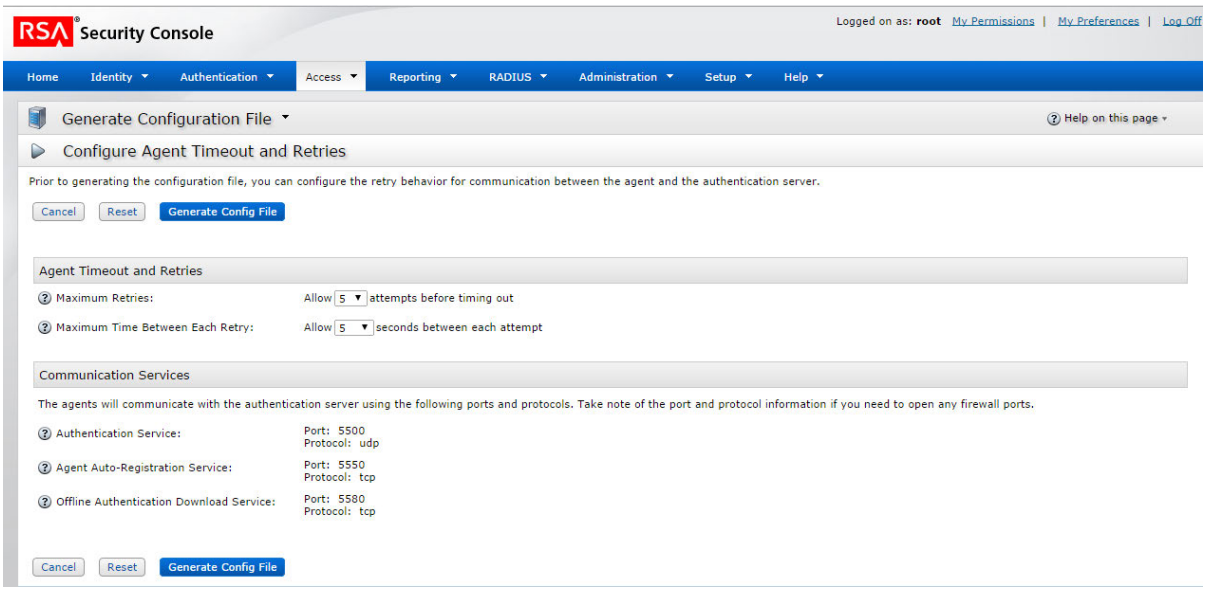


2. In the Security Console, add a new authentication agent.
   Click **Access > Authentication Agents > Add New.**

The Add New Authentication Agent page is displayed.



3. In the **Hostname** field, type the hostname of the NetWitness Server.
4. Click **Resolve IP**.
   The IP address of the NetWitness Server is automatically displayed in the **IP Address** field.
5. Keep the default settings and click **Save**.
6. Generate a configuration file.
   Go to **Access > Authentication Agents > Generate Configuration File**.
   The Generate Configuration File page is displayed.



7. Keep the defaults and click **Generate Config File**.
   This creates **AM_Config.zip**, which contains two files.
8. Click **Download Now**.

To install and configure the PAM SecurID module:

1. On the NetWitness Server, make a directory:
   `mkdir /var/ace`
2. On the NetWitness Server, copy `sdconf.rec` from the .zip file to `/var/ace`.
3. Create a text file `sdopts.rec` in the `/var/ace` directory.
4. Insert the following line:
   `CLIENT_IP=<IP address of NetWitness Server>`
5. Install the SecurID Authorization Agent for PAM, which is available in the yum repository:
   `yum install sid-pam-installer`
6. Run the install script:
   `/opt/rsa/pam-agent-installer/install_pam.sh`
7. Follow the prompts to accept or change the defaults.
8. Edit the NetWitness Server PAM configuration file, `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   `auth sufficient pam_securid.so`

This completes the installation of the SecurID PAM module. Next, test the connectivity and authentication. Then, follow the procedures in Configure and Test the NSS Service.

Note: If the PAM SecurID setup is not complete, it may crash the Jetty server and the NetWitness Suite UI will not be displayed. You must wait until the PAM authentication configuration is complete and then restart the Jetty server.

To test connectivity and authentication:

1. Run `/opt/pam/bin/64bit/acetest`, enter **username** and **passcode**.
2. (Optional) If acetest fails, turn on debugging:
   `vi/etc/sd_pam.conf`
   `RSATRACELEVEL=15`
3. Run `/opt/pam/bin/64bit/acestatus`. Output below

```
RSA ACE/Server Limits
 ---------------------
 Configuration Version : 15 Client Retries : 5
 Client Timeout : 5 DES Enabled : Yes

RSA ACE/Static Information
 -------------------------
 Service : securid Protocol : udp Port Number : 5500

RSA ACE/Dynamic Information
 --------------------------
 Server Release : 8.1.0.0 Communication : 5

RSA ACE/Server List
 ------------------
 Server Name :  auth81.netwitness.local
 Server Address :  192.168.100.10
 Server Active Address : 192.168.100.10
 Master : Yes Slave : No Primary : Yes
 Usage : Available for Authentications
```

4. (Optional) To troubleshoot the Authentication Manager server, go to **Reporting > Real-time Activity Monitors > Authentication Activity Monitor.** Then click **Start Monitor**.
5. If you changed the setting, reset RSATRACELEVEL to 0:
   `vi/etc/sd_pam.conf`
   `RSATRACELEVEL=0`

Caution: After installation, verify that VAR_ACE in the `/etc/sd_pam.conf` file points to the correct location of the sdconf.rec file. This is the path to the configuration files. The command needed for this is: `chown -R netwitness:netwitness /var/ace`.

This completes the configuration for PAM Agent for SecurID. Now, proceed to the next section, *Configure and Test the NSS Service*.

Configure and Test the NSS Service

Choose an NSS Service

There are two NSS service options: LDAP and UNIX. There are advantages and disadvantages to each option.

NSS LDAP Pros	NSS LDAP Cons
Basic configuration is simpler	May require additional configuration and roles inside of Active Directory
Can communicate with any LDAP implementation	Requires configuration of an LDAP bind account
Uses a single TCP port for communication - easier to work with firewalls and proxies	More difficult to enable secure transport unless configured to not validate server certificates
Does not require joining NW host to AD domain	

NSS UNIX

No configuration is necessary to enable the NSS UNIX module; it is enabled in the host operating system by default. To authorize a user for a specific group, simply add that user to the operating system and add them to a group:

1. Create an OS group to use add your external user to with this command:
   `groupadd <groupname>`
2. Add the external user to the OS with this command:
   `adduser -G <groupname> -M -N <externalusername>`

Note: Note that this does NOT permit or allow access to the NW Server console.

This completes the configuration for NSS UNIX. Next, go to Test NSS Functionality.

NSS LDAP

An LDAP bind user must be created in directory server in order for NSS to be used. This user should be configured to not have its password expire. Because these credentials must be specified to the NSS LDAP service in plaintext, the permissions of `/etc/nslcd.conf` should be left at their default of 600 so the file cannot be read by system users other than root.

LDAP Communication Ports - TCP 389 or TCP 636

TCP 389 can be used for both unencrypted and in most cases encrypted traffic and is usually sufficient. Most modern LDAP implementations support the `start_tls` command once connected to port 389, which upgrades the connection from an unencrypted to an encrypted state. In this instance, LDAP URIs still begin with `ldap://` even when using `start_tls`.

TCP 636 is only used in instances where the LDAP server does not support the `start_tls` command. In this instance, LDAP URIs begin with `ldaps://` and the `start_tls` command is not used.

To configure the NSS module for LDAP:

1. Execute the following command (but first verify that the `nss-pam-ldapd` package is installed in your environment):
   ```
   yum install nss-pam-ldapd
   ```
2. Edit `/etc/nslcd.conf` to include the lines below, ensuring that all existing lines in the file are first commented out using a hash mark # at the beginning of the line:
   ```
   uid nslcd
   gid ldap
   uri ldap://<server.domain.com>
   base <dc=domain,dc=com>
   binddn <cn=binduser,dc=domain,dc=com
   bindpw <secret>
   ```
   Note: You will need to add additional mappings between NSS lookups and LDAP lookups for your specific environment. Please refer to Linux man page for nslcd for specific details.
3. (Optional) To enable secure transport for LDAP communication with peer certificate verification (more secure), refer to Linux man page for nslcd for the correct code modification for the `/etc/nslcd.conf` file.
4. (Optional) To enable secure transport for LDAP communication without peer certificate, refer to Linux man page for nslcd for the correct code modification for the `/etc/nslcd.conf` file.
5. Edit the NSS configuration file `/etc/nsswitch.conf`. Update only the below two entries and leave the rest at their default values:

```
passwd:files ldap
group:files ldap
```

6. To enable and start the NSLCD service, enter these commands:
   ```
   systemctl enable nslcd
   systemctl start nslcd
   ```
7. Test NSS functionality using guidance in the *Test NSS Functionality* section. If NSS tests fail, troubleshoot NSS LDAP as described in *Troubleshoot NSS LDAP*.
8. When you have confirmed that NSS is working properly from the command line, reboot the host for the NSS changes to take effect.
   ```
   reboot
   ```

To troubleshoot NSS LDAP:

1. To troubleshoot NSS LDAP, first stop the nslcd service by entering the following command:
   ```
   systemctl stop nslcd
   ```
2. To output troubleshooting and status information from the service to the console, run the nslcd service in debug mode from the command line.
   ```
   nslcd -d
   ```
3. (Optional) To increase debug verbosity, add an additional d multiple times to the end of nslcd -d, for example, enter the following command:
   ```
   nslcd -ddd
   ```
4. From a separate ssh session, use the `getent` commands from the Testing NSS Functionality section of this guide to test NSS. Watch the debug output from nslcd for any indications of where the failure is occurring. Increase nslcd debugging verbosity as needed.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
5. Make any necessary adjustments to `/etc/nslcd.conf` based on the output of step 2 or 3.
6. In the nslcd debug window from step 2 or 3, stop `nslcd` with `CTRL-C`. Repeat step 2 or 3 and continue troubleshooting until the `getent` command succeeds.
7. When `getent` succeeds, stop the command line `nslcd` and start the service daemon:
   ```
   systemctl start nslcd
   ```

Common problems may include:

- LDAP secure transport SSL certificate not installed on LDAP/AD server.
- CA certificate verification failed – comment out the `tls_cacert` line in `/etc/nslcd.conf` and instead try `tls_reqcert never`. If it succeeds, you know that certificate verification that is failing.
  - Root CA certificate is not in PEM format.
  - Using issuing CA certificate rather than root CA certificate.
  - LDAP server's SSL certificate name does not match its hostname.
- Incorrect base DN.
- LDAP bind user or password is not specified correctly.
- Incorrectly specifying `ldaps://` instead of `ldap://` in `uri` line of `/etc/nslcd.conf`. `ldaps://` should only be used when using LDAPS but not using the `start_tls` command.
- Active Directory users and groups do not have `uidNumber` or `gidNumber` attributes set.
- Network firewall is blocking communications.
- LDAP server hostname specified cannot be resolved.
  - Incorrect DNS settings in `/etc/resolv.conf`.
  - Bad hostname specified in `uri` line of `/etc/nslcd.conf`.

This completes the configuration for NSS LDAP. Next, go to Test NSS Functionality.

Test NSS Functionality

To test whether NSS is working with any of the previous NSS services, use the following commands:

```
getent passwd <pamUser>
 getent group <groupOfPamUser>
```

Output should be similar to:

```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
```

```
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

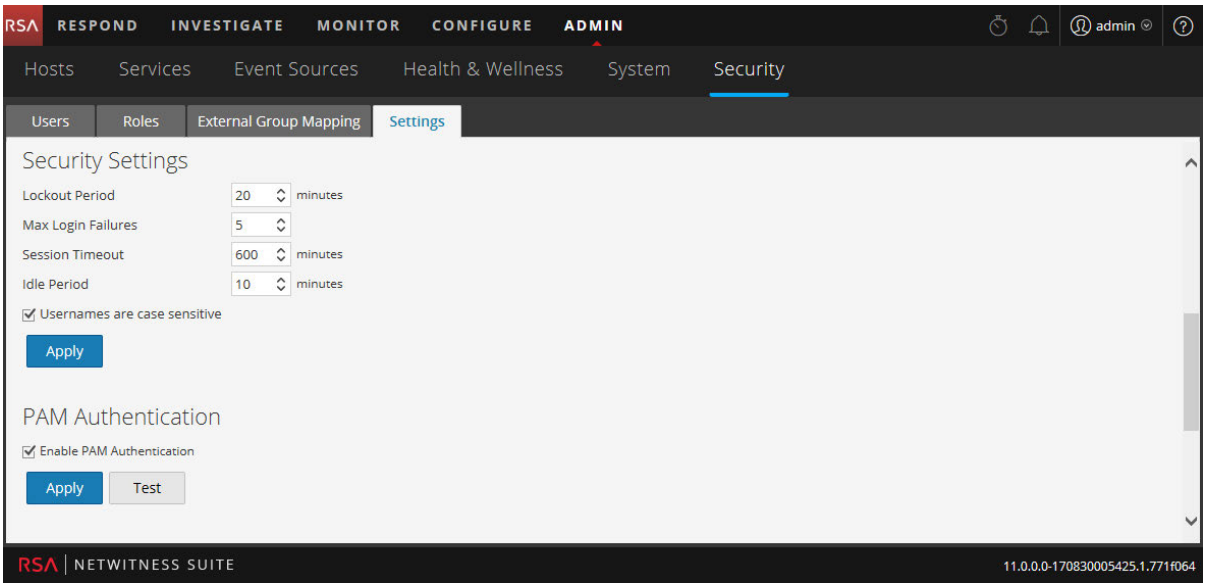
- If neither command produces output, NSS is not working properly for external authorization. Refer to the troubleshooting guidance for your NSS module provided in this document.

- If `getent` commands succeed and authentication success is confirmed in `/var/log/secure` but NetWitness Suite still fails to allow External users to login:
  - Was the correct group name specified for the NSS group in NW External Group Mapping? See Enable PAM and Create Group Mappings below.
  - It is possible that the NSS configuration has changed and NetWitness Suite has not picked up the change. A reboot of the NetWitness Suite host will cause NetWitness Suite to pick up NSS configuration changes. A restart of the Jetty server is not sufficient.

Proceed to the next section, Enable PAM in NetWitness Server.

Enable PAM in NetWitness Server

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Admin > Security view is displayed with the Users tab open.
2. Click the **Settings** tab.
3. Under **PAM Authentication**, select **Enable PAM Authentication** and click **Apply**.

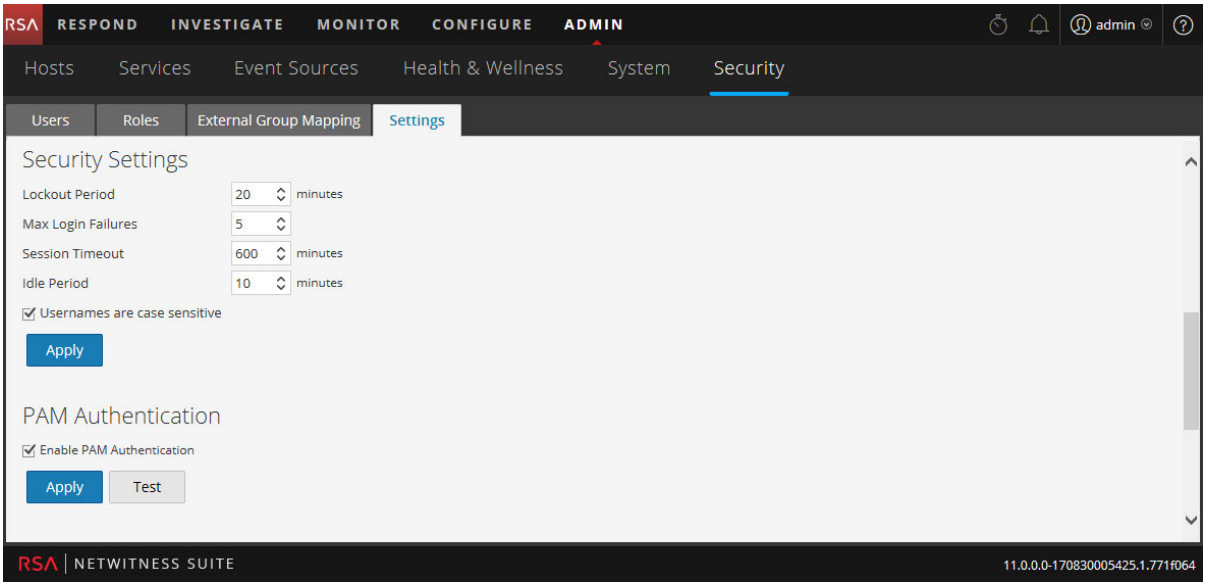


Test PAM Authentication

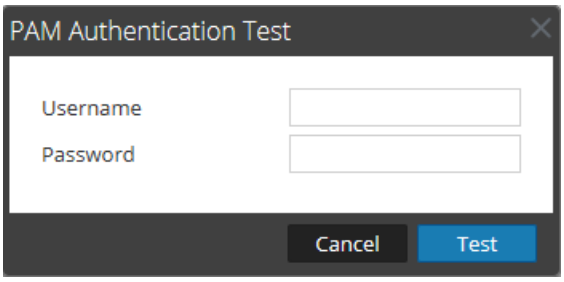
To test external authentication for PAM:

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.

3. Under **PAM Authentication**, select **Enable PAM Authentication**.



4. Under **PAM Authentication** options, click **Test.**
   The **PAM Authentication Test** dialog is displayed.



5. Type a user name and password that you want to test for authentication using the current PAM configuration.
6. Click **Test**.
   The external authentication method is tested to ensure connectivity.
7. If the test does not succeed, review and edit the configuration.

PAM is enabled, and Active Directory configurations will also remain enabled. PAM configurations are automatically populated in the External Group Mapping tab so that you can map security roles to each group. To configure security roles used for PAM access, see Step 5. (Optional) Map User Roles to External Groups.

How Role-Based Access Control Works

This topic explains role-based access control (RBAC) when there is a trusted connection between NetWitness Server and a Core service.

In the RSA NetWitness® Suite, roles determine what users can do. A role has permissions assigned to it and you must assign a role to each user. The user then has permission to do what the role allows.

Pre-Configured Roles

To simplify the process of creating roles and assigning permissions, there are pre-configured roles in NetWitness Suite. You can also add roles customized for your organization.

The following table lists each pre-configured role and the permissions assigned to it. All permissions are assigned to the Administrators role. A subset of permissions is assigned to each of the other roles.

Role	Permission
Administrators	Full system access. The System Administrators persona is granted all permissions by default.
Operators	Access to configurations but not to meta and session content. The System Operators persona is focused on system configuration, but not Investigation, ESA, Alerting, Reporting, and Respond.
Analysts	Access to meta and session content but not to configurations. The Security Operation Center (SOC) Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Respond, but not system configuration.
Respond_ Administrator	Access to all Respond permissions.
SOC_ Managers	Same access as Analysts plus additional permission to handle incidents. The SOC Managers persona is identical to Analysts, but with permissions necessary to configure Respond.

Role	Permission
Malware_ Analysts	Access to investigations and malware events. The only access granted to the Malware Analysts persona is the Malware Analysis module.
Data_Privacy_ Officers	The Data Privacy Officer (DPO) persona is similar to Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system (see *Data Privacy Management*). Users with the DPO role can see which meta keys are flagged for obfuscation, and they also see obfuscated meta keys and values created for the flagged meta keys.

Trusted Connections Between Server and Service

In a trusted connection, a service explicitly trusts NetWitness Server to manage and authenticate users. This reduces administration on each service because authenticated users do not have to be defined locally in each Core service.

As the following table shows, you perform all user management tasks on the server.

Task	Location
Add a user	Server
Maintain usernames	Server
Maintain passwords	Server
Authenticate internal NetWitness Suite users	Server
(Optional) Authenticate external users with: - Active Directory - PAM	 Server Server
Install and configure PAM	Server

The benefits of a trusted connection and centralized user management are that:

- You perform all user administration tasks once, on NetWitness Server only.
- You control access to services but do not have to set up and authenticate users on the services.
- Users enter passwords once at NetWitness Suite logon and are authenticated by the server.
- Users, already authenticated by the server, access every Core service in ADMIN > Services without entering a password.

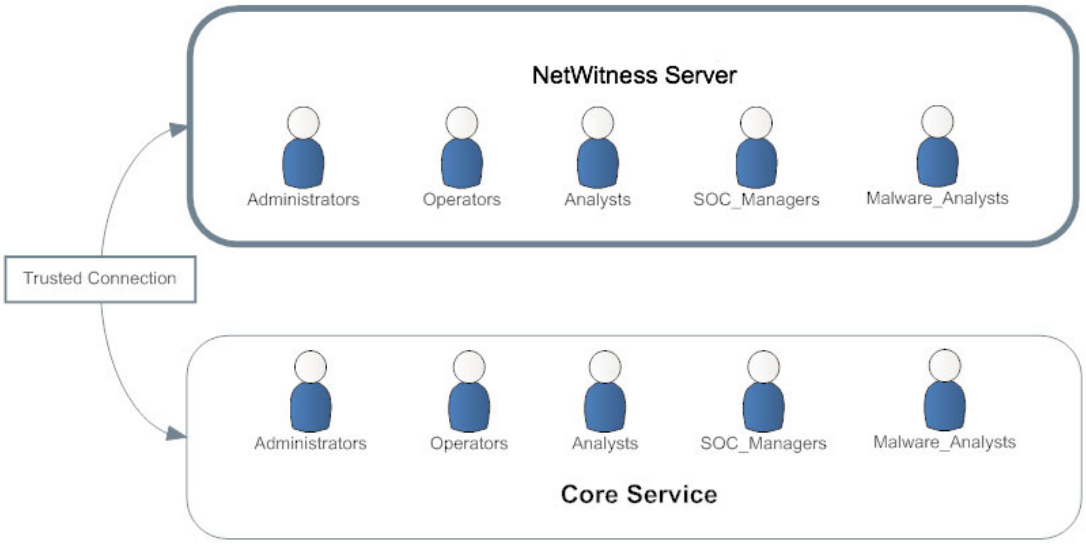
How Trusted Connections Are Established

When you install or upgrade to 11.0, trusted connections are established by default with two settings:

1. SSL is enabled.
2. The Core service is connected to an encrypted SSL port.

Common Role Names on the Server and Services

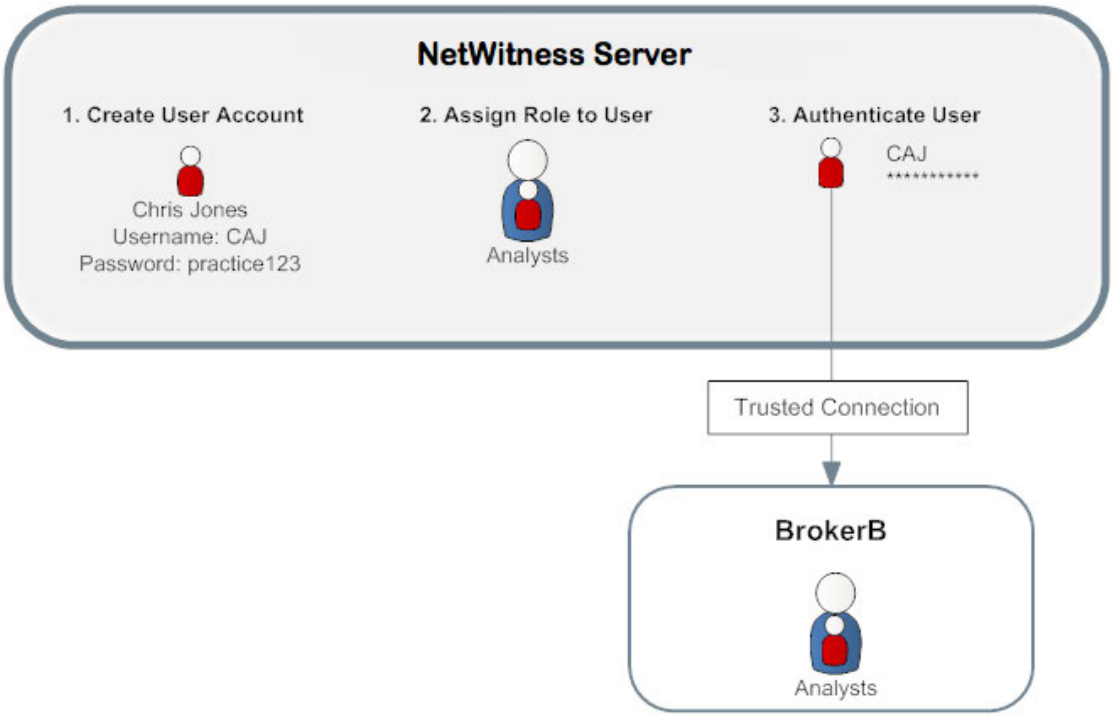
Trusted connections rely on common role names on the server and service. On a fresh installation, NetWitness Suite installs the five pre-configured roles on the server and each Core service.



If you add a custom role, such as JuniorAnalysts, you must add the role to each service, such as ArchiverA and BrokerB. Role names are case-senstive, cannot contain spaces and must be identical. For example, JuniorAnalyst (singular) and JuniorAnalysts (plural) do not meet the requirements for common role names.

End-to-End Workflow for User Setup and Service Access

This workflow shows how role-based access control works when there is a trusted connection between NetWitness Server and the service BrokerB.



1. On NetWitness Server, create an account for a new user:
   Name: Chris Jones
   Username: CAJ
   Password: practice123
2. Determine if you want to assign a pre-configured or custom role to Chris Jones:
   - **Pre-Configured role**
     a. Keep or modify the default permissions assigned to the **Analysts role,** which include permissions such as access to the Alerting, Investigation and Malware modules,
     b. Assign the Analysts role to Chris Jones.
   - **Custom role**
     a. Create the custom role, such as JuniorAnalysts.
     b. Assign permissions to the **JuniorAnalysts role**.

c. Assign the JuniorAnalysts role to Chris Jones.

d. Add the JuniorAnalysts role to the service, such as BrokerB.

3. The user, Chris Jones, logs on to NetWitness Server:
   Username: CAJ
   Password: practice123
4. The server authenticates Chris.
5. The trusted connection allows the authenticated user, Chris, to access BrokerB without entering another password.

For more detailed descriptions and procedures, see Manage Users with Roles and Permissions.

Related Topic

- Role Permissions

Role Permissions

This topic describes access to the user interface that users assigned to the built-in NetWitness Suite roles have by default.

Within NetWitness Suite, user access to each module, dashlet, and view is restricted based on the assigned permissions described in this topic. You can locate these role permissions in the Add or Edit Roles dialogs accessible from the Admin > Security > Roles tab.

In the Add or Edit Role dialogs, the tabs in the Permission section represent different areas of the NetWitness Suite and show the available permissions for those areas. For example, the Administration tab shows the permissions available in the Admin view.

Note: There is no Configure tab in the Add/Edit Role dialogs that corresponds to the Configure view. To assign permissions in the Configure view, assign permissions to the views contained within the Configure view: Live Content (Live), Incident Rules (Incidents), Respond Notifications (Incidents, Respond-server, Integration server), ESA Rules (Alerting), Subscriptions (Live), and Custom Feeds (Live).

Note: To the left of the Administration tab is a tab marked with an asterisk (*). This tab indicates access to management of backend services only.

The tables that follow show the default permissions assigned to each NetWitness Suite user role:

- Administrators
- Operators
- Analysts
- Respond Administrator
- SOC Managers (SOC Mgrs)
- Malware Analysts (MAs)
- Data Privacy Officers (DPOs)

Since the Administrators role has all of the permissions by default, it is not included in the tables.

Service Permissions Format for New Services

The service permissions for some new NetWitness Suite services contain three parts in the following format:

<service name>.<resource>.<action>

For example, for the **investigate-server.metrics.read** permission:

- service name = **investigate-server**
- resource = **metrics**
- action = **read**

Users assigned this permission can read any metrics that the investigate-server service exposes.

Administration

The following table lists the permissions in the Administration tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Administration Module	Yes	Yes	Yes	Yes	Yes
Access Health & Wellness	Yes	Yes	Yes	Yes	Yes
Apply System Updates	Yes				
Can Opt In to Live Intelligence Sharing	Yes				
Manage Advanced Settings	Yes				
Manage ATD Settings	Yes				
Manage Auditing	Yes				Yes
Manage Email	Yes				
Manage Global Auditing	Yes				Yes
Manage Health & Wellness Policy	Yes				
Manage LLS	Yes				
Manage Logs	Yes				Yes
Manage Notifications	Yes				
Manage Plugins	Yes				

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Manage Predicates	Yes				
Manage Reconstruction	Yes				
Manage Security	Yes				Yes
Manage Services	Yes				Yes
Manage System Settings	Yes				
Modify ESA Settings	Yes				
Modify Event Sources	Yes				
Modify Hosts	Yes				
Modify Services	Yes				Yes
View Event Sources	Yes		Yes		
View Health & Wellness Policy	Yes	Yes	Yes		
View Health & Wellness Stats Browser	Yes	Yes	Yes		Yes
View Hosts	Yes				Yes
View Services	Yes				Yes

Admin-server

The following table describes the permissions in the Admin-server tab. The Administrators role has all of the permissions and is the only role granted permissions by default.

Permission	Description
admin-server.configuration.manage	Permission to modify all service configuration parameters

Permission	Description
admin-server.health.read	Permission to view any health notifications that the service exposes
admin-server.logs.manage	Permission to change log-related configuration
admin-server.metrics.read	Permission to view any metrics that the service exposes
admin-server.process.manage	Permission to start and stop the service
admin-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
admin-server.security.read	Permission to view security-related resources

Alerting

The following table lists the permissions in the Alerting tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Alerting Module	Yes	Yes	Yes		Yes
Manage Rules			Yes		Yes
View Alerts	Yes	Yes	Yes		Yes
View Rules			Yes		Yes

Cloud-gateway-server

The following table describes the permissions in the Cloud-gateway-server tab. The Administrators role has all of the permissions and is the only role granted permissions by default.

Permission	Description
cloud-gateway-server.configuration.manage	Permission to modify all service cloud gateway parameters

Permission	Description
cloud-gateway-server.health.read	Permission to view any health notifications that the service exposes
cloud-gateway-server.logs.manage	Permission to change log-related configuration
cloud-gateway-server.metrics.read	Permission to view any metrics that the service exposes
cloud-gateway-server.process.manage	Permission to start and stop the service
cloud-gateway-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
cloud-gateway-server.security.read	Permission to view security-related resources
cloud-gateway-server.uploadstream.manage	Permission to edit uploadstream configuration settings
cloud-gateway-server.uploadstream.read	Permission to view uploadstream configuration settings

Config-server

The following table describes the permissions in the Config-server tab. The Administrators role has all of the permissions and is the only role granted permissions by default.

Permission	Description
config-server.*	All permissions (everything below)
config-server.configuration.manage	Permission to modify all service configuration parameters
config-server.health.read	Permission to view any health notifications that the service exposes

Permission	Description
config-server.logs.manage	Permission to change log-related configuration
config-server.metrics.read	Permission to view any metrics that the service exposes
config-server.process.manage	Permission to start and stop the service
config-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
config-server.security.read	Permission to view security-related resources

Contexthub-server

The following table describes the permissions in the Contexthub-server tab.

Permission	Description
contexthub-server.*	All permissions (everything below)
contexthub-server.configuration.manage	Permission to modify all service configuration parameters
contexthub-server.connection.manage	Permission to modify all connection settings
contexthub-server.connection.read	Permission to view all connection settings
contexthub-server.connectiontypes.read	Permission to view all configured connection types
contexthub-server.datasource.manage	Permission to modify data source settings
contexthub-server.datasource.read	Permission to view data source settings
contexthub-server.health.read	Permission to view any health notifications that the service exposes

Permission	Description
contexthub-server.listentries.manage	Permission to modify list entries
contexthub-server.logs.manage	Permission to change log-related configuration
contexthub-server.metrics.read	Permission to view any metrics that the service exposes
contexthub-server.process.manage	Permission to start and stop the service
contexthub-server.query.read	Permission to view queries
contexthub-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
contexthub-server.security.read	Permission to view security-related resources
contexthub-server.stix.read	Permission to view stix settings
contexthub-server.taxiidatasource.manage	Permission to modify settings for the taxii data source
contexthub-server.taxiidatasource.read	Permission to view settings for the taxii data source

The following table lists the permissions in the Contexthub-server tab assigned to each role. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
contexthub-server.*					Yes
contexthub-server.configuration.manage					
contexthub-server.connection.manage					
contexthub-server.connection.read		Yes	Yes	Yes	

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
contexthub-server.connectiontypes.read			Yes		
contexthub-server.datasource.manage		Yes	Yes	Yes	
contexthub-server.datasource.read		Yes	Yes	Yes	
contexthub-server.health.read					
contexthub-server.listentries.manage		Yes	Yes	Yes	
contexthub-server.logs.manage					
contexthub-server.metrics.read					
contexthub-server.process.manage					
contexthub-server.query.read		Yes	Yes	Yes	
contexthub-server.security.manage					
contexthub-server.security.read					
contexthub-server.stix.read		Yes	Yes	Yes	
contexthub-server.taxiidatasource.manage		Yes	Yes	Yes	
contexthub-server.taxiidatasource.read		Yes	Yes	Yes	

Dashboard

The following table lists the permissions in the Dashboard tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Admin Device List Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Admin Device Monitor Dashlet					Yes
Dashlet Access - Admin News Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Alert Variance Dashlet		Yes	Yes		Yes
Dashlet Access - Alerting Recent Alerts Dashlet		Yes	Yes		Yes
Dashlet Access - Investigation Jobs Dashlet		Yes	Yes		Yes
Dashlet Access - Investigation Top Values Dashlet		Yes	Yes		Yes
Dashlet Access - Live Featured Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live New Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live Subscriptions Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live Updated Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Malware Jobs Dashlet		Yes	Yes		Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Reporting Recent Report Dashlet		Yes	Yes		Yes
Dashlet Access - Reporting Charts Dashlet		Yes	Yes		Yes
Dashlet Access - Top Alerts Dashlet		Yes	Yes		Yes
Dashlet Access - Unified RSA First Watch Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Unified Shortcuts Dashlet	Yes	Yes	Yes		Yes

Endpoint-server

The following table describes the permissions in the Endpoint-server tab. The Administrators role has all of the permissions by default.

Permission	Description
endpoint-server*	All permissions (everything below)
endpoint-server.agent.manage	Permission to download and manage agent packager configuration
endpoint-server.agent.read	Permission to view the agent packager configuration
endpoint-server.ca.manage	Permission to generate and download the agent packager
endpoint-server.ca.read	Permission to generate and download the agent packager
endpoint-server.configuration.manage	Permission to modify all endpoint configuration parameters
endpoint-server.dataretention.manage	Permission to configure the data retention policy

Permission	Description
endpoint-server.dataretention.read	Permission to view the data retention policy
endpoint-server.filter.manage	Permission to delete filters
endpoint-server.filter.read	Permission to view filters
endpoint-server.health.read	Permission to view any health notifications that the service exposes
endpoint-server.logs.manage	Permission to change log-related configuration
endpoint-server.machine.manage	Permission to delete hosts
endpoint-server.machine.read	Permission to view hosts
endpoint-server.metrics.read	Permission to view any metrics that the service exposes
endpoint-server.policy.manage	Permission to update and save schedule scan configuration
endpoint-server.policy.read	Permission to view existing schedule scan configuration
endpoint-server.process.manage	Permission to start and stop the service
endpoint-server.scan.manage	Permission to perform endpoint scan
endpoint-server.scan.read	Permission to view endpoint scan data
endpoint-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
endpoint-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Endpoint-server tab assigned to each role. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
endpoint-server*	Yes				
endpoint-server.agent.manage					
endpoint-server.agent.read					
endpoint-server.ca.manage					
endpoint-server.ca.read					
endpoint-server.configuration.manage					
endpoint-server.dataretention.manage					
endpoint-server.dataretention.read					
endpoint-server.filter.manage		Yes			
endpoint-server.filter.read		Yes			
endpoint-server.health.read					
endpoint-server.logs.manage					
endpoint-server.machine.manage		Yes			
endpoint-server.machine.read		Yes			
endpoint-server.metrics.read					
endpoint-server.policy.manage	Yes				
endpoint-server.policy.read	Yes				
endpoint-server.process.manage					
endpoint-server.scan.manage		Yes			

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
endpoint-server.scan.read		Yes			
endpoint-server.security.manage					
endpoint-server.security.read					

Esa-analytics-server

The following table describes the permissions in the Esa-Analytics-server tab. The Administrators and Operators roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
esa-analytics-server.*	All permissions (everything below)
esa-analytics-server.analytics.manage	Permission to modify ESA analytics
esa-analytics-server.analytics.read	Permission to view ESA analytics
esa-analytics-server.configuration.manage	Permission to modify all service configuration parameters
esa-analytics-server.health.read	Permission to view any health notifications that the service exposes
esa-analytics-server.logs.manage	Permission to change log-related configuration
esa-analytics-server.metrics.read	Permission to view any metrics that the service exposes
esa-analytics-server.model.manage	Permission to modify ESA models
esa-analytics-server.model.read	Permission to view ESA models
esa-analytics-server.process.manage	Permission to start and stop the service

Permission	Description
esa-analytics-server.security.manage	Permission to modify security-related resources
esa-analytics-server.security.read	Permission to view security-related resources

Incidents

The following table lists the permissions in the Incidents tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Incident Module		Yes	Yes	Yes	Yes
Configure Incident Management Integration			Yes		Yes
Delete Alerts and incidents					Yes
Manage Alert Handling Rules			Yes		Yes
View and Manage Incidents		Yes	Yes	Yes	Yes

Integration-server

(The Integration-server permissions are available in NetWitness Suite version 11.1 and later.)

The following table describes the permissions in the Integration-server tab.

Permission	Description
integration-server.*	All permissions (everything below)
integration-server.api.access	Permission to authorize external requests from 3rd party applications
integration-server.configuration.manage	Permission to view and modify all service integration configuration parameters

Permission	Description
integration-server.health.read	Permission to read any health notifications that the service exposes
integration-server.logs.manage	Permission to change log-related integration configurations
integration-server.metrics.read	Permission to read any metrics that the service exposes
integration-server.notification.manage	Permission to change global notification configurations (for example, SMTP server)
integration-server.notification.read	Permission to read global notification configurations (for example, SMTP server)
integration-server.notification.send	Permission to send notifications (for example, Email)
integration-server.process.manage	Permission to start and stop the service
integration-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
integration-server.security.read	Permission to read security-related resources
integration-server.template.manage	Permission to change notification template
integration-server.template.read	Permission to read notification template

The following table lists the permissions in the Integration-server tab assigned to each role. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
integration-server.*					Yes
integration-server.api.access					
integration-server.configuration.manage					
integration-server.health.read					
integration-server.logs.manage					
integration-server.metrics.read					
integration-server.notification.manage	Yes		Yes		
integration-server.notification.read	Yes		Yes		
integration-server.notification.send	Yes		Yes		
integration-server.process.manage					
integration-server.security.manage					
integration-server.security.read					
integration-server.template.manage	Yes		Yes		
integration-server.template.read	Yes		Yes		

Investigate

The following table lists the permissions in the Investigate tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Investigation Module		Yes	Yes	Yes	Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Context Lookup		Yes	Yes	Yes	
Create Incidents from Investigation		Yes	Yes	Yes	
Manage List from Investigation		Yes	Yes	Yes	
Navigate Events		Yes	Yes	Yes	Yes
Navigate Values		Yes	Yes	Yes	Yes

Investigate-server

The following table describes the permissions in the Investigate-server tab. The Administrators, Analysts, SOC Managers, Malware Analysts, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
investigate-server.*	All permissions (everything below) for the Event Analysis view
investigate-server.configuration.manage	Permission to change any configuration properties for the service
investigate-server.content.export	Permission to export content from the service
investigate-server.content.reconstruct	Permission to view the summary view, the packet, packet map, text, log, and file reconstructions, as well as the packet count
investigate-server.event.read	Permission to view events that the service exposes
investigate-server.health.read	Permission to view any health notifications that the service exposes
investigate-server.logs.manage	Permission to change log-related configuration

Permission	Description
investigate-server.metagroup.manage	Permission to manage meta groups
investigate-server.metagroup.read	Permission to view and use meta groups
investigate-server.metrics.read	Permission to view any metrics that the service exposes
investigate-server.process.manage	Permission to start and stop the service
investigate-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
investigate-server.security.read	Permission to view security-related resources

Live

The following table lists the permissions in the Live tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Live					
Access Live Module	Yes	Yes	Yes		Yes
Manage Live System Settings	Yes				
Resources					
Deploy Live Resources	Yes				Yes
Manage Live Feeds	Yes				Yes
Manage Live Resources	Yes				Yes
Search Live Resources	Yes	Yes	Yes		Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
View Live Resource Details	Yes	Yes	Yes		Yes

Malware

The following table lists the permissions in the Malware tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Download Malware File(s)		Yes	Yes	Yes	Yes
Initiate Malware Analysis Scan		Yes	Yes	Yes	Yes
View Malware Analysis Events		Yes	Yes	Yes	Yes

Orchestration-server

The following table describes the permissions in the Orchestration-server tab. The Administrators, Operators, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
orchestration-server.*	All permissions (everything below)
orchestration-server.configuration.manage	Permission to modify all service configuration parameters
orchestration-server.file.read	Permission to view files
orchestration-server.health.read	Permission to view any health notifications that the service exposes
orchestration-server.logs.manage	Permission to change log-related configuration
orchestration-server.metrics.read	Permission to view any metrics that the service exposes
orchestration-server.process.manage	Permission to start and stop the service

Permission	Description
orchestration-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
orchestration-server.security.read	Permission to view security-related resources

Reports

The following table lists the permissions in the Reports tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Alert					
Define RE Alert		Yes	Yes		Yes
Export RE Alert Definition		Yes	Yes		Yes
Manage RE Alerts		Yes	Yes		Yes
View RE Alerts		Yes	Yes		Yes
View Scheduled RE Alerts		Yes	Yes		Yes
Chart					
Define Chart		Yes	Yes		Yes
Delete Chart		Yes	Yes		Yes
Export Chart Definition		Yes	Yes		Yes
Manage Charts		Yes	Yes		Yes
View Charts		Yes	Yes		Yes
List					
Define Lists		Yes	Yes		Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Delete List		Yes	Yes		Yes
Export List		Yes	Yes		Yes
Manage Lists		Yes	Yes		Yes
Report					
Define Report		Yes	Yes		Yes
Delete Report		Yes	Yes		Yes
Export Report		Yes	Yes		Yes
Manage Reports		Yes	Yes		Yes
View Reports		Yes	Yes		Yes
Reports					
Access Configure		Yes	Yes		Yes
Access Reporter Module		Yes	Yes		Yes
Access Reporter search		Yes	Yes		Yes
Access View		Yes	Yes		Yes
Rule					
Add RE Alert Definition from Rule		Yes	Yes		Yes
Define Rule		Yes	Yes		Yes
Delete Rule		Yes	Yes		Yes
Export Rule		Yes	Yes		Yes
Manage Rules		Yes	Yes		Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
View Rule Usage		Yes	Yes		Yes
Schedules					
Define Schedule		Yes	Yes		Yes
Delete Schedule		Yes	Yes		Yes
View Schedules		Yes	Yes		Yes
Warehouse Analytics					
Define Jobs		Yes	Yes		Yes
Delete Jobs		Yes	Yes		Yes
Manage Jobs		Yes	Yes		Yes
View Jobs		Yes	Yes		Yes

Respond-server

The following table describes the permissions in the Respond-server tab.

Permission	Description
respond-server.*	All permissions (everything below)
respond-server.alert.delete	Permission to delete alerts
respond-server.alert.manage	Permission to create, update, or delete alerts
respond-server.alert.read	Permission to view alerts
respond-server.alertrule.manage	Permission to create, update, or delete alert aggregation rules
respond-server.alertrule.read	Permission to view alert aggregation rules

Permission	Description
respond-server.configuration.manage	Permission to change any configuration properties for the service
respond-server.health.read	Permission to view any health notifications that the service exposes
respond-server.incident.delete	Permission to delete incidents
respond-server.incident.manage	Permission to create, update, or delete incidents
respond-server.incident.read	Permission to view incidents
respond-server.journal.manage	Permission to create, update, or delete journal entries for an incident
respond-server.journal.read	Permission to view journal entries for an incident
respond-server.logs.manage	Permission to change log-related configuration
respond-server.metrics.read	Permission to view any metrics that the service exposes
respond-server.notification.manage	(This permission is available in NetWitness Suite version 11.1 and later.) Permission to configure Respond notification settings such as the selected email server, SOC Managers, and who will be sent the notifications (Assignee and SOC Managers).
respond-server.notification.read	(This permission is available in NetWitness Suite version 11.1 and later.) Permission to view Respond notification settings.
respond-server.process.manage	Permission to start and stop the service

Permission	Description
respond-server.remediation.manage	Permission to create, update, or delete remediation tasks
respond-server.remediation.read	Permission to view remediation tasks
respond-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
respond-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Respond-server tab assigned to each role. The Administrators and Respond Administrator roles have all of the permissions by default and are not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
respond-server.*					Yes
respond-server.alert.delete					
respond-server.alert.manage		Yes	Yes	Yes	
respond-server.alert.read		Yes	Yes	Yes	
respond-server.alertrule.manage			Yes		
respond-server.alertrule.read			Yes		
respond-server.configuration.manage					
respond-server.health.read					
respond-server.incident.delete					
respond-server.incident.manage		Yes	Yes	Yes	

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
respond-server.incident.read		Yes	Yes	Yes	
respond-server.journal.manage		Yes	Yes	Yes	
respond-server.journal.read		Yes	Yes	Yes	
respond-server.logs.manage					
respond-server.metrics.read					
respond-server.notification.manage			Yes		
respond-server.notification.read			Yes		
respond-server.process.manage					
respond-server.remediation.manage		Yes	Yes	Yes	
respond-server.remediation.read		Yes	Yes	Yes	
respond-server.security.manage					
respond-server.security.read					

Respond Notification Settings Permissions

(The Respond notification setting permissions are available in NetWitness Suite version 11.1 and later.)

Note: If you are updating from NetWitness Suite version 11.0 to 11.1, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. For all upgrades to 11.1, you will need to add additional permissions to custom roles.

The following permissions are required for Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (CONFIGURE > Respond Notifications).

Incidents tab:

- Configure Incident Management Integration

Respond-server tab:

- respond-server.notification.manage
- respond-server.notification.read

Integration-server tab:

- integration-server.notification.read
- integration-server.notification.manage

Security-server

The following table describes the permissions in the Security-server tab. The Administrators, Operators, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
security-server.*	All permissions (everything below)
security-server.account.manage	Permission to view, create, modify, or remove NetWitness Suite local accounts
security-server.account.read	Permission to view NetWitness Suite local accounts
security-server.ca.manage	Permission to manage NetWitness Suite deployment PKI parameters (for example, sign certificates, and so on)
security-server.ca.read	Permission to view NetWitness Suite deployment PKI parameters
security-server.configuration.manage	Permission to modify all service configuration parameters
security-server.health.read	Permission to view any health notifications that the service exposes
security-server.logs.manage	Permission to change log-related configuration
security-server.metrics.read	Permission to view any metrics that the service exposes

Permission	Description
security-server.permission.manage	Permission to create or remove NetWitness Suite permissions
security-server.process.manage	Permission to start and stop the service
security-server.role.manage	Permission to create, modify, or remove NetWitness Suite roles (for example, add role permissions)
security-server.role.read	Permission to view NetWitness Suite role definitions
security-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
security-server.security.read	Permission to view security-related resources
security-server.user.manage	Permission to view, create, modify, or remove NetWitness Suite user profiles
security-server.user.read	Permission to view NetWitness Suite user profile details (for example, roles, login times, and so on)

Manage Users with Roles and Permissions

This topic introduces a set of end-to-end procedures for managing users in NetWitness Suite. These steps explain how to add a user in NetWitness Suite and then how to control what the user can do.

Topics

- Step 1. Review the Pre-Configured NetWitness Roles
- Step 2. (Optional) Add a Role and Assign Permissions
- Step 3. Verify Query and Session Attributes per Role
- Step 4. Set Up a User
- Step 5. (Optional) Map User Roles to External Groups

Step 1. Review the Pre-Configured NetWitness Roles

To simplify the process of creating roles and assigning permissions, there are pre-configured roles in NetWitness Suite.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to meta and session content
Analysts	Access to meta and session content but not to configurations
Respond_ Administrator	Access to all Respond server and Incidents permissions
SOC_ Managers	Same access as Analysts plus additional permission to handle incidents
Malware_ Analysts	Access to malware events and to meta and session content
Data_Privacy_ Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).

The administrator can also add custom roles.

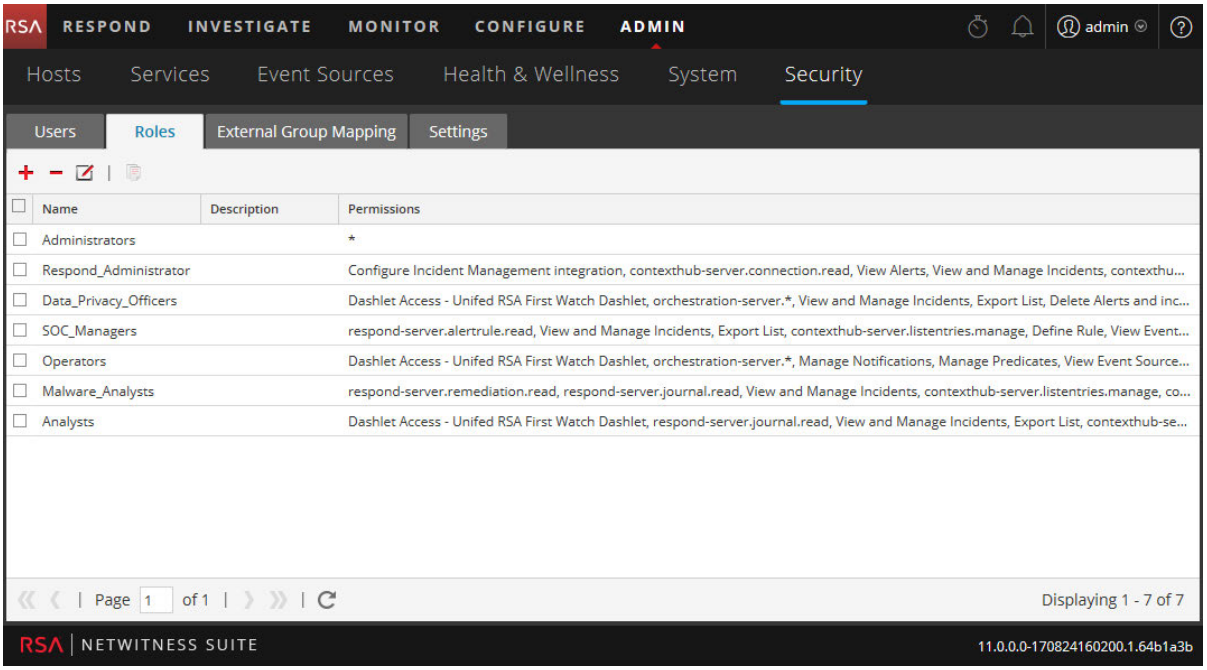
Step 2. (Optional) Add a Role and Assign Permissions

Although NetWitness Suite has pre-configured roles, you can add custom roles. For example, in addition to the pre-configured Analysts role you could add custom roles for AnalystsEurope and AnalystsAsia. For a detailed list of permissions, see Role Permissions.

Each of the following procedures starts on the **Roles** tab.

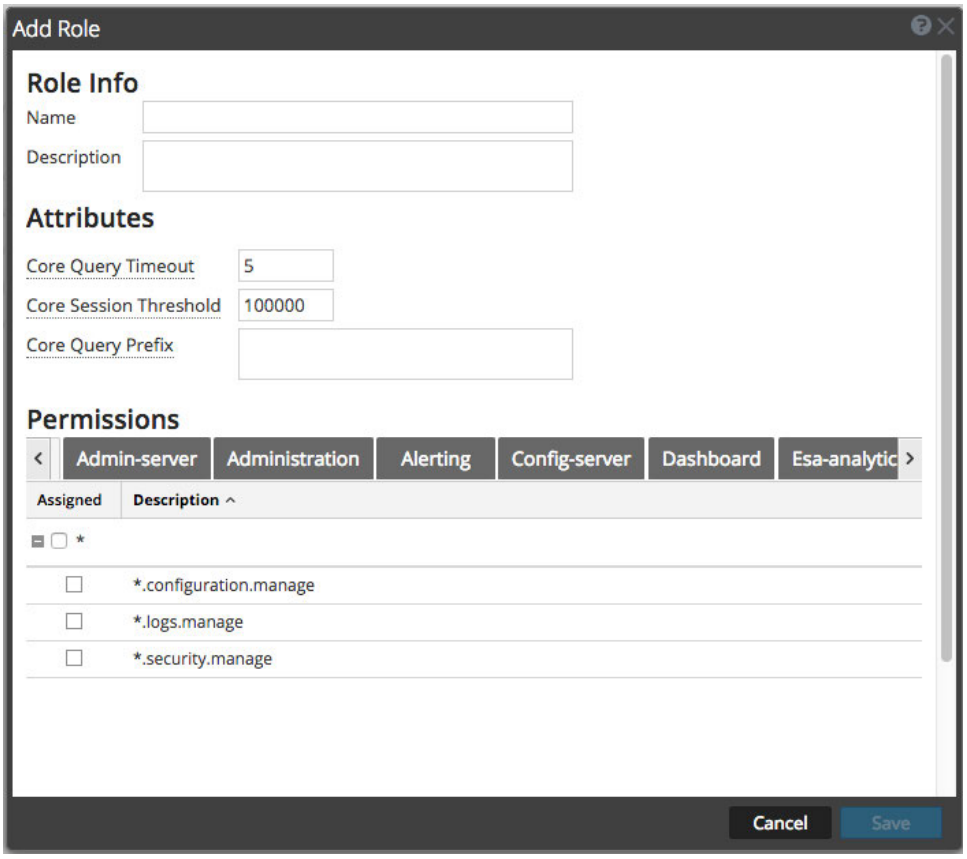
To navigate to the Roles tab:

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Roles** tab.



Add a Role and Assign Permissions

1. In the **Roles** tab, click ✚ in the toolbar.
2. The **Add Role** dialog is displayed.



3. In the **Role Info** section, type the following information for the role:
   - **Name**
   - (Optional) **Description**
4. In the **Attributes** section, enter the desired values for each attribute. For more information on attributes, see Step 3. Verify Query and Session Attributes per Role.
5. In the **Permissions** section:
   - Click ‹ and › to scroll through the modules.
   - Select a module the role will access.
   - Select each permission the role will have.

5. Repeat the previous step until you select all permissions to assign to the role.
6. Click **Save** to add the new role, which is effective immediately. You can now assign the new role to users.

Duplicate a Role

An efficient way to add a new role is to duplicate a similar role, save it with a new name and revise the permissions that are already assigned.

1. In the **Roles** tab, select the role you want to duplicate and click .
2. Type a new role name and click **Save**.
3. To change the permissions, follow the steps in the next procedure.

Change Permissions Assigned to a Role

1. In the **Roles** tab, select the role and click .
   The **Edit Role** dialog is displayed.
2. In the **Permissions** section:
   - Click and to scroll through the modules.
   - Select a module to revise permissions for it.
   - Select or deselect each permission.
3. Repeat the previous step until the role has the required permissions.
4. Click **Save**. The revised permissions are effective immediately.

Delete a Role

You can delete a role if it is not assigned to any users.

1. In the **Roles** tab, select the role and click .
2. A dialog requests confirmation that you want to delete the role. Click **Yes**.

Step 3. Verify Query and Session Attributes per Role

This topic explains the query and session attributes and provides instructions for setting these attributes for user roles. This topic also describes how these role settings impact individual user settings and what happens if a user is a member of multiple roles.

After you define your user roles, it is important to verify the query and session attributes that are set for each role. You can adjust these settings according to your requirements.

Query and Session Attributes

Query and session attributes determine how to handle the queries that a user runs. These attributes enable you to lock down the information that users can retrieve. These attributes apply to all sessions of users assigned to a role.

Depending on your requirements, you can specify the following query-handling attributes for a user role:

- **Core Query Timeout** is an optional setting that applies to NetWitness Suite Core services. It specifies the maximum number of minutes that a user can run a query. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout. The default value is 5 minutes.
- **Core Session Threshold** is a required setting. This value must be zero (0) or greater. The default is 100000. The limit you specify here overrides the **Max Session Export** value defined in the Investigate view settings. If the threshold is greater than zero, a query optimization will extrapolate the total session counts that exceed the threshold. When the meta value count returned by the query reaches the threshold, the system will:
  - Stop its determination of the session count.
  - Show the threshold and percentage of query time used to reach the threshold.
- **Core Query Prefix** is an optional filter applied to queries the user runs. The prefix restricts query results that the user sees. For example, the `'service' = 80` query prefix is prepended to any queries run by the user, and the user can only access metadata of HTTP sessions.

Note: In Version 11.1 and later, you can use configured meta entities in a Core Query Prefix. For additional information about configuring meta entities, refer to the *Core Database Tuning Guide*.

The query-handing attribute settings applied for a user depend on the role memberships of the user. It is important to verify the query-handling attribute settings for your roles.

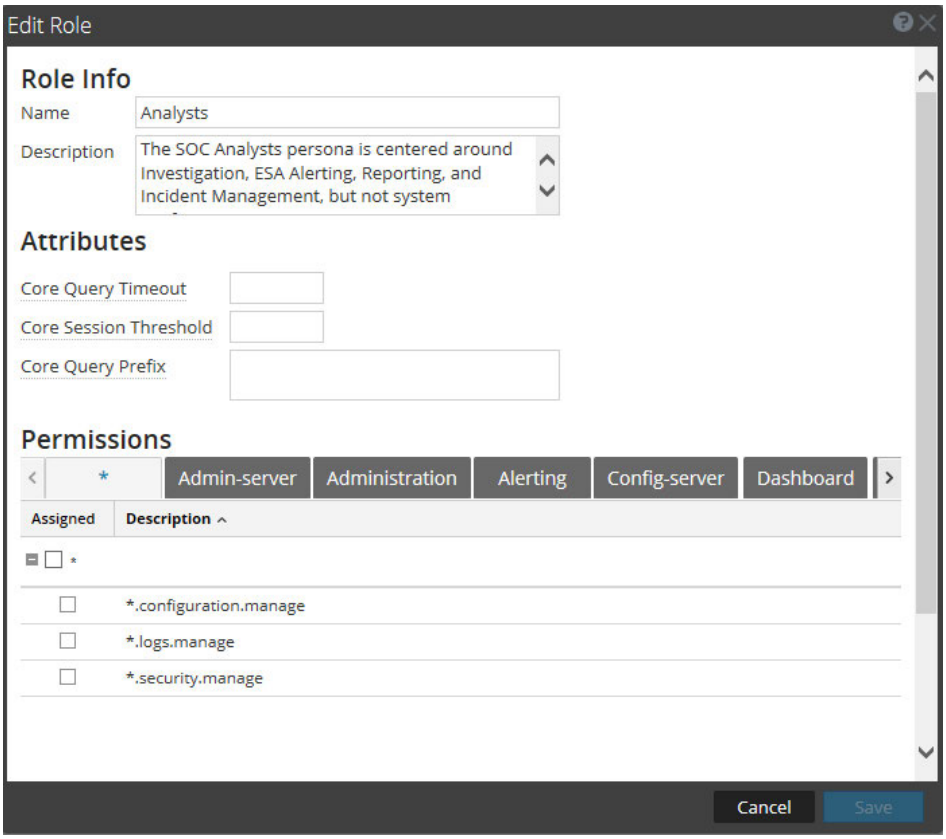
How Query-Handling Attribute Settings Apply to Individual Users

If a user is a member of multiple roles, the following logic applies for the user:

- **Query Timeout:** The most permissive (highest) value of all assigned roles is applied to the user.
- **Query Prefix:** The query prefixes of each of the user roles are AND'd together.
- **Session Threshold:** The highest value of all the assigned roles is applied to the user.

Set Query Handling Attributes for a User Role

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Roles** tab. If you are adding a role, click . If you are editing a role, select the role and click .
   The Add or Edit Role dialog is displayed.



3. To set the attributes for the role, in the **Attributes** section:
   - (Optional) In the **Core Query Timeout** field, type the maximum number of minutes that a user can run a query. This timeout applies to queries performed from Investigate.
   - Type a **Core Session Threshold** for the system to stop its determination of the session count.
   - (Optional) Type a **Core Query Prefix** to filter query results that role members see in the Investigate Navigate view, Events view, and Event Analysis view. You can specify a query that is prepended to all queries executed by users with a specific role. For example, if the `'service' = 80` query prefix is prepended to all queries by users in this role, the users can only access metadata of HTTP sessions. If users attempt to navigate to non-HTTP event, the view is not displayed.
4. Click **Save.**

Step 4. Set Up a User

This topic introduces procedures to set up a new user.

Topics

- Add a User and Assign a Role
- Enable, Unlock, and Delete User Accounts

Add a User and Assign a Role

This topic explains how to add a new user to each type of user account, local and external. It also explains how to assign a role to a local user.

All NetWitness Suite users must have a local or external user account.

The following considerations are important when managing local and external user accounts.

Local User Account	External User Account
Managed within NetWitness Suite	Managed externally and outside the scope of this document
Roles assigned directly	Roles assigned by external group mapping
Derives permissions from each role assigned to the user, as explained in this topic	Derives permissions from each role mapped to the account's external user group, as explained in Step 5. (Optional) Map User Roles to External Groups.
NetWitness Suite manages all user information.	NetWitness Suite manages user identification only. This includes Username, Full Name and Email.

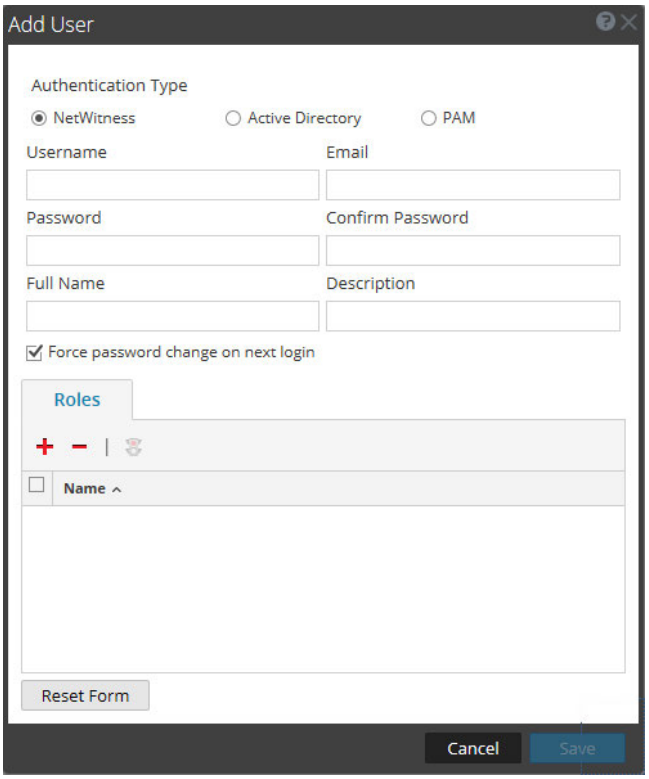
Procedures

Each of the following procedures starts on the Users tab. To navigate to the Users tab, go to **ADMIN > Security**. The Security view is displayed with the Users tab open.

Add a User and Assign a Role

To add a local user account and assign a role to the user:

1. In the **Users** tab, click + in the toolbar.
   The **Add User** dialog is displayed.



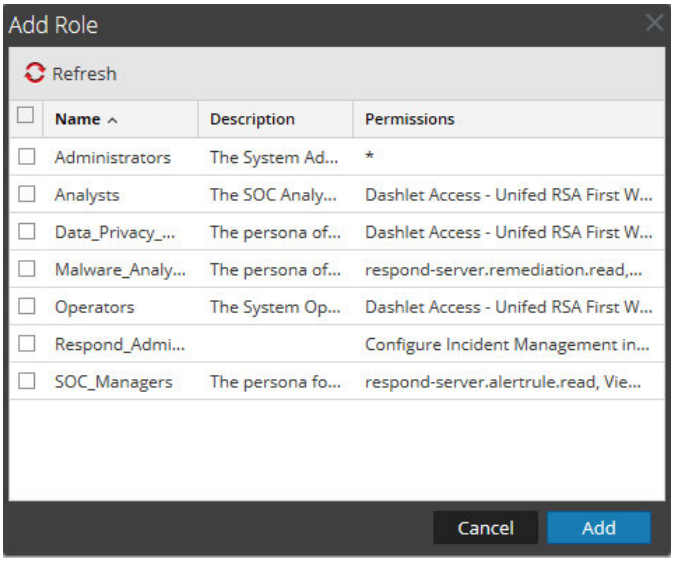
2. Type the following account information for the new user:
   - **Authentication Type**: **NetWitness** is selected by default and is the correct choice when adding a local user. This option is only displayed when there are AD or PAM configurations set up to allow for selecting that authentication type. If there are no AD or PAM configurations, the authentication type is set to NetWitness automatically and there are no other options available.
   - **Username** for logging on to NetWitness Suite
   - **Email** address
   - Password for logging on to NetWitness Suite, in the **Password** and **Confirm Password** fields
   - **Full Name** of the new user
   - (Optional) **Description** of the user account
3. To expire the user password the next time the user logs on, select **Force password change on next login**.

   This does not affect any active user sessions. The appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is

cleared the next time you edit the user account.

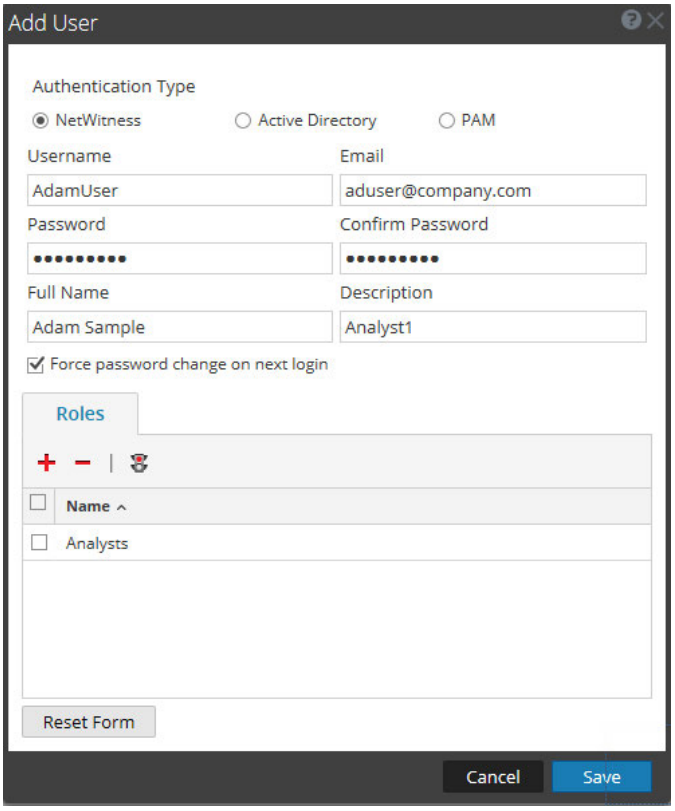
4. To assign a role to the user, click + in the **Roles** tab.

   The **Add Role** selection dialog shows the list of available roles.



5. Select each role to assign and click **Add**.

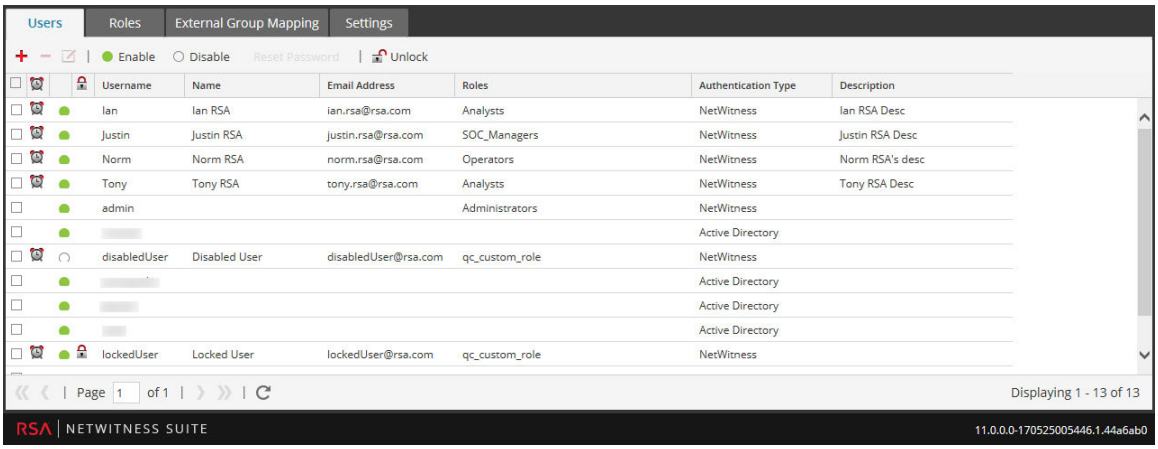
   The **Add User** dialog shows each role assigned to the user.



6. (Optional) Select a role and click to **Show all permissions** for the role.

7. Click **Save**.

   The **Users** tab shows the new user and each role assigned to the user. The account is active immediately.



Add a User for External Authentication

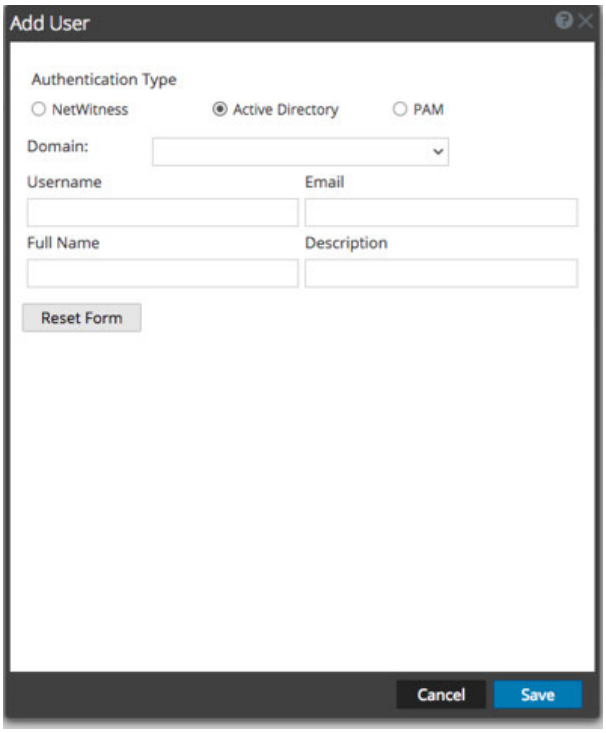
Prerequisite: External authentication must be configured. Refer to Step 4. (Optional) Configure External Authentication.

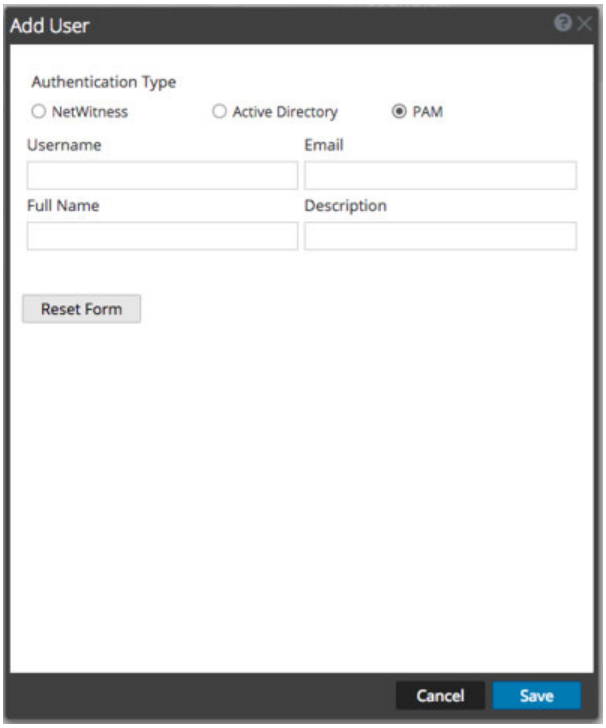
To add a user that is authenticated externally, outside of NetWitness Suite:

1. In the **Users** tab, click + in the toolbar.

   The **Add User** dialog is displayed.

2. For **Authentication Type**, select either **Active Directory** or **PAM**. The dialog will update to show the required fields for the selected external authentication type.





3. Type the following information:

   - **Domain** (if select Active Directory authentication only): Select the Active Directory domain for the user from the drop-down list of available domains.

- **Username** for logging on to NetWitness Suite
- **Email** address
- **Full Name** of the new user
- (Optional) **Description** of the user account

4. Click **Save**. The Users tab shows the new user account, which still needs a role and permissions.
5. To map a role to the new user, see Step 5. (Optional) Map User Roles to External Groups.

Change User Information or Roles

To change a user's account information or assigned roles:

1. In the **Users** tab, select a user and click in the toolbar.
   The **Edit User** dialog is displayed.
2. To edit user information, change any of the following fields:
   - **Email**
   - **Full Name**
   - **Description**
3. To expire the **internal** user password the next time the user logs on, select **Force password change on next login**.
   This does not affect any active user sessions. The appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is cleared the next time you edit the user account.
4. In the **Roles** section:
   - To assign another role, click , select a role and click **Add**.
   - To remove an assigned role, select the role and click .
7. Click **Save**.

Delete a User

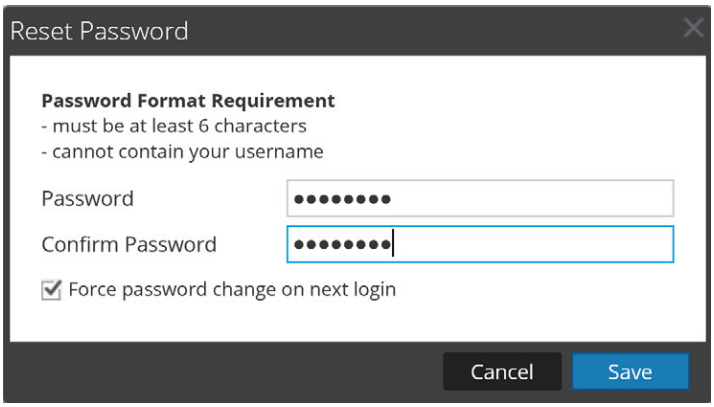
1. In the **Users** tab, select a user.
2. In the toolbar, click .

3. Click **Save**.

Note: To fully delete a user that is externally authenticated by Active Directory, you must also delete the user from the AD Group.

Reset a User Password

1. In the **Users** tab, select a user.
2. In the toolbar, click **Reset Password**.



The **Password Format Requirement** section lists the specific requirements for the password. Administrators can adjust these requirements for all internal users in the password policy. See Step 1. Configure Password Complexity.

3. Choose whether to force a password change the next time the user logs in to NetWitness Suite.
4. Click **Save**.

Enable, Unlock, and Delete User Accounts

This topic provides instructions for enabling, unlocking, and deleting user accounts.

All users of NetWitness Suite must either have a local user account with username and password or have an external user account. Within NetWitness Suite, you can enable, disable, and delete local user accounts.

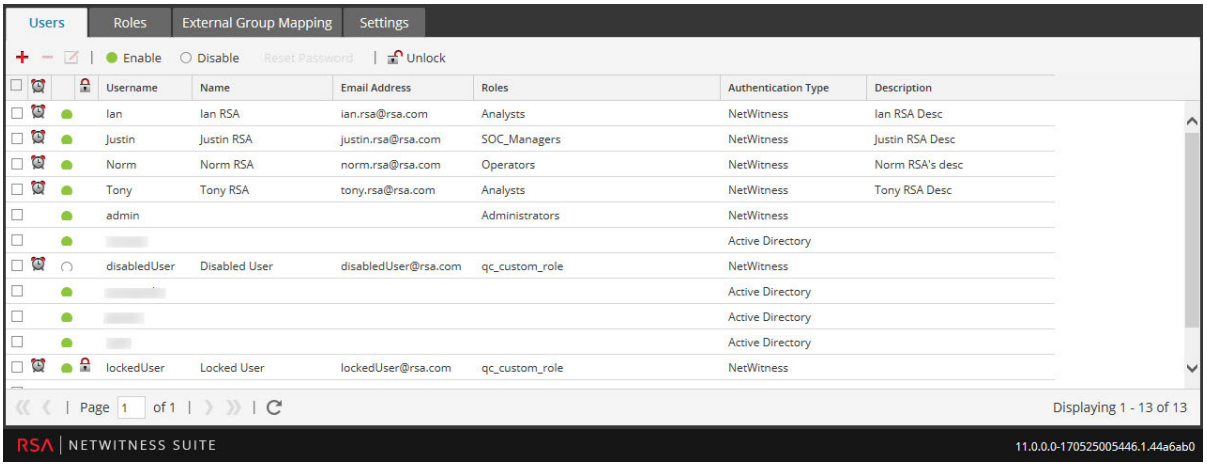
The first time an external user logs into NetWitness Suite, a new user entry is automatically created with NetWitness Suite. NetWitness Suite manages only user identification information; for example, Full Name and Email.

You can unlock locked accounts for both local and external users.

Enable Disabled NetWitness Suite User Accounts

To enable NetWitness Suite user accounts that have been disabled:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.



2. In the **Users** grid, select one or more accounts.
3. Click Enable.
   A dialog requests confirmation.
4. If you want to enable the accounts, click **Yes**.
   The accounts are enabled, and the user can log in to NetWitness Suite.

Disable NetWitness Suite User Accounts

You can block user access by disabling users. Disabling the user does not delete user preferences. This action blocks user access without deleting user preferences so that upon re-enabling users, user preferences are intact. You can re-enable users to restore user access. Disabling users applies only to Local users and not External Users.

To disable NetWitness Suite user accounts:

1. In the **Users** grid, select one or more accounts.
2. Click Disable.

   A dialog requests confirmation.
3. If you want to disable the accounts, click **Yes**.

   The accounts are disabled, and the user can no longer log in to NetWitness Suite.

Unlock Locked NetWitness Suite User Accounts

A user is locked out for a period of time after a number of failed consecutive login attempts. To unlock NetWitness Suite user accounts that are locked due to excessive failed login attempts:

1. In the **Users** grid, select one or more accounts.
2. Click Unlock.

   A dialog requests confirmation.
3. If you want to unlock the accounts, click **Yes**.

   The accounts are unlocked, and the user can log on to NetWitness Suite.

Delete NetWitness Suite User Accounts

If not using External Authentication, a user can log on to NetWitness Suite using a local account. These local accounts are directly managed using NetWitness Suite. To revoke access to a local user, either disable the account or delete the account completely from the system.

Note: This deletes all user preferences for the account from NetWitness Suite. If this is not the intention, disable the user instead of deleting the user.

To delete NetWitness Suite user accounts:

1. Go to **ADMIN > Security**.

   The Security view is displayed with the **Users** tab open.
2. In the Users list, select one or more accounts.
3. Click −.

   A warning dialog requests confirmation.
4. If you want to delete the accounts, click **Yes**.

   The accounts are removed from NetWitness Suite, and the users can no longer log in to NetWitness Suite.

Step 5. (Optional) Map User Roles to External Groups

This topic describes the method for mapping NetWitness Suite user roles to external groups.

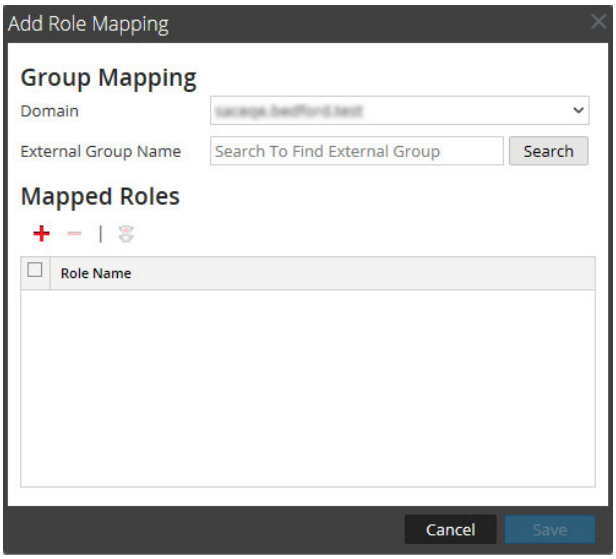
In NetWitness Suite, external groups derive permissions for various modules and views from NetWitness Suite user roles, which have permissions assigned to them. To provide access to an external group, map user roles to it. To modify an external group's access, edit the roles mapped to it. Add and delete roles until the external group has the necessary access. Changes take effect immediately.

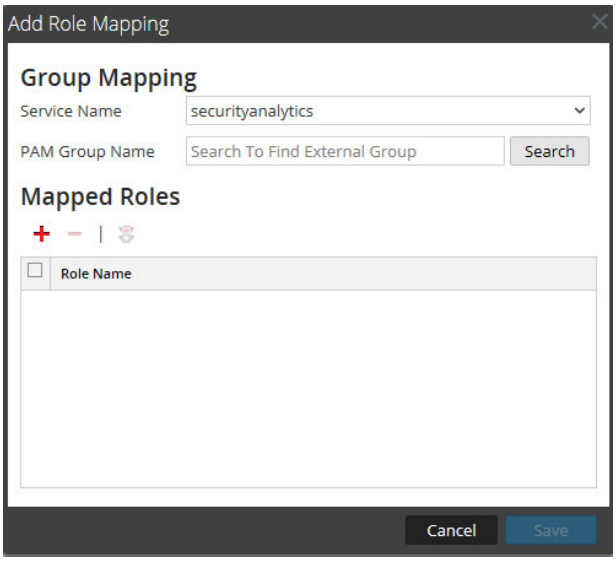
Prerequisites

In the Settings tab, you must set up a method for external user authentication to make external groups visible to NetWitness Suite.

Add Role Mapping for an External Group

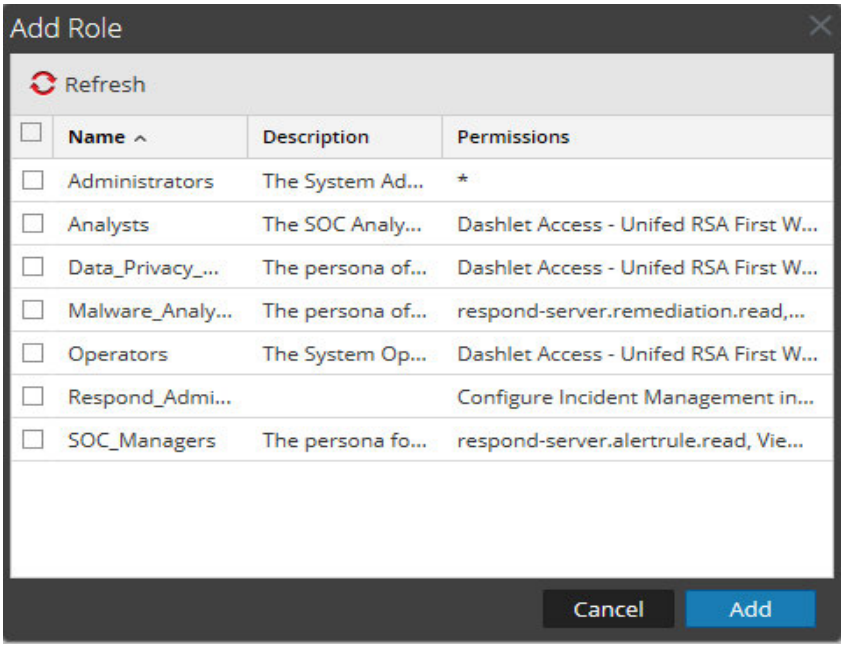
1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.
   The **Add Role Mapping** dialog for the external authentication method you selected is displayed.





4. Click **Search** and search for an external group name in the Search for External Groups, then select an external group name.

5. To add roles to the group mapping, click + in the **Mapped Roles** section.
   The **Add Role** dialog is displayed.



6. Click the checkbox in the title bar to select all roles, or select roles individually.
7. To add the roles to the **Mapped Roles** section in the Add Role Mapping dialog, click **Add**.
   The dialog closes and the selected roles are displayed in the Mapped Roles section.
8. If you want to delete roles from the **Mapped Roles** section, select the roles and click −.
9. When the **Add Role Mapping** dialog reflects the role mapping that you want to define for the group, click **Save**.
   The Add Role Mapping dialog closes, and the new role mapping is listed in the External Group Mapping tab list.

Edit Role Mapping for a Group

1. In the **External Group Mapping** action bar, click **Edit**.
   The **Edit Role Mapping** dialog is displayed with the group name in the **External Group Name** field.
2. To add roles to the mapping, click + in the **Mapped Roles** section.
   The Add Role dialog is displayed.
3. Click the checkbox in the title bar to select all roles, or select roles individually.
4. To add the roles to the **Mapped Roles** section in the **Add Role Mapping** dialog, click **Add**.
   The dialog closes, and the selected roles are displayed in the Mapped Roles section.

5. If you want to delete roles from the **Mapped Roles** section, select the roles and click −.
6. When the **Edit Role Mapping** dialog reflects the role mapping that you want to define for the group, click **Save**.
   The dialog closes, and the edited role mapping is listed in the External Group Mapping tab.

Related Topic

- Search for External Groups

Search for External Groups

This topic provides instructions for searching for external groups that have NetWitness Suite user roles mapped to them.

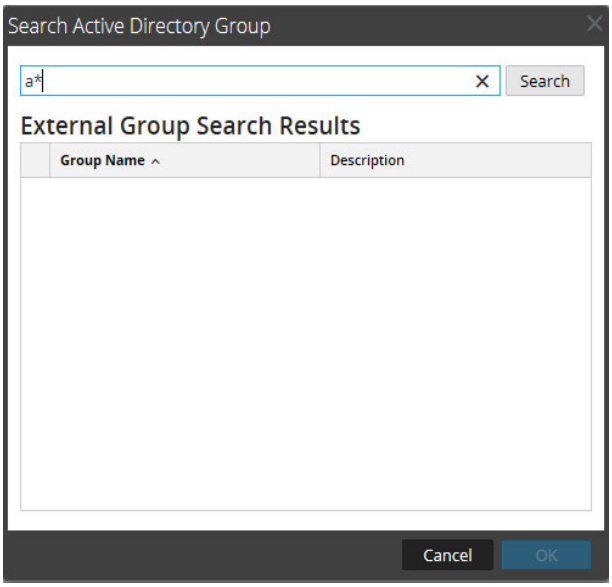
Prerequisites

A method for external user authentication must be enabled.

Procedure

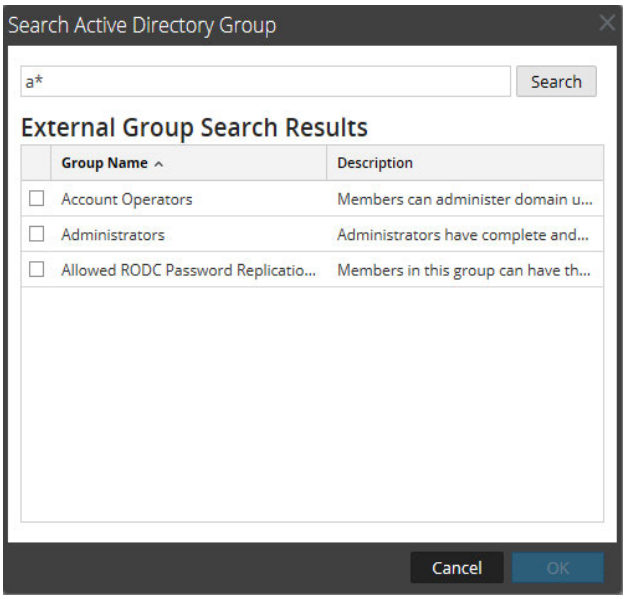
To search for an external group:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click + or .
   The **Add Role Mapping** dialog for the external authentication method you selected is displayed.
4. The **Group Mapping** section is dependent on the selected external authentication method.
   - For **Active Directory**, select a **Domain**. Then click **Search** next to **External Group Name**.
   - For **PAM**, click **Search** next to **PAM Group Name**.
     The **Search External Groups** dialog is displayed.
5. In **Common Name**, type a group name or part of a group name with the wild card character (*).



6. Click **Search**.

   The results are displayed in the **External Group Search Results** section.



7. Select the group to which you want to assign roles and click **OK**.

References

This topic is a collection of references for system security and user management in NetWitness Suite.

Topics

- Admin Security View
- Users Tab
- Add or Edit User Dialog
- Roles Tab
- Add or Edit Role Dialog
- External Group Mapping Tab
- Add Role Mapping Dialog
- Search External Groups Dialog
- Settings Tab

Admin Security View

This topic describes each user interface element in the Admin > Security view and in all related dialogs and tabs. The interface components are listed in alphabetical order.

The Admin > Security view provides the capability to manage user accounts, manage user roles, map external groups to NetWitness Suite roles, and modify other security-related system parameters. These apply to the NetWitness Suite system and are used in conjunction with the security settings for individual services.

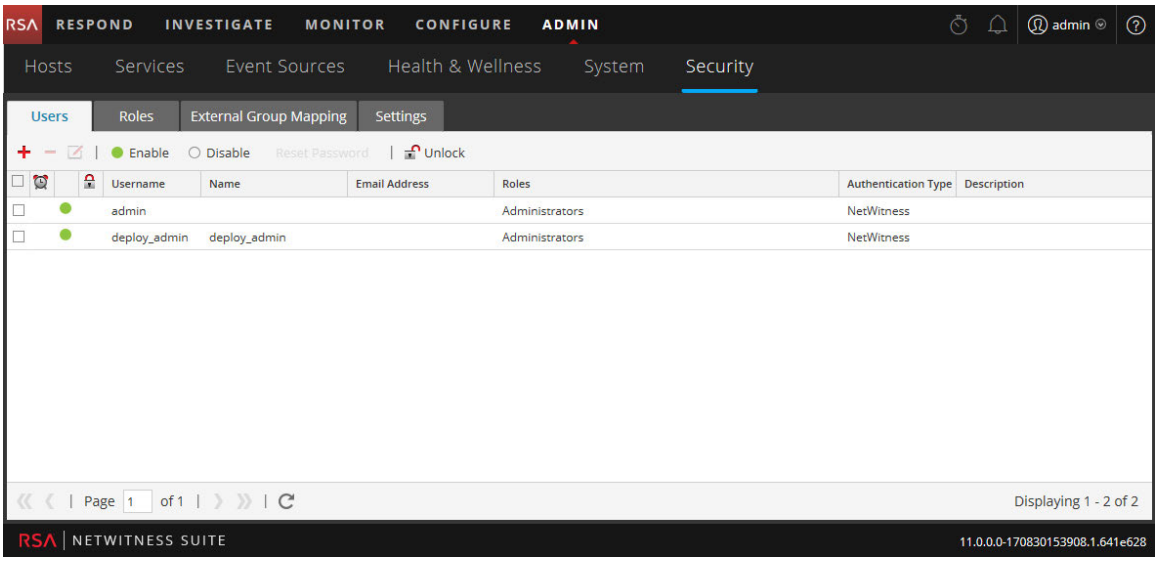
What do you want to do?

Role	I want to ...	Show me how
Admin	Manage users	Step 4. Set Up a User
Admin	Manage roles	Step 1. Review the Pre-Configured NetWitness Roles Step 2. (Optional) Add a Role and Assign Permissions
Admin	(Optional) Configure external group mappings	Step 5. (Optional) Map User Roles to External Groups
Admin	Configure settings	Step 3. Configure System-Level Security Settings

Related topics

- Users Tab
- Roles Tab
- External Group Mapping Tab
- Settings Tab

To display the Admin Security view, go to **ADMIN > Security**.



The Admin > Security view has four tabs:

- The **Users** tab provides a way to manage user accounts.
- The **Roles** tab provides a way to define security roles and assign roles to user accounts.
- The **External Group Mapping** tab provides a way to manage access parameters for LDAP groups.
- The **Settings** tab provides a way to configure password complexity and expiration for internal NetWitness Suite users and to configure system behavior due to failed logins and inactivity. It also provides a way to configure external authentication.

Users Tab

This topic introduces the features and functions to set up a user account in the Admin > Security view > Users tab.

Each NetWitness Suite user must have a user account. In the Users tab, you can create, edit, delete, enable/disable and unlock a user account.

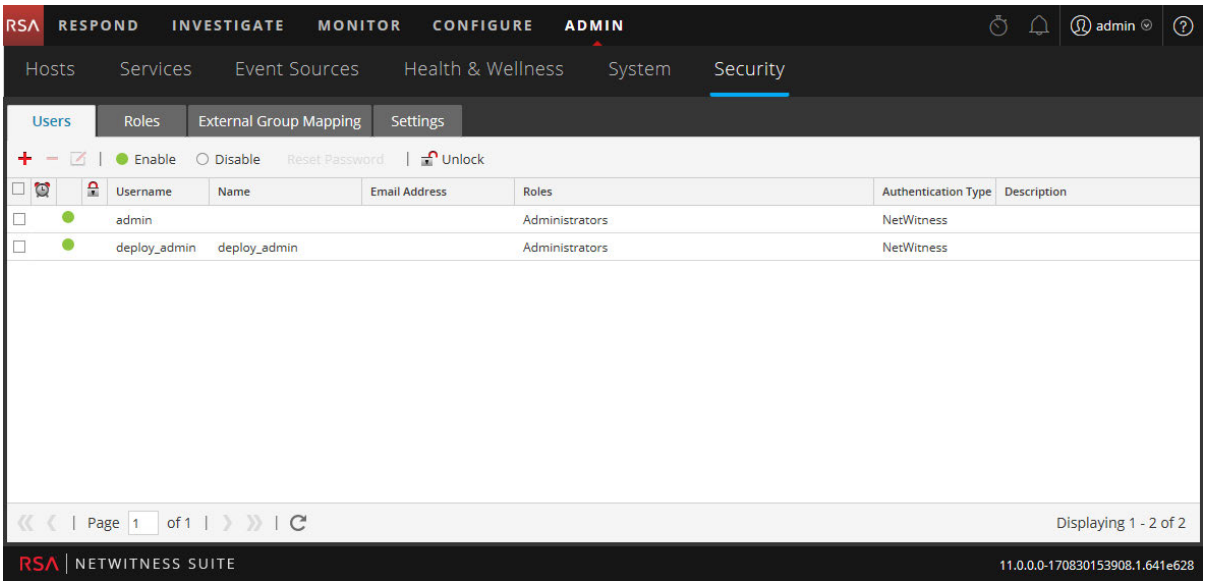
What do you want to do?

Role	I want to ...	Show me how
Admin	Set up a new user	Step 4. Set Up a User Add a User and Assign a Role
Admin	Manage user accounts	Enable, Unlock, and Delete User Accounts

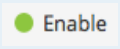
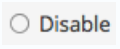
Related Topics

- Add or Edit User Dialog

To access this view, go to **ADMIN > Security**. The Security view opens to the **Users** tab by default.



The Users tab consists of the User list with a toolbar at the top. These are the toolbar features.

Feature	Description
	Opens the Add User dialog.
	Deletes the selected user.
	Opens the Edit User dialog for the selected user.
	Enables a disabled user account with all user preferences intact.
	Blocks user access without deleting user preferences so that upon re-enabling users, user preferences are intact.
Reset Password	Opens the Reset Password dialog, which enables you to change the password of the selected user. This dialog lists the password format requirements necessary to change the password and allows you to force the user to change their password on the next login.
Unlock	Unlocks a user account that has been locked due to too many failed login attempts.

The **Users** list has these columns.

Column	Description
	If this icon appears in a user row, it indicates that the user password has expired.
Username	Username to log on to NetWitness Suite.
Name	Name of the user to whom the account belongs.
Email Address	Email address of the user.
Roles	Role assigned to the user.
External	Authentication method, which could be external by Active Directory or PAM or internal by NetWitness Suite.
Description	Description of the user account.

Add or Edit User Dialog

This topic introduces the Add User and Edit User dialogs accessible from the Admin > Security view > Users tab.

All users must either have a local user account with username and password or an external user account that is mapped to NetWitness Suite.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a User and Assign a Role	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Change User Information	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Reset a User Password	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Add a User for External Authentication	Step 2. (Optional) Add a Role and Assign Permissions

Related Topics

- Manage Users with Roles and Permissions
- Enable, Unlock, and Delete User Accounts

User Preferences

To display the **Add User** or **Edit User** dialog:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Do one of the following:
   - In the action bar, click .
     The **Add User** dialog is displayed.

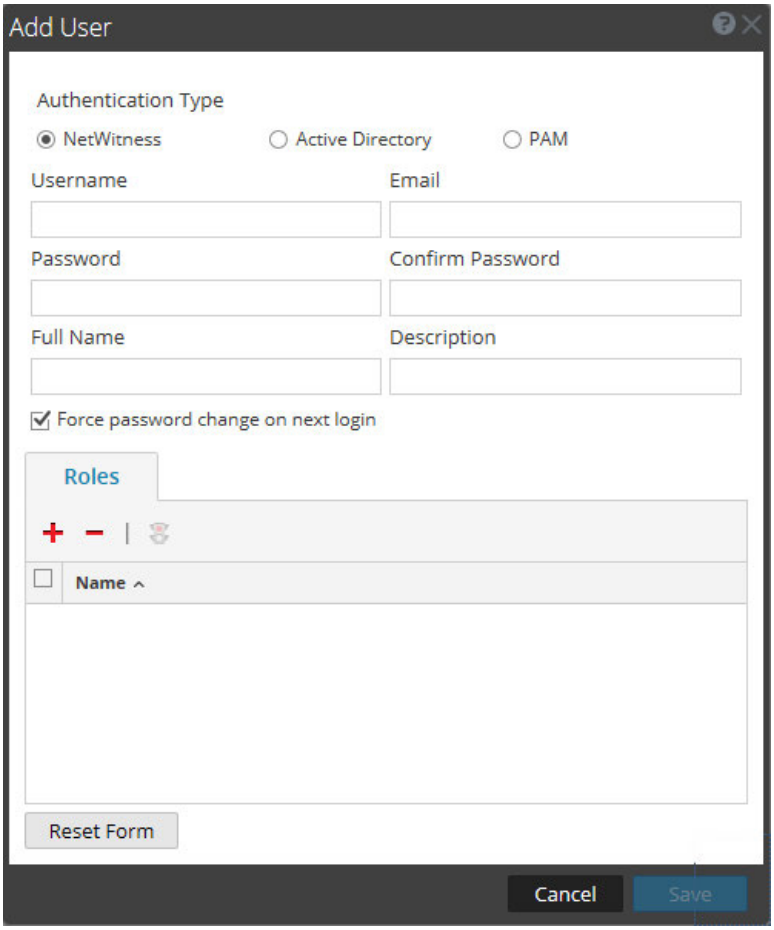
- Select a user and in the action bar, click .

  The **Edit User** dialog is displayed.

The Add User and Edit User dialogs are the same except that the Add User dialog contains additional **Password** and **Confirm Password** fields. You can add a password for a new user in the Add User dialog. Users can change their own passwords in the user preferences. You can reset a password for a user directly from the Users tab.

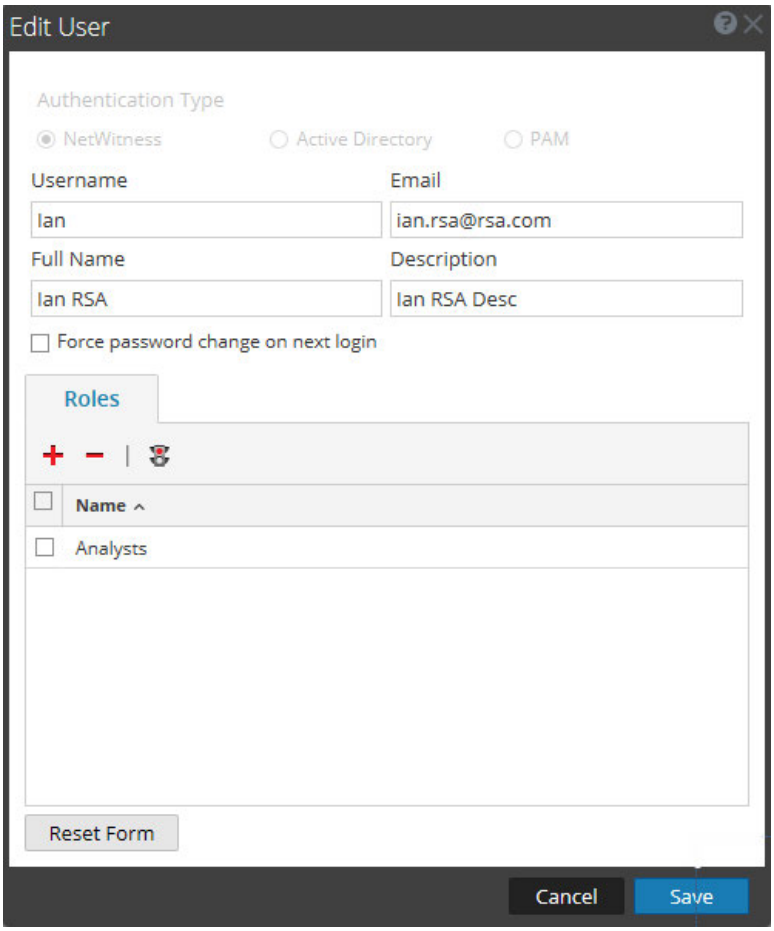
Add User Dialog

This is the Add User dialog for an internal user.



Edit User Dialog

This is the Edit User dialog for an internal user.



The Add User and Edit User dialogs show:

- Authentication type
- User information
- Roles to which the user belongs

User Information

The following table provides descriptions of the user information.

Field	Description
Authentication Type	The authentication type for the user. Default selection is NetWitness, which designates an internal user. Options for external users are Active Directory and PAM. This field is disabled when editing a user.
Username	Username for the NetWitness Suite user account.

Field	Description
Full Name	Name of the user.
Password	(Add User dialog only) Password to log on to NetWitness Suite.
Confirm Password	(Add User dialog only) Password confirmation for adding the user password.
Email	Email address of the user.
Description	(Optional) Description of the user.
Force password change on next login	Expires the user password the next time the user logs on to NetWitness Suite. This field applies only to internal users. This does not affect any active user sessions. The appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is cleared the next time you edit the user account.
Reset Form	Removes any changes in process.

Roles Tab

The following table provides descriptions of the Roles tab options. The Roles tab shows the roles that are assigned to the user.

Option	Description
	Opens the Add Role dialog that lists roles you could assign to the user.
	Removes the selected role from being assigned to the user.
	Shows permissions for the selected role.
Name	Lists each role assigned to the user.

Roles Tab

This topic introduces the functions of the Admin > Security view > Roles tab.

Roles are assigned to all NetWitness Suite users. Users receive the permissions the roles allow. In the Roles tab you can create, duplicate, edit and delete a role. You can also see a list of all roles and their respective permissions.

What do you want to do?

Role	I want to ...	Show me how
Admin	View preconfigured roles	Step 1. Review the Pre-Configured NetWitness Roles
Admin	Create a new role	Step 2. (Optional) Add a Role and Assign Permissions

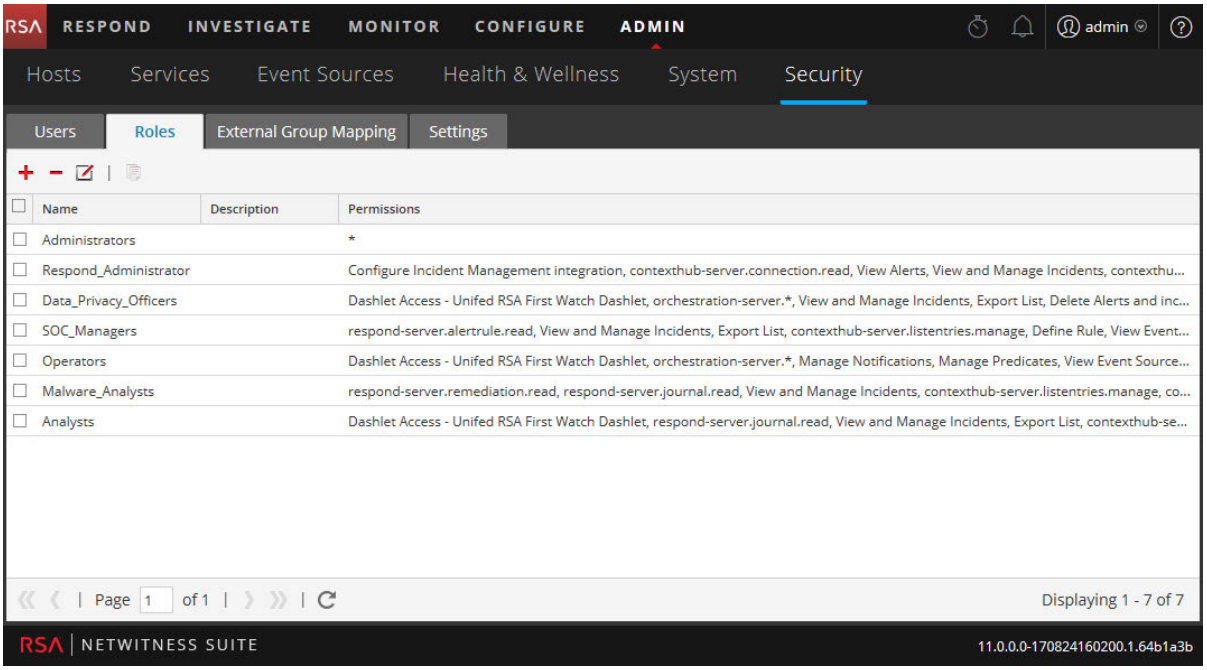
Related Topics

- Add or Edit Role Dialog

To access this view:

1. Go to **ADMIN > Security**.
   The Security view opens to the **Users** tab by default.

2. Click the **Roles** tab.



The Roles tab consists of the Roles list with a toolbar at the top.

The following table describes the toolbar features.

Feature	Description
+	Displays the Add Role dialog.
	Displays the Edit Role dialog.
−	Displays a warning message, and asks for confirmation that you want to delete a role.
	Duplicates a role to save with a different name.

The following table describes the roles list features.

Column	Description
Name	Displays the name of a role that can be given to a user.
Description	Displays a description of the role.
Permissions	Displays the permissions assigned to the role.

Add or Edit Role Dialog

This topic introduces the Add Role and Edit Role dialogs accessible from the Admin > Security view > Roles tab.

In the Add Role and Edit Role dialogs, you can add or edit a role and the permissions assigned to it. You can also specify the query-handling attributes for role members to lock down the information that they can retrieve. The structure of these dialogs is the same. The only difference is that you either add a new role or modify an existing role.

When you change permissions for a role, the change is immediately applied to users who are assigned the particular role after the role is saved.

What do you want to do?

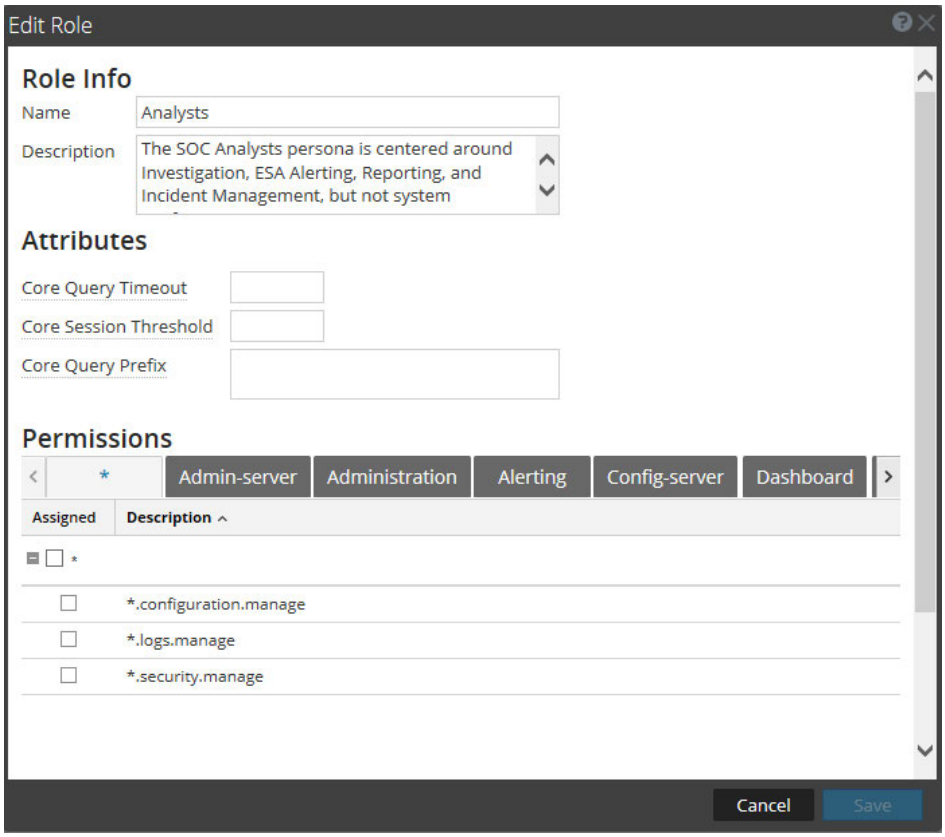
Role	I want to ...	Show me how
Admin	View preconfigured roles	Step 1. Review the Pre-Configured NetWitness Roles
Admin	Create a new role	Step 2. (Optional) Add a Role and Assign Permissions
Admin	Edit a role	Step 2. (Optional) Add a Role and Assign Permissions
Admin	Delete a role	Step 2. (Optional) Add a Role and Assign Permissions

To access this view:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view opens to the **Users** tab by default.
2. Click the **Roles** tab.
3. Do one of the following:
   - In the action bar, click .
     The **Add Role** dialog is displayed.

- Select a role and in the action bar, click .

  The **Edit Role** dialog is displayed.



The Add Role and Edit Role dialogs include three sections: **Role Info**, **Attributes**, and **Permissions**.

Role Info

This is the information in the **Role Info** section.

Feature	Description
Name	The name of the user role.
Description	An optional description of the user role.

Attributes

This is the information in the **Attributes** section. A value shown in italics indicates a default value, for example, *5*. A value shown without italics indicates a change from the default value, for example, `1200`. Step 3. Verify Query and Session Attributes per Role provides more information.

Feature	Description
Core Query Timeout	(Optional) Specifies the maximum number of minutes that a user can run a query. The default value is 5 minutes. This timeout only applies to queries performed from Investigation. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout. When migrating to NetWitness Suite 10.5 and later, if there is no value set in the roles, 5 minutes is set by default. **Note:** NetWitness Suite 10.5 and later Core services use this field.
Core Session Threshold	Controls how the service scans meta values to determine session counts. This value must be zero (0) or greater. If this value is greater than zero, a query optimization will extrapolate the total session counts that exceed the threshold. When the meta value returned by the query reaches the threshold, the system will: • Stop its determination of the session count • Show the threshold and percentage of query time used to reach the threshold The default value is `100000`. The limit you specify here overrides the **Max Session Export** value defined in the INVESTIGATE view settings.
Core Query Prefix	(Optional) Filters query results to restrict what the role members see. By default, this is blank. For example, the `'service' = 80` query prefix prepends to any queries run by the user and the user can only access meta of HTTP sessions.

Permissions

This is the information in the **Permissions** section. Role Permissions describes the permissions.

Feature	Description
Module tabs	There are eight tabs, one for each module: Administration, Alerting, Incidents, Investigation, Live, Malware, Reports, and Dashboard. Each tab lists the permissions for a module.
Description column	List of all permissions for the module.
Assigned column	Checkbox that indicates if a module permission is assigned to the role.
Save	Saves the role with the selected permissions assigned to it.
Cancel	Cancels any work and closes the dialog.

External Group Mapping Tab

If you set up external user authentication, you can map NetWitness Suite user roles to an external group. The External Group Mapping tab provides information about each external group to which you have mapped roles.

What do you want to do?

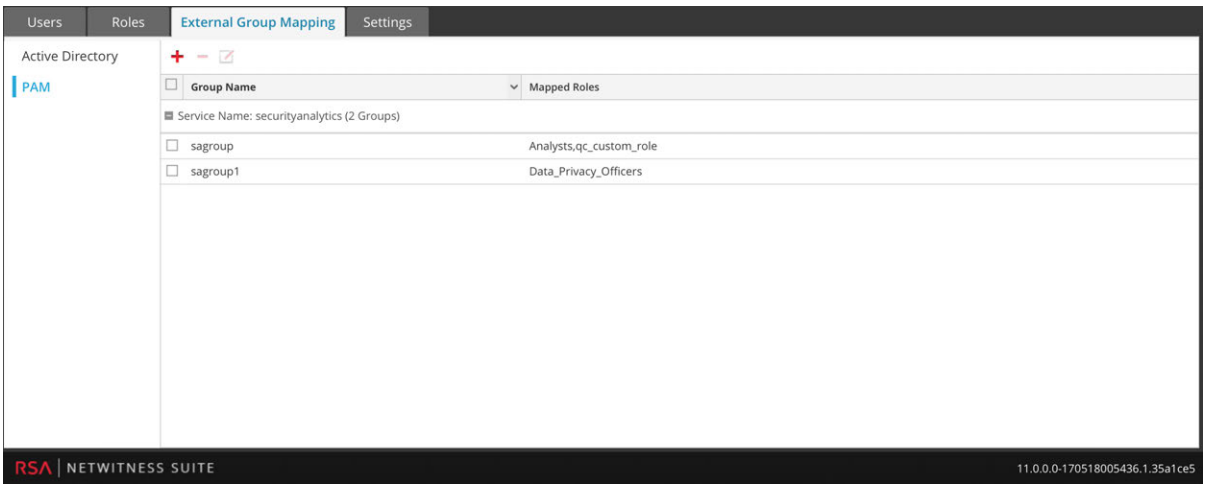
Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

Related Topics

- Add Role Mapping Dialog
- Search External Groups Dialog

To access this view:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.



The External Group Mapping tab consists of a toolbar and list.

The list has the following features.

Feature	Description
Group type	In the column on the left, click either **Active Directory** or **PAM** to show groups for the selected type.
Selection box	In a row, toggles selection of a group name. In the title bar, toggles selection of all group names.
Group Name	Displays the name of the external group that has access to NetWitness Suite.
Mapped Roles	Displays the NetWitness Suite roles mapped to the external group.

The **toolbar** has the following features.

Feature	Description
	Displays the Add Role Mapping dialog in which you can select an external group and map it to a NetWitness Suite role.
	Displays a warning message and asks for confirmation to remove all NetWitness Suite roles mapped to the external group.
	Displays the Edit Role Mapping dialog in which you can add or remove NetWitness Suite roles from the external group.

Add Role Mapping Dialog

This topic introduces the features of the Admin >Security > External Group Mapping tab > Add Role Mapping dialog.

In NetWitness Suite each user role has its own set of permissions. You can map one or more NetWitness Suite roles to an external group, which grants the group the same set of permissions that each role has.

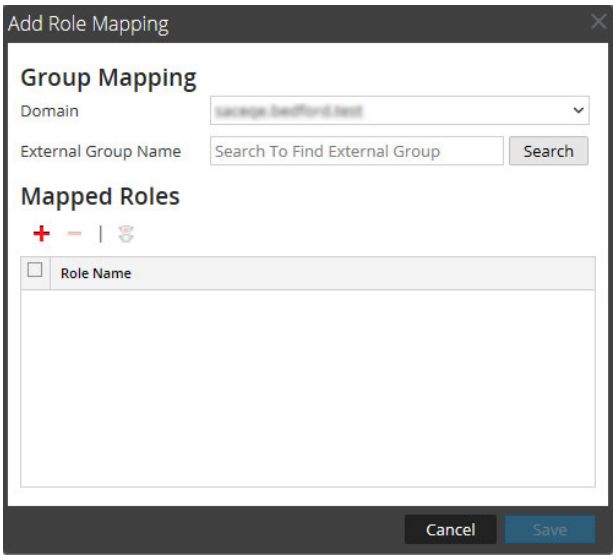
What do you want to do?

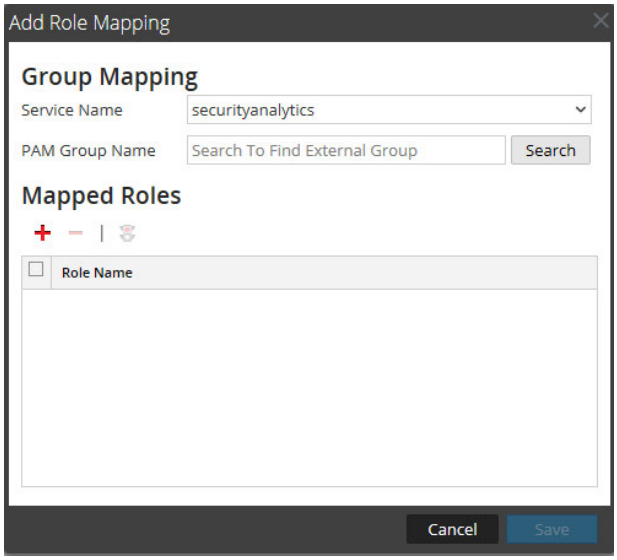
Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

To access this dialog:

1. In NetWitness Suite, go to **ADMIN > Security**.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.

   The **Add Role Mapping** dialog for the external authentication method you set up is displayed.





The Add Role Mapping and the Edit Role Mapping dialogs are nearly identical. The only difference is that you cannot search in the Edit Role Mapping dialog.

Group Mapping

The **Group Mapping** section has the following features.

Feature	Description
Domain	Displayed if you set up Active Directory for external user authentication.The domain name of the external AD group to which roles are mapped.

Feature	Description
External Group Name	Displayed if you set up Active Directory for external user authentication.The external group to which roles are mapped.
PAM Group Name	Displayed if you configured PAM for external user authentication. The name of the external group to which roles are mapped.
Search	Displays a search dialog in which you can search for external groups. Search is not available in the Edit Role Mapping dialog.

Mapped Roles

The **Mapped Roles** section has the following features.

Feature	Description
+	Opens the Add Role dialog, in which configured NetWitness Suite user roles to add are listed.
−	Removes selected roles from the Mapped Roles grid.
Name	Displays the name of the NetWitness Suite user role.
Permissions	Displays the permissions associated with the NetWitness Suite user role.
Cancel	Cancels the new group mapping or changed group mapping and closes the dialog.
Save	Saves the new group mapping or changed group mapping and closes the dialog.

Search External Groups Dialog

This topic describes the features of the Admin > Security view > Search External Groups dialog.

If you set up external user authentication, you can map NetWitness Suite user roles to external groups. You search for external groups to select the groups to which you want to map NetWitness Suite roles.

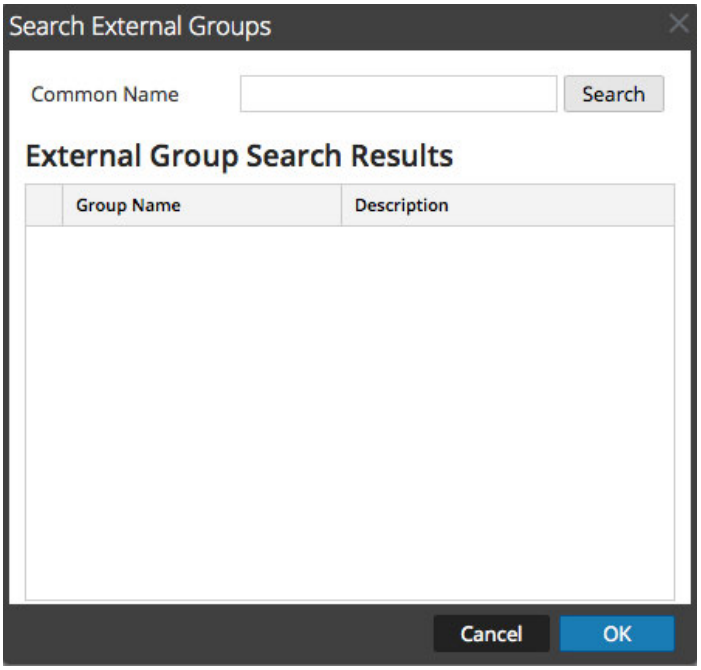
What do you want to do?

Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (Optional) Map User Roles to External Groups
Admin	View external group mappings	External Group Mapping Tab
Admin	Search for external groups	Search for External Groups

To access this dialog:

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.
   The Add Role Mapping dialog for the external authentication method you set up is displayed.
4. In the Group Mapping section, select a **domain**.

5. In the Group Mapping section, click **Search**.
   The **Search External Groups** dialog is displayed.



The following table describes the features of the Search External Groups dialog.

Feature	Description
Common Name	Group name for which you are searching. Can be the exact name or can contain the wild card character (*) to match any character.
Group Name	External group to which you could map roles.
Description	Optional text about the group.
OK	Displays the Add Role Mapping dialog, showing the external group you selected.
Cancel	Closes the dialog.

Settings Tab

This topic explains the ADMIN > Security view > Settings tab. In the Settings tab, you configure password complexity for internal NetWitness Suite users and system-wide security parameters.

For information on configuring NetWitness Suite security, see Set Up System Security.

Password complexity requirements apply only to internal users and are not enforced for external users. External users rely on their own methods and systems to enforce password complexity.

What do you want to do?

Role	I want to ...	Show me how
Admin	Configure password complexity	Step 1. Configure Password Complexity
Admin	Configure system-level security settings	Step 3. Configure System-Level Security Settings
Admin	(Optional) Configure external authentication	Step 4. (Optional) Configure External Authentication

Related Topics

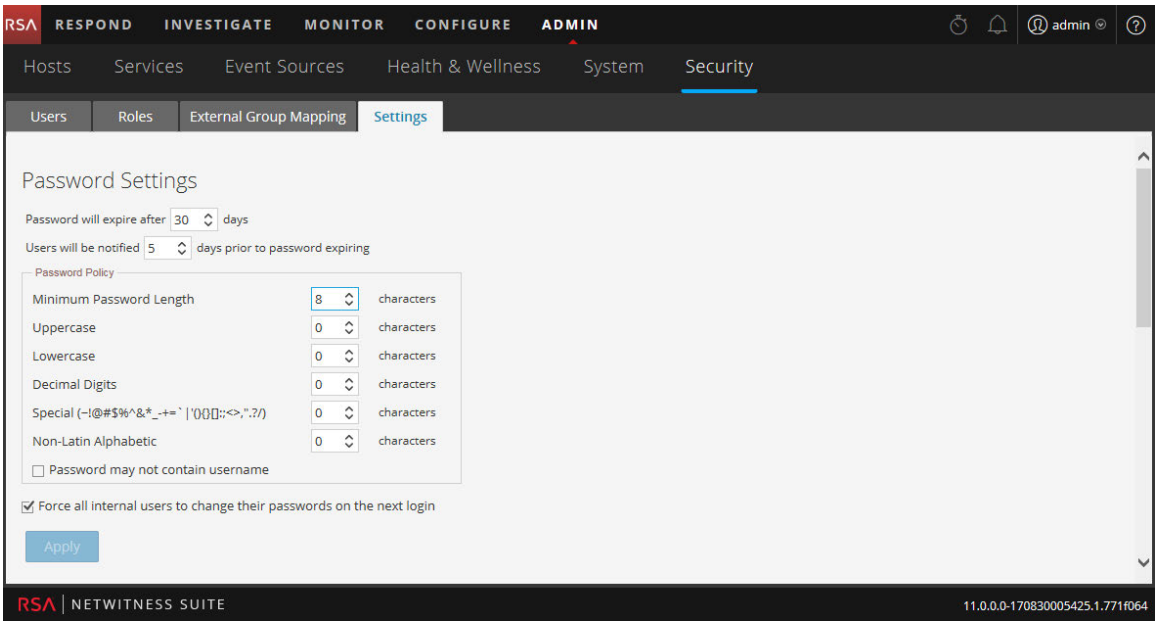
- Set Up System Security

Admin Security View Settings Tab

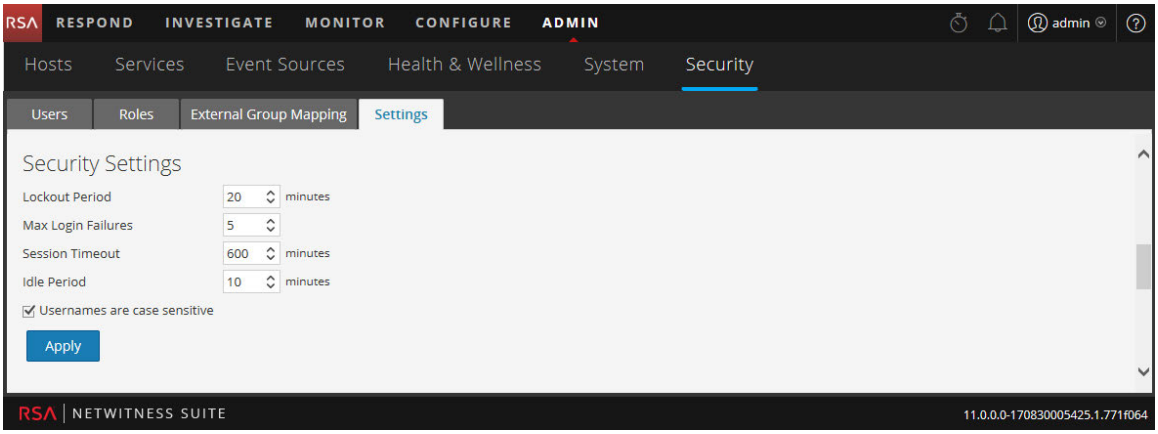
To access the Settings tab:

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.

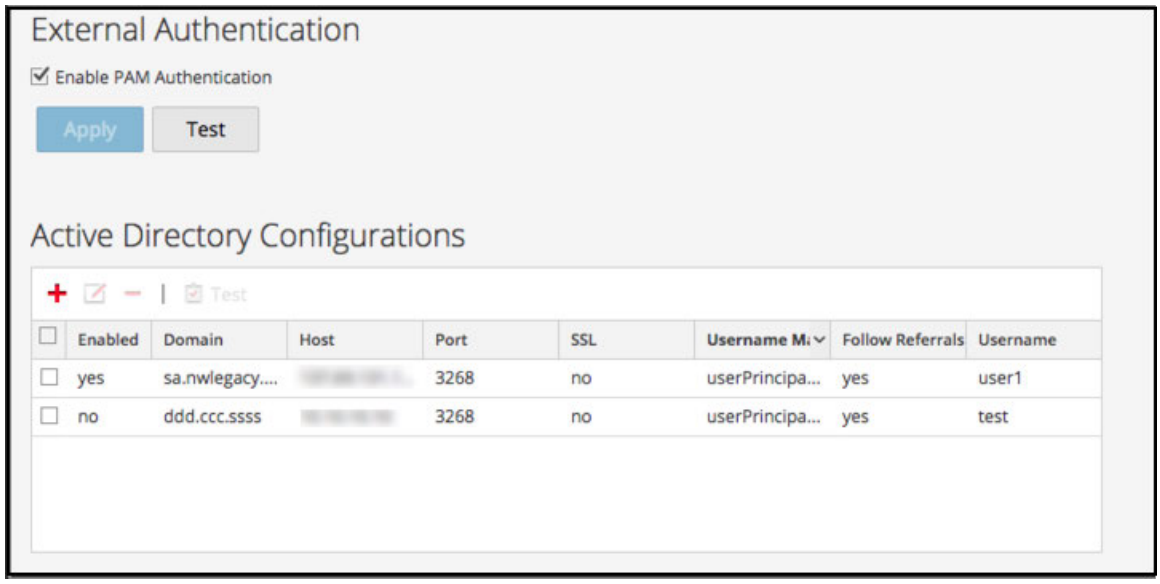
The following figure shows the Password Settings section of the Settings tab.



The following figure shows the Security Settings section of the Settings tab.



The following figure shows the PAM Authentication and Active Directory Configurations sections of the Settings tab.



Password Settings

The Password Policy section enables you to configure password complexity requirements for internal NetWitness Suite users when they set their passwords.

Option	Description
Password will expire after <n> days	The default number of days before a password expires for all internal NetWitness Suite users. A value of zero (0) disables password expiration. For new installations, the default value is 30. For upgrades, the previous value will migrate automatically to the upgraded installation.
Users will be notified <n> days prior to password expiring	The number of days before the password expiration date, to notify a user that their password is about to expire. Users receive a one-time email on the specified date before their passwords expire. They also see a Password Expiration Message dialog when they log on to NetWitness Suite. The minimum value is 1 day.
Minimum Password Length	Specifies a minimum password length requirement for NetWitness Suite user passwords. A minimum password length prevents users from using short passwords that are easy to guess.

Option	Description
Uppercase	Specifies a minimum number of uppercase characters for the password. This includes European language characters A through Z, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic uppercase: Д Ц • Greek uppercase: Π Λ
Lowercase	Specifies a minimum number of lowercase characters for the password. This includes European language characters a through z, sharp-s, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic lowercase: д ц • Greek lowercase: π λ
Decimal Digits	Specifies a minimum number of decimal characters (0 through 9) for the password.
Special (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Specifies a minimum number of special characters for the password: `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Non-Latin Alphabetic	Specifies a minimum number of Unicode alphabetic characters that are not uppercase or lowercase. This includes Unicode characters from Asian languages. For example: • Kanji (Japanese): 頁 (leaf) 栞 (tree)
Password May Not Contain Username	Specifies that a password cannot contain the case-insensitive username of the user.

Option	Description
Force all internal users to change their passwords on the next login	Forces all internal users to change their passwords the next time they log on to NetWitness Suite instead of when they create or change their passwords. Note that this setting is checked by default.
Apply	Password strength settings take effect when NetWitness Suite users create or change their passwords. If **Force all internal users to change their passwords on the next login** is selected, all internal users must change their password the next time they log on to NetWitness Suite.

Security Settings

The Security Settings section enables you to configure global security settings for NetWitness Suite users.

Option	Description
Lockout Period	Number of minutes to lock a user out of NetWitness Suite after the configured number of failed logins is exceeded. The default value is 20 minutes.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5
Session Timeout	The maximum duration of a user session before timing out in minutes. The default value is 600. If the value is 0, there is no maximum time for a session. If the value is a positive integer, the session times out when the configured time has elapsed. The user must log in again.
Idle Period	Number of minutes of inactivity before a session times out. The default value is 10. If the value is 0, the session will not timeout.
Usernames are case sensitive	Select this option if you want the Username field on the NetWitness Suite login screen to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness Suite, but you could not use Admin.

Option	Description
Apply	Makes the settings become effective immediately.

PAM Authentication

The PAM Authentication section enables you to configure NetWitness Suite to use Active Directory or PAM to authenticate and test external user logins.

Option	Description
Enable PAM Authentication	Allows NetWitness Suite to use Pluggable Authentication Modules (PAM) to authenticate external user logons.
Apply	Makes the PAM configuration settings become effective in the next logon.
Test	Prompts for a username and password, then tests the currently enabled PAM authentication method.

Active Directory Configurations

The Active Directory Configuration section enables you to configure NetWitness Suite to use Active Directory to authenticate external user logins.

Option	Description
Enabled	Enables Active Directory authentication for NetWitness Suite users.
Domain	Domain name where the Active Directory Service is located.
Host	Host name or IP address where the Active Directory Service is located.
Port	Port on the host that is used for Active Directory Service authentication.
SSL	Indicates whether the Active Directory Service uses Secure Sockets Layer (SSL). To enable SSL so that your Active Directory Service can communicate with NetWitness Suite version 11.1 and later, you must upload an Active Directory server certificate.
Username Mapping	Indicates the Active Directory search field to use for username mapping. You can specify userPrincipalName (UPN) or sAMAccountName.

Option	Description
Follow Referrals	Indicates whether NetWitness Suite will follow LDAP referrals made by Active Directory.
Username	If Username is provided here, it binds to the Active Directory Service while searching Active Directory groups. This credential is not used for any other purpose.

RSA NETWITNESS® SUITE

Workbench Configuration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Workbench Overview 5

Workbench Configuration Procedures 6

Adding Workbench Service as a Data Source to Broker 8

Adding Workbench as a Data Source to Reporting Engine 11

Managing Collections 13

- Mount Archiver Directories 13
- Create a Collection 13
- Delete a Collection 15
- Example Procedure: How to Restore a Collection for Reporting and Investigation 17
- Investigate a Collection 18
- View Workbench Collection Statistics 20
- View Workbench Logs 21

References 22

Services Config View - Workbench 23

Services Config View - Collections Tab 26

- Toolbar 28

Services Config View - General Tab 30

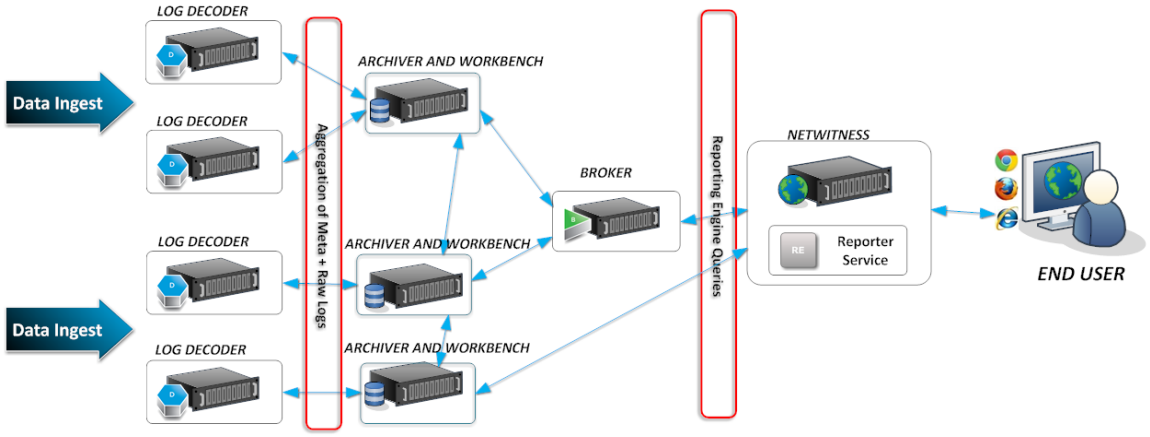
- System Configuration Panel 31
- Workbench Configuration Panel 32

Troubleshooting 33

Workbench Overview

The NetWitness Suite Workbench service allows collections to be created with restored data that was saved offline from an Archiver. Once the data has been copied and saved into a collection, it can be analyzed from Investigation and Reporting.

The following diagram depicts the architecture of a NetWitness Suite network that implements the Workbench.

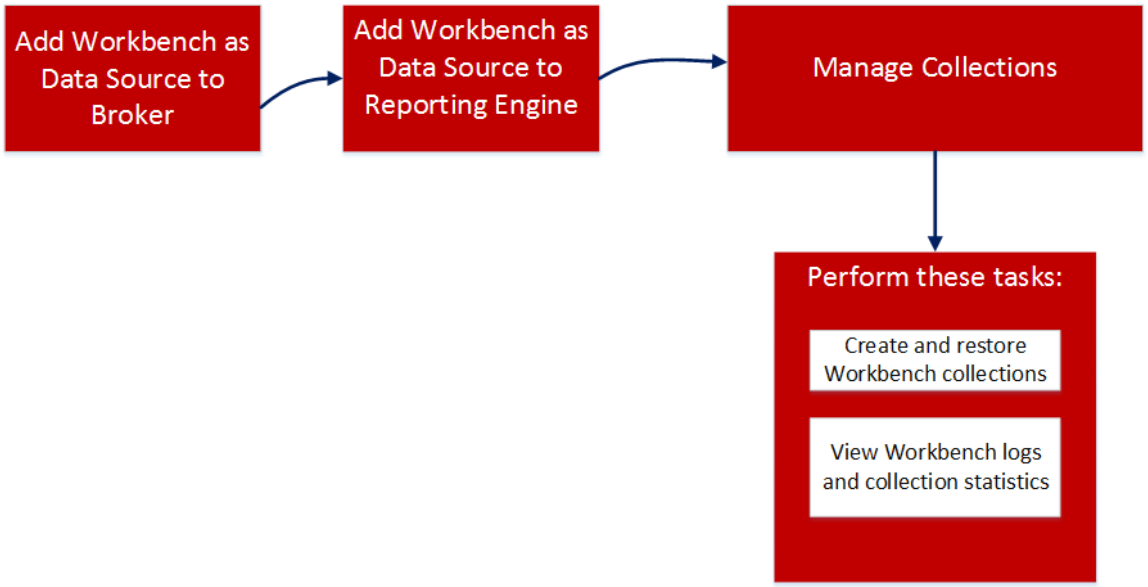


Workbench Configuration Procedures

Note: While NetWitness Suite 11.1 continues to support the Workbench, and some customers may have configured Workbench to handle restoring of data, the best practice for restoring data is to use the Archiver. to configure archival and restoring of data, following the instructions provided in the *Archiver Configuration Guide*.

Workflow

These are the basic steps for configuring and managing a Workbench service.



1. Add a Workbench service as a data source to Broker (see Adding Workbench Service as a Data Source to Broker).
2. Add a Workbench service as a data source to Reporting Engine (see Adding Workbench as a Data Source to Reporting Engine
3. Manage collections on a Workbench service (see Managing Collections).
4. Investigate a Workbench (see Managing Collections).

Prerequisites

Before configuring the Workbench service, you must:

- Add the NetWitness Suite workbench service to the host in your network environment. (Refer to Workbench Overview.)
- Install the NetWitness Suite Workbench host in your network environment. For more information, refer to the *Host and Services Getting Started Guide*.

The steps to configure the Workbench service are:

1. Adding Workbench Service as a Data Source to Broker
2. Adding Workbench as a Data Source to Reporting Engine

When configuration is complete, you can create and manage collections as described in Managing Collections.

Adding Workbench Service as a Data Source to Broker

Prerequisites

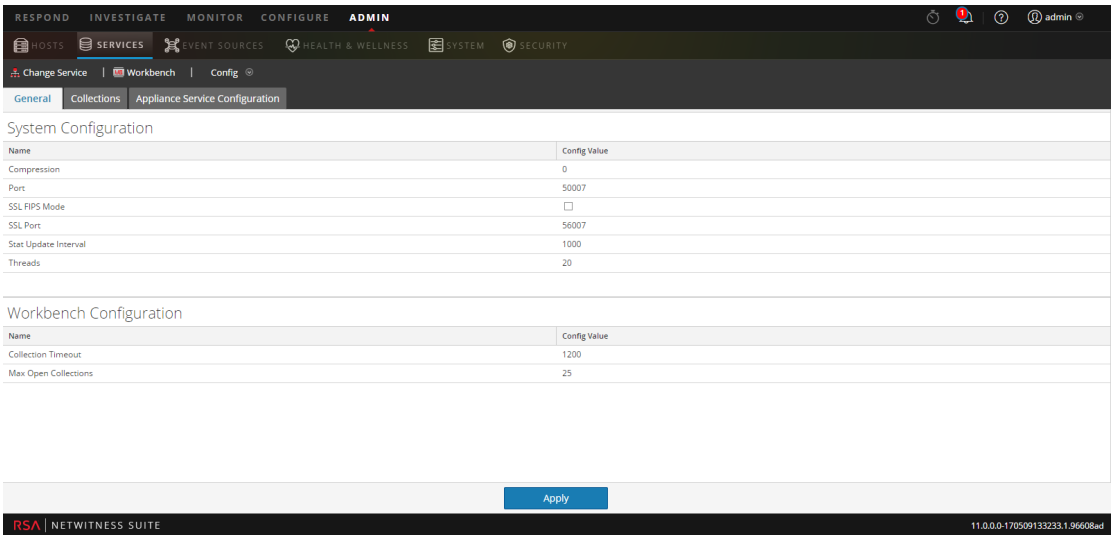
Before adding the Workbench service, you must:

- Install the Workbench service on the Archiver appliance.
- Add a collection on the workbench service.

To add the Workbench service as a data source on the Broker:

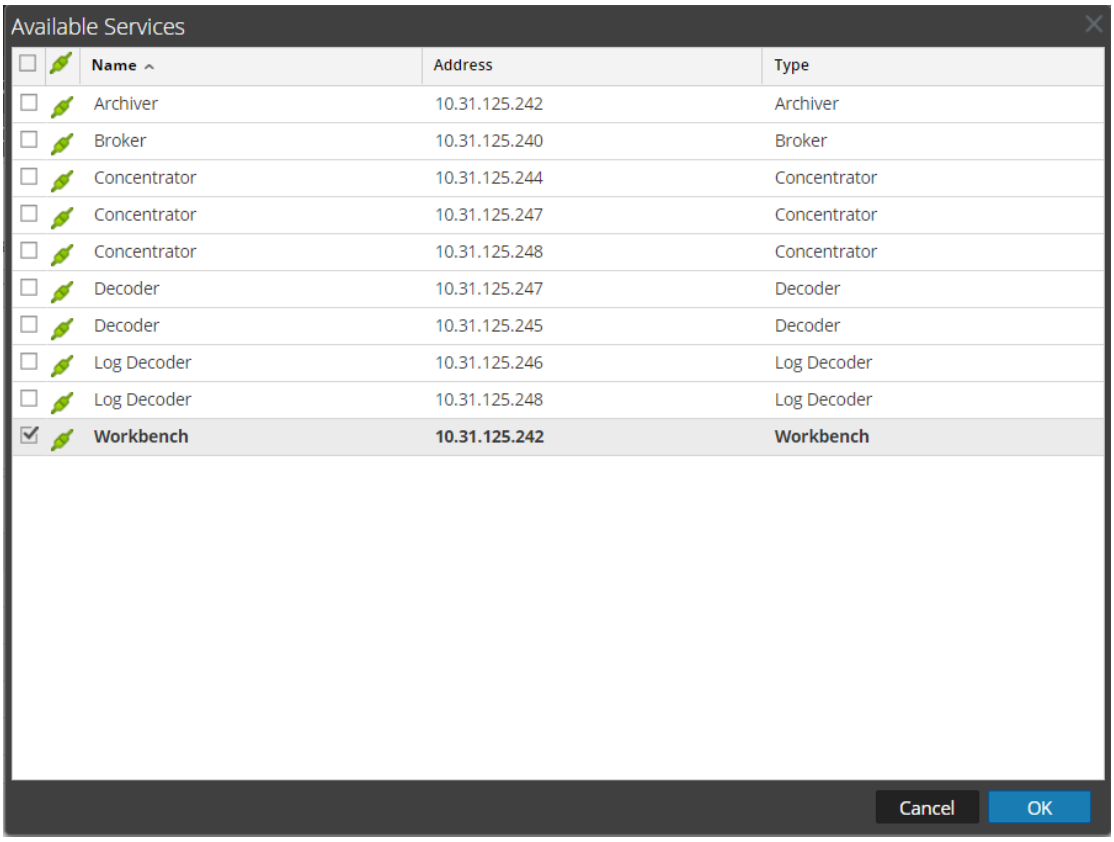
1. Go to **ADMIN >Services**.
2. Select a Broker service, and select **> View > Config.**

   The Service Config view is displayed.

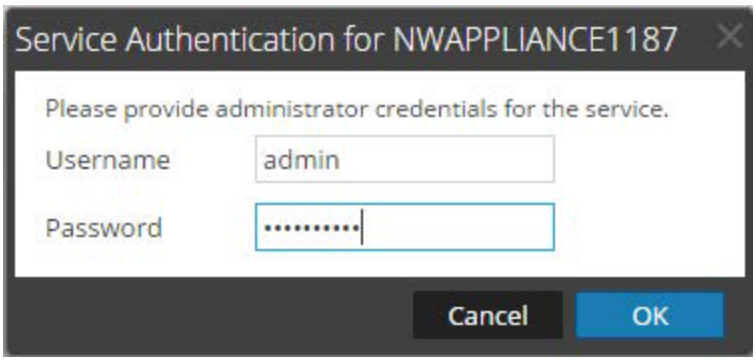


3. Select the **General** tab.
4. Click and select **Available Services**.

   The Available Services dialog is displayed.

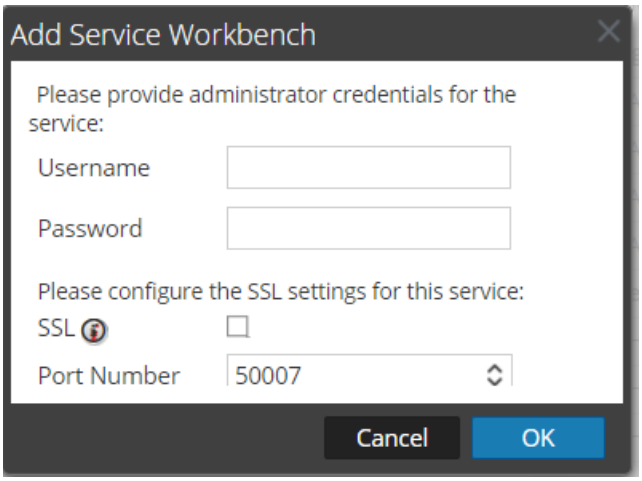


5. Select the Workbench service and click **OK**.
6. If the Workbench service is using a Trust Model, a Service Authentication dialog for the selected service is displayed.



7. Type the username and password for admin credentials for the service and click **OK**.

   The Add Service Workbench dialog is displayed.



8. Type the username and password for admin credentials for the service and click **OK**.

   The workbench service is now added as a data source to the Broker and is listed in the NWDATA Sources list.

Note: This procedure has to be performed for each collection.

Adding Workbench as a Data Source to Reporting Engine

Prerequisites

These are the tasks required before adding the Workbench as a data source to Reporting:

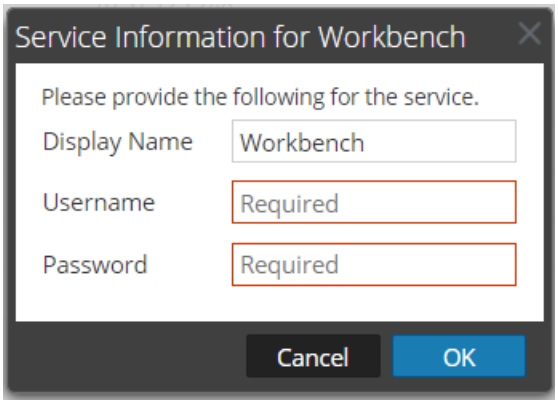
1. Add the Reporting Engine as a service to your NetWitness Suite deployment.
2. Add the Workbench as a service to your NetWitness Suite Archiver host (if not already installed).

Note: Adding Workbench collections as a data source to Reporting Engine depends on a trusted connection. If the Workbench is established with a trusted connection, you must manually add Workbenchcollections as a source to the Reporting Engine.

To associate the Workbench data source with the Reporting Engine:

1. Go to **ADMIN > Services**.
2. Select a **Reporting Engine** in the Services grid. Select **View > Config**.
3. Switch to the **Sources** tab.
4. Select .
5. Select **Available Services**. Select a Workbench service in the Available Services dialog.
6. Click **OK**.

   The Service Information dialog is displayed.



7. Enter User Name and Password.

- Required if the Workbench service is Trusted.
- Optional if the Workbench service is not trusted (added manually).

8. Click **OK**.
9. Select **Collection** in Add a Collection from Workbench dialog.
10. Click **OK**.

Result

You can now create reports on the data collected by the Workbench.

Managing Collections

An Administrator can create and delete Workbench collections and view Workbench statistics and logs. This topic provides all of these procedures and an example procedure for restoring a collection for Reporting and Investigation.

- Mount Archiver Directories
- Create a Collection
- Delete a Collection
- Investigate a Collection
- View Workbench Collection Statistics
- View Workbench Logs

Mount Archiver Directories

If data is in offline storage or cold-tier storage, you need to mount the Archiver directories in order to restore the data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select an **Archiver** from the Services grid and select **> View > Explore**.
   The Explorer view for the Archiver is displayed
3. Right-click on the **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
4. Run the **manifest** command for a time range, for example, 2017-April-01 to 2017-April-10.
   The search returns all files that need to be restored for the selected query.

Create a Collection

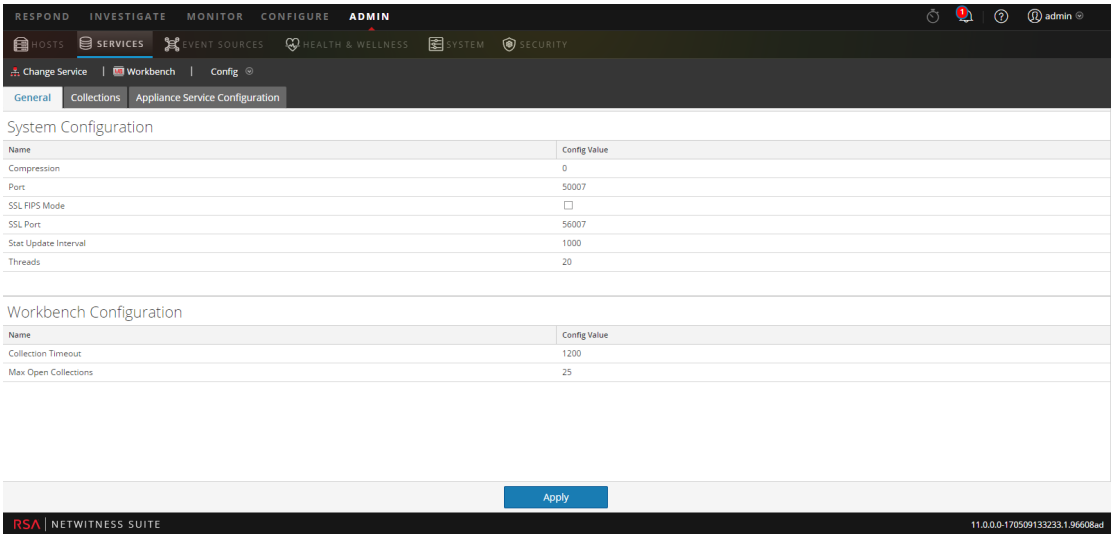
Administrators can create collections of restored data from a backup or from an existing set of data.

Note: You can point the source path to the location of the database files and the restore command copies them to the workbench. You need to mount those directories to the Archiver (where the Workbench is installed) before a restoration collection can be created.

To create a collection using data restored from the backed up data or existing subset of data:

1. Go to **ADMIN> Services.**
2. In the Services view, select a **Workbench**, then select **> View > Config**.

   The Services Config view is displayed with the General tab open.

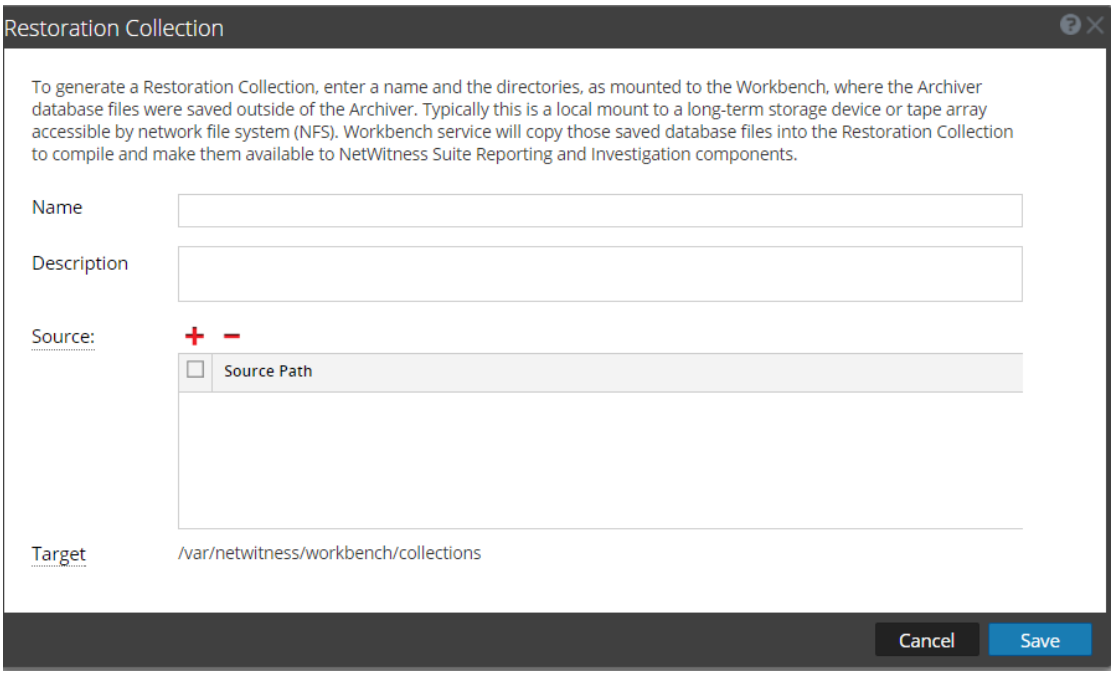


3. Click the **Collections** tab.

   The Collections grid is displayed.

4. Click in the toolbar.

   The Restoration Collection dialog is displayed.



5. Provide the following information:

- **Name:** Name of the Workbench collection that you want to restore.
- **Source:** Location where the Archiver database files have been moved from cold storage.

Note: Target is the location where the collection is created.

6. Click **Save** to restore the collection.

Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:

```
The source path does not exist '/xxx/xxx/'.
```

If there is insufficient storage to restore your collection, the following error is displayed:

```
Error during disk space checking. Insufficient disk space in
location '/xxx/xxx'.
```

The Schedule Job dialog is displayed with the following message:

```
Restoring data into a new collection. Check the jobs page for
progress.
```

7. Click the **Jobs** icon in the NetWitness Suite toolbar to expand the list of restoration collection jobs with their current status.

Note: Restoring a collection that is larger than 550 GB may take several hours to process.

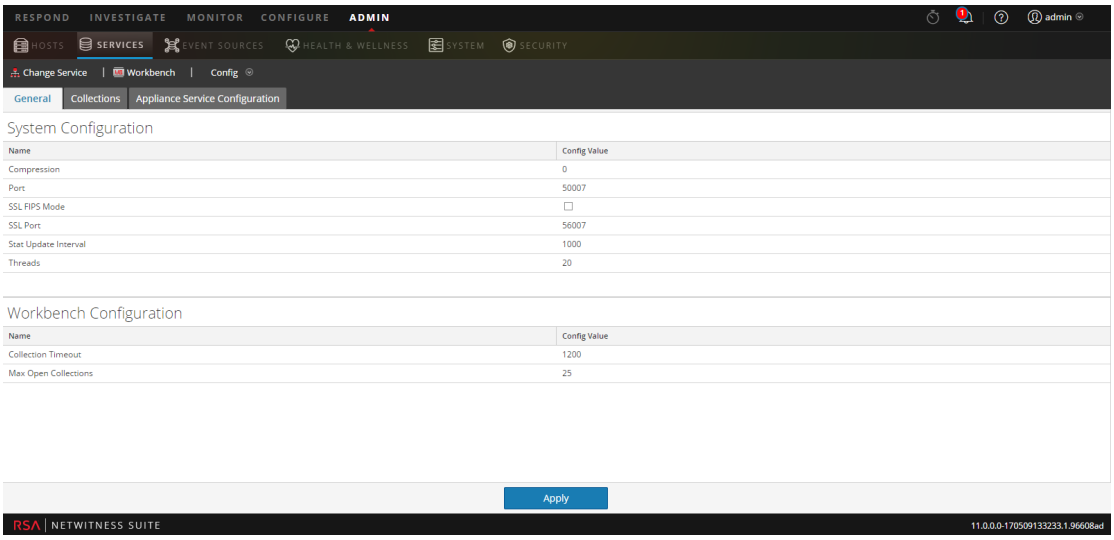
Delete a Collection

Administrators can delete collections from the Workbench service.

Perform the following steps to delete a collection:

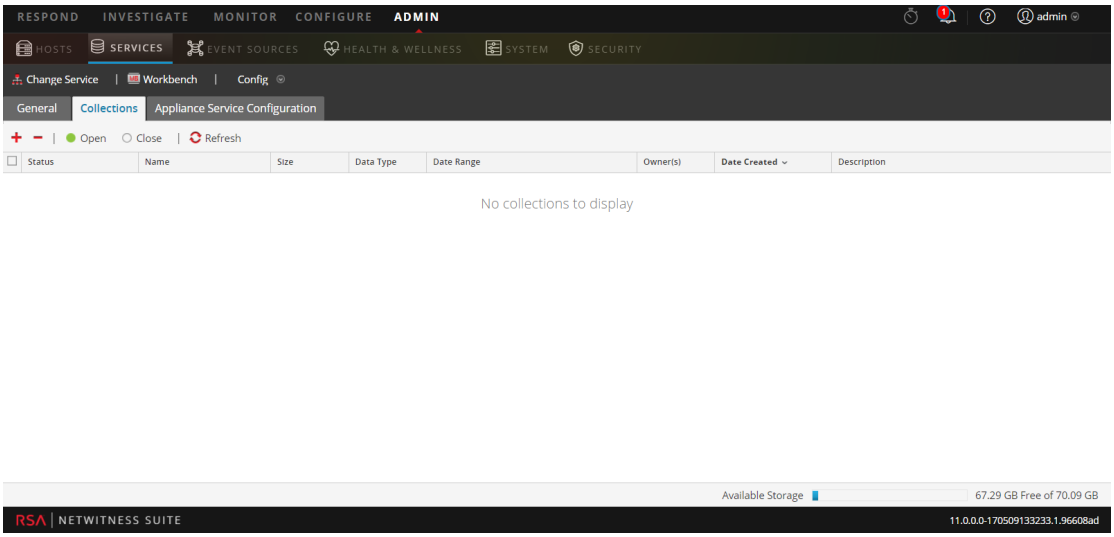
1. Go to **ADMIN > Services.**
2. From the Services view, select a **Workbench** and click **> View > Config**.

   The Services Config view opens with the General tab displayed.



3. Select the **Collections** tab.

   The Collections grid is displayed.



4. In the Collections grid, select the collection that you want to delete.
5. Click − from the toolbar.

   A warning dialog requests confirmation.
6. If you want to delete the collection, click **Yes**.

   The collection is removed from the Workbench service.

Example Procedure: How to Restore a Collection for Reporting and Investigation

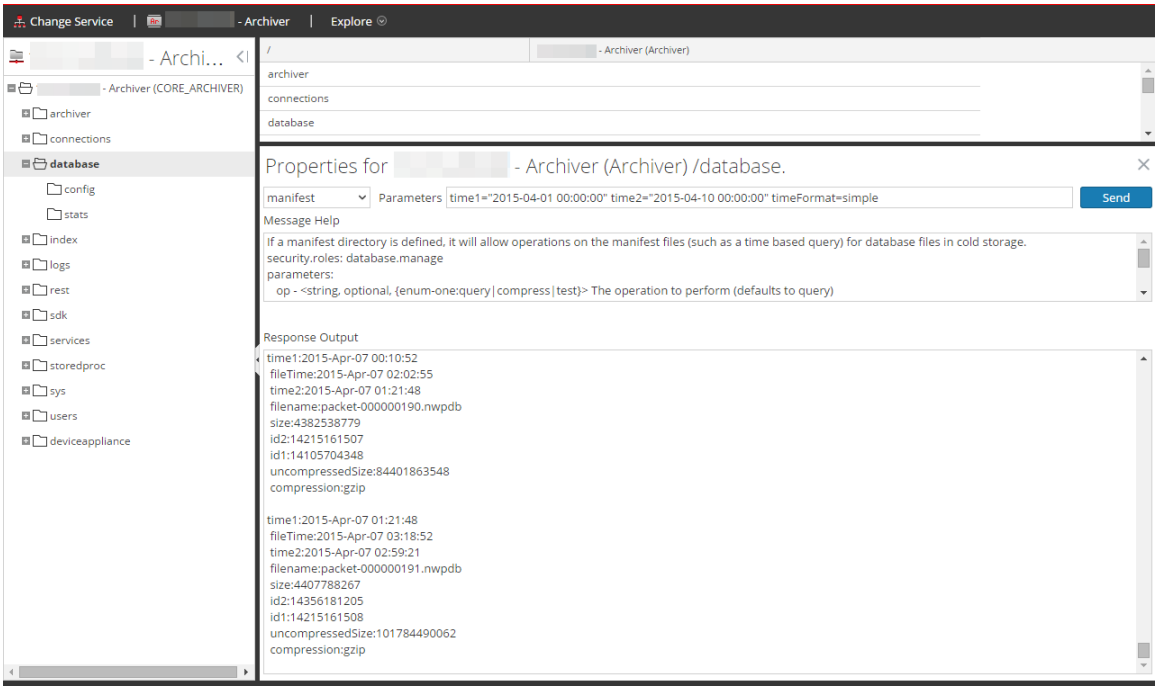
The following steps illustrate how to restore data for reporting and investigation purposes that is in offline storage or cold-tier storage. In the following example, data is restored for the time range beginning on 2015-April-01 through 2015-April-10.

To restore data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select the **Archiver** from the Services grid.
3. Navigate to the Explorer view of the Archiver appliance by selecting **> View > Explore**.
   The Explorer view for Archiver is displayed
4. Right click on **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
5. Run the **manifest** command for the selected time range 2015-April-01 to 2015-April-10.
   The search returns all files that need to be restored for your selected query.

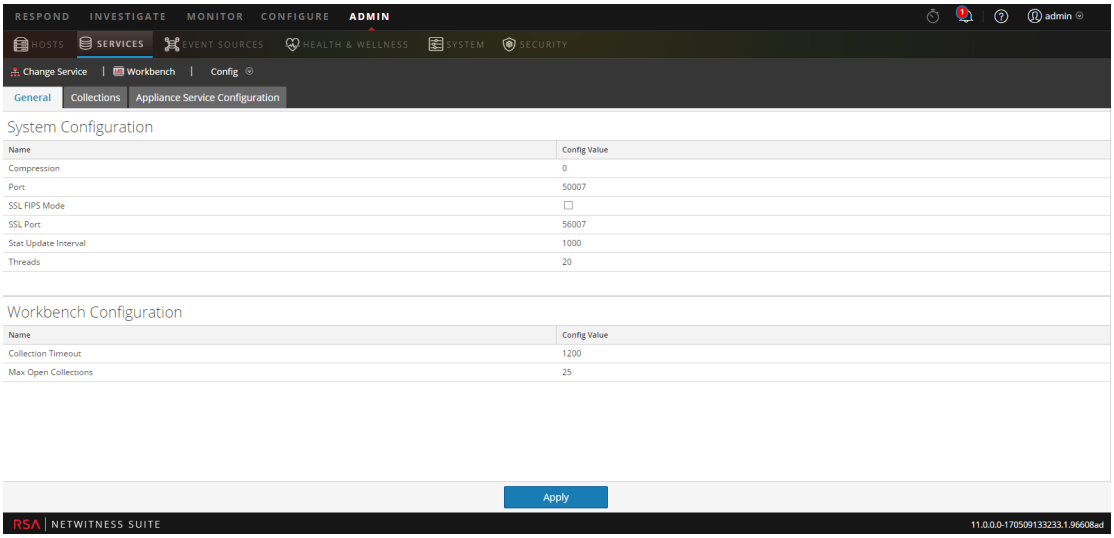
Example Search:

```
time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
timeFormat=simple
```



6. Go to **ADMIN > Services**.
7. In the Services view, select a **Workbench**, then select **> View > Config**.

   The Services Config view is displayed with the General tab open.



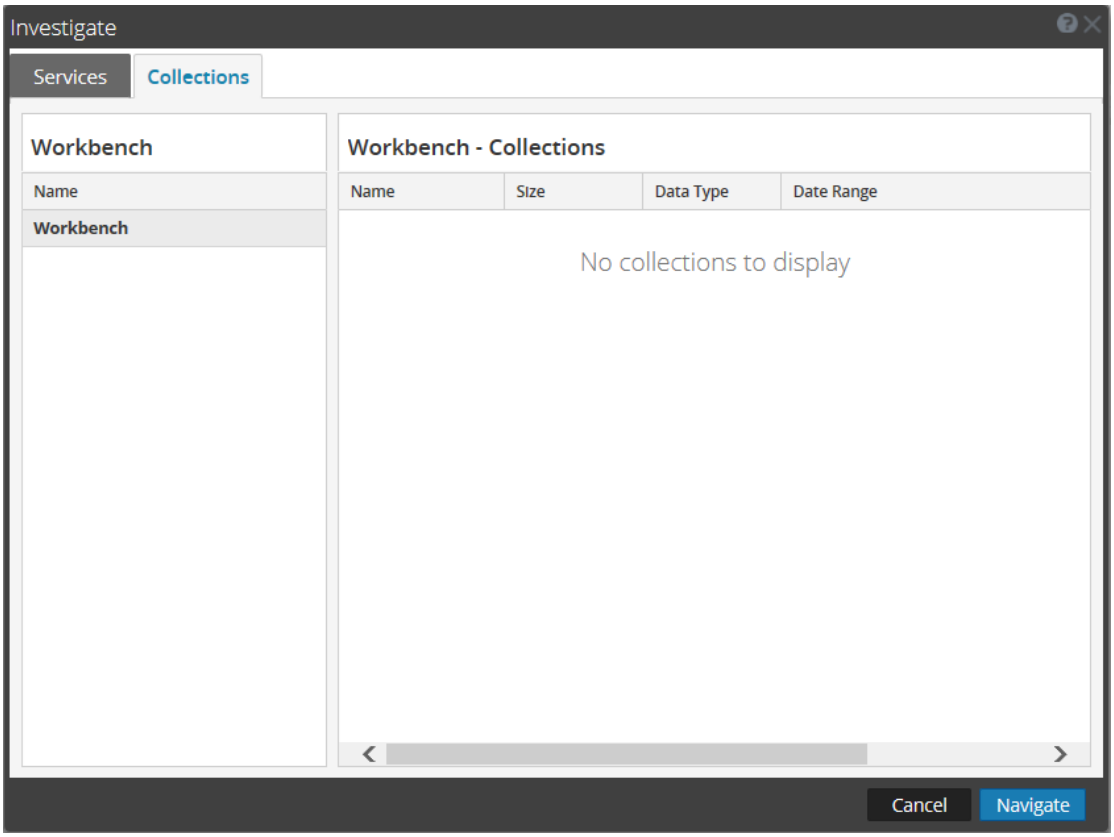
8. Select the **Collections tab.**
9. Create a restoration collection with the source path pointing to files listed in the manifest command output.
10. Save the collection.

    After successfully creating a collection, you can use this collection for reporting and investigation purposes.

Investigate a Collection

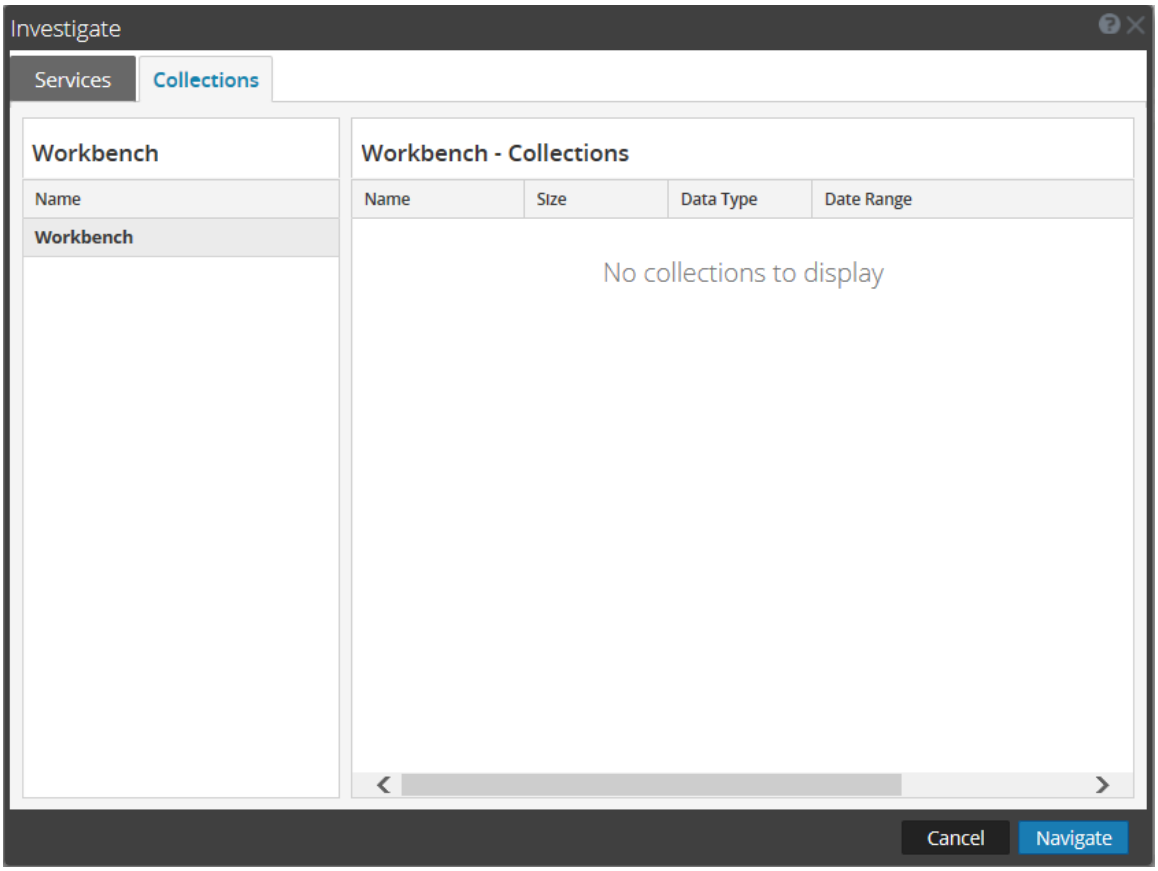
To perform an investigation on a workbench collection:

1. Select **Investigate**.
   The Investigate dialog is displayed.



2. Click the **Collections** tab in the Investigate dialog.
3. Select a Workbench service in the left panel.
4. Select the collection you want to investigate in the right panel.
5. Click **Navigate**.

The Navigate view is displayed showing data pertaining to the Workbench collection that you selected.



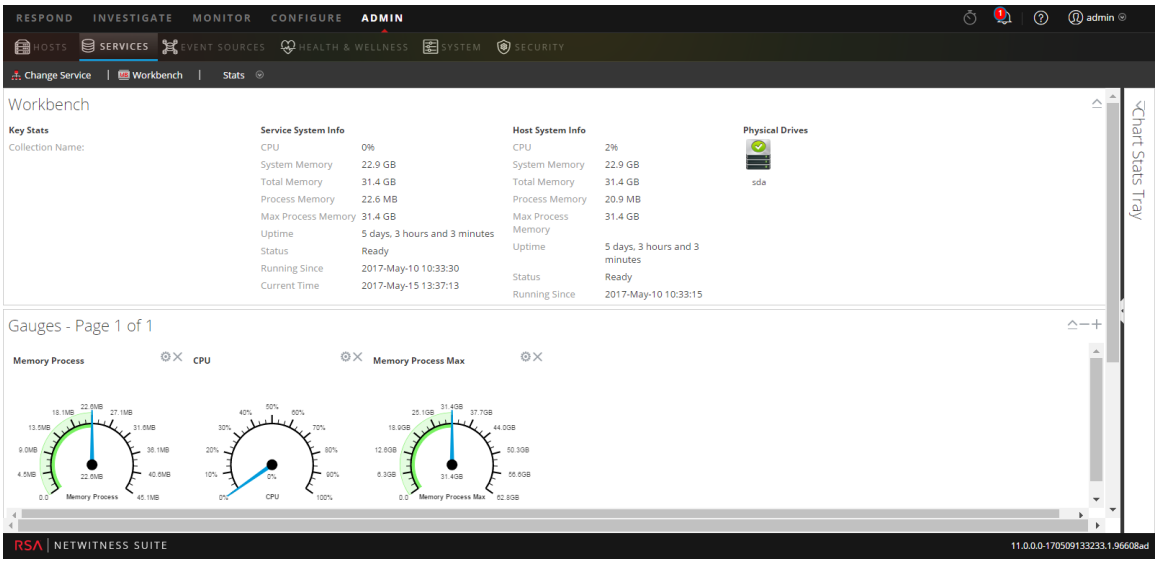
Note: For detailed information about using Investigation, see *Investigation and Malware Analysis Guide*.

View Workbench Collection Statistics

The same statistics available for other services are provided for the Workbench service. The Services Stats view displays key statistics and system information that pertain to your selected Workbench service. The information is displayed in several different sections within the Stats view: Workbench, Gauges, Timeline Charts and Chart Stats Tray. The Chart Stats Tray lists all available statistics for the Workbench. Any statistic in the Chart Stats Tray can be displayed in a gouge or a timeline chart.

Perform the following steps to view workbench statistics:

1. Go to **ADMIN > Services**.
2. In the Services view, select a **Workbench**, then select **> View > Stats**.
   The Services Stats view is displayed.



Note: For more information about Workbench statistics, see the *Host and Services Getting Started Guide*.

View Workbench Logs

Perform the following steps to view logs on a Workbench service:

1. Go to **ADMIN > Services.**
2. In the Services view, select a **Workbench**, then select **> View > Logs**.
   The Services Logs grid is displayed.

Note: For information about viewing and configuring audit logs, see the topic "Configure Global Audit Logging" in the *System Configuration Guide* .

References

Workbench Reference Topics:

- Services Config View - Workbench
- Services Config View - Collections Tab
- Services Config View - General Tab

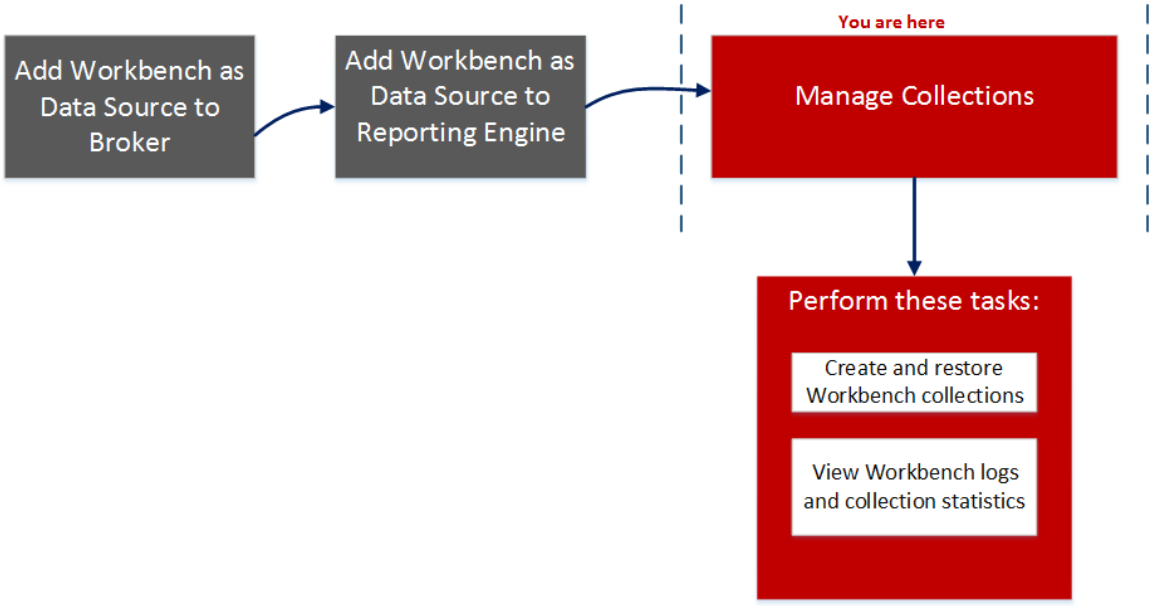
Services Config View - Workbench

In the Services Config view for workbench, some of the parameters are the same as other NetWitness Suite services, while others are specific to the Workbench service.

The Services Config view - Workbench (ADMIN > Services >, select Workbench service and select View > Config) provides a way to configure a Workbench service.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Add Workbench as data source to Broker	Adding Workbench Service as a Data Source to Broker
Administrator	Add Workbench as a Data Source to Reporting Engine	Adding Workbench as a Data Source to Reporting Engine
Administrator	*Create or delete a collection	Managing Collections

Role	I want to...	Show me how...
Administrator	*View Workbench statistics and logs	Managing Collections
Administrator	View configuration information about appliances that are connected to the Workbench service.	Select the **Appliance Service Configuration** tab. The Appliance Service Configuration tab is the same for all NetWitness Suite services. It provides configuration information about appliances that are connected to the Workbench service. For information on the **Appliance Service Configuration** tab, see **Appliance Service Configuration Tab** in the *Host and Services Getting Started Guide*.

*You can perform this task here.

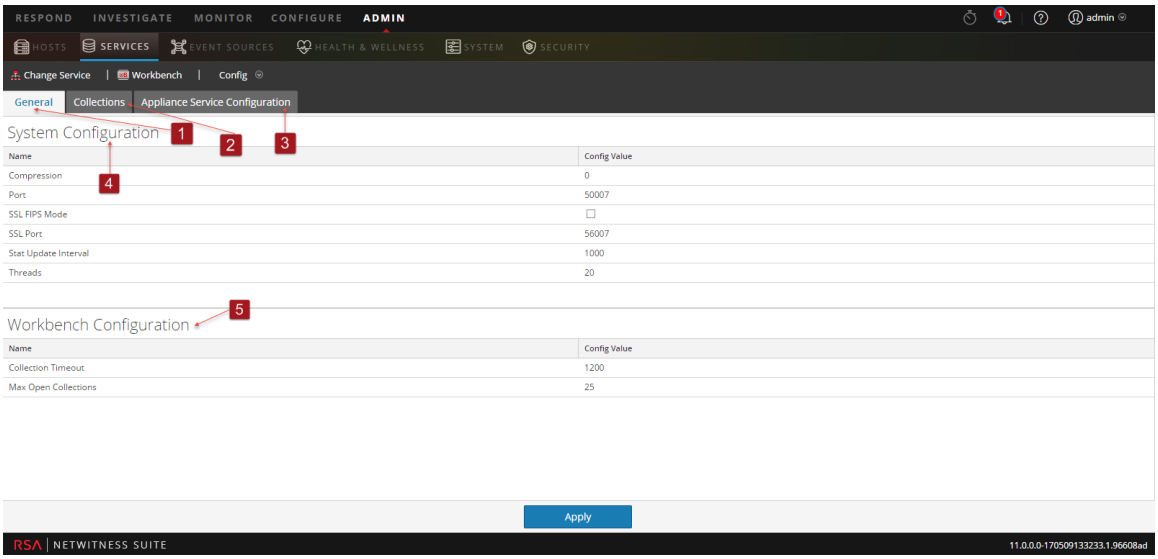
Related Topics

- Workbench Configuration Procedures

Quick Look

The Workbench service has three tabs and two panels in the Config view:

- General tab
- Collections tab
- Appliance Service Configuration tab
- System Configuration panel
- Workbench Configuration panel



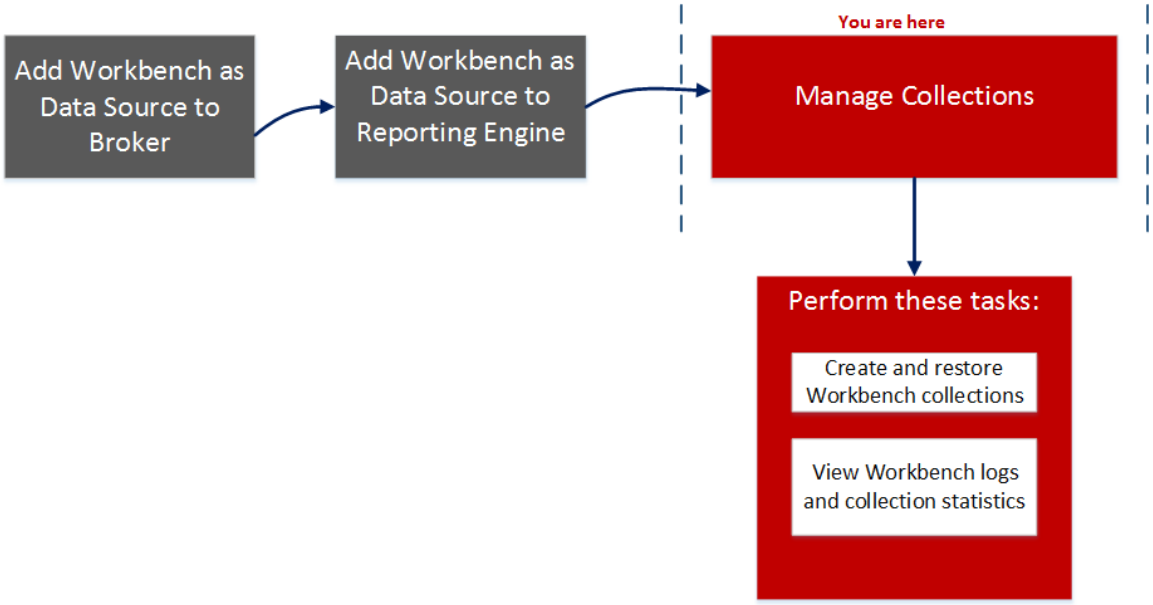
1	General tab provides a way to manage basic Workbench service configuration.
2	Collections tab provides a way to manage collections on a Workbench service.
3	Appliance Service Configuration tab provides a way to configure a Workbench service.
4	System Configuration panel provides a way to manage service configuration for a Workbench service.
5	Workbench Configuration panel provides a way to start and stop a Workbench service.

Services Config View - Collections Tab

The Collections tab for the Workbench service provides a way to manage workbench collections. To access the Collections tab, go to **ADMIN > Services >** select a Workbench service, select **View > Config** and select the **Collections** tab.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Documentation
Administrator	*Create and restore Workbench collections.	Managing Collections
Administrator	*View Workbench logs and collection statistics.	Managing Collections

Role	I want to...	Documentation
Administrator	View configuration information about appliances that are connected to the Workbench service.	Select the **Appliance Service Configuration** tab. The Appliance Service Configuration tab is the same for all NetWitness Suite services. It provides configuration information about appliances that are connected to the Workbench service. For information on the **Appliance Service Configuration** tab, see **Appliance Service Configuration Tab** in the *Host and Services Getting Started Guide*.

*You can perform this task here.

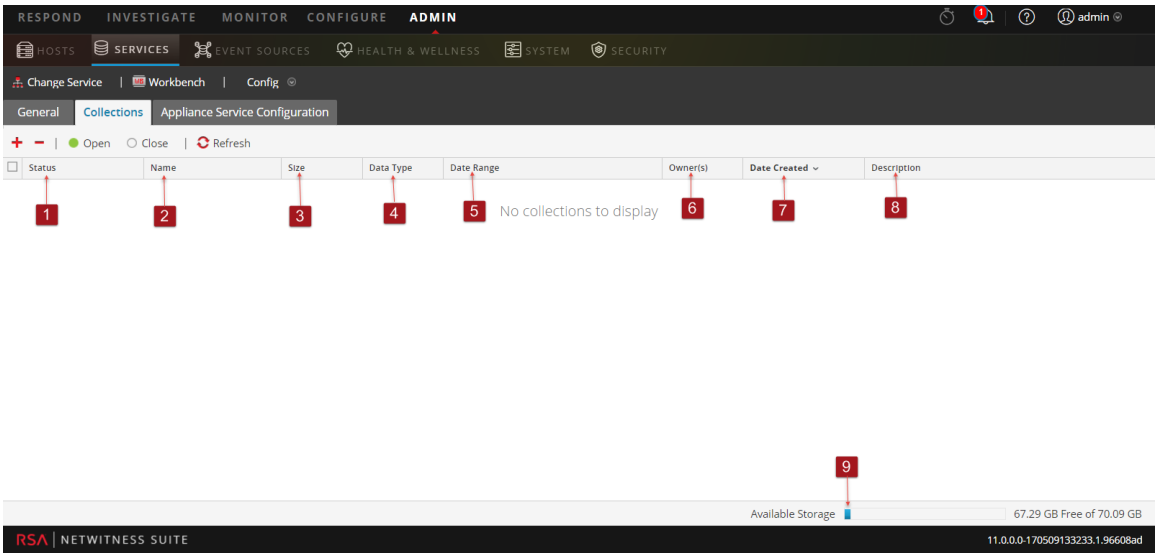
Related Topics

- Workbench Configuration Procedures

Quick Look

The Collections tab has a toolbar and a grid that lists relevant information about the Workbench collections.

The following figure is an example of the Collections grid.



1	Status of the Restoration Collection: • **Resorting Data** - Data restoration is in progress. • **Closed** - Data is restored. • **Opening** - Data is being indexed. • **Ready** - Indexing is complete. • **Closing** - Collection is closing.
2	**Name**: Name of the file being restored.
3	**Size**: Collection size.
4	**Data Type**: Logs.
5	**Date Range**: Lists the range of dates when the collection is being restored.
6	**Owner**: Lists the Collection creator.
7	**Date Created**: Shows the date when the collection was created.
8	**Description**: Description of the Restoration collection.
9	**Available Storage Indicator**: Shows the available disk space, given in gigabytes (GB). The Workbench validates to ensure there is enough available space when attempting to create a restoration collection.

Toolbar

These are the toolbar options.

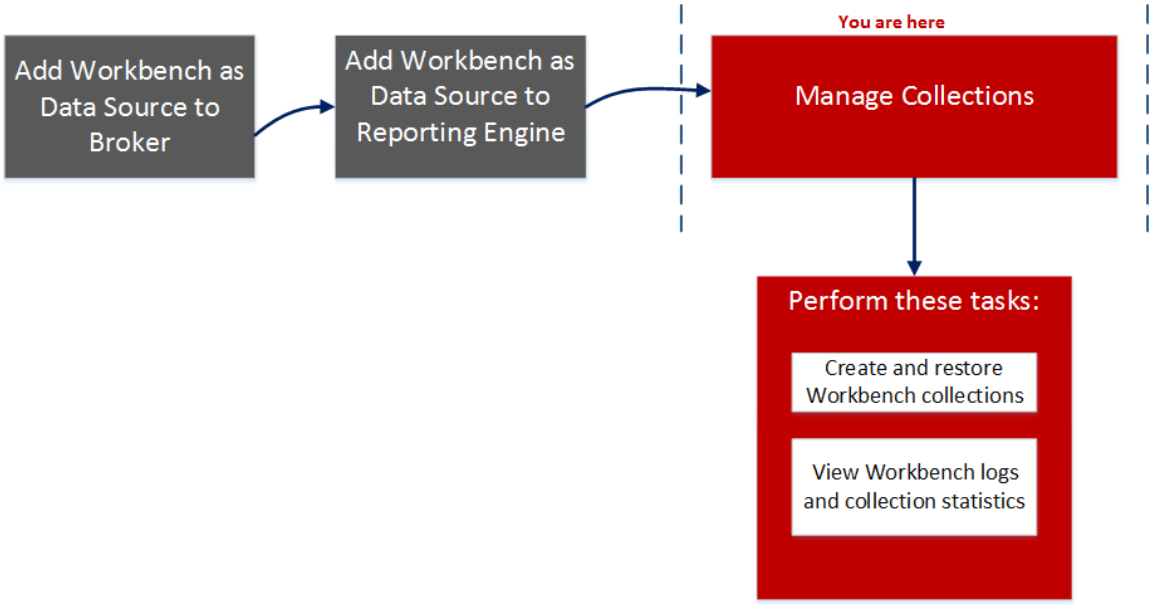
Parameter	Description
	Creates a new restoration collection.
	Deletes the selected Workbench collection.
Open and Close - Refers to the status of the restoration collection.	Open - Makes collection available for investigation and reporting. Close - Makes collection unavailable for investigation and reporting while preserving resources.
	Refreshes the list of Workbench collections.

Services Config View - General Tab

The General tab for the Workbench service provides a way to manage basic service configuration. To access the General tab, go to **Admin** > **Services** > select service and select > **View** > **Config**.

Workflow

These are the basic steps for configuring and managing a Workbench service.



What do you want to do?

Role	I want to...	Show me how...
Administrator	*Create and restore Workbench service collections.	Managing Collections
Administrator	*View Workbench logs and collection statistics.	Managing Collections
Administrator	*Process Workbench collections.	Managing Collections

*You can perform this task here.

Related Topics

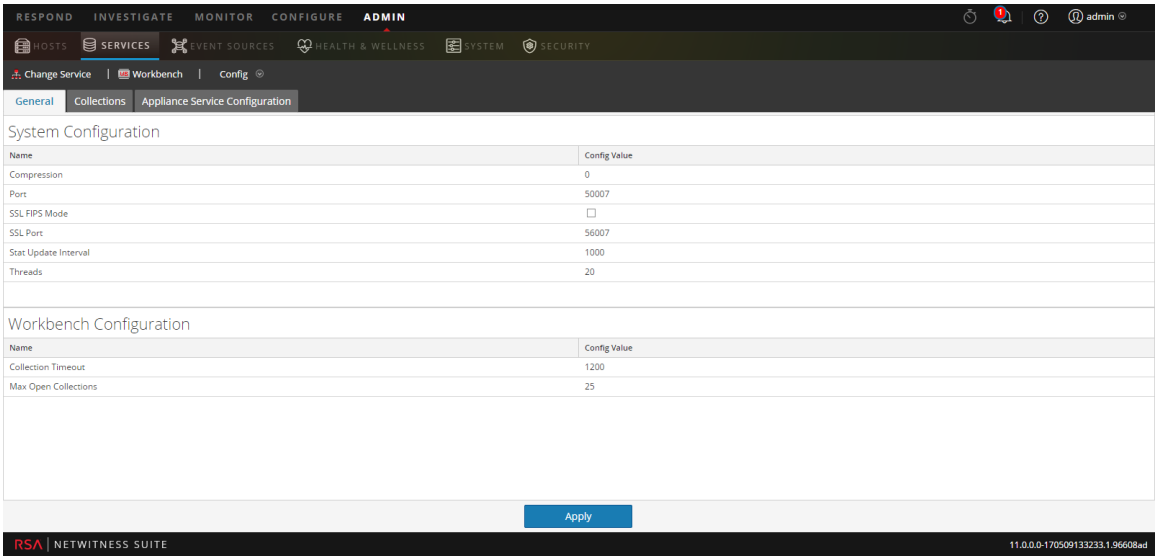
- Workbench Configuration Procedures

Quick Look

The General tab has two panels:

- System Configuration
- Workbench Configuration

The following figure is an example of the General tab.



System Configuration Panel

The System Configuration panel displays configuration parameters for the Workbench service. The following table describes the System Configuration panel features.

Parameter	Description
Compression	When set to a positive value, the minimum amount of bytes before a message is compressed. **0** means no compression for any message. Change takes effect on subsequent connections.
Port	The unencrypted port this service will listen on. **0** means disabled. Change takes effect on service restart.
SSL FIPS Mode	Determines whether the OpenSSL library will enter FIPS mode. Change takes effect on service restart.

Parameter	Description
SSL Port	The SSL port this service will listen on. **0** means disabled. Change takes effect on service restart.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system. Change takes effect immediately.
Threads	The number of threads in the thread pool to handle incoming requests. Change takes effect immediately.

Workbench Configuration Panel

The Workbench Configuration panel displays configuration parameters for the Workbench collections. The following table describes the Workbench Configuration panel features.

Parameter	Description
Collection Timeout	The number of seconds before an idle collection is automatically closed.
Max Open Collections	The number of collections that can be open at once. A setting of 0 disables the limit.
Apply	Updates the modified configurations in the panel.

Troubleshooting

NetWitness Suite notifies users of issues using popup notifications.

NetWitness Suite Workbench returns the following types of error messages explained in the following table.

Problem	Possible Causes	Solutions

Unable to connect to workbench service from NetWitness Suite **user interface Administration page.**	NetWitness Suite service is not running.	Verify that your NetWitness Suite service is running. Log in to your NetWitness Server and run the following command:
		`status nwworkbench`
		Firewall rules should allow connections from 50007, 50607 and 50107.
		Verify your connection by running the following command:
		`service iptables status`
		Verify that you are able to launch REST. Execute the following command for your appliance:
		`https://<IPAddress>:50107 service`
		If you are able to launch REST service for your appliance, you can confirm that there is no problem with the appliance. Navigate to the NetWitness Suite side for further investigation as follows:
		• Enable debug mode and watch for sa.log errors located at:
		`/var/lib/netwitness/uax/logs`
		• Enable developer tools using the shortcut `Ctrl+Shift+I` for Chrome and verify the preview and response for the request.

Problem	Possible Causes	Solutions
Not able to view Appliance service configuration tab for workbench appliance running in SSL mode.		Enable SSL for appliance service and restart the appliance service.

The following error message is displayed when trying to load meta in order to create a report on a workbench collection: "Unable to fetch schema from data source when trying to load meta."		Load meta for the appliance from the NetWitness Suite User Interface Rule library and watch for any errors in Reporting Engine log located at:
		`/home/rsasoc/rsa/soc/reporting-engine/logs`
		Launch REST for the device and watch for any error if you run the following query:
		`/sdk?msg=language&force-content-type=text/plain&expiry=600&size=10`

Problem	Possible Causes	Solutions
No results are displayed after running query from NetWitness Suite User Interface via the Reporting Engine.		Run the query on the Reporting Engine and watch for `/var/log/messages` on the data source. Look for an exact query that matches the data source. **TIP**: Search for `[SDK-Query]` in log file. Copy the exact query and run from REST SDK to see if you get any results. REST Query: /sdk?msg=query&force-contenttype=text/plain&expiry=600&query=select%20user.dst&size=10
Workbench Available storage indicator in Workbench Collections Tab is not accurate.	Available storage indicator in the User Interface displays the default Collections directory shown below: /VAR/NETWITNESS/WORKBENCH/COLLECTIONS	None.
Unable to open new collections after opening existing collections.	There is a workbench configuration called “Max Open Collections” that is set to 25 by default. This configuration specifies the number of collections that can be open at the same time.	You can modify this number. A setting of zero disables the limit of maximum open collections.

Problem	Possible Causes	Solutions
Successfully opened a collection that got to Ready state. But after a while, the collection automatically changed to Closed state.	There is a workbench configuration called “collection.timeout” that is set to 1200 seconds by default. This configuration specifies the number of seconds before an idle collection is automatically closed. Maximum time allowed before timeout occurs is 86,400 seconds (24 hours).	A setting of zero disables the timeout.
Querying for a time range using `/database manifest` command returned blank output.	Blank output indicates that there are no **nwdb** files available for the time range.	None.
Created collection, but collection status is not available in Jobs, and collection is not displayed in workbench Collections tab.	You might be running in a mixed mode environment (for example, creating a collection on a 10.4.x version of workbench from a 10.5 NetWitness Suite User Interface.	The collection is displayed in the workbench Collections tab after you reload the page.

Problem	Possible Causes	Solutions
Noticed blank Date Range and Date Created values for collections.	All collections display blank Date Range and blank Date Created values.	Date Range and Date Created values are displayed after upgrading to 10.5.
Discrepancy in behavior of adding workbench collections as a data source to Reporting Engine.	This behavior depends on whether you have a trusted connection or a non-trusted connection.	If your workbench service is established with a trusted connection, you should manually add workbench collections as a source to Reporting Engine. If your workbench service is not established with a trusted connection when the workbench restoration collection was created, it automatically sends a message to the Reporting Engine to add it as a source in the Reporting Engine.
Collection attributes (size, date range and date created) are not displayed.	Date range is not displayed for a collection if Jetty service is restarted while restoration is in process. Restoration collections created from an Explorer view display a blank Date Range. Any collections created on a 10.4 Workbench will display blank Date Range and blank Date Created values after upgrading to 10.5. In a mixed mode environment (10.5 NetWitness Server and 10.4.x workbench), size, date range, and date created are not displayed.	None.

Problem	Possible Causes	Solutions
Exception or blank page is displayed when drilling down on a workbench collection.	Collection closed because it exceeded the collection time out.	Investigate the collection from the beginning.
Empty collection is created.	Empty collection is displayed if restoration fails because Workbench service is restarted during collection creation.	None.
Service abruptly shuts down.		Run the service from command line and watch for any errors. For an example, run the command from the server console `/usr/sbin/NwWorkbench` for workbench.
REST request denied.		Verify user.agent.whitelist config located at `/rest/config/`. If non-blank, this should be a regex expression to match valid HTTP user agents. If the regex fails to match, all REST requests will be denied (see allow.missing.user.agent for the potential exception). If blank, all requests are allowed.

Problem	Possible Causes	Solutions
Queries with raw meta return blank values for Raw field.		Verify that you have a relevant `packet db`.

RSA NETWITNESS® SUITE

Security Configuration Guides

for Version 11.1.0.0

RSA NETWITNESS® SUITE

Security Configuration Guide

for Version 11.0

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

Security Configuration Guide Overview 6

Security Configuration Settings 7

Access Control Settings 8

User Authentication 9

- NetWitness Suite Core Trusted Connection 9
- User Accounts 9
- Configuring New Accounts 10
- Authentication Configuration 10
- User Passwords 11
- Security Parameter Settings 11

User Authorization 13

- Access Roles 13

Component Authentication 14

- Host Configuration and Service Authentication 14
- Changing Credentials for Default Configuration Service Accounts 14
- Configuring Live Account Authentication 15
- Configuring Lockbox Authentication 15
- Display Logon Banner for Remote SSH Connections 15

Log Settings 17

- Log Description 17
- Log Management and Retrieval 17

Communication Security Settings 19

- Port Usage 19
- NW Server Host 21
- Archiver Host 22
- Broker Host 22
- Concentrator Host 23
- Event Stream Analysis (ESA) Host 24
- Log Collector Host 26

Log Decoder Host 27
Log Hybrid Host 28
Malware Host 29
Packet Decoder Host 30
Packet Hybrid Host 31

Network Encryption 33

NetWitness Suite Web Server Communications 33
Reporting Engine, ESA and Warehouse Connector : External Communication 33
Log Collector Service 33

Data Security Settings 36

Securing Data 36
Data Privacy 36
Default Storage Passwords 37

Alert System Settings 38

FIPS Compliance 39

NetWitness Suite Components working in FIPS mode 39

Other Security Considerations 41

Changing the RabbitMQ Management Password for Windows Legacy Collectors 41
Hardening the NetWitness Suite Core service 42
Example: 43
NFS Access Controls 43

Secure Deployment and Usage Settings 46

Security Controls Map 47

Securely Enclave 47
Secure Deployment Guidelines 48

Firewall Rules 51

DMZ to Corporate Network 51
Corporate Network to Site 52
Site to Site 52
Live CMS to DMZ 53
RSA Download Central to DMZ 54
External Email Server to DMZ 54

Syslog Server to Site 54
SNMP Server to Site 54

Secure Deployment Settings 55

Secure Maintenance 56

Security Patch Management 56
Virus Scanning 56
Ongoing Monitoring and Auditing 57
Hardware Replacement 57

Physical Security Controls Recommendations 58

Recommendations 58

Supporting Users 59

Preventing Social Engineering Attacks 59
Confirming User Identities 59
Advice for Your Users 60

Security Configuration Guide Overview

This guide provides information about the security configuration settings and security best practices for RSA NetWitness Suite.

This guide applies to NetWitness Suite version 11.0 or later. There will be periodic updates made to the content.

Anyone using this guide should possess experience as a network engineer, equivalent to at least that of a journeyman, and also have a strong understanding of network concepts and TCP/IP communications.

Security Configuration Settings

This topic describes information about various security configuration settings that are designed to help you securely operate RSA NetWitness Suite.

You can adjust the following security configuration settings:

- Access Control Settings
- Log Settings
- Communication Security Settings
- Data Security Settings
- Alert System Settings
- Other Security Considerations

Access Control Settings

Access control settings are designed to enable the protection of resources against unauthorized access or by external components.

- User Authentication
- User Authorization
- Component Authentication

User Authentication

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing RSA NetWitness Suite.

NetWitness Suite Core Trusted Connection

NetWitness Suite Core 11.0 has the ability to connect and authenticate over SSL without having to provide user account information on the service itself. This feature is only available over the native port and not the REST interface. For more information on trusted connection, see *Host and Services Getting Started Guide*.

User Accounts

The following table identifies the default RSA NetWitness Suite user roles including the Administrator (admin) account and several service accounts. When deploying, you must enter a password for the system administrator account and all the service accounts. For more information on passwords and password strength, see "Settings Tab" Help topic in *System Security and User Management Guide*.

Note: Custom roles can be added as required. For instructions, see "Add a Service User Role" topic in *Host and Services Configuration Guides*.

User Roles	Description
Administrators	Full system access
Operators	Access to configurations but not to meta and session content.
Analysts	Access to meta and session content but not to configurations.
SOC_Managers	Same access as Analysts plus additional permission to handle incidents.
Malware_Analysts	Access to malware events and to meta and session content.
Data_Privacy_Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).
Respond_Adminstrator	Access to all Respond server and Incidents permissions.

Note: By default, the Administrator user is assigned to each NetWitness Suite service.

Configuring New Accounts

Each RSA NetWitness Suite user must have an account to log on to the UI. For instructions on adding new user accounts, see "Manage Users with Roles and Permissions" Help topic in *System Security and User Management Guide*.

Caution: RSA recommends that you ensure that users are approved by the company for logging on to the system before creating an account for them. Even if users are approved, RSA recommends that you only assign the minimum set of access permissions that enable the users to perform their jobs.

Authentication Configuration

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing NetWitness Suite. For more information, see "Set Up System Security" topic in the *System Security and User Management Guide*.

Below are recommendations for some of the configurations:

- **Default System Administrator Account**: RSA recommends that you instruct RSA NetWitness Suite administrators on your corporate IT policy and security best practices to generate and manage passwords for the default System Administrator account. RSA recommends that you change the default System Administrator password and the admin passwords for the service accounts per your company's password policy. For more information on password strength settings, see "Password Strength" topic in the *System Security and User Management Guide*. You should change the System Administrator password using the Admin user preferences. For instructions on how to change the password, see "Change the Default admin Passwords" in the *System Security and User Management Guide*.
- **External Authentication**: RSA NetWitness Suite supports external authentication. For more information, see "Configure External Authentication" topic in the *System Security and User Management Guide*.

User Passwords

NetWitness Suite Users

Administrators can set the appropriate level of password strength for the user and can force users to change their passwords when password strength policy changes. Administrators can specify global default user password expiration period and the notification period for the password expiry. For more information, see "Configure System-Level Security Settings" topic in the *System Security and User Management Guide*.

The following table shows the default security parameters settings for passwords.

Caution: RSA recommends that you change these settings in accordance with your corporate policy. Users must ensure the idle period and session time-out is specified.

Parameter	Default Setting
Global Default User Password Expiration Period	0
Notify User <n> Days Prior to Password Expiry	5

NetWitness Suite Core Service Users

Administrators can change the password of a service user and replicate the new password to all the NetWitness Suite Core services with the defined user account. For more information, see "Change a Service User Password" topic in the *Host and Services Configuration Guides*.

You can also change your password from the Preferences panel in the Profile view. For more information, see "Profile View Preferences Panel" topic in the *NetWitness Suite Getting Started Guide*.

Security Parameter Settings

The following table shows the default security parameters settings.

Caution: RSA recommends that you change these settings in accordance with your corporate policy.

Parameter	Default Setting
Lockout Period	20 minutes
Idle Period	10 minutes
Session Timeout	600 minutes

Parameter	Default Setting
Max Login Failures	5

For more information on security parameter settings, see "Security Settings" topic in the *System Security and User Management Guide*.

User Authorization

User authorization settings are designed to control rights or permissions that are granted to a user for accessing a resource managed by RSA NetWitness Suite.

Access Roles

RSA NetWitness Suite allows you to create access roles that you can assign to users. Each access role is mapped to a list of user authorization settings.

For more information, see the following NetWitness Suite 11.0 topics:

- "Role Permissions" in the *Alerting Using ESA Guide*.
- "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Note: Additionally, RSA NetWitness Suite recommends that you review users' task permissions on a routine basis to ensure that each user is granted the correct task permissions.

RSA NetWitness Suite allows access roles to be assigned to users through external group membership or directly to user accounts. RSA recommends that you assign permissions through group membership and not assign permissions directly to user accounts. For more information, see "Map User Roles to External Groups" Help topic in the *System Security and User Management Guide*.

The user roles assigned also control permissions that are granted to accounts that need access to a specific component of NetWitness Suite.

Component Authentication

This topic describes Component authentication settings control the process of verifying an identity claimed by an external or internal system or component.

Host Configuration and Service Authentication

When you install or upgrade to RSA NetWitness® Suite 11.0 or later, trusted connections are established by default with two settings:

1. SSL is enabled.
2. NetWitness Server is connected to core services using the encrypted SSL port.

RSA NetWitness Suite allows secure authentication services for the following hosts as SSL is enabled by default:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Archiver
- ESA
- Malware Analysis

Note: By default all the services on the hosts have SSL enabled.

For more information, see Help topic in the *Host and Service Configuration Guides*.

Changing Credentials for Default Configuration Service Accounts

For instructions on resetting the password for the admin of the host service accounts, see "Users Tab" topic in the *Host and Services Configuration Guides*.

Note: The default user name that the host service accounts admin cannot be modified.

Configuring Live Account Authentication

RSA NetWitness Suite supports secure authentication for the Live account connection to Content Management System (CMS) as the SSL is enabled by default. The default communications port on the CMS is 443. For instructions on configuring this setting, see "Configure Live Settings" topic in the *System Configuration Guide*.

Configuring Lockbox Authentication

Lockbox provides an encrypted file that Warehouse Connector or Log Collector uses to store and protect sensitive data. You need to create the lockbox by providing a lockbox password while configuring the Warehouse Connector or Log Collector for the first time. For more information on lockbox setup, see the following topics:

- "Log Collector - Step 3: Set Up a Lockbox" in the *Log Collection Guides*.
- "Warehouse Connector - Step 2: Create Lockbox" in the *Host and Services Configuration Guides*.

Display Logon Banner for Remote SSH Connections

RSA NetWitness Suite allows you to customize the logon banner to display standard government or corporate warning signs for SSH remote connections to the hosts. An example message would be the following:

"This system is private. Use or misuse may be logged and invalid access pursued."

1. Log on to the appliance using root credentials.
2. Type **cd /etc/** to switch to the **/etc/** directory.
3. Edit the **/etc/issue.net** file with the required banner text.
4. Save the changes and exit.
5. Type **cd /etc/ssh** to switch to the **/etc/ssh** directory.
6. Edit the **/etc/ssh/sshd_config** file to remove the comment for the banner and provide the location of the banner text file (For example, **/etc/issue.net**).
   The following file is an example of an **sshd.config** file before being modified:

   ```
   # no default banner path
   #Banner none
   ```

   The following file is an example of an **sshd.config** file after being modified:

   ```
   # no default banner
   #Banner /etc/issue.net
   ```

7. Save the changes and exit.
8. Type **service sshd restart** in order to restart the sshd service.

Log Settings

A log is a chronological record of system activities that enables the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction.

Global Audit Logging provides NetWitness Suite Auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location. NetWitness Suite audit logs collect in a centralized system that converts them into the required format and forwards them to an external syslog system. The external syslog system can be a third-party syslog server or a Log Decoder. For more information, see "Global Audit Logging Overview" topic in the *System Configuration Guide*.

Log Description

The following table shows the security-relevant logs provided by RSA NetWitness Suite.

Component	Reference
Appliance and Service Logs	See "Services Explore View and Services Logs View" topics in the *Host and Services Configuration Guides* and "Configure Log File Settings" topic in the *System Configuration Guide*.
Audit Logs	See " Configure Global Audit Logging" topic in *System Configuration Guide*.
Syslogs	See " Configure Syslog and SNMP Settings" topic in the *System Configuration Guide*.

Log Management and Retrieval

For more information on:

- Log settings: See "Configure Log File Settings" topic in the *System Configuration Guide*.

  Note: RSA recommends that you set the maximum log file size in accordance to your corporate policy.

- Log forwarding: See "Set Syslog Forwarding" topic in the *Host and Services Configuration Guides*.
- Setting log overrides:
  You may override the default logging levels if you want to include messages generated by specific modules.

`Syntax: <module>=<level>`

`SDK-Language=none`

Where level is one or more of `"none|debug|info|warning|failure|audit|all"`, all options must be separated by a pipe |

none and all are mutually exclusive with each other and all other options.

Overrides are useful for query auditing (that is, those modules that begin with SDK-) or for debugging by module (that is, Index)

- Data
- Engine
- Index
- Network
- Packet
- Parse
- Decoder
- Rules
- Concentrator
- Appliance
- SDK
- SDK-Query
- SDK-Values
- SDK-Language
- SDK-Info
- SDK-Session
- SDK-Timeline
- SDK-Content
- SDK-Search

Note: RSA recommends that you restrict permissions to the log files folder to the appropriate user.

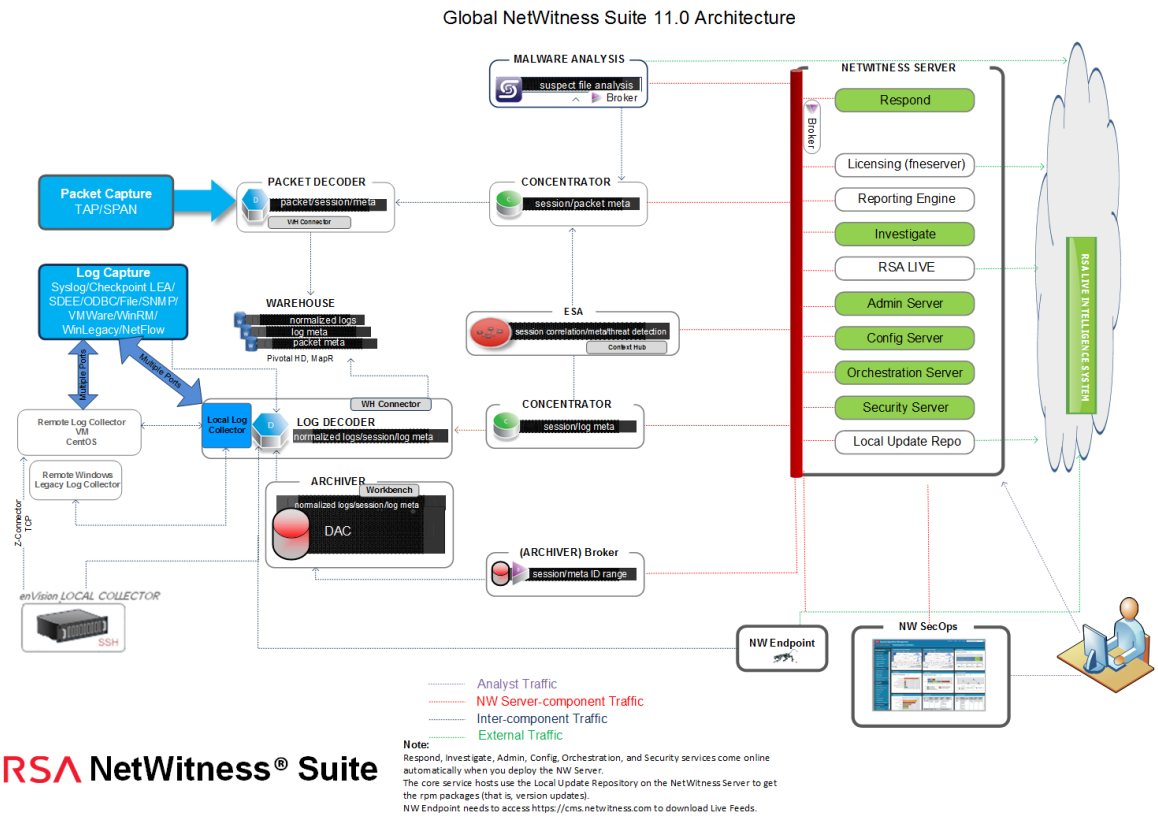
Communication Security Settings

Communication security settings are designed to enable the establishment of secure communication channels between RSA NetWitness Suite components, as well as between RSA NetWitness Suite components and external systems or components.

Port Usage

To help ensure security, RSA recommends that you configure your firewall rules and access control lists to expose only the ports and protocols necessary for the operation of RSA NetWitness Suite. The services, such as Reporting Engine, Respond Service, Malware, Log Collector, Live account, Broker, Concentrator, Decoder, and Log Decoder, use specific TCP ports to communicate with each other and the following:

- Web user client interfaces
- Live CMS
- LDAP synchronization
- Third-party email server
- NetWitness Suite console



RSA NetWitness® Suite

All communication from NetWitness Suite is over the native NetWitness Suite Core ports as against the REST API ports. The additional native NetWitness Suite Core port per appliance allows an administrator to enable secure (SSL) network communications while still being able to utilize non-secure (HTTP and NetWitness Suite Core native) connectivity methods for communication between services that are present on the same system. Administrators can toggle the ports on and off to support only SSL, only non-SSL, or both.

Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness Suite deployment to communicate with each other.

This section contains the port specifications for the following hosts.

NW Server Host

Archiver Host

Broker Host

Concentrator Host

Event Stream Analysis Host

Log Collector Host

Log Decoder Host

Log Hybrid Host

Malware Host

Packet Decoder Host

Packet Hybrid Host

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
Admin Work-station	NW Server	TCP 443, 80	nginx - NetWitness UI
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
Admin Work-station	NW Server	TCP 22	SSH
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Server	NW Server	TCP 50003, 50103, 56003	Broker Ports
NW Server	NW Server	TCP 5671	RabbitMQ-amqp
NW Server	NW Server	UDP 50514	Audit Ports
NW Server	NW Server	TCP 7000, 7003, 7009, 7010	Launch Ports
NW Server	NW Server	TCP 50006, 50106, 56006	NetWitness Appliance Ports
NW Hosts	NW Server	UDP 123	NTP
NW Hosts	NW Server	TCP 27017	MongoDB
NW Server	NW Server	UDP 123	NTP
NW Server	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations
NW Server	NW Endpoint	TCP 443, 9443	

Archiver Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Archiver	TCP 15671	RabbitMQ Management UI
Admin Workstation	Archiver	TCP 22	SSH
NW Server	Archiver	TCP 56008 (SSL), 50008 (Non-SSL), 50108 (REST)	Archiver Application Ports
NW Server	Archiver	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Archiver	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Non-SSL), 50107 (REST), UDP 514	Workbench Application Ports
Archiver	Archiver	UDP 50514	Audit Data
Archiver	Archiver	UDP 123	NTP
Archiver	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Broker Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 22	SSH
NW Server	Broker	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
NW Server	Broker	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Broker	Broker	UDP 50514	Audit Data
Broker	Broker	UDP 123	NTP
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Concentrator Host

Source Host	Destination Host	Destination Ports	Comments
Admin Work-station	Concentrator	TCP 15671	RabbitMQ Management UI
Admin Work-station	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW Server	Concentrator	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Concentrator	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Concentrator	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations
Concentrator	Concentrator	UDP 50514	Audit Data
Concentrator	Concentrator	UDP 123	NTP

Event Stream Analysis (ESA) Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI
Admin Workstation	ESA	TCP 22	SSH
NW Server, NW End-point, ESA Sec-ondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 50030 (SSL)	ESA Applic-ation Port

Source Host	Destination Host	Destination Ports	Comments
NW Server	ESA	TCP 50035 (SSL)	ESA Application Port
NW Server	ESA	TCP 50036 (SSL)	ESA Application Port
NW Server	ESA	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
ESA	cms.netwitness.com	TCP 443	Live
ESA	NFS Server	TCP 111 2049 UDP 111 2049	NTP
ESA	Active Directory	636 (SSL)/389 (Non-SSL)	
NW Server	ESA	80 (HTTP)/ 443 (HTTPS) (REST)	
ESA Primary	Archer	443 (SSL)/80 (Non-SSL)	
ESA Primary	ESA Primary	TCP 7007	Launch Port
ESA Primary	ESA Primary	UDP 50514	Audit Data
ESA Primary	ESA Primary	UDP 123	NTP

Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Collector	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*. (missing or bad snippet)	
Log Event Sources	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Log Collection Ports
Log Event Sources	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Log Collection FTP/S Ports
NW Server	Log Collector	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Collector	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Collector	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Collector	Log Collector	UDP 50514	Audit Data
Log Collector	Log Collector	UDP 123	NTP

Source Host	Destination Host	Destination Ports	Comments
Log Collector	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC installations

Log Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Log Event Sources	See *Log Collection Configuration Guide*.	
Log Event Sources	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Decoder	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Decoder	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Decoder	Log Decoder	UDP 50514	Audit Data
Log Decoder	Log Decoder	UDP 123	NTP
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*.	
Log Event Sources	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports

Source Host	Destination Host	Destination Ports	Comments
Log Event Sources	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Log Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
Admin Workstation	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malware Application Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Malware	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Malware	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Malware	TCP 5432	Postgresql
NW Server	Malware	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	Malware	UDP 50514	Audit Data
Malware	Malware	UDP 123	NTP
Malware	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Packet Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Decoder	TCP 22	SSH

Source Host	Destination Host	Destination Ports	Comments
NW Server	Packet Decoder	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Decoder	Packet Decoder	UDP 50514	Audit Data
Packet Decoder	Packet Decoder	UDP 123	NTP
Packet Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Packet Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Hybrid	TCP 22	SSH
NW Server	Packet Hybrid	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Packet Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Hybrid	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

Note: For the latest architecture and port usage information, see "Network Architecture and Ports" topic in the *Deployment Guides*.

Topics

- Network Encryption

Network Encryption

You can configure RSA NetWitness Suite to send or receive data from external data sources.

Note: RSA recommends that whenever you have the option to choose between unsecured and secured versions of a communication protocol, you choose the secured version.

NetWitness Suite Web Server Communications

The RSA NetWitness Suite UI or web server which communicates with the Live Service (CMS) over port 443 using the HTTPS protocol.

Note: During installation, the system is engineered to set the default communication protocol to HTTPS over port 443.

Reporting Engine, ESA and Warehouse Connector : External Communication

RSA recommends that you use the secure tcp protocol and enable an SSL connection while configuring Reporting Engine, ESA, Warehouse Connector, Licensing, and Malware.

For more information on Reporting Engine, see "Step 4: Configure Output Actions" topic in the *Host and Services Configuration Guides*.

For more information on Malware external communication, see " Step 1. Configure Malware Analysis Operating Environment" topic in the *Host and Services Configuration Guides*.

For more information on ESA, see " Notification Methods" topic in the *Alerting Using ESA Guide*.

For more information on the Warehouse Connector, see "Configure Warehouse Connector" topic in the *Host and Services Configuration Guides*.

For more information on Licensing, see "Configure NetWitness Suite Notifications" topic in the *Alerting Using ESA Guide*.

Log Collector Service

To help secure communication between the Log Collector service running on the Log Decoder and the event sources, RSA recommends the protocols in the following table

Event Source	Protocol	Resources
File	SFTP, SCP, FTPS	For more information, see " File Collection Protocol Configuration" topic in the *Log Collection Guides*.
ODBC	ODBC	For more information on configuring an ODBC event source, see "ODBC Collection Configuration" topic in the *Log Collection Guides*. **Note:** Note: Depending on the event source, administrators can configure additional progress driver parameter for secure connections. For more information, see Progress document at https://www.progress.com/odbc/resources/documentation/books-and-readme-file. For more information on using a Certificate, see the certificate creation kit at http://openssl.org/. For more information on securing communication with SQL Server, Oracle, and ODBC, see the URLs: http://technet.microsoft.com/en-us/l...QL.105%29.as http://technet.microsoft.com/en-us/l.../cc754431.aspx http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html http://www.psdn.progress.com/progres...92/odr/odr.pdf
Windows	HTTPS	For more information on configuring a Windows event source to use certificates and enable HTTPS, see NetWitness Suite 11.0 Help topic *Windows Collection Configuration Guide*.
Check Point	OPSEC LEA	For more information on configuring a Check Point event source to use certificates, see NetWitness Suite 11.0 Help topic *Check Point Collection Configuration Guide*.
Netflow	Netflow	For more information on configuring a Netflow event source to use certificates, see NetWitness Suite11.0 Help topic *Netflow Collection Configuration Guide*.

Event Source	Protocol	Resources
SDEE	SDEE	For more information on configuring a SDEE event source to use certificates, see NetWitness Suite 11.0 Help topic *SDEE Collection Configuration Guide*.
SNMP	SNMP	For more information on configuring a SNMP event source to use certificates, see NetWitness Suite 11.0 Help topic *SNMP Collection Configuration Guide*.
VMware		For more information on configuring a VMware event source to use certificates, see NetWitness Suite11.0 Help topic *VMware Collection Configuration Guide*.
Legacy Windows and NetApp		For more information on configuring a Legacy Windows event source to use certificates, see NetWitness Suite11.0 Help topic *Legacy Windows and NetApp Collection Configuration Guide*
Amazon Web Services (AWS) Cloud Trail	HTTPS	For more information on configuring an AWS Cloud Trail event source to use certificates, see NetWitness Suite 11.0 Help topic *AWS (CloudTrail) Collection Configuration Guide*.

Note: For more information on enabling SSL for component communications, see Component Authentication.

Data Security Settings

Data security settings are designed to enable the definition of controls to prevent data permanently stored by RSA NetWitness Suite from being disclosed in an unauthorized manner.

Securing Data

To help protect online data, such as current database, log, and configuration files, RSA recommends that you restrict access to the files and database and configure permissions so that only trusted administrators are allowed to access them.

RSA recommends that you back up your sensitive data, encrypt it, and keep it in a secure physical location in accordance with your corporate disaster recovery and business continuity policies.

The backup can be done in the following ways:

- Regular backup of Configuration and Data files – You can back up and restore data and configuration files for the core host and services and all the modules of NetWitness Suite. For more information, see "Back Up and Restore Data for Hosts and Services" topic in the *System Maintenance Guide*.
- Regular backup of critical configuration – You can export configurations using the Export option available on the UI. For example, you can take a backup of critical rules, reports, alerts, ESA rules, dashboards, investigation profiles, meta groups, event sources, global notifications, and so on. For more information, see topics:
  - "Export a Rule, Export an Alert and Export a Report" in the *Reporting Guide*.
  - "Rule Library View and Dashboard" in the *Alerting using ESA Guide*.
  - "Manage Profiles Dialog and Export a Meta Group" in the *Investigation and Malware Analysis Guide*.
  - "Events View and Export Event Sources" in the *Event Source Management Guide*.
  - "Global Notifications Panel Toolbar" in the *System Configuration Guide*.

Data Privacy

Data Privacy is very integral and helps you manage privacy-sensitive data. You can achieve data privacy using the Data Privacy Officer (DPO) role. The DPO can configure NetWitness Suite to limit the exposure of meta data and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness Suite include:

- Data Obfuscation
- Data Retention Enforcement
- Auditing Logging

For more information, see topics in the Data Privacy Management.

Default Storage Passwords

The default storage passwords for database accounts that store alerts in ESA, Respond Service, and Data Science can be changed. For more information, see "Change Default Storage Passwords" topic in the *Host and Services Configuration Guide*.

Alert System Settings

For instructions on configuring NetWitness Suite to send alerts or notifications, see following topics in the *System Configuration Guide*:

- "Email Configuration Panel"
- "Global Audit Logging Configurations Panel"
- "Global Notifications Panel"

FIPS Compliance

This topic provides information on the Federal Information Processing Standards (FIPS) compliant mode for RSA NetWitness Suite. The FIPS publications are guidelines that set best practices for software and hardware security products for the protection of valuable and sensitive information.

When the FIPS compliant mode is used, products that support one or more FIPS standards can be set into a mode where the product uses FIPS approved algorithms and methods only.

NetWitness Suite supports both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

NetWitness Suite Components working in FIPS mode

The table below lists the NetWitness Suite components that work in FIPS mode. The method you use to activate or deactivate FIPS depends on the type of security library used by your NetWitness Suite services. Your NetWitness Suite services use the security libraries, as mentioned in the following table.

Services	Security Library
Event Stream Analysis (ESA), Malware Analysis, Reporting Engine, NetWitness Suite Host, Respond Service, and Context Hub	BSAFE
Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, Archiver, and Workbench	BSAFE

FIPS 140-2 Certified Cryptographic Modules are enabled for all services that perform cryptographic operations. For the following services, although the FIPS Cryptographic Module is leveraged, the use of FIPS cipher suites is not being enforced:

- NTP: UPD Port 123
- TCP: SSH Port 22
- TCP: Salt API Loopback Port 8000
- CollectD
- Log Collector
- Log Decoder

Note: In 11.0, FIPS is enabled by default for all services, except for Log Collector and Log Decoder. For more information on how to enable FIPS on log Collector and Log Decoder see *RSA NetWitness® Suite 11.0 Release note.*

Note: Security Technical Implementation Guide (STIG) is not supported for version 11.0.

Other Security Considerations

This topic describes various other security configuration settings that are not covered in previous sections.

Changing the RabbitMQ Management Password for Windows Legacy Collectors

For Windows Legacy Log Collectors (WLCs), a default password is used for the "logcollector" username to access the RabbitMQ broker on that machine. RSA recommends that you change the password for WLCs, per the procedure outlined, which involves changing the RabbitMQ password for the Log Collector and for the RabbitMQ broker.

Note: For CentOS, changing the RabbitMQ password is not supported.

If you are using a Log Collector, you may have to initialize the "lockbox". For instructions, see "Step 3: Set Up a Lockbox" topic in the *Log Collection Guides*.

To change the RabbitMQ password:

1. Change the RabbitMQ password in Log Collector:
   a. Go to the Explore view for the Log Collector service.
   b. Right-click the **event-broker** node and select **config**.
   c. Type the new password in the **amqp_password** field. The password is encrypted by a key that is managed through the lockbox of this Log Collector. This only changes the password on the Log Collector side.

   Note: Most of the settings should not be changed. Ensure you do NOT change the Message Queue User Name "amqp_username" because it is referred to in some certificate checks.
2. Change the RabbitMQ password for the RabbitMQ broker:
   a. Go to the Explore view for the Log Collector service.
   b. Right-click the **event-broker** node and select **properties**.
   c. Select **passwd** in the drop-down list.
   d. In the **Parameters** field, type the old and new password.
   Ensure you remember your old password. If it was never changed, it should be "netwitness" by default.

Example: `Parameters: oldpw=<netwitness> newpw=<YourNewPasswordHere>`

e. Click **Send**.

Hardening the NetWitness Suite Core service

By default, all NetWitness SuiteCore services ship with a default username and password and with SSL turned off. To harden the service, you have to run it with the command line option `-s harden=true`.

Using a Decoder, here's an example command line:

```
NwDecoder -s harden=true -s defaultUsername=<username> -s
defaultPassword=<password>
```

The above command does the following:

1. Removes the default admin account (with caveats, see below).
2. Creates a new account <username> with a password of <password> (thus meeting the password requirements below).
3. Enables SSL on both the native and REST ports.
4. Strengthens default password requirements:
   - /users/config/account.lockout.time = 60
   - /users/config/password.alpha.lowercase.min = 1
   - /users/config/password.alpha.uppercase.min = 1
   - /users/config/password.length.min = 8
   - /users/config/password.numeric.min = 1
   - /users/config/password.symbol.min = 1
5. Sets /rest/config/user.agent.whitelist = Apache-HttpClient/\d\.\d\.\d

   Note: This setting prevents the browsers to connect to the REST port.

The caveat for changing the default user account is that there cannot be an already existing configuration file. This is always true the first time the service is run or before the service is licensed. To harden a service, you must run it before a configuration is written or delete whatever configuration file exists and then harden.

To alter the command line for a service that writes its own upstart script without actually SSHing into the box and modifying the script, there is a new parameter that you can pass to either the /sys shutdown or /decoder reset command (substitute decoder for the actual service name) and this parameter is called "cl" for command line. What you do is pass name=value pairs to the "cl" parameter and those parameters will take affect on the next restart of the service.

Example:

```
/sys shutdown reason="Restart because license was applied"
cl="harden=true default
Username=<username> defaultPassword=<password>"
```

The above command shuts down the service (which should be restarted by Linux upstart) and the command line parameters will be applied on the restart. This command line exactly matches the command line given above for the decoder service. If you want to do a configuration reset, you can use the following:

```
 /broker reset config=true cl="harden=true defaultUsername=<username>
defaultPassword=<password>"
```

This will delete the broker configuration file and create a new default configuration that is automatically hardened with the given default account and credentials. The admin account will not exist when the broker restarts, only the <username> account exists.

NFS Access Controls

By default, the NFS mounts are wide open. To lock them down to a specific address, you must edit the exports file and specify the IP addresses that are allowed to interact with the SAW.

The SAW NFS service is managed from the command line using *mapr-nfsserver*.

```
[root@saw-node1 ~]# service mapr-nfsserver
Usage: /etc/init.d/mapr-nfsserver {start|stop|status|restart|}
[root@saw-node1 ~]# service mapr-nfsserver status
nfsserver (pid 5692 5691) is running...
[root@saw-node1 ~]#
```

If nfs-utils is installed on the node, you can execute a *showmount* on the localhost to see the exposed exports.

```
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
[root@saw-node1 ~]#
```

Exports are controlled using the exports file in the */opt/mapr/conf* directory.

```
[root@saw-node1 ~]# cat /opt/mapr/conf/exports
# Sample Exports file
# for non /mapr exports
# <Path> <comma separated cldb addresses=host:port> <exports_control>
# for /mapr exports
# <Path> <exports_control>
#access_control -> order is specific to default
# list the hosts before specifying a default for all
# a.b.c.d,1.2.3.4(ro) d.e.f.g(ro) (rw)
# enforces ro for a.b.c.d & 1.2.3.4 and everybody else is rw
# special path to export clusters in mapr-clusters.conf. To disable
exporting,
# comment it out. to restrict access use the exports_control
#
/mapr (rw)
#to export only certain clusters, comment out the /mapr & uncomment.
# Note: this will cause /mapr to be unexported
#/mapr/clustername (rw)
#to export /mapr only to certain hosts (using exports_control)
#/mapr a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster1 rw to a.b.c.d & ro to e.f.g.h (denied for
others)
#/mapr/cluster1 a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster2 only to e.f.g.h (denied for others)
#/mapr/cluster2 e.f.g.h(rw)
# export /mapr/cluster3 rw to e.f.g.h & ro to others
#/mapr/cluster2 e.f.g.h(rw) (ro)
[root@saw-node1 ~]#
```

To restrict the SAW exports to a certain IP address or group of IPs, you must first edit the exports file and then restart the *mapr-nfsserver service*.

```
[root@saw-node1 ~]# vi /opt/mapr/conf/exports
[root@saw-node1 ~]# cat /opt/mapr/conf/exports | grep ^/mapr
/mapr 10.42.1.87(rw)
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
```

```
[root@saw-node1 ~]# service mapr-nfsserver restart
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr 10.42.1.87
/mapr/saw 10.42.1.87
[root@saw-node1 ~]# mount -t nfs -o nolock,tcp localhost:/mapr/saw
/saw
mount.nfs: access denied by server while mounting localhost:/mapr/saw
[root@saw-node1 ~]#
```

Note: Trying to mount the export on the localhost will fail as only a specific host IP is now allowed to use the NFS mount

Secure Deployment and Usage Settings

This topic describes the settings for secure deployment and usage. It is very important to protect all physical, local, and remote access to the RSA NetWitness Suite appliances. It is also important to restrict all access methods to the absolute minimum required to maintain RSA NetWitness Suite.

Note: RSA recommends that you do not set up the test environments to be exact copies of the full production environment. If the test environment is identical to the production environment, you should take the same precautions to protect the test environment as you do in the production environment.

Security Controls Map

This topic describes the security controls map. An RSA NetWitness Suite deployment can consist of the following components:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Context Hub
- Malware
- ESA
- Archiver
- NetWitness Warehouse
- NetWitness Server
- External Warehouse - Hortonworks
- External CMS Library (Live)

NetWitness Suite supports integration with products such as RSA NetWitness Endpoint and RSA Archer.

RSA recommends that you access the host on secure client machines within the network. If you must access the host through remote access, RSA recommends that you connect to the network through a secure VPN connection. Only allow remote access to NetWitness Suite hosts for secure maintenance using the Remote Desktop Protocol (RDP) through a secure VPN connection.

Caution: RSA recommends that you deploy the hosts in a secure location, where physical access to the hosts are restricted only to the personnel who manage the hosts.

Securely Enclave

To help protect NetWitness Suite against unauthorized authentication and access by end users or machines, RSA recommends that you deploy NetWitness Suite hosts such as Broker, Concentrator, and Decoder.

You can help create a secure enclave by separating the low security corporate network from the high security network with firewalls. To help create a secure enclave, RSA recommends that you:

- Implement basic physical security elements, policies, procedures, and processes for the low security network.
- Provide access to the hosts within the secure enclave through a secure virtual private network (VPN) tunnel only, such as IPSec tunnel, to establish encryption and authentication of all network traffic to and from the hosts.

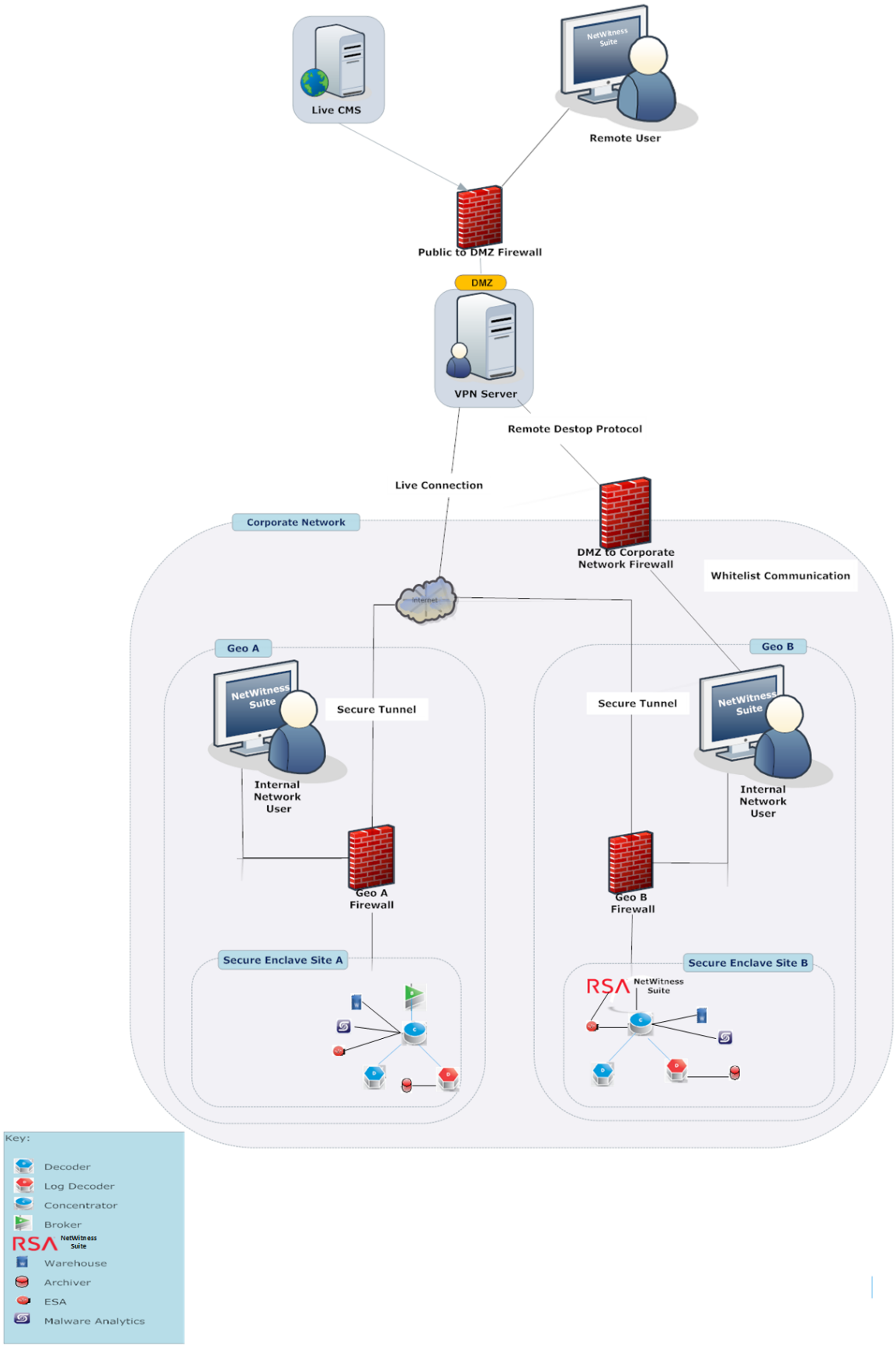
Note: The client machines through which you access NetWitness Suite can be present outside of the Secure Enclave.

Secure Deployment Guidelines

To help ensure a secure deployment, RSA recommends that you:

- Deploy multiple hosts in the corporate network. The multiple hosts in the example are in two geographic locations and include the following components:
  - NetWitness Suite
  - Broker
  - Packet Decoder
  - Log Decoder
  - Concentrator
  - ESA
  - Archiver
  - NetWitness Warehouse
  - Malware Analysis
- Ensure that all the components are connected to the same subnetwork.
- Deploy firewalls at each site to ensure the secure transfer of data from an instance of NetWitness Suite at one site to another instance of NetWitness Suite located at a different site.
- Configure firewall rules to control all communication between different sites and other components in the network as depicted in the previous figure.
- Implement data transfer between sites using a secure tunnel IPSec.

The following figures show the deployment of multiple sites within a corporate network:


Live CMS
NetWitness Suite
Remote User
Public to DMZ Firewall
DMZ
VPN Server
Remote Destop Protocol
Live Connection
Corporate Network
DMZ to Corporate Network Firewall
Whitelist Communication
Internet
Geo A
Geo B
NetWitness Suite
Secure Tunnel
Secure Tunnel
NetWitness Suite
Internal Network User
Internal Network User
Geo A Firewall
Geo B Firewall
Secure Enclave Site A
Secure Enclave Site B
RSA NetWitness Suite
Key:
Decoder
Log Decoder
Concentrator
Broker
RSA NetWitness Suite
Warehouse
Archiver
ESA
Malware Analytics

Firewall Rules

It is important that you use a firewall to restrict network traffic between RSA NetWitness Suite and external systems. RSA NetWitness Suite recommends that you configure firewall rules to help ensure secure communication for the following connections:

- Demilitarized zone (DMZ) to corporate network
- Corporate network to site sub network
- Site to site
- Live CMS to DMZ
- External email server to DMZ

Note: RSA recommends that you restrict access from client hosts to only known IP addresses. For example, if you set up the NetWitness Suite Client UI on IP address 192.168.0.1, configure your firewall to allow only the IP address 192.168.0.1 to connect to the NetWitness Suite host.

Note: The firewall rules should be configured on an external firewall and not on any of the NetWitness Suite host.

RSA recommends that you configure firewall rules as described in the sections below. These recommendations are based on the following assumptions:

- You have a stateful firewall, indicating that only the establishment of TCP ports is considered.
- You specify the direction of communication for the UDP ports because the connections are sessionless.
- You deploy NetWitness Suite as shown in the Security Controls Map.
- The firewall processes the rules top to bottom, finishing with a generic drop of all the packets.

DMZ to Corporate Network

RSA recommends that you:

- Configure whitelist communication from the VPN server in the DMZ to the client machines on which you run RSA NetWitness Suite applications such as NetWitness Suite Web UI.
- Create firewall rules for all the machines from which you intended to remotely access the corporate network through Remote Desktop Protocol (RDP).

Corporate Network to Site

RSA recommends that the firewall at each RSA NetWitness Suite site allow access only from designated client machines through a whitelisted IP address and port.

RSA recommends that you secure the following ports to ensure secure communication between the client machine that is set as the RSA NetWitness Suite Web UI and the NetWitness Suite site:

- TCP 443

For more information, see Communication Security Settings. To help ensure secure communication between the client machines that access the NetWitness Suite UI and a site, you must set up the firewall rules as shown below:

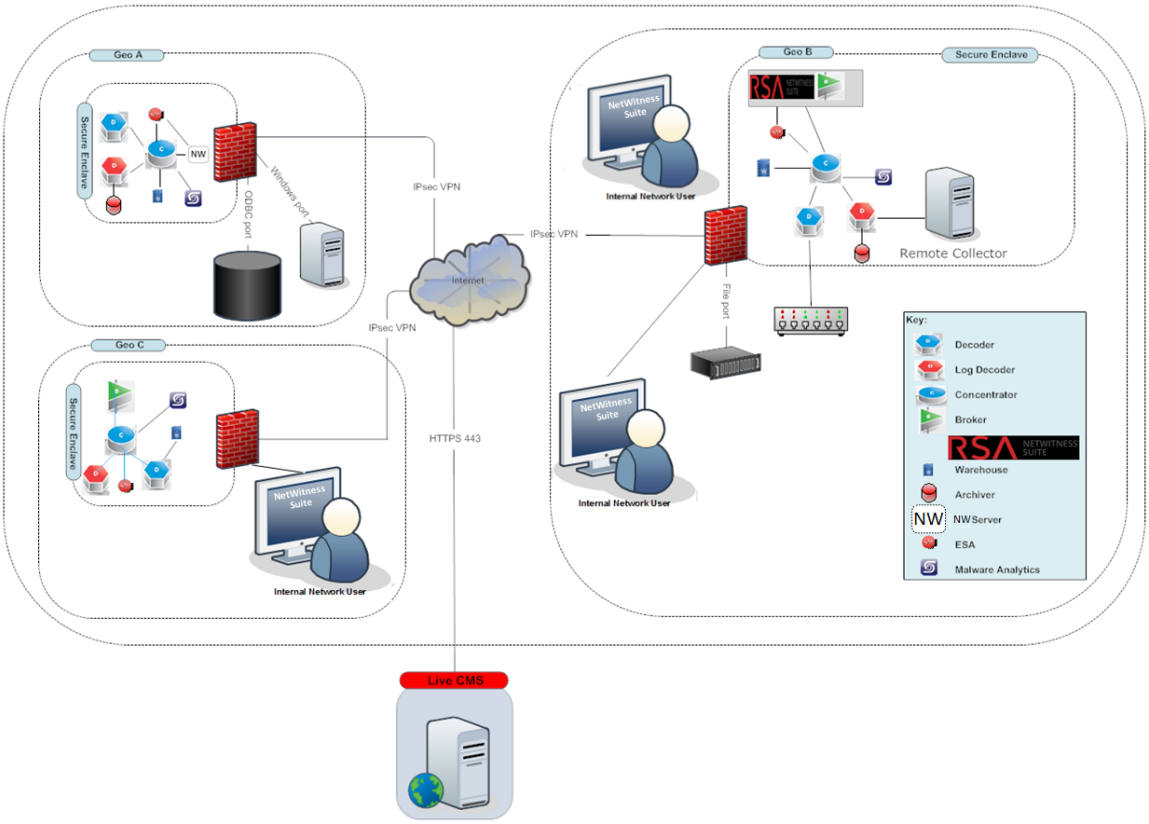
ALLOW $nwclient_IP to $nwsite_IP on port 443/tcp

DROP all from * to *

where **nwclient_IP** is the IP address assigned to the client machine that is set as the NetWitness Suite web UI and **nwsite_IP** is the IP address assigned to the Broker host within which the RSA NetWitness Suite web server is running.

Site to Site

RSA NetWitness Suite may run in multiple sub-networks within your corporate network, called sites. You can configure RSA NetWitness Suite to allow the hosts located in one site to communicate with the hosts in another site.



For this scenario, RSA recommends that you do the following:

- Ensure that the firewall at each RSA NetWitness Suite site allows communication between two sites only through a whitelisted IP address and port. For a graphical depiction of the site-to-site security control map showing the site firewalls, see the above figure.
- NetWitness Suite system update uses port 80. That means NetWitness Server site to another site (where brokers, decoders exist), port 80 should be open.

Live CMS to DMZ

To ensure secure communication between the RSA NetWitness Suite site and Live CMS, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Live_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Live_IP** are the IP addresses assigned to the NetWitness Suite site and the Live CMS respectively.

Note: If you are using proxy server with self-signed certificate, you must add exception in proxy server rule to allow traffic between Live CMS server (cms.netwitness.com, port 443) and NetWitness Server.

RSA Download Central to DMZ

To ensure secure communication between the RSA NetWitness Suite site and RSA Download Central, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $rsa_DLC_IP on port 80/tcp

DROP all from * to *

where **nw_site_IP** and **rsa_DLC_IP** are the IP addresses assigned to the NetWitness Suite site and RSA Download Central respectively.

External Email Server to DMZ

To ensure secure communication between the RSA NetWitness Suite site and the External Email Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Email_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Email_IP** are the IP addresses assigned to the NetWitness Suite site and the external email server respectively.

Syslog Server to Site

If you have enabled the syslog port, to ensure secure communication between the RSA NetWitness Suite site and the Syslog Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Syslog_IP on port 514/udp

DROP all from * to *

where **nw_site_IP** and **Syslog_IP** are the IP addresses assigned to the NetWitness Suite site and the syslog server respectively.

SNMP Server to Site

If you have enabled the SNMP port, to ensure secure communication between the RSA NetWitness Suite site and the SNMP Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $SNMP_IP on port 1610/SNMP

DROP all from * to *

where **nw_site_IP** and **SNMP_IP** are the IP addresses assigned to the NetWitness Suite site and the SNMP server respectively.

Secure Deployment Settings

The following table shows the security controls that RSA recommends putting in place to help secure the deployment.

Default Deployment Setting	Secure Deployment Settings	Pros of Secure Deployment Settings	Cons of Secure Deployment Settings	Instructions on how to configure secure deployment settings
HTTPS is enabled by default between the NetWitness Suite client and the server	For the best possible security between the client and the server, use certificates from CA.	Provides a high level of protection for the communication between client and server by avoiding tampering, spoofing, and man-in-the middle attacks.	May have impact on performance	For instructions on installing external certificates, see SSL Certificate Guidance for NetWitness Suite

Secure Maintenance

This topic describes some common solutions to help ensure secure maintenance.

Security Patch Management

All security patches for RSA NetWitness Suite originate at RSA and are available for you via the NetWitness Suite User Interface. For more information, see "Manage NetWitness Suite Updates" topic in the *System Maintenance Guide* .

The following table lists the third-party components for which patches are needed.

Third-party Component for which patch is needed	Frequency of Patch	EMC Respons-ibility (Y/N)	Customer Responsibility (Y/N)	Reference to instructions for Applying Patch
NetWitness Suite Hosts	Monthly and Quarterly	Y	Y	Based on EMC RSA recom-mendations

Note: From 2016 onwards, security patches will be part of the product release only and will not be shipped out separately.

Virus Scanning

RSA recommends that you:

- Deploy anti-virus client software on the deployed servers in accordance with your enterprise requirements.
- Run anti-virus and anti-malware tools with the most current definition files on the deployed servers.
- Scan all files/drivers before uploading on the deployed server.
- Follow best practices for patch management and regularly review available patches for all anti-virus and anti-malware software.

Ongoing Monitoring and Auditing

As with any critical infrastructure component, RSA NetWitness Suite recommends that you constantly monitor your system and perform periodic and random audits (for example, configuration, permissions, and security logs). You should ensure that the configurations and user access settings match your company policies and needs. For more information, see "Global Audit Logging Configurations Panel" topic in the *System Configuration Guide*.

Hardware Replacement

If RSA NetWitness Suite hardware fails or is faulty, order a replacement by contacting RSA Customer Support. While awaiting a replacement, the Redundant Array of Independent Disks (RAID) configuration is designed to ensure that there is no data loss due to a hardware failure.

The RAID configuration on NetWitness Suite:

- Hosts are RAID 1.
- Direct Attach Capacity (DAC) disk shelves is RAID 5.

Physical Security Controls Recommendations

This topic describes physical security controls.

Recommendations

Physical security controls help to enable the protection of resources against unauthorized physical access and physical tampering. RSA recommends that the physical devices and servers for RSA NetWitness Suite are deployed in a secure data center leveraging the organization's best practices for physically securing a data center, server rack, and/or server.

Supporting Users

This topic describes well-defined policies around help desk procedures for your RSA NetWitness Suite installation.

It is important to have well-defined policies around help desk procedures for your RSA NetWitness Suite installation. RSA recommends that your help desk administrators understand the importance of password strength and the sensitivity of data, such as user logon names and passwords. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and help desk administrators to request, the least amount of information needed in each situation.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. RSA recommends that you use the following guidelines to help reduce the likelihood of a successful social engineering attack:

- Help desk administrators should only ask for User IDs over the phone when receiving help desk calls. Help desk administrators should never ask for user passwords.
- The help desk telephone number should be well known to all users.
- Help desk administrators should perform an action to authenticate the user's identity before performing any administrative action on a user's behalf. For example, ask users one or more questions to which only they know the answer.
- If help desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call the help desk back at a well-known help desk telephone number to ensure that the original request is legitimate.

Confirming User Identities

It is critical that your help desk administrators verify end users' identities before performing any help desk operations on their behalf. RSA recommends that you verify user identity using the following methods:

- Call the end user back on a phone owned by the organization and on a number that is already stored in the system.

Caution: Be wary of using mobile phones for identity confirmation, even if they are owned by the company because mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

- Send the user an email to a company email address. If possible, use encrypted email.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.
- Use multiple open-ended questions from employee records. For example, "Name one person in your group" or "What is your badge number?" Avoid yes or no questions.

Advice for Your Users

RSA recommends that you instruct your users to do the following:

- Never give passwords to anyone.
- Change passwords at regular intervals.
- Inform your users of what information requests to expect from help desk administrators.
- Always log off from the web interface when finished.
- Always lock their desktops when stepping away from their computers.
- Regularly close their browser and clear their cache of data.

Note: Consider regular training to communicate this guidance to users.

RSA NETWITNESS® SUITE

Integration Guides for Other RSA Products

for Version 11.1

RSA NETWITNESS® SUITE

RSA Archer Integration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

RSA Archer Integration 4

Configure NetWitness to Work With Archer 5

Create RSA Archer User Accounts for Push and Pull 5

Integrate NetWitness Suite With Archer SecOps Manager 7

RSA Unified Collector Framework (UCF) 7

Configure Respond for Integration with Archer SecOps Manager 8

Configure Endpoints in RSA Unified Collector Framework 11

Configure Reporting Engine for Integration with NetWitness SecOps Manager 14

Configure Event Stream Analysis for Integration with Archer SecOps Manager 16

RSA Archer Feeds 19

Manage Unified Collector Framework 23

Troubleshoot RSA Archer Integration 24

Setting the CA Truststore 24

Remediation Tasks in RSA Archer Security Operations Manager 24

Errors between RSA NetWitness Suite and RSA Unified Collector Framework 24

RSA Archer Integration

Administrators can integrate RSA NetWitness Suite with RSA NetWitness Security Operations (SecOps) Manager to send alerts and incidents from NetWitness Suite to Archer for incident management and remediation. This guide provides a high-level workflow for configuring this integration.

Note: When you upgrade from Security Analytics 10.6.5 to NetWitness Suite 11.1, the Archer SecOps integration is no longer valid and must be re-configured.

The following table list the NetWitness Suite 11.1 integration options with NetWitness SecOps Managert Version 1.3.1.2.

NetWitness SecOps Manager Version	NetWitness Suite 11.1 Integration	Reference
1.3.1.2	Event Stream Analysis (ESA)	For more information, see "Configure Event Stream Analysis for Integration with Archer SecOps" section.
1.3.1.2	Reporting Engine (RE)	For more information, see "Configure Reporting Engine for Integration with Archer SecOps" section.
1.3.1.2	Respond	For more information, see "Configure Respond for Integration with Archer SecOps 1.3.1.2" section.
1.3.1.2	Archer Feeds	For more information, see "RSA Archer Feeds" section.

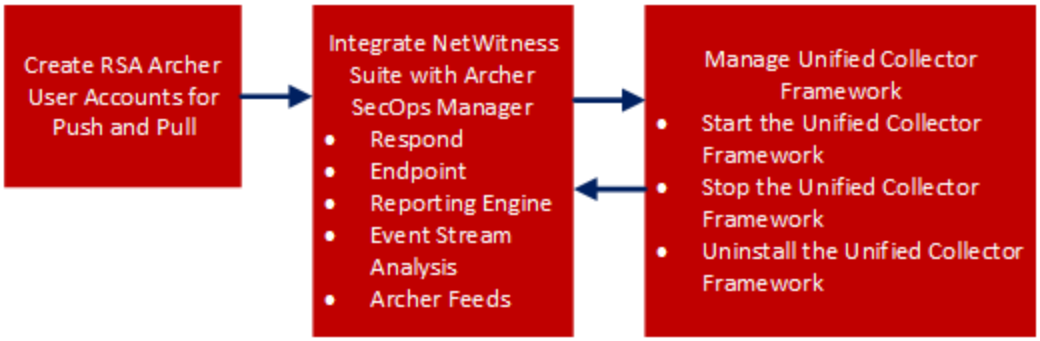
Configure NetWitness to Work With Archer

The RSA NetWitness SecOps Manager solution enables you to aggregate all actionable security alerts, allowing you to become more effective, proactive, and targeted in your incident response and SOC management. For more information on RSA NetWitness SecOps capabilities, see RSA Archer documentation on the RSA Archer Community or on the RSA Archer Exchange Community.

The version of RSA Archer determines how NetWitness Suite will be integrated. See the *SecOps Installation Guide* for Archer platforms supported.

NetWitness SecOps Manager 1.3.1.2 integrates with NetWitness Suite using the RSA UCF (Unified Collector Framework) which comprises of NetWitness Respond integration service and SecOps Watchdog service.

This figure represents the flow of NetWitness Suite 11.1 integration with NetWitnessSecOps Manager 1.3.1.2.



Create RSA Archer User Accounts for Push and Pull

You must create a user account for the web service client to transfer data to the RSA Archer GRC Platform.

You require two RSA Archer user accounts to avoid conflicts while sending and receiving data from RSA NetWitness Suite.

To create a user account for push and pull, perform the following:

1. On RSA Archer UI, click **Administration** > **Access Control** > **Users** > **Add New**.
2. In the **First Name** and **Last Name** fields, enter a name that indicates that the UCF uses this account to push data into RSA Archer GRC. For example, UCF User, Push.

   Note: When configuring the Pull account, enter a name that indicates that the UCF uses this account to pull data from RSA Archer GRC. For example, UCF User, Pull.
3. (Optional) Enter a user name for the new user account.

Note: If you do not specify a user name, the RSA Archer GRC Platform creates the user name from the first and last name entered when you save the new user account.

4. In the **Contact Information** section, in the **Email** field, enter an email address to associate with the new user account
5. In the **Localization** section, change the time zone to (UTC) Coordinated Universal Time.

Note: The UCF uses UTC time to baseline all the time-related calculations.

6. In the **Account Maintenance** section, enter and confirm a new password for the new user account.

Note: Make a note of the user name and password for the new user account that you just created. You need to enter these credentials when you set up the UCF to communicate with the RSA Archer GRC Platform through the web service client.

7. Clear the Force Password Change On **Next Sign-In** option.
8. In the **Security Parameter** field, select the security parameter that you want to use for this user.

Note: If you assign a default security parameter with a password change interval of 90 days, you also must update the user account password stored in the SA IM integration service every 90 days. To avoid this, you can optionally create a new security parameter for the SA IM integration service user account and set the password change interval to the maximum value allowed by your corporate standards.

9. Click the **Groups** tab, and perform the following:
   a. In the **Groups** section, click **Lookup**.
   b. In the **Available Groups** window, expand Groups.
   c. Scroll down and select SOC: Solution Administrator and EM: Read Only.
   d. Click **OK**.
10. Click **Apply**, then click **Save**.
11. If the machine language and regional settings of your RSA Archer GRC system are set to anything other than English-US, perform the following:
    a. Open the user account you just created, and in the **Localization** section, in the Locale field, select **English (United States)**, and click **Save**.
    b. On the Windows system hosting your RSA Archer GRC Platform, open Internet Information Services (IIS) Manager.

c. Expand your RSA Archer GRC site, click **.Net Globalization**, in both the **Culture** and **UI Culture** fields, select **English (United States)**, and click **Apply**.

d. Restart your RSA Archer GRC site.

12. Repeat steps 1 – 11 to create a second user account for the UCF to pull data from RSA Archer GRC.

Integrate NetWitness Suite With Archer SecOps Manager

You have to configure the system integration settings to manage incident workflow in RSA NetWitness SecOps Manager.

For information on how to configure system integration settings to manage incident workflow in RSA Archer Security Operations, see the "Manage Incidents in NetWitness SecOps Manager" topic in the *NetWitness Respond Configuration Guide*.

RSA Unified Collector Framework (UCF)

RSA NetWitness Suite integrates with RSA Archer SecOps Manager 1.3.1.2 using the RSA Unified Collector Framework (UCF). The RSA Unified Collector Framework (UCF) integrates with all supported SIEM tools and the RSA NetWitness SecOps Manager solution. After you configure the system integration settings, all incidents are managed in NetWitness SecOps Manager instead of NetWitness Respond. Incidents created before the integration will not be managed in NetWitness SecOps Manager.

Note:
• You must configure the same option in both RSA NetWitness Suite and the Unified Collector Framework.
• Integration of the RSA NetWitness Respond module with Reporting Engine or Event Stream Analysis can result in duplicate events, alerts, and incidents created in RSA Archer SecOps Manager.

UCF supports multiple SIEM tools connections at the same time, such as supporting NetWitness Suite Reporting Engine, HP ArcSight, and NetWitness Respond. However, different instances of the same SIEM tool are not supported, such as two NetWitness Suite servers connected to the same UCF.

Prerequisites

- Install the RSA_Archer_Security_Operations_Management package on Archer. See RSA Archer documentation RSA Archer Community or on the Content Tab at https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Install NetWitness SecOps Manager 1.3.1.2.

- Ensure you have NetWitness Suite 11.1 as it is compatible with NetWitness SecOps Manager 1.3.1.2.
- Ensure that Respond is configured in RSA NetWitness Suite.

The RSA Unified Collector Framework (UCF) allows you to integrate your RSA Archer Security Operations Manager system with the following:

- NetWitness Respond
- NetWitness Suite Reporting Engine
- NetWitness Suite Event Stream Analysis
- Archer Feeds

Configure Respond for Integration with Archer SecOps Manager

To configure Respond for Archer SecOps, perform the following in NetWitness Suite:

Step 1: Select the Mode for NetWitness Respond

1. Go to **ADMIN** > Services, select the Respond Server service, and then select > **Config** > **Explore**.
2. Navigate to `respond/integration/export`.
3. Set the `archer-sec-ops-integration-enabled` field to **true**.
4. Restart the Respond service by running the following command:
   `systemctl restart rsa-nw-respond-server`

Step 2: Configure NetWitness Respond to forward alerts to UCF

1. Navigate to `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` in the SecOps middleware box.
2. Copy both `keystore.crt.pem` and `rootcastore.crt.pem` from the certs folder (to the import folder of NW-server):
   `cp rootcastore.crt.pem /etc/pki/nw/trust/import`

   `cp keystore.crt.pem /etc/pki/nw/trust/import`

   Note: Before you copy the files from UCF to NetWitness Admin server, examine the files to remove any blank lines and save them.
3. SSH to NW-server box
   a. Run the update-admin-node command
   `orchestration-cli-client --update-admin-node`

b. Restart the RabbitMQ service

```
systemctl restart rabbitmq-server
```

c. Create user archer and set permissions for the virtual host '/rsa/system'

```
rabbitmqctl add_user archer archer

rabbitmqctl clear_password archer

rabbitmqctl set_permissions -p /rsa/system archer ".*" ".*" ".*"
```

Step 3: Forward Alerts to the NetWitness Respond

- **To forward NetWitness Suite Event Stream Analysis alerts to NetWitness Respond, perform the following:**
  a. Go to **ADMIN > Services > ESA** service.
  b. Select an Event Stream Analysis service and then select > **View** > **Config**.
  c. Click the **Advanced** tab.
  d. Ensure that the **Forward Alerts on Message Bus** checkbox is selected by default. If not, select the **Forward Alerts on Message Bus** checkbox and click **Apply**.
- **To forward NetWitness Suite Reporting Engine alerts to NetWitness Respond, perform the following:**
  a. Go to **ADMIN > Services > Reporting Engine** service.
  b. Select the Reporting Engine service, and then select > **View** > **Config**.
  c. Click the **General** tab.
  d. In the **System Configuration section**, select the **Forward Alerts to Respond** checkbox and click **Apply**.
- **To forward NetWitness Suite Malware Analysis alerts to NetWitness Respond, perform the following:**
  a. Go to **ADMIN > Services > Malware Analysis** service
  b. Select the Malware Analysis service, and then select > **View** > **Config**.
  c. Click the **Auditing** tab.
  d. In the **Respond Alerting** section, verify that the **Enabled Config Value** checkbox is selected. If the checkbox is not selected, select the checkbox, and click **Apply**.

Step 4: Forward Endpoint Alerts to the NetWitness Respond

RSA Endpoint alerts can be sent to RSA Archer GRC through NetWitness Respond. For more information on how to Configure NetWitness Endpoint Alerts via Message Bus, see "Configure NetWitness Endpoint Alerts via Message Bus" topic in the *NetWitness Endpoint Integration Guide*.

Step 5: Aggregate Alerts into Incidents

The Respond Server service consumes alerts from the message bus and normalizes the data to a common format (while retaining the original data) to enable simpler rule processing. It periodically runs rules to aggregate multiple alerts into an incident and set some attributes of the Incident (for example, severity, category, and so on). For more information on aggregating alerts, see the "Configure Alert Sources to Display Alerts in Respond View" topic in the *NetWitness Respond Configuration Guide*.

To configure alert aggregation:

1. Go to **CONFIGURE > Incident Rules**.
2. To enable the rules provided out of the box, perform the following:
   a. Double-click the rule.
   b. Select **Enabled**.
   c. Click **Save**.
   d. Repeat steps a-c for each rule.
3. To add a new rule, do the following:
   a. Click +.
   b. Select **Enabled**.
   c. Complete the following fields:
      - Rule Name
      - Action
      - Match Conditions
      - Grouping Options
      - Incident Options
      - Priority
      - Notifications
4. Click **Save**.

Configure Endpoints in RSA Unified Collector Framework

Endpoints provide the connection details required for the UCF to reach both your RSA NetWitness Suite and RSA Archer GRC systems.

Note: Some endpoints are necessary to use different integrations. The following list shows the mandatory endpoints.

Mandatory Endpoint Integration

- Archer Push endpoint
- Archer Pull endpoint
- Mode selection: SecOps or Non SecOps mode.

Note:
• If Non SecOps mode is selected, incidents are managed in NetWitness Respond instead of RSA Archer Security Operations Management.
• You must configure the port depending on the protocol (TCP, UDP, or secure TCP).
• Ensure the certificate subject name for your RSA Archer GRC server matches the hostname.

Procedure

1. On the UCF system, open the Connection Manager, as follows:
   a. Open a command prompt.
   b. Change directories to `<install_dir>\SA IM integration service\data-collector`.
   c. Enter:
   ```
   runConnectionManager.bat
   ```
2. In the **Connection Manager**, enter **1** for Add Endpoint.
3. Add an endpoint for pushing data to RSA Archer Security Operations Management, as follows:
   a. Enter the number for Archer.

      Note: SSL must be enabled to add the RSA Archer endpoints.

   b. For the endpoint name, enter **push**.
   c. Enter the URL of your RSA Archer GRC system.
   d. Enter the instance name of your RSA Archer GRC system.

e. Enter the user name of the user account you created to push data into your RSA Archer GRC system.

f. Enter the password for the user account you created to push data into your RSA Archer GRC system, and confirm the password.

g. When asked whether this account is used for pulling data, enter **False**.

4. Add an endpoint for pulling data from RSA Archer Security Operations Management, as follows:

a. Enter the number for Archer.

> **Note:** SSL must be enabled to add the RSA Archer endpoints.

b. For the endpoint name, enter **pull**.

c. Enter the URL of your RSA Archer GRC system.

d. Enter the instance name of your RSA Archer GRC system.

e. Enter the user name of the user account you created to pull data from your RSA Archer GRC system.

f. Enter the password for the user account you created to pull data from your RSA Archer system, and confirm the password.

g. When asked whether this account is used for pulling data, enter **True**.

5. Add an endpoint for RSA NetWitness Suite

- For RESPOND

a. Enter the number for Security Analytics IM.

b. Enter a name for the endpoint.

c. Enter the SA Host IP address.

d. For SA Messaging Port, enter **5671**.

e. Enter the target queue for remediation tasks. Selecting All processes both the RSA Archer Integration (GRC) and IT Helpdesk (Operations).

f. When asked whether to automatically add certificates to the SA trust store, enter **No**. The certificates were added manually in previous steps.

g. In UCF connection manager, select the mode, as follows:

i. Enter the number for Mode Selection.

ii. Select Manage incident workflow exclusively in RSA Archer Security Operations Management from the drop-down.

Note: Make sure you select the second option as the first option is not supported in NetWitness Suite 11.1 release.

- For Reporting Engine and Event Stream Analysis

a. To use third-party integrations, add the Syslog Server Endpoint, as follows:

i. Enter the number for Syslog Server Endpoint.

ii. Enter the following:

- User defined name
- SSL Configured TCP port number

  Note: Defaults to 1515. If you do not want to host the Syslog server in this mode, enter **0**.

- TCP port number - Enter the TCP port if the Syslog client sends the Syslog message in TCP mode.

  Note: Defaults to 1514. If you do not want to host the Syslog server in this mode, enter **0**.

- UDP port number - Enter the UDP port if the Syslog client sends the Syslog message in UDP mode.

  Note: Defaults to 514. If you do not want to host the Syslog server in this mode, enter **0**.

By default, the Syslog server will run in the above three modes, unless it is disabled by entering **0**.

b. To test the Syslog client, enter the number for Test Syslog Client. Use the Test Syslog client with the files from `<install_dir>\SA IM integration service\config\mapping\test-files\`.

6. In the Connection Manager, enter **5** to test each endpoint.

Configure Reporting Engine for Integration with NetWitness SecOps Manager

To configure Syslog Output Action for the Reporting Engine, perform the following:

1. Select **ADMIN > Services**.
2. Select your Reporting Engine Service, and click **View** > **Config**.
3. Click the **Output Actions** tab.
4. In the **NetWitness Suite Configuration** section, in the **Host Name** field, enter the host name or IP address of your Reporting Engine server.
5. In the **Syslog Configuration** section, add the Syslog Configuration as follows:
   a. In the **Server Name** field, enter the hostname of the UCF.
   b. In the **Server Port** field, enter the port that you selected in the UCF Syslog configuration.
   c. In the **Protocol** field, select the transport protocol.

   Note: If you select Secure TCP, SSL must be configured.
6. Click **Save**.

To Configure NetWitness Suite Reporting Engine SSL for Secure Syslog Server:

If the Syslog server is configured with Secure TCP, configure the SSL.

1. Copy the certificate `keystore.crt.der` from the UCF machine to NetWitness Suite server box at `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4.x86_64/jre/lib/security`.
2. Run the following command:

   ```
   keytool -import -file keystore.crt.der -alias ucf-syslog -keystore /etc/pki/nw/trust/truststore.jks -storepass changeit
   ```

   Note: Do not copy and paste the above code. Type it in to avoid errors.
3. Enable **ServerCertificateValidationEnabled** to **true:**
   - Navigate to **ADMIN** > **Service**.
   - Click > **View > Explore** of the Reporting Engine service .

- Expand **com.rsa.soc.re** > **Configuration** > **SSLContextConfiguration**.
- Expand **sslContextConfiguration** and set **ServerCertificateValidationEnabled** to **true**.

4. Restart the Reporting Engine service by running the following command:
   `service rsasoc_re restart`

To Configure Rules in NetWitness Suite:

1. Click **MONITOR >Reports > Manage**.
   The Manage tab is displayed.
2. In **Rule Groups** panel, click ✚.
3. Enter a name for the new group.
4. Select the group you created, and in the Rule toolbar, click ✚.
5. In the **Rule Type** field, select NetWitness DB.
6. Enter a name for the rule.
7. Enter values in the **Select** and **Where** fields based on the rule that you want to create.

   Note: Add the Syslog configuration with the Syslog name set above.

8. Click **Save**.

Note: To see the same number of alerts in the Reporting Engine and RSA Archer GRC, ensure that you've selected Once for execute in both the Syslog and Record tabs.

To Add Alert Templates for the Reporting Engine in NetWitness Suite:

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates`

1. Click **MONITOR > Reports > Manage > Alerts**.
2. Click the **Template** tab.
3. Click ✚.

Note: After you copy the template in the Create/Modify Template window, make sure to replace `cs25=${sa.host} cs25Label=sahost` to `cs25=${nw.host} cs25Label=nwhost`.

1. In the **Name** field, enter a name for the alert template.
2. In the **Message** field, enter the alert message.
3. Click **Create**.
4. Repeat steps 3 to 6 for each alert template that you want to add.

To Configure Alerts in NetWitness Suite:

In RSA NetWitness Suite Reporting Engine, an alert is a rule that you can schedule to run on a continuous basis and log its findings to several different alerting outputs.

1. Click **MONITOR > Reports > Manage > Alerts**.
2. Click +.
3. Select **Enable**.
4. Select the rule you created.
5. Select **Push to Decoders**.

   Note: If you do not enter a value in this field, the link in the RSA Archer Security Alerts application to RSA NetWitness Suite will not work.
6. From the Data Sources list, select your data source.
7. In the **Notification** section, select **Syslog**.
8. Click +.
9. Complete the Syslog configuration fields.
10. In the **Body Template** field, select the template that you want to use for this Syslog alert.
11. Click **Save**.

Configure Event Stream Analysis for Integration with Archer SecOps Manager

To Configure Event Stream Analysis Syslog Notification Settings in NetWitness Suite:

1. Click **ADMIN** > **System** > **Global Notifications**.
2. Click the **Output** tab.
3. Define and enable an Event Stream Analysis Syslog notification.
4. Click the **Servers** tab.
5. Define and enable a Syslog notification server.

6. In the Syslog Server Configuration section, enter the following:

   Field Description:

   - Name - Specify the custom name
   - Server IP (Hostname) - Specify the hostname or IP Address of the system on which you installed the UCF.
   - Port - Specify the port number on which you want the UCF to listen for.
   - Facility - Specify the Syslog facility
   - Protocol - Select the protocol.

7. Click **Save**.

To Configure NetWitness Suite Event Stream Analysis SSL for Secure Syslog Server:

If the Syslog server is configured with Secure TCP, configure the SSL.

1. Select **ADMIN > Services**.
2. Select the Event Stream Analysis service. Go to **Explore > Configuration > SSL** .
3. Set **ServerCertificateValidationEnabled** to **true.**
4. Copy the `rootcastore.cert.pem` from UCF machine to Event Stream Analysis server to `/etc/pki/ca-trust/source/anchors`.
5. Run the following command:

   ```
   update-ca-trust
   ```

6. Restart the Event Stream Analysis server by running the following command:

   ```
   service rsa-nw-esa-server restart
   ```

To Add Event Stream Analysis Alert Templates

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_`

`Templates\SecOps_SA_ESA_templates.txt`

1. Select **ADMIN > System > Global Notifications**.
2. Click the **Templates** tab.
3. Click ✚.
4. In the **Template Type** field, select Event Stream Analysis.

5. In the **Name** field, enter the name for the template.
6. (Optional) In the **Description** field, enter a brief description for the template.
7. In the **Template** field, enter the alert message.
8. Click **Save**.
9. Repeat steps 3 – 8 for each alert template that you want to add.

To Create Event Stream Analysis Rules

1. Click **CONFIGURE** > **ESA Rules**.
2. In the **Rule Library**, click ✚.
3. Select **Rule Builder**.
4. In the **Rule Name** field, enter a name for the rule.
5. In the **Description** field, enter a description for the rule.
6. Select the **Severity**.
7. In the **Condition** section, do the following:
   a. Click ✚ to build a statement.
   b. Enter a name, select a condition type, and add meta data/value pairs for your statement.
   c. Click **Save**.
   d. Repeat steps a – c until you have built all your statements for the rule.
8. In the **Notifications** section, select **Syslog**.
9. Select the notification, Syslog server, and template that were created previously.
10. Click **Save** and **Close**.
11. Click **Configure** > **Deployments**.
12. Click ✚ for Event Stream Analysis services section.
13. Select the Event Stream Analysis Service.
14. Click **Deploy Now**.
15. In the **Event Stream Analysis Rules** section, click ✚ to choose the Event Stream Analysis Rule that you created, and click **Deploy Now**.

RSA Archer Feeds

By default, only the IP Address and Criticality Rating fields in the RSA Archer Devices application are fed into RSA NetWitness Suite by the SA IM Integration Service. You can customize the Enterprise Management plug-in to include the Business Unit and Facility fields that are cross-referenced in the Devices application in the feed. For more details, see Archer documentation at https://community.emc.com/community/connect/grc_ecosystem/rsa archer or https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.

Note: If you plan to feed Business Unit and Facility information from your RSA Archer GRC Platform into Live, you must also add keys for these fields to the index-concentrator-custom.xml file.

Update the Concentrator and Decoder Services

The SA IM Integration Service in NetWitness SecOps Manager manages the files for a custom feed and deposits these files in a local folder that you specify when you configure the Enterprise Management Endpoint. The Live module of RSA NetWitness Suite retrieves the feed files from this folder. Live then pushes the feed to the Decoders, which start creating metadata based on captured network traffic and the feed definition. To make each Concentrator aware of the new metadata created by the Decoders, you must edit the `index-concentrator-custom.xml`, `index-logdecoder-custom.xml`, and `index-decoder-custom.xml files`.

1. Select **ADMIN > Services**.
2. Select your Concentrator, and select > **View > Config**.
3. Click the **Files** tab.
4. From the drop-down list, select index-concentrator-custom.xml. Do one of the following:
   - If content already exists in the file, add a key for the new meta data element as follows:

     ```
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     ```

     Note: Do not copy and paste code. Type it in to avoid errors.
   - If the file is blank, add the following content:

     ```
     <?xml version="1.0" encoding="utf-8"?>
     <language level="IndexNone" defaultAction="Auto">
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     </language>
     ```
5. Click **Apply**.
6. To add multiple devices, do the following:

a. Click **Push**.

b. Select the devices to which you want to push this file.

c. Click **OK**.

7. Repeat steps 1-7 for the Log Decoders and Index Decoders, using index-logdecoder-custom.xml and index-decoder-custom.xml.

8. Restart the Concentrator and Decoder services by running the following commands:

```
service nwdecoder restart
service nwconcentrator restart
```

Add the RSA Archer Enterprise Management Endpoint in the UCF

1. In the UCF connection manager, select the mode, as follows:

   a. Enter the number for Mode Selection.

   b. Select one of the following options:

   - Manage incident workflow in RSA NetWitness Suite.
   - Manage incident workflow exclusively in RSA Archer Security Operations Management.

2. Add the RSA Archer Enterprise Management Endpoint, as follows:

   a. Enter the number for Enterprise Management.

   b. Complete the fields in the table below.

Field	Description
Endpoint Name	Optional endpoint name.
Web Server Port	Defaults to 9090. Can be configured to host the web server url. The URL with the port number should be provided as the URL in NetWitness Suite live feed: http://hostname:port/archer/sa/feed

Field	Description
Criticality	Criticality of the assets to be pulled from RSA Archer GRC. If **false**, pull assets with any criticality. If **true**, pull assets with only high criticality. To configure this manually, edit the em.criticality property in the collector-config properties file to provide a comma-separated list of criticalities: LOW, MEDIUM, HIGH.
Feed Directory	Directory where the assets CSV file from RSA Archer GRC are saved. **Note:** The directory path provided must exist.
Web Server Username	Username for authenticating to the EM web server.
Web Server Password	Password for authenticating to the EM web server.
SSL Mode	Defaults to No. If **No**, the URL uses `http mode: http://hostname:port/archer/sa/feed` If you have not updated the host file, see "Update the RSA NetWitness Suite Host File" section. **Note:** NetWitness Suite currently does not support Archer recurring feeds in SSL mode.

Update the RSA NetWitness Suite Host File

1. Edit the host file on the NetWitness Suite server at the following location: vi /etc/hosts
2. Enter the following for the UCF host IP address:

   ```
   <ucf-host-ip> <ucf-host-name>
   ```

3. Restart NetWitness Suite server by running the following command:

   ```
   service jetty restart
   ```

4. While configuring the NetWitness Suite live feed, enter the hostname for the URL instead of the IP address and the port number configured for Enterprise Management endpoint in the

UCF:

`http: //<ucf-host-name> : <EM_Port>/archer/sa/feed.`

5. Verify that the connection works.

Create a Recurring Feed Task

In order for RSA NetWitness Suite to download feed files from the NetWitness Respond Integration Service and push the feeds to Decoders, you must create a recurring feed task and define the feed settings.

Note: For RSA Archer SecOps 1.2: In order for RSA NetWitness Suite to download feed files from your UCF machine and push the feeds to Decoders, you must create a recurring feed task and define the feed settings. The procedure is similar to RSA Archer SecOps 1.3, with a few exceptions. See documentation on the RSA Archer Exchange Community for details.

1. Select **CONFIGURE > Custom Feeds**.
2. In the Feeds view, Click +.
3. Select **Custom Feed**, and click **Next**.
4. Select **Recurring**.
5. Enter a name for the feed.
6. In the URL field, enter the following:

   `http://ucf_hostname/archer/sa/feed`

   where *`http :ucf_hostname_or_ip:port`* is the address of your NetWitness Respond Integration Service system. For example: `http://<ucf-host-name>` .
7. Select **Authenticated**.
8. In the **User Name** and **Password** fields, enter the credentials of the user account you created in the Add the RSA Archer Enterprise Management Endpoint in the UCF procedure.
9. Define the recurrence interval for the feed.
10. In the **Date Range** section, define a start and end date for the feed, and click **Next.**
11. Select each Decoder to which you want to push this feed, and click **Next**.
12. In the **Type** field, ensure that IP is selected.
13. In the **Index Column** field, select 1.
14. In the second column, set the Key value to criticality, and click **Next**.
15. Review your feed configuration details, and click **Finish**.

Manage Unified Collector Framework

This section provides additional tasks for configuring and managing the RSA Unified Collector Framework (UCF) for Archer SecOps Manager 1.3.1.2 Integration.

Start the RSA Unified Collector Framework

1. Click **Control Panel > Administrative Tools > Services**.
2. Select RSA Unified Collector Framework.
3. Click **Start**.

Stop the RSA Unified Collector Framework

1. Click **Control Panel > Administrative Tools > Services**.
2. Stop the RSA SecOps WatchDog Service.

   Note: If you do not stop the Watchdog service, the Watchdog service starts the NetWitness Respond Service before intended.

3. Select RSA Unified Collector Framework.
4. Click **Stop**.

Note: If the service takes too long to shutdown, use the Task Manager to end the RSASAIMDCService.

Uninstall the RSA Unified Collector Framework

1. Click **Control Panel** > **Programs and Features**.
2. Select **RSA Unified Collector Framework**.
3. Click **Uninstall**.

Troubleshoot RSA Archer Integration

This section provides resolutions to common problems that you may encounter while configuring Archer SecOps Manager 1.3.1.2 with NetWitness Respond.

Setting the CA Truststore

Problem: After adding the endpoint for NetWitness Respond, the CA truststore fails to set.

Resolution:

1. Ensure that the SSH credentials for the NetWitness Suite host are valid.
2. If the credentials are correct, but the error still occurs, manually copy certificates.

Remediation Tasks in RSA Archer Security Operations Manager

Problem: Remediation Tasks being pushed to the operations queue through the UCF are not appearing in RSA Archer Security Operations Manager as Findings.

Resolution:

1. Open the Connection Manager:
    - Open a command prompt
    - `Change directories to <install_dir>\SA IM integration service\data-collector.`
    - `Type: runConnectionManager.bat`
2. Enter 2 to edit endpoint.
3. Enter 3 to NetWitness Suite Respond.
4. Ensure the Target Queue is set to All or Operations.

Errors between RSA NetWitness Suite and RSA Unified Collector Framework

Problem: In the `<install_dir>\SA IM integration service\logs\collector.log`, there are SSL errors between RSA NetWitness Suite and RSA Unified Collector Framework.

Resolution:

1. Verify that the SSL certificates are valid.

   Note: NetWitness Respond certificates are valid for two years.

2. If your certificates are expired, regenerate and copy the expired certificates.

To regenerate and copy the certificates, do the following:

1. In Command Prompt, go to `<install_dir>\SA IM integration service\data-collector`.
2. Enter: `runConnectionManager.bat`
3. Enter the number for Regenerate SA IM Integration Service Certificate.
4. In the NetWitness Suite Respond endpoint, in Connection Manager, enter the number for Edit Endpoint.
5. Enter Yes to copy the certificates automatically to the NetWitness Suite trust store.

Note: If certificates fail to copy, manually copy the certificates.

RSA NETWITNESS® SUITE

RSA NetWitness Endpoint Integration Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

RSA NetWitness Endpoint Integration 4

Integration Options 4

Built-in NetWitness Endpoint Lookup 4

Integration Methods 5

NetWitness Endpoint Meta Integration 6

NetWitness Endpoint Alerts and Indicators of Compromise 6

Configure NetWitness Endpoint Alerts via Message Bus 7

Configure NetWitness Endpoint to Forward NetWitness Endpoint Alerts 8

Configure Contextual Data from NetWitness Endpoint via Recurring Feed 11

Enable the NetWitness Endpoint Feed for NetWitness Suite 12

Export the NetWitness Endpoint SSL Certificate 15

Configure the NetWitness Suite Concentrator Service 16

Configure the Recurring Custom Feed Task in NetWitness Suite 17

Configure Endpoint Alerts via Syslog into a Log Decoder 22

Configure NetWitness Endpoint to Send Syslog Output to NetWitness Suite 23

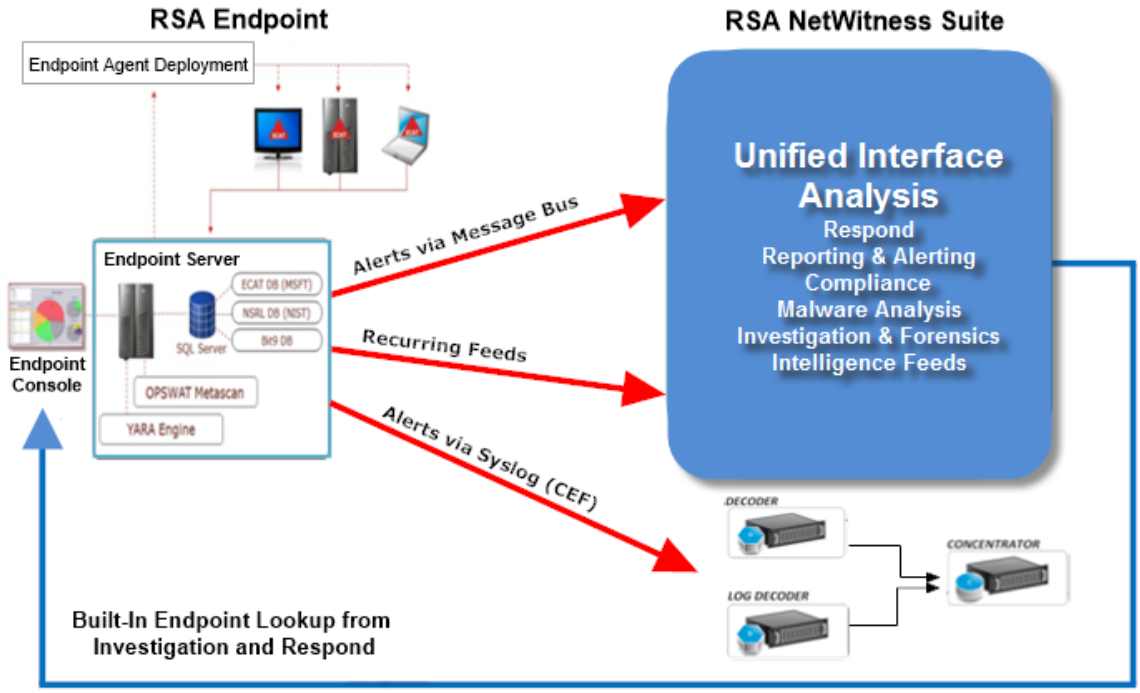
Edit the Table Mapping in table-map-custom.xml 24

Configure the NetWitness Suite Concentrator Service 27

RSA NetWitness Endpoint Integration

RSA customers who are using RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 can integrate NetWitness Endpoint and RSA NetWitness Suite in several different ways. This guide is for RSA NetWitness Suite version 11.1.

Integration Options



Built-in NetWitness Endpoint Lookup

With the RSA NetWitness Endpoint user interface (UI) installed on the same machine where the analyst is using a browser to access NetWitness Suite, the built-in NetWitness Endpoint Lookup from NetWitness Suite Investigation and NetWitness Suite Respond provides right-click access to the NetWitness Endpoint console server for the following meta keys: IP address (ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip), host (alias-host, domain.dst), client, and file-hash. These are described in the "Launch an External Lookup of a Meta Key" topic in *Investigation and Malware Analysis User Guide* and the "View Alerts" topic in *NetWitness Respond User Guide*.

NetWitness Suite configuration is not required for endpoint lookup when you are using one of the built-in parsers, NetWitness Endpoint or CEF, and you have not customized the default meta keys used when loading metadata in Investigation. For more information, see "Manage and Apply Default Meta Keys in an Investigation" topic in the *Investigation and Malware Analysis User Guide*.

Note: The exception occurs if you customize NetWitness Suite by editing the display setting for the default meta keys in Investigation, add meta keys to the table-map-custom.xml file, or customize NetWitness Endpoint feeds. Some configuration is required to add the custom meta keys to the context menu NetWitness Endpoint Lookup in the **ADMIN** > **System** view as described in the "Add Custom Context Menu Actions" topic in the *System Configuration Guide*.

Integration Methods

With an RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 console server installed on a Windows host and proper configuration of NetWitness Endpoint and NetWitness Suite by an administrator, three additional integrations of NetWitness Endpoint analysis data are possible.

The following are the RSA NetWitness Endpoint integration methods:

- Configure Endpoint Alerts via Message Bus
- Configure Contextual Data from Endpoint via Recurring Feed
- Configure Endpoint Alerts via Syslog into a Log Decoder

Endpoint alerts via message bus into NetWitness Respond. This integration provides the capability for forwarding Endpoint alerts to Respond via message bus.

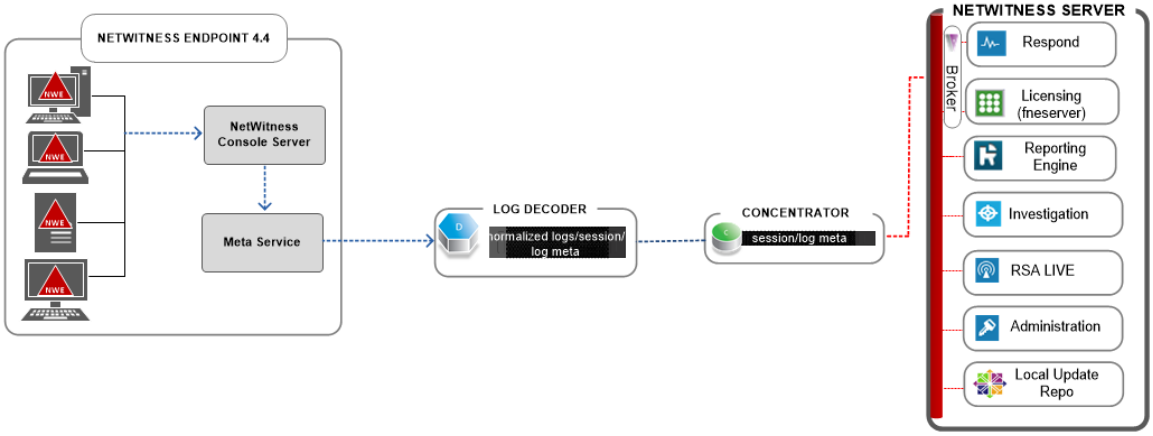
Contextual data from Endpoint via a NetWitness Suite Live recurring feed. This integration can enrich the session displayed in NetWitness Suite Investigation with contextual information; some examples include the host operating system, MAC address, IIOC score, and other data that may not be present in the log or packet data.

NetWitness Endpoint alerts via Syslog (CEF) into NetWitness Suite Log Decoders. This integration provides the capability to forward Endpoint events via Syslog and to correlate the events with other log or packet metadata in the NetWitness Suite ecosystem.

NetWitness Endpoint Meta Integration

The NetWitness Endpoint Meta Integration with RSA NetWitness Suite offers customers that have both products a way to more easily take advantage of their products in a single user interface. The following diagram illustrates how NetWitness Endpoint integrates with the NetWitness Suite. The NetWitness Endpoint metadata is collected and published from all machines where NetWitness Endpoint agents are deployed, and then sent to the NetWitness Suite Log Decoder.

The meta can then be viewed in the associated NetWitness Suite Concentrator and also in NetWitness Suite Investigate.



NetWitness Endpoint Alerts and Indicators of Compromise

NetWitness Endpoint IIOC (Instant Indicator of Compromise) is a database query that NetWitness Endpoint runs on collected NetWitness Endpoint scan data to determine the presence of potential malware on scanned hosts. RSA NetWitness Endpoint 4.1.2 or later ships with IOCs that users can enable and mark as alertable. RSA NetWitness Endpoint runs IOC queries regularly on new scan data, which is collected and stored in the database. If the IOC query is satisfied, this indicates a potential indicator of compromise, and the event can be reported to a user or sent to an external system as an alert.

Possible types of alerts are:

- Machine alert: This alert indicates that the machine in question is suspicious.
- Module alert: This alert indicates that a module, such as a file, a DLL, or an executable, is suspicious. It contains details about the module in question.
- Event alert: This alert represents any other suspicious activity detected by NetWitness Endpoint that does not fall into the above categories.

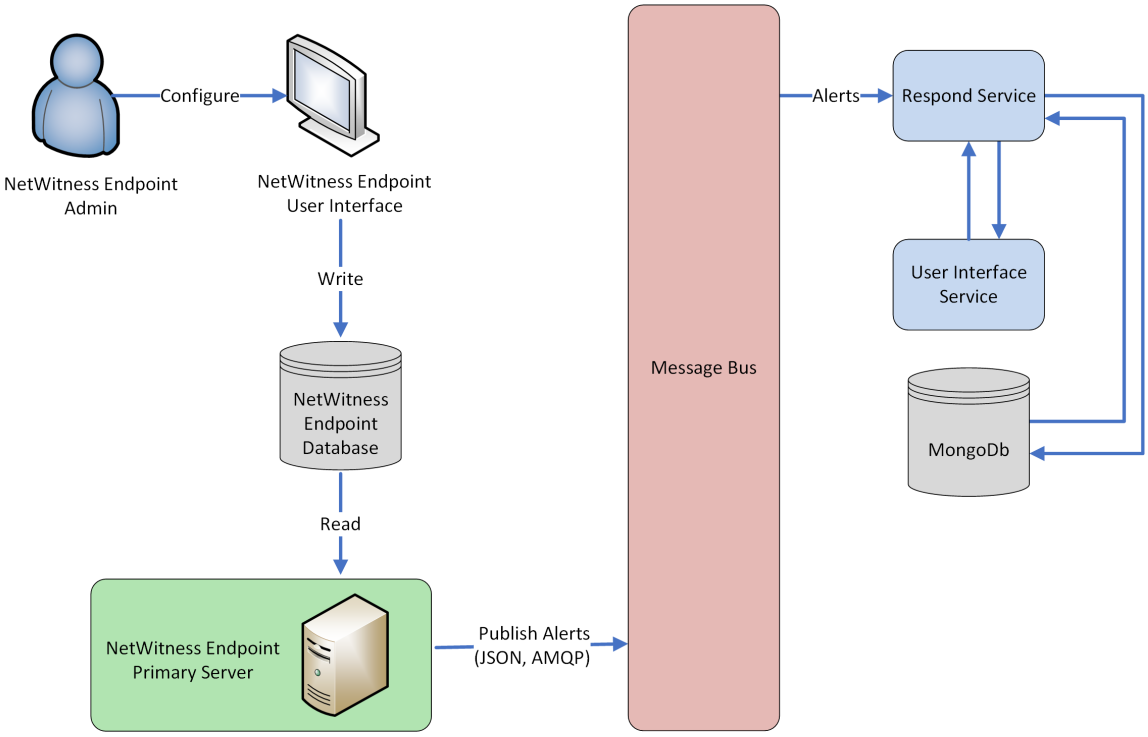
Each of these alert types can be sent to NetWitness Suite.

Configure NetWitness Endpoint Alerts via Message Bus

This procedure is required to integrate NetWitness Endpoint with NetWitness Suite so that the NetWitness Endpoint alerts are picked up by the Respond component of NetWitness Suite and displayed in the **RESPOND > Alerts** view.

Note: RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, or 4.4 for NetWitness Respond integration. For more information, see the "RSA NetWitness Suite Integration" topic in the *NetWitness Endpoint User Guide*.

The diagram below represents the flow of NetWitness Endpoint alerts to the Respond Incident List view of NetWitness Suite and its display in the **RESPOND > Alerts** view.



Prerequisites

Ensure that you have the following:

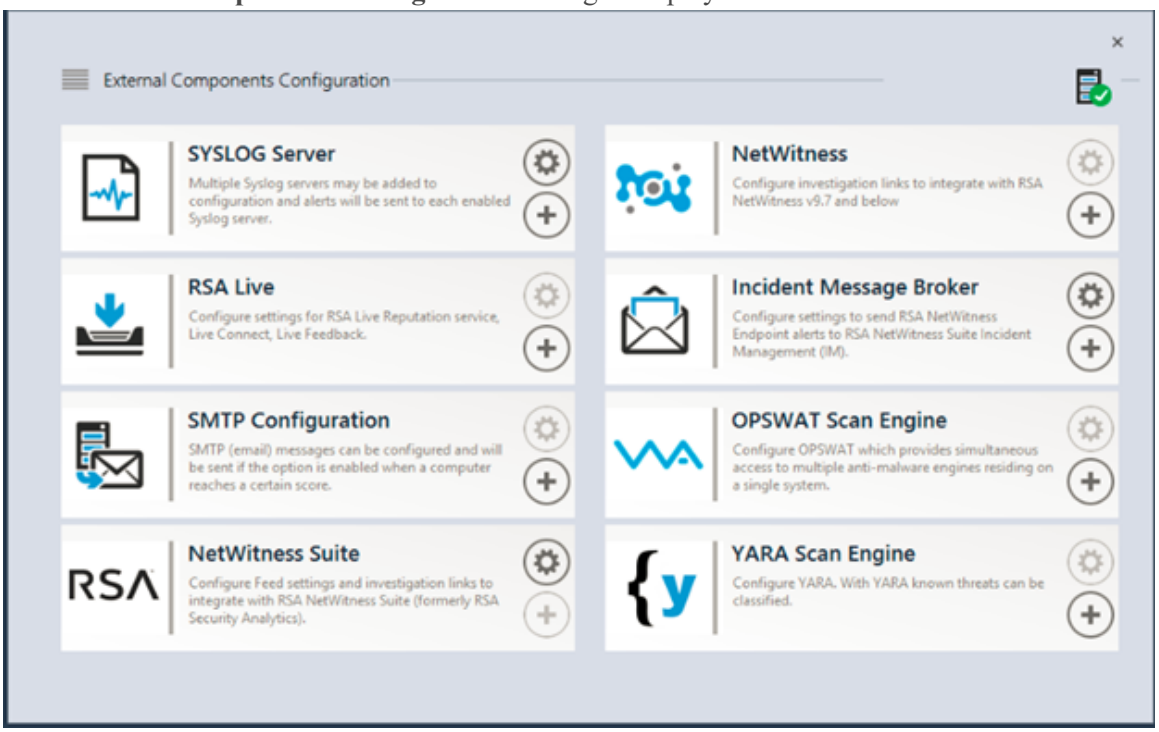
- The Respond service is installed and running on NetWitness Suite.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 is installed and running.

Configure NetWitness Endpoint to Forward NetWitness Endpoint Alerts

To configure NetWitness Endpoint to send alerts over the message bus to the NetWitness Suite user interface:

1. In the NetWitness Endpoint user interface, click **Configure > Monitoring and External Components**.

   The **External Components Configuration** dialog is displayed.



   1. From the components listed, select **Incident Message Broker** and click + to add a new IM broker.

2. Enter the following fields:

   a. **Instance Name**: Enter a unique name to identify the IM broker.

   b. **Server Hostname/IP address**: Enter the Host DNS or IP address of the IM broker (NetWitness Server).

   c. **Port number**: The default port is 5671.

3. Click **Save**.

4. Navigate to the **ConsoleServer.exe.config** file in **C:\Program Files\RSA\ECAT\Server**.

5. Modify the virtual host configurations in the file as follows:
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite11.0 and 11.1, the virtual host is "/rsa/system". For version 10.6.x and below, the virtual host is "/rsa/sa".

6. Restart the API Server and Console Server.

7. To set up SSL for Respond Alerts, perform the following steps on the NetWitness Endpoint primary console server to set the SSL communications:

   a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key).

   b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You MUST set the CN name to ecat. Run cmd.exe console with Administrator rights.)

   ```
   makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
   sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir
   LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
   cy end -sy 12 c:\client.cer
   ```

   Note: In the previous code sample, if you upgraded to version 4.3 (or later) from a previous version and did not generate new certificates, you should substitute `"EcatCA"` for `"NweCA"`.

   Or, if your current operating system has PowerShell version 5.1 or later, you can use the following code sample:

   ```
   PS C:\> New-SelfSignedCertificate -KeyExportPolicy Exportable -
   Subject "CN=ecat" -KeyAlgorithm RSA -KeyLength 2048 -
   CertStoreLocation "cert:\LocalMachine\My" -HashAlgorithm SHA256 -
   KeySpec KeyExchange -TextExtension @("2.5.29.37=
   {text}1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1") -Provider "Microsoft
   RSA SChannel Cryptographic Provider" -KeyUsage DigitalSignature,
   KeyEncipherment, KeyAgreement -Signer (Get-ChildItem -Path
   Cert:\LocalMachine\My\ -DnsName NweCA)-NotAfter (Get-
   Date).AddYears(5); Export-Certificate –Cert (Get-ChildItem –Path
   Cert:\LocalMachine\My\ -DnsName ecat) –FilePath C:\Client.cer
   ```

   c. Make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the IMBrokerClientCertificateThumbprint section of the ConsoleServer.Exe.Config file as shown.

   ```
   <add key="IMBrokerClientCertificateThumbprint"
   value="896df0efacf0c976d955d5300ba0073383c83abc"/>
   ```

8. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:
   `/etc/pki/nw/trust/import`

9. Issue the following command to initiate the necessary Chef run:
   `orchestration-cli-client --update-admin-node`
   This appends all of those certificates into the truststore.
10. Restart the RabbitMQ server:
    `systemctl restart rabbitmq-server`
    The NetWitness Endpoint account should automatically be available on RabbitMQ.
11. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NetWitness Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Troubleshooting

This section suggests how to resolve problems you may encounter when you configure NetWitness Endpoint alerts via Message Bus.

Known Issues	Solutions
Orchestration fails on admin node.	You must copy and paste the content of EcatCA certificate in `/etc/rabbitmq/ssl/truststore.pem` and restart the Rabbitmq service.

Configure Contextual Data from NetWitness Endpoint via Recurring Feed

You can configure RSA NetWitness Endpoint data in RSA NetWitness Suite to provide contextual data from NetWitness Endpoint to Decoder and Log Decoder sessions. This configuration adds contextual meta values in addition to the instant IOC alerts that can be used to build correlations to other metadata in the NetWitness Suite ecosystem.

Administrators can configure NetWitness Suite to consume system scan contextual data from NetWitness Endpoint via a NetWitness Suite Live recurring feed. This integration can enrich the session from a Decoder or Log Decoder with contextual information displayed in NetWitness Suite Investigation; some examples include the host operating system, MAC address, IIOC score, and other data that may not be present in the log or packet data into sessions from a Decoder or Log Decoder.

Note: Although this feature is targeted for customers with a packet Decoder, a recurring feed can also be implemented in Log Decoders.

Caution: In environments with many NetWitness Endpoint hosts, use of this recurring feed may result in decreased performance on the NetWitness Suite ingest devices (Decoder and Log Decoder).

Prerequisites

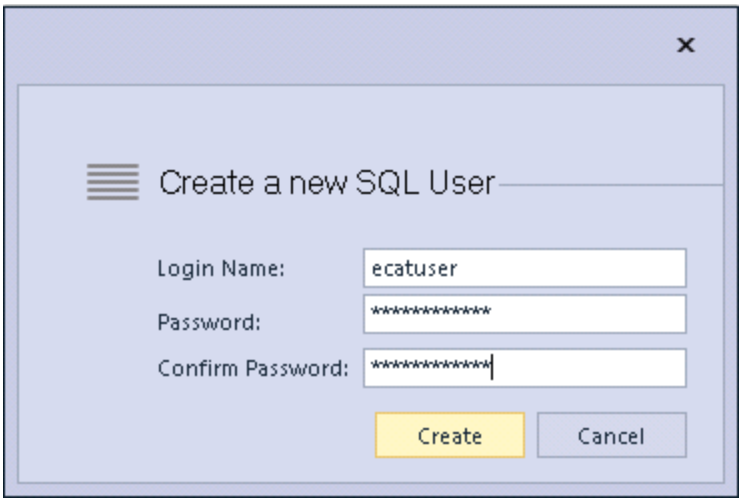
- Version 4.3.0.4, 4.3.0.5, or 4.4 NetWitness Endpoint Console server and NetWitness Server Version 10.4 and above installed.
- Version 11.0 RSA Decoder and Concentrator connected to the NetWitness Server in the network.

To Configure Contextual Data from NetWitness Endpoint via Recurring Feed, perform the following:

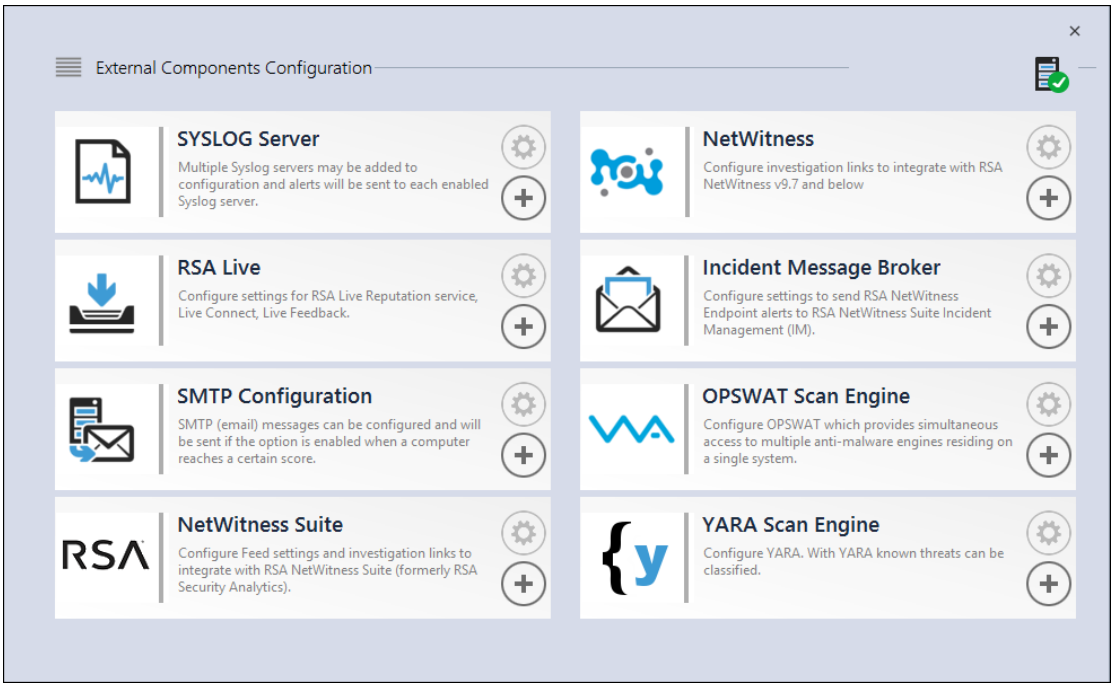
1. Enable the NetWitness Endpoint Feed for NetWitness Suite in the NetWitness Endpoint User Interface.
2. Export the NetWitness Endpoint CA Certificate from the NetWitness Endpoint Console server and Import it into NetWitness Suite trust store.
3. Configure the NetWitness Suite Concentrator service to define which meta keys are indexed.
4. Create a recurring feed in NetWitness Suite Live.

Enable the NetWitness Endpoint Feed for NetWitness Suite

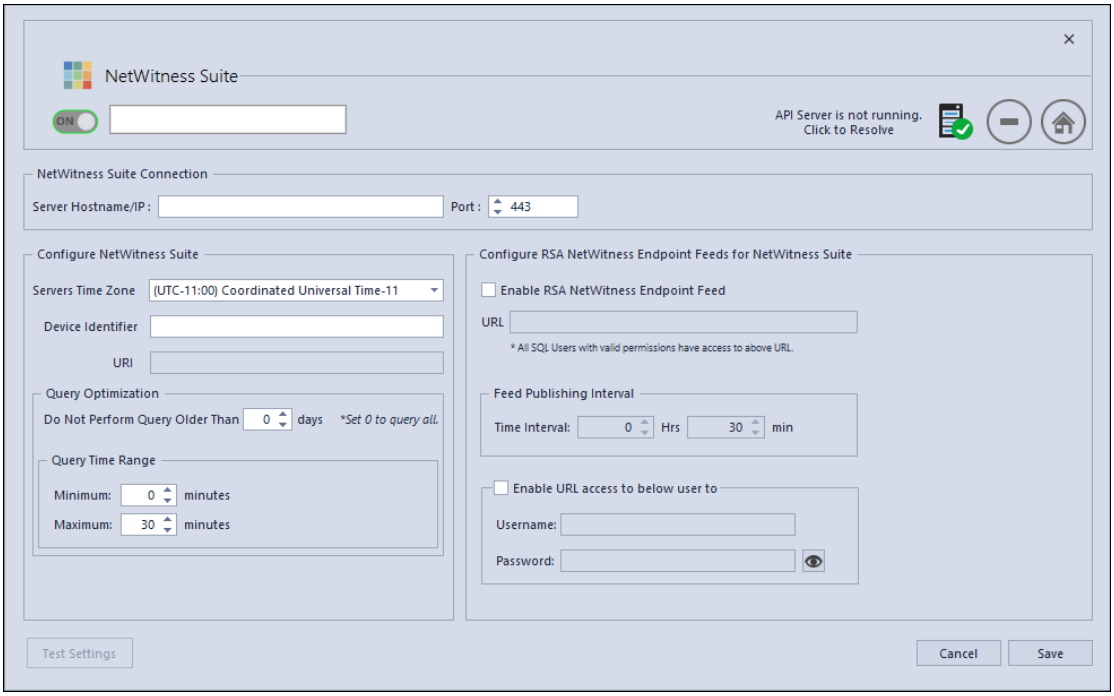
1. In the NetWitness Endpoint user interface, create SQL user in NetWitness Endpoint:
   a. Open the NetWitness Endpoint user interface and log on using the proper credentials.
   b. From the menu bar, select **Configure > Manage Users and Roles**, right-click in the pane, and select **create sql user**.
   The Create a new SQL User dialog is displayed.



   c. Enter the **Login Name** and **Password** and click **Create**.
2. From the menu bar, select **Configure > Monitoring External Components**.
   The External Components Configuration dialog is displayed.



3. In NetWitness Suite, click +.
   The NetWitness Suite dialog is displayed.



4. In the **NetWitness Suite** panel, in **On**, enter the name to identify the NetWitness Suite component.

5. In the **NetWitness Suite Connection** panel, perform the following.
   a. In the **Server Hostname/IP** field, enter the host name or IP address of the NetWitness Server.
   b. In the **Port** field, enter the port number. By default port number is 443.
6. In the **Configure NetWitness Suite** panel, perform the following:
   a. In the **Servers Time Zone** field, select the time zone for the component from the drop-down list.
   b. In the **Device Identifier** field, enter the NetWitness Suite concentrator device ID.

   Note: You can find the Device Identifier in NetWitness Suite when you look up a Concentrator or Broker in **Investigation > Navigate >***<Concentrator or Broker Name>*. The Device Identifier is the number in the URL after "investigation." For example, in the URL `https://<IP address>investigation/319/navigate/values`, the Device Identifier is **319**.

   The **URI** field is populated when you click **Save**.
7. In the **Query Optimization** panel, in the **Do Not Perform Query Older Than** field, enter the number of days to limit the query period. Enter **0** if you want to discard this feature.
8. In the **Query Time Range** panel, perform the following:
   a. In the **Minimum** field, enter the number of minutes for the minimum query time range. This value is used to automatically increase the time range submitted to NetWitness Suite. This ensures that a query returns a positive response if the NetWitness Endpoint Agent's reported time is slightly different than NetWitness Endpoint's time.
   b. In the **Maximum** field, enter the number of minutes to limit the time range. This value is used to automatically limit the time range submitted to NetWitness Suite, so that a query does not overload the NetWitness Server.
9. In the **Configure RSA NetWitness Endpoint Feeds for NetWitness Suite** panel, perform the following:
   a. Select **Enable RSA NetWitness Endpoint Feed**.
   b. In the **URL** field, enter the SQL **Username** and **Password** (configured in step 1) to access the location of the feed.
      The **URL** field is populated when you click **Save**.
   c. Enter the time interval for the frequency at which feeds are published.

10. In the **Feed Publishing Interval** panel, in the **Time Interval** field, select the time interval in **hrs** and **mins** for the frequency at which feeds are published.
11. In the **Enable URL access to below user to** panel, enter the **Username** and **Password** of the NetWitness Endpoint user.
12. Click **Save**.
    A feed is created.

Export the NetWitness Endpoint SSL Certificate

Note: This procedure works only for NetWitness Suite 10.5 and above because Java 8 support was added for 10.5. If you are using an earlier version of NetWitness Suite, refer to the applicable version of this guide.

To export the NetWitness Endpoint CA certificate from the NetWitness Endpoint Console server and copy it to the NetWitness Suite host:

1. Log on to the NetWitness Endpoint Console.
2. Open **MMC**.
3. Add a certificate snap-in for **Computer account**.
4. Export the certificate named **`NweCA`** (in NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 fresh install) or **`EcatCA`** (in NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5).
   a. Export without a private key.
   b. Export in DER encoded binary X.509 (`.CER`) format.
   c. Name it **`NweCA.cer`** (in NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 fresh install) or **`EcatCA.cer`** (in NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5).
5. Copy the NetWitness Endpoint CA certificate to the NetWitness Suite host:
   - For NetWitness Endpoint 4.3.0.4, 4.3.0.5 or 4.4 fresh installation:
     `scp NweCA.cer root@<sa-machine>:.`
   - For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5:
     `scp EcatCA.cer root@<sa-machine>:.`
6. To import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store, perform the following:

a. Check the Java version installed on your NetWitness Suite using the following command:
`java -version`
The openjdk version is displayed. For example, openjdk version "`1.8.0_71`"

b. To set the JDK parameter, navigate to java directory. Enter the following commands:

- JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/
- For NetWitness Endpoint fresh installation:

  $JDK/bin/keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
- For NetWitness Endpoint upgraded from previous version:

  $JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit

When prompted for certificate update confirmation, enter **Yes**.

7. On the NetWitness Suite host, do one of the following:
   - For NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 fresh installation, edit **`/etc/hosts`** to map the IP address of the NetWitness Endpoint Console server to the name **NweServerCertificate** by adding the following line to the file:

     <ip-address-ecat-cs> NweServerCertificate
   - For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5, edit **`/etc/hosts`** to map the IP address of the upgraded NetWitness Endpoint Console server to the name **`ecatserverexported`** by adding the following line to the file:

     <ip-address-ecat-cs> ecatserverexported
8. To restart NetWitness Suite, enter the following command:

   service jetty restart

Configure the NetWitness Suite Concentrator Service

1. Log on to NetWitness Suite and go to **ADMIN > Services**.
2. Select a Concentrator from the list and select **View > Config.**
3. Select the **Files** tab, and from the **Files to Edit** drop-down menu, select **index-concentrator-custom.xml**.
4. Add the following NetWitness Endpoint meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them. The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:
   description is the name of the meta key you want to display in NetWitness Suite

Investigation.

level is "IndexValues"

name matches the column name of the CSV file that NetWitness Suite uses while defining the recurring feed (see the table in *Configure the Recuring Custom Feed Task in NetWitness Suite* below).

```
<key description="Gateway" format="Text" level="IndexValues" name="gateway" valueMax="250000" defaultAction="Open"/>
<key description="Risk Number" format="Float64" level="IndexValues" name="risk.num" valueMax="250000" defaultAction="Open"/>
<key description="Strans Addr" format="Text" level="IndexValues" name="stransaddr" valueMax="250000" defaultAction="Open"/>
<key description="Domain" format="Text" level="IndexValues" name="domain" valueMax="250000" defaultAction="Open"/>
<key description="User Account" format="Text" level="IndexValues" name="username" valueMax="250000" defaultAction="Open"/>
<key description="Ecat Connectiontime" format="Text" level="IndexValues" name="ecat.ctime" valueMax="250000" defaultAction="Open"/>
<key description="Ecat Scantime" format="Text" level="IndexValues" name="ecat.stime" valueMax="250000" defaultAction="Open"/>
```

5. Restart the Concentrator to activate the custom key updates.

Configure the Recurring Custom Feed Task in NetWitness Suite

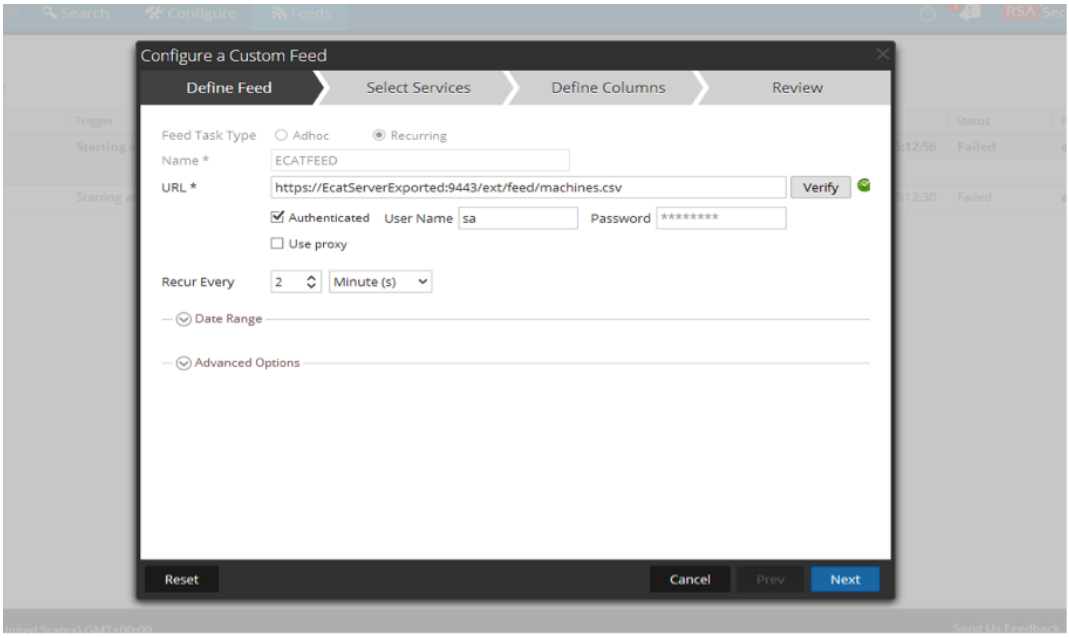
1. Log on to NetWitness Suite and go to **CONFIGURE > Custom Feeds**.
   The Feeds view is displayed.
2. In the toolbar, click .
   The Setup Feed dialog is displayed.
3. In the Setup Feed dialog, select **Custom Feed** and click **Next**.
   The Configure a Custom Feed wizard is displayed, with the Define Feed form open.
4. In the **Define Feed**, perform the following:
   a. In the **Feed Task Type** field, select **Recurring**.
   b. In the **Name** field, enter the name of the feed. For example, EndpointFeed.
   c. In the **URL** field, enter the URL with the hostname of the Windows server on which NetWitness Endpoint is installed:

- For NetWitness Endpoint 4.3.0.4, 4.3.0.5 or 4.4 fresh installation, use the URL **`https://NweServerCertificate:9443/api/v2/feed/machines.csv`**.
- For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5, use the URL **`https://ecatserverexported:9443/api/v2/feed/machines.csv`**.

d. Enable the checkbox **Authenticated** and enter the username and password as noted in *Enable the ECAT Feed* above.

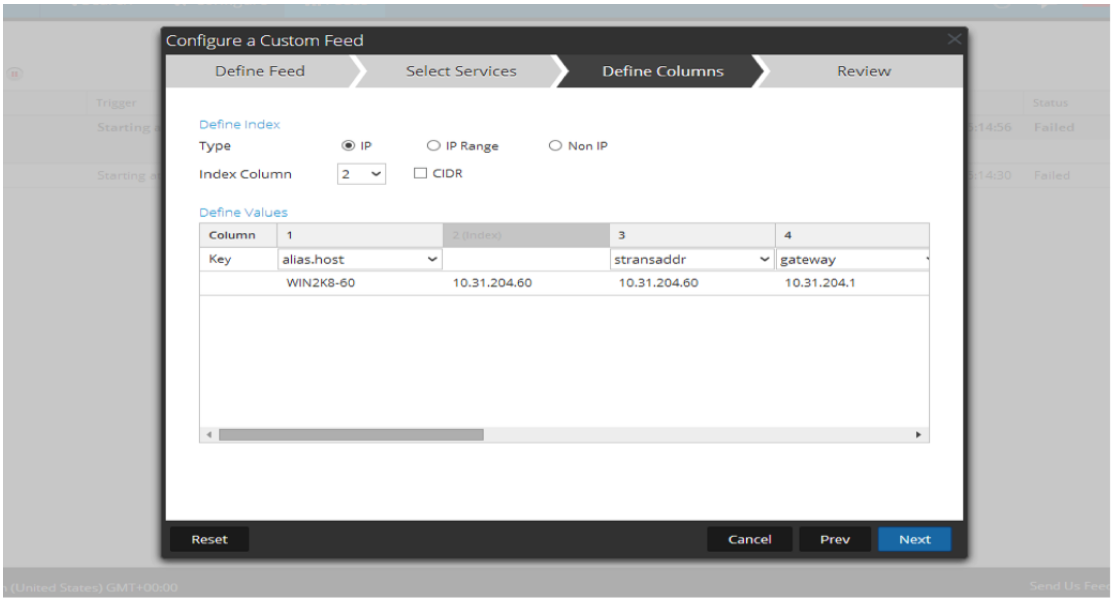
e. Click **Verify** to check if NetWitness Suite can reach the web resource.

f. Define the schedule and click **Next**.



5. In the **Select Services** tab, select the Decoder or groups to consume the feed. Click **Next**.

6. In the **Define Columns** tab, enter the column names as shown in the table below and save the feed.

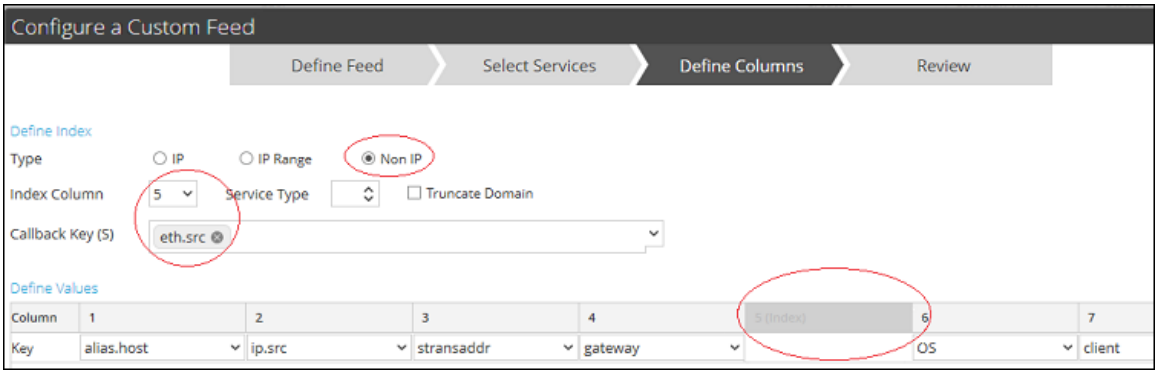


The following table shows the columns in the CSV file for the NetWitness Endpoint feed.

Column	Name	Description	Column Name in NetWitness Suite (Meta Key Name)
1	MachineName	Host name of the Windows agent	alias.host
2	LocalIp	IPv4 address	IP type (indexed column)
3	RemoteIp	Far end IP as seen by the router	stransaddr
4	GatewayIp	IP of the gateway	gateway
5	MacAddress	MAC address	eth.src
6	OperatingSystem	Operating system used by the Windows Agent	OS

Column	Name	Description	Column Name in NetWitness Suite (Meta Key Name)
7	AgentID	Agent ID of the host (unique ID assigned to the agent)	client
8	ConnectionUTCTime	Last time when the agent connected to NetWitness Endpoint server	ecat.ctime
9	Source Domain	Domain	domain.src
10	ScanUTC time	Last time when the agent was scanned	ecat.stime
11	UserName	Username of the client machine	username
12	Machine Score	Score of the agent indicating the suspicious level	risk.num

Note: In the table, the recommended index setting is LocalIp. However, if the LocalIp for NetWitness Endpoint Agent PC is allocated by a DHCP Server and the DHCP lease has expired, and if the IP is then re-allocated to another PC, the metadata created by the feed will be incorrect. To avoid this risk, use the machine name or the Mac address instead of the localIP address as the Feed's index. For example, to use a Mac address, you could enter the values as shown in the following figure.



Result

When viewing feed data in NetWitness Suite, upon a match of the indexed value (ip.src), meta data is populated in Investigation, Reporting, and Alerting Interfaces.

Configure Endpoint Alerts via Syslog into a Log Decoder

You can configure the use of RSA NetWitness Endpoint data in RSA NetWitness Suite to provide NetWitness Endpoint alerts via Syslog into Log Decoder sessions. This generates metadata that is used by NetWitness Suite Investigation, Alerts, and Reporting Engine.

For NetWitness Suite networks that are consuming logs, this integration of NetWitness Endpoint with NetWitness Suite pushes NetWitness Endpoint events to the Log Decoder via common event format (CEF) syslog messages and generates metadata that is used by NetWitness Suite Investigation, Alerts, and Reporting Engine. The use case for this integration is SIEM Integration to allow centralized event management, correlation of NetWitness Endpoint events with other Log Decoder data, NetWitness Suite reporting on NetWitness Endpoint events, and NetWitness Suite alerting of NetWitness Endpoint events.

Prerequisites

The following are required for this integration:

- Version 4.3.0.4, 4.3.0.5, or 4.4 NetWitness Endpoint UI.
- NetWitness Server Version 11.1 is installed.
- Version 10.4 or later RSA Log Decoder and Concentrator connected to the NetWitness Server in the network.
- Port UDP- 514 or TCP - 1514 open from NetWitness Endpoint server to Log Decoder in the firewall.

Procedure

1. Deploy the required parser (CEF or rsaecat) to the Log Decoder as described in the "Manage Live Resources" topic in *Live Services Management*. After you deploy the parser, make sure the parser is enabled. For more information, see Services Config View - General Tab.

Note: Use only one of these parsers. When the CEF parser is deployed, it supersedes the NetWitness Endpoint parser, and all CEF messages into NetWitness Suite are processed by the CEF parser. Enabling both parsers is an unnecessary burden on performance.

2. Configure NetWitness Endpoint to send syslog output to NetWitness Suite and generate NetWitness Endpoint alerts to the Log Decoder.

3. (Optional) Edit the table mapping in `table-map-custom.xml` and the `index-concentrator-custom.xml` to add fields based on user preferences for metadata to be mapped to NetWitness Suite.

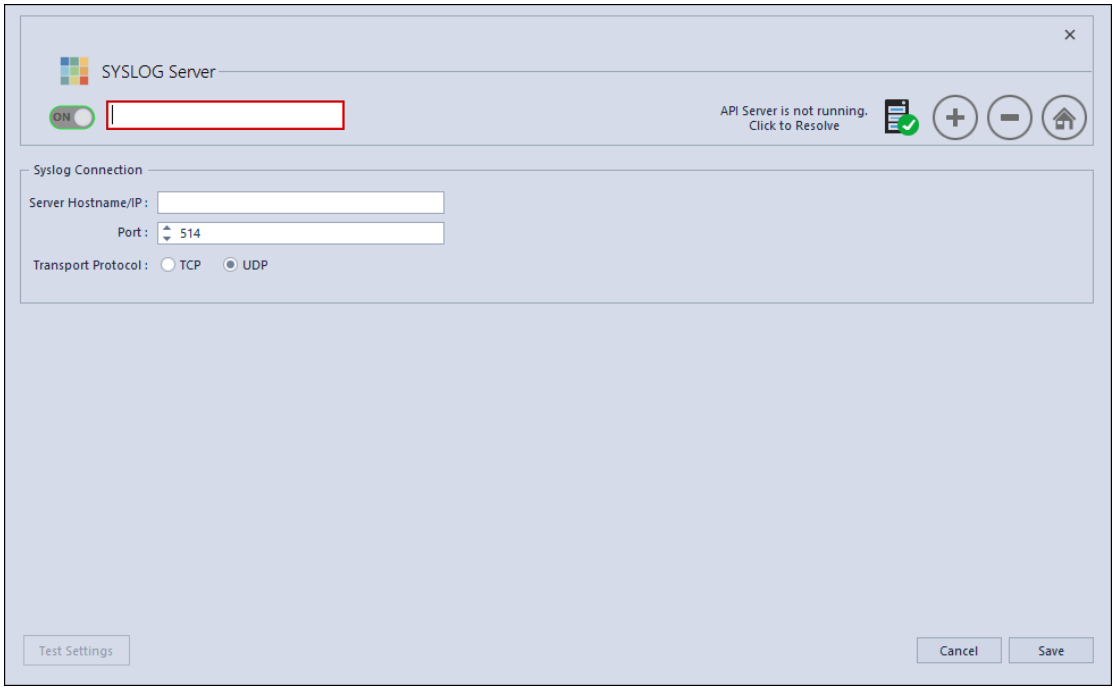
Configure NetWitness Endpoint to Send Syslog Output to NetWitness Suite

To add the Log Decoder as a Syslog external component and generate NetWitness Endpoint alerts to the Log Decoder:

1. Open the NetWitness Endpoint user interface and log on using the proper credentials.
2. From the menu bar, select **Configure > Monitoring and External Components**.

   The External Components Configuration dialog is displayed.
3. In **SYSLOG Server**, click ✚.

   The SYSLOG Server dialog is displayed.

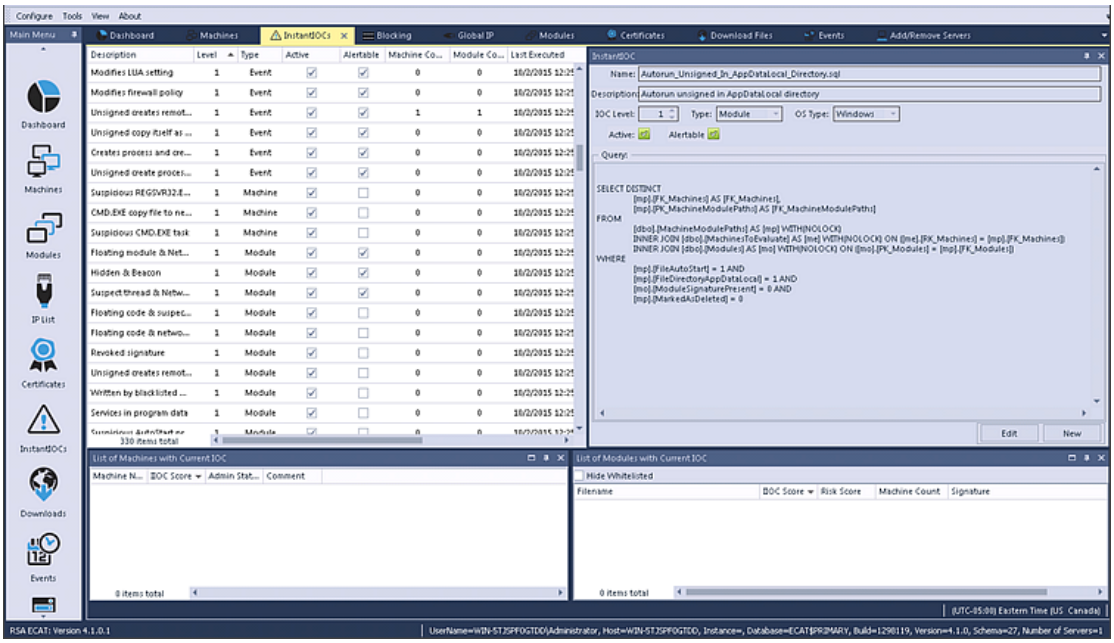


4. In the **NetWitness Suite** panel, in **On**, enter the descriptive name for the Log Decoder.
5. In the **Syslog Connection** panel, perform the following to enable Syslog messaging:

   Server Hostname/IP = The hostname DNS or IP address of the RSA Log Decoder
   Port = 514

Transport Protocol = Select **UDP** or **TCP** as appropriate for your Syslog server for the transport protocol.

6. Click **Save**.
7. Open the **InstantIOCs** window in the NetWitness Endpoint UI and, in the **Alertable** column, click to enable each IIOC for which you want alerts sent to the Log Decoder.



When the instant IOCs are triggered, Syslog alerts from the NetWitness Endpoint server are sent to the Log Decoder. Log Decoder alerts are then aggregated to the Concentrator. These events are injected into the Concentrator as metadata.

Edit the Table Mapping in table-map-custom.xml

In the default RSA table-map.xml provided by RSA, the meta keys in the `table-map.xml` file are set to `Transient`. In order to view the meta keys in Investigation, the keys must be set to `None`. To make changes to the mapping, you must add the entries to the `table-map-custom.xml` on the Log Decoder.

This is the list of meta keys in `table-map.xml`.

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
agentid	client	No
CEF Header Hostname Field	alias.host	No

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
CEF Header Product Version	version	Yes
CEF Header Product Name	Product	Yes
CEF Header Severity	severity	Yes
CEF Header Signature ID	event.type	No
CEF Header Signature Name	event.desc	No
destinationDnsDomain	ddomain	Yes
deviceDnsDomain	domain	Yes
dhost	host.dst	No
dst	ip.dst	No
end	endtime	Yes
fileHash	checksum	Yes
fname	filename	No
fsize	filename.size	Yes
gatewayip	gateway	Yes
instantIOCLevel	threat.desc	No
instantIOCName	threat.category	No
machineOU	dn	Yes
machineScore	risk.num	No
md5sum	checksum	Yes
os	OS	Yes

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
port	ip.dstport	No
protocol	protocol	Yes
Raw Message	msg	Yes
remoteip	stransaddr	Yes
rt	alias.host	No
sha256sum	checksum	Yes
shost	host.src	No
smac	eth.src	Yes
src	ip.src	No
start	starttime	Yes
suser	user.dst	No
timezone	timezone	Yes
totalreceived	rbytes	Yes
totalsent	bytes.src	No
useragent	user.agent	No
userOU	org	Yes

The following seven keys are not in `table-map.xml`; to use these keys in NetWitness Suite you need to add them to `table-map-custom.xml`, and set the flags to `None`.

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
moduleScore	cs.modulescore	Yes

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
moduleSignature	cs.modulesign	Yes
Target module	cs.targetmodule	Yes
YARA result	cs.yararesult	Yes
Source module	cs.sourcemodule	Yes
OPSWATResult	cs.opswatresult	Yes
ReputationResult	cs.represult	Yes

Here are the entries to be added to the `table-map-custom.xml` if required.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
 <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
 <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
 <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
 <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
 <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
 <mapping envisionName="cs_yararesult" nwName="cs.yararesult" flags="None"
envisionDisplayName="YaraResult"/>
```

Note: Restart the Log Decoder or reload the log parsers for the changes to take effect.

Configure the NetWitness Suite Concentrator Service

1. Log on to NetWitness Suite and go to **ADMIN** > **Services**.
    1. Select a Concentrator from the list and select **View > Config.**
2. Select the **Files** tab, and from the **Files to Edit** drop-down list, select **index-concentrator-custom.xml**.
3. Add the NetWitness Endpoint meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them.
4. Restart the Concentrator.

5. To add the Concentrator as a data source in the Reporting Engine, in the **ADMIN** > **Services** view, select the Reporting Engine and Select **View> Config > Sources.** NetWitness Endpoint meta is populated in Reporting Engine, and you can run reports by selecting the appropriate meta keys.

Example

Note: The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:
description is the name of the meta key you want to display in NetWitness Suite Investigation.
level is "IndexValues"
name is the NetWitness Endpoint meta key name from the table below

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
 <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
 <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
 <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
 <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
 <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
 <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
 <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
 <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
 <key description="Module Sign" format="Text" level="IndexValues"
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
 <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
 <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
 <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
 <key description="yara result" format="Text" level="IndexValues"
```

```
name="cs.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
 <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
 <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
 <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
 <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
 <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
 <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
 <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
 <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
 </language>
```

Result

Analysts can:

- Create NetWitness Suite alerts based on NetWitness Endpoint events by configuring NetWitness Endpoint events as an enrichment source.
- Create ESA rules using NetWitness Endpoint meta as described in the "Add Rules to the Rules Library" topic in the *Alerting with ESA Correlation Rules User Guide*.
- Report on NetWitness Endpoint events using NetWitness Endpoint meta as described in the "Configure a Rule" topic in the *Reporting Guide*.
- View NetWitness Endpoint alerts in NetWitness Respond as described in the "View Alerts" topic in *NetWitness Respond User Guide*.
- View NetWitness Endpoint meta keys in Investigation along with standard NetWitness Suite core meta keys as described in the "Conduct an Investigation" topic in *Investigation and Malware Analysis User Guide*.

RSA NETWITNESS® SUITE

Release Notes

for Version 11.1.0.0

RSA NETWITNESS® SUITE

Release Notes

for Version 11.1.0.0

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

Introduction 7

What's New 8

NetWitness Endpoint Insights 8

NetWitness Respond 9

NetWitness Investigate 9

Reporting 11

Health and Wellness 11

Event Stream Analysis and ESA Analytics 11

Core Services 11

User Interface 12

Platform 12

Administration 12

Log Parsing 13

Unified Data Model 14

Upgrade Instructions 15

Fixed Issues 16

Security 16

Investigate 16

Log Collector, Virtual Log Collector 17

Context Hub 18

Respond 18

Event Stream Analysis and ESA Analytics 18

Features Not Supported 19

Features Not Supported in 11.1.0.0 or later releases 19

Features Available in Future Releases 19

Known Issues 21

Known Issues During Upgrade to 11.1 21

Context Hub 27

General Application Issues 28

Endpoint 28

Respond 30

Log Collector 35
Investigate 36
Workbench 39
Custom Feeds 40
Malware Analysis 40
Event Stream Analysis 41
Reporting 43
Administration 44
Event Source Management 45
Core Services 46

Product Documentation 47

Contacting Customer Care 48

Revision History 49

Introduction

This document lists enhancements and fixes in RSA NetWitness Suite 11.1.0.0. Read this document before deploying or updating toRSA NetWitness Suite 11.1.0.0.

- What's New
- Upgrade Instructions
- Fixed Issues
- Features Not Supported
- Known Issues
- Product Documentation
- Contacting Customer Care
- Revision History

What's New

The RSA NetWitness Suite 11.1.0.0 release provides RSA NetWitness Endpoint Insights as part of the RSA NetWitness Suite thus presenting a common platform for investigations on logs, packets and endpoints.

NetWitness Endpoint Insights

RSA NetWitness Endpoint Insights provides visibility to vital host and user information. A new RSA NetWitness Endpoint Insights agent facilitates endpoint data to licensed RSA Netwitness Suite customers. It also transforms the collected endpoint data into powerful metadata that is correlated with network data across the entire suite. This helps to drive and prioritize investigation and response analyst workflows.

NetWitness Endpoint Insights Agent. This solution includes a lightweight agent for collecting host inventories, processes, user activity, and Windows logs thus reducing overall complexity of capturing logs and saving valuable time and resources for Security Operations Center (SOC) operations. This endpoint agent can be installed on Windows, Mac, or Linux hosts. It scans the hosts and sends data to the Endpoint Hybrid or Endpoint Log Hybrid over HTTPS. For more information, see the *Endpoint Insights Agent Installation Guide*.

NetWitness Endpoint Insights introduces two new services, Endpoint Hybrid and Endpoint Log Hybrid. You can deploy either one of these services.

Endpoint Hybrid. Is used for collection of endpoint data. There is no license required to collect endpoint data. The Endpoint Hybrid consists of an Endpoint Server, a Log Decoder, and a Concentrator. It can:

- Perform instant scans to understand the host behavior at any point in time.
- Store multiple scan snapshots.
- Process endpoint metadata for analysis and aggregation.
- Optimally store and manage scan data using retention policies.

Endpoint Log Hybrid. Is used to collect both endpoint and log data. In addition to the capabilities of an Endpoint Hybrid, this service can collect logs from Windows hosts through Endpoint agents, and all other event sources that are supported for log collection. The agent forwards the collected logs to a Log Decoder or Remote Log Collector. A license is required to collect log data. If you have throughput or perpetual licenses for Log Decoders, you can use them. If not, you must procure a license to collect logs both from the endpoint agent and any other log events collected using a Log Collector or Log Decoder. The Endpoint Log Hybrid consists of an Endpoint Server, Log Decoder, Concentrator, and Log Collector. For more information, see the *RSA NetWitness Endpoint Insights Configuration Guide*. Log collection capability can be enabled during agent installation. Logs can be filtered based on channels and a list of events that you want to collect. For more information, see the *Endpoint Insights Agent Installation Guide* and *Log Collection Configuration Guide* .

Endpoint Metadata. Data collected can be forwarded as metadata to a Log Decoder for seamless investigation for analysts along with log and packet data. You can generate reports and alerts with this metadata. For more information, see the *Endpoint Insights Configuration Guide*.

NetWitness Respond

Unassign Incidents. You can now change an incident assignee to "(unassign)" (RESPOND > Incidents).

Filter for Unassigned Incidents. You can now filter the Incidents List to show only unassigned incidents (RESPOND > Incidents – Filters panel).

Add Alerts to Incidents. In addition to creating incidents from alerts, you can now add alerts to existing incidents from the Alerts List view (RESPOND > Alerts).

Improved Search for Related Indicators. In the Related Indicators panel for an incident, when searching for related indicators, it is no longer necessary to specify a Source, Destination, and Detector. The search for related indicators now queries all fields applicable to the search (Incident Details view - Related Indicators panel). For more information, see the *NetWitness Respond User Guide*.

New Incident Rules User Experience. Aggregation rules are now called Incident Rules. The Incident Rules pages have been redesigned for ease of use and there is now an Incident Rules List view and an Incident Rule Details view (CONFIGURE > Incident Rules). To better differentiate incident rule enabled status, the icons now have different shapes as well as different colors.

Added a User Behavior Default Incident Rule. The User Behavior default incident rule captures network user behavior. This rule uses deployed RSA Live ESA Rules to create incidents from alerts. You can select the RSA Live ESA Rules that you want to monitor.

Updated Some Preconfigure (Default) Incident Rules with the Source IP Address Group by Value. The following default incident rules changed slightly and now have "Source IP Address" as the Group By value:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

For more information, see the *NetWitness Respond Configuration Guide*.

Send Respond Email Notifications. You can now send email notifications to Analysts assigned to incidents and to SOC Managers when incidents are created or updated (CONFIGURE > Respond Notifications). For more information, see the *NetWitness Respond Configuration Guide*.

NetWitness Investigate

Integrated User Interface for Endpoints. The new Hosts and Files views (available in the Investigate submenu) provide a view of all hosts and files found in the deployment. For more information, see the *NetWitness Investigate User Guide*.

Direct Access to Event Analysis in the Investigate Submenu. The Event Analysis view is accessible from the Investigate submenu, in addition to the previous methods of opening the view. For more information on the investigation activities and features of Event Analysis, see the *NetWitness Investigate User Guide*.

Meta Entities in Investigate. Administrators can create meta entities (groups of meta keys) that represent two or more meta keys. Meta entities can be used in the same ways that a meta key is used in Investigate, except in Parallel Coordinates visualizations. Predefined meta entities are available for typical scenarios. For example, to find entities such as all IP addresses, all user names, all files, or all hosts, analysts can use the meta entity to build a simple query without having to know the specific meta keys in the entity. For more information, see "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*.

Interactive Breadcrumb in Event Analysis with Autocomplete and Validation. The user interface lets analysts enter filters by clicking and typing, or using only keyboard actions. Analysts can add a `<meta key><operator><value>` filter to the breadcrumb, edit the filter, and delete one or more filters. Invalid filters are highlighted in a red box. Clicking the Query button executes the query, individual filters are ANDed, and the results are displayed in the Events List Panel. For more information, see “Filtering Events in the Events Analysis View" in the *NetWitness Investigate User Guide*.

Default and Custom Column Groups in the Event Analysis view. Column Groups have been enabled in the Event Analysis view. You can view and select default column groups and custom column groups, and the default is persisted per user. To manage column groups, go to INVESTIGATE > Events. In addition to the column groups in 11.0, the Endpoint Analysis, Outbound HTTP, and Outbound SSL/TLS groups have been added. For more information, see the *NetWitness Investigate User Guide*.

Ability to Reconstruct an Event Directly from the Navigate View. Given a known Event ID, analysts can reconstruct an event directly from the Navigate view. The **Actions > Go to event in Event Analysis** and **Actions > Go to event in Event Reconstruction** options in the Navigate view toolbar provide this capability. You can use this option without executing a query as you usually do when beginning an investigation. For more information, see “Reconstruct an Event from the Navigate View” in the *NetWitness Investigate User Guide*.

Pagination in the Event Analysis view > Packet Analysis. Pagination of packet data allows you to step through all the packets without rendering too much data at once. For more information, see the *NetWitness Investigate User Guide*.

Configurable Event Analysis View Using Event Preferences Panel. Analysts can personalize the Event Analysis views using the new Event Preferences panel. You can configure the default Event Analysis (Text, Packets, or File) and more display settings when you are analyzing an event. For more information, see "Configure User Preferences in Investigate" in the *NetWitness Investigate User Guide*.

Direct Link to Events View Email and Web Reconstruction from Event Analysis View. A link in the Event Analysis view opens the Web and email reconstructions of the selected event in the Events view reconstruction.

Right-click Actions on Meta values in the Event Analysis View. You can right-click a meta value in the Event Analysis view and launch actions such as look up the IP search and more. For more information, see the *NetWitness Investigate User Guide*.

Right-Click Meta Value Count in the Navigate View. Right-clicking the count next to a meta value in the Navigate view opens a context menu, from which you can send the event to a new tab in the Events view or the Event Analysis view. For more information, see the *NetWitness Investigate User Guide*.

Reporting

Reports for Endpoint Insights. Analysts can define and generate reports using endpoint metadata for analysis. To generate reports, the endpoint metadata must be forwarded to a Log Decoder. For more information, see the *Reporting User Guide*.

Health and Wellness

Monitor Endpoint Server. Administrators can monitor the health and wellness of the Endpoint Server from the Health and Wellness statistics. To monitor any statistics, you can create custom policies. For more information, see the *System Maintenance Guide*.

Event Stream Analysis and ESA Analytics

ESA Correlation Rules can use Context Hub data within rule logic. Lists of values created as data sources in Context Hub can now be configured as data enrichment sources in ESA and used within correlation rules as blacklist or whitelist sources. New Context Hub lists are available by default in the ESA rules for Netwitness 11.1 users. Users upgrading from previous versions to 11.1 will see these default lists in addition to their previously created context hub lists. For more information, see “Configure Context Hub List as an Enrichment Source” in the *Alerting with ESA Correlation Rules User Guide*.

Password change for ESA data source now available in UI. When editing settings for a data source, users may now change the configured password through the UI for ESA services. For more information, see “Configure ESA Correlation Rules” in the *ESA Configuration Guide*.

Core Services

Truncation options added to balance analytic value and storage space. An administrator can configure the system to save storage space by truncating data while still providing an analyst enough network data for analysis purposes. For more information, see “Configure Application Rules” in the *Decoder and Log Decoder Configuration Guide*.

Meta Entities in Correlation Rules and Application Rules. Administrators can create meta entities that represent two or more meta keys, and meta entities can be used anywhere that a meta key is used in the Log Decoder, Packet Decoder, and Concentrator rule builder. See the *Core Database Tuning Guide* for details.

Search API enhanced to return matches across entire word. This feature enhances the existing search API (msearch) to implement substring searches. A substring search is defined as finding arbitrary text somewhere in the middle, end, or beginning of a meta item. For example, an analyst can now search for "ball" in addition to "basket" to match "basketball." For more information, see the *Core Database Tuning Guide*.

Size buckets created to index size-related meta keys at the value level. This feature provides the option to use size buckets to index size-related meta keys at the value level, which facilitates doing further queries on the data not available when meta keys are indexed at the key level. For more information, see the *Core Database Tuning Guide*.

Capability added to optimize read/write operations on NWDB when adding new storage. The 10G Decoder now supports the capability to run a command on an existing NWDB (packet, log, meta, or session), that has at least two volumes, to stagger the files across all volumes in the most optimal read-write pattern. This is useful when adding new storage to an existing Decoder so the volumes can be staggered before restarting capture. For more information, see "Optimize Read/Write Operations When Adding New Storage" in the *Decoder Configuration Guide*.

Filter and rule hit counts provided to aid in troubleshooting. An administrator can now generate statistics in the form of hit counts for implemented rules and see the aggregate value to gauge the impact of specific rules or filters. This provides more insight into the impact of filters and rules on the local environment. For more information, see "Monitor Application Rules" in the *Decoder Configuration Guide*.

User Interface

Choose Light and Dark themes. You can now change the appearance of selected areas of NetWitness Suite User Interface from the global User Preferences settings. You have the option of viewing either the light or dark theme. For more information, see the *NetWitness Suite Getting Started Guide*.

Platform

Upgrade to CentOS 7.4 version. The OS version of NetWitness Suite is upgraded from CentOS 7.3 to CentOS 7.4 in the 11.1 release.

Administration

Manage Access for Endpoints. New roles and permissions are configurable in the ADMIN > Security > Roles and Permissions tabs to manage access for Endpoint related tasks. For more information, see the *System Security and User Management Guide*.

Introduced Respond Notification Settings permissions. These permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (CONFIGURE > Respond Notifications), which enable them to send email notifications when incidents are created or updated. For more information, see the *NetWitness Respond Configuration Guide* and the *System Security and User Management Guide*.

Configurable Permissions to Manage Access to Reconstruction in the Event Analysis View. New permissions for the investigate-server are configurable in the ADMIN > Security > Roles tab. A message is displayed in the Event Analysis view when the administrator has restricted parts of the user interface by blocking individual permissions for a user role. For more information, see the "Role Permissions" section in the *System Security and User Management Guide*.

Log Parsing

Introduced Default Log Parser and Log Parser Rules tab. Logs that do not have a corresponding parser will be processed against rules and metadata is then extracted by those rules and is available for Enrichment, Investigation, Reporting, and Alerting. To view this new tab, go to **ADMIN > Event Sources > Log Parser Rules**. This will provide immediate visibility into logs from custom or unsupported sources. Administrators can view and test sample log messages and rules for their log parsers, including the newly added Default log parser. The default log parser is used to parse logs coming from the Log Decoder that do not match any of your configured log parsers. In this new Default log parser, you can:

- View the rules for a particular log parser, including the default log parser.
- View the names, literals, patterns, and meta for each configured log parser.
- Edit sample log messages to view how they would be parsed by a particular log parser.

Introduced Log Parser Customization. You may need to modify one or more of your log parsers. For example, you may need to fix an unknown message, or to parse certain fields differently than in the manner provided by default. Log Parser Customization allows you to add a new file with new parser elements or modify existing custom files. All customizations in this separate file do not get removed or overwritten by Log Decoder upgrades or the updating of parsers through RSA Live. This feature is described in detail in the Log Parser Customization topic in the RSA Content space on RSA Link

Remote Log Collector accepts secure Syslog. The RLC now accepts secure Syslog messages, and can optionally verify the peer.

Improved capture rate performance of Checkpoint Logs.

> **Note:** The following new features are located on the Event Source Discovery page.

Introduced filtering by event source type. Administrators can filter the event source discovery grid by device types to ensure that no extra event source types are included.

Introduced acknowledging multiple event sources. Administrators can select multiple event sources that have been discovered correctly and acknowledge them by clicking on the **Toggle Acknowledge** button. Acknowledged event sources are filtered from the view by default.

Introduced mapping multiple event sources. Administrators can select multiple event sources that have the same types that are not being discovered correctly and bulk map them to the appropriate parsers. This provides the ability to compare the event sources to an external list and quickly remediate the ones that do not match the list.

Introduced Automatic Mapping. The system automatically maps incoming events to a type based on previous logs received from that address, reducing the number of items that need attention in the Discovery workflow. The UI indicates that an address has been auto-mapped in the Discovery workflow.

Moved the Acknowledge and Map filters to the Filter Panel on the Event Source Discovery page. Administrators can quickly view and manage event sources.

Introduced searching for event sources on the Event Source Discovery page.

Unified Data Model

Unified Data Model for organizing various data. Unified Data Model (UDM) in RSA NetWitness Suite provides a combined insight from Logs, Packets, and Endpoints. It organizes the various elements of data coming into NetWitness from disparate sources into one standardized data model. The Analysts can then look for data concepts in one place as defined by the Unified Data Model. Meta concepts defined in the UDM should be used uniformly across the suite to get the best consistent results. NetWitness uses Meta Keys as a way to retain context of the raw data after its parsed and stored on disk. Hence, it’s extremely important to parse out data in the most accurate Meta key to retain context that's needed for Threat Detection, Analytics and Response. For more information, see the UDM content on RSA link.

Upgrade Instructions

The following upgrade paths are supported for RSA NetWitness Suite 11.1.0.0:

- RSA NetWitness Suite 10.6.5.x to 11.1.0.0
- RSA NetWitness Suite 11.0.0.x to 11.1.0.0

For more information on upgrading to 11.1.0.0, see the update instructions in the Product Documentation section.

Fixed Issues

This section lists issues fixed since the last major release.

Security

Tracking Number	Description
Libraries updated in 11.1 to address security vulnerabilities	• Apache Commons Collections: to 3.2.2 • Apache Commons Validator: to 1.5.1 • Salt: to salt-2017.7.2-1.el7 • Jpython: to 2.7.1 • Jetty: Java based HTTP, Servlet, SPDY, WebSocket Server: to 8.1.2
ASOC-49307	Samba https://access.redhat.com/errata/RHSA-2017:3260
ASOC-49306	Curl https://access.redhat.com/errata/RHSA-2017:3263
ASOC-43884	Logstash Upgraded to 5.6.4, vulnerabilities addressed: ESA ID — CVE ESA-2017-05 — CVE-2017-5645 ESA-2016-08 — CVE-2016-10362 ESA-2016-06 — CVE-2016-10363 ESA-2016-02 — CVE-2016-1000221 ESA-2016-01 — CVE-2016-1000222
ASOC-43718	Kernel https://access.redhat.com/errata/RHSA-2017:2930
ASOC-42524	Kernel https://access.redhat.com/errata/RHSA-2017:2679
ASOC-49308	Tcpdump https://access.redhat.com/errata/RHSA-2017:1871

Investigate

Tracking Number	Description

ASOC-41703	In a mixed mode environment the Event Reconstruction View > File View displays the word "terminated" instead of the list of files.
ASOC-41696	Analyst is unable to unzip the downloaded file archive due to the zip file not having the restricted content.
ASOC-37989	Right-click action in the Log View does not launch Event Reconstruction on Event Analysis when you click on a Logs column that wraps to more than one row.
ASOC-37348	In Event Analysis, the rendered packets message is not displayed for events with a small payload but large number of packets.

Log Collector, Virtual Log Collector

Tracking Number	Description
ASOC-49091, SMC-13792	Rebranded the Security Analytics Netflow Collector to Netwitness Netflow Collector in the CEF parser. RSA has renamed the **product name** value from “Security Analytics Log Collector” to “**NetWitness NetFlow Collector**” for the Netflow protocol on LogCollector. If you have any rules that that use “Product name” meta, and is matching on the value “Security Analytics Log Collector,” then that rule will not fire when you upgrade your Log Collector to 11.1. In this case, manually update these rules to match the new product name “**NetWitness NetFlow Collector**” .
ASOC-45452	Reworded an ODBC test connect log message to be more clear.
ASOC-45451	Resolved a Log Collector crash when closing an ODBC connection.
ASOC-45448	Added an ODBC configuration option to select whether **device.ip** is the actual source IP address, or if Log Collector event source IP address should be used for the **device.ip** meta value.
ASOC-31313	Added better handling for Windows log messages that contain malformed XML.
ASOC-16717	Bandwidth throttling configuration changes to control the rate that the Remote Collector sends event data to a Local Collector did not persist after a reboot. This issue has been fixed. The `set-shoveltransfer-limit.sh` script is used to set the bandwidth throttle for event data transferred from a remote collector to local collector.

Context Hub

Tracking Number	Description
ASOC-40944, ASOC-50159	Pivot to Investigate navigates to an incorrect URL when rabbitmq server is not reachable.

Respond

Tracking Number	Description
ASOC-41855	Unable to create an incident using 1000 alerts.
ASOC-41934	In 11.0, the "Suspected Command & Control Communication By Domain" aggregation rule Group By condition "Domain by Suspected C&C" was not functioning as expected and had to be changed to "Domain" to aggregate alerts and enable incidents to be created for "Suspected C&C." The "Domain by Suspected C&C" condition works correctly in 11.1 and should be used as the Group By condition for the "Suspected Command & Control Communication By Domain" aggregation rule (known as incident rule in 11.1). If you changed the "Suspected Command & Control Communication By Domain" aggregation rule Group By condition to "Domain" for 11.0, you will need to change it back to "Domain by Suspected C&C" for 11.1. (To do this, go to CONFIGURE > Incident Rules. In the Incident Rules list, locate the **Suspected Command & Control Communication by Domain** rule and click the link in the **NAME** field to open it. In the Incident Rules Details view Grouping Options section, set the **Group By** field to **Domain for Suspected C&C** and click **Save**.)

Event Stream Analysis and ESA Analytics

Tracking Number	Description
ASOC-39880	Trial rules become disabled despite low memory usage.
ASOC-45568	After upgrading to Security Analytics 10.5.1.1, ESA rules that leverage PostgreSQL database integration appear to no longer work.
ASOC-45569	When deploying an advanced rule with post-alert enrichment, if the advanced rule syntax does not contain @RSAAlert, rule deployment fails.

Features Not Supported

The following tables provide information on features no longer supported in RSA NetWitness Suite 11.1 or Later Releases.

Features Not Supported in 11.1.0.0 or later releases

No.	Feature	Notes
1	Malware Colo	Malware co-located is not supported in 11.1.0.0 and later releases. Malware Analysis is supported using a standalone Malware Analysis.
2	All-In-One (AIO) Deployment	All-in-one deployment is not supported. Fresh Install AIO has been removed.
3	Standalone Warehouse Connector	Standalone Warehouse Connector is not supported.
4	Administration Features	1. Forgot my password. 2. Email Notification to user when password expires. 3. Changing the Login banner is not supported. 4. Test/Search AD user.
5.	Pivotal	Pivotal is not supported.
6.	ESA Cross-Site Correlation	The ESA Cross-Site Correlation configuration option (previously found by going to ADMIN > System > ESA) has been removed and will not be supported as part of the 11.1 release going forward. If a 10.6.5.x user that was using this feature upgrades to 11.1, a message will inform them that the feature is no longer available, but they will still be able to see and modify the correlation rules that had previously been used for Cross-Site Correlation.

Features Available in Future Releases

The following features are not available in 11.1 and may be available in a future release.

No.	Feature	Notes
1	IPDB Reporting	IPDB Extractor service is not supported in 11.1.0.0 and will be available in later releases.
2	STIG	If you have a STIG hardened host, you cannot upgrade to 11.1.0.0 as the backup scripts do not support that.
3	Multiple Security Analytics Server (NetWitness Server) support	Multiple server deployment is not supported.
4	PKI Authentication	PKI Authentication feature is not available in 11.1.0.0
5	Warehouse Analytics	Warehouse Analytics is not supported for 11.1.0.0 and will be available in later releases.
6	Endpoint Analytics	Analytics, such as risk score or IOC calculation is not supported on the endpoint scan data
7	Endpoint Remediation	Response functionality (containment/blocking) is not supported.
8	Endpoint Tracking	Tracking network events is not supported.
9	Endpoint Kernel mode	Endpoint agent currently works in the User mode and does not support the Kernel mode detection
10	Endpoint File reputation	File reputation, such as OPSWAT, YARA, and Reversing Lab lookups are not supported and hence cannot whitelist or blacklist files.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround is available, it is noted or referenced in detail.

Known Issues During Upgrade to 11.1

The following known issues occur during upgrade from 10.6.5.x to 11.1 or update from 11..0.0.x to 11.1.

After offline update and reboot the UI still notifies to reboot host

Tracking Number: ASOC-50839

Problem: When you perform an offline update from 11.0.0.x to 11.1 and reboot through CLI, the UI still Notifies to reboot host.

Workaround: Reboot the host using the UI.

After upgrading to 11.1, there is Concentrator Initialization error if you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have the same fields indexed on the Concentrator

Tracking Number: ASOC-50702

Problem: This error occurs when you have done customized meta keys on your Log Decoder and Concentrator.

Workaround: If you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have those same fields indexed on the Concentrator, then you must change data type of these fields to IPv4 on both the Log Decoder and Concentrator.

Integration-server service is missing on the UI after update

Tracking Number: ASOC-50835

Problem: After upgrading 11.0.0.x to 11.1.0.0, the integration-server service is missing on the UI.

Workaround: None.

After upgrade from 10.6.5.x to 11.1.0.0, offline licenses are not retained.

Tracking Number: ASOC-41757

Problem: Even if you upload a new response bin file from Download Central, offline licenses still do not work. Though old files are restored in `/var/lib/fneserver`, the licenses still remain deactivated.

Workaround: Perform the following steps to restore the licenses:

1. Generate a new response bin file from Download Central.
2. SSH into a Netwitness Server host 11.1.0.0 (AdminServer).
3. Move ra* files (3 files) out of `/var/lib/fneserver/`

4. Log in to RSA NetWitness 11.1.0.0 UI with admin user credentials and navigate to ADMIN > System > Licensing Overview tab.
5. Under Licensing actions, click Refresh licenses.
6. Upload the response file received from Download Central under ADMIN > System > Licensing > Settings Tab > Upload Response.

Note: Upgrade using Online mode (RSA Netwitness Suite 11.1.0.0 connected to the Internet) works successfully and all licenses are restored after upgrade to 11.1.0.0.

After you upgrade to 11.1.0.0, the logstash files are not updated in Logstash output configuration file

Tracking Number: ASOC-49843

Problem: When you upgrade from 10.6.5 to 11.1.0.0 or 11.0.0.x to 11.1.0.0, logstash files are not updated in the Logstash output configuration file. This happens when they have a global audit setup.

Workaround: If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click Save to apply the latest Audit log configuration.

Configure Feed data from Endpoint via recurring feed not working after upgrade

Tracking Number: ASOC-50601

Problem: After upgrade, the recurring feed configured from legacy NetWitness Endpoint does not work due to the change in Java version

Workaround: Import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store. For more information, see the 'Export the NetWitness Endpoint SSL Certificate' section in the *RSA NetWitness Endpoint Integration Guide*

Respond Notification Settings do not migrate from 10.6.5.x to 11.1

Tracking Number: ASOC-49390

Problem: The Incident Management notification settings in NetWitness Suite 10.6.5.x are different from the Respond notification settings available in 11.1, so your existing 10.6.5.x settings will not migrate to 11.1.

Workaround: Manually update the Respond Notification Settings in 11.1. To do this, go to CONFIGURE > Respond Notifications and set the notification settings. You will need to add the list of SOC Manager email addresses. See the “Configure Respond Email Notification Settings” procedure in the *NetWitness Respond Configuration Guide*.

Notification Servers from previous releases will not display in the Email Server drop-down list. The email servers settings must be edited and saved in the Global Notification Servers (ADMIN > System > Global Notifications > Server tab).

Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

To access these settings, you will need additional permissions. See “Respond Notification Settings Permissions” in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*

Unable to select Domain for Suspected C&C and Domain in the rule builder

Tracking Number: ASOC-46834

Problem: When adding a condition to an Incident Rule, there is no option to select **Domain for Suspected C&C** from the match conditions drop-down list. Also, after upgrade to 11.1, for some incident rules, the **Domain** and **Domain for Suspected C&C** fields are blank.

Workaround: Use **Domain** in the Match Conditions drop-down list for both **Domain** and **Domain for Suspected C&C**. Pre-upgrade, make note of the rules that contain the Domain and Domain for Suspected C&C match conditions including the operators and values. After upgrade, manually add the conditions to 11.1 using only **Domain** in the Match Conditions.

1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update.
2. In the **Match Conditions** section, select **Domain** in the drop-down list (instead of Domain for Suspected C&C) and enter the rest of the condition.
3. Enter the remaining information for your rule and click **Save**. For more information about incident rules, see the *NetWitness Respond Configuration Guide*.

Respond – Missing Group By field in Aggregate Alert will not fire

Tracking Number: ASOC-49820

Problem: In 10.6.5.x, you do not require incident rules to use the **Group By** field. If you have any rules that do not use the Group By field in 10.6.5, then after upgrade you will need to manually add a value to the Group By field as it is a required field in 11.1. Without a Group By field value, the rules will not work and they will not create incidents.

Workaround: Add a Group By field value to the rules that do not use the Group By field. For each incident rule:

1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update.
2. In the **Group By** field, verify that a Group By value is selected. If not, select a Group By value.
3. Click **Save** to update the rule.

For more information about incident rules, see the *NetWitness Respond Configuration Guide*.

Aggregation Stops after Reconnection to Mongo.

Tracking Number: ASOC-50911

Problem: After configuring the Mongo database and rebooting the ESA server, incidents are not being created. The ESA primary server acts the database host for NetWitness Respond application data. The NetWitness Server acts as the database host for NetWitness Respond control data. After the application database is configured on the ESA server and restarted, you must also restart the Respond service on the NetWitness Server..

Workaround: After configuring the Mongo database and rebooting the ESA server, restart the respond-server service..

From the command line:

```
systemctl restart rsa-nw-respond-server
```

Or from NetWitness suite:

Go to **ADMIN** > **services**, select the Respond Server service, and then select > Restart.

FIPS is disabled by default for the Log Collector Service

Tracking Number: ASOC-41841

Problem: FIPS is disabled by default for the Log Collector service, even if FIPS was enabled in 10.6.5.x.

Note: Even if FIPS is enabled in 10.6.5.x, it becomes disabled post-migration.

Workaround: To enable FIPS on the Log collector service, perform the following steps:

1. Stop the Log Collector service.
2. Open the `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` file.
3. Change the value of the following variable to **off** as described here:

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```
   to
   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```
4. Reload the system daemon by running `systemctl daemon-reload` command.
5. Restart the Log Collector service.
6. Set the FIPS mode for the Log Collector service on the UI:

   Note: This step is not required in case of upgrade, if FIPS was enabled on 10.6.5.x.

   a. Go to ADMIN > Services.

   b. Select the Log Collector service and go to View > Config.

   c. In SSL FIPS Mode, select the checkbox under Config Value and click **Apply**.

   Note: To enable Log Decoder and Packet Decoder, in `/sys/config` set `ssl.fips` to ON and restart the service.

The investigation links are disabled for static charts during 10.6.5.x to 11.1 post-upgrade

Tracking Number: ASOC-42136

Problem: The investigation link is disabled for the static chart (the result of the report is in chart format) which has the datasource as NetWitness Suite-Broker (This service is available by default).

Workaround: There are two workarounds for this issue:

- The rules that have the result in a static chart can be viewed in Tabular format and the investigation works as expected.
- Or you can perform the following steps to fix the issue:
  1. Delete and add the NetWitness Suite-Broker again as the datasource to Reporting Engine with the same name.
  2. If the reports with a static chart are scheduled reports, then in the next run, the investigation link will work as expected.
  3. If the report is an Adhoc report, then re-run the report for getting the investigation links.

Post upgrade from 10.6.5.x to 11.1.0.0, Warehouse Connector is not installed on Decoders

Problem: The Warehouse Connector is not installed on the Decoders by default.

Workaround: If, after an upgrade there is a need to re-establish a Warehouse connection, a utility is provided to reinstall the service. The utility is deployed during the bootstrap phase. To install Warehouse Connector, you must run the following command and specify the host by ID (--host-id), name (--host-name), or address (--host-addr). The latest available version will be installed by default unless a specific version is specified with --version. To install the Warehouse Connector on a host, run the following command on the Admin server:

[root]warehouse-installer --host-id <*uuid of the host*>

Details about the command:

Location: /usr/bin

Utility Name: warehouse-installer

Usage:

[root@nw11pds5 bin]# warehouse-installer --help

Warehouse Connector Installer

warehouse-installer [options]

Install options:

--host-id <id> Specify host to install (by ID)

--host-name <name> Specify host to install (by name)

--host-addr <address> Specify host to install (by address)

--version <#.#.#.#> Install version (defaults to latest)

General options:

-v, --verbose Enable verbose output

Post upgrade from 10.6.5.x to 11.0.0.x, duplicate dashboards for threat indicators.

Tracking Number: ASOC-41701

Problem: The dashboard, Threat–Indicators, was updated to report against new Hunting meta keys and renamed to Threat–Malware Indicators. On upgrade, both will appear in the UI instead of the old being replaced.

Workaround: Enable the Threat–Malware Indicators report charts and dashboard and disable the old Threat–Indicators dashboard.

On upgrade, the Health and Wellness custom policies for Context Hub Server are not available.

Tracking Number: ASOC-41826

Problem: When you upgrade to Netwitness Suite 11.1.0.0, the Health and Wellness custom policies configured for 10.6.5.x Context Hub server will not be available.

Workaround: You must define these custom policies in 11.0.0.x.

On upgrade to 11.0.0.x, collections created from a 10.4 or later Workbench display blank Date Range and Date Created values

Tracking Number: ASOC-9035

Problem: Any collections created from a 10.4 or later Workbench displays blank Date Range and Date Created values after upgrading to 11.0.0.x.

Workaround: None.

On upgrade from 10.6.5.x to 11.1, the Geo-map dashlet cannot be created using a pre-configured (OOTB) chart.

Tracking Number: ASOC-41896

Problem: When you upgrade to Netwitness Suite 11.1.0.0, the Geo-map dashlet cannot be created using a preconfigured chart. This happens if a custom dashboard uses a Geo-map dashlet, which is created using a preconfigured chart.

Workaround: The data source must be manually updated for that preconfigured chart that is required to be used in the dashlet with Geo-map. Or, create a new chart using the same preconfigured rule and use the new chart in the dashlet with Geo-map.

On upgrade from 11.0 to 11.1, if you have been using the Entropy Parser and indexing payload, you will need to add the bucket flag to the index file so that the Entropy Parser can use index buckets.

Tracking Number: ASOC-45721

Problem: When you upgrade to Netwitness Suite 11.1.0.0, if you have been using the Entropy Parser on the Decoder (packets only) and are indexing payload, you must add the bucket flag to your index file to take advantage of the new index buckets feature.

Workaround: Add bucket flag to index file so Entropy Parser can use index buckets, as follows:

1. In the NetWitness Suite menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each Concentrator service that is aggregating traffic from the decoders.
3. Under (actions), select **View** > **Config** and select the **Files** tab.

4. Select the `index-concentrator.xml file` and set the `bucket` flag to `true` for `payload.req` and `payload.res`. For example:

```
<key description="Payload Size Request" format="UInt 32"
level="IndexNone" bucket="true" name="payload.req"
valueMax="500000"/>

<key description="Payload Size Response" format=UInt32"
level="IndexNone" bucket="true" name="payload.res"
valueMaz="500000"/>
```

5. Click Apply.
6. For changes in the `index-concentrator.xml` file to take effect, you must restart the jetty service on the NW Server:
   `systemctl restart jetty.service`

On upgrade from 11.0 to 11.1, if your `Entropy=log2` flag was set to false, NetWitness resets the flag to true.

Tracking Number: ASOC-49115

Problem: When you upgrade to NetWitness Suite 11.1.0.0, if your `Entropy=log2` flag was set to false (`Entropy="log2=false"`), NetWitness resets this flag to true (`Entropy="log2=false"`) after you upgrade to 11.1 to align for all sources to include packets and NetWitness Endpoint Insights.

Workaround: If desired, you can set the flag back to false to retain the log10 calculation: `Entropy="log2=false"`

Context Hub

Workaround: You should add only those entries in the .csv file which they wish to append to the existing .csv file. If, you do not want to append any entries to the list then perform one of the options, as applicable:

OutOfMemory Error in the Context Hub service when large number of TAXII feeds are configured

Tracking Number: ASOC-41664, ASOC-42002

Problem: The Context Hub service runs into OutOfMemoryError and becomes unresponsive, if a large number of TAXII feeds are configured to fetch data.

Workaround: Restart the Context Hub service and make sure that the time range you select to fetch TAXII feeds from the TAXII server is not more than 6 months. If the issue persists even after updating the time range, see the Troubleshooting topic in the *Live Services Management Guide*.

Single-column and multi-column lists added from the Data Source tab are not supported for Add to a list and Remove from list.

Tracking Number: ASOC-37998

Problem: When you do a lookup on a specific context meta in the Investigation, Events, or Respond view, the list names displayed are the ones which have matching values.

When you right-click on a specific meta value and select the Add or Remove list option, the single-column and multi-column list names added from the data source tab will not be displayed. It will only display the lists added from the UI using the Lists tab.

Workaround: You need to manually add the values that were added from the Data Source tab to the specific CSV file. So that, next time when the scheduler runs, the values from the updated CSV file will be available in the specific lists.

Empty list is imported when list has values with missing quotes

Tracking Number: ASOC-34187

Problem: When you import a list with missing quotes such as “172.16.0.0, the list is saved without any data. This is because of the Apache bug (CSV-141), which does not parse the CSV file with incorrect format.

Workaround: Import a list with correct quotes. For example, “172.16.0.0”, “host.mycompany.com” and so on.

SSL handshake with RSA Archer certificate fails while adding it as a data source

Tracking Number: ASOC-32654

Problem: When you try to add RSA Archer as a data source using valid credentials, the test connection fails (ARCHER-37085). This happens when the 'Trust all Certificates' option is unchecked and you try to upload an RSA Archer trust certificate.

Workaround: Select the ‘Trust All Certificates’ checkbox and do not upload a certificate.

General Application Issues

The System Logs Off Idle Users in Respond and Some Investigate Views

Tracking Number: ASOC-46483

Problem: In the Respond view and some Investigate views (Event Analysis, Hosts, and Files), if a user is not actively querying data, the system logs off the user after the Idle Period is reached. The default Idle Period is 600 seconds (10 minutes). This can cause the work of an Analyst to be interrupted.

Workaround: If this becomes an issue with the Analysts, in the global security settings (ADMIN > Security), consider increasing the values of the **Session Timeout** and the **Idle Period**.

Endpoint

Unable to export files list to a CSV file

Tracking Number: ASOC-47549

Problem: While exporting data to a CSV file, database query takes a longer time when the database is under heavy load, and the UI request times-out.

Workaround: Apply appropriate filters and use at least one indexed field with an **Equals** operator to reduce the files for export. For more information on Filtering Hosts and Files, see *NetWitness Investigate User Guide*.

Sorting on Agent Scan Status and Agent Last Seen fields are not accurate

Tracking Number: ASOC-50057

Problem: In the **Investigate > Hosts** view, sorting on Agent Scan Status and Agent Last Seen fields do not display the correct order.

Workaround: None

Unable to generate Agent Packager if the auto uninstall is set in seconds

Tracking Number: ASOC-49324

Problem: In the **Auto Uninstall** field, if the seconds value is more than 9, for example, 02/12/2018 12:00:**10** PM, then click **Generate Agent** fails to generate the packager.

Workaround: Enter a value below 10 seconds in the Auto Uninstall field.

Sorting on columns should not be case-sensitive

Tracking Number: ASOC-32595

Problem: Sorting on columns in the Hosts and Files view is case-sensitive. It sorts the number first, uppercase, and then the lowercase.

Workaround: None.

No message is displayed when filtering the values takes more than 60 seconds.

Tracking Number: ASOC-50197

Problem: In the Hosts and Files view, while filtering the values, if it takes more than 60 seconds, the UI does not display any message or results.

Workaround: None.

*Generate and copy *nwelcfg file, does not update the timestamp*

Tracking Number: ASOC-49847

Problem: After installing the Endpoint Insights Agent, if the Administrator wants to update a new Log Collection configuration and the endpoint agent

After installing the Endpoint agent, if the administrator wants to update a new Log collection config via any of the copy methods or third party endpoint management tool, the config file timestamp remains as that of the Endpoint server time and not the agent time. As a result, if the endpoint agent is on a different timezone from the endpoint server, the timestamp does not get updated properly.

.**Workaround**: After copying the file, run the command on the Endpoint Agent: `copy /b <filename.nwelcfg> +,,` from the folder %programdata%\NWEAgent\ where the nwelcfg file is there.

Disable log collection in Windows Endpoint Agent is not supported

Tracking Number: ASOC-49846

Problem: Once an Endpoint Agent is installed with the windows log collection feature enabled, the user is unable to disable windows log collection.

Workaround: Run the uninstall command provided in the "Uninstall Agents" section in the *Endpoint Agent Install guide*. Reinstall an agent with windows log collection disabled.

Endpoint Agent - Account for Unresponsive UDP

Tracking Number: ASOC-40844

Problem: When the Primary Log Decoder/Remote Log Collector is not reachable and the Endpoint agent is configured to use UDP, the Secondary Log Decoder/Remote Log Collector is not used - this can lead to event loss.

Workaround: None.

Secondary LD/VLC cannot be unselected

Tracking Number: ASOC-48755

Problem: When an option is selected in the secondary channel for LD/VLC, then it cannot be unselected.

Workaround: Primary LD/VLC is a required field and it always needs a destination. Secondary option is an optional field. You can click **Reset** in the Packager UI and start again or refresh the page.

Respond

Related Links URL created for Malware Events is invalid

Tracking Number: ASOC-48392

Problem: In the Respond Alert Details and Incident Details views, the URL link for a Malware Analysis alert is invalid. To view the URL link in the Alert Details view, go to RESPOND > Alerts and in the Alerts list, click the link in the NAME column for a Malware Analysis alert. In the Event Details, you can see the URL for the Malware Analysis alert.

To view the URL link in the Incident Details view, go to RESPOND > Incidents and in the Incidents list, click the link in the ID or NAME column for a Malware Analysis incident. In the Incident Details view, click the View Datasheet icon ( ) to view the event details. If there are multiple events listed, click an event to view the event details. In the Event Details, you can see the URL for the Malware Analysis alert.

Workaround: None

Overlapping Relationship Data in the Nodal Graph for Certain Data

Tracking Number: ASOC-48034

Problem: In the Respond Incident Details view nodal graph, when there are multiple relationships within an incident, the text can overlap on the arrows between the nodes, which is difficult to read. This issue appears in an incident when the source IP of the alert is also the destination IP of another alert and the destination IP of the first alert is the source IP of the second.

Workaround: None

Respond Administrator cannot query Investigate or view Live dashlets in the Dashboard

Tracking Number: ASOC-40749

Problem: The Respond_Administrator role does not have permission to query Investigate. This is necessary so that the Respond Administrator can pivot to Investigate or create incidents from events. The Respond_ Administrator Role also does not have the Live: Access Live Module permission, which is required to view Live dashlets in the dashboard.

Workaround:

1. Manually create the Respond_Administrator role on the Core services. To do this, go to ADMIN > Services, select a Core service, and then in the Actions drop-down list, select View > Security > Roles Tab. Click + to add the Respond_Administrator role. Add the following permissions to the Respond_ Administrator role:
   - sdk.content
   - sdk.meta
   - sdk.packets
   - storedproc.execute

Replicate the Respond_Administrator role to other Core services that may be used by the users.

2. In the ADMIN > Security > Role tab, add the Live: Access Live Module permission to the Respond_ Administrator role.

Malware event File name with Korean characters is not shown properly in the Respond view

Tracking Number: ASOC-40159

Problem: If there are Korean characters in an alert that is received from Malware Analysis, they will not be displayed correctly in the Respond view.

Workaround: None.

Unable to query domain in source/destination.device.geolocation

Tracking Number: ASOC-39938

Problem: Geo-location that comes from ESA Correlation Rules is not available in the Incident Details view Related Indicators panel. (To access the Related Indicators panel, Go to RESPOND > Incidents and in the Incidents List, click the ID or NAME link of the incident. In the Incident Details view toolbar, click the Journal, Task, and Related icon. The Journal is displayed on the right. Click the RELATED tab.)

Workaround: None. This is a new functionality, so it is just data that is not searchable.

Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is not valid in NetWitness Suite 11.1.0.0

Tracking Number: ASOC-41891

Problem: NetWitness Suite 11.1.0.0 will only work with NetWitness SecOps Manager 1.3.1.2. However, the Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is navigating to the legacy Security Analytics Incident Management page, which is not valid in NetWitness Suite 11.1.0.0.

Workaround: None.

ESA Rules with severity as High or Low are not populated in the RSA Archer UI

Tracking Number: ARCHER-47101

Problem: When ESA alerts with severity High or Low are forwarded to RSA Archer, the Security Alert Priority field is not populated in the RSA Archer UI.

Workaround: None.

ESA Command and Control Aggregate Scores details are not populated in the RSA Archer UI.

Tracking Number: ASOC-50183

Problem: When ESA Command and Control Aggregate Scores details are forwarded from NetWitness Suite to RSA Archer UI, fields such as Beaconing Behavior, Rare Domains, Rare User Agents, Missing Referrers, and Suspicious Domains Aggregate Score do not get populated.

Workaround: None.

Incidents and Tasks are still available when RSA NetWitness SecOps Manager integration is enabled

Tracking Number: ASOC-39886

Problem: After enabling NetWitness SecOps Manager integration in the Respond Server service, all incidents are managed in NetWitness SecOps Manager. In previous versions, when SecOps was enabled, incidents and remediation tasks were hidden. In NetWitness Suite 11.0.0.x, users are still able to access incidents and tasks in the Respond view (RESPOND > Incidents and RESPOND > Tasks). They are also not prevented from creating incidents in NetWitness Suite. If they create incidents from the Respond Alert List view (RESPOND > Alerts) or from Investigate, those incidents will not go to NetWitness SecOps Manager.

Workaround: If you enabled SecOps Manager integration in the Respond Server service, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Also, do not create incidents from the Respond Alerts List view or from Investigate.

For migrated incidents, the event count always shows as 0 in the Overview panel

Tracking Number: ASOC-38026

Problem: In the Incidents Overview panel Catalysts field, the number of events for migrated incidents always shows as 0 (zero). This is expected behavior in NetWitness Suite 11.0.0.x (To access the Overview panel, go to Respond > Incidents. If you click an incident in the Incidents List, the Overview panel appears to the right. If you click a link in the ID or NAME field in the Incidents List, the Incident Details view opens with the Overview panel on the left.)

Workaround: None.

Unable to Pivot to Investigate on all username, filename, and domain values when multiple values are present.

Tracking Number: ASOC-37997

Problem: If username fields contain commas that do not represent delimiters between values, you may not be able to pivot to Investigate on certain meta if there is more than one value in the field.

Workaround: You can query or pivot on other data, or manually investigate the meta. You can still access the meta through Investigate.

In memory table enrichment info is not displayed for ESA alerts

Tracking Number: ASOC-37533

Problem: You cannot view custom enrichments for ESA Correlation Rules in the Respond Alerts view.

Workaround: None.

DOMAIN and HOST metas do not display correctly in the Respond view

Tracking Number: ASOC-37232

Problem: Domain and Host metas may be incorrectly labeled in the Respond Incidents Details view when alias.host contains different types of data. The Domain field behavior is inconsistent and it may be populated with hostnames.

Workaround: None. Multiple types of information will continue to exist in the Domain field.

After upgrade, unable to filter incidents using the Assignee field

Tracking Number: ASOC-36973

Problem: After upgrading incidents from 10.6.5.x to 11.0.0.x, Analysts are not able to filter the migrated incidents using the Assignee field (RESPOND > Incidents - Filter panel).

Workaround: None.

Respond - Create Incidents from Alerts in the Respond Alert List view

Tracking Number: ASOC-35811

Problem: When you manually create an incident from alerts in the Respond Alert List view (RESPOND > Alerts) in 11.0.0.x, you just have the minimum functionality to create an incident from alerts. You can only provide a name for the incident and the priority defaults to Low. When manually creating an incident, you do not have additional options, such as adding a Priority, Assignee, or Category.

Workaround: You can update additional fields by manually editing the incident after you create it, such as changing the priority from Low to High. However, you cannot add a category to an incident.

Whitelist Domains while closing Incidents as False Positive

Tracking Number: ASOC-25135

Problem: In 10.6.5.x, if a Suspected C&C Incident was marked as "Closed - False Positive" , an entry was made to the "Whitelisted Domains" list from context hub. There should be a similar functionality in the Respond view.

Workaround: Analysts can manually add domains to a whitelist in the Respond view. The *NetWitness Respond User Guide* provides procedures.

Integration Settings for SecOps Manager should be exposed in the User Interface

Tracking Number: ASOC-25127

Problem: The Integration settings for sending all incidents to RSA NetWitness SecOps Manager should be exposed in the user interface.

Workaround: The user interface for partial RSA NetWitness SecOps Manager integration was removed in 11.0.0.x. Administrators can complete the integration from the Explorer view for the Respond Server service.

Incidents are not flagged when a user manually adds alerts to an existing incident.

Tracking Number: ASOC-16640

Problem: Investigation values are not highlighted when alerts in Respond have manually been added to an incident. Alerts that are dynamically added to an incident will get highlighted.

Workaround: None.

Log Collector

The vsftpd service has been changed to support only TLSv1.2

Tracking Number: ASOC-42497

Problem: For compliance reasons, the **vsftpd** service configuration on Log Collector and Virtual Log Collector nodes has been changed to support only TLSv1.2 and high encryption ciphers. TLSv1.0, 3DES and NULL encryption will no longer be accepted by default. This will break uploading of log files by FTPS protocol from event sources that do not support higher encryption.

Workaround: Use the following procedures to restore collection.

If you have event sources requiring TLSv1.0, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_tlsv1=NO` to `ssl_tlsv1=YES`
2. Restart **vsftpd** service by running this command:

   ```
   systemctl restart vsftpd
   ```

If you have event sources requiring 3DES and/or NULL encryption, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_ciphers=HIGH:-3DES:-aNULL` to `ssl_ciphers=HIGH`
2. Restart **vsftpd** service by running this command:

   ```
   systemctl restart vsftpd
   ```

DPO Role missing on Log Collector

Tracking Number: ASOC-7937

Problem: The new Data Privacy Officer role does not exist on the Log Collector.

Workaround: None.

Checkpoint collection not working with error "peer ended the session"

Tracking Number: ASOC-8351

Problem: The checkpoint collection is not working and the logs show the error: **peer ended the session**

Workaround: To resolve this issue:

1. Make a backup and then remove the checkpoint position file (**/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_Security.xml**).
2. Restart the service to regenerate the file.
3. (Optional) If the **Max Idle Time Poll** is set to 0, set it to 20.

Note: By removing the position file, your Log Collector may re-collect a substantial amount of log data.

Investigate

Three new meta groups for 11.0 and the same column groups for 11.1 are not created when you upgrade from 10.6.5 to 11.x: RSA Endpoint Analysis, RSA Outbound HTTP, RSA Outbound SSL/TLS.

Tracking Number: ASOC-51011

Problem: When you upgrade from Version 10.6.5 to 11.x, three out-of-the-box meta groups (RSA Endpoint Analysis, RSA Outbound HTTP, and RSA Outbound SSL/TLS) are not created due to a conflict with a column group added in Version 11.0. When you upgrade from Version 10.6.5 to 11.1, three out-of-the-box column groups (RSA Endpoint Analysis, RSA Outbound HTTP, and RSA Outbound SSL/TLS) are not created. These meta groups should appear in the Manage Meta Groups dialog and the Manage Column Groups dialog.

Workaround: None.

After upgrading to 11.1, there are mismatched data types between the Log Decoder (table-map.xml) and Concentrator (index-concentrator.xml) definitions.

Tracking Number: ASOC-50702

Problem: This error occurs when you have done customized meta keys on your Log Decoder and Concentrator.

Workaround: If you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have those same fields indexed on the Concentrator, then you must change data type of these fields to IPv4 on both the Log Decoder and Concentrator.

If the URL for a drill point is very long and you use the query in the Event Analysis view, an error (414 Request error) is returned.

Tracking Number: ASOC-50196

Problem: Several situations create a very long query that the browser cannot handle, especially if you are using Internet Explorer, which has a much lower character limit than most browsers. Pivoting to Event Analysis from Reporting can result in a very long query, and a number of pivots in the Navigate view can create a very long query.

Workaround: Continue to work in the Navigate view or Events view when the URL becomes too long to render in the Event Analysis view.

Attempting a direct query, or query via link, that uses an IPV6 meta value with unsupported special characters generates an error in the Event Analysis view and the Navigate view.

Tracking Number: ASOC-50924

Problem: Literal ipv6 addresses with a percent (%) sign and also UNC Path Names such as 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net are not supported. The error in the Event Analysis view is Internal Server Error. The Navigate page shows a syntax error.

Workaround: None.

If you got to Event Analysis by way of the Events view, either by clicking the Event Analysis link or by right-clicking one of the events, the right-click options on meta values do not work.

Tracking Number: ASOC-50771

Problem: If you clicked Event Analysis in the Detail View of the Events view, the Event Analysis view opens as usual. However, the right-click options on a meta value in the Event Meta panel do not work.

Workaround: If you go through **Navigate** > **Event Analysis**, or if you go through Events and a reconstruction of an event, the right-click options function in Event Analysis.

The service keeps loading infinitely.

Tracking Number: ASOC-49854

Problem: This sometimes occurs when you open Event Analysis from the Navigate view or the Event view, and when you refresh the Event Analysis view.

Workaround: Refresh the page in the browser.

Cannot add meta entities to a custom column group in the Events view with the Optimize Investigation Page Loads option disabled.

Tracking Number: ASOC-50712

Problem: Meta keys belonging to meta entities are not displayed in custom column groups. This issue is seen in the Events view when you disable Optimize Investigate Page Loads in the Events view settings and then refresh the page.

Workaround: If you want to use meta entities in a custom column group, ensure that the Optimize Investigation Page Loads option is enabled.

Custom column groups that contain meta entities can be created in the Events view, but when the custom column group is used in the Event Analysis view, you cannot see the meta keys included in the meta entity in the results.

Tracking Number: ASOC-50349

Problem: Custom column groups are not displaying meta keys that belong to meta entities. This issue is seen in the Events list in the Event Analysis view.

Workaround: Use a column group that does not contain meta entities. However, meta entities can still be queried and used in the query builder.

When downloaded from the Event Reconstruction view, logs and metadata are always in text format irrespective of the format selected in the Events view.

Tracking Number: ASOC-50091

Problem: When you download metadata or a log in the Event Reconstruction view, the format that you selected in the Events view is not used. The exported data is always in text format.

Workaround: Download metadata and logs from the Events view if you want to use a format other than text format.

When you right-click on a meta value that contains a semicolon in the Event Analysis view and attempt to apply the drill in a new tab in the Navigate view, there is an error: Unable to build visualization

Tracking Number: ASOC-50041

Problem: The URL is correctly formed in the Event Analysis view, but when received in the Navigate view, only the part of the string before semicolon is queried, and everything after it is stripped off.

Workaround: Enter the query, complete with the semicolon, directly in the Query dialog in the Navigate view or Events view.

The query builder in the Event Analysis view is unresponsive for filters that contain a space.

Tracking Number: ASOC-49427

Problem: When adding a filter, if you add an extra space before <meta key>, between <meta key> and <operator>, and after <operator>, the query builder becomes unresponsive and the Query Events button is disabled so that you cannot continue adding filters.

Workaround: Click on an existing filter, and then click the query builder. If that does not work, refresh the page.

When you alter the URL and the new URL is for a restricted event, the reconstructed content for the previous query persists in the Event Analysis view and no error message is displayed.

Tracking Number: ASOC-45198

Problem: After viewing an event that you have access to, if you change the URL to an event you are restricted from viewing the content of the previous event is still displayed.

Workaround: None.

When you enter a query to a session to which you do not have access in the Event Analysis view, no data is displayed and there is no error message.

Tracking Number: ASOC-48945

Problem: If you enter a query in the Event Analysis view query builder that would result in viewing an event you are restricted from viewing, no data is displayed and there is no error message.

Workaround: You can check the URL in the Navigate view (**Navigate** > **Actions** > **Go to event in Event Analysis**), and the following message will be displayed: "Session is unavailable for viewing.".

When investigating in the Event Analysis view, the following error message is returned: "An Unexpected error has occurred."

Tracking Number: ASOC-48710

Problem: This error is displayed when the session you are attempting to access has been removed, rolled out, or you have insufficient permission to view the session.

Workaround: None.

In a mixed-mode environment, an analyst with insufficient permissions can download PCAPs and logs from a 10.6.5.x service in the Investigate > Event Analysis View, but not files or payloads.

Tracking Number: ASOC-49676, 41698

Problem: Role-Based Access Control (RBAC) on the 11.0.0.x and 11.1 NW Server is not applied uniformly to downloads when investigating 10.6.5.x services. If the sdk.packets setting has not been disabled, analysts with SDK Meta and roles permission in place to restrict viewing and reconstructing event content can download the PCAP and log of an event that has content restrictions. Other types of downloads appear to download, then generate errors due to insufficient permissions, and the data is still protected.

Workaround: Disable the sdk.packets setting on 10.6.5.x services to limit the analyst from downloading any PCAPs or logs during phased upgrade. When the upgrade of all services is complete, re-enable the sdk.packets setting in all services. The RBAC experience will be consistent across all services. See the "UpgradeTasks" section in the *Physical Host Upgrade Guide* for details.

Issue with Interaction between Expand and Contract Icons in Investigate Event Analysis.

Tracking Number: ASOC-47670

Problem: When you contract the left panel in the Event Analysis view, the right panel expands, but the expand/contract icon on right panel does not change to the contract icon. To contract the right panel using the expand/contract icon on the right panel you have to press it twice. The behavior should be that when you contract the left panel and the right panel expands, the expand/contract icon for right panel switches to contract and vise versa. There is a similar issue with the Show/Hide Events panel icon. If the Event panel is contracted and you click on the Show/Hide Events Panel icon, the left panel disappears and the right panel expands. The expand/contract icon on the right (and now only) panel remains in expanded form. When you click on the expand icon in this configuration, the left panel reappears and the right panel effectively contracts.The behavior should be: after you hide the left panel, the expand/contract icon on the right panel should take its contract form.

Workaround: When the expand/contract icon in the right panel or the Show/Hide Events panel icon in the toolbar has not changed to the correct state, click the icon twice.

PCAP and payload download issues in Event Analysis view in a Mixed Mode Environment

Tracking Number: ASOC-37309

Problem: The Event Analysis workflow requires all services to be running 11.0.0.x. If the NW Server, Broker, and Concentrator are running 11.0.0.x, and the Decoders are running 10.6.5.x, the admin user will not be able to download files, logs, PCAPs, and payloads.

Workaround: Download files from Event Reconstruction.

Parallel Coordinate visualization is not displaying special characters correctly

Tracking Number: ASOC-9346

Problem: When configuring the meta key content type as one of the meta for the axis, if the meta value contains any special characters, the values do not display correctly.

Workaround: None.

Workbench

Empty collection seen in Collections tab

Tracking Number: ASOC-6859

Problem: An empty collection is seen in the Collections tab if the workbench service stops or restarts during restoration process

Workaround: None.

Data range is not displayed for collection if workbench service or Jettysrv is restarted while restoration is in process

Tracking Number: ASOC-6822

Problem: The date range is not displayed for a collection if the workbench service or Jettysrv is restarted while the restoration is in process.

Workaround: None.

Custom Feeds

RSA Archer Recurring Feeds failing in SSL mode

Tracking Number: ARCHER-41524

Problem: RSA Archer recurring feeds does not work in SSL mode.

Workaround: You must create the RSA Archer recurring feeds in non-SSL mode..

The status of STIX feed progress bar is incomplete.

Tracking Number: ASOC-40642

Problem: Sometimes, the status of the progress bar for some of the STIX feeds are incomplete even if the feeds are successfully pushed to the Decoder(s).

Workaround: None.

Malware Analysis

Users with Analyst role are not able to run the on-demand malware scan

Tracking Number: ASOC-5425

Problem: A user who has the Analyst role has access to the Investigation and Malware Analysis modules. But when the user tries to run the on-demand Malware Analysis scan from the Investigation screen, it fails with an invalid username error. The job gets submitted but fails because of the credentials.

Workaround: None.

If the Core device is not configured with IP address, the View Network Session option is disabled for Malware Analysis events

Tracking Number: ASOC-5571

Problem: Due to the new service ID and changes to the ASG, Malware Analysis is not showing the View Network Session option from the Malware Event Summary. It looks like the device ID is coming as null.

Workaround: None.

Event Stream Analysis

ESA Rules deployed not listed while creating policy using statistics ESA Rule Memory Usage

Tracking Number: ASOC-50201

Problem: When you deploy new ESA rules in the Health and Wellness page and create a new policy under Event Stream Analytics using the statistic ESA Rule Memory usage, all ESA rules deployed are not listed.

Workaround: Run the following restart command on NetWitness Server: `systemctl restart rsa-sms`.

Unable to deploy ESA rule with array meta in Enrichment

Tracking Number: ASOC-47584

Problem: If a user configures an In-Memory table as an Enrichment Source in ESA where a table column has type as string, creates an ESA rule with a whitelist condition, and maps the string list column to a string array event meta key, when the rule is deployed, the rule is disabled as the datatype conversion from String[] to String is not allowed.

Workaround: None.

For ESA rules that use enrichment sources, the Ignore Case option does not work for first statement

Tracking Number: ASOC-49906

Problem: When creating an ESA rule that uses any enrichment source, if the Ignore Case option is enabled on the first enrichment statement, no results are returned. Note that this issue does not apply to any statements after the first statement (that is, substatements).

Workaround: When creating a new rule, the Ignore Case option is now disabled. For existing rules that have the Ignore Case option enabled for an enrichment statement, the option is still enabled but users will be prompted to disable the option when opening the rule in ESA and then save the updated rule.

ESA rule with meta entity does not get triggered

Tracking Number: ASOC-47522

Problem: When meta entities are configured for use in the Investigate interface, they are not available for use in the ESA Correlation Rule Builder. Customers are not able to build ESA correlation rules using meta entity information, and they must specify the exact pieces of metadata to use in the rules.

Workaround: None

Deployment (called Synchronization in 10.4 and earlier) fails if you deploy this rule from RSA Live: No Log Traffic detected from device in given time frame

Tracking Number: SAENG-5888

Problem: Deployment, formerly called synchronization, fails for rule "No Log Traffic detected from device in given time frame" deployed from Live. This issue is not observed if you deploy the rules from Live on a 10.4 setup and do the synchronization. The issue is observed if you update your system from a pre-10.4 where the rules are deployed from Live with incorrect Module IDs.

Workaround: Delete the rules with incorrect Module IDs and redeploy them from Live.

Case-sensitive sorting is not working properly in ESA All Rules grid

Tracking Number: SAENG-3605

Problem: When rule names begin with lower and upper case letters, the sort does not work properly in the Rule Name column of ESA All Rules grid. For example, "Rule 1" is not followed by "rule 2" when you sort by name.

Workaround: None.

Cannot set ESA compression level as in other appliances

Tracking Number: ASOC-26481

Problem: Administrators cannot set the compression level in ESA like they can with other appliances, even using the Explorer view.

Workaround: Delete the Concentrator source from ESA and add it again so that the compression level changes are reflected:

1. Remove the Concentrator data source from ESA. (Go to ADMIN > Services, select the Event Stream Analysis service, and from the actions menu select View > Config. On the Config view Data Sources tab, remove the Concentrator data source.)
2. Set compression level in ESA. (Go to the Explore view, and in the node list, navigate to Workflow/Source/nextgenAggregationSource and set the CompressionLevel.)
3. Add the Concentrator Data Source again to ESA. (Return to the Config view Data Sources tab and add the Concentrator data source.)

Event Stream Analysis service becomes unresponsive when using Query-based aggregation for automated threat detection for Logs

Tracking Number: ASOC-25174

Problem: Event Stream Analysis may become unresponsive due to heavy resource usage, and the configuration for the wrapper may need to be adjusted.

Workaround: You may need to change the ping time settings in the `wrapper.conf` file. Perform the following:

1. Go to **Administration > Services > Event Stream Analysis> Explorer** and navigate to the **`/opt/rsa/esa/conf/`**folder.
2. Change the settings to the following values:
   `wrapper.ping.timeout=300`
3. Add the following lines at the end of the file:
   ```
   wrapper.restart.delay=40
   wrapper.ping.timeout.action=RESTART
   ```
4. Restart the Event Stream Analysis service.

ESA Displays Warning For Array Operators

Tracking number: ASOC-14157

Problem: When writing an advanced rule, array operators, such as anyOf, fails. For example:

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

results in an error similar to the following:

```
Logger name: com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class java.util.Vector
```

Workaround: To do a fuzzy comparison, first convert the array to a string. For example:

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

> **Note:** If you used array operators in EPL developed in versions 10.5, 10.5.0.1, and 10.6, you will need to modify the EPL to use the above workaround.

Deployment fails if the server that hosts an external database goes down

Tracking Number: ASOC-9011

Problem: You configure a database connection to use the database as an enrichment source for a rule. A reference to the database is deployed on every ESA, even if the ESA does not deploy any rules that use the database. If the server that hosts the database goes down, any new deployment will fail.

Workaround: Restart the server that hosts the database.

Trial rules configuration: Out-of-Bound Values are Capped

Tracking Number: ASOC-6633

Problem: When configuring parameters for trial rules, you can configure the following values:

- **MemoryCheckPeriod**: Defines the polling interval to check the ESA memory consumption.
- **MemoryThresholdForTrialRules**: Defines the threshold value; when reached, all trial rules will be disabled.

  If you configure these parameters with out-of-bound values, the values are capped to the system's minimum or maximum values rather than the values defined in the parameters.

Workaround: None.

Reporting

Post-upgrade from 10.6.5.x to 11.1, Categories meta for incident collection is not supported.

Tracking Number: ASOC-40851

Problem: When using the Categories meta for incident collection, the results rendered are in an incorrect format. Hence this meta is not supported and you cannot use the categories meta in either select clause or where clause. Also, it is not available in the list of metas for selection in the Rule Builder page.

Workaround: None.

Incorrect data displayed for Charts.

Tracking Number: ASOC-35523, ASOC-37958

Problem: When a chart is executed for defined time ranges, the results are inconsistent between test chart and a view chart.

Workaround: None.

When querying on the Respond DB, empty rows are displayed.

Tracking Number: ASOC-37846

Problem: When querying on the Respond DB, and if the data is not available for the requested columns, then empty rows are displayed on the UI.

Workaround: None.

Hide and Investigate options are not supported in Google Chrome and Mozilla Firefox browsers on Windows 10 operating system.

Tracking Number: ASOC-37590

Problem: If you are using Chrome or Firefox browsers on a Windows 10 operating system, and click on a chart data point, the hide and investigate options are not displayed. However, these options are available using the Internet Explorer browser.

Workaround: Disable the touch feature on Chrome and Firefox browsers. To disable this option in Chrome use the following procedure:

1. Navigate to - chrome://flags/ on Chrome or Firefox Browser.
2. Select the "Disable" option for "Touch Events API" flag.
3. Relaunch the browser.

To disable this option in Firefox, use the following procedure:

1. Navigate to - "about:config".
2. Click on "I accept the risk".
3. Search for the "Preference Name" - "dom.w3c_touch_events.enabled".
4. Update the "Value" column to 0.
5. Relaunch the browser.

Administration

Audit Logs: SA_SERVER is not capturing the value for queryString

Tracking Number: ASOC-8994

Problem: When changing file contents of a NetWitness Suite service, the NetWitness Suite server audit logs do not indicate which file the user changed.

Workaround: None.

Password expiry email lacks source information

Tracking Number: ASOC-9187

Problem: The password expiry email sent by the NetWitness Suite server does not mention the name or URL of the NetWitness Suite server that sent the email. If there are multiple NetWitness Suite servers, you may not know where to go to update your password.

Workaround: None.

Audit logs do not report the page (name) accessed when user tries to access NetWitness Suite pages where the user does not have permissions

Event Source Management

Renaming the Log Collector or Log Decoder hostname is not reflected in Event Source Manage View

Tracking Number: ASOC-9235

Problem: On the **Administration > Host** page, if you edit the Log Collector or Log Decoder appliance "name," then the change will not be reflected on the **Administration > Event Sources > Manage** page in the Log Collector or Log Decoder columns.

Workaround: Once you update a name from the Host page, perform the following steps:

1. SSH to the NetWitness Suite appliance.
2. Restart the SMS service by running this command:

   ```
   systemctl restart rsa-sms
   ```

3. On the NetWitness Suite UI, wait for the **Event Source Manage** page to come back up, then delete the event sources with the old Log Collector or Log Decoder names.

Not all types are displayed for auto-mapped addresses.

Tracking Number: ASOC-48328

Problem: If a new application is added on an existing Event Source that is auto-mapped, there could be a delay in when that type shows in Event Source Discovery and is un-auto-mapped.

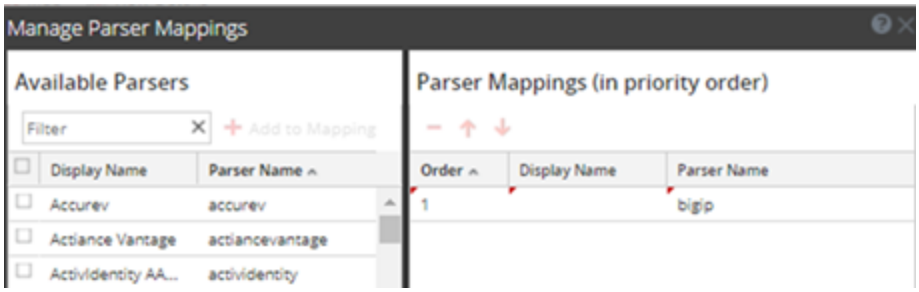
Workaround: None.

Suggested mappings do not load when the Event Source is created manually.

Tracking Number: ASOC-49492

Problem: For an Event Source that is manually added without entering a value for Log Decoder, when the **Manage Parser Mappings** dialog is opened, suggested Parser Mappings may not have a Display Name.

Workaround: Close the **Manage Parser Mappings** dialog, then reopen it and the Display Name is displayed as shown in the following example.



Core Services

The SSL FIPS Mode checkbox in the Services Config view should be disabled for Brokers, Concentrators, and Archivers, because changing the checkbox value does not turn off FIPS enforcement for the service.

Tracking Number: ASOC-41902

Problem: In 11.0.0.x, the Broker, Concentrator, and Archiver are always FIPS enforced and the administrator does not have the option to toggle between between FIPS and Non-FIPS. The admin can use the SSL FIPS Mode checkbox to toggle FIPS mode on and off on a Log Decoder, Packet Decoder, or Log Collector.

Workaround: None.

Broker System roles do not show the custom meta keys defined in Concentrator

Tracking Number: ASOC-6749

Problem: If any custom meta keys are defined, the same meta keys should show up in the Broker, too. But the Broker system roles are not showing the custom meta.

Workaround: You can copy the Concentrator Language file and the custom index file (if it exists) to the Broker to add the SDK meta key roles to the system roles.

Custom Feed configuration- Advanced Option XML file invalid error for multi metacallback.

Tracking Number: ASOC-40867

Problem: Netwitness Suite does not support uploading feeds for the xmls where there are more than one callback.

Workaround: The Adhoc Feed can be uploaded using NwConsole, or using the REST URL of the decoder directly. This is not applicable for Recurring Feed.

Ability to Create Source and Destination IP-Based Feeds Using CIDR or Range

Tracking Number: SATCE-628

Problem: When creating a source and destination-based feed on a Log Decoder, it only populates the source meta key. You cannot use a range-based or CIDR feed. You must list every single IP address.

Workaround: Create two different feeds using IP addresses and you can use CIDR in these feeds.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Suite 11.1.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Upgrade Instructions	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Upgrade Checklist	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Contacting Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Suite product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA SecurCare	https://knowledge.rsasecurity.com
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email	nwsupport@rsa.com
Community	https://community.rsa.com/docs/DOC-1294
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Revision History

Revision	Date	Description
1.0	7-Mar	Release Notes for RSA NetWitness Suite v11.1

RSA NETWITNESS® SUITE

RSA NetWitness Log Parser Tool Release Notes

for Version 1.0

RSA

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

Introduction **4**

Product Description 4

Product Documentation 5

Installation **6**

Installation Instructions for New Users 6

Installation Instructions for Beta Event Source Integrator Users 6

Product Features **7**

Easy Deployment of NetWitness Parsers 7

Generate Parsing Summary 7

Advanced Search on Parsers 7

Advanced Log Filtering 7

Undo and Redo Functions 7

Validation Checks for Headers and Messages 7

Direct Link to GitHub Community 8

Continuous Parsing and On-Demand Parsing 8

Auto Splitting of Large Log Files 8

Automatic Periodic Saving 8

Importing Table-Map and Table-Map-Custom Files 8

Graceful Error Handling 8

Advanced Tag-Value Functionality 9

Known Issues **10**

Product Feedback **12**

Preparing to Contact Customer Care 12

Revision History **13**

Introduction

This document describes RSA® NetWitness Log Parser Tool, Version 1.0. RSA recommends reading this document before installing and using the NetWitness Log Parser Tool.

This document contains the following sections.

- Product Documentation
- Installation
- Product Features
- Known Issues
- Product Feedback
- Revision History

Product Description

The RSA NetWitness Log Parser Tool (NwLPT) enables content users to build and modify NetWitness log parsers in an offline environment without affecting NetWitness. The Log Parser Tool enables analysts to create custom parsers for critical or custom sources in their environment that are not currently parsed in NetWitness.

The Log Parser Tool enables you to create custom parsers in less time with an easier to use user interface and an improved workflow over previous methods.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA® NetWitness Log Parser Tool User Guide 1.0	https://community.rsa.com/docs/DOC-85016

Installation

Installation Instructions for New Users

You can install the RSA NetWitness Log Parser Tool standalone on a Microsoft Windows or MacOS computer. Download the Windows and MacOS versions of the NetWitness Log Parser Tool from the following location and running the installer locally on your computer:

https://community.rsa.com/docs/DOC-85016

Installation Instructions for Beta Event Source Integrator Users

If you are a Beta Event Source Integrator user, you need to un-install the Event Source Integrator tool and download the new NetWitness Log Parser Tool installer from the following location:

https://community.rsa.com/docs/DOC-85016

Note: The Recent Parsers and Open Recent sections are empty, since this is a new installer.

Product Features

RSA NetWitness Log Parser Tool 1.0 includes the following features:

Easy Deployment of NetWitness Parsers

Using the NetWitness Log Parser Tool, you can deploy parsers on a single Log Decoder or multiple Log Decoders.

Generate Parsing Summary

You can generate a report on the parsing details of the parser and log file that you loaded. This report provides detailed information about the parsed messages and headers, as well as information about unused headers and messages and top 10 meta values.

Advanced Search on Parsers

The NetWitness Log Parser Tool supports advanced search options on the headers and messages sections.

Advanced Log Filtering

The NetWitness Log Parser Tool supports advanced search options on the logs section. The NetWitness Log Parser Tool allows you to filter for selected log values, HeaderIDs, MessageIDs, and regex patterns in the logs section.

Undo and Redo Functions

The Undo and Redo options allow you to undo and redo any number of commands while the parser is being built or updated.

Validation Checks for Headers and Messages

- Multiple validation checks have been added to ensure the parser follows the right syntax and best practices.
- For example, an empty Header ID is not allowed, only 1 MessageID allowed per Header definition, creation of messages is not allowed unless the MessageID and Payload are defined.

Direct Link to GitHub Community

The GitHub Community link provides access to a repository where you can share and contribute event source log parsers for the NetWitness Log Decoder.

Continuous Parsing and On-Demand Parsing

The NetWitness Log Parser tool features two parsing modes: Continuous Parse and On-Demand Parse.

- By default, the NetWitness Log Parser Tool uses Continuous Parse mode, which means the log file is reparsed whenever there is a change to the parser.
- On-demand parsing can be used to parse large log files exceeding 25 MB so that the parser does not attempt to parse the log file after every change.

Auto Splitting of Large Log Files

The Log File Auto Splitting option allows you to split the size of a log file that exceeds 25 MB.

Automatic Periodic Saving

All parsers opened in the tool are auto-saved to a temporary location at an interval of 30 seconds. The last saved time is displayed in the Status Bar at the bottom of the tool.

Importing Table-Map and Table-Map-Custom Files

Table-Map and Custom-Table-Map files can be uploaded to your environment using the NetWitness Log Parser Tool.

Graceful Error Handling

- Error and Exception handling added to multiple parts of the tool.
- Appropriate user readable error messages are displayed. For example, read-only files cannot be edited, you cannot open a non-compliant parser.

Advanced Tag-Value Functionality

The **<TAGVALMAP>** feature is an advanced feature that enables easy parsing of event logs using the **<TAGVAL>** format.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Description: Close icon is not visible in the Parser tab in MacOS.

Tracking Number: ASOC-45687

Workarounds: From the main menu, select **File > Close**.

The following shortcut can also be used to exit from the Parser tab:

- Windows: **CTRL+W**
- MacOS: **CMD+W**

Description: Header and Message section controls are draggable and movable in Windows 10.

Tracking Number: ASOC-45675

Workaround: None. Does not impact functionality.

Description: Tab cannot be directly typed as a TagVal delimiter in the tool.

Tracking Number: ASOC-45684

Workaround:

1. Type the tab spacing in a text editor such as Notepad**.**
2. Copy the tab spacing from Notepad and paste it in the **Delimiter** field under the **Parser Details > TagVal** section.

Description: Does not work on Windows Server 2008 VMs that do not have a video card backend.

Tracking Number: ASOC-23434

Workaround: None.

Description: Sometimes Payload Rewind rectangle periodically overlaps at the end of a header on MacOS.

Tracking Number: None.

Workaround: None. Does not impact functionality.

Description: Vertical scrolling of events in the Log Data section may not be smooth when you are using the Tools scroll bar.

Tracking Number: ASOC-17707

Workaround: Use your mouse to scroll in the Log Data section.

Description: *Invalid empty Header/Message node is created when Header or Message is deleted from the Detail View*.

Tracking Number: ASOC-32031

Workaround: This is a user interface issue only. Click on a different Header/Message, then click on the invalid Header/Message to get rid of the empty Header/Message node.

Description: Log Parser Tool dialog box text may overflow if the Display is set to Medium (125%) or Larger (150%) on a Windows System".

Tracking Number: None.

Workaround: Follow the steps below.

1. Click **Start** button in Windows.
2. Select **Control Panel**.
3. Click **Appearance and Personalization**.
4. Click on **Display**.
   A page opens that displays three radio buttons: **Smaller**, **Medium**, and **Larger**.
5. Select the **Smaller** radio button to reduce the size of the text and click **Apply**.
6. Restart your computer for the change to take effect.

Description: Advanced functions are not documented.

Tracking NumberASOC-17293

Workaround: None.

Description: All comments are removed from the parser.

Tracking Number: ASOC-31782

Workaround: None

Product Feedback

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com/
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email	support@rsa.com
Community	http://www.emc.com/security/security-analytics/security-analytics.htm
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Log Parser Tool you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
1.0	December 2017	Initial product release of the NetWitness Log Parser Tool.

RSA NETWITNESS® SUITE

Installation and Upgrade Guides

for Version 11.1.x.x

RSA NETWITNESS® SUITE

Physical Host Installation Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **4**

Supported Hardware 4

Physical Host Installation Workflow 4

Contact Customer Support 4

Installation Preparation - Open Firewall Ports **5**

Installation Tasks **6**

Task 1 - Install 11.1 on the NetWitness Server (NW Server) Host 6

Task 2 - Install 11.1 on Other Component Hosts 17

Update or Install Legacy Windows Collection **28**

Post Installation Tasks **29**

General 29

(Optional) Task 1 - Re-Configure DNS Servers Post 11.1 29

RSA NetWitness® Endpoint Insights 30

(Optional) Task 2 - Install Endpoint Hybrid or Endpoint Log Hybrid 30

Troubleshooting **32**

Command Line Interface (CLI) 32

Backup (nw-backup script) 34

Event Stream Analysis 36

Log Collector Service (nwlogcollector) 37

NW Server 39

Reporting Engine Service 39

Appendix B. Create an External Repository **40**

Revision History **42**

Introduction

The instructions in this guide apply to physical hosts exclusively. See the RSA *NetWitness Suite Virtual Host Installation Guide* for instructions on how to set up virtual hosts in 11.1.

Supported Hardware

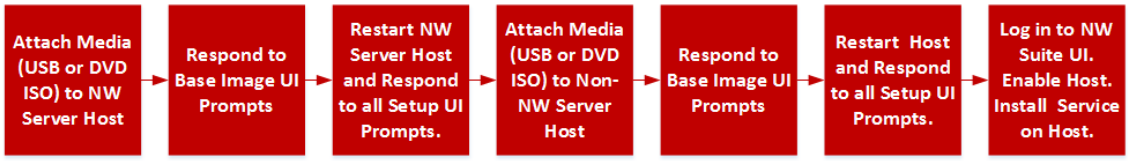
Series 4, Series 4S and Series 5.

Refer to the RSA *NetWitness Suite* Hardware Setup Guides for detailed information on each series type (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

Note: You must install the new Endpoint Hybrid or Endpoint Log Hybrid on the S5 or Dell R730 appliance. See "(Optional) Task 2 - Install Endpoint Hybrid or Endpoint Log Hybrid" in Post Installation Tasks for instructions on how to install Endpoint Hybrid and Endpoint Log Hybrid.

Physical Host Installation Workflow

The following diagram illustrates the RSA NetWitness® Suite 11.1 Physical Host Installation workflow.



Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Suite 11.1.

Installation Preparation - Open Firewall Ports

The"Network Architecture and Ports" topic in the *RSA NetWitness® Suite Deployment Guide* lists all the ports in a deployment. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Caution: Do not proceed with the installation until the ports on your firewall are configured.

Installation Tasks

This topic contains the tasks you must complete to install NetWitness Suite 11.1 on physical hosts.

There are two main tasks that you must complete in the order shown.

Task 1 - Install 11.1 on the NetWitness Server (NW Server) Host

Task 2 - Install 11.1 on All Other Component Hosts

Task 1 - Install 11.1 on the NetWitness Server (NW Server) Host

For the NW Server, this task:

- Creates a base image.
- Sets up the 11.1 NW Server host.

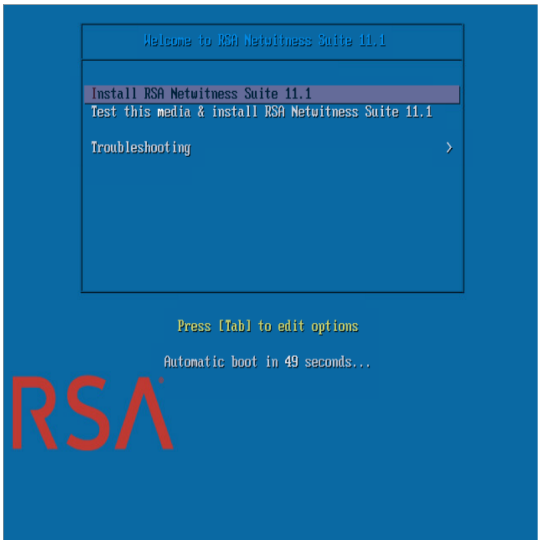
Complete the following steps to install the 11.1 NW Server host.

1. Create a base image on the host.
   a. Attach media (ISO) to the host.
      See the *RSA NetWitness Suite Build Stick Instructions* for more information.
      - Hypervisor installations - use the ISO image.
      - Physical media - use the ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the ISO. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO file.
   b. Log in to the host and reboot it.

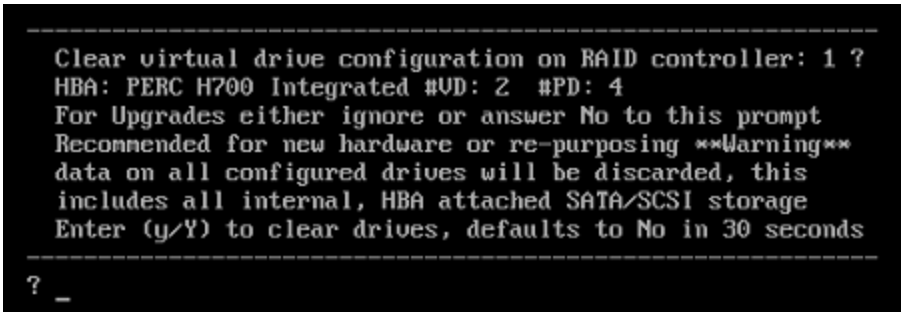
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   c. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media.
      After some system checks during booting, the following **Welcome to RSA NetWitness**

Suite 11.1 installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

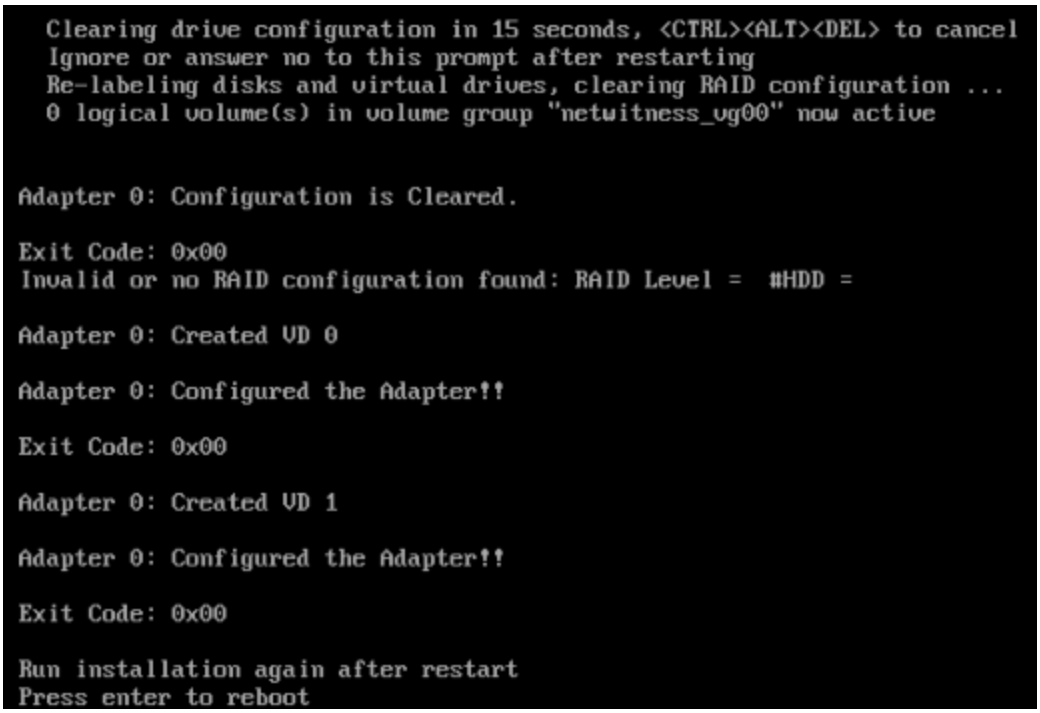


d. Select **Install RSA Netwitness Suite 11.1** (default selection) and press **Enter**.
The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



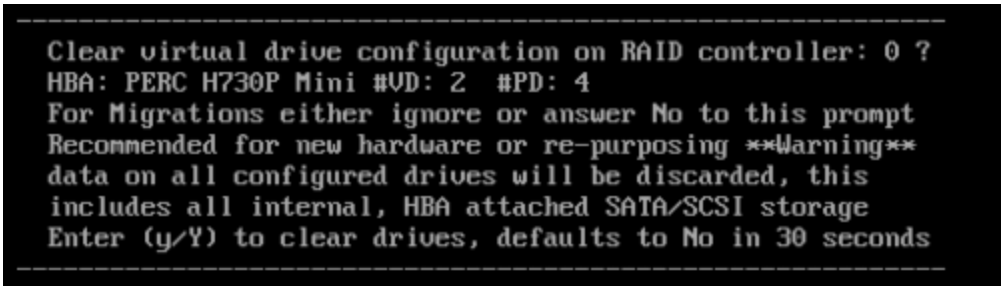
e. Type **Y** to continue.

The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives. The **Press enter to reboot** prompt is displayed.



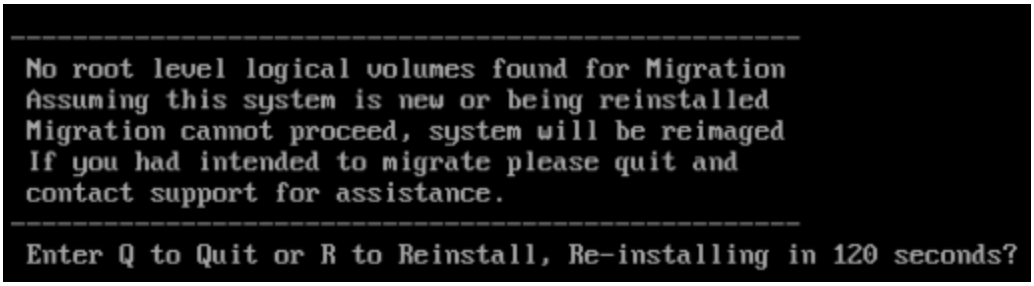
f. Press **Enter** to reboot the host.

The Installation program asks you to clear the drives again.



g. Type **N** because you already cleared the drives.

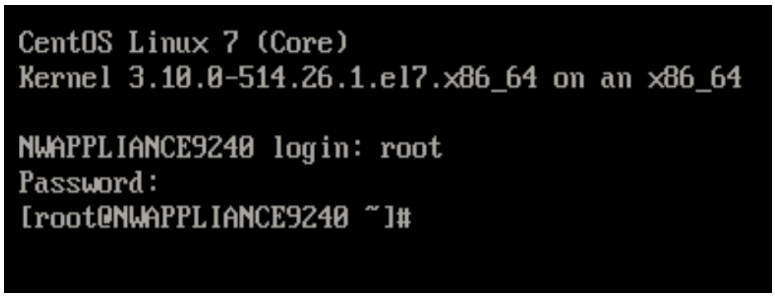
The **Enter Q (Quit) or R (Reinstall)** prompt is displayed.



h. Type **R** to install the base image.

The installation program displays the components as they are installed, which varies depending on the appliance, and reboots.

Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).

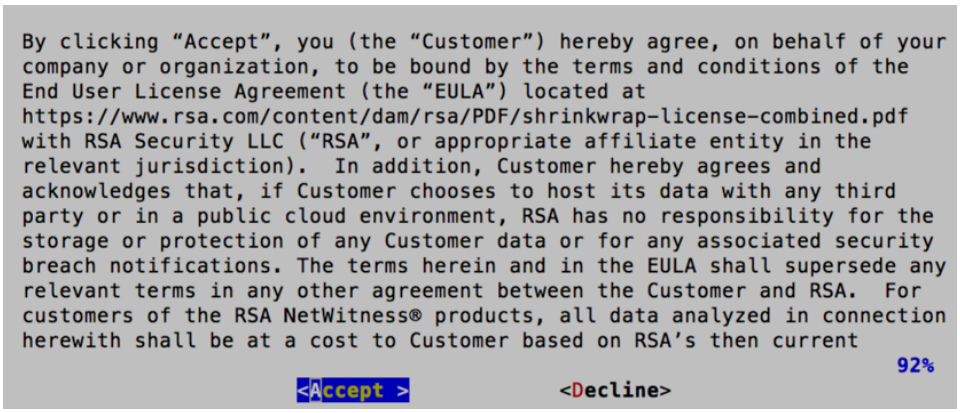


i. Log in to the host with the `root` credentials.

2. Run the `nwsetup-tui` command to set up the host.

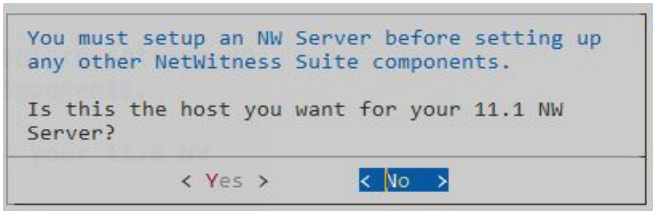
This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console you use access the host.
3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach a DNS server after setup that is unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Optional) Task 1 - Re-Configure DNS Servers Post 11.1 .
If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).



3. Tab to **Accept** and press **Enter**.

   The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

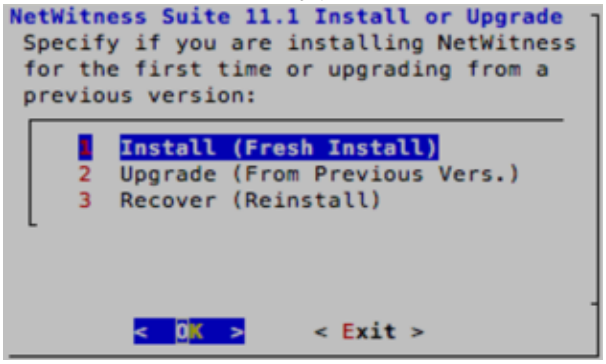


4. Tab to **Yes** and press **Enter**.

   Choose **No** if you already installed 11.1 on the NW Server.

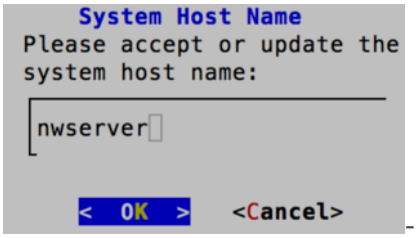
   Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program and complete (steps 2 -14) to correct this error.

   The **Install or Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disater Recovery.).



5. Press **Enter**. **Install (Fresh Install)** is selected by default.

   The **Host Name** prompt is displayed.



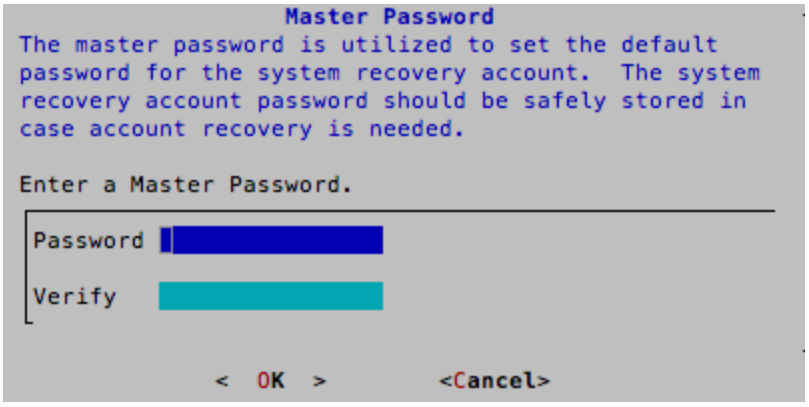
6. Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

   The **Master Password** prompt is displayed.

   The following list of characters are supported for Master Password and Deployment Password:

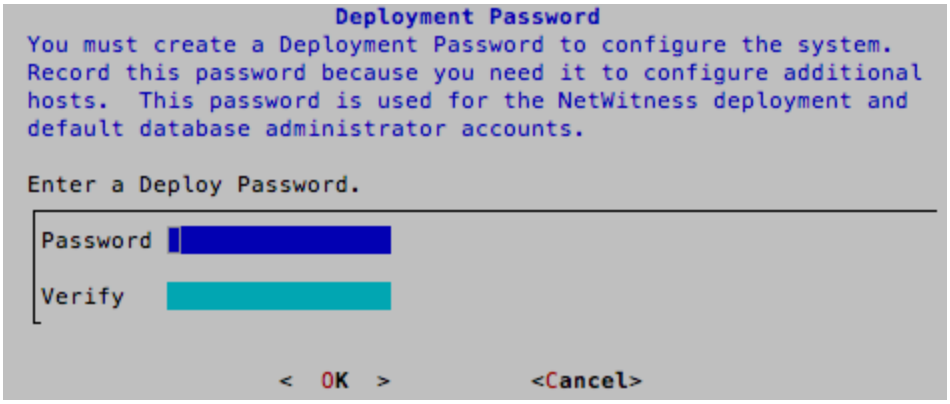
   - Symbols : ! @ # % ^ +
   - Numbers : 0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z

   No ambiguous characters are supported for Master Password and Deployment Password. For example:
   space { } [ ] ( ) / \ ' " ` ~ ; : . < > -



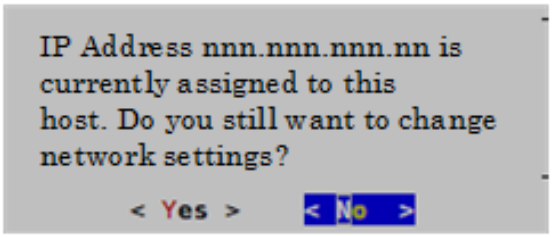
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

The **Deployment Password** prompt is displayed.



8. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
   One of the following conditional prompts is displayed.

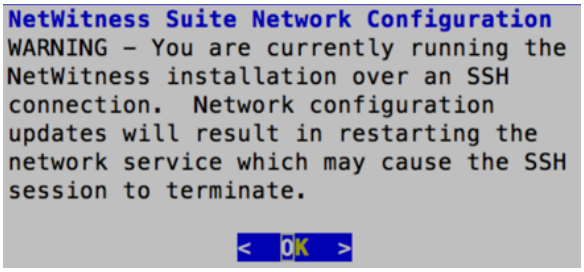
   - If the Setup program finds a valid IP address for this host, the following prompt is displayed.

     Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** if you want to change the IP configuration found on the host.

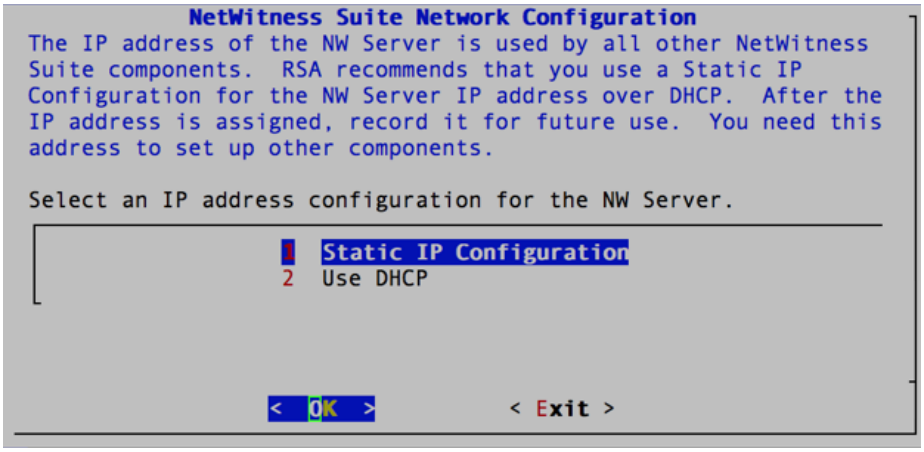
   - If you are using an SSH connection, the following warning is displayed.

     Note: If you connect directly from the host console, the following warning will not be displayed.

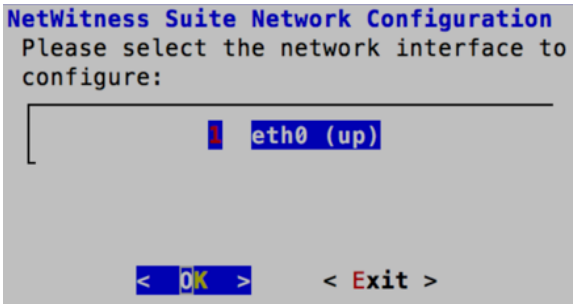
     

     Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

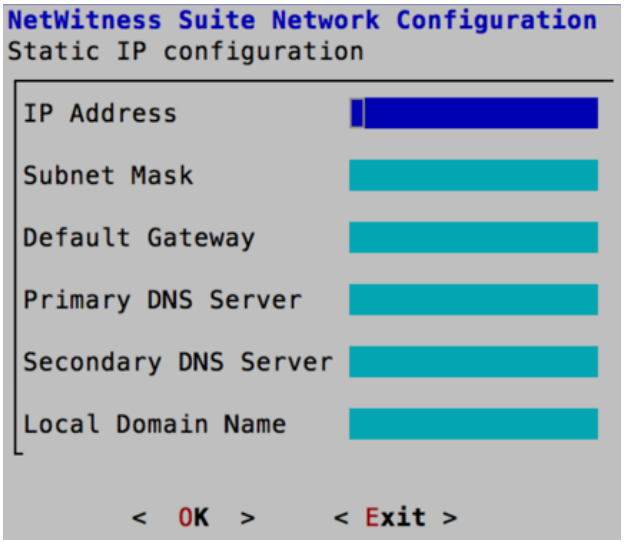


9. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.
   The **Network Configuration** prompt is displayed.



10. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**

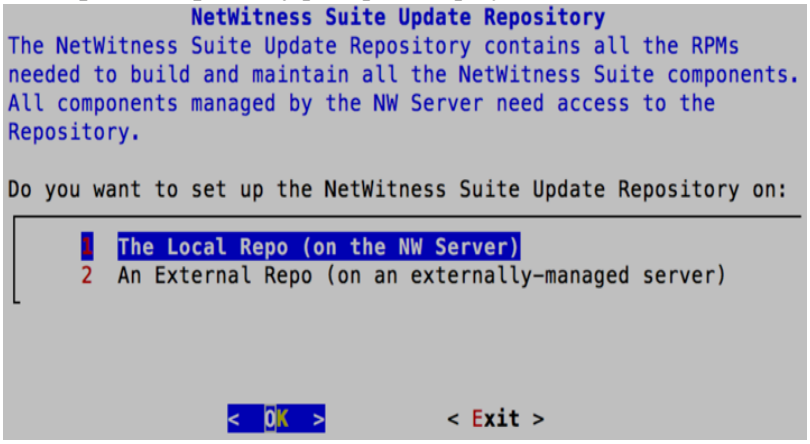
The **Static IP Configuration** prompt is displayed.



11. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required). If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

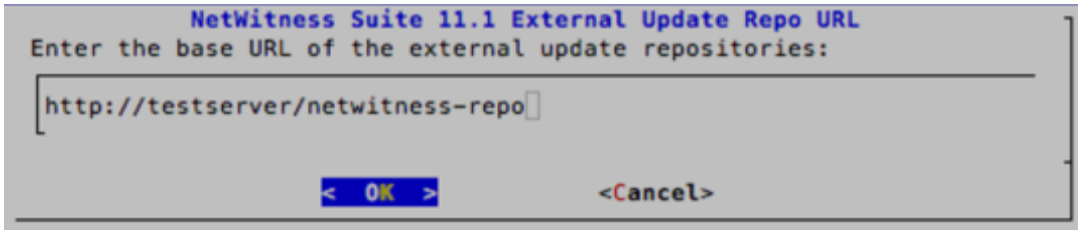
The **Update Repository** prompt is displayed.



12. Press **Enter** to choose the **Local Repo** on the NW Server.
    If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.

- If you select **1 The Local Repo (on the NW Server)** in the Setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness Suite 11.1.0.0. If the program cannot find the attached media, you receive the following prompt.

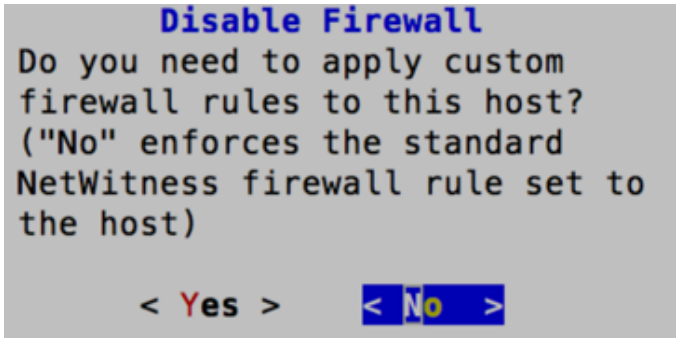
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to Appendix B. Create an External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



Enter the base URL of the NetWitness Suite external repo and click **OK.** The **Start Install** prompt is displayed.

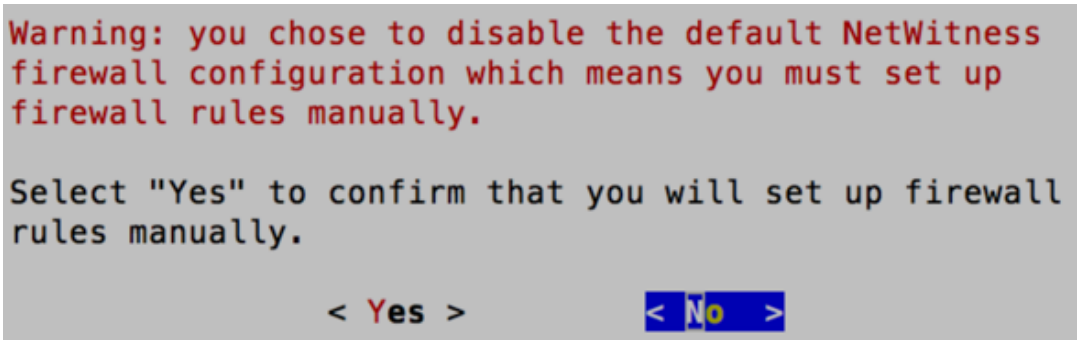
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

The Disable firewall prompt is displayed.

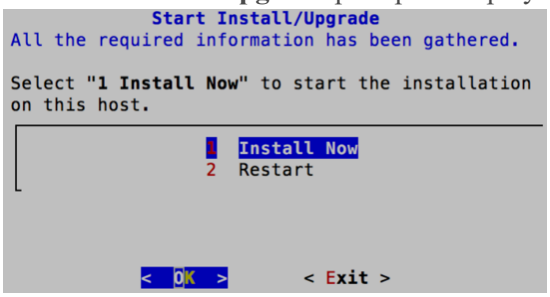


13. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



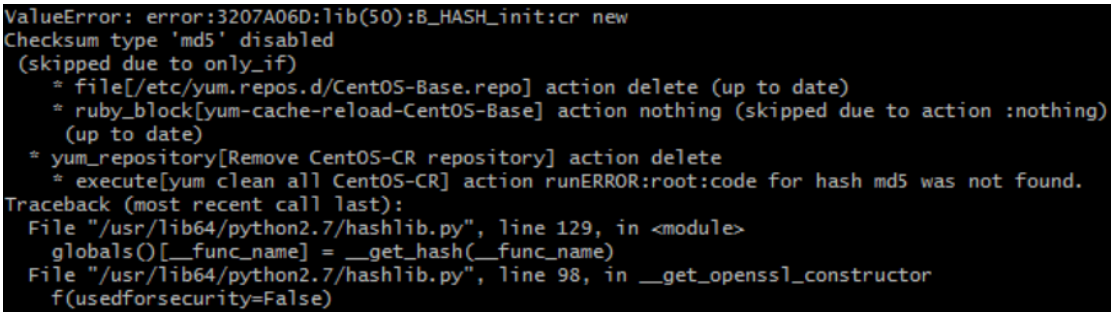
The **Start Install/Upgrade** prompt is displayed.



14. Press **Enter** to install 11.1 on the NW Server.

    When **Installation complete** is displayed, you have installed the 11.1 NW Server on this host.

> **Note:** Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.



Task 2 - Install 11.1 on Other Component Hosts

For a non-NW Server host this task:

- Creates a base image.
- Sets up the 11.1 non-NW Server host.

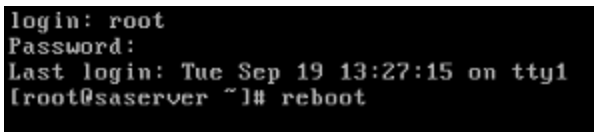
For ESA hosts:

- Install your primary ESA Host and install the **ESA Primary** service on it after you finish the Set Up program in the UI on the **ADMIN > Hosts** view.
- (Conditional) If you have a secondary ESA host, install it and install the **ESA Secondary** service on it after you finish the Set Up program in the UI on the **ADMIN > Hosts** view.

Complete the following steps to install NetWitness Suite 11.1 on a non-NW Server host.

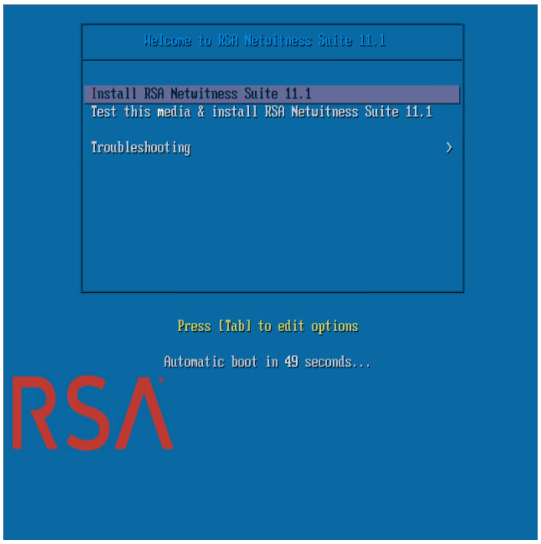
1. Create a base image on the host.
   a. Attach media (media that contains the ISO file, for example a build stick) to the host. See the *RSA NetWitness Suite Build Stick Instructions* for more information.
      - Hypervisor installs - use the ISO image.
      - Physical media - use the ISO file to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the ISO file. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO file.

        See the *RSA NetWitness Suite Build Stick Instructions* for more information.
   b. Log in to the host and reboot it.



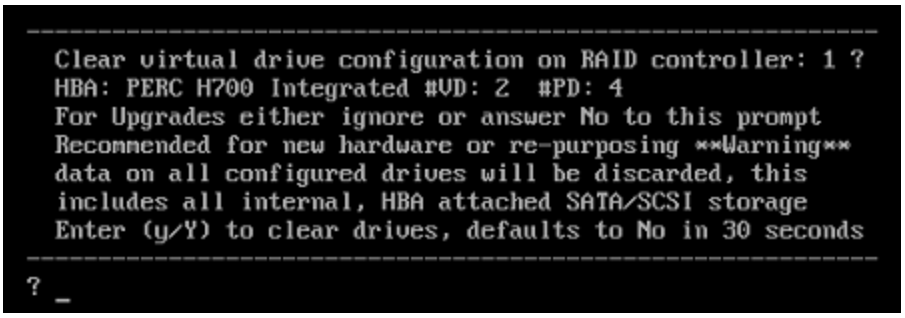
c. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media.

After some system checks during booting, the following **Welcome to RSA NetWitness Suite 11.1** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



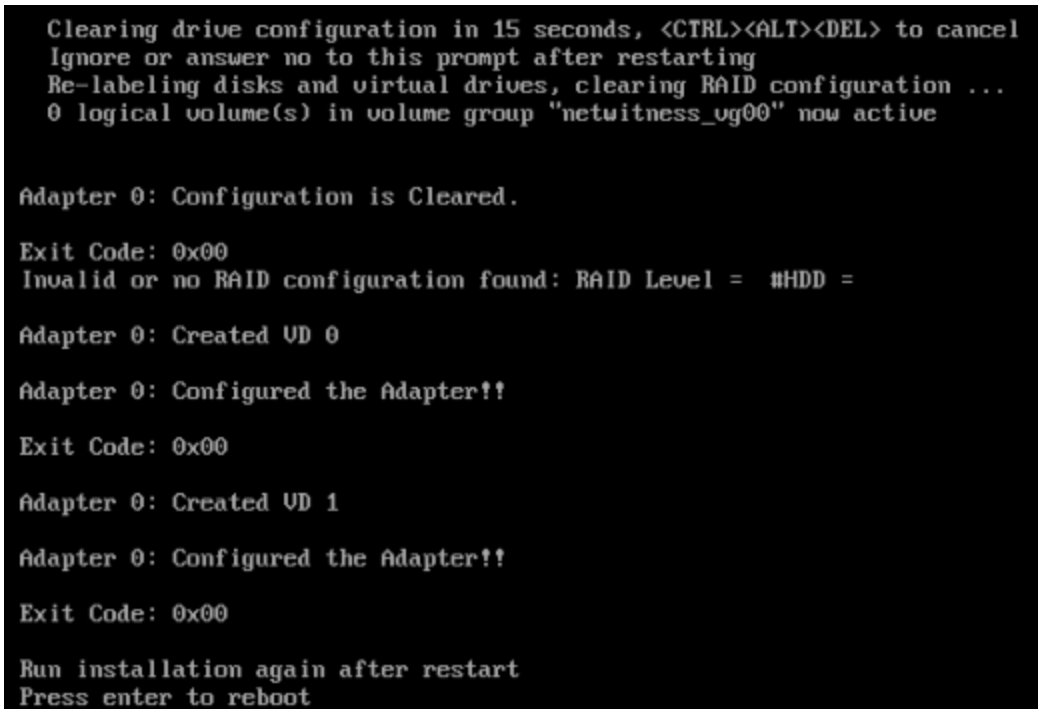
d. Select **Install RSA Netwitness Suite 11.1** (default selection) and press **Enter**.

The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



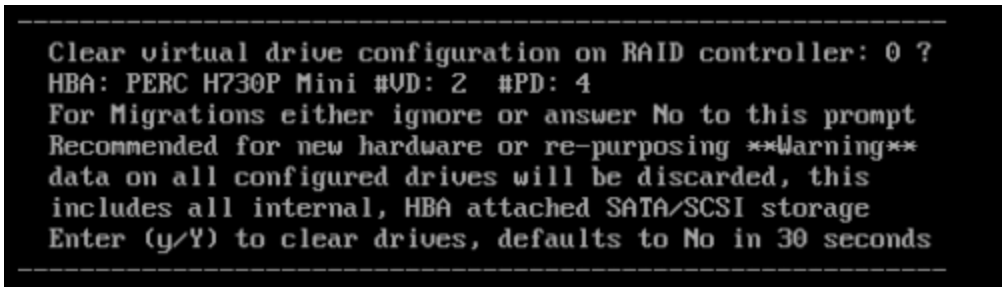
e. Type **Y** to continue.

The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives. The **Press enter to reboot** prompt is displayed.



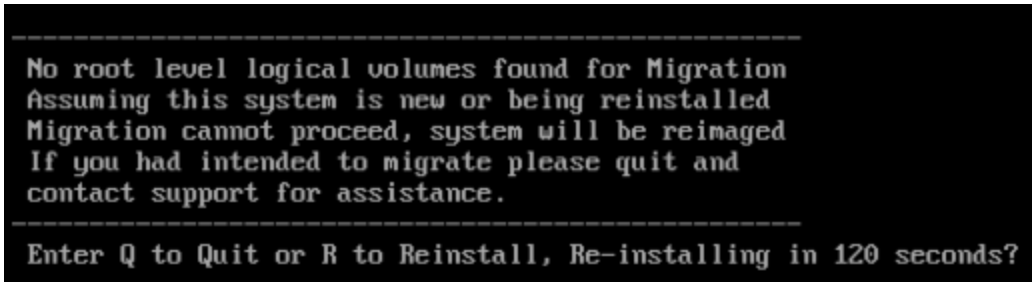
f. Press **Enter** to reboot the host.

The Installation program asks you to clear the drives again.



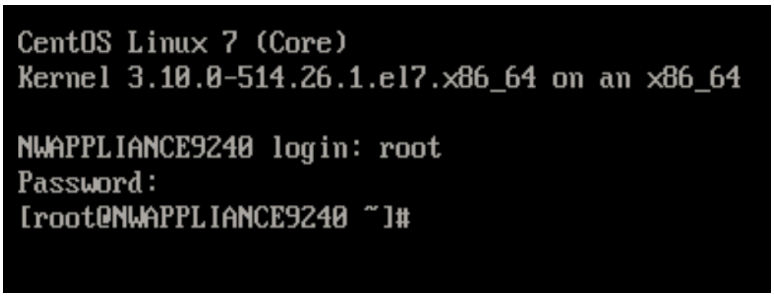
g. Type **N** because you already cleared the drives.

The **Enter Q (Quit) or R (Reinstall)** prompt is displayed.



h. Type **R** to install the base image.
The installation program displays the components as they are installed, which varies depending on the appliance, and reboots.

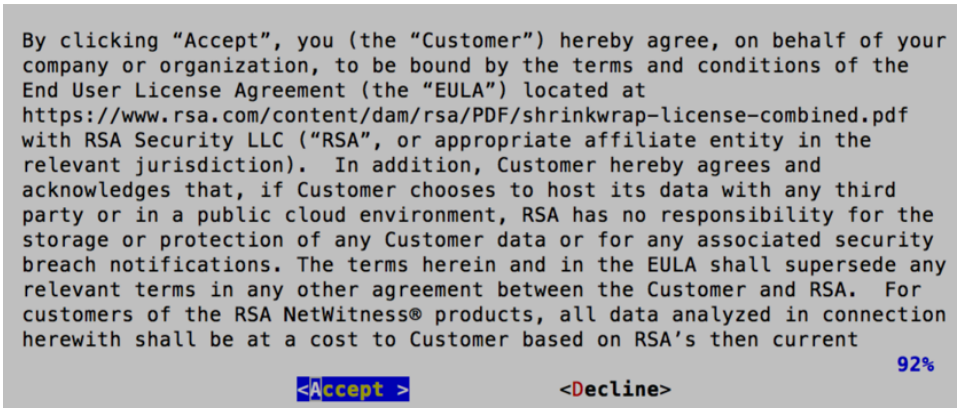
Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).



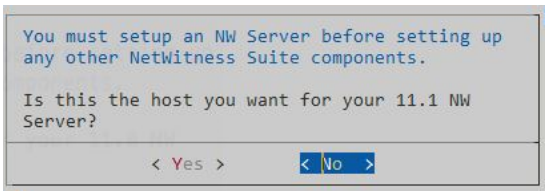
i. Log in to the host with the `root` credentials.

2. Run the `nwsetup-tui` command to set up the host..
This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

Note: If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach a DNS server after setup that is unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Optional) Task 1 - Re-Configure DNS Servers Post 11.1 .
If you do not specify DNS servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 11 (the DNS servers are not defined so the system cannot access the external repo).



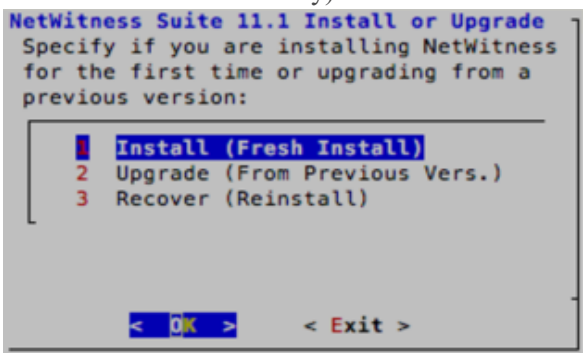
3. Tab to **Accept** and press **Enter**.
The **Is this the host you want for your 11.1 NW Server** prompt is displayed.



Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete (steps 2 - 14) of Task 1 - Install 11.1 on the NetWitness Server (NW Server) Host to correct this error.

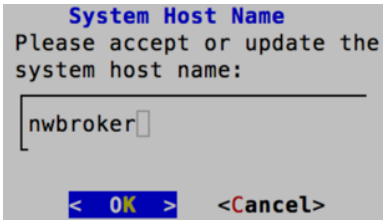
4. Press **Enter** (No).

   The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).



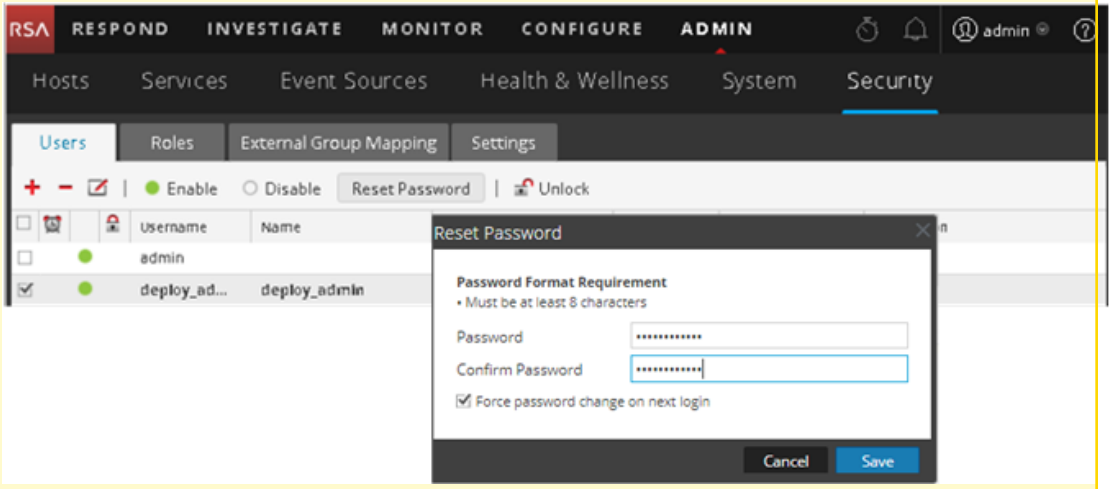
5. Press **Enter**. **Install (Fresh Install)** is selected by default.

   The **Host Name** prompt is displayed.



6. If want to keep this name, press **Enter**. If you want to change this name, edit it, tab to **OK**, and press **Enter**.

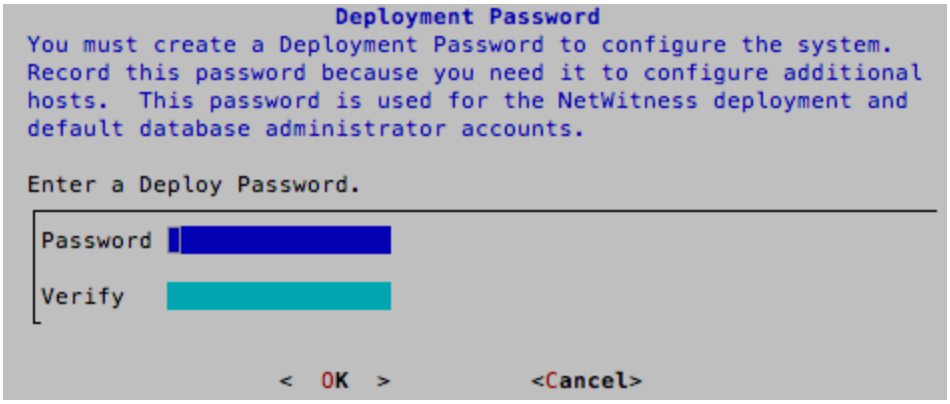
Caution: If you change the **deploy_admin** user password in the NetWitness Suite User Interface (**ADMIN**>**Security** >Select **deploy-admin - Reset password**),



you must:

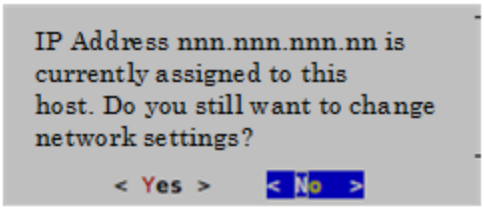
1. SSH to the NW Server host.
2. Run the `(/opt/rsa/saTools/bin/set-deploy-admin-password` script.
3. Use the new password when installing any new non-NW Server hosts.
4. Run `(/opt/rsa/saTools/bin/set-deploy-admin-password` script on all non-NW Server hosts in your deployment.
5. Write down the password because you may need to refer to it later in the installation.

The **Deployment Password** prompt is displayed.



Note: You must use the same deployment password that you used when you installed the NW Server.

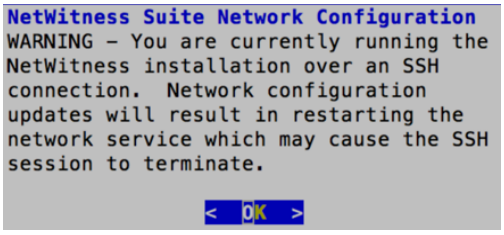
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
   - If the Setup program finds a valid IP address for this host, the following prompt is displayed.



Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** If you want to change the IP configuration found on the host.

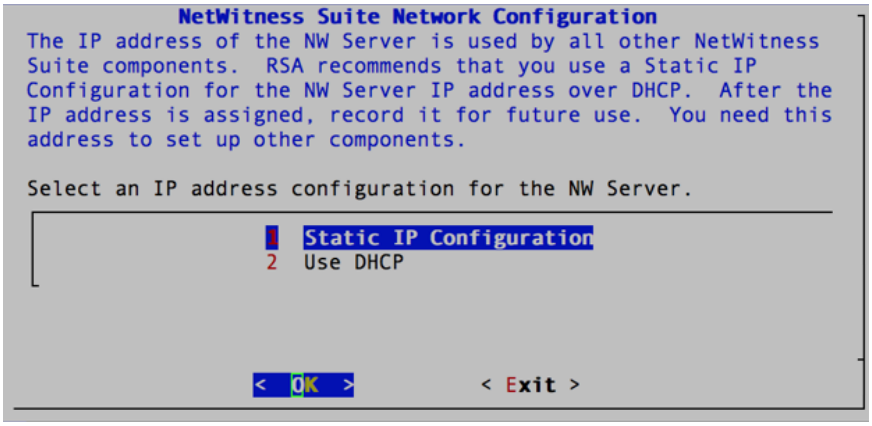
- If you are using an SSH connection, the following warning is displayed.

Note: If you connect directly from the host console, the following warning will not be displayed.



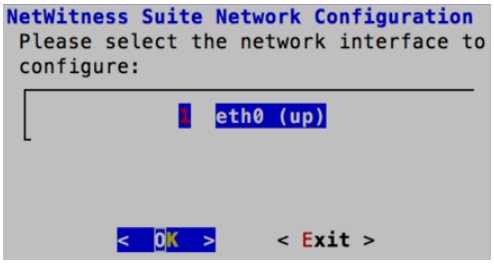
Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 11 to and complete the installation.
- If the Setup Program could not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



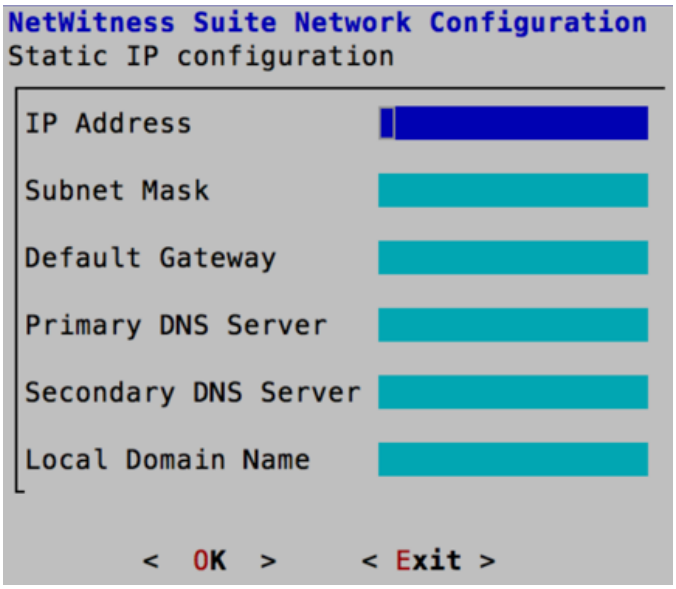
8. Tab to **OK** and press **Enter** to use a **Static IP**.
   If you want to use **DHCP**, down arrow to **2 Use DHCP** and press **Enter**.

The **Network Configuration** prompt is displayed.



9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.

   The **Static IP Configuration** prompt is displayed.



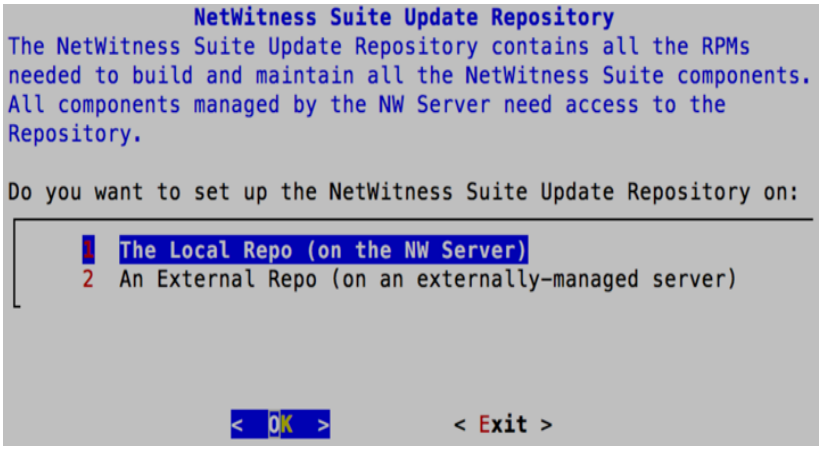
10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

    If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required).

    If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

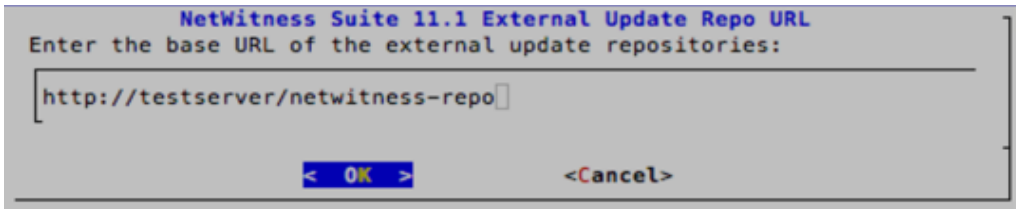
    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

The **Update Repository** prompt is displayed.
Select the same repo you selected when you installed the NW Server Host for all hosts.

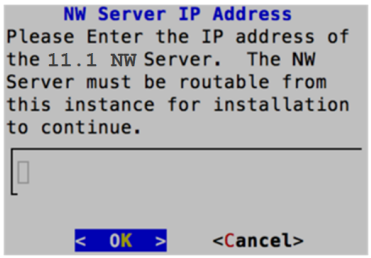


11. Press **Enter** to choose the **Local Repo** on the NW Server.
    If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.

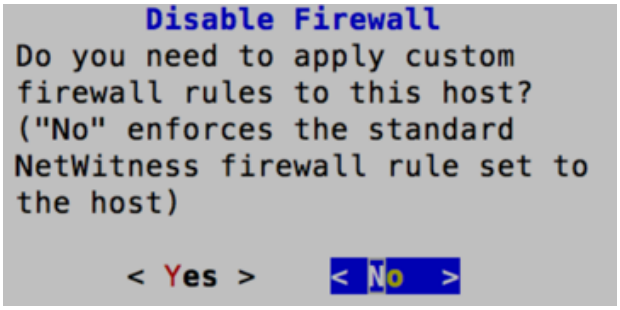
    - If you select **1 The Local Repo (on the NW Server)** in the setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness Suite 11.1.0.0.
    - If you select **2 An External Repo (a server managed externally - not on the NW Server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to Appendix B. Create an External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



Enter the base URL of the NetWitness Suite external repo, tab to **OK** and press **Enter**.
The **NW Server IP Address** prompt is displayed.

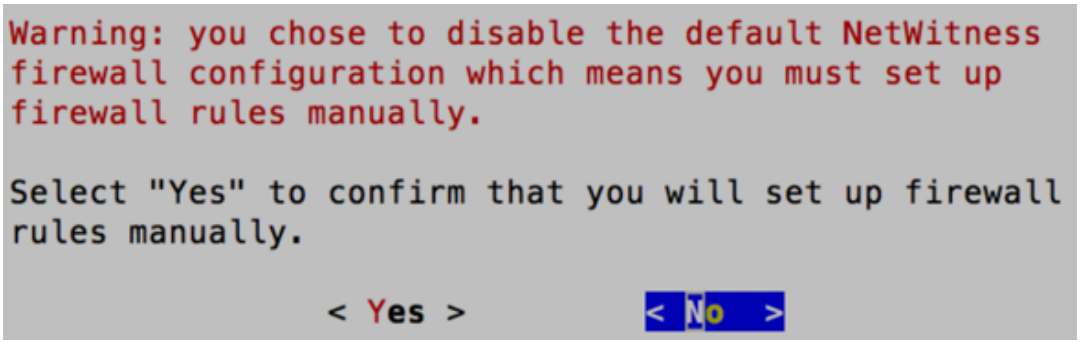


12. Type the NW Server IP address. Tab to **OK** and press **Enter**.
    The **Disable Firewall** prompt is displayed.

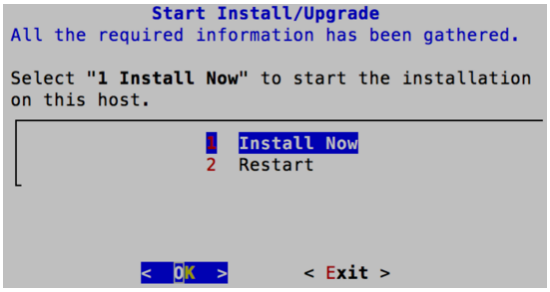


13. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

    - If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



      The **Start Install** prompt is displayed.



14. Press **Enter** to install 11.1 on the non-NW Server.
    When **Installation complete** is displayed, you have a generic non-NW Server host with an operating system compatible with NetWitness Suite 11.1.

15. Install a component service on the host.

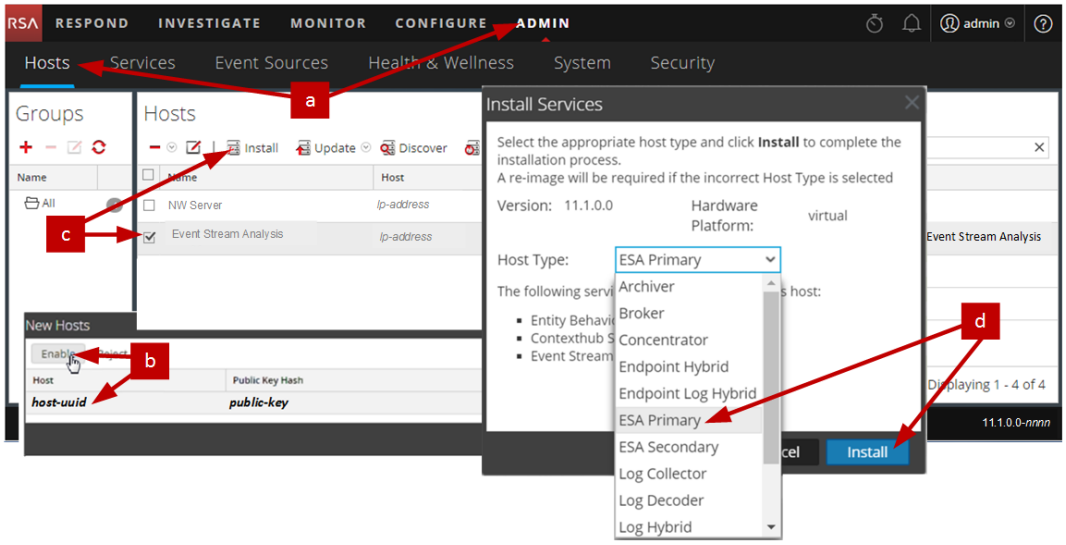
    a. Log into NetWitness Suite and click **ADMIN** > **Hosts**.
       The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

b. Select the host in the **New Hosts** dialog and click **Enable**.
The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click Install.
The **Install Services** dialog is displayed.

d. Select the appropriate host type (for example, **ESA Primary**) in **Host Type** and click **Install**.



You have completed the installation of the non-NW Server host in NetWitness Suite.

16. Complete steps 1 through 15 for the rest of the NetWitness Suite non-NW Server components.

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Installation Tasks

This topic contains the task you complete after you install 11.1.

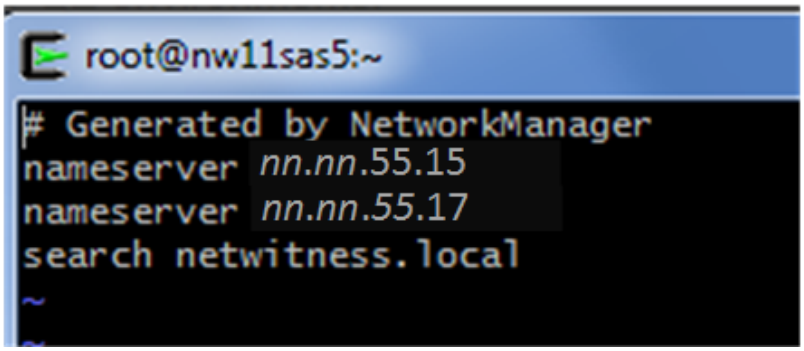
- General
- RSA NetWitness® Endpoint Insights

General

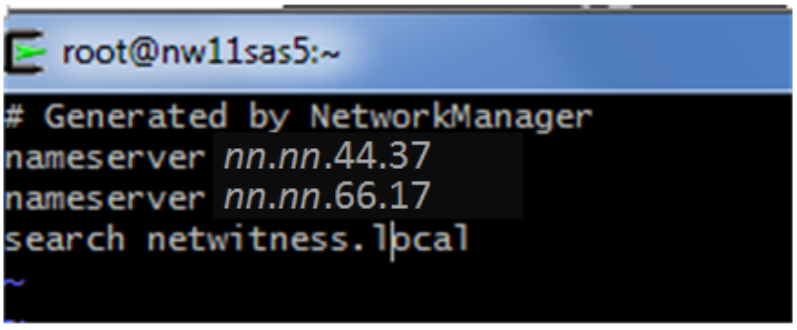
(Optional) Task 1 - Re-Configure DNS Servers Post 11.1

Complete the following steps to re-configure the DNS servers in NetWitness Suite 11.1.

1. Login to the server host with your `root` credentials.
2. Edit the `/etc/resolv.conf` file:
   a. Replace the IP address corresponding to `nameserver`.
   If you need to replace both DNS servers , replace the IP entries for both the hosts with valid addresses.
   The following example shows both DNS entries.



   The following example shows the new DNS values.



   b. Save the `/etc/resolv.conf` file.

RSA NetWitness® Endpoint Insights

(Optional) Task 2 - Install Endpoint Hybrid or Endpoint Log Hybrid

You must install one of the following services to install NetWitness Suite Endpoint Insights in your deployment:

Caution: You can only install one instance of the following services in your deployment.

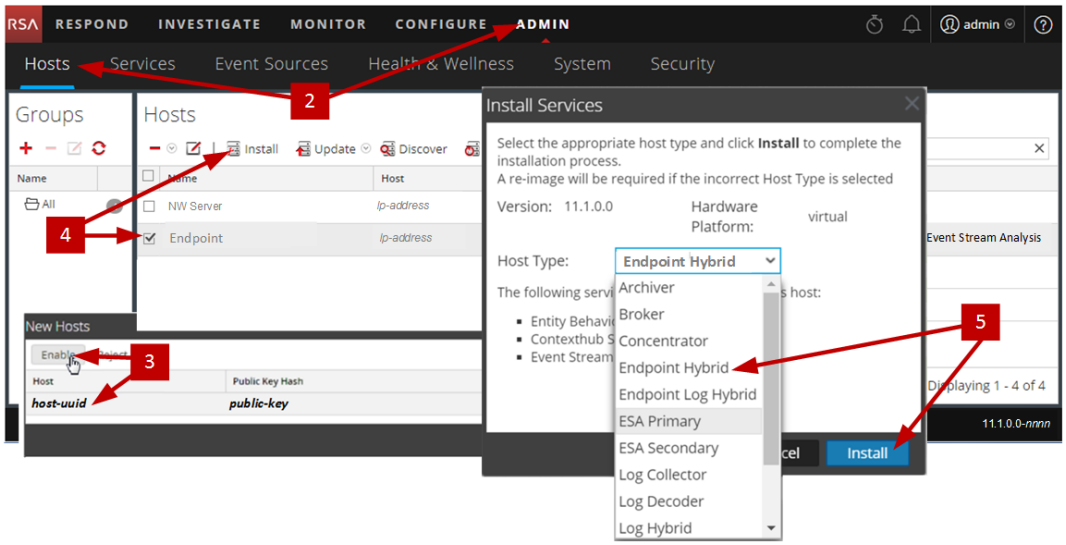
- Endpoint Hybrid
- Endpoint Log Hybrid

Note: You must install the Endpoint Hybrid or Endpoint Log Hybrid on the S5 or Dell R730 appliance.

1. Complete steps 1 - 14 in Task 2 - Install 11.1 on Other Component Hosts.
2. Log into NetWitness Suite and click **ADMIN** > **Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.
3. Select the host in the **New Hosts** dialog and click **Enable**.
   The New Hosts dialog closes and the host is displayed in the Hosts view.
4. Select that host in the **Hosts** view (for example, **Endpoint**) and click Install.
   The Install Services dialog is displayed.
5. Select the appropriate service, either **Endpoint Hybrid** or **Endpoint Log Hybrid**, and click **Install**.

Endpoint Hybrid is used as an example in the following screen shot.



6. Make sure that all Endpoint Hybrid or Endpoint Log Hybrid services are running.
7. Register the Endpoint server host IP address with the NW Server.
   a. SSH to the NW Server.
   b. Go to the `/opt/rsa/saTools/bin` directory.
      `cd /opt/rsa/saTools/bin`
   c. Run the `register-endpoint` script specifying the Endpoint host IP address.
      `./register-endpoint-ip -v --host-addr <ip-address>`

      Note: The script takes a few minutes to update the Endpoint Server IP address.
8. Configure Endpoint Meta forwarding.
   See *Endpoint Insights Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
9. Install the Endpoint Insights Agent.
   See *Endpoint Insights Agent Installation Guide* for detailed instructions on how to install the agent. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Troubleshooting

This section describes solutions to problems that you may encounter during installations and upgrades. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294) .

This section has troubleshooting documentation for the following services, features, and processes.

- Command Line Interface (CLI)
- Backup Script
- Event Stream Analysis
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

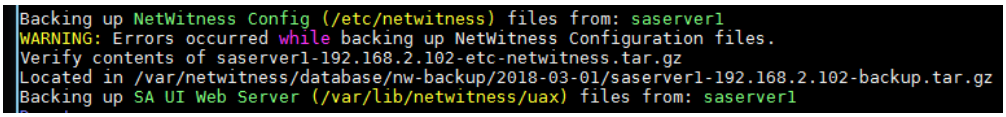
Command Line Interface (CLI)

Error Message	Command Line Interface (CLI) displays: "Orchestration failed." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Entered the wrong `deploy_admin` password in `nwsetup-tui`.
Solution	Retrieve your `deploy_admin` password password. 1. SSH to the NW Server host. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` SSH to the host that failed. 2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

Error Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Suite sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service. `systemctl restart rsa-sms`

Backup (`nw-backup` script)

Error Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the *Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Error	Backup errors caused by the `immutable` attribute setting. Here is an example of an error that can be displayed: 
Cause	If you have any files that have the immutable flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.
Solution	On the host that contains the files with the immutable flag set, run the following command to remove the immutable setting from the files: `chattr -i <filename>`

Error	Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: `/etc/sysconfig/network-scripts/ifcfg-em1` Verify contents of `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Cause	There are incorrect or duplicate entries for any one of the following fields: DEVICE, BOOTPROTO, IPADDR, NETMASK or GATEWAY, that were found from reading the primary Ethernet interface configuration file from the host being backed up.

Solution	Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format `<hostname>-<hostip>-network.info.txt`, and should contain the following entries:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1.0.0 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESA Primary host and log in.
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Submit the following command to restart ESA.
	`systemctl restart rsa-nw-esa-server`
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Suite and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Suite and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Suite and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.5.x to 11.1.0.0.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

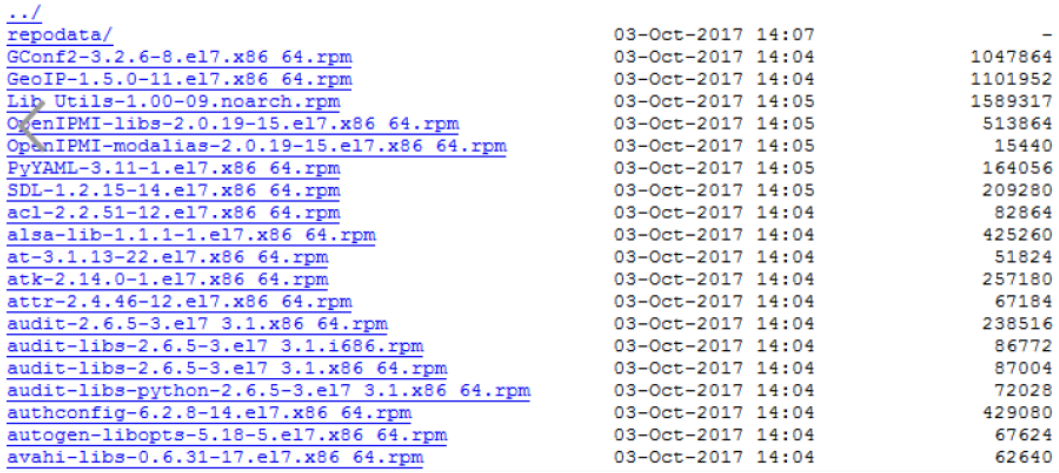
Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Error Message	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Appendix B. Create an External Repository

Complete the following procedure to set up an external repository (Repo).

1. Log in to the web server host
2. Create the `ziprepo` directory to host the NW repository (`netwitness-11.0.0.0.zip`) under `web-root` of the web server. For example, /var/netwitness is the web-root, submit the following command string.
   ```
   mkdir /var/netwitness/ziprepo
   ```
3. Create the 11.0.0.0 directory under `/var/netwitness/ziprepo`.
   ```
   mkdir /var/netwitness/ziprepo/11.0.0.0
   ```
4. Create the `OS` and `RSA` directories under `/var/netwitness/ziprepo/11.0.0.0`.
   ```
   mkdir /var/netwitness/ziprepo/11.0.0.0/OS
   mkdir /var/netwitness/ziprepo/11.0.0.0/RSA
   ```
5. Unzip the `netwitness-11.0.0.0.zip` file into the `/var/netwitness/ziprepo/11.0.0.0`directory.
   ```
   unzip netwitness-11.0.0.0.zip -d /var/netwitness/ziprepo/11.0.0.0
   ```
   Unzipping `netwitness-11.0.0.0.zip` results in two zip files (`OS-11.0.0.0.zip` and `RSA-11.0.0.0.zip`)and some other files.
6. Unzip the:
   a. `OS-11.0.0.0.zip` into the `/var/netwitness/ziprepo/11.0.0.0/OS` directory.
      ```
      unzip /var/netwitness/ziprepo/11.0.0.0/OS-11.0.0.0.zip -d
      /var/netwitness/ziprepo/11.0.0.0/OS
      ```
   b. `RSA-11.0.0.0.zip` into the `/var/netwitness/ziprepo/11.0.0.0/RSA` directory.
      ```
      unzip /var/netwitness/ziprepo/11.0.0.0/RSA-11.0.0.0.zip -d
      /var/netwitness/ziprepo/11.0.0.0/RSA
      ```



../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

The external url for the repo is `http://<web server IP address>/ziprepo`.

7. Use the `http://<web server IP address>/ziprepo` in response to **Enter the base URL of the external update repositories** prompt from NW 11.0 Setup program (nwsetup-tui) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD

RSA NETWITNESS® SUITE

Virtual Host Installation Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Virtual Host Setup Guide **5**

Basic Virtual Deployment **6**

Abbreviations Used in the Virtual Deployment Guide 6

Supported Virtual Hosts 7

Installation Media 8

Virtual Environment Recommendations 8

Virtual Host Recommended System Requirements 8

Scenario One 9

Log Decoder 9

Packet Decoder 9

Concentrator - Log Stream 10

Concentrator - Packet Stream 10

Archiver 10

Scenario Two 10

Log Decoder 11

Packet Decoder 11

Concentrator - Log Stream 11

Concentrator - Packet Stream 11

Warehouse Connector - Log Stream 12

Warehouse Connector - Packet Stream 12

Archiver - Log Stream 12

Event Stream Analysis with Context Hub 12

NetWitness Server and Co-Located Components 12

Scenario Three 13

Log Decoder 13

Packet Decoder 13

Concentrator - Log Stream 13

Concentrator - Packet Stream 14

Log Collector (Local and Remote) 14

Scenario Four 14

Endpoint Hybrid 14

Log Collector (Local and Remote) 15
Legacy Windows Collectors Sizing Guidelines 15

Install NetWitness Suite Virtual Host in Virtual Environment 16

Prerequisites 16
Step 1. Deploy the Virtual Host to create VM 16
Prerequisites 16
Procedure 16
Step 2. Configure the Network and Install RSA NetWitness Suite 19
Prerequisites 20
Procedure 20
Review Open Firewall Ports 20
Installation Tasks 20
Step 3. Configure Databases to Accommodate NetWitness Suite 36
Task 1. Review Initial Datastore Configuration 36
Initial Space Allocated to PacketDB 36
Initial Database Size 36
PacketDB Mount Point 37
Task 2. Review Optimal Datastore Space Configuration 38
Virtual Drive Space Ratios 38
Task 3. Add New Volume and Extend Existing File Systems 40
Create LVM Physical Volume on New Partition 47
Step 4. Configure Host-Specific Parameters 52
Configure Log Ingest in the Virtual Environment 52
Configure Packet Capture in the Virtual Environment 52
Use of a Third-Party Virtual Tap 53
Step 5. Post Installation Tasks 53
General 53
RSA NetWitness® Endpoint Insights 54

Appendix A. Create External Repository 57

Revision History 60

Virtual Host Setup Guide

This document provides instructions on the installation and configuration of RSA NetWitness® Suite 11.1.0.0 hosts running in a virtual environment.

Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying RSANetWitness Suite 11.1.0.0 in a virtual environment.

Abbreviations Used in the Virtual Deployment Guide

Abbreviations	Description
CPU	Central Processing Unit
EPS	Events Per Second
VMware ESX	Enterprise-class, type-1 hypervisor, Supported versions - 6.5, 6.0 and 5.5
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigbit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
IOPS	Input/Output Operations Per Second
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
NAS	Network Attached Storage
OVF	Open Virtualization Format
OVA	Open Virtual Appliance. For purposes of this guide, OVA stands for Open Virtual Host.
RAM	Random Access Memory (also known as memory)
SAN	Storage Area Network
SSD/EFD HDD	Solid-State Drive/Enterprise Flash Drive Hard Disk Drive

Abbreviations	Description
SCSI	Small Computer System Interface
SCSI (SAS)	Point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives.
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
vRAM	Virtual Random Access Memory (also known as virtual memory)

Supported Virtual Hosts

You can install the following NetWitness Suite hosts in your virtual environment as a virtual host and inherit features that are provided by your virtual environment:

- NetWitness Server
- Event Stream Analysis - ESA Primary and ESA Secondary
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid

You must be familiar with the following VMware infrastructure concepts:

- VMware vCenter Server
- VMware ESXi
- Virtual machine

For information on VMware concepts, refer to the VMware product documentation.

The virtual hosts are provided as an OVA. You need to deploy the OVA file as a virtual machine in your virtual infrastructure.

Installation Media

Installation media are in the form of OVA packages, which are available for download and installation from Download Central (https://download.rsasecurity.com). As part of your order fulfillment, RSA gives you access to the OVA.

Virtual Environment Recommendations

The virtual hosts installed with the OVA packages have the same functionality as the NetWitness Suite hardware hosts. This means that when you implement virtual hosts, you must account for the back-end hardware. RSA recommends that you perform the following tasks when you set up your virtual environment.

- Based on resource requirements of the different components, follow best practices to use the system and dedicated storage appropriately.
- Make sure that back-end disk configurations provide a write speed of 10% greater than the required sustained capture and ingest rate for the deployment.
- For OVA, 32 GB RAM per host appliance is required.
- Build Concentrator directories for meta and index databases on the SSD/EFD HDD.
- If the database components are separate from the installed operating system (OS) components (that is, on a separate physical system), provide direct connectivity with either:
  - Two 8-Gbps Fiber Channel SAN ports per virtual host,
    or
  - 6-Gbps Serial Attached SCSI (SAS) connectivity.

Note: 1.) Currently, NetWitness Suite does not support Network Attached Storage (NAS) for Virtual deployments.
2.) The Decoder allows any storage configuration that can meet the sustained throughput requirement. The standard 8-Gbps Fiber Channel link to a SAN is insufficient to read and write packet data at 10 Gb. You must use multiple Fiber Channels when you configure to the connection from a **10G Decoder** to the SAN.

Virtual Host Recommended System Requirements

The following tables list the vCPU, vRAM, and Read and Write IOPS recommended requirements for the virtual hosts based on the EPS or capture rate for each component.

- Storage allocation is covered in Step 3 “Configure Databases to Accommodate NetWitness Suite”.
- vRAM and vCPU recommendations may vary depending on capture rates, configuration and content enabled.
- The recommendations were tested at ingest rates of up to 25,000 EPS for logs and two Gbps for packets, for non SSL.
- The vCPU specifications for all the components listed in the following tables are Intel Xeon CPU @2.59 Ghz.
- All ports are SSL tested at 15,000 EPS for logs and 1.5 Gbps for packets.

Note: The above recommended values might differ for 11.1.0.0 installation when you install and try the new features and enhancements.

Scenario One

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder, Concentrator, and Archiver.
- The Packet Stream included a Packet Decoder and Concentrator.
- The background load included hourly and daily reports.
- Charts were configured.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	6 or 15.60 GHz	32 GB	50	75
5,000	8 or 20.79 GHz	32 GB	100	100
7,500	10 or 25.99 GHz	32 GB	150	150

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	32 GB	50	150

Mbps	CPU	Memory	Read IOPS	Write IOPS
100	4 or 10.39 GHz	32 GB	50	250
250	4 or 10.39 GHz	32 GB	50	350

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	32 GB	300	1,800
5,000	4 or 10.39 GHz	32 GB	400	2,350
7,500	6 or 15.59 GHz	32 GB	500	4,500

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	32 GB	50	1,350
100	4 or 10.39 GHz	32 GB	100	1,700
250	4 or 10.39 GHz	32 GB	150	2,100

Archiver

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	32 GB	150	250
5,000	4 or 10.39 GHz	32 GB	150	250
7,500	6 or 15.59 GHz	32 GB	150	350

Scenario Two

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder, Concentrator, Warehouse Connector, and Archiver.

- The Packet Stream included a Packet Decoder, Concentrator, and Warehouse Connector.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included reports, charts, alerts, investigation, and incident management.
- Alerts were configured.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	16 or 41.58 GHz	50 GB	300	50
15,000	20 or 51.98 GHz	60 GB	550	100

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	8 or 20.79 GHz	40 GB	150	200
1,000	12 or 31.18 GHz	50 GB	200	400
1,500	16 or 41.58 GHz	75 GB	200	500

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	10 or 25.99 GHz	50 GB	1,550 + 50	6,500
15,000	12 or 31.18 GHz	60 GB	1,200 + 400	7,600

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	12 or 31.18 GHz	50 GB	250	4,600
1,000	16 or 41.58 GHz	50 GB	550	5,500

Mbps	CPU	Memory	Read IOPS	Write IOPS
1,500	24 or 62.38 GHz	75 GB	1,050	6,500

Warehouse Connector - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	8 or 20.79 GHz	30 GB	50	50
15,000	10 or 25.99 GHz	35 GB	50	50

Warehouse Connector - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	6 or 15.59 GHz	32 GB	50	50
1,000	6 or 15.59 GHz	32 GB	50	50
1,500	8 or 20.79 GHz	40 GB	50	50

Archiver - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	12 or 31.18 GHz	40 GB	1,300	700
15,000	14 or 36.38 GHz	45 GB	1,200	900

Event Stream Analysis with Context Hub

EPS	CPU	Memory	Read IOPS	Write IOPS
90,000	32 or 83.16 GHz	94 GB	50	50

NetWitness Server and Co-Located Components

The NetWitness Server, Jetty, Broker, Incident Management, and Reporting Engine are in the same location.

CPU	Memory	Read IOPS	Write IOPS
12 or 31.18 GHz	50 GB	100	350

Scenario Three

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder and Concentrator.
- The Packet stream included a Packet Decoder and the Concentrator.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included hourly and daily reports.
- Charts were configured.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	32 or 83.16 GHz	75 GB	250	150

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	16 or 41.58 GHz	75 GB	50	650

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	16 or 41.58 GHz	75 GB	650	9,200

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	24 or 62.38 GHz	75 GB	150	7,050

Log Collector (Local and Remote)

The Remote Log Collector is a Log Collector service running on a remote host and the Remote Collector is deployed virtually.

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 or 20.79 GHz	8 GB	50	50
30,000	8 or 20.79 GHz	15 GB	100	100

Scenario Four

The requirements in these tables were calculated under the following conditions for Endpoint Hybrid.

- All the components were integrated.
- Endpoint Server is installed.
- The Log stream included a Log Decoder and Concentrator.

Endpoint Hybrid

Agents	CPU	Memory	IOPS Values		
5000	16 or 42 GHz	32 GB		**Read IOPS**	**Write IOPS**
			Log Decoder	250	150
			Concentrator	150	7,050
			MongoDb	250	150

Log Collector (Local and Remote)

The Remote Log Collector is a Log Collector service running on a remote host and the Remote Collector is deployed virtually.

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 or 20.79 GHz	8 GB	50	50
30,000	8 or 20.79 GHz	15 GB	100	100

Legacy Windows Collectors Sizing Guidelines

Refer to the *RSA NetWitness Suite Legacy Windows Collection Update & Installation* for sizing guidelines for the Legacy Windows Collector.

Install NetWitness Suite Virtual Host in Virtual Environment

Complete the following procedures according to their numbered sequence to install RSA NetWitness® Suite in a virtual environment.

Prerequisites

Make sure that you have:

- A VMware ESX Server that meets the requirements described in the above section. Supported versions are 6.5, 6.0, and 5.5.
- vSphere 4.1, 5.0, or 6.0 Client installed to log on to the VMware ESX Server.
- Administrator rights to create the virtual machines on the VMware ESX Server.

Step 1. Deploy the Virtual Host to create VM

Complete the following steps to deploy the OVA file on the vCenter Server or ESX Server using the vSphere client.

Prerequisites

Make sure that you have:

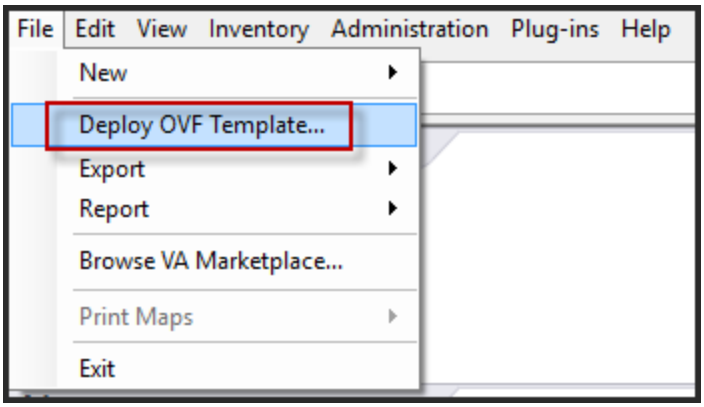
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Suite virtual host package file for example, rsanw-11.1.0.xxxx.el7-x86_64.ova. (You download this package from Download Central (https://community.rsa.com).)

Procedure

Note: The following instructions illustrate an example of deploying an OVA host in the ESXi environment. The screens you see may be different from this example.

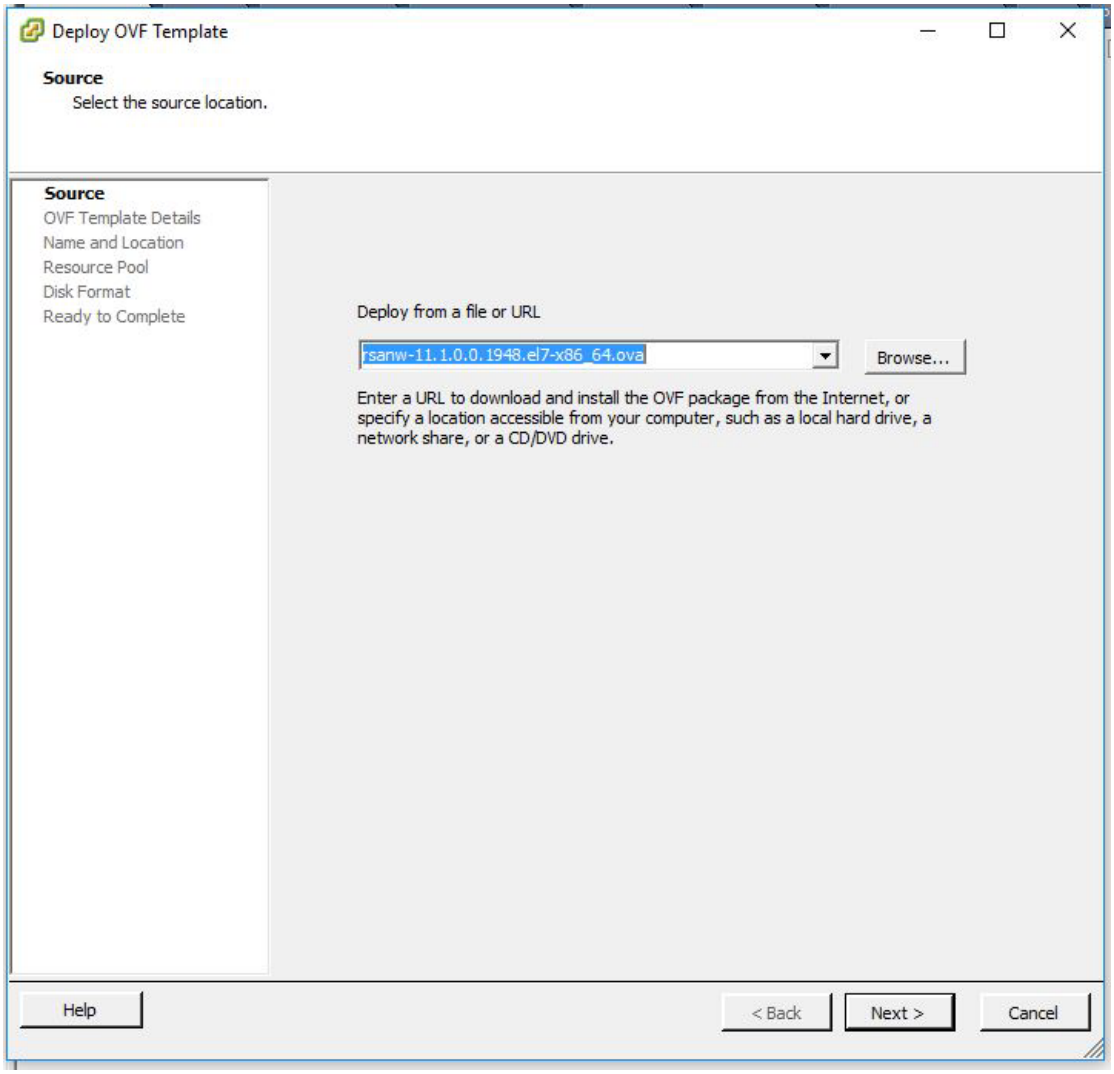
To deploy the OVA host:

1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.

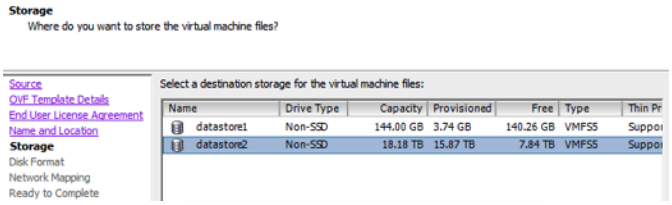


3. The Deploy OVF Template dialog is displayed. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V11.1**

GOLD\\rsanw-11.1.0.0.1948.el7-x86_64.ova), and click **Next**.



4. The Name and Location dialog is displayed. The designated name does not reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.
5. Make a note of the name, and click **Next**.
   Storage Options are displayed.

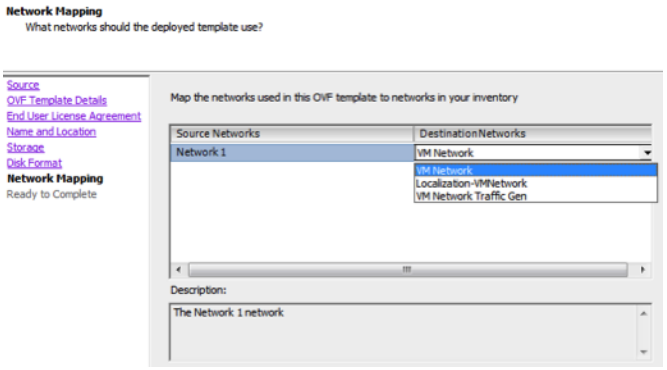


6. For Storage options, designate the datastore location for the virtual host.

Note: This location is for the host operating system (OS) exclusively. It does not have to be the same datastore needed to set up and configure additional volumes for the NetWitness Suite databases on certain hosts (covered in the following sections).

7. Click **Next**.

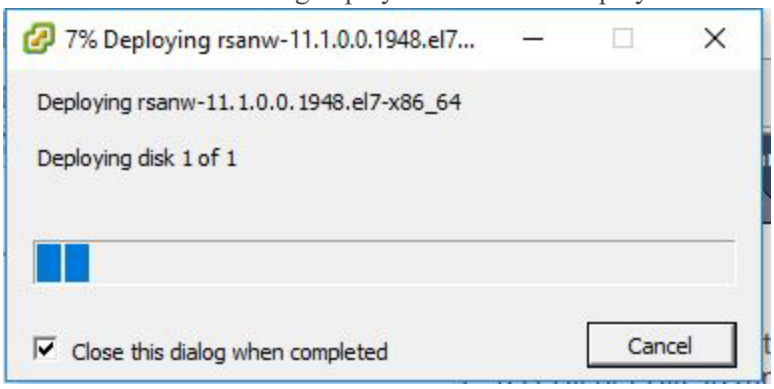
   The Network Mapping options are displayed.



8. Leave the default values, and click **Next**.

Note: If you want to configure Network Mapping now, you can select options, but RSA recommends that you keep the default values and configure network mapping after you configure the OVA. You configure the OVA in Step 4: Configure Host-Specific Parameters.

A status window showing deployment status is displayed.



After the process is complete, the new OVA is presented in the designated resource pool visible on ESXi from within vSphere. At this point, the core virtual host is installed, but is still not configured.

Step 2. Configure the Network and Install RSA NetWitness Suite

Complete the following steps to configure the network of the Virtual Appliance.

Prerequisites

Make sure that you have:

- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.

Procedure

Perform the following steps for all virtual hosts to get them on your network.

Review Open Firewall Ports

Review the ***Network Architecture and Ports*** topic in the ***Deployment Guide*** in the NetWitness Suite help so that you can configure NetWitness Suite services and your firewalls.

Caution: Do not proceed with the installation until the ports on your firewall are configured.

There are two main tasks that you must complete in the order listed below to install NetWitness Suite 11.1

Installation Tasks

Task 1 - Install 11.1.0.0 on the NetWitness (NW) Server Host

Task 2 - Install 11.1.0.0 on Other Component Hosts

Task 1- Install 11.1.0.0 on the NW Server Host

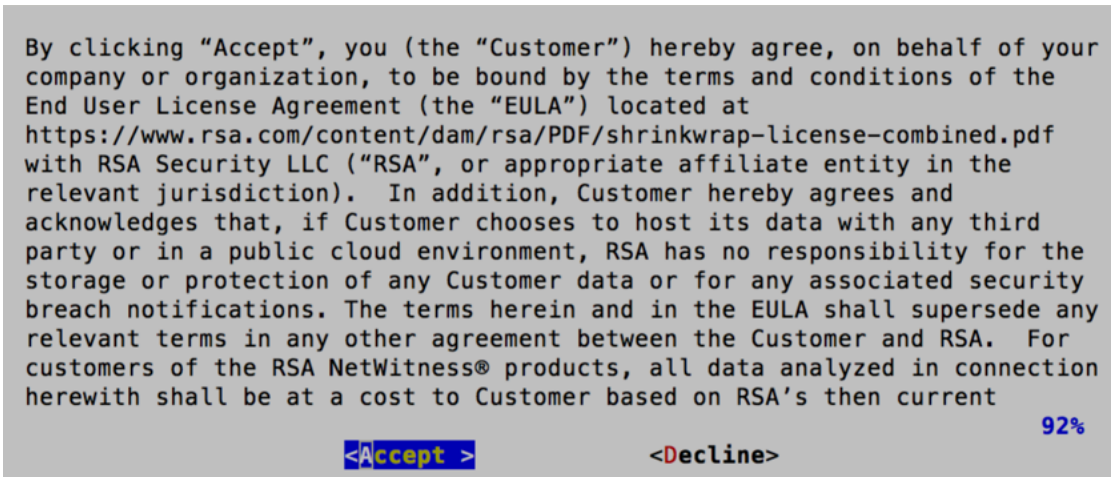
On the host you have deployed for the NW Server, this task installs:

- The 11.1.0.0 NW Server environmental platform.
- The NW Server components (that is, Admin, Config, Orchestration, Integration Server, Broker, Investigate Server, Reporting Engine, Respond Server and Security server).
- A repository with the RPM files required to install the other functional components or services.

1. Deploy your 11.1.0.0 environment:
   a. Add new VM.
   b. Configure storage.
   c. Set up firewalls.

2. Run the `nwsetup-tui` command. This initiates the Setup program and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as <Yes>, <No>, <OK>, and <Cancel>. Press Enter to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console you use access the host.
3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Optional) Task 1 - Re-Configure DNS Servers Post 11.1 in Post Installation Tasks.
If you do not specify DNS Servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

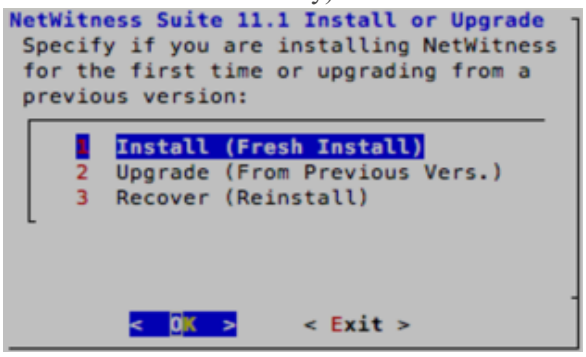


3. Tab to **Accept** and press Enter.
The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

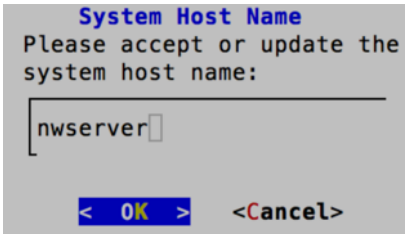
4. Tab to **Yes** and press Enter.
Choose **No** if you already installed 11.1.0.0 on the NW Server.

Caution: If you choose the wrong host for the NW Server and complete the Setup, you must start the Setup Program (step 3) and complete all the subsequent steps to correct this error.

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).



5. Press **Enter**. **Install (Fresh Install)** is selected by default.
   The **Host Name** prompt is displayed.

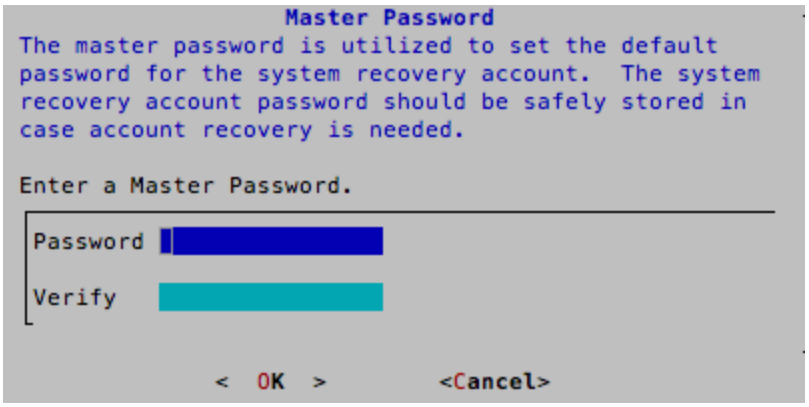


6. Press **Enter** if want to keep this name. If not edit the host name, Tab to **OK**, and press Enter to change it.

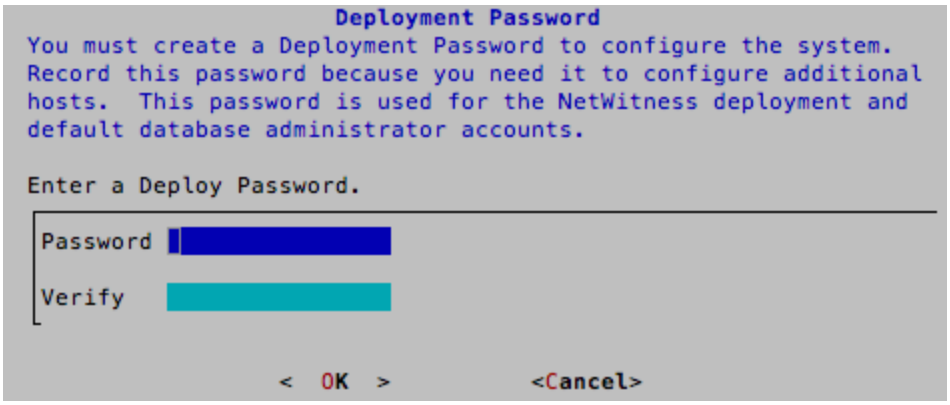
   1. Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.
      The **Master Password** prompt is displayed.
      The following list of characters are supported for Master Password and Deployment Password:

      - Symbols : ! @ # % ^ +
      - Numbers : 0-9
      - Lowercase Characters : a-z
      - Uppercase Characters : A-Z

      No ambiguous characters are supported for Master Password and Deployment Password. For example:
      space { } [ ] ( ) / \ ' " ` ~ ; : . < > -



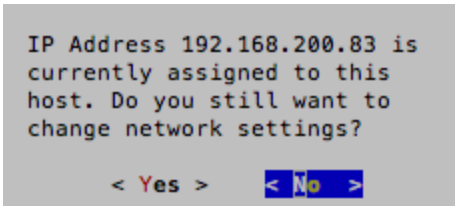
7. Down arrow to **Password** and type it in, down arrow to **Verify** and retype the password, Tab to **OK**, and press Enter.
   The **Deployment Password** prompt is displayed.



8. Type in the **Password**, down arrow to **Verify**, retype the password, Tab to **OK**, and press Enter.

One of the following conditional prompts is displayed.

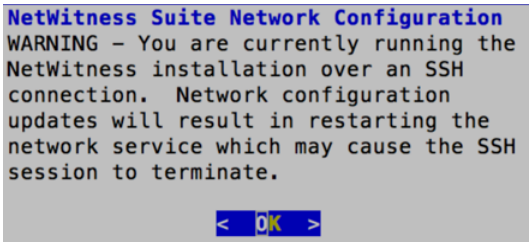
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



  Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** If you want to change the IP configuration found on the host.

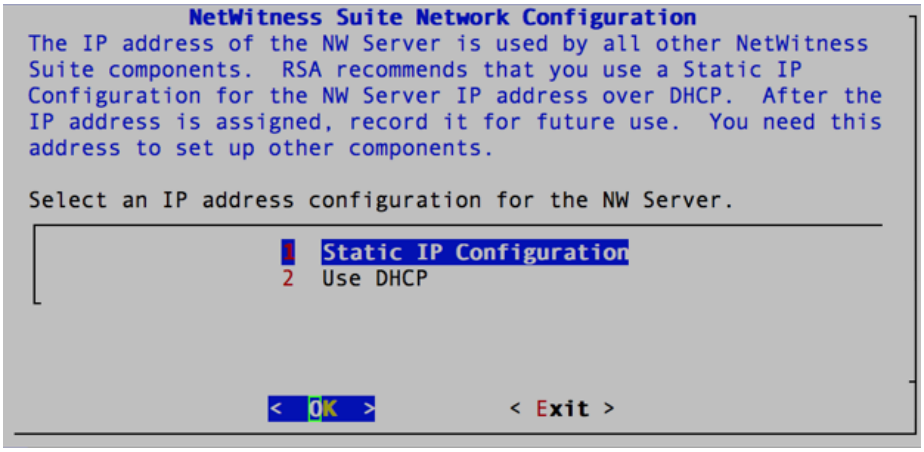
- If you are using an SSH connection, the following warning is displayed.

> **Note:** If you connect directly from the host console, the following warning will not be displayed.



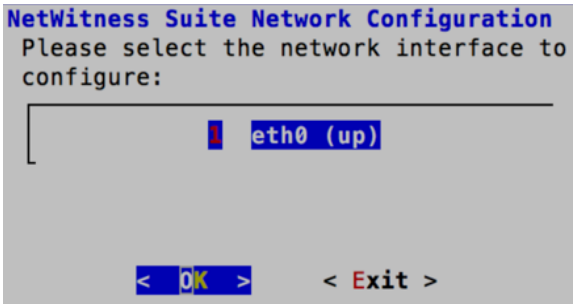
  Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If no IP configuration was found or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



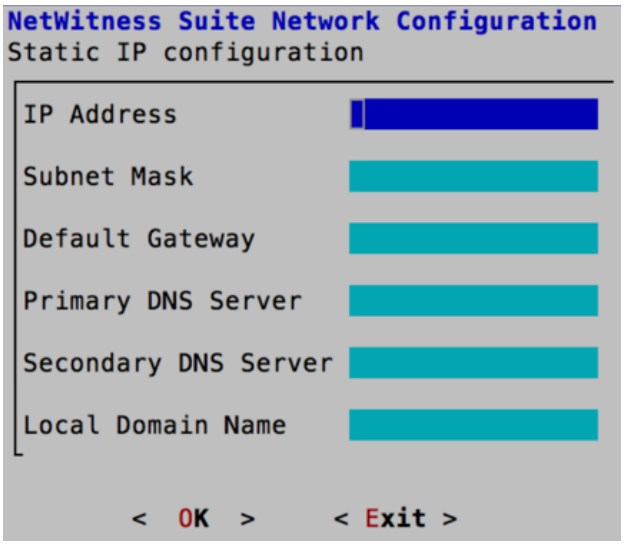
9. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

The **Network Configuration** prompt is displayed.



10. Down arrow to the network interface you want, Tab to **OK**, and press **Enter**. If you do not want to continue, Tab to **Exit**

    The **Static IP Configuration** prompt is displayed.



11. Type the configuration values (using the down arrow to move from field to field), Tab to **OK**, and press **Enter**.

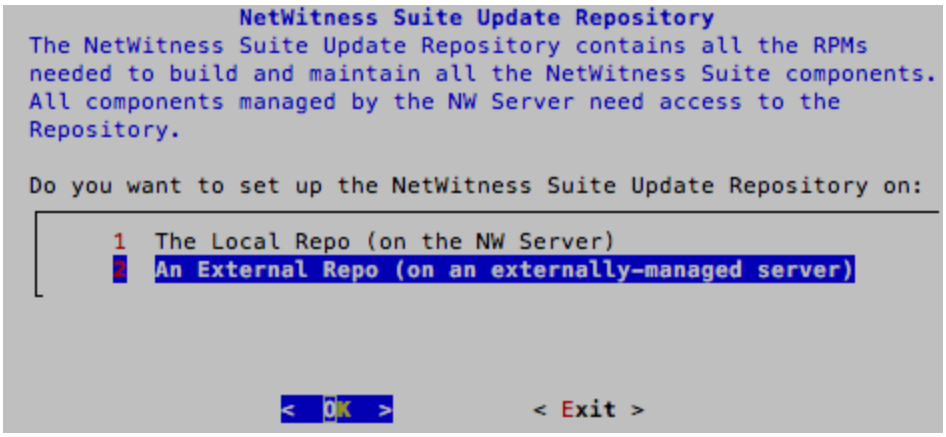
    If you do not complete all the required fields, an an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required.)

    If you use the wrong syntax or character length for any of the fields, an Invalid <field-name> error message is displayed.

    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the install.

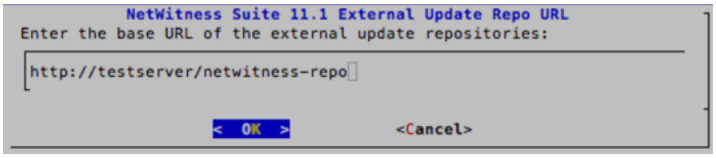
    The **Update Repository** prompt is displayed.

12. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.



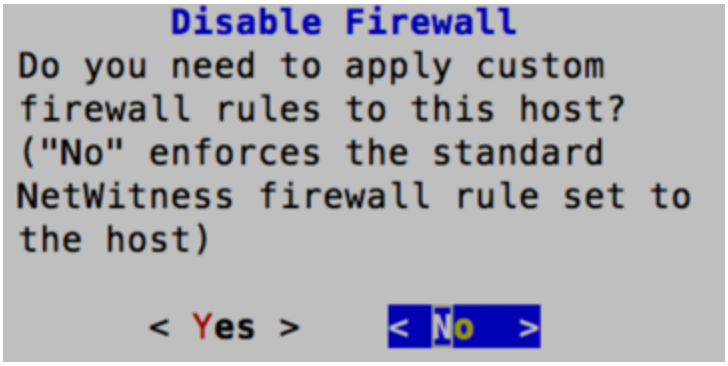
The **External Update Repo URl** prompt is displayed.
Refer to Appendix A. Create External Repository for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.1 to find NetWitness Suite 11.1 documents.

13. Enter the base URL of the NetWitness Suite external repo (for example, **http:/testserver/netwitness-repo**) and click **OK**.

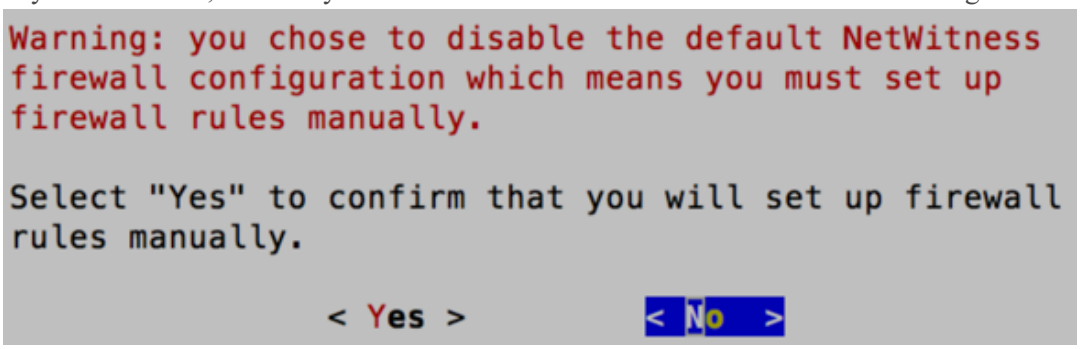


The **Disable** or use standard **Firewall** configuration prompt is displayed.

14. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

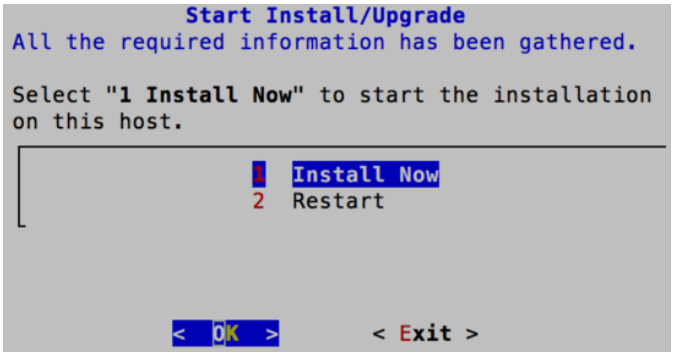


- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



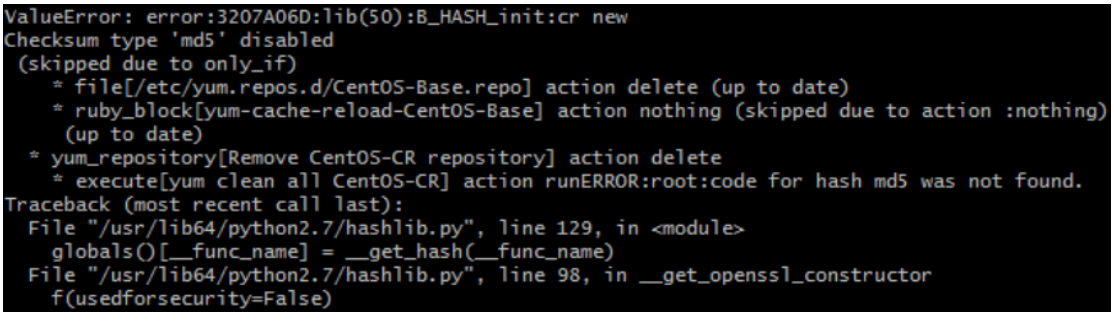
The **Start Install/Upgrade** prompt is displayed.

15. Press **Enter** to install 11.1.0.0 on the non-NW Server (**Install Now** is the default value).



When **Installation complete** is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.



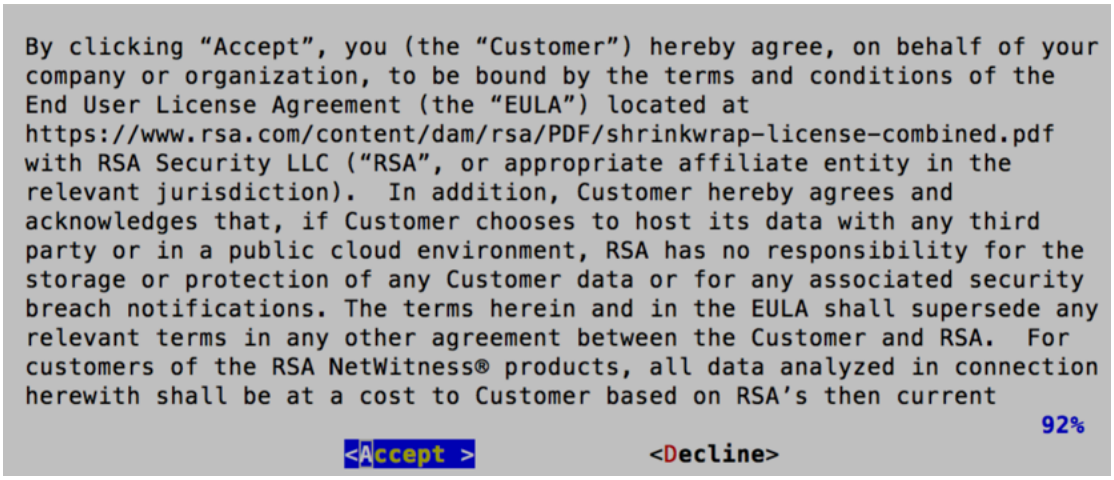
Task 2 - Install 11.1 for on Other Component Hosts

For a functional service, complete the following tasks on a non-NW Server host.

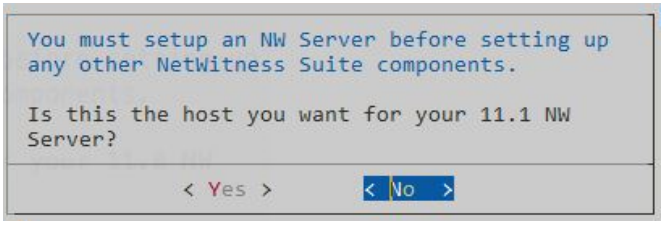
- Install the 11.1.0.0 environmental platform.
- Apply the 11.1.0.0 RPM files to the service from the NW Server Update Repository.

1. Deploy 11.1 OVA.
2. Run the `nwsetup-tui` command to set up the host..
   This initiates the Setup program and the EULA is displayed.

   Note: If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Optional) Task 1 - Re-Configure DNS Servers Post 11.1 in Post Installation Tasks.
   If you do not specify DNS Servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

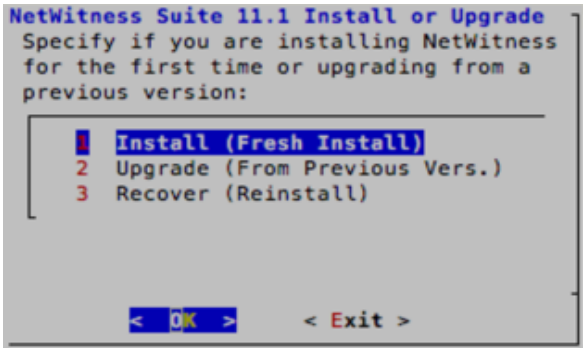
3. Tab to **Accept** and press Enter.
   The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

   Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete (steps 2 - 14) of Task 1- Install 11.1.0.0 on the NW Server Host to correct this error.

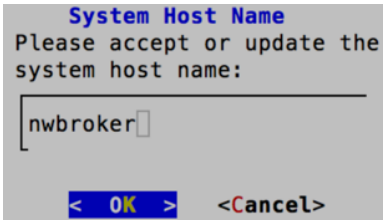
4. Press **Enter** (No).

   The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).



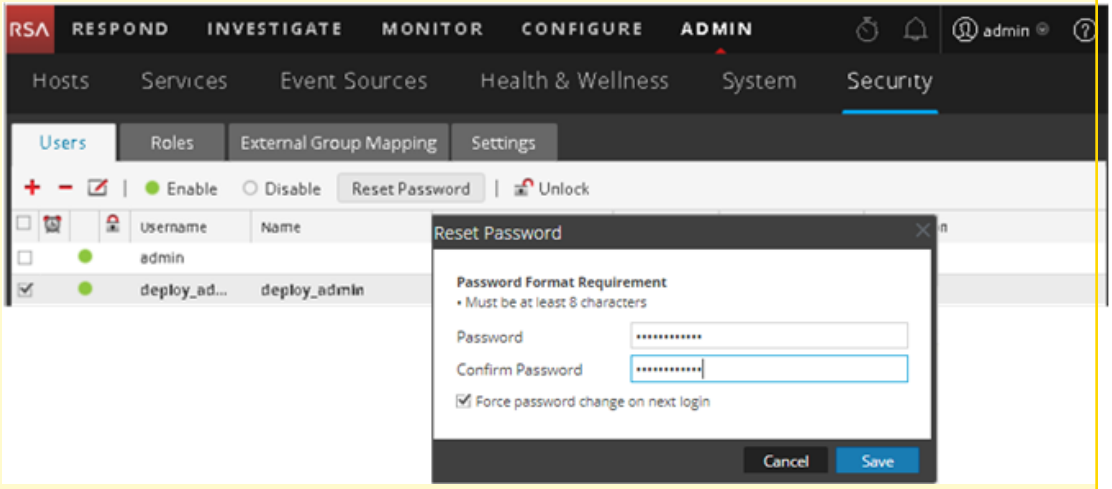
5. Press Enter. **Install (Fresh Install)** is selected by default).

   The **Host Name** prompt is displayed.



6. If want to keep this name, press **Enter**. If you want to change this name, edit it, tab to **OK**, and press **Enter**

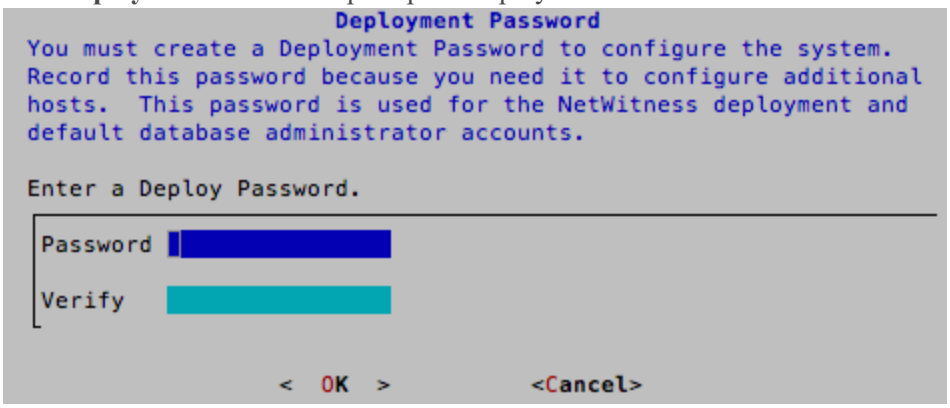
Caution: f you change the **deploy_admin** user password in the NetWitness Suite User Interface (**ADMIN**>**Security** >Select **deploy-admin - Reset password**),



you must:

1. SSH to the NW Server host.
2. Run the `(/opt/rsa/saTools/bin/set-deploy-admin-password` script.
3. Use the new password when installing any new non-NW Server hosts.
4. Run `(/opt/rsa/saTools/bin/set-deploy-admin-password` script on all non-NW Server hosts in your deployment.
5. Write down the password because you may need to refer to it later in the installation.

The **Deployment Password** prompt is displayed.

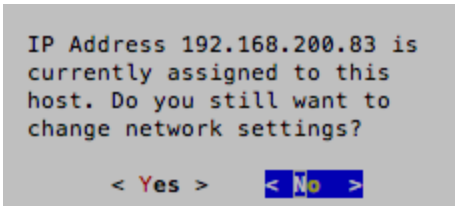


Note: You must use the same deployment password that you used when you installed the NW Server.

7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

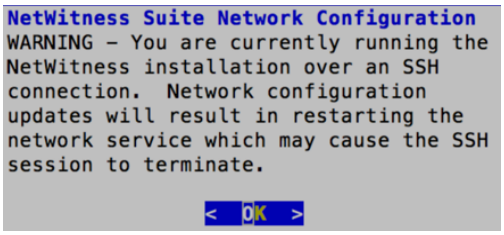
One of the following conditional prompts is displayed.

- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



  Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** If you want to change the IP configuration found on the host.

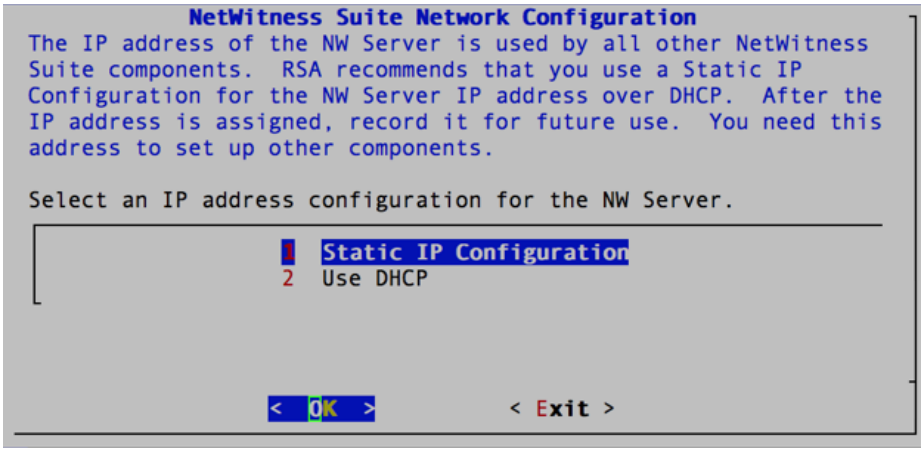
- If you are using an SSH connection, the following warning is displayed.



  Press **Enter** to close warning prompt.

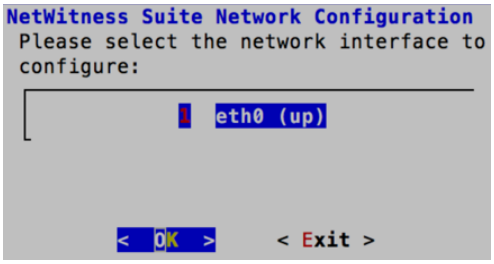
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 11 to and complete the installation.

- If no IP configuration was found or If you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



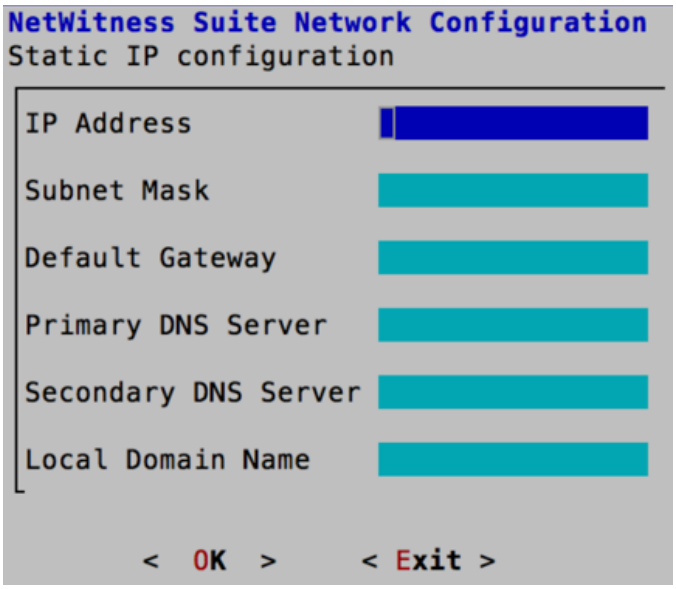
8. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to **2 Use DHCP** and press **Enter**.

The **Network Configuration** prompt is displayed.



9. Down arrow to the network interface you want, Tab to **OK**, and press **Enter**. If you do not want to continue, Tab to **Exit**

   The **Static IP Configuration** prompt is displayed.



10. Type the configuration values (using the down arrow to move from field to field), Tab to **OK**, and press **Enter**.

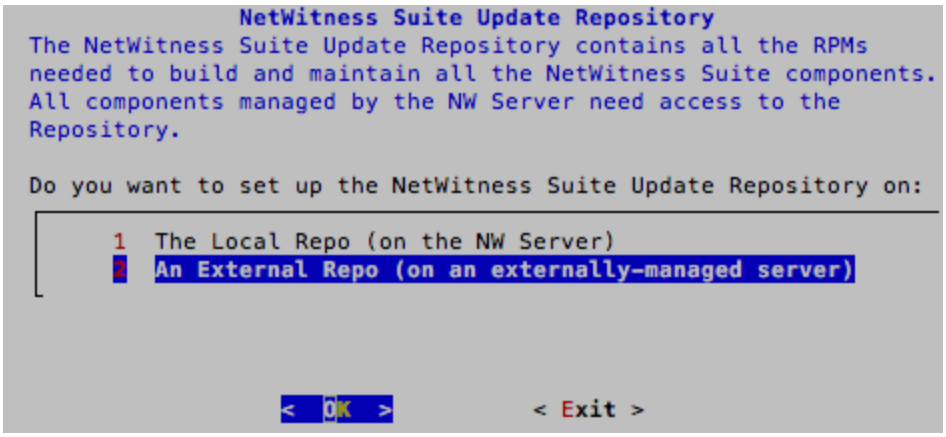
    If you do not complete all the required fields, an an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required.)

    If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

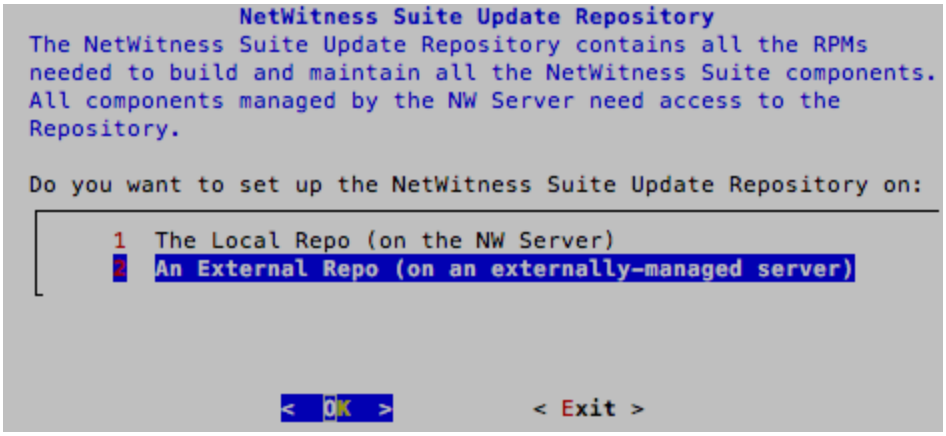
    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the install.

    The **Update Repository** prompt is displayed.

.



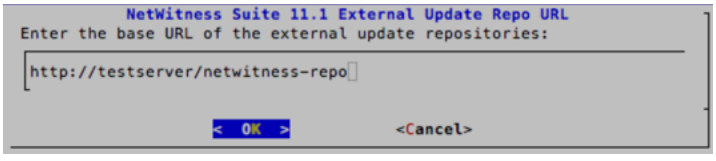
11. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, tab to **OK**, and press **Enter**.



The **External Update Repo URL** prompt is displayed.

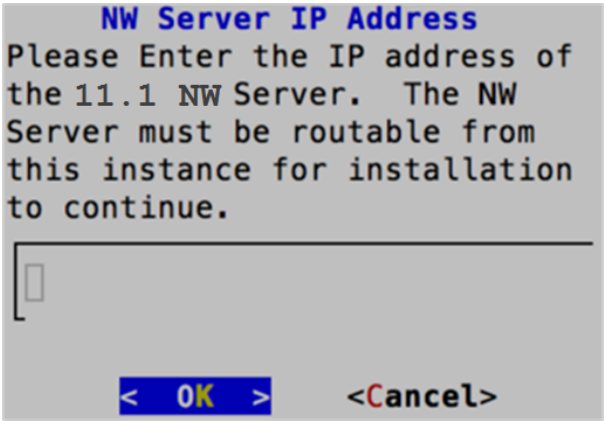
The repositories give you access RSA updates and CentOS updates.

12. Enter the base URL of the NetWitness Suite external repo (for example, **http://testserver/netwitness-repo**)and click **OK**. Refer to Appendix A. Create External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



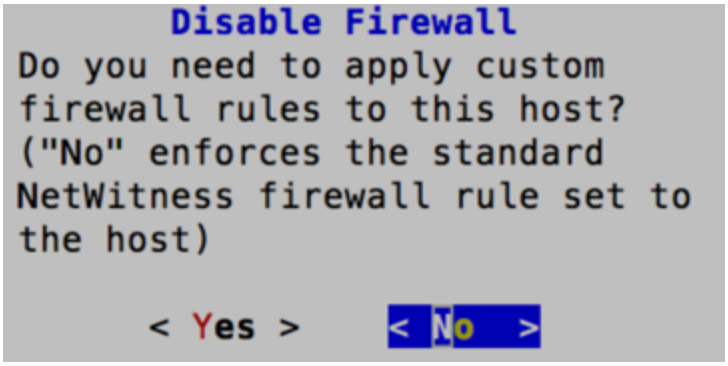
The **NW Server IP Address** is displayed.

13. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

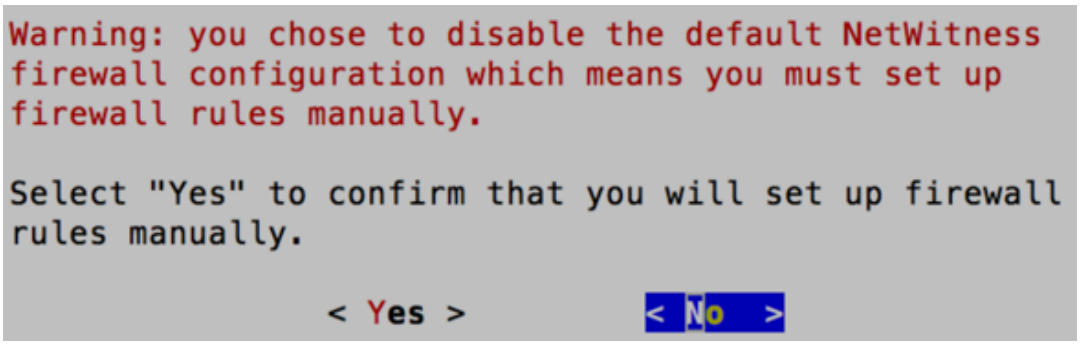


The **Disable** or use standard **Firewall** configuration prompt is displayed.

14. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.



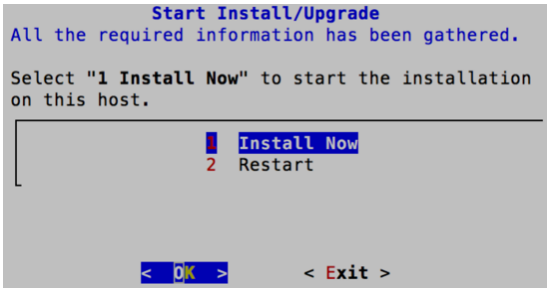
- If you select **Yes**, confirm your selection.



- If you select **No**, the standard firewall configuration is applied.

The **Start Install** prompt is displayed.

15. Press **Enter** to install 11.1.0.0 on the non-NW Server (**Install Now** is the default value).



When **Installation complete** is displayed, you have a generic host with an operating system compatible with NetWitness Suite 11.1.0.0.

16. Install a component service on the non-NW Server host.

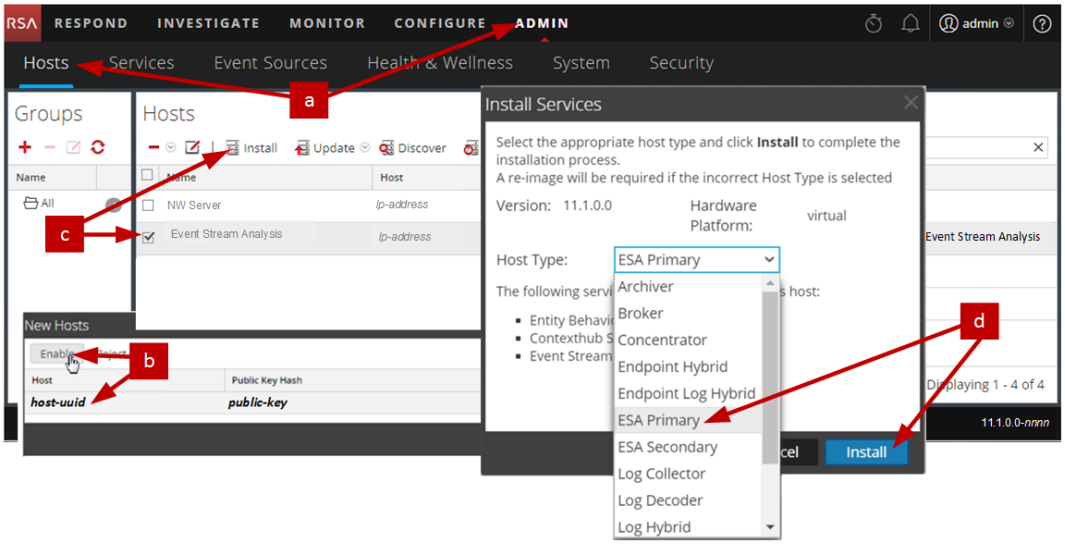
    a. Log into NetWitness Suite and click **ADMIN** > **Hosts**.
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

    Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

    b. Select the host in the **New Hosts** dialog and click **Enable**.
    The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

    c. Select that host (for example, **Event Stream Analysis**) and click Install.
    The **Install Services** dialog is displayed.

    d. Select the appropriate host type (for example, **ESA Primary**) in **Host Type** and click **Install**.



You have completed the installation of the non-NW Server host in NetWitness Suite.

17. Complete steps 1 through 16 for the rest of the NetWitness Suite non-NW Server components.

Step 3. Configure Databases to Accommodate NetWitness Suite

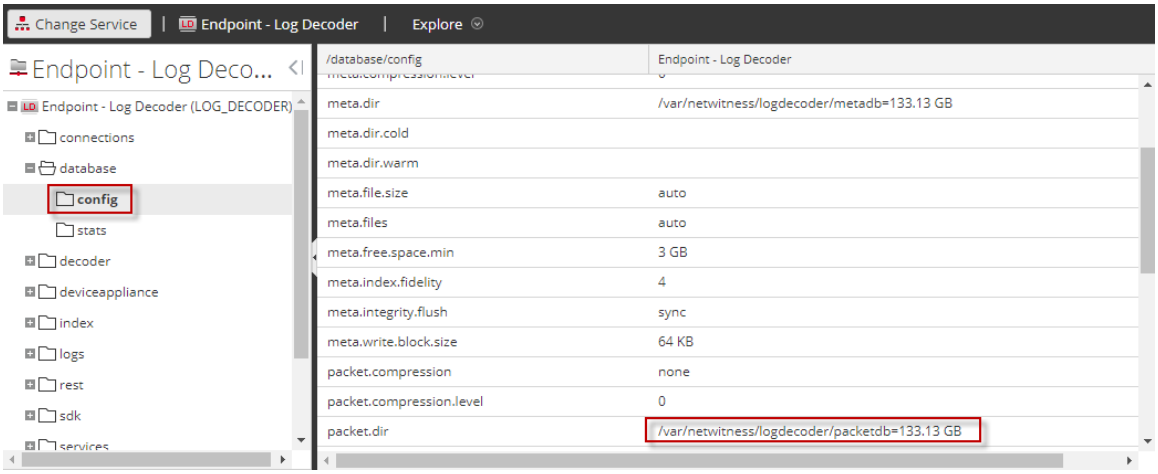
When you deploy databases from OVA, the initial database space allocation may not be adequate to support NetWitness Server. You need to review the status of the datastores after initial deployment and expand them.

Task 1. Review Initial Datastore Configuration

Review the datastore configuration after initial deployment to determine if you have enough drive space to accommodate the needs of your enterprise. As an example, this topic reviews the datastore configuration of the PacketDB on the Log Decoder host after you first deploy it from an Open Virtualization Archive (OVA) file.

Initial Space Allocated to PacketDB

The allocated space for the PacketDB is about 133.13 GB). The following NetWitness Suite Explore view example shows the size of the PacketDB after you initially deploy it from OVA.



Initial Database Size

By default, the database size is set to 95% of the size of file system on which the database resides. SSH to the Log Decoder host and enter the `df -k` command string to view the files system and its size. The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# df -kh
Filesystem                              Size  Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root         30G  3.0G   27G  10% /
devtmpfs                                 16G     0   16G   0% /dev
tmpfs                                    16G   12K   16G   1% /dev/shm
tmpfs                                    16G   25M   16G   1% /run
tmpfs                                    16G     0   16G   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome      10G   33M   10G   1% /home
/dev/mapper/netwitness_vg00-varlog       10G   42M   10G   1% /var/log
/dev/mapper/netwitness_vg00-nwhome      141G  396M  140G   1% /var/netwitness
/dev/sda1                              1014M   73M  942M   8% /boot
tmpfs                                    3.2G     0  3.2G   0% /run/user/0
[root@LogDecoder ~]#
```

PacketDB Mount Point

The database is mounted on the `packetdb` logical volume in `netwitness_vg00` volume group. `netwitness_vg00` and this is where you start your expansion planning for the file system.

Initial Status of netwitness_vg00

Complete the following steps to review the status of `netwitness_vg00`.

1. SSH to the Log Decoder host.
2. Enter the `lvs` (Logical Volumes Show) command string to determine which logical volumes are grouped in `netwitness_vg00`.

   `[root@nwappliance32431 ~}# lvs netwitness_vg00.`

   The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# vgs
  VG             #PV #LV #SN Attr   VSize    VFree
  netwitness_vg00   1   5   0 wz--n- <194.31g 100.00m
```

3. Enter the pvs (Physical Volumes Show) command string to determine which physical volumes belong to a specific group.

   `[root@nwappliance32431 ~}# pvs`

   The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# pvs
  PV         VG             Fmt  Attr PSize    PFree
  /dev/sda2  netwitness_vg00 lvm2 a--  <194.31g 100.00m
```

4. Enter the `vgs` (Volume Groups Show) command string to display the total size of specific volume group.

   `[root@nwappliance32431 ~}# vgs`

   The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# vgs
  VG              #PV #LV #SN Attr   VSize    VFree
  netwitness_vg00   1   5   0 wz--n- <194.31g 100.00m
```

Task 2. Review Optimal Datastore Space Configuration

You need to review the datastore space configuration options for the different hosts to get the optimal performance from your virtual NetWitness Suite deployment. Datastores are required for virtual host configuration, and the correct size is dependent on the host.

Note: (1.) Refer to the "**Optimization Techniques**" topic in the RSA NetWitness SuiteCore Database Tuning Guide for recommendations on how to optimize datastore space. (2.) Contact Customer Care for assistance in configuring your virtual drives and using the Sizing & Scoping Calculator.

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts. Additional partitioning and sizing examples for both packet capture and log ingest environments are provided at the end of this topic.

Decoder			
Persistent Datastores	**Cache Datastore**		
PacketDB	**SessionDB**	**MetaDB**	**Index**
100% as calculated by Sizing & Scoping Calculator	6 GB per 100Mb/s of traffic sustained provides 4 hours cache	60 GB per 100Mb/s of traffic sustained provides 4 hours cache	3 GB per 100Mb/s of traffic sustained provides 4 hours cache

Concentrator		
Persistent Datastores	**Cache Datastores**	
MetaDB	**SessionDB** **Index**	**Index**

Concentrator		
Calculated as 10% of the PacketDB required for a 1:1 retention ratio	30 GB per 1TB of PacketDB for standard multi protocol network deployments as seen at typical internet gateways	5% of the calculated MetaDB on the Concentrator. Preferred High Speed Spindles or SSD for fast access

Log Decoder			
Persistent Datastores	**Cache Datastores**		
PacketDB	**SessionDB**	**MetaDB**	**Index**
100% as calculated by Sizing & Scoping Calculator	1 GB per 1000 EPS of traffic sustained provides 8 hours cache	20 GB per 1000 EPS of traffic sustained provides 8 hours cache	0.5 GB per 1000 EPS of traffic sustained provides 4 hours cache

Log Concentrator		
Persistent Datastores	Cache Datastores	
MetaDB	SessionDB Index	Index
Calculated as 100% of the PacketDB required for a 1:1 retention ratio	3 GB per 1000 EPS of sustained traffic per day of retention	5% of the calculated MetaDB on the Concentrator. Preferred High Speed Spindles or SSD for fast access

Task 3. Add New Volume and Extend Existing File Systems

After reviewing your initial datastore configuration, you may determine that you need to add a new volume. This topic uses a Virtual Packet/Log Decoder host as an example.

Complete these tasks in the following order.

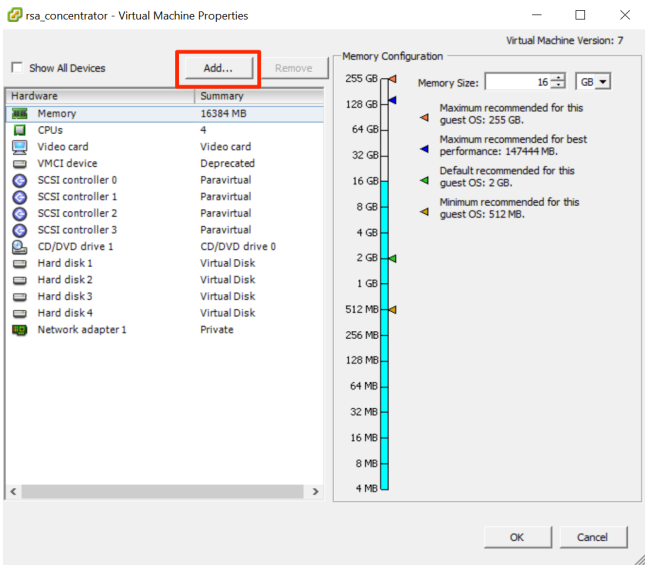
1. Add New Disk
2. Create New Volumes on the New Disk
3. Create LVM Physical Volume on New Partition
4. Extend Volume Group with Physical Volume
5. Expand the File System
6. Start the Services
7. Make Sure the Services Are Running
8. Reconfigure LogDecoder Parameters

Add New Disk

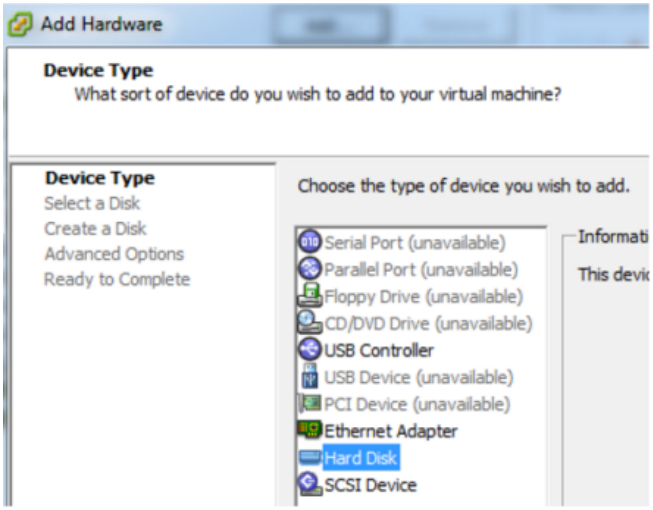
This procedure shows you how to add a new 100GB disk on the same datastore.

Note: The procedure to add a disk on different datastore is similar to the procedure shown here.

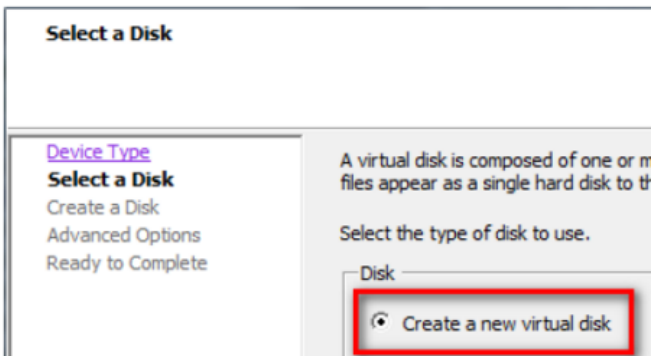
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



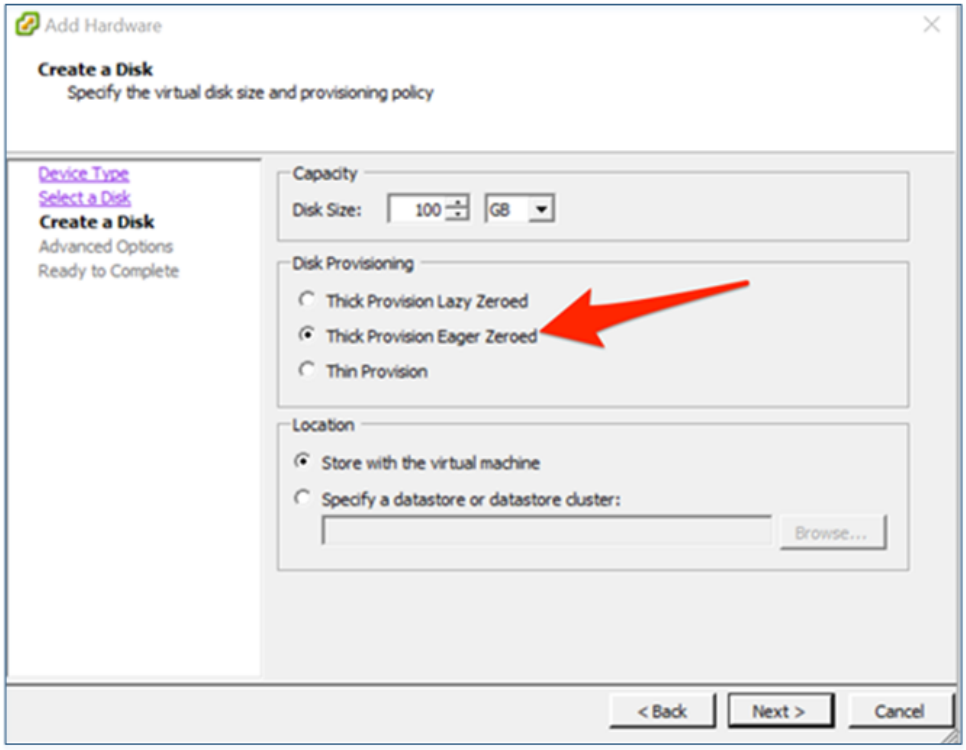
2. Select **Hard Disk** as the device type.



3. Select **Create a new virtual disk**.

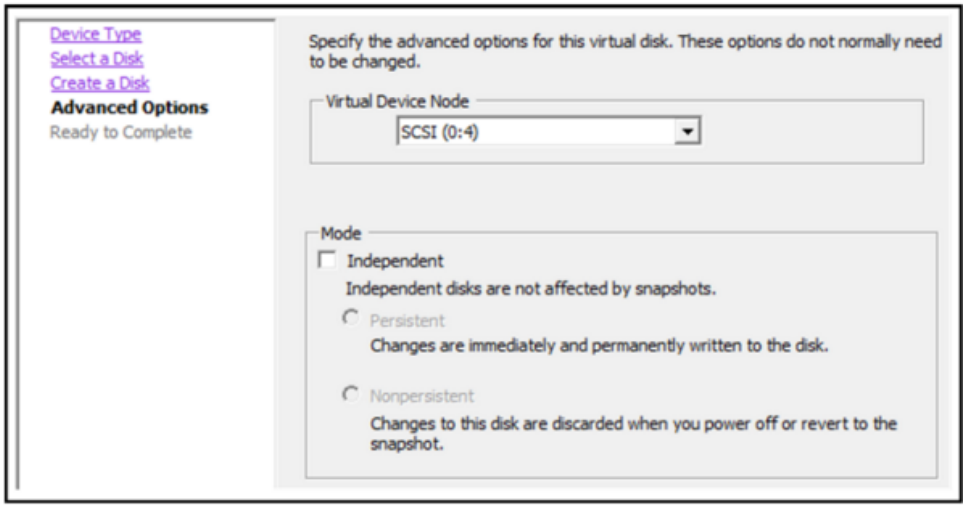


4. Choose the size of the new disk and where you want to create it (on the same datastore or a different datastore).



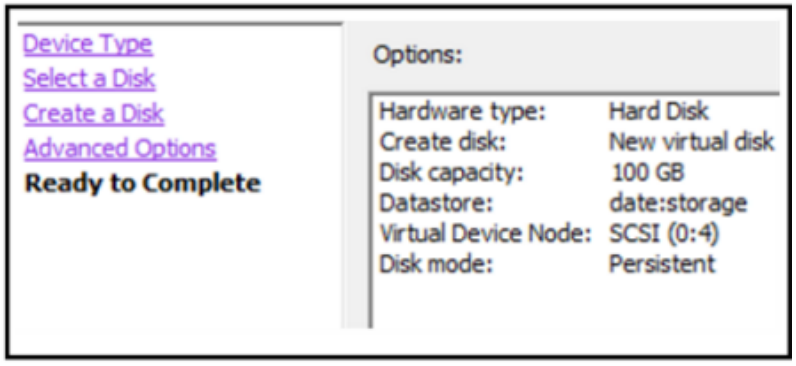
Caution: Allocate all the space for performance reasons.

5. Approve the proposed Virtual Device Node.



Note: The Virtual Device Node can vary, but it is pertinent to `/dev/sdX` mappings.

6. Confirm the settings.



7. Start virtual machine.
8. SSH to the machine.
9. Restart the machine and enter the following command.

   `lsblk`

   The following output is displayed showing the new disk.

```
[root@NWAPPLIANCE2599 database]# lsblk
NAME                          MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0                             2:0    1     4K  0 disk
sda                             8:0    0 195.3G  0 disk
├─sda1                          8:1    0     1G  0 part /boot
└─sda2                          8:2    0 194.3G  0 part
  ├─netwitness_vg00-nwhome    253:15   0 140.2G  0 lvm  /var/netwitness
  ├─netwitness_vg00-varlog    253:16   0    10G  0 lvm  /var/log
  ├─netwitness_vg00-usrhome   253:17   0    10G  0 lvm  /home
  ├─netwitness_vg00-root      253:18   0    30G  0 lvm  /
  └─netwitness_vg00-swap      253:19   0     4G  0 lvm  [SWAP]
sdb                             8:16   0    48G  0 disk
└─sdb1                          8:17   0    48G  0 part
  ├─VolGroup00-usr            253:6    0     4G  0 lvm
  ├─VolGroup00-usrhome        253:7    0     2G  0 lvm
  ├─VolGroup00-var            253:8    0     4G  0 lvm
  ├─VolGroup00-log            253:9    0     4G  0 lvm
  ├─VolGroup00-tmp            253:10   0     6G  0 lvm
  ├─VolGroup00-vartmp         253:11   0     2G  0 lvm
  ├─VolGroup00-opt            253:12   0     4G  0 lvm
  ├─VolGroup00-rabmq          253:13   0    10G  0 lvm
  └─VolGroup00-nwhome         253:14   0    12G  0 lvm
sdc                             8:32   0   104G  0 disk
└─sdc1                          8:33   0   104G  0 part
  ├─VolGroup01-decoroot       253:0    0    20G  0 lvm  /var/netwitness/logdecoder
  ├─VolGroup01-index          253:1    0    10G  0 lvm  /var/netwitness/logdecoder/index
  ├─VolGroup01-sessiondb      253:2    0    30G  0 lvm  /var/netwitness/logdecoder/sessiondb
  └─VolGroup01-metadb         253:3    0    44G  0 lvm  /var/netwitness/logdecoder/metadb
sdd                             8:48   0   168G  0 disk
└─sdd1                          8:49   0   168G  0 part
  ├─VolGroup01-logcoll        253:4    0    64G  0 lvm  /var/netwitness/logcollector
  └─VolGroup01-packetdb       253:5    0   104G  0 lvm  /var/netwitness/logdecoder/packetdb
sde                             8:64   0    10G  0 disk
sr0                            11:0    1  1024M  0 rom
[root@NWAPPLIANCE2599 database]#
```

Note: 1.) You receive an **unknown partition table** error because the new disk has not been initialized. 2.) The **sd 2:0:4:0** pertains to the **SCSI:0:4** Virtual Device Node that appeared when you added the new device. 3.) The new disk device is **sde** (or `/dev/sde`).

10. Enter the following command string to stop the service.

    `root@LogDecoderGM ~] # service nwlogcollector stop; service nwlogdecoder stop`.

    This procedure uses the Log Decoder as an example.

    If you wanted to stop services on a Concentrator, you would enter:

    `service nwconcentrator stop`

    If you wanted to stop services on a Packet Decoder, you would enter:

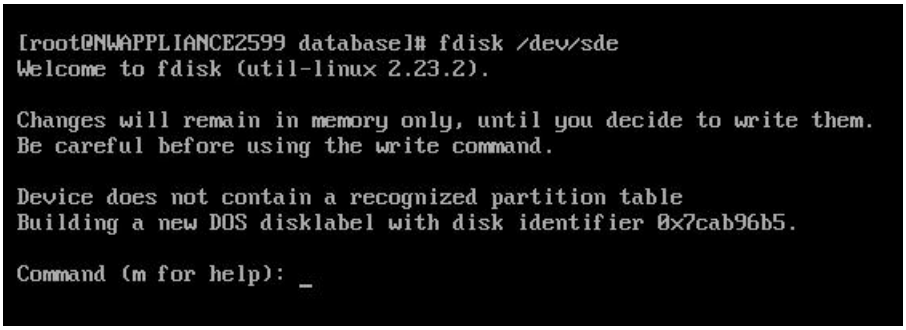
    `service nwdecoder stop`

Create Volumes on New Disk

1. SSH to the LogDecoder host.
2. Create a partition on the new disk and change its type to Linux LVM.

   `[root@NWAPPLIANCE2599 ~]# fdisk /dev/sde`

   The following information and prompt is displayed.



3. Type `p`.

   The following information is displayed.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System

Command (m for help):
```

The default partition type is **Linux (83)**. You need to change it to Linux **LVM (8e)**.

4. Type `n`.

   The following prompt is displayed.

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help): _
```

Partition 1 of type Linux and of size 10 GB is set

1. At the `Command m for help:` prompt type `t`.

   The following information and prompt is displayed.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help):
```

2. Type `8e`.

   The following information and prompt is displayed.

```
Changed system type of partition 1 to 8e (Linux LVM).

Command (m for help):
```

3. Type `p`.

The following information is displayed.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1            2048    20971519    10484736   8e  Linux LVM

Command (m for help):
```

4. At `Command (m for help):` prompt type `w`.

   The new partition table is written to the disk and fdisk quits to root shell.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
[ 9838.504920]  sde: sde1
Syncing disks.
[root@NWAPPLIANCE2599 database]# _
```

   The new `/dev/sde1` partition is created on the new disk.

5. Complete one of the following steps to verify that the new partition exists.

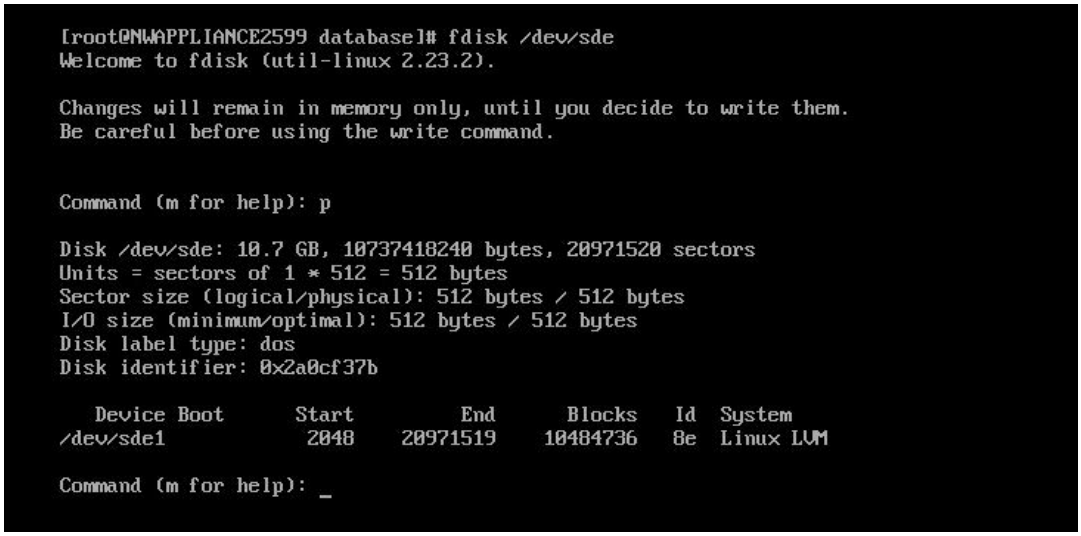
   - Type `dmesg | tail`.

     The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# dmesg | tail
[  773.090059] XFS (dm-2): Mounting V4 Filesystem
[  773.214176] XFS (dm-2): Ending clean mount
[  785.595678] XFS (dm-3): Mounting V4 Filesystem
[  785.758078] XFS (dm-3): Ending clean mount
[  802.874171] XFS (dm-4): Mounting V4 Filesystem
[  803.028083] XFS (dm-4): Starting recovery (logdev: internal)
[  803.041709] XFS (dm-4): Ending recovery (logdev: internal)
[  813.249001] XFS (dm-5): Mounting V4 Filesystem
[  813.439422] XFS (dm-5): Ending clean mount
[ 9838.504920]  sde: sde1
[root@NWAPPLIANCE2599 database]#
```

   - Type `fdisk /dev/sde`.
   - Type `p`.

The following information is displayed.

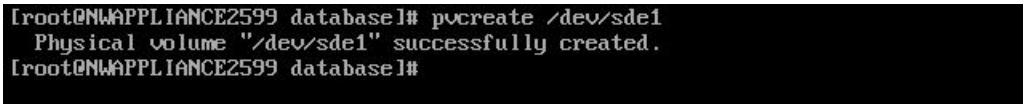


Create LVM Physical Volume on New Partition

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

   ```
   [root@LogDecoderGM ~]# pvcreate /dev/sde1
   ```

3. The following information is displayed.

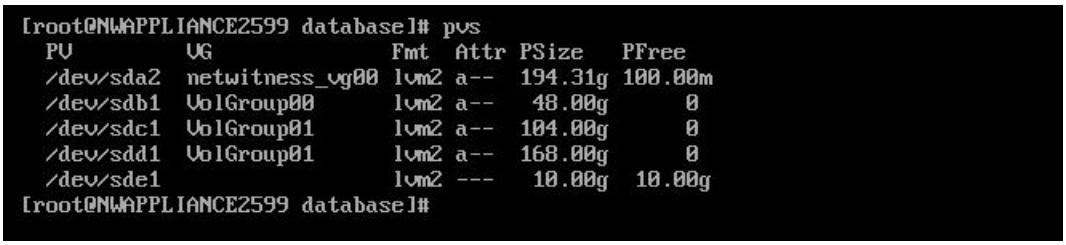


Extend Volume Group with Physical Volume

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

   ```
   [root@LogDecoderGM ~]# pvs
   ```

   The following information is displayed.



`netwitness_vg00` consists of `/dev/sdc1`and `/dev/sdd1` physical volumes (PV), and LVM system. Note that the new`/dev/sde1` volume has 10GB of free space.

3. To add the physical volume to `netwitness_vg00`.

   a. Enter `vgextend netwitness_vg00 /dev/sde1`.

      The following information is displayed.

      ```
      Volume group "netwitness_vg00" successfully extended
      ```

   b. Enter pvs.

      The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# vgextend netwitness_vg00 /dev/sde1
  Volume group "netwitness_vg00" successfully extended
[root@NWAPPLIANCE2599 database]# pvs
  PV         VG              Fmt  Attr PSize   PFree
  /dev/sda2  netwitness_vg00 lvm2 a--  194.31g 100.00m
  /dev/sdb1  VolGroup00      lvm2 a--   48.00g      0
  /dev/sdc1  VolGroup01      lvm2 a--  104.00g      0
  /dev/sdd1  VolGroup01      lvm2 a--  168.00g      0
  /dev/sde1  netwitness_vg00 lvm2 a--   10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

      The volume was added to `netwitness_vg00`, but it has not been extended yet (you still have 10GB of free space). There are several Logical Volumes in `netwitness_vg00`, in this example involves the PacketDB.

4. To extend the PacketDB logical volume so that it uses all of the 10GB of free space.

   a. Enter `lvs netwitness_vg00`.
   The following information is displayed

```
[root@NWAPPLIANCE2599 database]# lvs
  LV      VG              Attr       LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  nwhome  netwitness_vg00 -wi-ao---- 140.21g
  root    netwitness_vg00 -wi-ao----  30.00g
  swap    netwitness_vg00 -wi-ao----   4.00g
  usrhome netwitness_vg00 -wi-ao----  10.00g
  varlog  netwitness_vg00 -wi-ao----  10.00g
[root@LogDecoder ~]#
```

   b. Enter `lvextend -L+9.5G /dev/netwitness_vg00/nwhome`.

      The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# lvextend -L+9.5G /dev/netwitness_vg00/nwhome
  Size of logical volume netwitness_vg00/nwhome changed from 140.21 GiB (35894 extents) to 149.71 GiB (38326 extents).
  Logical volume netwitness_vg00/nwhome successfully resized.
[root@NWAPPLIANCE2599 database]#
```

   b. Enter`lvs netwitness_vg00`.

      The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# lvs netwitness_vg00
  LV      VG             Attr       LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  nwhome  netwitness_vg00 -wi-ao---- 149.71g
  root    netwitness_vg00 -wi-ao----  30.00g
  swap    netwitness_vg00 -wi-ao----   4.00g
  usrhome netwitness_vg00 -wi-ao----  10.00g
  varlog  netwitness_vg00 -wi-ao----  10.00g
[root@NWAPPLIANCE2599 database]#
```

The `packetdb` Logical Volume has been expanded to 149.71 GB, but the `/var/netwitness` filesystem still has 140.21 GB.

Expand the File System

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

   `[root@LogDecoderGM ~]# xfs_growfs /var/netwitness/`

   The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# xfs_growfs /var/netwitness/
meta-data=/dev/mapper/netwitness_vg00-nwhome isize=256    agcount=4, agsize=9188864 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=36755456, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=17947, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 36755456 to 39245824
[root@NWAPPLIANCE2599 database]# _
```

Start Services

Enter the following command string to start the services on the LogDecoder host.

```
[root@LogDecoderGM ~]# service nwlogcollector start; service
nwlogdecoder start
```

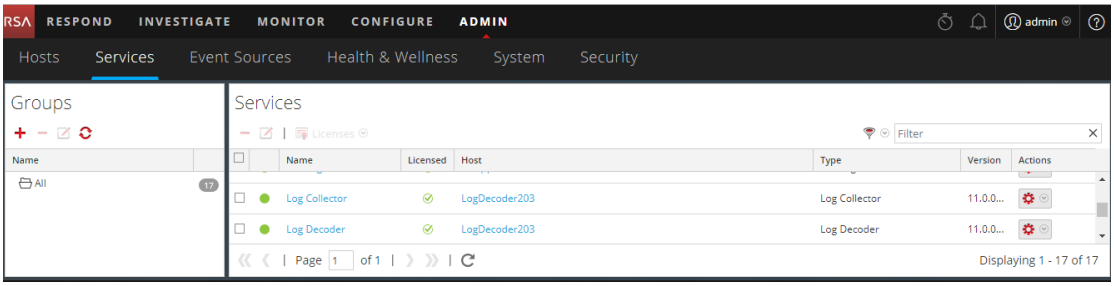
The following information is displayed.

```
nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069
```

Make Sure that the Services Are Running

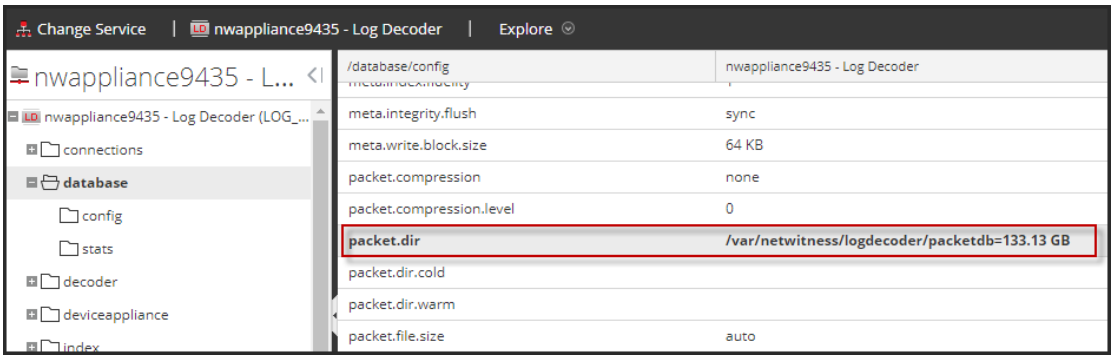
1. Log on to NetWitness Suite.
2. Click **Administration** > **Services**.

3. Make sure that the Log Collector and Log Decoder services are running.



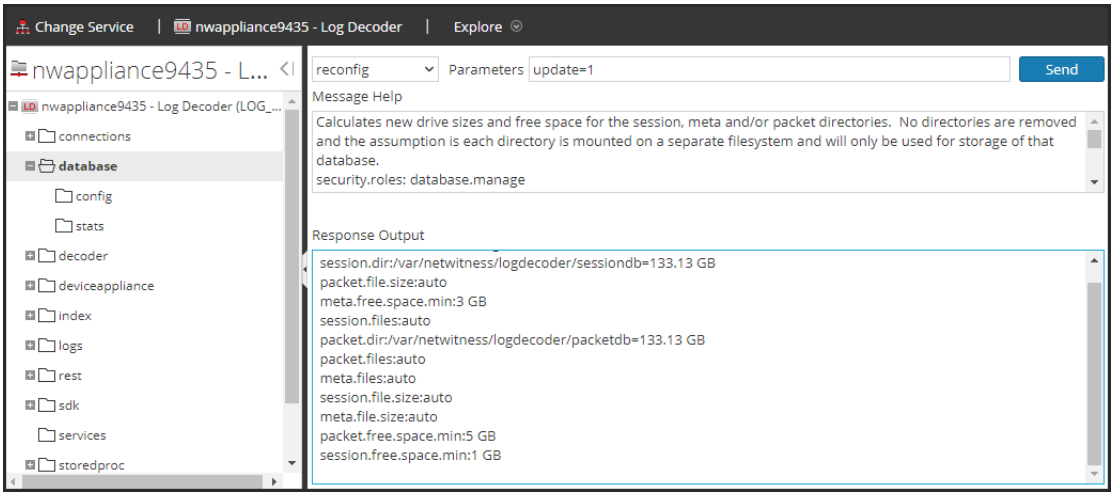
Reconfigure Log Decoder Parameters

1. Log on to NetWitness Suite.
2. Click **Administration** > **Services**.
3. Select the LogDecoder service.
4. Under actions, select View > Explore.
5. Click `database > config > packet.dir`.

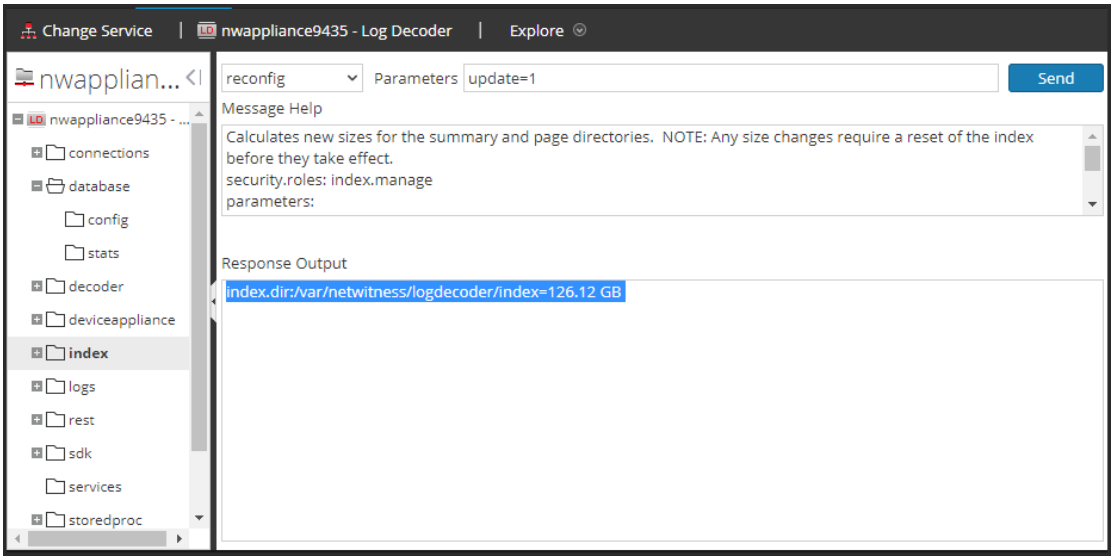


6. Right-click `database`, click **Properties**, select the **reconfig** command, specify **update=1** in **Parameters**, and click **Send**.

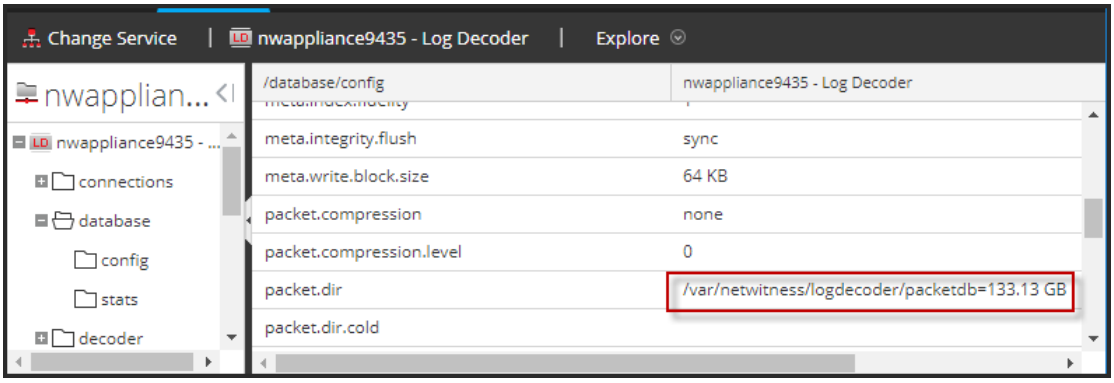
The `packetdb`parameter value changed from 98.74 GB to 133.13 GB.



7. Right-click `index`, click **Properties**, select the **reconfig** command, specify **update=1** in **Parameters**, and click **Send**.



8. Close the Properties dialog to return to the Explore view. The `packet.dir` parameter value is now 133.13 GB (95% of 203 GB).



Step 4. Configure Host-Specific Parameters

Certain application-specific parameters are required to configure log ingest and packet capture in the Virtual Environment.

Configure Log Ingest in the Virtual Environment

Log ingest is easily accomplished by sending the logs to the IP address you have specified for the Decoder. The Decoder's management interface allows you to then select the proper interface to listen for traffic on if it has not already selected it by default.

Configure Packet Capture in the Virtual Environment

There are two options for capturing packets in a VMWare environment. The first is setting your vSwitch in promiscuous mode and the second is to use a third-party Virtual Tap.

Set a vSwitch to Promiscuous Mode

The option of putting a switch whether virtual or physical into promiscuous mode, also described as a SPAN port (Cisco services) and port mirroring, is not without limitations. Whether virtual or physical, depending on the amount and type of traffic being copied, packet capture can easily lead to over subscription of the port, which equates to packet loss. Taps, being either physical or virtual, are designed and intended for loss less 100% capture of the intended traffic.

Promiscuous mode is disabled by default, and should not be turned on unless specifically required. Software running inside a virtual machine may be able to monitor any and all traffic moving across a vSwitch if it is allowed to enter promiscuous mode as well as causing packet loss due to over subscription of the port..

To configure a portgroup or virtual switch to allow promiscuous mode:

1. Log on to the ESXi/ESX host or vCenter Server using the vSphere Client.
2. Select the ESXi/ESX host in the inventory.
3. Select the **Configuration** tab.
4. In the **Hardware** section, click **Networking**.
5. Select **Properties** of the virtual switch for which you want to enable promiscuous mode.
6. Select the virtual switch or portgroup you want to modify, and click **Edit**.
7. Click the **Security** tab. In the **Promiscuous Mode** drop-down menu, select **Accept**.

Use of a Third-Party Virtual Tap

Installation methods of a virtual tap vary depending on the vendor. Please refer to the documentation from your vendor for installation instructions. Virtual taps are typically easy to integrate, and the user interface of the tap simplifies the selection and type of traffic to be copied.

Virtual taps encapsulate the captured traffic in a GRE tunnel. Depending on the type you choose, either of these scenarios may apply:

- An external host is required to terminate the tunnel, and the external host directs the traffic to the Decoder interface.
- The tunnel send traffic directly to the Decoder interface, where NetWitness Suite handles the de-encapsulation of the traffic.

Step 5. Post Installation Tasks

This topic contains the task you complete after you install 11.1.

- General
- RSA NetWitness® Endpoint Insights

General

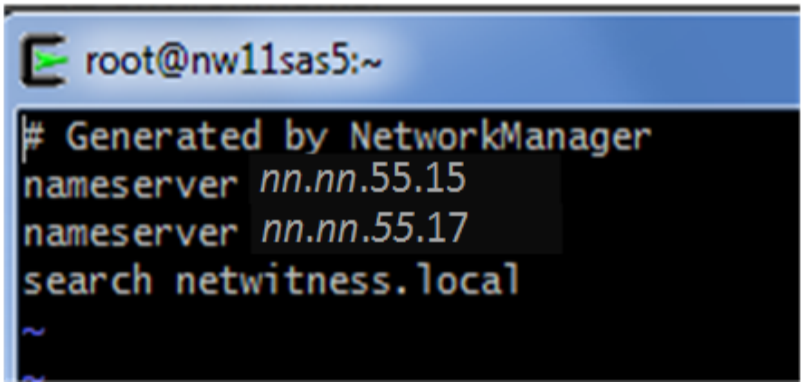
(Optional) Task 1 - Re-Configure DNS Servers Post 11.1

Complete the following steps to re-configure the DNS servers in NetWitness Suite 11.1.

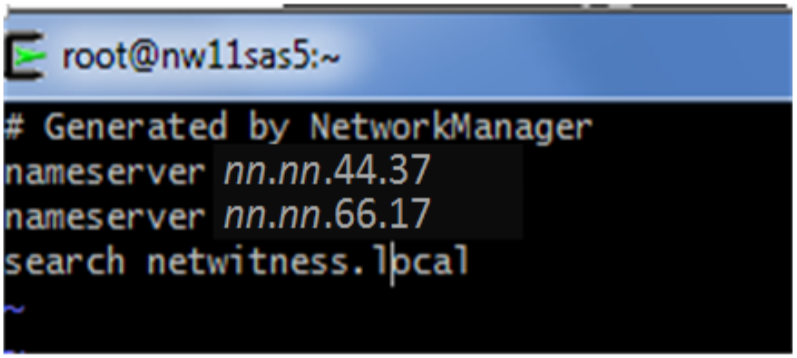
1. Login to the server host with your `root` credentials.
2. Edit the `/etc/resolv.conf` file:
   a. Replace the IP address corresponding to `nameserver`.
   If you need to replace both DNS servers , replace the IP entries for both the hosts with

valid addresses.

The following example shows both DNS entries.



The following example shows the new DNS values.



b. Save the `/etc/resolv.conf` file.

RSA NetWitness® Endpoint Insights

(Optional) Task 2 - Install Endpoint Hybrid or Endpoint Log Hybrid

You must install one of the following services to install NetWitness Suite Endpoint Insights in your deployment:

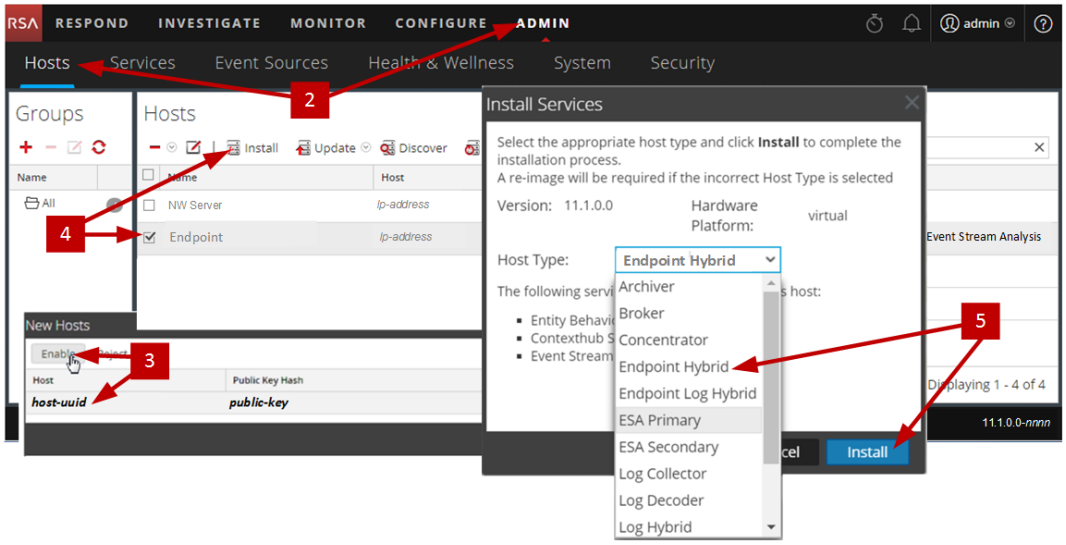
Caution: You can only install one instance of the following services in your deployment.

- Endpoint Hybrid
- Endpoint Log Hybrid

1. Complete steps 1 - 14 in Task 2 - Install 11.1 on Other Component Hosts.
2. Log into NetWitness Suite and click **ADMIN** > **Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.

3. Select the host in the **New Hosts** dialog and click **Enable**.
   The New Hosts dialog closes and the host is displayed in the Hosts view.
4. Select that host in the **Hosts** view (for example, **Endpoint**) and click Install.
   The Install Services dialog is displayed.
5. Select the appropriate service, either **Endpoint Hybrid** or **Endpoint Log Hybrid**, and click **Install**.
   Endpoint Hybrid is used as an example in the following screen shot.



6. Make sure that all Endpoint Hybrid or Endpoint Log Hybrid services are running.
7. Register the Endpoint server host IP address with the NW Server.
   a. SSH to the NW Server.
   b. Go to the `/opt/rsa/saTools/bin` directory.
      `cd /opt/rsa/saTools/bin`
   c. Run the `register-endpoint` script specifying the Endpoint host IP address.
      `./register-endpoint-ip -v --host-addr <ip-address>`

      Note: The script takes a few minutes to update the Endpoint Server IP address.
8. Configure Endpoint Meta forwarding.
   See *Endpoint Insights Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.Go to the Master Table of Contents for NetWitness Logs & Packets

11.1 to find NetWitness Suite 11.1 documents.

9. Install the Endpoint Insights Agent.
   See *Endpoint Insights Agent Installation Guide* for detailed instructions on how to install the agent. Go to the Master Table of Contents for NetWitness Logs & Packets 11.1 to find NetWitness Suite 11.1 documents.

Appendix A. Create External Repository

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. Log in to the web server host
2. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo`under `web-root` of the web server. For example, /var/netwitness is the web-root, submit the following command string.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0`directory.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`)and some other files.
6. Unzip the:
   a. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

b. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (nwsetup-tui) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD

RSA NETWITNESS® SUITE

Build Stick Instructions

for Version 11.x

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Create Host Build Stick **4**

Resources Required 4

Automated Tool to Create Build Stick 4

Build Stick Installation Media 4

NetWitness Suite ISO Files 4

Create a NetWitness Suite USB Build Stick 5

Revision History **8**

Create Host Build Stick

These instructions tell you how to image an RSA NetWitness Suite host with the NetWitness Suite software image.

Resources Required

You need the following tools to complete these instructions.

- Automated tool to create a build stick [for example Universal Netboot (UNetbootin) installer tool]
- NetWitness Suite USB file
- USB drive with 8GB capacity

Automated Tool to Create Build Stick

You can use an automated tool to create the build stick. The UNetbootin tool is used in the examples in this document.

Note: Make sure that you have all of the resources listed above before starting the process.

Build Stick Installation Media

Installation media is in the form of ISO files, which are available for download from Download Central (https://download.rsasecurity.com). As part of your order fulfillment, RSA gives you access to the ISO files that pertain to each customer order.

NetWitness Suite ISO Files

The `rsa-<release number>.<build-number>.<OS number>-usb.iso` is the file naming convention for ISO files. When installing software on your NetWitness Suite host, make sure you are using the correct release. This document uses `rsa-11.x.x.x.<build-number>.el7-usb.iso` as an example of an ISO file.

Contact Customer Care at nwsupport@rsa.com for assistance.

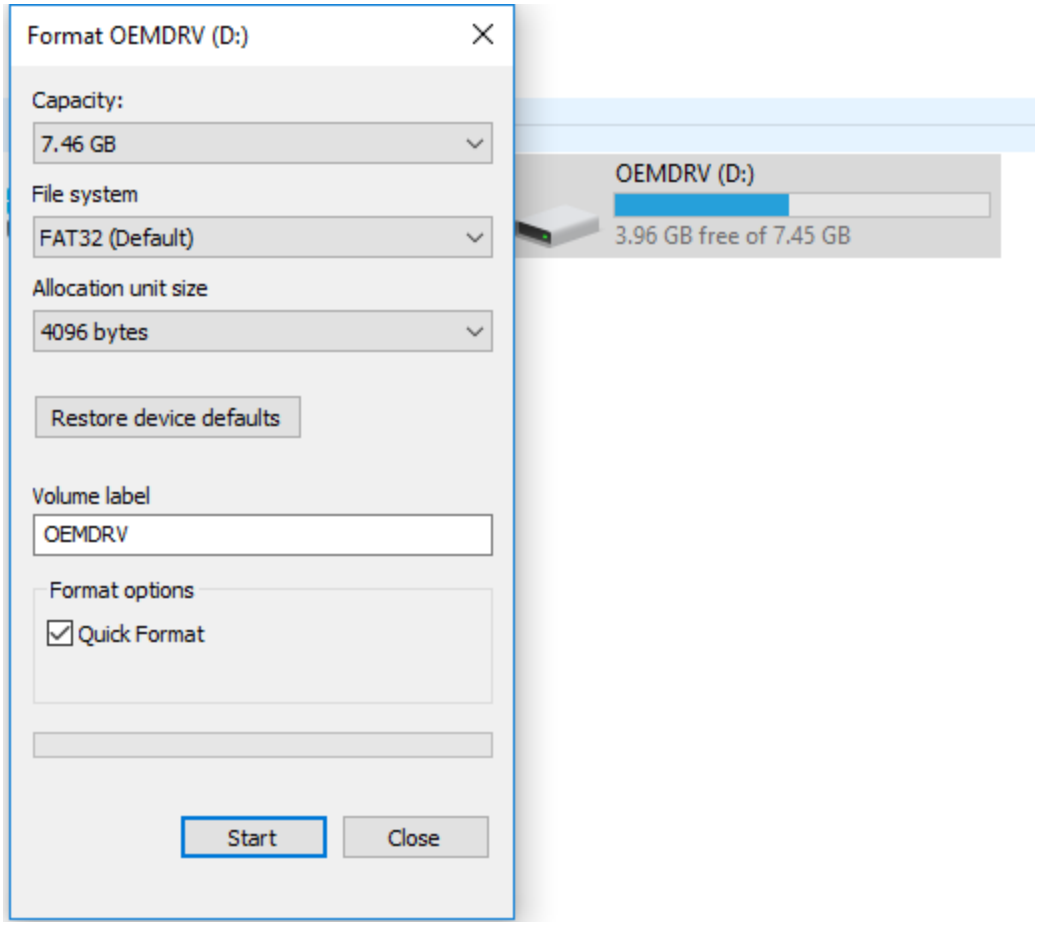
Create a NetWitness Suite USB Build Stick

Note: You must use a USB drive that is 8GB or larger and is formatted as FAT32.

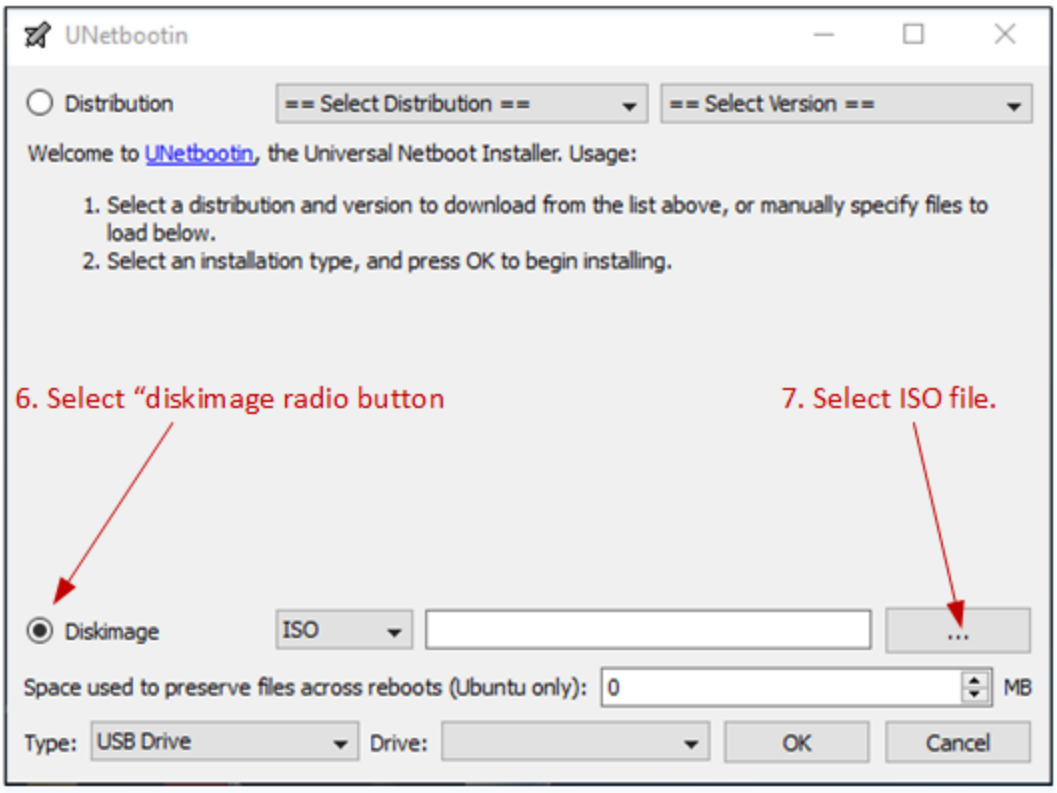
These instructions tell you how to create a USB "build-stick" to load the operating system and NetWitness Suite software onto your NetWitness Suite host.

Caution: All existing data on the USB drive will be destroyed.

1. Insert the USB drive that you will use as the build stick.
2. Format the USB drive.
   a. In Microsoft Windows Explorer, go to "**This PC**" for Windows 10 or **Computer** for older Windows Operating Systems.
   b. Right click the USB device, and click **Format**.
   c. In the format menu, make sure that your drive has **OEMDRV** for the **Volume label**, check the **Quick Format** checkbox, and click **Start**.

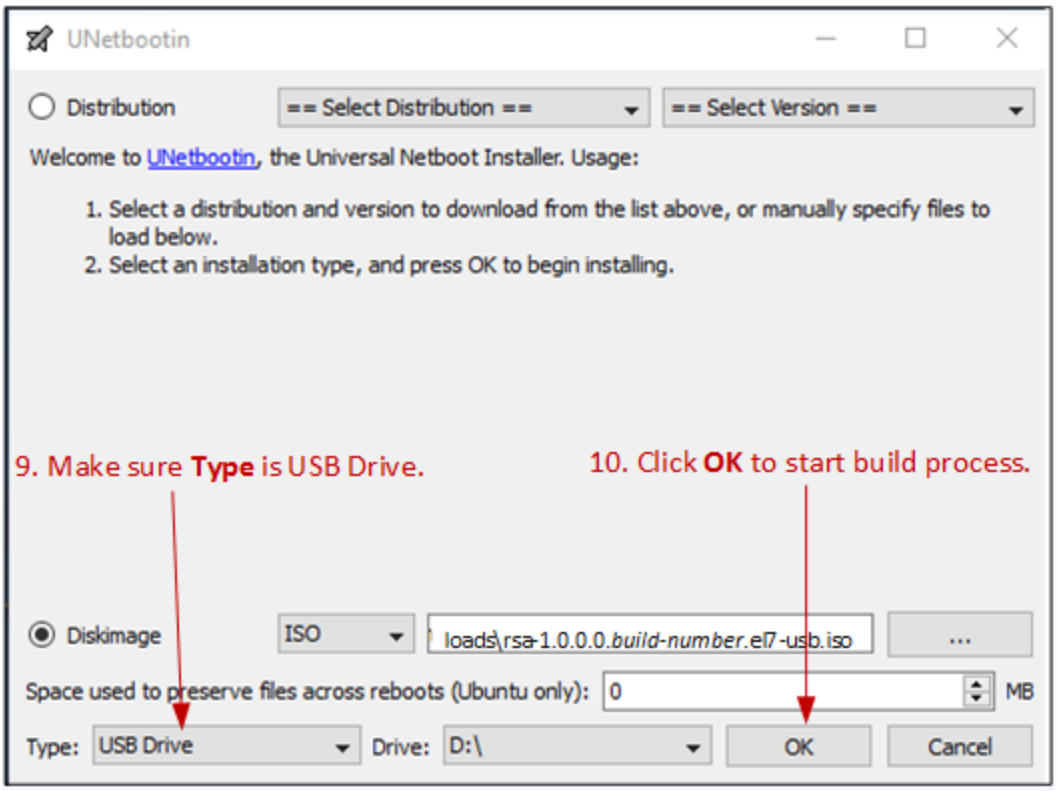


3. Download the NetWitness Suite USB ISO image.
4. Download an automated tool to create a build stick (for example UNetbootin).
5. Launch the tool.



6. Select the **Diskimage** radio button.
7. Select the appropriate version of the NetWitness Suite ISO by clicking on ... and navigating to the ISO file in your Local directory (for example, **C:/temp/rsa-11.x.x.x.<build-number>.el7-usb.iso**).

8. Highlight the usboot file and click **Open** to select the ISO file.



9. Confirm the **Type** is set to USB Drive and the **Drive** is set to the appropriate USB drive.
10. Click **OK** to start the build process.
11. After the process completes, **Exit** to complete the automated file extraction. (Do not click **Reboot Now** unless you want to reboot your Windows computer.)
12. Go to My Computer, right click **USB** and click **Safely Remove or Eject**.
13. After the USB drive is ejected, unplug the USB device.
    The bootable USB is now ready.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD

RSA NETWITNESS® SUITE

Endpoint Insights Agent Installation Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **5**

Supported Operating Systems 5

Windows 5

Linux 6

Mac 6

Installation Flowchart 6

Prerequisites **8**

Generate an Endpoint Agent Packager **9**

Generating an Agent Packager for Endpoint Data Collection 9

Generating an Agent Packager with Windows Log Collection 12

Generate Endpoint Agent Installers **16**

Deploy and Verify Endpoint Agents **17**

Deploying Agents (Windows) 17

Verifying Windows Agents 17

Deploying Agent (Linux) 17

Verifying Linux Agents 17

Deploying Agent (Mac) 18

Verifying Mac Agents 18

Configuring the Communication Between Endpoint Server and Endpoint Agents on Windows Vista, 2008 Server, Mac OS X 10.9 and 10.10 18

Uninstall Agents **20**

Uninstalling Windows Agent 20

Uninstalling Linux Agent 20

Uninstalling Mac Agent 20

Introduction

Note: The information in this guide applies to Version 11.1 and later.

Hosts can be laptops, workstations, servers, tablets, routers, or any system, physical or virtual, where a supported operating system is installed. An Endpoint Insights Agent can be deployed on a host with either a Windows, Mac, or Linux operating system. The installation process involves:

1. Generating an agent packager to collect only endpoint data or to collect both endpoint and log data (Windows only)
2. Generating the agent installer

You can run the agent installer specific to your operating system to deploy agents on the hosts. The agents collect endpoint data and Windows logs (if enabled) from these hosts. It monitors activities and reports data and scan results to the Endpoint Hybrid or Endpoint Log Hybrid over HTTPs.

Supported Operating Systems

Windows

The agent software runs on the following Windows operating systems:

- Windows Vista (32 and 64-bit)
- Windows 7 (32 and 64-bit)
- Windows 8 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 (32 and 64-bit)
- Windows 2008 Server (32 and 64-bit)
- Windows 2008 R2 (32 and 64-bit)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 Server

Linux

The agent software runs on either i386 or x84_64 architecture and on the following Linux operating systems:

- CentOS 6.x and 7.x
- Red Hat Linux 6.x and 7.x

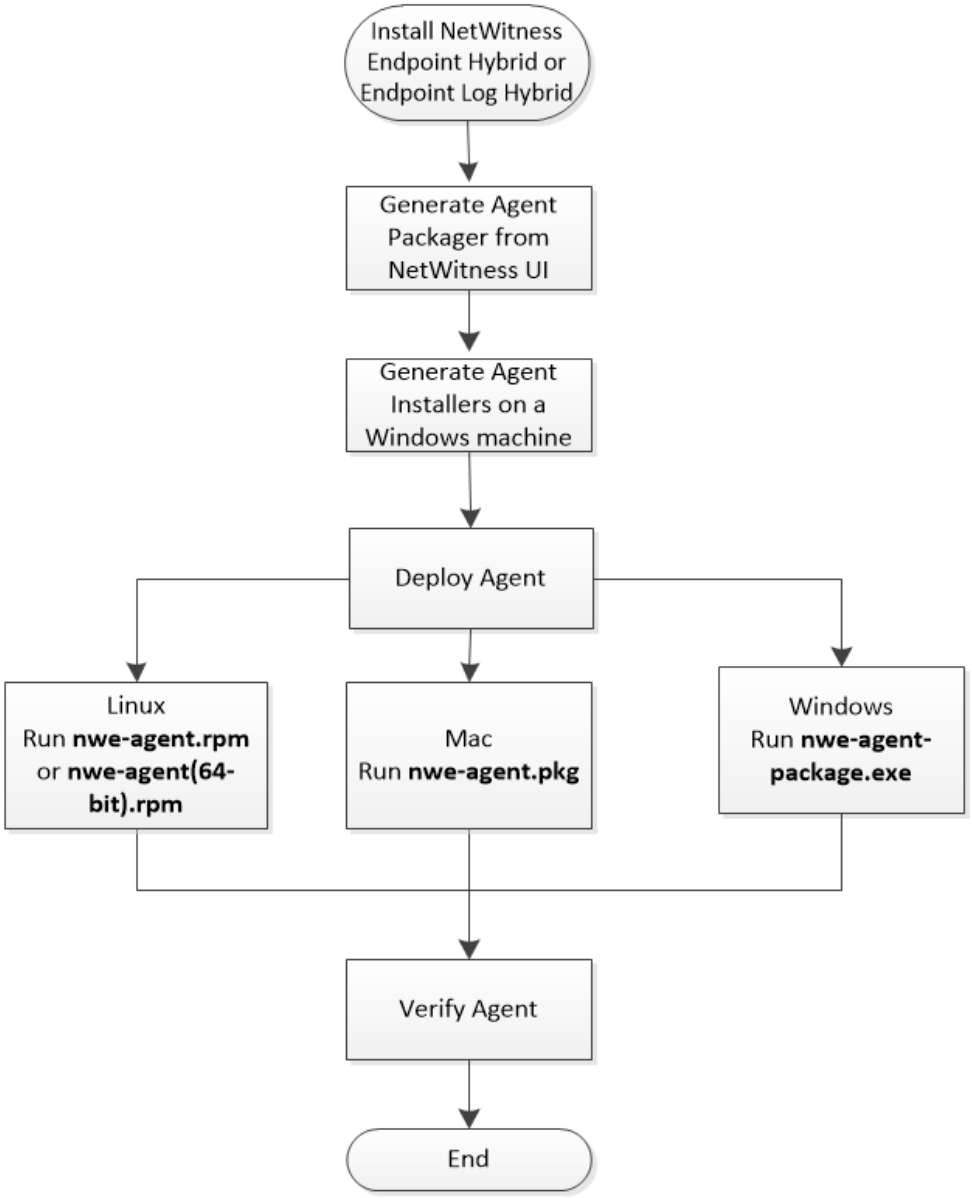
Mac

The agent software runs on the following Mac operating systems:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.11 (El Capitan)
- Mac OS X 10.12 (Sierra)

Installation Flowchart

The following flowchart illustrates the Endpoint agent installation process:


Install NetWitness Endpoint Hybrid or Endpoint Log Hybrid
Generate Agent Packager from NetWitness UI
Generate Agent Installers on a Windows machine
Deploy Agent
Linux
Run **nwe-agent.rpm** or **nwe-agent(64-bit).rpm**
Mac
Run **nwe-agent.pkg**
Windows
Run **nwe-agent-package.exe**
Verify Agent
End

Prerequisites

- Install RSA NetWitness Suite. For more information, see the *Physical Host Installation Guide* or *Virtual Host Installation Guide*.
- Configure NetWitness Endpoint Hybrid or Endpoint Log Hybrid. For more information, see the *Endpoint Insights Configuration Guide*.

Generate an Endpoint Agent Packager

Generating an Agent Packager for Endpoint Data Collection

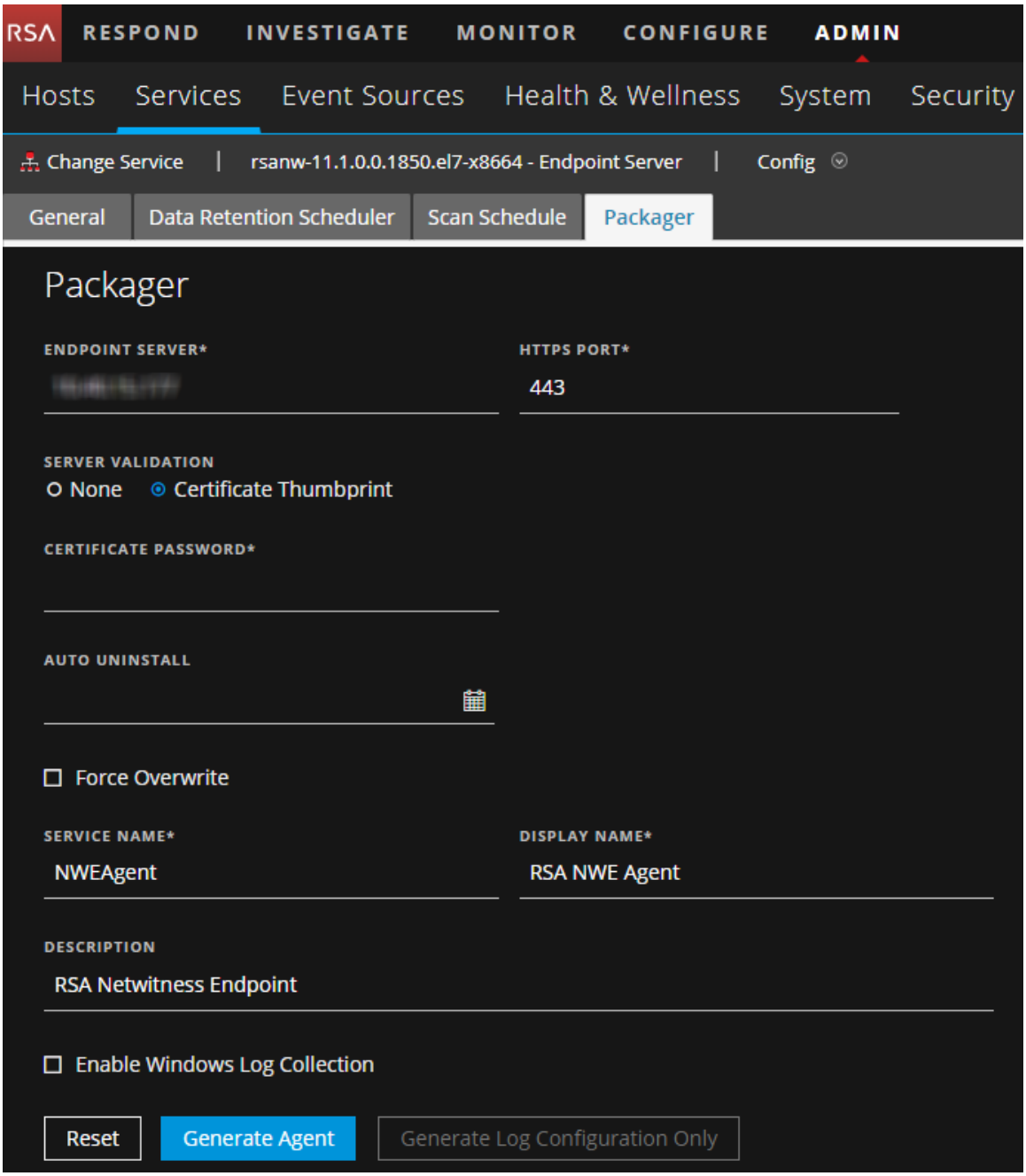
To generate an agent packager for collecting only endpoint data from hosts:

1. Log into NetWitness Suite.

   Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Suite Login screen.

2. Click **ADMIN > Services**.

3. Select the **Endpoint Server** service and click **> View > Config > Packager** tab. The Packager tab is displayed.



4. Enter the values in the following fields:

Field	Description
Endpoint Server	Host name or IP address of the Endpoint Server. For example, 10.10.10.3.

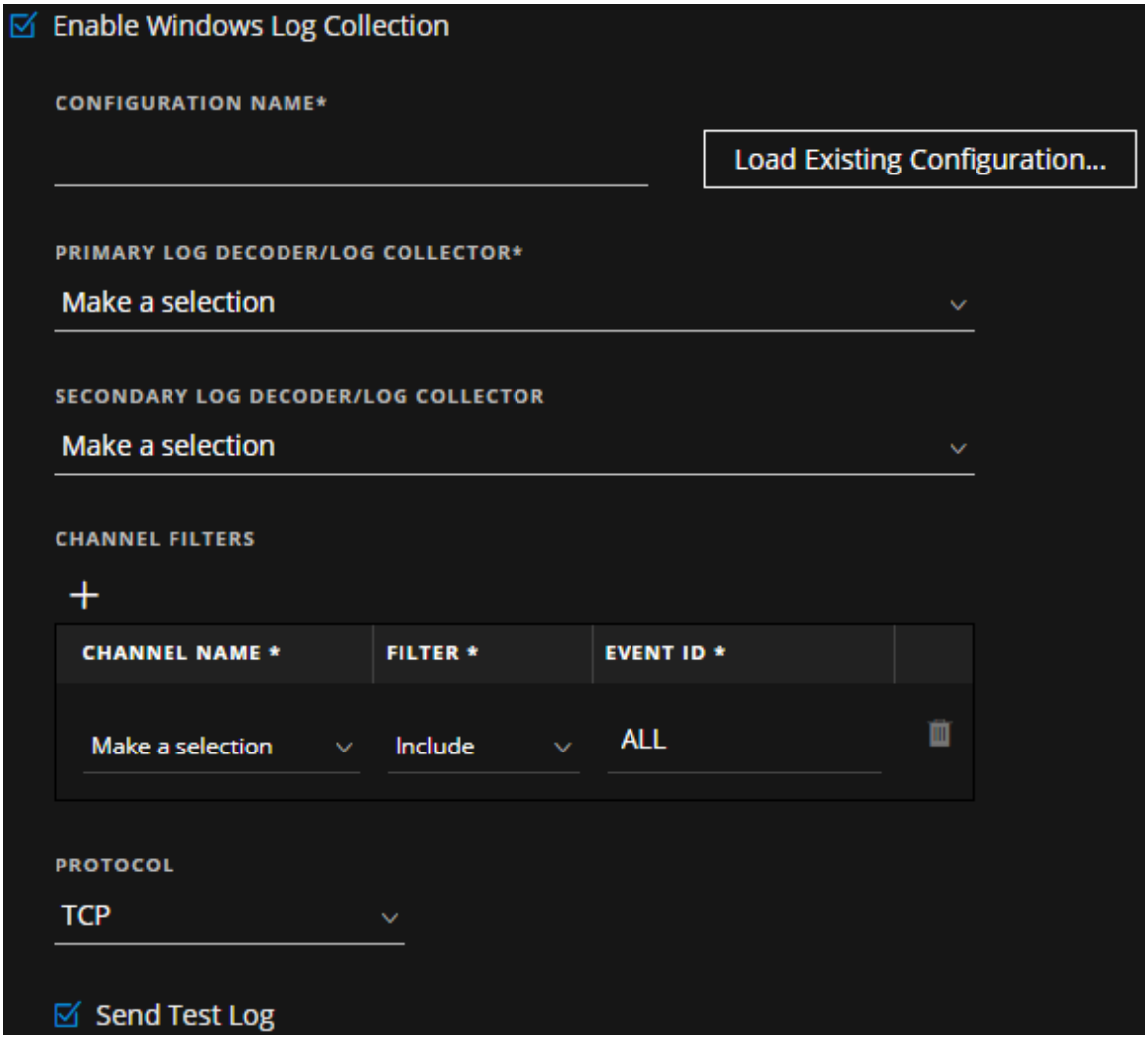
Field	Description
HTTPS Port	Port number. For example, 443.
Server Validation	Determines how the agent validates the Endpoint Server certificate: • None – The agent will not validate the server certificate. • Certificate Thumbprint – default selection. The agent identifies the server by validating the thumbprint of the Root CA of the server certificate.
Certificate Password	Password used to download the packager. The same password is used while generating the agent installer. For example, netwitness.
Auto Uninstall	Date and time the agent automatically uninstalls. You can leave it blank if not required.
Force Overwrite	Overwrites the installed Windows agent regardless of the version. If this option is not selected, the same installer can be run multiple times on a system, but installs the agent only once. **Note:** If you enable this option, make sure that you provide the same service name as the previously installed agent, while creating a new agent.
Service Name	Name of the agent. This field is applicable only for Windows. For example, NWEAgent.
Display Name	Display name of the agent. This field is applicable only for Windows. For example, NWE.
Description	Description of the agent. This field is applicable only for Windows. For example, RSA NetWitness Endpoint.
Generate Agent	Generates an agent packager.

5. Click **Generate Agent**.
   This downloads an agent packager (**AgentPackager.zip**) on the host where you are accessing the NetWitness Suite user interface.

Generating an Agent Packager with Windows Log Collection

You can enable the Windows Log Collection feature in the agent while generating the agent packager. By enabling this option, a Log Configuration file is generated, and the agent can collect and forward Windows logs. To enable the Windows Log Collection:

1. Perform steps 1 to 4 in Generating an Agent Packager for Endpoint Data Collection.
2. Select **Enable Windows Log Collection**.

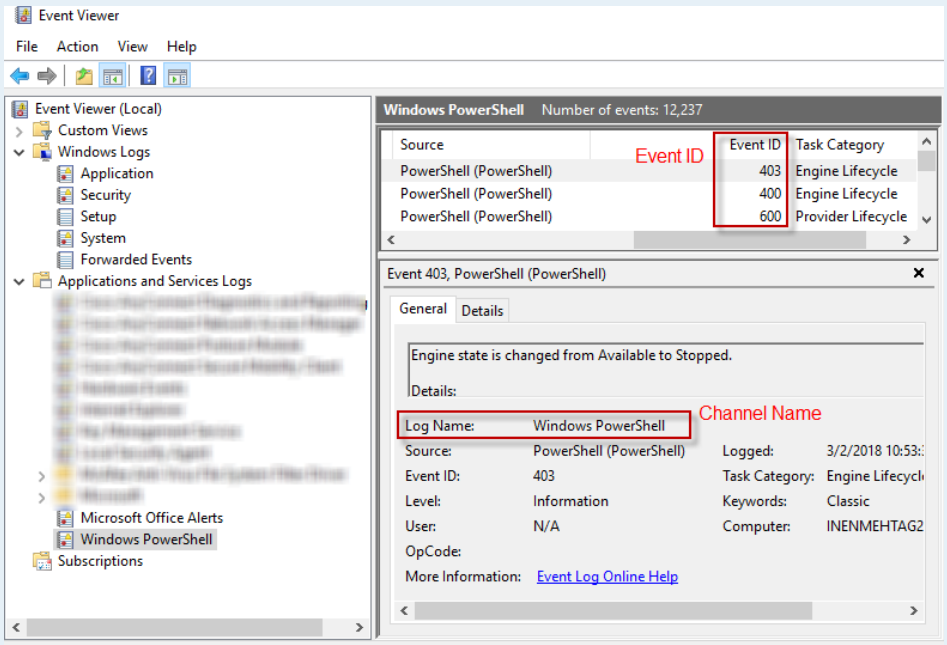


3. Enter or select the values in the following fields:

Field	Description
Configuration Name	Name of the configuration. Configuration name can have special characters, alphanumeric values, hyphens, spaces, and underscores.

Field	Description
Load Existing Configuration	Loads an existing configuration from the user system. The Windows Log Collection fields get populated with the information on a successful upload. **Note:** Warning messages are displayed during upload if there are any errors or warning.
Primary Log Decoder/Log Collector	Primary Log Decoder or Log Collector for forwarding logs. This displays the list of Log Decoders or Remote Log Collectors in the current deployment. This field is a combination of display name of service, host name, and service type.
(Optional) Secondary Log Decoder/Log Collector	Secondary Log Decoder or Log Collector for forwarding logs. The secondary Log Decoder or Log Collector receives the Windows events if the agent cannot reach the primary Log Decoder or Log Collector. **Note:** For the UDP protocol, the secondary Log Decoder or Log Collector is not functional. The logs are not forwarded to the secondary Log Decoder or Log Collector when the primary is down, thus resulting in the event loss.
Protocol	Select the protocol from the drop-down menu. The available options are UDP, TCP, and TLS. By default, the protocol is TCP.

Field	Description
Channel Filters	Channels from which the logs are collected. You can add or remove a channel filter. There should be at least one channel filter to collect the logs. • **Channel Name**: Select the channel from the drop-down menu. The available options are System, Security, Application, Setup, and Forwarded Events. You can also create a custom channel by entering a custom channel name path. This is added to the channel name list. To find custom channels, go to the **Windows Event Viewer** on your computer. • **Filter**: Click to add a channel filter. Click the drop-down menu to Include or Exclude the event IDs from a particular channel when generating the agent packager or the Log Configuration file. By default, for the Include option, the Event ID is set to **ALL**. For the Exclude option, the Event ID is set to blank. Click to remove a channel filter. • **Event ID**: Enter the Event IDs for this channel. These are specific to channels and are the IDs that need to be collected. The event IDs can be numeric or a range. For example, use it in a range, 15-32. But, a reverse range is not allowed, for example, 32-15. Event IDs can also be used as combinations, for example, list of event IDs separated by commas, such as 248, 903, 16384, and so on. **Note:** When you enter ALL, it implies all event IDs for that channel. You can use Windows Event Viewer to identify event IDs and channel name to be configured in the UI. The following example displays the navigation to get event ID and channel name for Windows Powershell. To view the information, go to Run and type `Event Viewer`, go to **Applications and Services Logs** > **Windows Powershell**. The event IDs and channel name in Application and Services Logs for Windows Powershell are displayed.

Field	Description
	
Send test log	Sends a test log message. By default, this option is enabled. A test log message is sent on a new agent deployment or configuration change from the agent to the Log Decoder. It contains all the fields configured for the agent. These events can help understand agents' connectivity to the destination.
Generate Agent	Generates an agent packager. The Log Configuration file is created in the AgentPackager.zip file.
Generate Log Configuration Only	Generates the Log Configuration file as per the parameters specified above or if uploaded using the Load Existing Configuration option. **Note:** The contents of the generated Log Configuration file should not be tampered. If any changes are made, the agent does not read the information from the file.

Note: You can enable the Windows Log Collection feature later by downloading and deploying the Log Configuration file. For more information, see the "Add/Update Windows Log Collection file using Endpoint Agent" section in the *Log Collection Configuration Guide*.

Generate Endpoint Agent Installers

To generate endpoint agent installers to deploy on hosts:

Note: Use a Windows machine to execute the agent packager file.

1. Unzip the **AgentPackager.zip** file. It includes the following:
   - **agents** folder – Contains executables for Linux, Mac, and Windows.
   - **config** folder – Contains configuration file and the certificates required to communicate between the Endpoint Server and the agent.
   - **AgentPackager.exe** file.
2. Run the **AgentPackager.exe** file.
3. Enter the same password used while generating the agent packager and press **Enter**. This creates the following installers in the root folder:
   - nwe-agent-package.exe (for Windows)
   - nwe-agent.pkg (for Mac)
   - nwe-agent.rpm (for Linux 32-bit)
   - nwe-agent(64-bit).rpm (for Linux 64-bit)

Deploy and Verify Endpoint Agents

This section provides instruction on how to deploy and verify agents.

Deploying Agents (Windows)

To deploy the agent, run the **nwe-agent-package.exe** file on the hosts you want to monitor.

Verifying Windows Agents

After deploying the Windows agents, you can verify if a Windows agent is running by using any of the following methods:

- Using the NetWitness Endpoint UI
  The Hosts view contains the list of all hosts with an agent. You can look for the host name on which the agent is installed.

Note: Click **Investigate** > **Hosts** or press F5 to refresh the list for latest data.

- Using Task Manager
  Open Task Manager and look for service name that you configured while generating the agent packager.
- Using Services.msc
  Open Services.msc in run and look for NWEAgent.

Deploying Agent (Linux)

To deploy the agent, run the **nwe-agent.rpm** (for 32-bit) or **nwe-agent(64-bit).rpm** (for 64-bit) file on the hosts you want to monitor. Use the 32-bit rpm for i386 and 64-bit rpm for x84_64 machines.

Verifying Linux Agents

After deploying the Linux agents, you can verify if a Linux agent is running by using any of the following methods:

- Using the NetWitness Endpoint UI.
  The Hosts view contains the list of all hosts with an agent.

Note: Click **Investigate > Hosts** or press F5 to refresh the list for latest data.

- Using Command Line

  Run the following command to get the PID:

  ```
  pgrep nwe-agent
  ```

- To check the NetWitness Endpoint version, run the command:

  ```
  cat /opt/rsa/nwe-agent/config/nwe-agent.config | grep version
  ```

Deploying Agent (Mac)

To deploy the agent, run the **nwe-agent.pkg** file on the hosts you want to monitor.

Verifying Mac Agents

After deploying the Mac agents, you can verify if a Mac agent is running by using any of the following methods:

- Using the NetWitness Endpoint UI

  The Hosts view contains the list of all hosts with an agent.

Note: Click **Investigate > Hosts** or press F5 to refresh the list for the latest data.

- Using Activity Monitor

  Open Activity Monitor (/Applications/Utilities/Activity Monitor.app) and look for NWEAgent.

- Using Command Line

  Run the following command to get the PID

  ```
  pgrep NWEAgent
  ```

- To check the NetWitness Endpoint version, run the command:

  ```
  grep a /var/log/system.log | grep NWEAgent | grep Version:
  ```

Configuring the Communication Between Endpoint Server and Endpoint Agents on Windows Vista, 2008 Server, Mac OS X 10.9 and 10.10

By default, the FIPS mode is enabled on the Endpoint Server, which means that agents installed on Windows Vista, 2008 Server, Mac OS X 10.9 and 10.10 cannot communicate with the Endpoint server.

To resolve this, perform the following steps on the Endpoint Hybrid or Endpoint Log Hybrid to disable the FIPS mode:

1. Go to `/etc/pki/tls/owb.cnf` and edit the file to disable the FIPS mode.

```
# FIPS Mode
#   Configures the BSAFE Libraries to be in FIPS Mode.
#
#   Values: "on", "off".
#   Default: "off"
fips_mode = off
```

2. Go to `/etc/nginx/conf.d/nginx.conf` and edit the file to comment the following lines:

```
#    ssl_ciphers AES256+EECDH:AES256+EDH:!aNULL;
#    ssl_prefer_server_ciphers on;
```

3. Restart the Nginx server using the following command:

```
systemctl restart nginx
```

Uninstall Agents

This section provides the commands to uninstall the agent.

Uninstalling Windows Agent

Run the following command:

```
msiexec /x{63AC4523-5F19-42F0-BC43-97C8B5373589}
```

Uninstalling Linux Agent

Run the following command:

```
rpm –ev nwe-agent
```

Uninstalling Mac Agent

Run the following commands:

1. `sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
2. `sudo rm -Rf /usr/local/nwe`
3. `sudo rm -Rf '/Library/Application Support/NWE'`
4. `sudo rm –Rf /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
5. `sudo pkgutil --forget com.rsa.pkg.nwe`

RSA NETWITNESS® SUITE

Physical Host Upgrade Guide

for Version 10.6.5.x to 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **7**

CentOS6 to CentOS7 Upgrade 7

RSA NetWitness® Suite 11.1 Upgrade Path 8

Supported Host Upgrade Path 8

Hardware, Deployments, Services, and Features Not Supported in 11.1 8

Event Stream Analysis (ESA) Upgrade Considerations 9

Upgrade Phases 9

Investigate in Mixed Mode 11

Upgrade Workflow 15

Contact Customer Support 15

Upgrade Preparation Tasks **16**

Global 16

Task 1 - Review Core Ports and Open Firewall Ports 16

Task 2 - Record Your 10.6.5.x admin user Password 17

Task 3 - Create a Backup of the /etc/fstab File 17

Respond 17

Task 4 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C” 17

Reporting Engine 18

(Conditional) Task 5 - Unlink External Storage 18

Warehouse Connector 19

(Conditional) Task 6 - Copy keytab files in root or etc Directory Stored in Other Directory 19

Backup Instructions **20**

Task 1 - Set up an External Host for Backing up Files 21

Task 2 - Create a List of Hosts to Back up 23

Troubleshooting Information 25

Task 3 - Set up Authentication Between Backup and Target Hosts 27

Task 4 - Check for Backup Requirements for Specific Types of Hosts 27

For All Host Types 27

For ESA Hosts with Mongo Databases 28

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation 28
Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh 28
For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords 30
For Bluecoat Event Sources 30
Task 5 - Check for Adequate Space for the Backup 30
Task 6 - Back up Your Host Systems 31
Post Backup Tasks 35
Task 1 - Save a Copy of the all-systems File and the Backup Tar files 35
Task 2 - Ensure Required Backup Files Were Generated 35
Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host 36
Task 4 - Ensure All Required Backup Files are on Each Host 36

Upgrade Tasks 39

Phase 1 - Upgrade SA Server, Event Stream Analysis, Malware Analysis Hosts, and Broker or Concentrator 39
Task 1 - Upgrade the 10.6.5.x SA Server to 11.1 NW Server 39
Task 2 - Upgrade 10.6.5.x ESA to 11.1 39
Task 3 - Upgrade 10.6.5.x Malware Analysis to 11.1 40
Task 4 - Upgrade 10.6.5.x Broker or 10.6.5.x Concentrator to 11.1 40
Phase 2 - Upgrade All Other Hosts 40
Decoder and Concentrator Hosts 40
Log Decoder Host 40
Virtual Log Collector Host 41
All Other 10.6.5.x Hosts to 11.1 42
Upgrade the 10.6.5.x SA Server Host to the 11.1 NW Server Host 42
Upgrade a 10.6.5.x non-SA Server Host to 11.1. 51

Update or Install Legacy Windows Collection 60

Post Upgrade Tasks 61

NW Server 61
Task 1 - Migrate Active Directory (AD) 61
Task 2 - Modify Migrated AD Configuration to Upload Certificate 62
Task 3 - Reconfigure Pluggable Authentication Module (PAM) in 11.1 62
Task 4 - Restore NTP Servers 62

Task 5 - Restore Licenses for Environments without FlexNet Operations-On Demand Access 62
(Conditional) Task 6 - If You Disabled Standard Firewall Config - Add Custom IPtables 63
(Conditional) Task 7 - Specify SSL Ports If You Never Set Up Trusted Connections 63
Task 8 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File 64
RSA NetWitness® Endpoint 65
Task 9 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed 65
RSA NetWitness® Endpoint Insights 65
(Optional) Task 10 - Install Endpoint Hybrid or Endpoint Log Hybrid 65
Task 11 - Reconfigure Endpoint Alerts Via Message Bus 65
Event Stream Analysis Tasks 66
Task 12 - Reconfigure Automated Threat Detection for ESA 66
Task 13 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL 66
Task 14 - Enable Threat - Malware Indicators Dashboard 67
Investigate 67
Task 15 - Make Sure User Roles Have Customized User Roles Have Investigate-server Permissions for Event Analysis Access 67
Log Collection 68
Task 16 - Reset Stable System Values for Log Collector after Upgrade 68
(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders)Task 17 - Enable FIPS Mode 69
Reporting Engine 69
(Conditional) Task 18 - Restore the CA certificates for External Syslog Servers for Reporting Engine 69
(Conditional) Task 19 - Restore External Storage for Reporting Engine 70
Respond 70
(Conditional) Task 20 - Restore Custom Analysts Roles 70
Task 21 - Restore Respond Service Custom Keys 70
Task 22 - Restore Customized Respond Service Normalization Scripts 71
Task 23 - Add Respond Notification Settings for Custom Roles 71
Task 24 - Manually Configure Respond Notification Settings 72
Task 25 - Update Default Incident Rule Group By Values 73
Task 26 - Add Group By Field to Incident Rules 74

Task 27 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task 75
SecOps Manager 76
Task 28 - Reconfigure NW SecOps Manager Integration 77
Warehouse Connector 77
Task 29 - Restore keytab Files, Mount NFS, Install Service 77
Task 30 - Refresh Warehouse Connector Lockbox and Start Stream 77
Backup 78
Task 31 - Remove Backup-Related Files from Host Local Directories 78
Appendix A. Troubleshooting 79
Section 1 - General Troubleshooting information 79
Command Line Interface (CLI) 79
Backup (nw-backup script) 82
Event Stream Analysis 84
Log Collector Service (nwlogcollector) 85
NW Server 87
Reporting Engine Service 87
Section 2 - Hardware-Related Troubleshooting Information 88
Import Foreign Config for Series 4 Appliance with External Storage 88
Restore Files for 10G Decoder 91
Appendix B. Stopping and Restarting Data Capture and Aggregation 92
Stop Data Capture and Aggregation 92
Start Data Capture and Aggregation 94
Appendix C. Using iDRAC 95
Configure NFS Server - NFS Server config File 95
Boot iDRAC to NFS Configuration 96
Appendix D. Create External Repository 97
Revision History 100

Introduction

The instructions in this guide apply to the upgrade of physical hosts to RSA NetWitness® Suite 11.1 exclusively. See the *RSA NetWitness® Suite 10.6.5 to 11.1 Virtual Host Upgrade Guide* for instructions on how to upgrade your virtual hosts to 11.1.

NetWitness Suite 11.1 is a major release that affects all products in the NetWitness Suite. The components of the suite are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, and Security sever), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.

Refer to the *RSA NetWitness Suite Getting Started Guide* to become familiar with the major changes to the 11.x User interface. Refer to the *RSA NetWitness Suite Deployment Guide* to become familiar with the major platform changes in 11.x.

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: The Reporting Engine is installed on the NW Server host, Workbench is installed on the Archiver host, Warehouse Connector can be installed on the Decoder host or Log Decoder host.

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.1 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.1 platform environment has been improved greatly to accommodate current and future physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Suite 11.1 Upgrade Path

The earliest supported Upgrade path for RSA NetWitness® Suite 11.1 is Security Analytics 10.6.5.x. If you are running a version of NetWitness Suite that is prior to 10.6.5.x, you must update to 10.6.5.x before you can upgrade to 11.1. See the *RSA Security Analytics 10.6.5 Update Guide* (https://community.rsa.com/docs/DOC-85119) on RSA Link.

Supported Host Upgrade Path

You must upgrade a host to the same host type:

- Same Series RSA Physical Appliance to Same Series RSA Physical Appliance (that is, Series 4 to Series 4, Series 5 to Series 5).
  RSA does not support third-party physical hosts in 11.1.
- On-Prem Virtual to On-Prem Virtual

Caution: The 11.1 upgrade does not support mixed-platform upgrades (for example, it does not support physical to virtual).

Hardware, Deployments, Services, and Features Not Supported in 11.1

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.1.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- IPDB service
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.1.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.1.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.1, your custom policy is not present. In its place, there is the out-of-the-box Context hub Server Monitoring Policy in the user interface, which is specific for version 11.1.

- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Suite 11.1, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.1, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.5.x has been removed.

Caution: If you do not use Incident Management in 10.6.5.x, carefully consider whether or not to upgrade to version 11.1.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.1.

In your 10.6.5.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.1.
- Multiple ESA hosts configured to use Incident Management – The system will continue to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.5.x, you can upgrade to version 11.1.
- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.1.

Note: If you did not use Incident Management in 10.6.5.x, you cannot view the 10.6.5.x ESA alerts in the 11.1 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.1 that will allow Respond to view them. See the *ESA Alert Migration Instructions* knowledge base article (https://community.rsa.com/docs/DOC-81680) in RSA Link for instructions on how to run this script.

Upgrade Phases

RSA recommends that you stagger host upgrades as described in this section. The update to CentOS7 and the need of a physical or iDRAC access cause the 11.1 upgrade to take more time than most upgrades.

Caution: If you stagger the upgrade, you:
• must upgrade the hosts in Phase 1 first, in the order shown.
• may not have all the features operational until you update your entire deployment.
• will not have service administrative features available until you upgrade all the hosts in your deployment.

Phase 1

You perform Phase 1 first and you must upgrade the hosts in the following order:

1. Security Analytics Server host
2. Event Stream Analysis hosts
3. Malware Analysis hosts
4. Broker hosts (if you do not have a Broker, upgrade your Concentrator hosts)
   The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2

Upgrade the rest of your hosts.

RSA recommends that you follow the order in Phase 2 to reduce:

- functionality loss during investigation.
- downtime that results in the loss of packet and log capture.

Note: Other than Log Collection hosts with downstream event destinations, there is no technical reason to upgrade your hosts in the order shown in Phase 2.

This is the Phase 2 host upgrade order recommended by RSA.

1. Decoder hosts
2. Concentrator hosts
3. Archiver hosts
4. Log Collection hosts - Log Collectors on Log Decoder hosts (LDs), Virtual Log Collectors (VLCs) and Legacy Windows Collectors (LWCs)
   Before you upgrade a log collection host, you must prepare it for the upgrade. Part of this preparation ensures that no event data remains in the queues. This requires you to keep the downstream destinations of event data (Log Collectors, Virtual Log Collectors and Log Decoders) up and functioning properly.

If you have event data destinations downstream from the Log Decoder, you must prepare and upgrade log collectors in the following order.

a. LDs (one LD at a time)

b. VLCs and LWCs

If you do not have event data destinations downstream from the Log Decoder, you can prepare and upgrade multiple LDs, VLCs, and LWCs together.

5. All other hosts

See "Running in Mixed Mode" under "The Basics" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for:

- Functionality gaps encountered while running in this mode.
- Examples of staggered upgrades.

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.1 and some are still on 10.6.5. This happens when you upgrade to 11.1 in phases.

Note: You must follow the host upgrade sequence as shown in Upgrade Phases to ensure complete Investigate functionality. The 11.1 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.1 to access the Event Analysis View. If the Broker is not upgraded, analysts see a warning icon next to the Broker and no data aggregated to that Broker can be displayed.

After you upgrade all services to 11.1, when an analyst conducts an investigation, Role-Based Access Control (RBAC) of downloads works consistently to limit access to restricted data.

In mixed mode (that is, some services are upgraded to 11.1 and some are still at 10.6.5), when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads.

If the `sdk.packets` setting has not been disabled on the 10.6.x services, analysts with SDK meta and roles permissions in place to restrict viewing and reconstructing an event's content can download the PCAP of an event that has content restrictions. Other types of downloads appear to be successful, then generate errors due to insufficient permissions, and the data is still protected.

During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.1 and re-enable `sdk.packets`, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NW Server at version 11.1 is connected to services at a lower version.

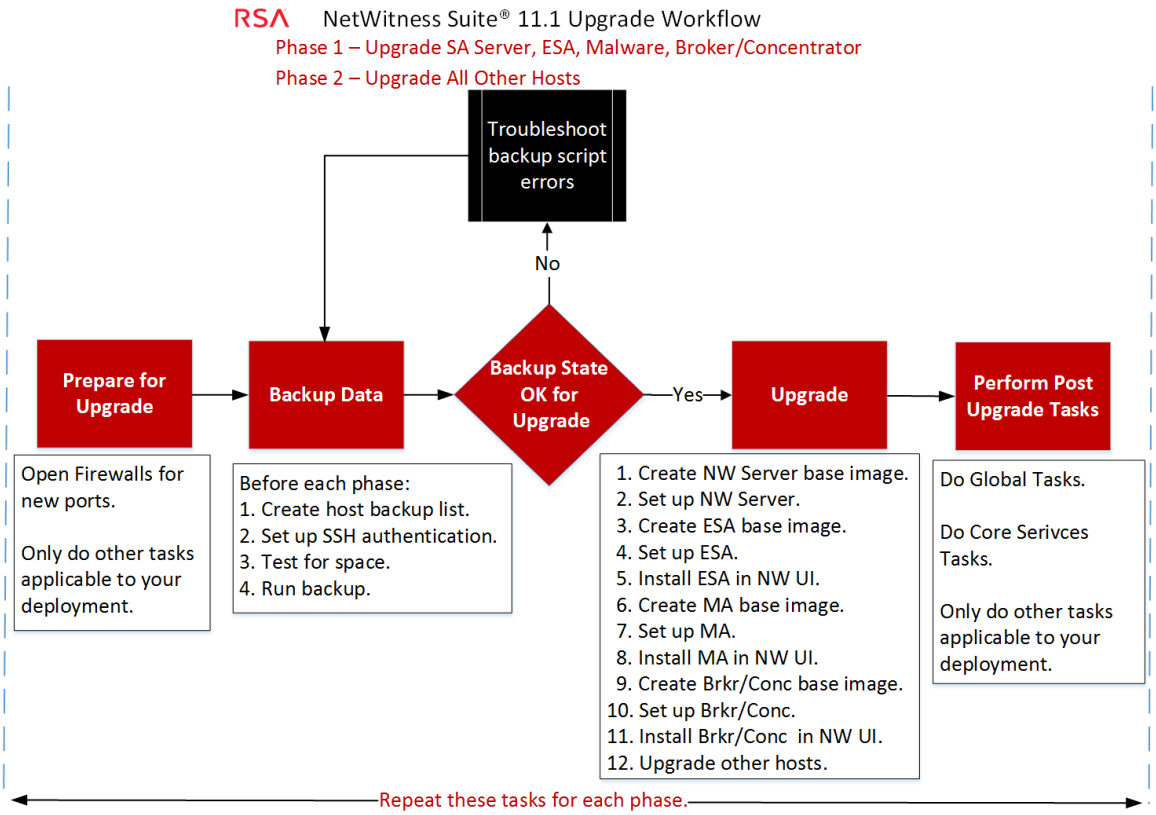
Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 10.6.5.x Concentrator -> 10.6.5.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst	RBAC permitted items	PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.1 Concentrator ->11.1 Decoder/Log Decoder	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items	PCAP	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.0.0.x Concentrator -> 11.0.0.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	None	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Reconstruction View	Analyst	RBAC permitted items	None	File archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Analysis View	Analyst	RBAC permitted items	None	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload PCAPs and logs are downloaded as zero bytes

Upgrade Workflow

The following diagram illustrates the RSA NetWitness® Suite 11.1 upgrade workflow.



Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Suite 11.1.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.1. These tasks are organized by the following categories.

- Global
- Reporting Engine
- Respond
- Warehouse Connector

Global

You must complete these tasks regardless of how you deploy NetWitness Suite and which components you use.

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.1.

Caution: Make sure that the new ports are implemented and tested before upgrading so that upgrade does not fail due to missing ports.

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 27017	MongoDB

ESA Host

Source Host	Destination Host	Destination Ports	Comments
NW Server, NW Endpoint, ESA Secondary	ESA Primary	TCP 27017	MongoDB

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5672	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

All NetWitness Suite core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® Suite Deployment Guide* in case you need to reconfigure NetWitness Suite services and firewalls. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 2 - Record Your 10.6.5.x `admin user` Password

Record your 10.6.5.x `admin user` password. You will need it to complete the upgrade.

Task 3 - Create a Backup of the `/etc/fstab` File

Copy the `/etc/fstab` file from all the physical hosts and into your local machine (backup host or remote machine).

Note: You need this file to restore a physical host with external storage mounts.

Respond

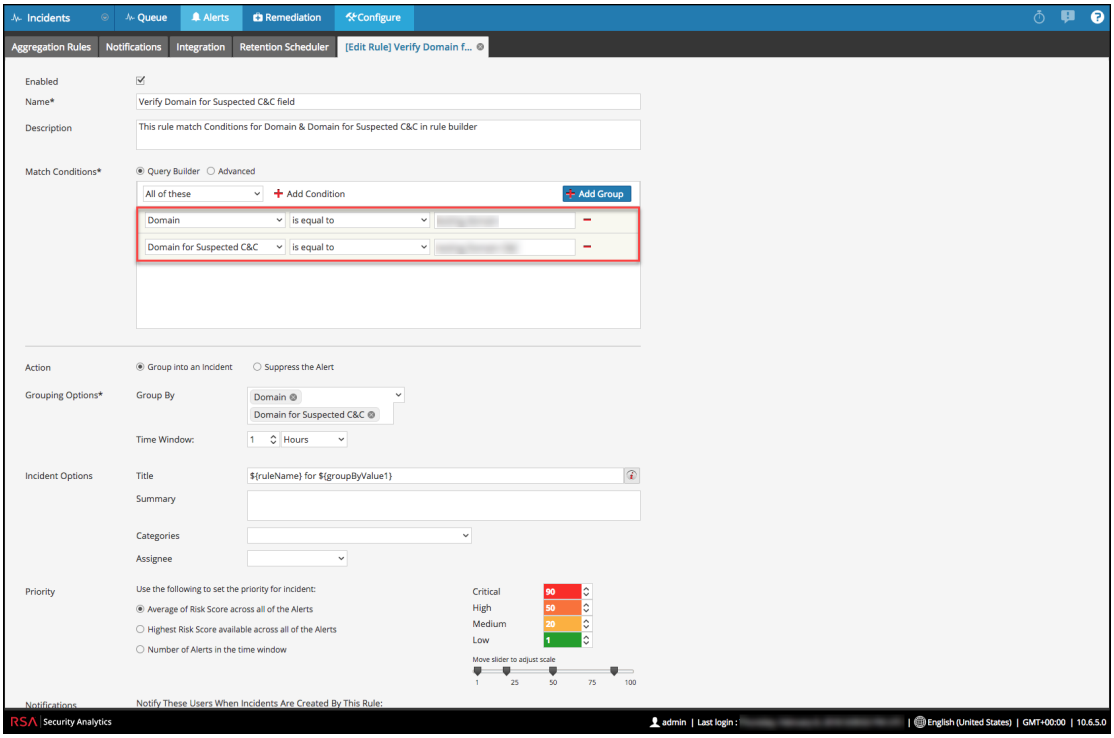
Task 4 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C”

Make a note of any Incident Management aggregation rules that have match conditions using Domain or Domain for Suspected C&C in the drop-down list in the rule builder. You will need to modify these rules to use Domain after you upgrade to 11.1 as described in the "Respond" Post Upgrade Tasks tasks .

Check the following for each aggregation rule:

1. In Security Analytics 10.6.5.x menu , click **Incidents** > **Configure** > **Aggregation Rules** tab and edit the rules to view the matching conditions.

2. In the **Match Conditions** section, look for **Domain** or **Domain for Suspected C&C** listed in the drop-down lists for the conditions.



3. Make a note of the rule name and the entire condition that uses **Domain** or **Domain for Suspected C&C**, including operators and values.

Reporting Engine

(Conditional) Task 5 - Unlink External Storage

If the Reporting Engine has external storage [such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports] you must perform the follow steps to unlink the storage.

In these steps:

- `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
- `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.
2. Stop the Reporting Engine service.
   ```
   stop rsasoc_re
   ```
3. Switch to `rsasoc` user.
   ```
   su rsasoc
   ```

4. Change to the Reporting Engine the home directory.
   `cd /home/rsasoc/rsa/soc/reporting-engine/`
5. Unlink the `resultstore` directory mounted to external storage.
   `unlink /externalStorage/resultstore`
6. Unlink the `formattedReports` directory mounted to external storage.
   `unlink /externalStorage/formattedReports`

Warehouse Connector

(Conditional) Task 6 - Copy `keytab` files in `root` or `etc` Directory Stored in Other Directory

Copy the `keytab` files in the `root` or `etc` directory if it is stored in some other directory.

1. Record the absolute path of NFS mount directory and the `keytab` file.
   You need this information to restore the Warehouse Connector after upgrade.
2. Unmount the NFS directory.
   a. SSH to the Warehouse Connector and log in with `root` credentials.
   b. Submit the following commands to unmount the NFS directory.
      `umount <NFS-absolute-path>`

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from Security Analytics 10.6.5.x releases to NetWitness Suite 11.1.

Note: It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.1, your custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types.

Caution: These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the Security Analytics Server
- Standalone Warehouse Connector
- Warehouse Analytics (Datascience)

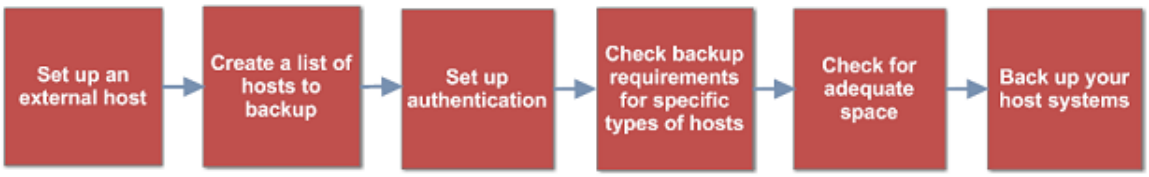
The following types of hosts can be backed up and are automatically restored during the upgrade process:

- **Security Analytics Admin Server** (may include Malware Analysis, Incident Management, Health and Wellness, and Reporting Engine)
- **Malware Analysis** (standalone)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and Incident Management database)
- **Concentrator**
- **Log Decoder** (including Local Log Collector and Warehouse Connector, if installed)
- **Log Hybrid**
- **Packet Decoder** (including Warehouse Connector, if installed)
- **Packet Hybrid**
- **Virtual Log Collector**

The following types of files are automatically backed up but must be restored manually after the upgrade process:

- PAM configuration files: For information about restoring the PAM configuration files, refer to "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.1.", in the "Global" section of the **Post Upgrade Tasks**.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of **Post Upgrade Tasks**.

The following diagram shows the high-level task flow of the steps you perform to back up your hosts.



The following sections describe each of these tasks:

- Task 1 - Set up an External Host for Backing up Files
- Task 2 - Create a List of Hosts to Back up
- Task 3 - Set up Authentication Between Backup and Target Hosts
- Task 4 - Check for Backup Requirements for Specific Types of Hosts
- Task 5 - Check for Adequate Space for the Backup
- Task 6 - Back up Your Host Systems
- Post Backup Tasks

Task 1 - Set up an External Host for Backing up Files

You must set up an external host to use for backing up files. The host must be running CentOS 6 with connectivity through SSH to the Security Analytics stack of hosts.

Note: If you are not able to use an external host for backing up files, contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

Ensure that the host names for the systems to be backed up are resolvable on the backup host machine, either by DNS or listed in the `/etc/hosts` file.

Note: These scripts are designed to run on CentOS 6 only. You must execute these scripts on CentOS 6 machines.

There are several scripts that you run during the backup process. You must download the zip file that contains the scripts (`nw-backup-v4.0.sh`) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your Security Analytics Servers and host systems to be backed up.
- `ssh-propagate.sh`: Automates sharing keys between the systems you are backing up and the backup host system so that you are not prompted for passwords multiple times.
- `nw-backup.sh`: Performs the backup of your hosts.
- `azure-mac-retention.ps1`: Applies only if you are using AZURE. See the *AZURE Deployment Guide* on for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

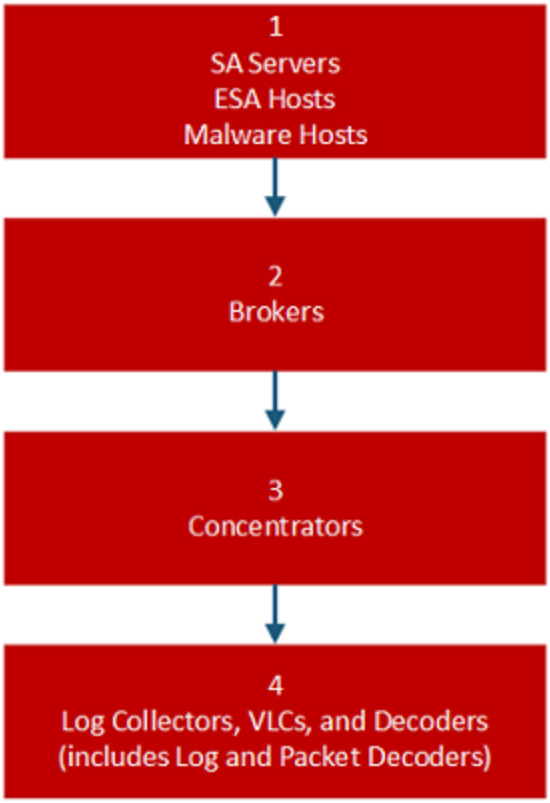
Note: If you have used the 10.6.x versions of the backup and restore scripts on your 10.6.5 hosts, you must still run all the scripts listed here.

Note: Do NOT use the scripts in the `nw-backup-v4.0.zip` file for regular backups. These scripts are specifically designed for upgrading from 10.6.5.x to 11.1.

Note: The backup scripts do not support backing up data for STIG-hardened hosts.

Task 2 - Create a List of Hosts to Back up

The script that you use to back up your files depends on the `all-systems` and `all-systems-master-copy` files, which contain a list of the hosts that you want to back up. The `all-systems-master-copy` file contains a list of all your hosts. The `all-systems` file is used for each backup session, and contains only those hosts which are being backed up for a particular session. You run the `get-all-systems.sh` script to generate these files. RSA recommends that you back up your hosts in groups, and not all at once. The recommended order and grouping of hosts for backup sessions is shown in the following diagram:



Limit each backup session to five hosts to ensure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference and then manually editing the `all-systems` file to contain specific hosts.

To generate the `all-systems` and the `all-systems-master-copy` files:

1. From the host on which you are running the backup process, make the `get-all-systems.sh` script executable by running the following command:
   ```
   chmod u+x get-all-systems.sh
   ```
2. At the root level, run the `get-all-systems.sh` script:
   ```
   ./get-all-systems.sh <IP-Address-of-SA-Admin-Server>
   ```
   You will be prompted for the password for each host system once per host.

This script saves the `all-systems` file and the `all-systems-master-copy` file to `/var/netwitness/database/nw-backup/`.

3. Validate that the `all-systems` and `all-systems-master-copy` files were generated and that they contain the right hosts.
4. Edit the `all-systems` file to contain only the systems you are backing up. You can do this by using the `all-systems-master-copy` file as a reference, and then opening the `all-systems` file in an editor (such as vi) and modifying it to include only the systems you want to back up. RSA recommends that you comment out the hosts that you do not want to back up (add the number sign (#) to the beginning of the line that contains the host that will not be backed up).
   The following examples shows how to comment out the 10.6.5 Security Analytics Server:
   `loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.5.0`
   `#nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.5.0`

   Note: If you use vi, be sure to include the path to the location of the `all-systems` file.

Here is an example of an `all-systems-master-copy` file:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.5.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.5.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.5.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.5.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.5.0
```

And here is an example of an `all-systems` file that could be used in the first backup session, where only the Security Analytics Server, ESA host, and Malware Analysis host are backed up:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

Troubleshooting Information

- Be sure to save copies of the `all-systems` and `all-systems-master-copy` files in a safe location. Follow these recommendations:
  - Do not edit the `all-systems-master-copy` file.
  - If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure that each version of the file lists only those hosts that are currently being backed up, and the other hosts are commented out.
    For more information, see Post Backup Tasks.
- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.
- The `get-all-systems.sh` script generates a list of hosts that were defined in the Security Analytics user interface. Ensure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to Security Analytics, you use the Security Analytics user interface to ensure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.

- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the Security Analytics Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the Security Analytics Server. (Any Windows Legacy Collectors or AWS Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)
- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

RSA recommends that you run the `ssh-propagate.sh` script to automate sharing keys between the backup host and the host systems.

Note: If you have SSH keys that are protected with pass phrases, you can use `ssh-agent` to save time. For more information, refer to the man page for `ssh-agent`.

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:
   `chmod u+x ssh-propagate.sh`
2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. You are prompted for the password once per host, but you will not need to enter it repeatedly later during the backup process.

Task 4 - Check for Backup Requirements for Specific Types of Hosts

After you create the `all-systems` file to use for backup, you must check to see if any of the hosts listed in the file have requirements that must be met before you run the backup process.

For All Host Types

Perform the following steps for all host types:

1. On the Security Analytics Server, place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directories will be automatically restored during the upgrade process. After upgrading to 11.1., your custom certificate files will be located in `/etc/pki/nw/trust/import`.
   You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the Security Analytics Server and run the following command strings to perform the conversions listed.
   Convert a DER file (.crt .cer .der) to PEM
   `openssl x509 -inform der -in certificate.cer -out certificate.pem`
   Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Note:** Add the following qualifier to the command string to:
> `-nocerts` convert private keys exclusively.
> `-nokeys` convert certificates exclusively.

2. Manually record any custom configurations made to CentOS 6 (for example, driver customizations) for restoration after you update to CentOS 7. Custom configurations to CentOS 6 are not automatically backed up and restored.

For ESA Hosts with Mongo Databases

The default 10.6.x Mongo database password is `netwitness`. If you have customized this password, you could encounter an error while running the backup script. You can either use your custom Mongo database password during the backup, or you could change that password back to `netwitness` before running the `nw-backup.sh` script.

1. Find out if the Mongo database password is `netwitness` or if it has been modified.
2. If it has been modified, either change it back to `netwitness`, or be sure you know what the customized password is so that you can enter it during the backup.

See "ESA Config: Change MongoDB Password for admin Account" in the *NetWitness Suite Event Stream Analysis Configuration Guide* for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for Decoder, Concentrator, or Broker hosts, stop data capture and aggregation on all the systems that you are backing up. For instructions, refer to Appendix B. Stopping and Restarting Data Capture and Aggregation

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run `prepare-for-migrate.sh`

> **Caution:** This task stops log collection so you must perform this step immediately before you upgrade to minimize the loss of event collection. Complete this task in accordance with the backup and upgrade tasks in this guide.

Prerequisites

You need the following information before you prepare LCs and VLCs for upgrade.

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.
- If you set the password for `logcollector` user for RabbitMQ, you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.
2. Submit the following command string.

   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```

   This command:

   - Stops the Puppet Agent service.
   - Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.1.
   - Stops all the collection protocols in the Log Collector service.
   - Saves the list of Plugin accounts and RabbitMQ accounts.
   - Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.
   - Waits until the Log Collector queues are empty.
   - Stops the Log Collector service.
   - Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

The `prepare-for-migrate.sh` script:

- Sends informational, warning, and error messages to the console.
- Saves a session log in the `/var/log/backup/` directory.

You must fix any of the following errors and resume the preparation. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

- Log Collector queues with events but without consumers are found.
- Unable to stop the Puppet Agent service.
- Unable to stop a collection protocol in the Log Collector service.
- Unable to block event publishers to the RabbitMQ server.
- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.
- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting.

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the Security Analytics Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.1. upgrade, you can restore RabbitMQ user accounts.

To get a list of RabbitMQ usernames and passwords, run the following command:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

To restore RabbitMQ user accounts, refer to *Task 2 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL* in **Post Upgrade Tasks**.

For Bluecoat Event Sources

Bluecoat ProxySG event sources use FTPS protocol to upload log files to the Log Collector (LC) and Virtual Log Collector (VLC). The event source documentation contains the steps to configure VSFTPD service on the LC and VLC.

- If key material exists in `/root/vsftpd/` directory in 10.6.5.x, this material area will be backed up and restored. **If the material was in another location, you must back it up and restore it manually.**
- If the `/etc/vsftpd/vsftpd.conf` file exits in 10.6.5.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

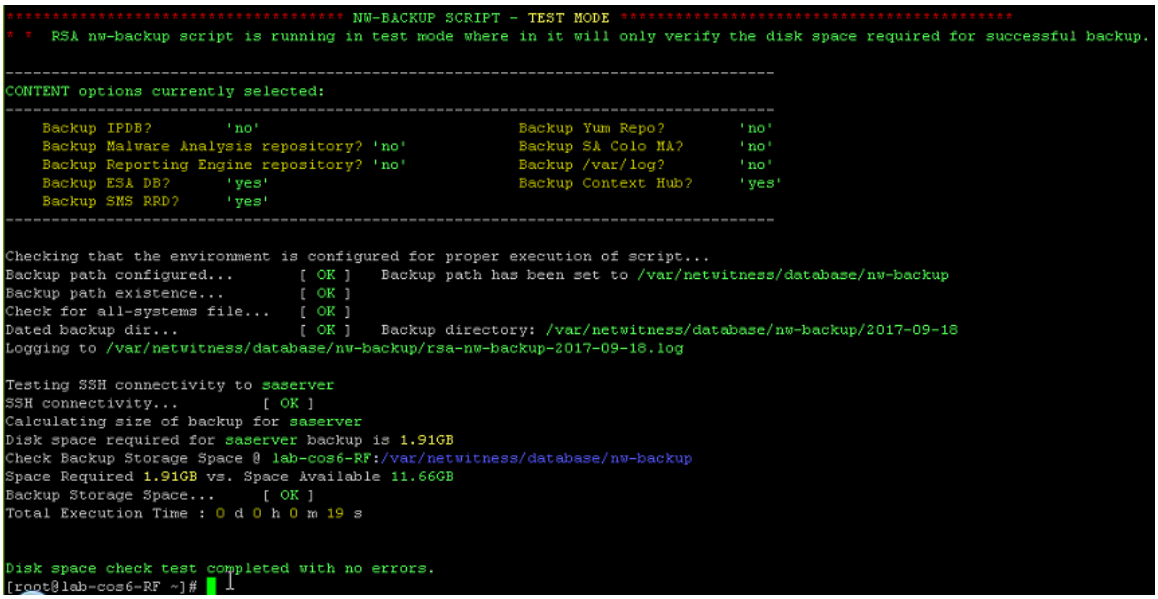
You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to ensure that you provide adequate space for the backup so that the backup captures all your data.

To check for adequate disk space:

1. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
2. Run the following command at the root directory level:
   `./nw-backup.sh -t`
   The output displays the amount of disk space that is required for the backup.

> **Note:** The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-d` option by using `-D`. Using the `-D` option will show how much space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

The following figure shows an example of the output from using the `-t` option.



Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.1.

> **Note:** The script will stop services as it runs. However, you can stop services manually before you run the script if needed.

When you run the backup script, you can choose from several options that are described in the following sections.

Usage:
`./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>`

General Options

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) -COPY`

`-b <path to write backups> : path to the location for storing backup files on a backup server.` **`For upgrading to 11.1, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

Note: Do **not** change the backup path in upgrade (-u) mode.

Note: When you run a backup with the `-u` option, all services are stopped. If you need to continue to use the 10.6.x machine after running the backup, reboot the 10.6.x system so that services are restarted.

Advanced Content Selection Options

`-c : back up Colocated Malware Analysis on SA servers. Default: (no)`

`-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)`

`-m : back up Malware Analysis File Repository. Default: (no)`

`-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)`

`-v : back up system logs (/var/log). Default: (no)`

`-y : back up YUM Web Server & RPM Repository. Default: (no)`

`-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)`

```
-C : If set: DISABLES back up of Context-Hub configuration and database.
Default: (not-set)

-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)
```

Test Options

```
 -t : performs script test run for disk space check only. Services are
not stopped and excludes execution of backup. Can be combined with (-d)
or (-D) and other flags. Default: (-t)
```

For example, the command:
`./nw-backup.sh`
would run the backup with options as set in the Header of the script itself.
OR, the command:
`./nw-backup.sh -ue /mnt/external_backup`
would run a normal backup using the backup path defined in the script, with the following options:

```
-u : enables the upgrade flag to run backup for upgrading to 11.1. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

When you run the script, the following text is displayed at the top of the script:

Caution:
```
RSA nw-backup script backs up configuration files, data, and
logs on the options provided in the script. It tars the content, with
options to store the backup files on the backup server, move or copy
them to external storage on a mount point (USB/NFS/SMB), or SCP them
back to the target host.
This backup script has been qualified on the following versions of
Security Analytics:
10.6.5.x
Use of this script on any other versions of the product may not give
expected results and may not be supported by RSA Customer
Service.Note: All non-RSA custom files, scripts, Cronjobs and other
important files should be placed in /root, /home/'user', OR /etc to be
included in the backup.
```

To run the backup script to back up your hosts:

1. Ensure that the `all-systems` file contains only the hosts to back up. For information, see Task 2 - Create a List of Hosts to Back up.
2. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
3. Begin the backup process by running the following command at the root directory level:

```
./nw-backup.sh -u
```

Note: You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.1. Do NOT make any changes to the header of the backup script for the backup path because the path is specific to the upgrade, and that data needs to be in a specific place.

When the text "`Backup completed with no errors`" is displayed, the backup has completed successfully.

A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:
`rsa-nw-backup-2017-03-15.log`

4. When the backup has completed, to ensure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   The following archive files are created:

   For all hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

   For Security Analytics Servers:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

   For ESA Hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `<hostname-IPaddress>-controldata-mongodb.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

The archived files are located in the `/var/netwitness/database/nw-backup` directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

Post Backup Tasks

Task 1 - Save a Copy of the `all-systems` File and the Backup Tar files

Make copies of the `all-systems` file, the `all-systems-master-copy` file, and the backup tar files and put the copies in a secure location. You cannot regenerate these files after you upgrade the Security Analytics Server (specifically the Admin service) to 11.1.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.1. upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

The following files are generated on all hosts by the backup scripts:

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

In addition to the files listed above, the following files will be generated on the Security Analytics Server and ESA hosts:

- `<hostname>-<host IP address>-mongodb.tar.gz`
- `<hostname>-<host IP address>-mongodb.tar.gz.sha256`

The backup script will also generate the following `controldata-mongodb.tar.gz` files.

Note: The backup script copies the following files from all ESA hosts to the Security Analytics Server's backup path .

- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz`
- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256`

Task 3 - (Conditional) For Multiple ESA Hosts, Copy `mongodb tar` files to Primary ESA Host

If you have multiple ESA host systems in your enterprise, copy the following two files from each ESA host to the `/opt/rsa/database/nw-backup/` directory on the Primary ESA host system (the host that has the ContextHub service running on it) :

- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Task 4 - Ensure All Required Backup Files are on Each Host

Before you upgrade to 11.1., ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

Note: The default paths for backup files are:
- Security Analytics Servers:`/var/netwitness/database/nw-backup`
- ESA hosts:`/opt/rsa/database/nw-backup`
- Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256`

Required Files for ESA Hosts

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Required Files for All Other Hosts

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Note: The following files are located in the `<hostname>-<host-IP-address>-backup.tar.gz` tar on all hosts:
`appliance_info`
`service_info`

Note: The paths to the location of the backup and restore files for iptables, NAT configurations, user accounts, and crontab entries are shown in the following list:
Backup paths:
`BUPATH=/opt/rsa/database/nw-backup` for the ESA Correlation Engine
`BUPATH=/var/lib/rsamalware/nw-backup` for the Malware Service
`BUPATH=/var/netwitness/database/nw-backup` for all other services
Restore locations:
`BUPATH/restore/etc/sysconfig` for Iptable rules
`BUPATH/restore/etc/sysconfig` for NAT configurations
`BUPATH/restore/etc` for Crontab entries
`BUPATH/restore/etc` for User Accounts (users are located in the `passwd` file, and groups are located in the `group` file. These are not restored during the upgrade process but can be restored manually.
`BUPATH/restore/etc/ntp.conf` for NTP configurations (must be restored using the NetWitness Suite UI)

Upgrade Tasks

This topic contains the tasks you must complete to upgrade Security Analytics 10.6.5.x to NetWitness Suite 11.1.

Caution: 1.) Make sure that you backed up your Security Analytics 10.6.5.x data before attempting to upgrade to NetWitness Suite 11.1.
2). Run the backup immediately before upgrading the hosts for each phase so that the data to avoid restoring stale data.
3.) This guide applies to physical host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite 11.1 Virtual Host Upgrade Guide* for the steps to upgrade virtual hosts. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

There two phases that you must complete in the order shown.

- Phase 1 - Upgrade SA Server, Event Stream Analysis (ESA), and Malware Analysis Hosts

  Note: For Event Stream Analysis, if you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

- Phase 2 - Upgrade All Other Hosts

Phase 1 - Upgrade SA Server, Event Stream Analysis, Malware Analysis Hosts, and Broker or Concentrator

Task 1 - Upgrade the 10.6.5.x SA Server to 11.1 NW Server

Follow the instructions under Upgrade 10.6.5.x SA Server Host to 11.1 NW Server Host.

Task 2 - Upgrade 10.6.5.x ESA to 11.1

Caution: If you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.1 to upgrade your ESA hosts.

1. Create the base image on your primary ESA host, set it up through the Setup program, and install **ESA Primary** on the host in the user interface on the **Admin Hosts** view.

   Note: If you have multiple ESA hosts in your enterprise, you must upgrade the ESA Primary host, where all the `mongodb` (Mongo Database) backup tar files are located, first, before you upgrade ESA Secondary hosts.

2. (Conditional) If you have a secondary ESA host, create the base image on your secondary ESA host, set it up through the Setup program, and install **ESA Secondary** on the host in the user interface on the **Admin Hosts** view.

Task 3 - Upgrade 10.6.5.x Malware Analysis to 11.1

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.1.

Task 4 - Upgrade 10.6.5.x Broker or 10.6.5.x Concentrator to 11.1

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.1.

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Upgrade All Other Hosts

See Appendix B. Stopping and Restarting Data Capture and Aggregation for instructions on how to stop and restart data capture and aggregation when upgrading the Decoder, Concentrator, and Log Collection hosts.

Decoder and Concentrator Hosts

1. Stop data capture and aggregation.
2. Complete the steps in Upgrade Non-NW Server Host to 11.1.
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the Backup Instructions.
2. Stop data capture on the Log Decoder.

3. Complete the steps in Upgrade Non-NW Server Host to 11.1.
4. Restart data capture on Log Decoder.

Note: After you upgrade, you will restart log collection after completing the Task 27 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task in the **Post Upgrade Tasks**.

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the Backup Instructions.
2. Back up your 10.6.5.x VLC by editing the `all-systems` file on host where you performed the backup.
   a. Make sure your `all-systems` file contents has this information before you perform this step.
   `vlc,<host-name>,<IP-address>,<UUID>,10.6.5.x`
   b. Run the following command to create backup.
   `./nw-backup.sh -u`
   See Backup Instructions for detailed procedures on how to back up the host.
3. Make sure the backup host contains the VLC backup in the following format.
   `<hostname>-<IPaddress>-root.tar.gz`
   `<hostname>-<IPaddress>-root.tar.gz.sha256`
   `<hostname>-<IPaddress>-backup.tar.gz`
   `<hostname>-<IPaddress>-backup.tar.gz.sha256`
   `<hostname-IPaddress>-network.info.txt`
   `all-systems-master-copy`
4. Power off the 10.6.5.x VLC so that a new 11.1 VM can be created with the same network configuration.
5. Deploy a fresh NetWitness 11.1 Non-NW Server host using the 11.1 NetWitness Suite ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.5.x VLC.
   This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.5.x VLC backup file.

Note: Make sure IPv6 is disabled.

a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings. Contents of `ifcfg-eth0` should be as follows.

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. Submit the following command string.

```
systemctl restart network.service
```

8. Create the backup directory.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new VLC in the `/var/netwitness/database/nw-backup` directory.
10. Complete the steps 2 through 12 inclusive in Upgrade a 10.6.5.x non-SA Server Host to 11.1 for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

All Other 10.6.5.x Hosts to 11.1

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.1.

Upgrade the 10.6.5.x SA Server Host to the 11.1 NW Server Host

Make sure that you have backed up 10.6.5.x data for the SA Server host. **You must follow the instructions in Backup Instructions to back up the host.**

Caution: Run the backup immediately before upgrading the SA Server to 11.1 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.1.

Complete the following steps to upgrade the 10.6.5.x SA Server host to the 11.1 NW Server host.

1. Create a base image on the host.

   a. Attach media (media that contains the ISO file, for example a build stick) to the host.
   You must use the build stick labeled "OEMDRV".
   See the *RSA NetWitness Suite Build Stick Instructions* for more information.

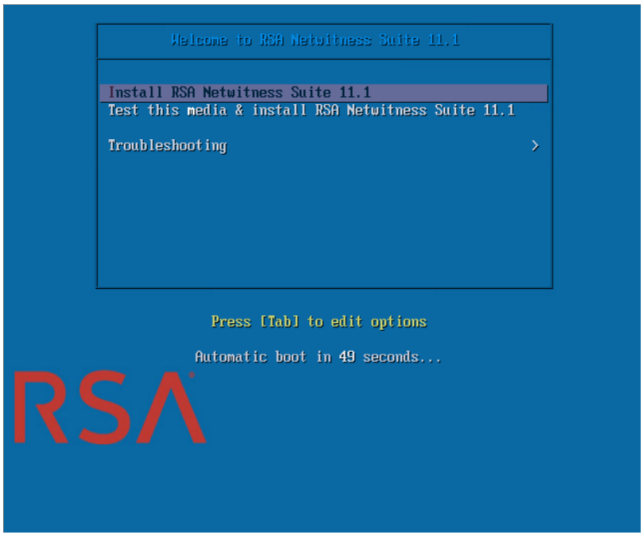
      - Hypervisor installations - use the ISO image.
      - Physical media - use the ISO file to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the ISO file. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO file.

   b. Log in to the host with and reboot it.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   c. Select **F11 (boot menu)** during reboot to select a boot device and boot to the connected media.
   After some system checks during booting, the following **Welcome to RSA NetWitness® Suite 11.1** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

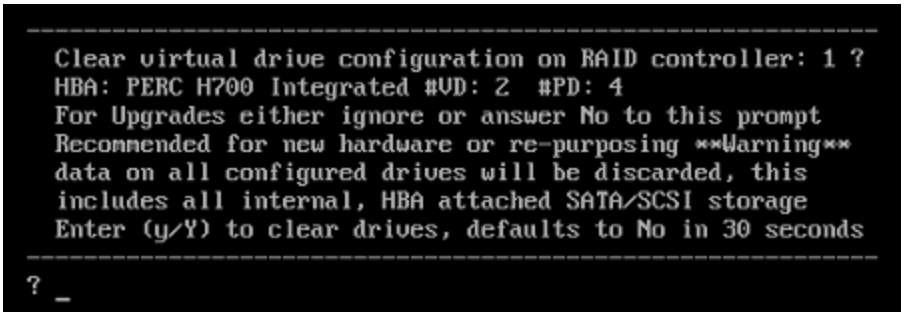
d. Select **Install RSA Netwitness Suite 11.1** (default selection) and press **Enter**.



The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**.

e. Enter **n** (No).

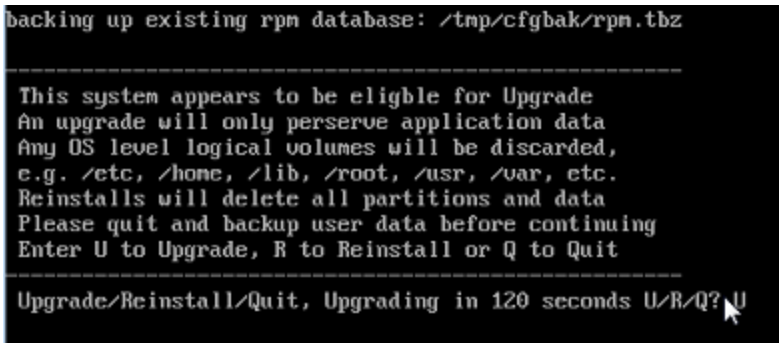
The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives.



The **Upgrade/Reinstall/Quit(U/Q/R?** prompt is displayed.

f. Type **U** to upgrade the host.

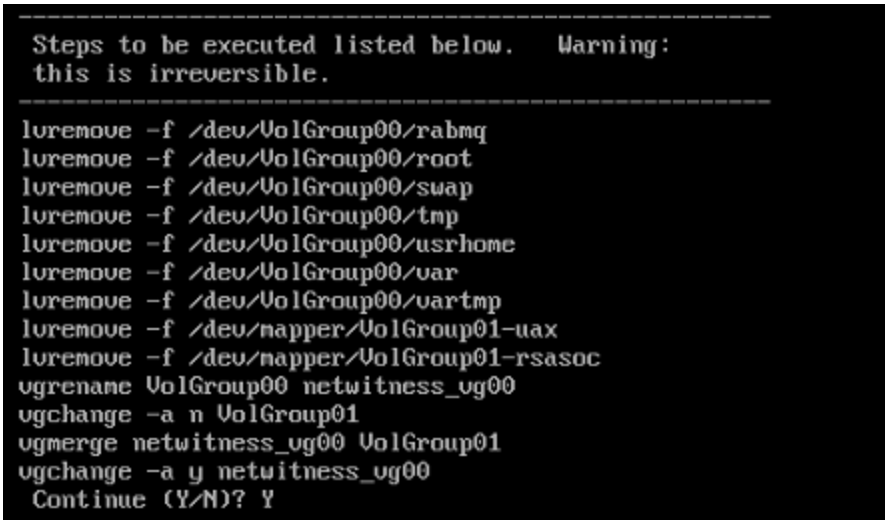
If you ignore the prompt, it will select U in 120 seconds.



It takes a few minutes for CentOS7 components to install. The installation program

displays the components as they are installed, which varies depending on the appliance. When CentOS7 installation is complete, the **Continue (Y/N)?** prompt is displayed.

g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.



The old operating system is about to be removed. Continue (Y/N)? warning is displayed.

h. Type **Y** and press **Enter** to confirm that you want to replace the operating system.

When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

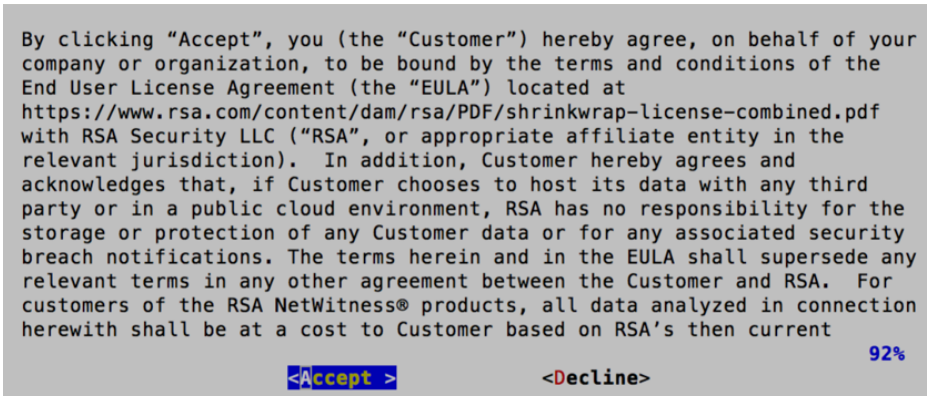
Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).

i. Log in to the host with the `root` credentials.

2. Run the `nwsetup-tui` command to set up the host.
   This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

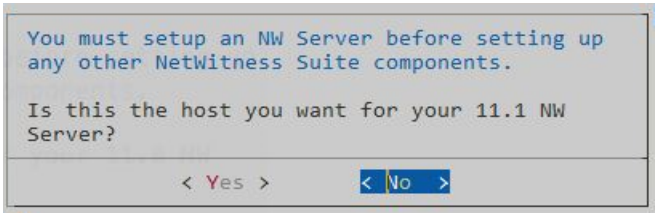
3. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.1 NW Server** NW Server prompt is displayed.

Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must restart the step up program and complete the all the steps (steps 2 through 11) to correct this error.

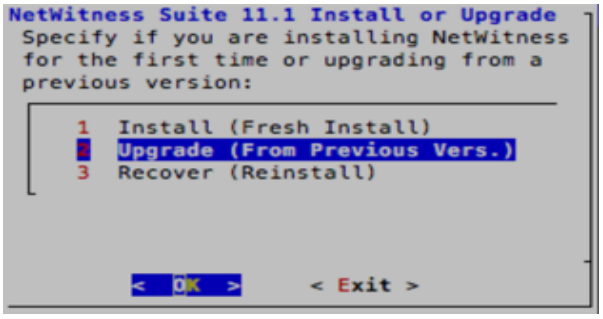
4. Tab to **Yes** and press **Enter**.



Choose **No** if you already upgraded the NW Server to 11.1.

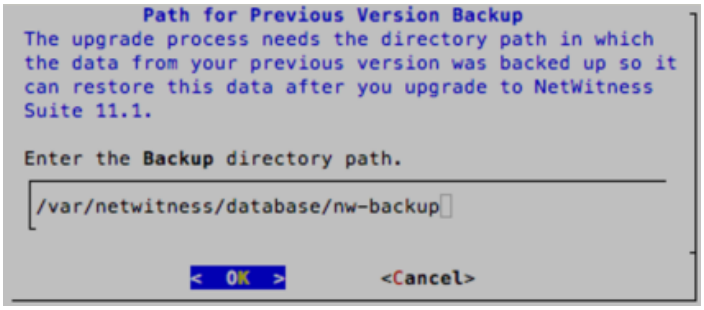
The **Install** or **Upgrade** prompt is displayed.

5. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.



The **Backup** path prompt is displayed.

6. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.



This table lists the backup and restore paths by host/service.

Host	Backup Path	Restore Path
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
All Other Hosts	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

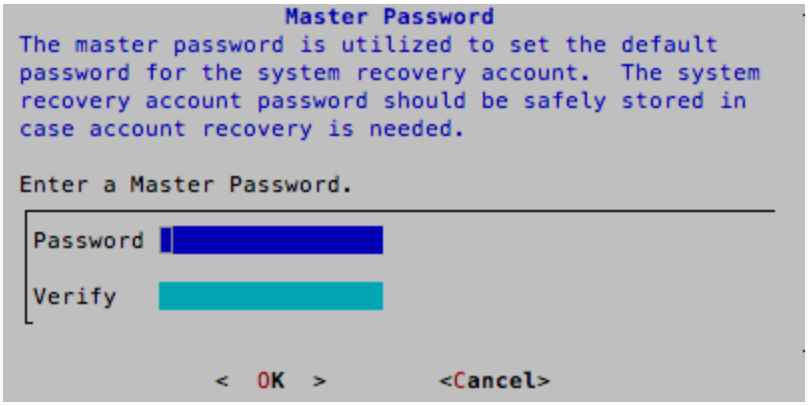
The **Master Password** prompt is displayed.

The following list of characters are supported for Master Password and Deployment Password:

- Symbols : ! @ # % ^ + ,
- Numbers : 0-9
- Lowercase Characters : a-z
- Uppercase Characters : A-Z

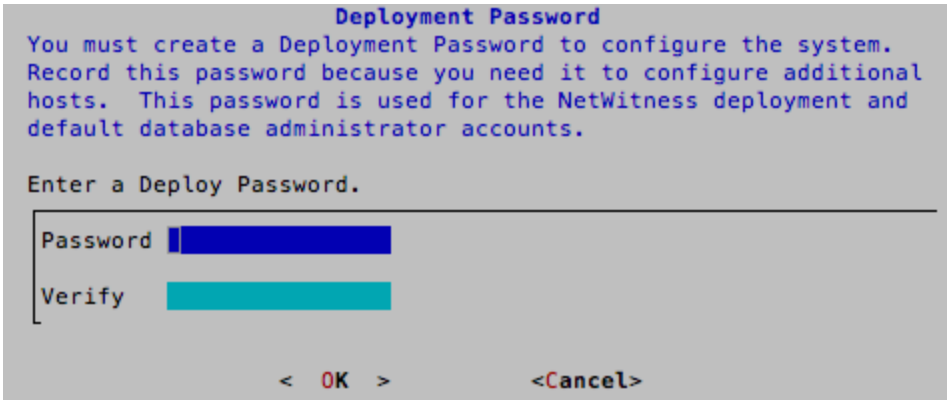
No ambiguous characters are supported for Master Password and Deployment Password. For example:
space { } [ ] ( ) / \ ' " ` ~ ; : . < > -

7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



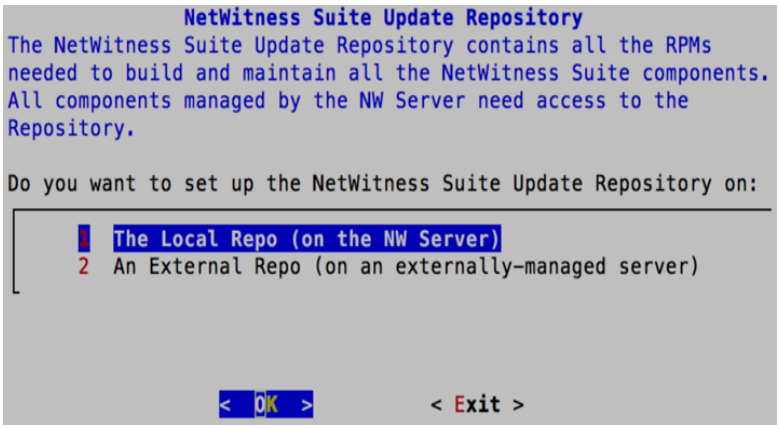
The **Deployment Password** prompt is displayed.

8. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



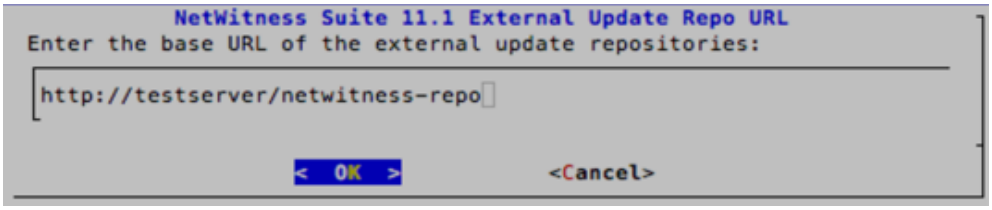
The **Update Repository** prompt is displayed.

9. Use the down and up arrows to select the location from which you want to apply version updates to your hosts, tab to **OK**, and press **Enter**.



- If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which upgrade to NetWitness Suite 11.1. If the program cannot find the attached media, you receive the following prompt.

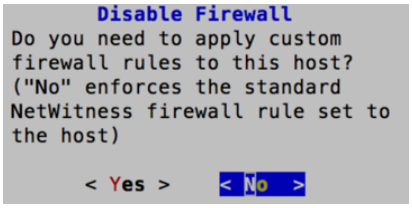
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates. Refer to Appendix D. Create External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



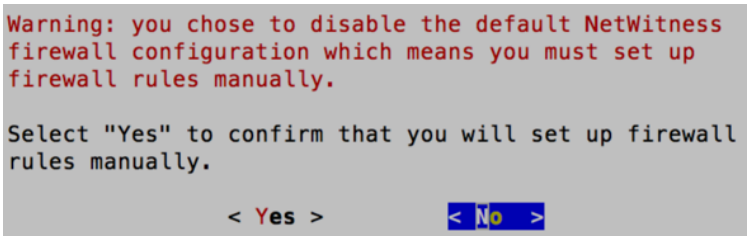
  Enter the base URL of the NetWitness Suite external repo and click **OK**.
  See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

The **Disable** or use standard **Firewall** configuration prompt is displayed.

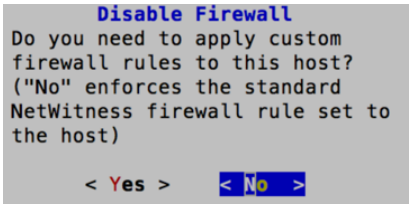
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.



- If you select **Yes** to confirm your selection.

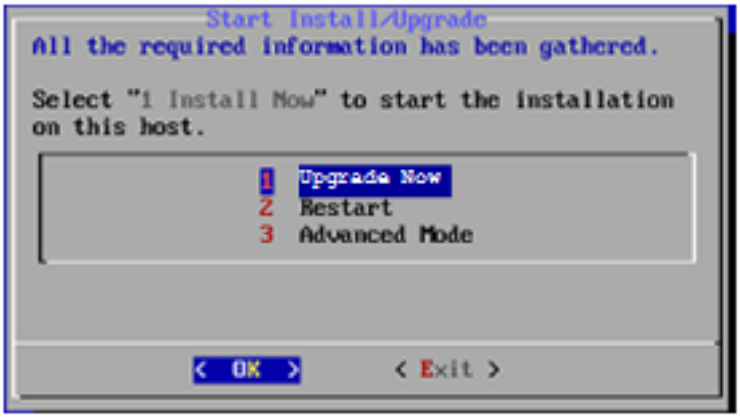


- If you select **No**, the standard firewall configuration is applied.



The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.



When **Installation complete** is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

12. Complete the NW Server before you upgrade any of the non-SA Server hosts to 11.1.

Upgrade a 10.6.5.x non-SA Server Host to 11.1.

Make sure that you backed up 10.6.5.x data for the host. **You must follow the instructions in Backup Instructions to back up the host.**

Caution: Run the backup immediately before upgrading the host to 11.1 so that the data is as recent as possible.

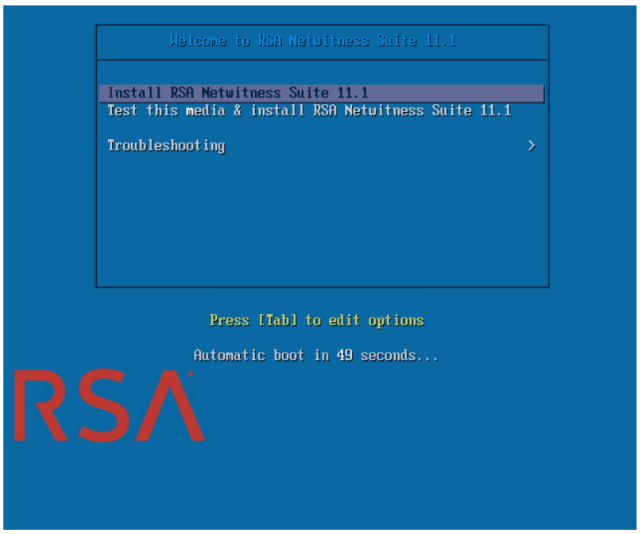
Complete the following steps to upgrade a 10.6.5.x non-SA Server Host to 11.1.

1. Create a base image on the host.
   a. Attach media (media that contains the ISO file, for example a build stick) to the host. See the *RSA NetWitness Suite Build Stick Instructions* for more information.
      - Hypervisor installations - use the ISO image.
      - Physical media - use the ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the ISO. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO file.
   b. Log in to the host and reboot it.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

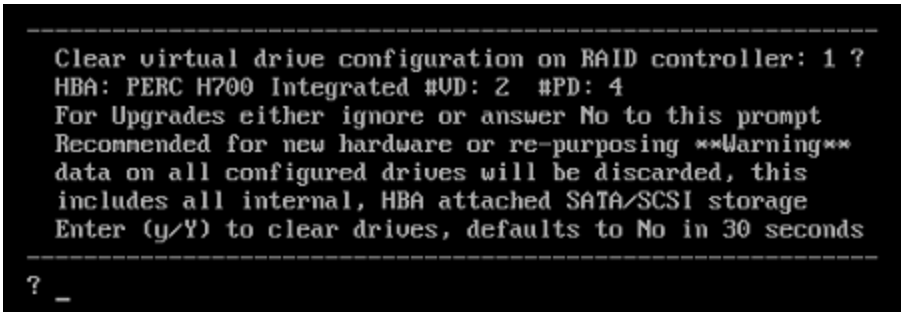
c. Select **F11 (boot menu)** during reboot to select a boot device and boot to the connected media.
After some system checks during booting, the following **Welcome to RSA NetWitness® Suite 11.1** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

d. Select **Install RSA Netwitness Suite 11.1** (default selection) and press **Enter**.



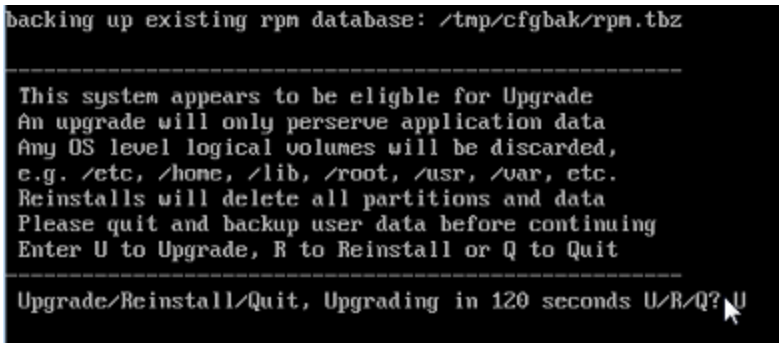
The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**.

e. Enter **n** (No).
The default action is **No**, so if you ignore the prompt and it will select **No** in 30 seconds and will not clear the drives.



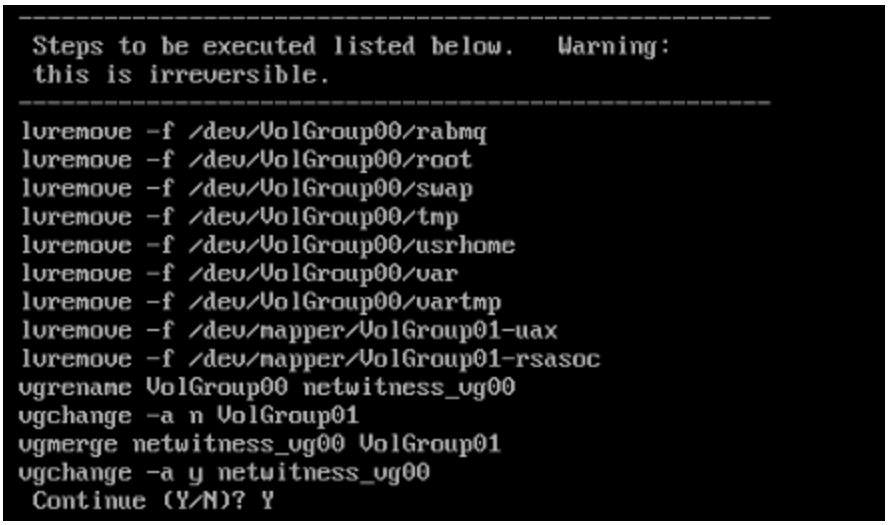
The **Upgrade/Reinstall/Quit (U/R/Q?)** prompt is displayed.

f. Type **U** to upgrade the host.
If you ignore the prompt, it will select **U** in 120 seconds.



It takes a few minutes for CentOS7 components to install. The installation program displays the components as they are installed which varies depending on the appliance. When CentOS7 installation is complete, the **Continue (Y/N)?** prompt is displayed.

g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.



The old operating system is about to be removed. Continue (Y/N)? warning is displayed.

h. Type **Y** and press **Enter** to confirm that you want to replace the operating system.

When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

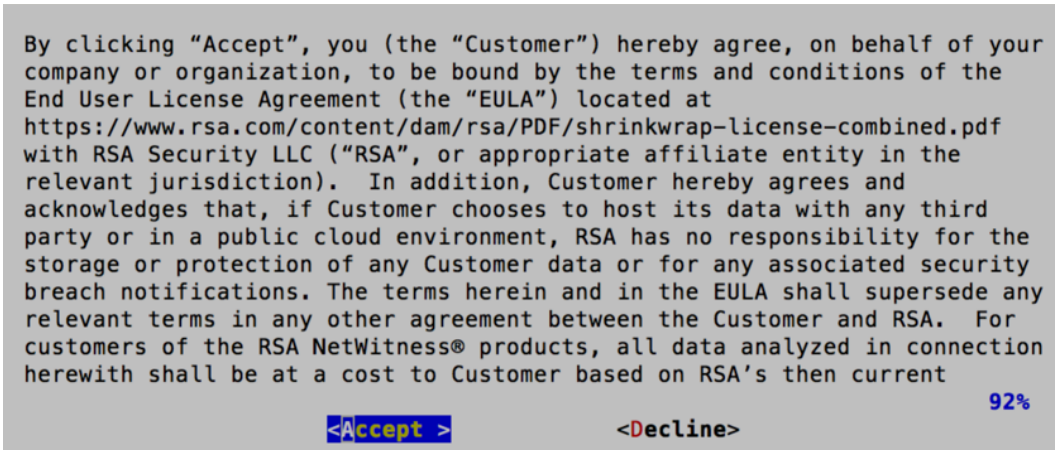
Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).

i. Log in to the host with the `root` credentials.

2. Run the `nwsetup-tui` command to set up the host.

   This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

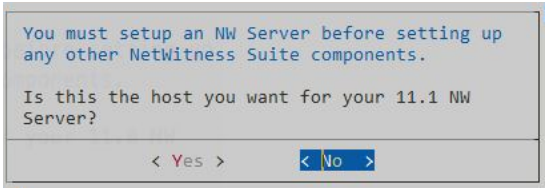
3. Tab to **Accept** and press **Enter**.



   The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

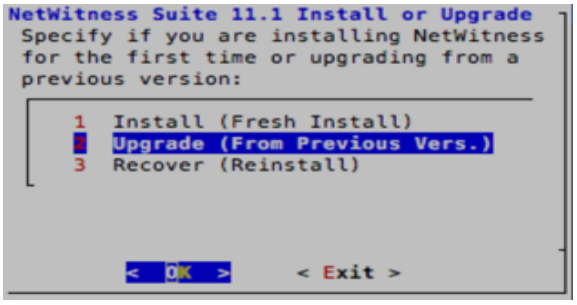
   Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must restart the step up program and complete the all the steps (steps 2 through 11) of Upgrade the 10.6.5.x SA Server Host to the 11.1 NW Server Host to correct this error.

4. Tab to **No** and press **Enter**.



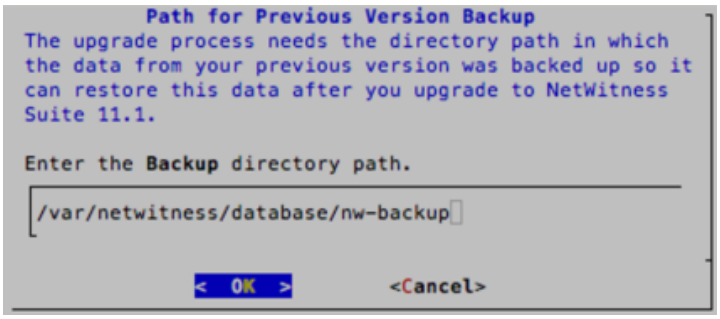
   The **Install** or **Upgrade** prompt is displayed.

5. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.



   The **Backup** path prompt is displayed.

6. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.



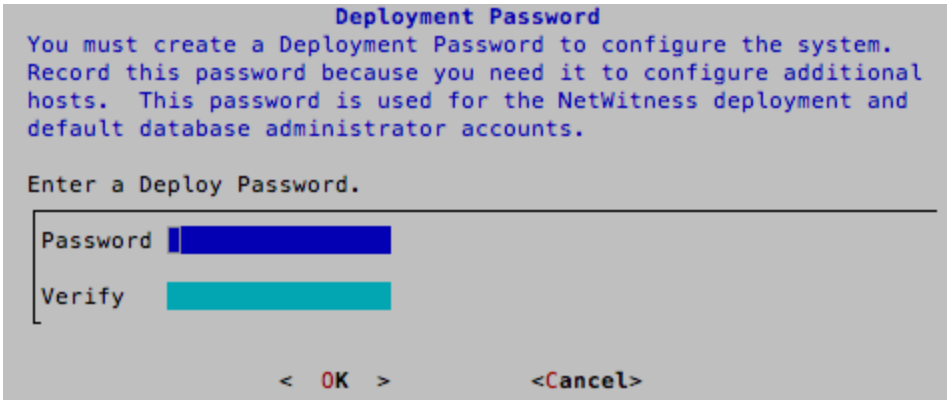
   This table lists the backup and restore paths by host/service.

Host	Backup Path	Restore Path
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
All Other Hosts	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

   The **Deployment Password** prompt is displayed.

Note: You must use the same deployment password that you used when you upgraded the NW Server.

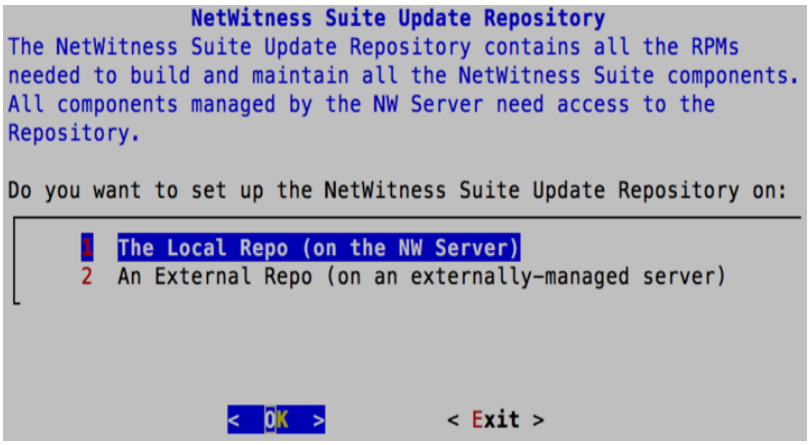
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



The **Update Repository** prompt is displayed.

Select the same repo you selected when you upgraded the NW Server Host for all hosts.

8. Use the down and up arrows to select the location from which you want to apply version updates to your hosts (for example, **1 The Local Repo (on the NW Server)** , tab to **OK**, and press **Enter** .

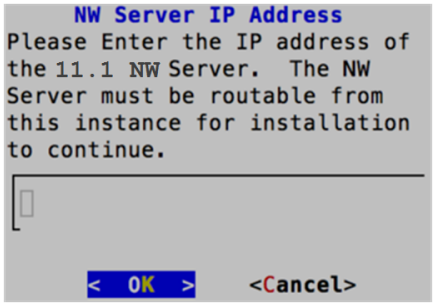


- If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can upgrade to NetWitness Suite 11.1.
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates. Enter the base URL of the NetWitness Suite external repo and click **OK**. The repositories give you access RSA updates and CentOS updates. Refer to Appendix D. Create External

Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

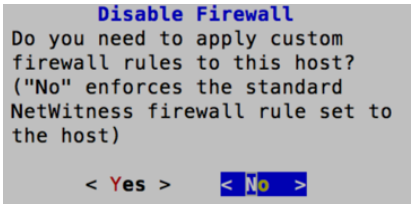
The **NW Server IP Address** prompt is displayed.

9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

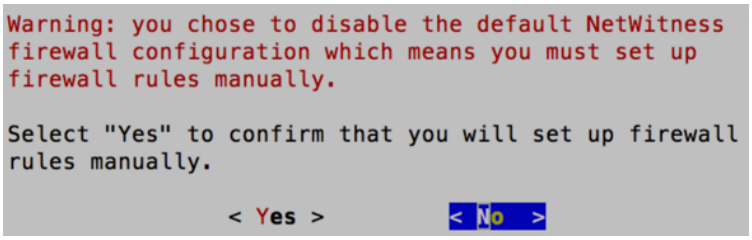


The **Disable** or use standard **Firewall** configuration prompt is displayed.

10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration. The following example shows **No** - standard firewall configuration selected.



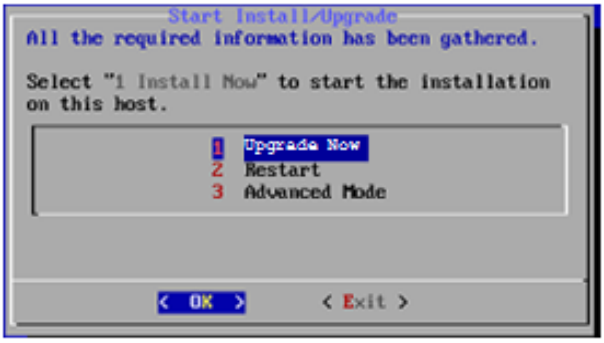
- If you select **Yes**, confirm your selection.



- If you select **No**, the standard firewall configuration is applied.

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.



When **Installation complete** is displayed, you have upgraded the host to the 11.1.

12. Install the service on this host:

    a. Log into NetWitness Suite and click **ADMIN** > **Hosts**.
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

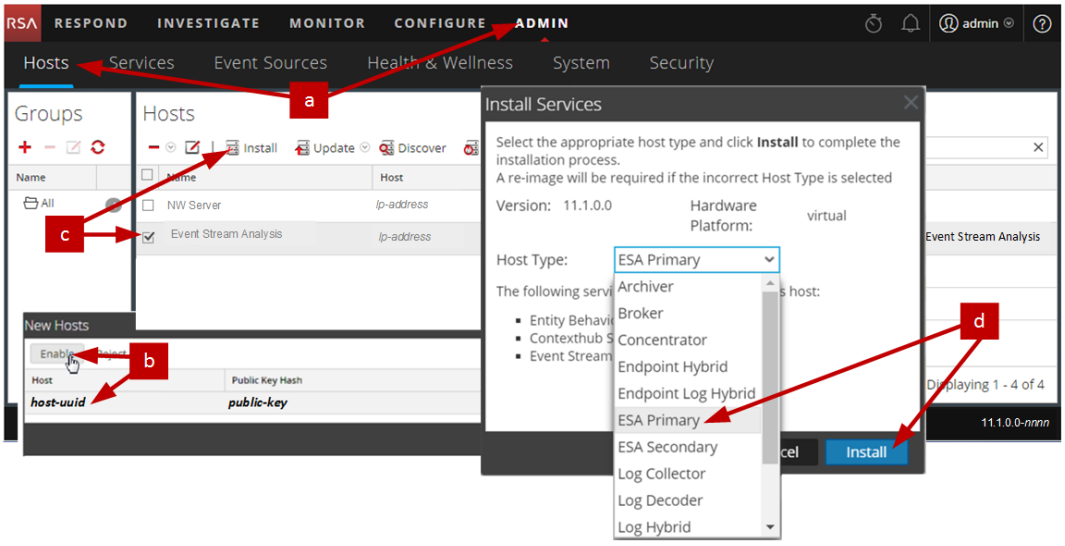
    Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

    b. Click on the host in the **New Hosts** dialog and click **Enable**.
    The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

    c. Select that host in the **Hosts** view (for example, **Event Stream Analysis** and click Install.

    The **Install Services** dialog is displayed.

    d. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



You have completed the upgrade of the non-NW Server host in NetWitness Suite

Note: When you upgrade a Respond host from 10.6.5.x to 11.1, it takes a period of time for Respond to come back online. This is caused by Respond indexing data while it is restored. The size of the data in the Mongo database will determine the time.

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.1. These tasks are organized by the following categories.

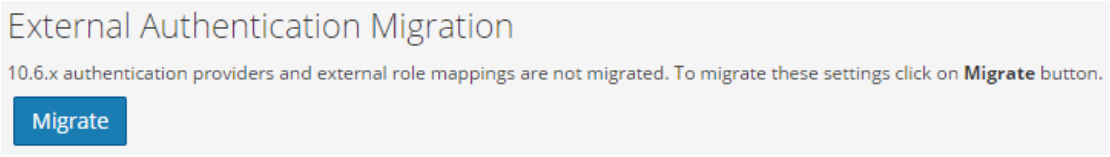
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Investigate
- Log Collection
- Reporting Engine
- Respond
- SecOps Manager (RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)
- Warehouse Connector
- Backup

NW Server

Task 1 - Migrate Active Directory (AD)

The first time you log into the NetWitness Suite 11.1 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Suite 11.1 with your `admin user` credentials.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.



3. Click **Migrate**.
   The migration is complete and the dialog closes.

Task 2 - Modify Migrated AD Configuration to Upload Certificate

If you authenticated through Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.5.x, you must modify the migrated AD configuration to upload the Active Directory server certificate.

Complete the following procedure to modify the migrated AD configuration to upload the certificate.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** and click the **Settings** tab.
2. Under **Active Directory Settings**, select an AD configuration and click .

   The Edit Configuration dialog is displayed.
3. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
4. Click **Save**.

Task 3 - Reconfigure Pluggable Authentication Module (PAM) in 11.1

You must reconfigure PAM after you upgrade to 11.1. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite System Security and User Management Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

You can refer to your 10.6.5.x PAM configuration files in the **/etc** directory in the your 10.6.5.x backup data for guidance.

Task 4 - Restore NTP Servers

You must use the NetWitness Suite 11.1 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *RSA NetWitness® Suite System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 5 - Restore Licenses for Environments without FlexNet Operations-On Demand Access

If your environment does not have access to FlexNet Operations-On Demand, you need to re-download your NetWitness Suite licenses. Refer to "Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on how to re-download licenses. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

(Conditional) Task 6 - If You Disabled Standard Firewall Config - Add Custom IPtables

During the upgrade, you have the option of using these rules or disabling them. If you disabled them, follow these instructions as a baseline to create a user-managed firewall rule sets on all the hosts for which you disabled the standard firewall configuration.

Note: You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the restore folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.
2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.
   `/etc/sysconfig/iptables`
   `/etc/sysconfig/ip6tables`
3. Reload the `iptables` and `ip6tables` services.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditional) Task 7 - Specify SSL Ports If You Never Set Up Trusted Connections

Complete this task only if you never set up Trusted Connections. You would not have set up Trusted Connections if you:

- Used the base ISO image for 10.3.2 or earlier.
- Updated the system using RPMs exclusively to get to 10.6.5.x.

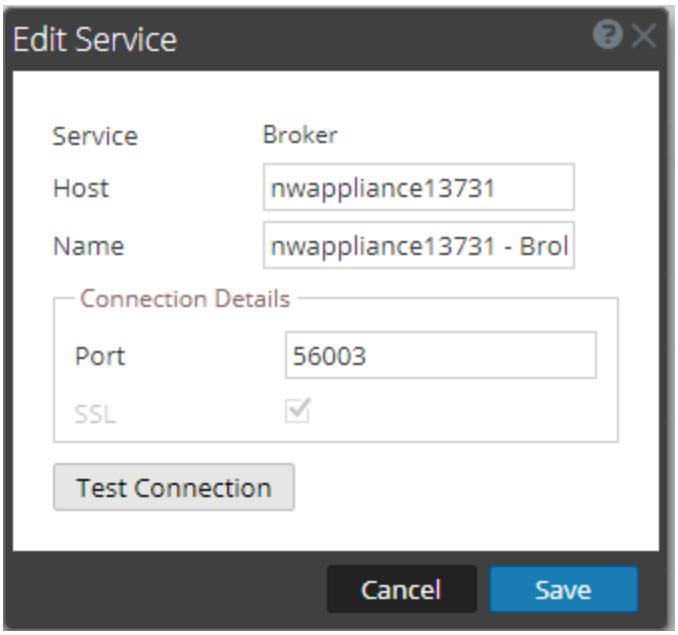
NetWitness Suite 11.1 cannot communicate with the core services for these customers because they are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Services**.
2. Select each core service and change there ports from Non-SSL to SSL ports.

Service	Non-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004

Service	Non-SSL	SSL
Log Decoder	50002	56002

3. Click (Edit) from the SERVICES view toolbar.
   The Edit Service dialog is displayed.
4. Change the port from Non-SSL to SSL as shown in the table and click **Save** (for example, change the Broker port from 50003 to 56003).



Task 8 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File

Problem: When a user updates from 10.6.5 to 11.1 and 11.0.0.0 to 11.1, if they have a global auditing set up, audit log templates are not getting updated in Logstash output conf file.

Workaround: If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click save to apply the latest Audit log configuration.

If you had global auditing configured in 11.0.x, you must complete the following procedure to apply the latest Global Auditing configuration.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications**.
   The **Global Notifications** view is displayed.
2. Click the **Servers** tab, select any syslog server.
3. Click (edit icon) and click **Save**.

RSA NetWitness® Endpoint

Task 9 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

You must reconfigure the Legacy Endpoint recurring feed due to the change in Java version. Complete the following step to fix this problem.

1. Import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness Endpoint Integration Guide* to import the certificate.
   Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint Insights

(Optional) Task 10 - Install Endpoint Hybrid or Endpoint Log Hybrid

See:

RSA NetWitness Suite 11.1 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Suite 11.1 Virtual Host Installation Guide for instructions for installation on a virtual host.

Task 11 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite 11.1, the virtual host is `/rsa/system`. For 10.6.5.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.
3. SSH to the NW Server and log in with `root` credentials.
4. Submit the following command to add all certificates to the truststore.
   `orchestration-cli-client --update-admin-node`

5. Submit the following command to restart the RabbitMQ server.
   `systemctl restart rabbitmq-server`
   The NetWitness Endpoint account should automatically be available on RabbitMQ.
6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Event Stream Analysis Tasks

Task 12 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.1.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
2. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. Click **ADMIN** > **Services**, select the Context Hub service, in the action commands ( ) drop-down menu, click **View** > **Config** > **Lists** tab).
   b. Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Suite ESA Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 13 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL

If you integrate with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint, you must configure Mutually Authenticated SSL on each integrated system so that the application can authenticate itself when connecting to the RabbitMQ message bus.

Note: Use the RabbitMQ usernames and passwords that were obtained when you backed up your 10.6.5.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Suite by logging into the host and running the following `rabbitmqctl` command.

   ```
   > rabbitmqctl add_user <username> <password>
   ```

   For example:

   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

2. Set permissions for users by running the following command (use the username from step 1):

   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"
   ```

   For example:

   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*", ".*", ".*"
   ```

Task 14 - Enable Threat - Malware Indicators Dashboard

In 11.1, the 10.6.5.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.5.x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.1.
2. Set datasource for new dashlets.

   See "Dashlets" in RSA Link (https://community.rsa.com/docs/DOC-81463) for a description of Dashlets in the context of NetWitness Suite.

Investigate

Task 15 - Make Sure User Roles Have Customized User Roles Have `Investigate-server` Permissions for Event Analysis Access

After you upgrade to 11.1.0.0, any customized user role does not have `investigate-server.*` permission enabled by default. Complete the following procedure to make sure that the appropriate user roles have permission to access Event Analysis.

1. Log in to NetWitness Suite 11.1.0.0 with your `Admin user` credentials.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** .
3. Click the **Roles** tab.
4. Select the roles that need `investigate-server.*` permissions and click (edit icon).
5. Select the **Investigate-server** tab under under **Permissions**.

6. If investigate-server checkbox is not checked, check it for the users that require Event Analysis access.

7. Click **Save**.

Log Collection

Task 16 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.1 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

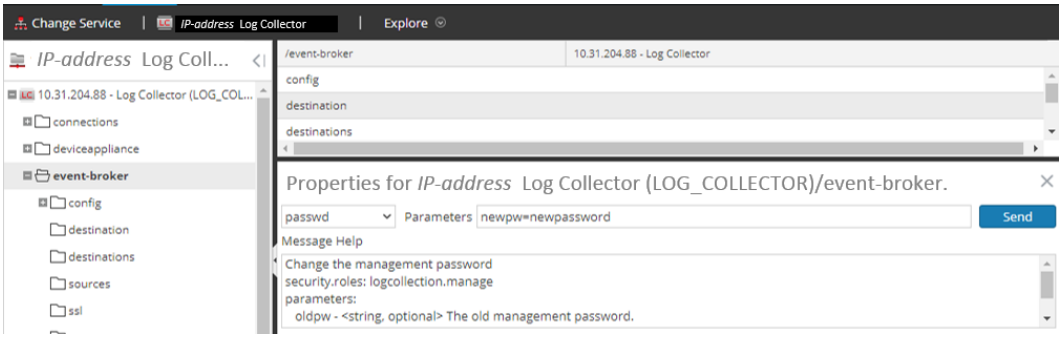
The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Update Log Collector Service RabbitMQ User Account Password

If the logcollector service RabbitMQ user account password was changed, you must reenter it after the 11.1 upgrade.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Services**.
2. Select the Log Collector service.
3. Click (Actions) > **View** > **Explore**.
4. Right click `event-broker` > **Properties** .

5. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders)

Task 17 - Enable FIPS Mode

FIPS is enabled on all services except Log Collector, Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder. For information about how to enable FIPS for these services, see the "Sys Maintenance: Activate or Deactivate FIPS" topic in the *RSA NetWitness® SuiteSystem Maintenance Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Reporting Engine

(Conditional) Task 18 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the back up you made prior to the upgrade. The Backup script backs up the 10.6.5.x CA certificates into the `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts` directory.

Complete the following procedure to restore the CA certificates in 11.1.

1. SSH to the NW Server host.
2. Export the CA certificates.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Copy the CA pem into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 19 - Restore External Storage for Reporting Engine

If you have external storage for the Reporting Engine (such as SAN or NAS for storing reports), you must restore the mount you unlinked before the upgrade. See "Reporting Engine: Add Additional Space for Large Reports" in the *RSA NetWitness® Suite Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

(Conditional) Task 20 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.1. See "Add a Role and Assign Permissions" in the *RSA NetWitness Suite System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 21 - Restore Respond Service Custom Keys

In 10.6.5.x, if you added custom key for use in the **groupBy** clause, the `alert_rules.json` file was modified. The `alert_rules.json` file contains aggregation rule schema. RSA moved the `alert_rules.json` file to the following new location: `/var/lib/netwitness/respond-server/scripts`

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.

   This directory is where the `alert_rules.json` file is restored from the 10.6.5.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.1.

   This is the new file for 11.1.

3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 22 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.1 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.x, you must:

1. Go to the to the `/opt/rsa/im/scripts` directory.
   This directory is where the following Respond service normalization scripts are restored from the 10.6.5.x backup.
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Copy any custom logic from the 10.6.5.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Suite 11.1 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
   The `alert_rules.json` file contains aggregation rule schema.

Task 23 - Add Respond Notification Settings for Custom Roles

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**CONFIGURE** > **Respond Notifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. You will also need to add permissions to your custom roles. See the "Respond Notification Settings Permissions" topic in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 24 - Manually Configure Respond Notification Settings

The Incident Management notification settings in NetWitness Suite 10.6.5.x are different from the Respond notification settings available in 11.1, so your existing 10.6.5.x settings will not migrate to 11.1.

NetWitness Respond notification settings enable email notifications to be sent to SOC Managers and the Analyst assigned to an incident when an incident is created or updated.

To manually configure the Respond Notification Settings, go to **CONFIGURE** > **Respond Notifications.** See the "Configure Respond Email Notification Settings" procedure in the *NetWitness Respond Configuration Guide*.

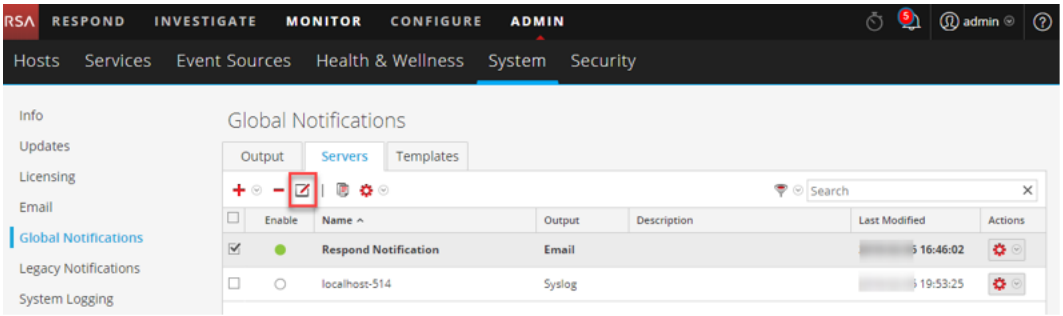
Notification Servers from 10.6.5.x will not display in the Email Server drop-down list. The email servers must be edited and saved in the Global Notification Servers panel (**ADMIN** > **System** > **Global Notifications** > **Server** tab).

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications** > **Server** tab.
2. Go to **CONFIGURE** > **Respond Notifications**. The Respond Notifications Settings view is displayed.

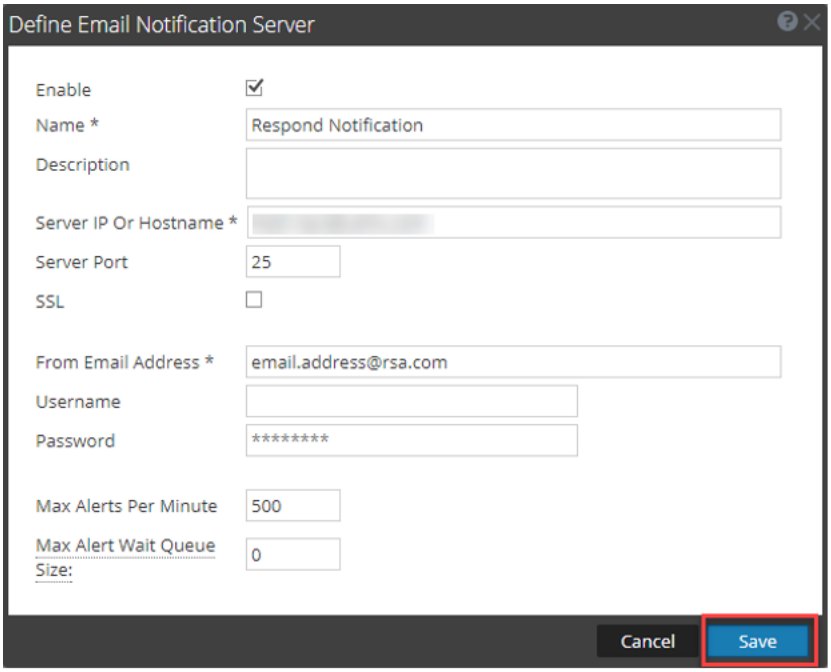
   Notice that the email notification servers do not appear in the EMAIL SERVER drop-down list.
3. Click the **Email Server Settings** link.

   You will see the Global Notifications panel.
4. Click the **Servers** tab.
5. For each of your email notification servers:

   a. Select the Email notification server and click .



b. In the Define Email Notification Server dialog, click **Save**.



6. Go back to **CONFIGURE** > **Respond Notifications**. Your servers will appear in the **EMAIL SERVER** drop-down list.
   Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

Task 25 - Update Default Incident Rule Group By Values

Four of the default incident rules now use ”Source IP Address” as the Group By value. To update the default rules, change the Group By value of the following default rules to “Source IP Address”:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

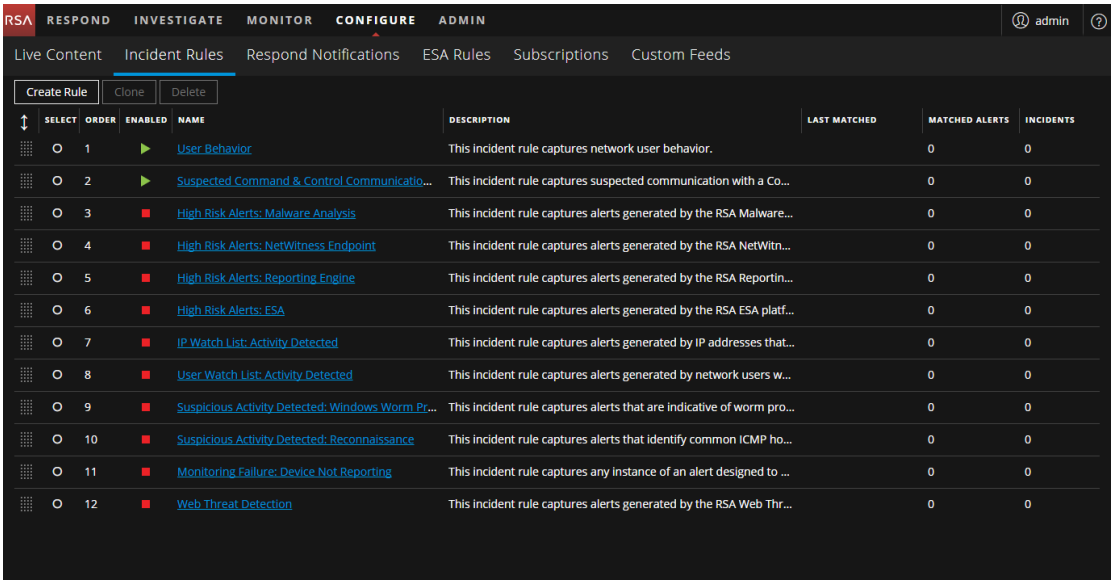
1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update. The Incident Rule Details view is displayed.
2. In the **Group By** field, select the new Group By value.
3. Click **Save** to update the rule.

Task 26 - Add Group By Field to Incident Rules

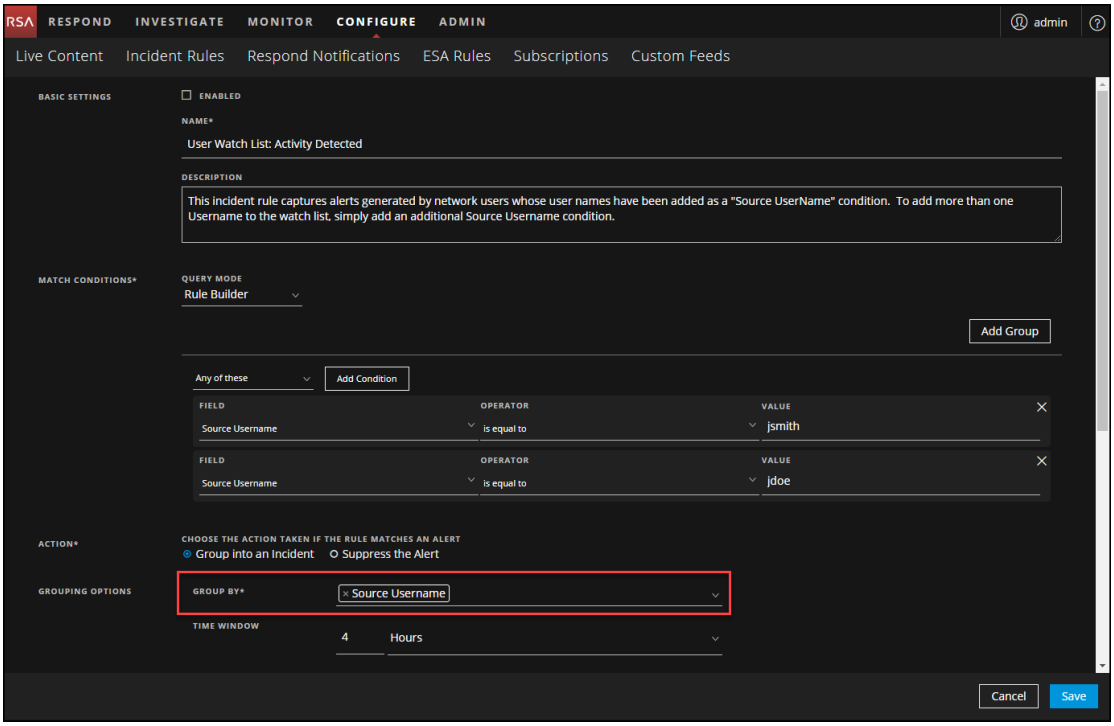
The **Group By** field is not required in 10.6.5, but it is required in 11.1. After you upgrade to 11.1, some incident rules will not have a **Group By** field, so you must add them to the rules or the rules will not work and they will not create incidents.

Complete the following steps for each incident rule:

1. Log in to RSA NetWitness® Suite.
2. Go to **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



3. In the Group By field, verify that a Group By value is selected. If not, select a Group By value.



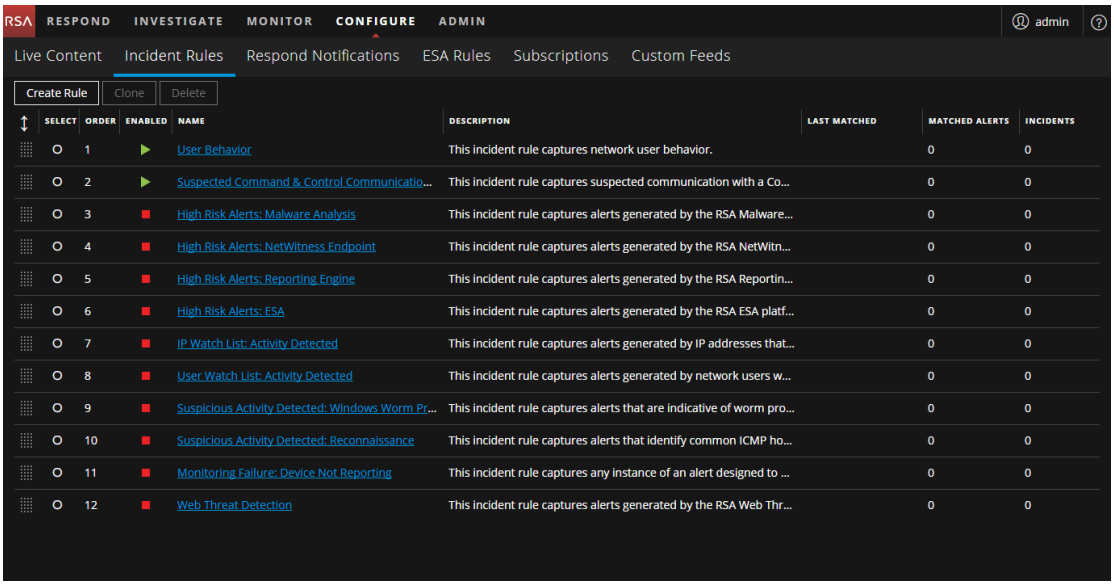
4. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 27 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task

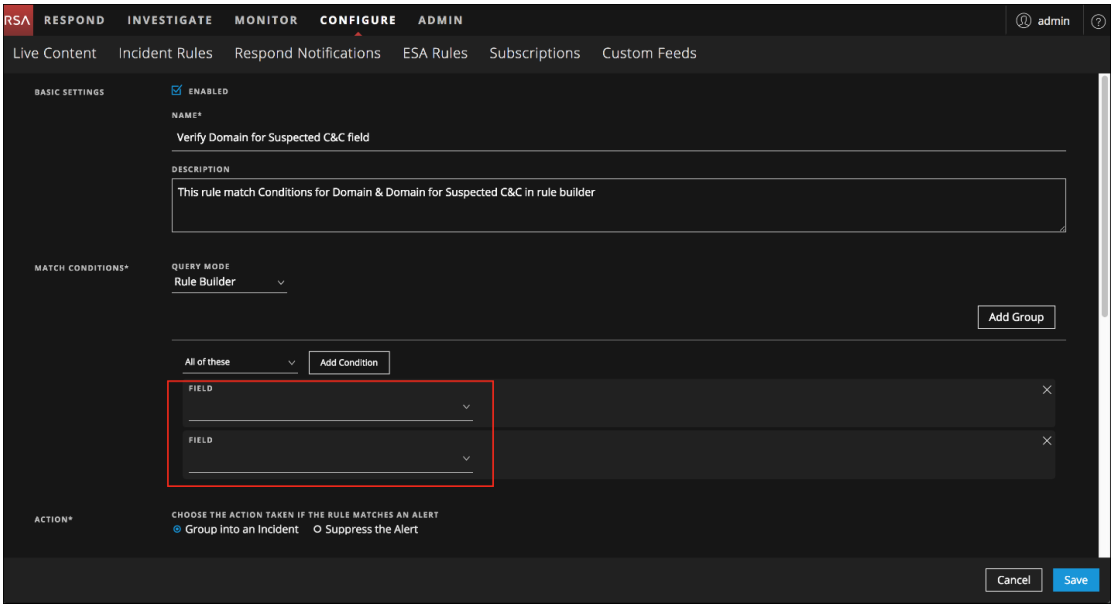
Modify the incident rules that you identified in the Task 4 - Check Aggregation Rules Match Conditions for "Domain" or "Domain for Suspected C&C" upgrade preparation task, which contained Domain or Domain for Suspected C&C in the matching conditions in rule builder, to use only Domain.

For each rule that you previously identified:

1. In the **NetWitness Suite** 11.1 menu, select **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



2. In the **Match Conditions** section, in the blank fields, select **Domain** in the drop-down list and then select the conditions that you previously identified in the pre-upgrade tasks.



3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

SecOps Manager

(RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)

Task 28 - Reconfigure NW SecOps Manager Integration

For information on how to reconfigure NW SecOps for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Warehouse Connector

Task 29 - Restore `keytab` Files, Mount NFS, Install Service

1. Restore the `keytab` files from `<backup-path>/restore` directory.
2. Restore the Kerberos Realm Configuration from the `<backup-path>/restore/etc/krb5.conf` into `/etc/krb5.conf`.
3. (Conditional) If you perform the upgrade from a Non - FIPS environment and the `isCheckValidationRequired` parameter is not enabled in the destination, to configure the SFTP destination:
   a. SSH to the Warehouse Connector host and submit the following commands:
      ```
      cd /root/.ssh/
       mv id_dsa id_dsa.old
      OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_dsa.old -out id_dsa
      ```
      You are prompted for the pass phrase.
   b. Enter the Encryption password.
   c. Run the following command.
      ```
      chmod 600 id_dsa
      ```
4. Install the Warehouse Connector.
   See the *NetWitness Suite Warehouse Connector Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 30 - Refresh Warehouse Connector Lockbox and Start Stream

Note: If the streams have auto start turned on in 10.6.5.x, there will be a small delay before you will see the Warehouse Connector service in the NetWitness Suite User Interface.

1. Refresh the Lockbox of Warehouse Connector.
2. SSH to the Warehouse Connector and log in with root credentials.
3. Restart the service.
   ```
   service nwwarehouseconnector restart
   ```

4. (Conditional) If the auto start was not enabled in 10.6.5.x, you must start the stream manually after the service restarts.

Backup

Task 31 - Remove Backup-Related Files from Host Local Directories

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.1. before you remove the backup-related files from the local directories on your 11.1. hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.1, you must remove:

- the backup files from the local directories on the hosts.
- all the files from `nw-backup` and `restore` directories on the hosts.

Host	Backup Path	Restore Path
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
All Other Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Appendix A. Troubleshooting

There two sections in this appendix.

- Section 1 - General Troubleshooting Information
- Section 2 - Hardware-Related Troubleshooting Information

Section 1 - General Troubleshooting information

This section describes solutions to problems that you may encounter during installations and upgrades. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294) .

This section has troubleshooting documentation for the following services, features, and processes.

- Command Line Interface (CLI)
- Backup Script
- Event Stream Analysis
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

Command Line Interface (CLI)

Error Message	Command Line Interface (CLI) displays: "Orchestration failed." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Entered the wrong `deploy_admin` password in `nwsetup-tui`.
Solution	Retrieve your `deploy_admin` password password. 1. SSH to the NW Server host. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password`

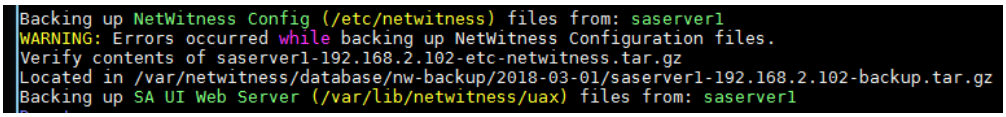
SSH to the host that failed.

2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

Error Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Suite sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service. `systemctl restart rsa-sms`

Backup (`nw-backup` script)

Error Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the *Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Error	Backup errors caused by the `immutable` attribute setting. Here is an example of an error that can be displayed: 
Cause	If you have any files that have the immutable flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.
Solution	On the host that contains the files with the immutable flag set, run the following command to remove the immutable setting from the files: `chattr -i <filename>`

Error	Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: `/etc/sysconfig/network-scripts/ifcfg-em1` Verify contents of `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Cause	There are incorrect or duplicate entries for any one of the following fields: DEVICE, BOOTPROTO, IPADDR, NETMASK or GATEWAY, that were found from reading the primary Ethernet interface configuration file from the host being backed up.

Solution	Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format `<hostname>-<hostip>-network.info.txt`, and should contain the following entries:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1.0.0 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESA Primary host and log in.
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Submit the following command to restart ESA.
	`systemctl restart rsa-nw-esa-server`
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Suite and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Suite and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Suite and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.5.x to 11.1.0.0.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Error Message	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

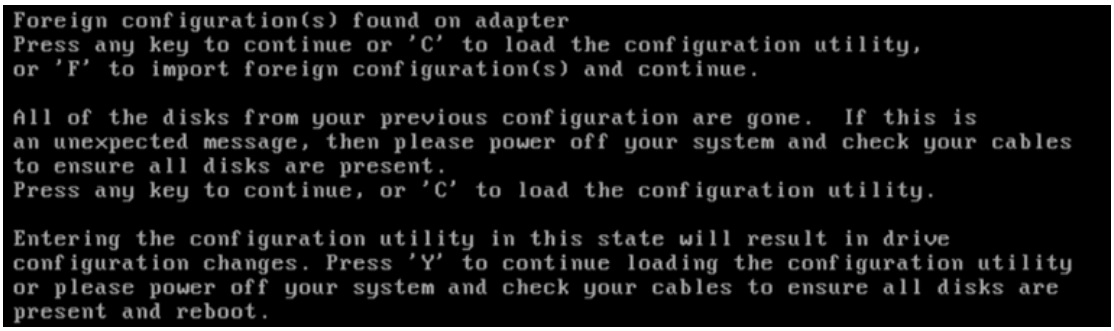
Section 2 - Hardware-Related Troubleshooting Information

Import Foreign Config for Series 4 Appliance with External Storage

If you upgrade a host with an external storage (for example, a DAC) to 11.1 and try to restart the appliance, the system may recognize it as having a foreign configuration. If you receive this error, complete the following steps.

1. Restart the appliance with external storage.

   The following messages are displayed.

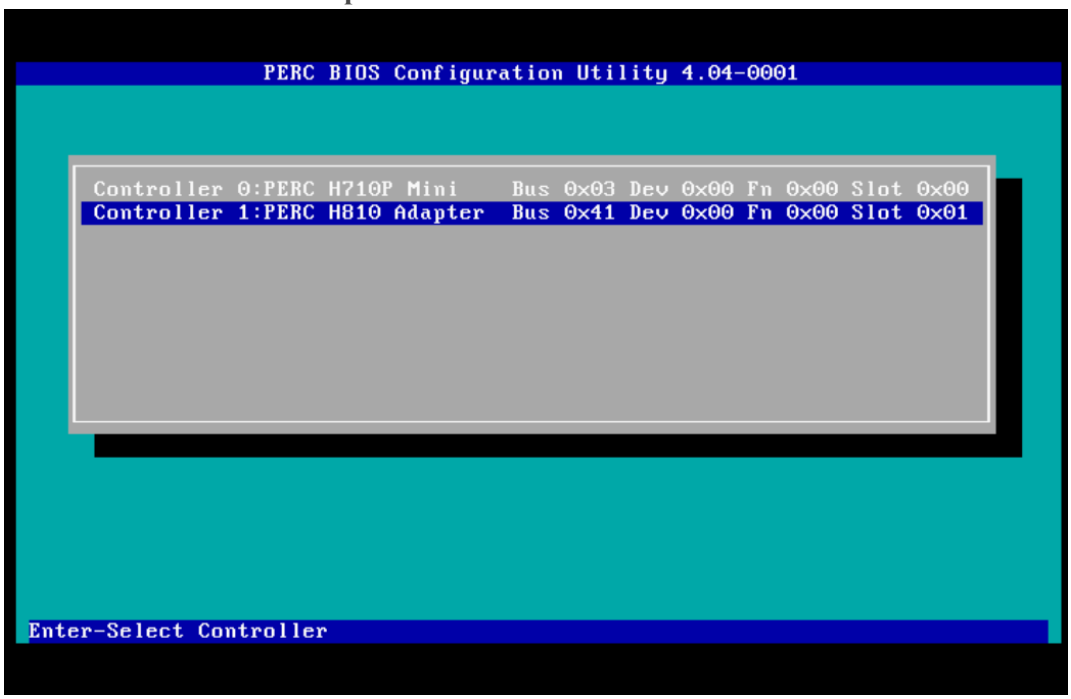


2. Press the **F** key and restart the appliance.

   If this successfully imports the configuration and restarts the appliance, you are finished. If it does not work, go to step 3.

3. Press **C** to start the Configuration utility.

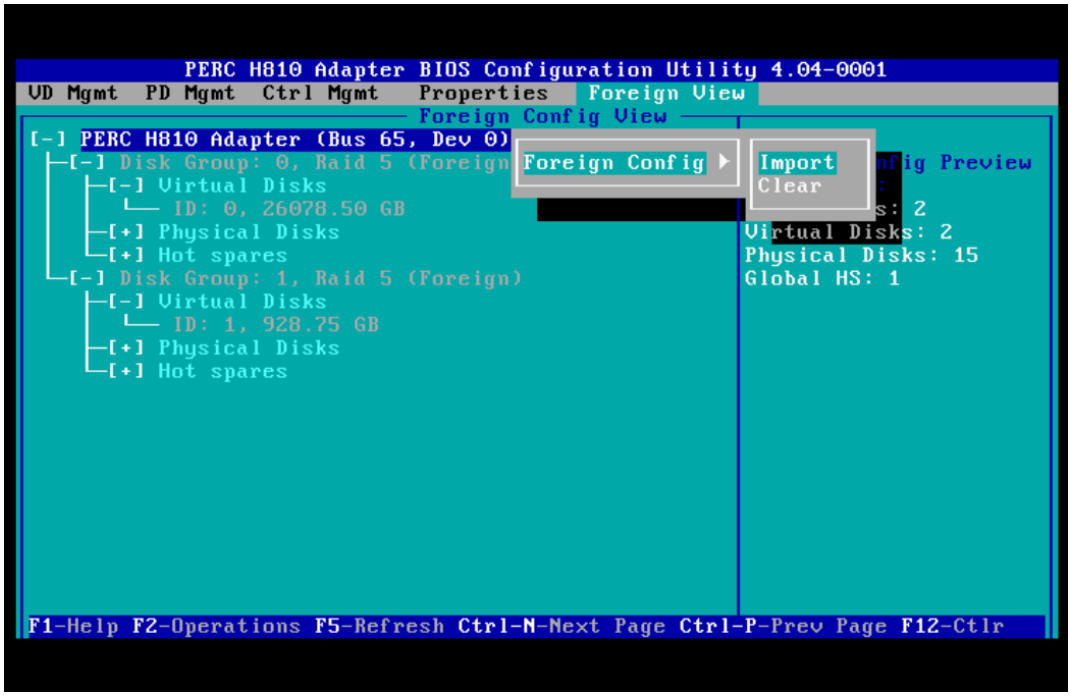
   a. Select the **PERC H8x0 Adapter**.



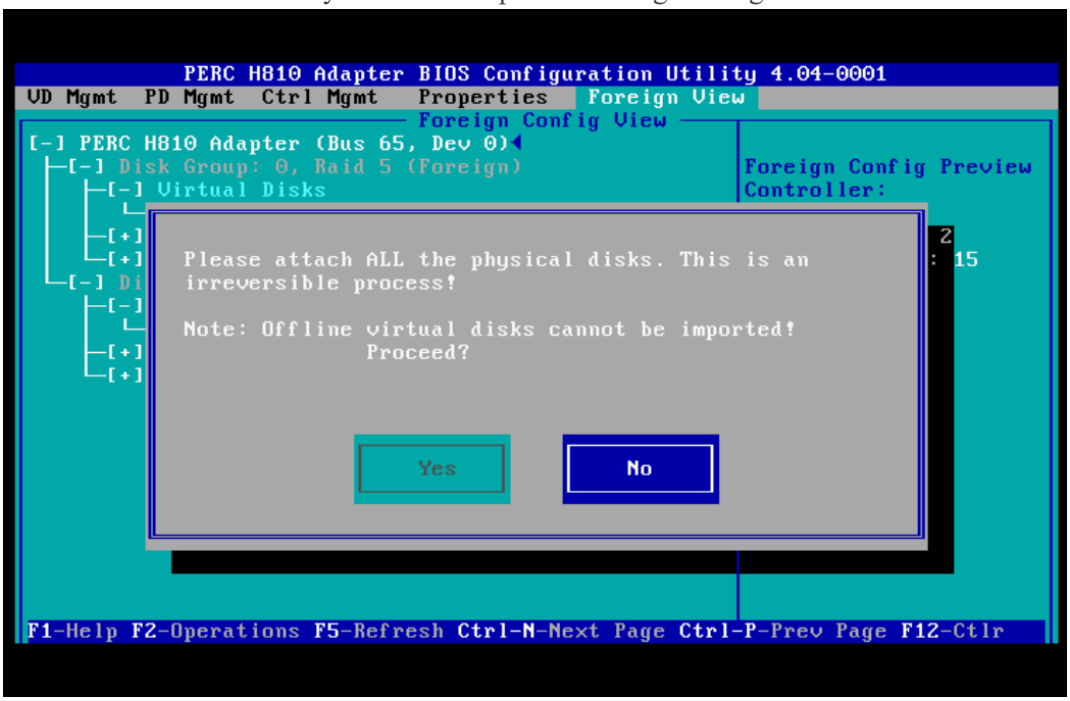
   b. Highlight the top row [for example, **PERC H810 Adapter (Bus 65, Dev 0)**].

   c. Select **Foreign View** from the menu bar.

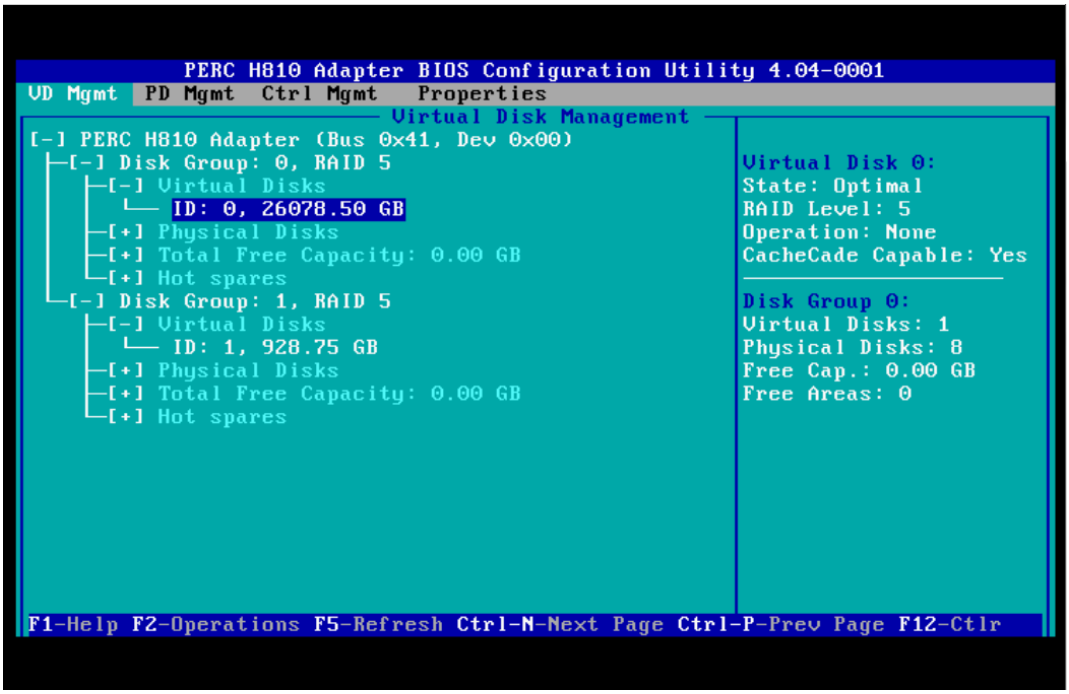
   d. Press **F2** to display the **Foreign Config** drop down menu and select **Import**.



e. Select **Yes** to confirm that you want to import the foreign config.

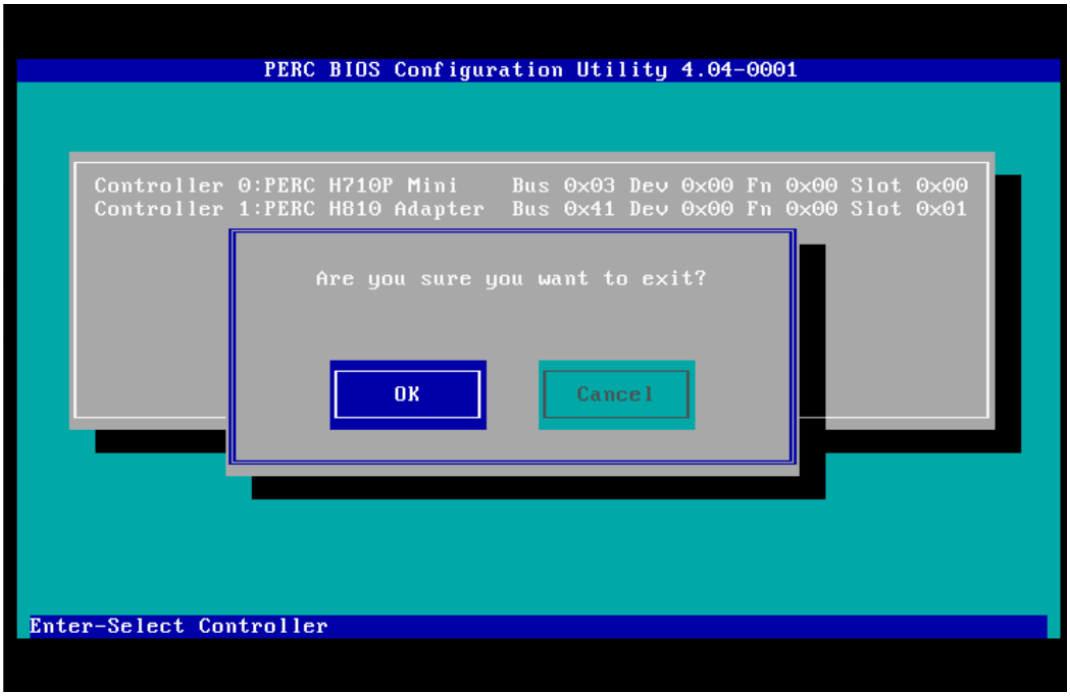


f. Verify that there are no more foreign configs present on the system.



g. Press the **Esc** key to exit.

h. Select **Yes** to confirm that you want to exit.



4. Press **Ctrl-Alt-Delete** to restart (reboot) the appliance.

Caution: If the foreign config fails, Contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Restore Files for 10G Decoder

If you use the 10G Decoder hardware driver and you customized the `/etc/init.d/pf_ring` script to use MTU from the `/etc/pf_ring/mtu.conf` file, you must restore `mtu.conf` and `pf_ring` files from the `./etc/init/pfring_bkup` directory.

1. Restore the `pf_ring` file to /etc/init.d/ directory in 11.1.
   `/etc/init.d/pf_ring`
2. Restore the `mtu.conf` file to `/etc/pf_ring/` directory in 11.1.
   `/etc/pf_ring/mtu.conf`

Appendix B. Stopping and Restarting Data Capture and Aggregation

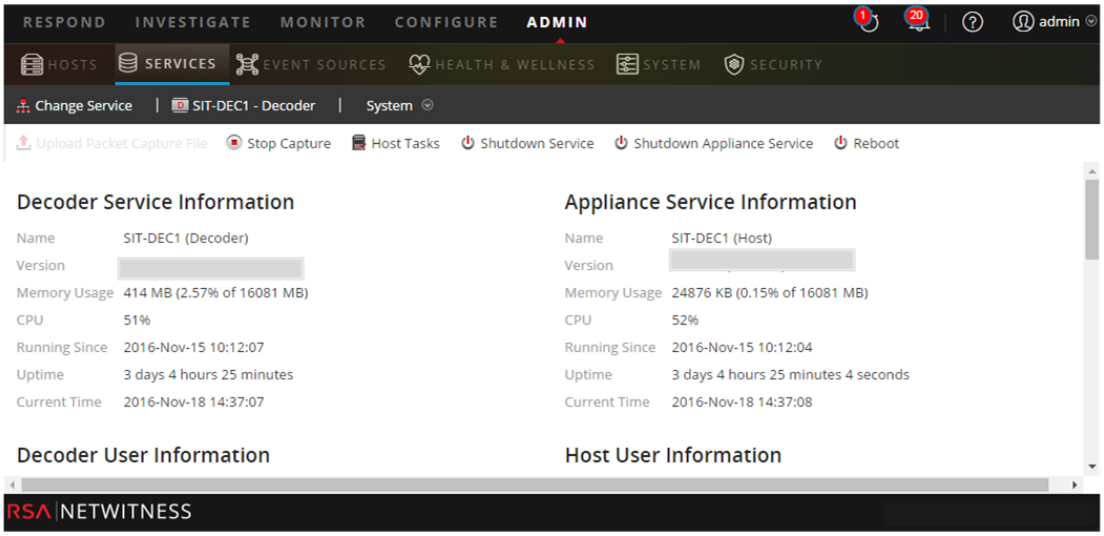
RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.1.0.0. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.



3. Under (actions), select **View** > **System**.
4. In the toolbar, click

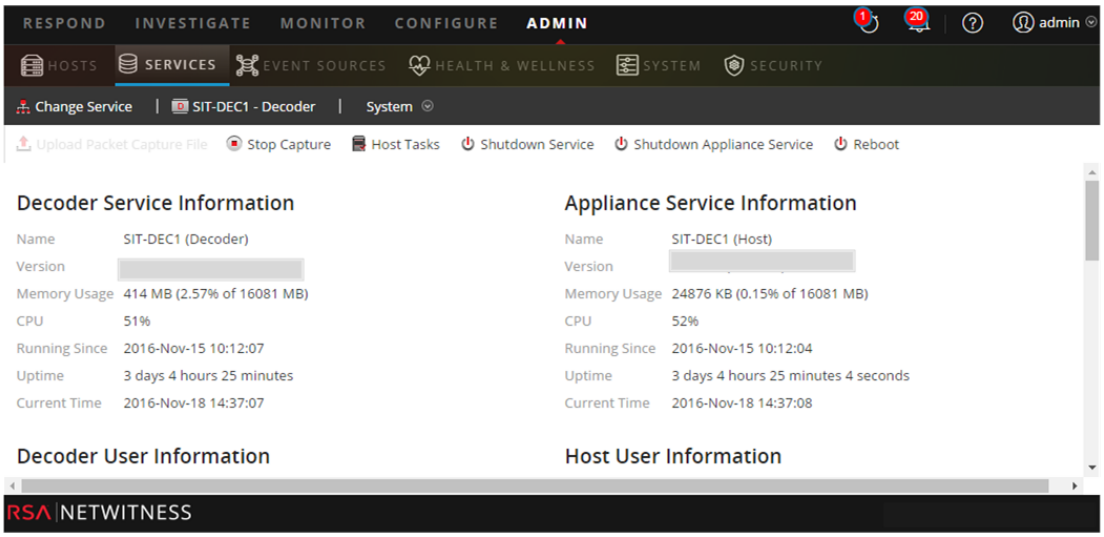
.

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.



3. Under (actions), select **View** > **System**.

4. In the toolbar, click

.

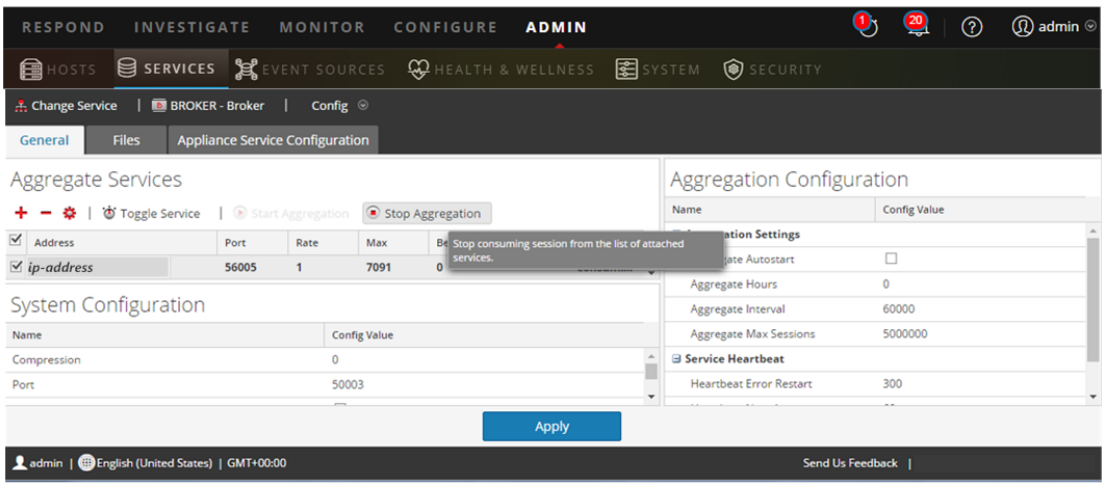
Stop Aggregation

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.

2. Select the **Broker** service.

3. Under (actions), select **View** > **Config**.

4. The **General** tab is displayed.



5. Under **Aggregated Services** click

.

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.0.0.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Log Capture

To start log capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Aggregation

To start aggregation:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. For each Concentrator and Broker service.
   a. Select the service.
   b. Under (actions), select **View** > **Config**.
   c. In the toolbar, click .

Appendix C. Using iDRAC

Many customers have remote sites with limited physical access and limited bandwidth from the administrator's desktop. If this the case, you may want to use iDRAC with the ISO Image shared out from an NFS share that is local to the devices being upgraded or installed. This also gives you the ability to use an existing NetWitness device as the sharing host.

For example, you have:

- a Concentrator and Decoder at a site in a remote geographic location.
- the bandwidth is relatively low to that site from the administrator's site.
- shipping a USB stick and arranging to have person to go plug it into the boxes while you upgrade is not practical.

In this situation, you can:

1. Install the nfs-utils rpm.
2. Configure the NFS share.
3. Configure iDRAC to connect to that share.
   Make sure that you update your iDRAC firmware Supported Windows and Linux Operating Systems. You do this by downloading and running the Dell Update Packages for supported Windows and Linux operating systems from Dell Support website at http://www.support.dell.com. For more information, see the Dell Update Package User's Guide available on the Dell Support website at http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.
4. Boot to the virtual media that contains the ISO file and continue with the upgrade.

Configure NFS Server - NFS Server config File

1. Install NFS and it’s common utilities using yum.
   ```
   yum install nfs-utils
   ```
2. Configure the NFS service to run at boot.
   ```
   chkconfig nfs on
   ```
3. Configure the rpcbind service to run at boot.
   This service is required by NFS and must be running before NFS can be started.
   ```
   chkconfig rpcbind on
   ```

4. Start the rpcbind service.
   `service rpcbind start`
5. Start the NFS service.
   `service nfs start`
6. Create a directory for our first export.
   `mkdir /exports/files`
7. Open the NFS exports file into a text editor.
   `vi /etc/exports`
8. To export the directory to everyone with read-only access, add the following line.
   `/exports/files *(ro)`
9. Save your changes and exit the editor.
   `:wq!`
10. Export the directory defined above.
    `exportfs -a`
11. Disable firewall rules while performing upgrades.
    `service iptables stop`
12. Copy install media that contains the ISO file to `/exports/files` directory.

Boot iDRAC to NFS Configuration

Note: You must verify idrac firmware is at least 1.57.57 for Series 4 (R620).

1. Log into iDRAC interface.
2. Attach media via Remote File Share.
   `<server ip>:/export/files/11.1.0.0.iso`
   For example: `10.10.10.10:/exports/files/rsa-11.1.0.0.1948.el7-usb.iso`
3. Click **Connect**.
4. Launch **Console**.
5. From **next boot** menu select **Virtual DVD/CD**.
6. Reboot device.

Appendix D. Create External Repository

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. Log in to the web server host.
2. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, `/var/netwitness` is the `web-root`, submit the following command string.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.
6. Unzip the:
   a. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

b. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD

10.6.5.x to 11.1 Physical Host Upgrade Checklist

RSA NETWITNESS® SUITE

Task	Description	√
Prepare for Upgrade		
1.	Download **RSANW-11.1-PhysUpgradeGde.pdf** from RSA Link and review it.	
2.	Carefully read the sections on Event Stream Analysis (ESA) Upgrade Considerations and Investigate in Mixed Mode.	
3.	Be aware of the hardware, deployments, services, and features not supported in 11.1.	
4.	Perform the upgrade preparation tasks for the features you use. **Caution:** Make sure that you implement and test the new ports so that upgrade does not fail due to missing ports.	
5.	Create CentOS 6 external host to save backup tar files.	
6.	Download the `nw-backup-v4.0.zip` file from RSA Link (https://community.rsa.com/docs/DOC-81514) to external host.	
7.	Execute `get-all-systems.sh` and `ssh-propagate.sh` script from external host.	
8.	Preserve a copy of the `get-all-systems-master` file for future reference.	
9.	Execute `nw-backup.sh` in `TEST` mode to evaluate the space requirements from external host (for example: `nw-backup -t -l -D`).	
10.	Review the back up options for `nw-backup.sh` by displaying the help menu (`nw-backup.sh -h`) .	

Task	Description	√
Phase 1 - Upgrade SA Server, ESA, Malware Analysis, and Broker/Concentrator Hosts		
11.	Update the contents of the `all-systems` so they consist of SA, ESA's, MA and Broker/Concentrator backup data.	
12.	Reset the Mongo Database admin password to 'netwitness' if it contains special characters .	
13.	Execute `nw-backup.sh` with `-u` flag for all Phase 1 hosts and confirm that it completes with no errors.	
14.	If your environment has multiple ESA appliances, designate a primary ESA (Where the Context Hub service is running) and copy `mongodb.tar.gz.*` files from the secondary ESAs to designated primary ESA default backup path.	
15.	Confirm that backup tar files are saved locally and remotely.	
16.	Attach media (media that contains the ISO file, for example a build stick) to the SA Server host. See **RSANW-11.x-BuildStickInstr.1.pdf** for instructions on how to get ISO and prepare it. **Caution:** You must use the build stick labeled “OEMDRV”.	
17.	Create base image on the host from the attached media.	
18.	Upgrade the host to 11.1 by running the `nwsetup-tui` program on the host.	
19.	Repeat steps 17., 18., and 19 on the: a. ESA Primary host (and other ESA hosts if you have any). b. Malware Analysis host. c. Broker or Concentrator host.	
20.	Install the ESA, Malware Analysis, and Broker or Concentrator services in the NetWitness 11.1User Interface.	

Task	Description	√
Phase 2 - Upgrade All Other Hosts		
21.	Update the contents of the `all-systems` so they consist of Phase 2 host backup data.	
22.	Execute `nw-backup.sh` in `TEST` mode to evaluate the space requirements from external host (for example: `nw-backup -t -l -D`).	
23.	Execute `nw-backup.sh` with `-u` flag for all Phase 2 hosts and confirm that it completes with no errors.	
24.	Confirm that backup tar files are saved locally and remotely.	
25.	For all other hosts: a. Attach media (that is Build Stick or DVD ISO) to the SA Server host. See **RSANW-11.x-BuildStickInstr.pdf** for instructions on how to get ISO and prepare it. b. Create base image on the host from the attached media. c. Upgrade the 10.6.5.x host to 11.1 by running the `nwsetup-tui` program on the host. d. Install the host service in the NetWitness 11.1 User Interface:	
Preform Post Upgrade Adjustments		
26.	Perform the post upgrade tasks for the features you use.	

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations	IDD

RSA NETWITNESS® SUITE

Virtual Host Upgrade Guide

for Version 10.6.5 to 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **7**

CentOS6 to CentOS7 Upgrade 7

RSA NetWitness® Suite 11.1 Upgrade Path 8

Supported Host Upgrade Path 8

Hardware, Deployments, Services, and Features Not Supported in 11.1 8

Event Stream Analysis (ESA) Upgrade Considerations 9

Upgrade Phases 9

Investigate in Mixed Mode 11

Contact Customer Support 15

Upgrade Preparation Tasks **16**

Global 16

Task 1 - Review Core Ports and Open Firewall Ports 16

Task 2 - Record Your 10.6.5.x admin user Password 17

Task 3 - Create a Backup of /etc/fstab File 17

Respond 18

Task 4 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C” 18

Reporting Engine 19

(Conditional) Task 5 - Unlink External Storage 19

Backup Instructions **20**

Task 1 - Set up an External Host for Backing up Files 21

Task 2 - Create a List of Hosts to Back up 23

Troubleshooting Information 25

Task 3 - Set up Authentication Between Backup and Target Hosts 27

Task 4 - Check for Backup Requirements for Specific Types of Hosts 27

For All Host Types 27

For ESA Hosts with Mongo Databases 28

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation 28

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh 28

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords 30

For Bluecoat Event Sources 30
Task 5 - Check for Adequate Space for the Backup 30
Task 6 - Back up Your Host Systems 31
Post Backup Tasks 35
Task 1 - Save a Copy of the all-systems File and the Backup Tar files 35
Task 2 - Ensure Required Backup Files Were Generated 35
Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host 36
Task 4 - Ensure All Required Backup Files are on Each Host 36

Migrate Disk Drives from 10.6.5.x to 11.1 39

Task 1 - Back Up Data in 10.6.5.x VMs 40
Task 2 - Deploy Same 10.6.5.x VM Stack in 11.1 40
Task 3 - Copy VMDK Files and Add Them as Hard Disk to New VMs 41
Task 4 - Retain MAC Address of Upgraded SA Server VM 46
Task 5 - Restore Backup Data in 10.6.5.x to 11.1 VMs 49

Set Up Virtual Hosts in 11.1 54

Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts 54
Task 1 - Set Up 11.1 NetWitness Server 54
Task 2 - Set Up 11.1 ESA 54
Task 3 - Set Up 11.1 Malware Analysis 54
Task 4 - Set Up 11.1 Broker or Concentrator 55
Phase 2 - Set Up The Rest of the Component Hosts 55
Decoder and Concentrator Hosts 55
Log Decoder Host 55
Virtual Log Collector Host 55
Set Up 11.1 NW Server Host 57
Set Up 11.1 Non-NW Server Host 62

Update or Install Legacy Windows Collection 68

Post Upgrade Tasks 69

NW Server 69
Task 1 - Migrate Active Directory (AD) 69
Task 2 - Modify Migrated AD Configuration to Upload Certificate 70
Task 3 - Reconfigure Pluggable Authentication Module (PAM) in 11.1 70

Task 4 - Restore NTP Servers 70
Task 5 - Restore Licenses for Environments without FlexNet Operations-On Demand Access 70
Task 6 - Remap Virtual NW Server License to 10.6.5.x MAC Address 71
(Conditional) Task 7 - If You Disabled Standard Firewall Config - Add Custom IPtables 71
(Conditional) Task 8 - Specify SSL Ports If You Never Set Up Trusted Connections 71
Task 9 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File 72
RSA NetWitness® Endpoint 73
Task 10 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed 73
RSA NetWitness® Endpoint Insights 73
(Optional) Task 11 - Install Endpoint Hybrid or Endpoint Log Hybrid 73
Task 12 - Reconfigure Endpoint Alerts Via Message Bus 73
Event Stream Analysis Tasks (ESA) 74
Task 13 - Reconfigure Automated Threat Detection for ESA 74
Task 14 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL 75
Task 15 - Enable Threat - Malware Indicators Dashboard 75
Investigate 75
Task 16 - Make Sure User Roles Have Customized User Roles Have Investigate-server Permissions for Event Analysis Access 75
Log Collection 76
Task 17 - Reset Stable System Values for Log Collector after Upgrade 76
(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders)Task 18 - Enable FIPS Mode 77
Reporting Engine 77
Task 19 - Restore the CA certificates for External Syslog Servers for Reporting Engine .. 77
(Conditional) Task 20 - Restore External Storage for Reporting Engine 78
Respond 78
(Conditional) Task 21 - Restore Custom Analysts Roles 78
Task 22 - Restore Respond Service Custom Keys 78
Task 23 - Restore Customized Respond Service Normalization Scripts 79
Task 24 - Add Respond Notification Settings for Custom Roles 79
Task 25 - Manually Configure Respond Notification Settings 80
Task 26 - Update Default Incident Rule Group By Values 81

Task 27 - Add Group By Field to Incident Rules 82
Task 28 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task 83
RSA NetWitness® SecOps Manager 84
Task 29 - Reconfigure NW SecOps Manager Integration 85
Backup 85
Task 30 - Remove Backup-Related Files from Host Local Directories 85
Appendix A. Troubleshooting 86
Command Line Interface (CLI) 86
Backup (nw-backup script) 88
Event Stream Analysis 90
Log Collector Service (nwlogcollector) 91
NW Server 93
Reporting Engine Service 93
Appendix B. Stopping and Restarting Data Capture and Aggregation 94
Stop Data Capture and Aggregation 94
Start Data Capture and Aggregation 96
Appendix C. Using iDRAC 97
Configure NFS Server - NFS Server config File 97
Boot iDRAC to NFS Configuration 98
Appendix D. Create External Repository 99
Revision History 102

Introduction

The instructions in this guide apply to the upgrade of virtual hosts to RSA NetWitness Suite11.1 exclusively. See the *RSA NetWitness Suite Physical Host Upgrade Guide* for instructions on how to upgrade your 10.6.5.x physical hosts to 11.1. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

NetWitness Suite 11.1 is a major release that affects all products in the NetWitness Suite. The components of the suite are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, and Security sever), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.

Refer to the *RSA NetWitness Suite Getting Started Guide* to become familiar with the major changes to the 11.x User interface. Refer to the *RSA NetWitness Suite Deployment Guide* to become familiar with the major platform changes in 11.x.

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: The Reporting Engine is installed on the NW Server host, Workbench is installed on the Archiver host, Warehouse Connector can be installed on the Decoder host or Log Decoder host.

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.1 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.1 platform environment has been improved greatly to accommodate current and future physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Suite 11.1 Upgrade Path

The earliest supported Upgrade path for RSA NetWitness® Suite 11.1 is Security Analytics 10.6.5.x. If you are running a version of NetWitness Suite that is prior to 10.6.5.x, you must update to 10.6.5.x before you can upgrade to 11.1. See the *RSA Security Analytics 10.6.5 Update Guide* (https://community.rsa.com/docs/DOC-85119) on RSA Link.

Supported Host Upgrade Path

You must upgrade a host to the same host type:

- Same Series RSA Physical Appliance to Same Series RSA Physical Appliance (that is, Series 4 to Series 4, Series 5 to Series 5).
  RSA does not support third-party physical hosts in 11.1.
- On-Prem Virtual to On-Prem Virtual

Caution: The 11.1 upgrade does not support mixed-platform upgrades (for example, it does not support physical to virtual).

Hardware, Deployments, Services, and Features Not Supported in 11.1

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.1.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- IPDB service
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.1.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.1.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.1, your custom policy is not present. In its place, there is the out-of-the-box Context hub Server Monitoring Policy in the user interface, which is specific for version 11.1.

- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Suite 11.1, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.1, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.5.x has been removed.

Caution: If you do not use Incident Management in 10.6.5.x, carefully consider whether or not to upgrade to version 11.1.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.1.

In your 10.6.5.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.1.
- Multiple ESA hosts configured to use Incident Management – The system will continue to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.5.x, you can upgrade to version 11.1.
- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.1.

Note: If you did not use Incident Management in 10.6.5.x, you cannot view the 10.6.5.x ESA alerts in the 11.1 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.1 that will allow Respond to view them. See the *ESA Alert Migration Instructions* knowledge base article (https://community.rsa.com/docs/DOC-81680) in RSA Link for instructions on how to run this script.

Upgrade Phases

RSA recommends that you stagger host upgrades as described in this section. The update to CentOS7 and the need of a physical or iDRAC access cause the 11.1 upgrade to take more time than most upgrades.

Caution: If you stagger the upgrade, you:
• must upgrade the hosts in Phase 1 first, in the order shown.
• may not have all the features operational until you update your entire deployment.
• will not have service administrative features available until you upgrade all the hosts in your deployment.

Phase 1

You perform Phase 1 first and you must upgrade the hosts in the following order:

1. Security Analytics Server host
2. Event Stream Analysis hosts
3. Malware Analysis hosts
4. Broker hosts (if you do not have a Broker, upgrade your Concentrator hosts)
   The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2

Upgrade the rest of your hosts.

RSA recommends that you follow the order in Phase 2 to reduce:

- functionality loss during investigation.
- downtime that results in the loss of packet and log capture.

Note: Other than Log Collection hosts with downstream event destinations, there is no technical reason to upgrade your hosts in the order shown in Phase 2.

This is the Phase 2 host upgrade order recommended by RSA.

1. Decoder hosts
2. Concentrator hosts
3. Archiver hosts
4. Log Collection hosts - Log Collectors on Log Decoder hosts (LDs), Virtual Log Collectors (VLCs) and Legacy Windows Collectors (LWCs)
   Before you upgrade a log collection host, you must prepare it for the upgrade. Part of this preparation ensures that no event data remains in the queues. This requires you to keep the downstream destinations of event data (Log Collectors, Virtual Log Collectors and Log Decoders) up and functioning properly.

If you have event data destinations downstream from the Log Decoder, you must prepare and upgrade log collectors in the following order.

a. LDs (one LD at a time)

b. VLCs and LWCs

If you do not have event data destinations downstream from the Log Decoder, you can prepare and upgrade multiple LDs, VLCs, and LWCs together.

5. All other hosts

See "Running in Mixed Mode" under "The Basics" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for:

- Functionality gaps encountered while running in this mode.
- Examples of staggered upgrades.

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.1 and some are still on 10.6.5. This happens when you upgrade to 11.1 in phases.

Note: You must follow the host upgrade sequence as shown in Upgrade Phases to ensure complete Investigate functionality. The 11.1 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.1 to access the Event Analysis View. If the Broker is not upgraded, analysts see a warning icon next to the Broker and no data aggregated to that Broker can be displayed.

After you upgrade all services to 11.1, when an analyst conducts an investigation, Role-Based Access Control (RBAC) of downloads works consistently to limit access to restricted data.

In mixed mode (that is, some services are upgraded to 11.1 and some are still at 10.6.5), when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads.

If the `sdk.packets` setting has not been disabled on the 10.6.x services, analysts with SDK meta and roles permissions in place to restrict viewing and reconstructing an event's content can download the PCAP of an event that has content restrictions. Other types of downloads appear to be successful, then generate errors due to insufficient permissions, and the data is still protected.

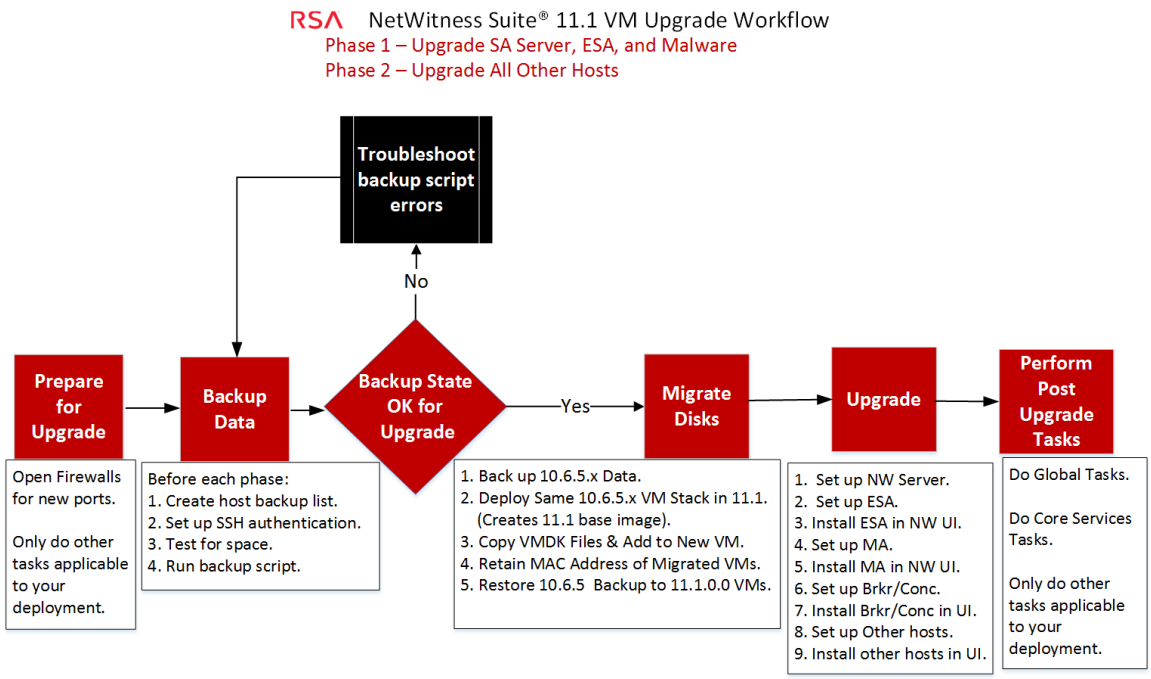
During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.1 and re-enable `sdk.packets`, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NW Server at version 11.1 is connected to services at a lower version.

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 10.6.5.x Concentrator -> 10.6.5.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst	RBAC permitted items	PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.1 Concentrator ->11.1 Decoder/Log Decoder	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items	PCAP	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.0.0.x Concentrator -> 11.0.0.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	None	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Reconstruction View	Analyst	RBAC permitted items	None	File archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Analysis View	Analyst	RBAC permitted items	None	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload PCAPs and logs are downloaded as zero bytes



Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Suite 11.1.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.1. These tasks are organized by the following categories.

- Global
- Respond
- Reporting Engine

Global

You must complete these tasks regardless of how you deploy NetWitness Suite and which components you use.

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.1.

Caution: Make sure that the new ports are implemented and tested before upgrading so that upgrade does not fail due to missing ports.

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 27017	MongoDB

ESA Host

Source Host	Destination Host	Destination Ports	Comments
NW Server, NW Endpoint, ESA Secondary	ESA Primary	TCP 27017	MongoDB

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5672	Message Bus

Source Host	Destination Host	Destination Ports	Comments
Endpoint Server	NW Server	TCP 27017	MongoDB

All NetWitness Suite core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® SuiteDeployment Guide* in case you need to reconfigure NetWitness Suite services and firewalls. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 2 - Record Your 10.6.5.x `admin user` Password

Record your 10.6.5.x `admin user` password. You will need it to complete the upgrade.

Task 3 - Create a Backup of `/etc/fstab` File

Copy the `/etc/fstab` file from all VMs to your local machine (backup host or remote machine).

Note: You need this file to restore a VM with external storage mounts.

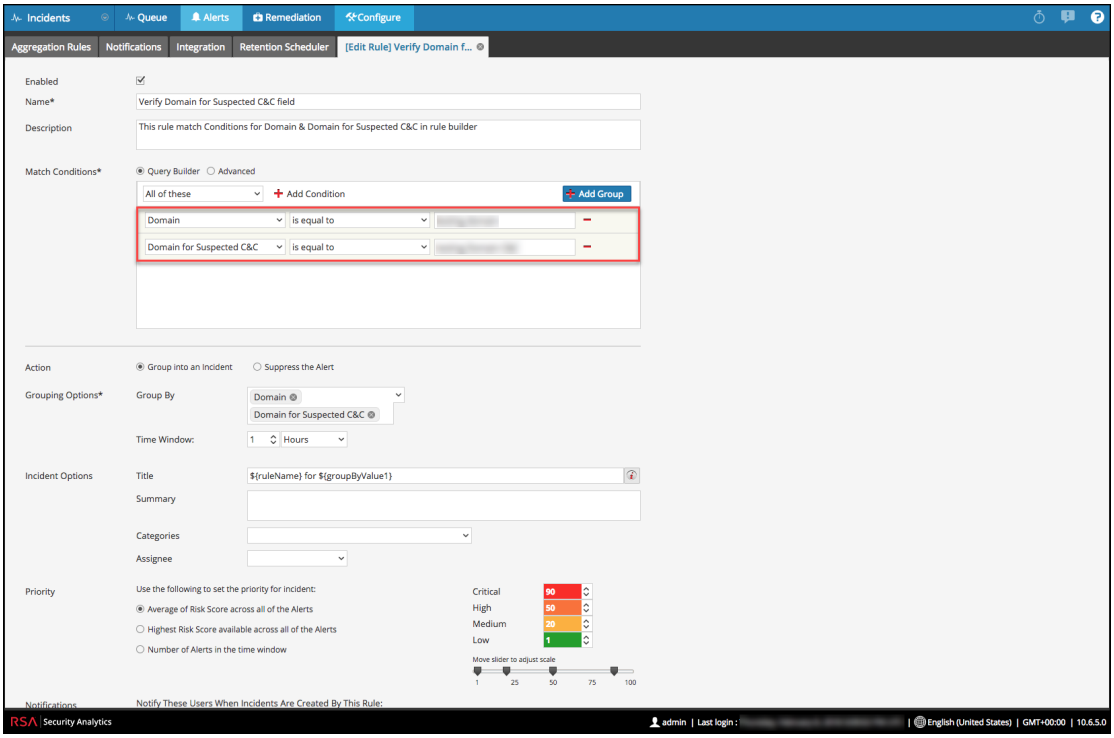
Respond

Task 4 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C”

Make a note of any Incident Management aggregation rules that have match conditions using Domain or Domain for Suspected C&C in the drop-down list in the rule builder. In NetWitness Suite 11.1, you will need to modify these rules to use Domain after you upgrade to 11.1 as described in the Respond Post Update Tasks.

Check the following for each aggregation rule:

1. In the Security Analytics 10.6.5.x menu, select **Incidents** > **Configure** > **Aggregation Rules** tab and edit the rules to view the matching conditions.
2. In the **Match Conditions** section, look for **Domain** or **Domain for Suspected C&C** listed in the drop-down lists for the conditions.



3. Make a note of the rule name and the entire condition that uses **Domain** or **Domain for Suspected C&C**, including operators and values.

Reporting Engine

(Conditional) Task 5 - Unlink External Storage

If the Reporting Engine has external storage [such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports] you must perform the follow steps to unlink the storage.

In these steps:

- `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
- `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.
2. Stop the Reporting Engine service.
   ```
   stop rsasoc_re
   ```
3. Switch to `rsasoc` user.
   ```
   su rsasoc
   ```
4. Change to the Reporting Engine the home directory.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. Unlink the `resultstore` directory mounted to external storage.
   ```
   unlink /externalStorage/resultstore
   ```
6. Unlink the `formattedReports` directory mounted to external storage.
   ```
   unlink /externalStorage/formattedReports
   ```

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from Security Analytics 10.6.5.x releases to NetWitness Suite 11.1.

Note: It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.1, your custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types.

Caution: These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the Security Analytics Server
- Standalone Warehouse Connector
- Warehouse Analytics (Datascience)

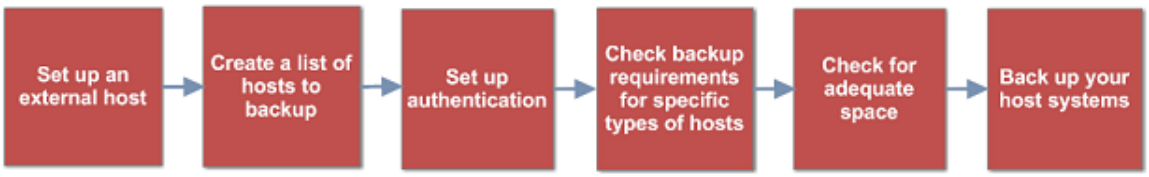
The following types of hosts can be backed up and are automatically restored during the upgrade process:

- **Security Analytics Admin Server** (may include Malware Analysis, Incident Management, Health and Wellness, and Reporting Engine)
- **Malware Analysis** (standalone)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and Incident Management database)
- **Concentrator**
- **Log Decoder** (including Local Log Collector and Warehouse Connector, if installed)
- **Log Hybrid**
- **Packet Decoder** (including Warehouse Connector, if installed)
- **Packet Hybrid**
- **Virtual Log Collector**

The following types of files are automatically backed up but must be restored manually after the upgrade process:

- PAM configuration files: For information about restoring the PAM configuration files, refer to "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.1.", in the "Global" section of the **Post Upgrade Tasks**.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of **Post Upgrade Tasks**.

The following diagram shows the high-level task flow of the steps you perform to back up your hosts.



The following sections describe each of these tasks:

- Task 1 - Set up an External Host for Backing up Files
- Task 2 - Create a List of Hosts to Back up
- Task 3 - Set up Authentication Between Backup and Target Hosts
- Task 4 - Check for Backup Requirements for Specific Types of Hosts
- Task 5 - Check for Adequate Space for the Backup
- Task 6 - Back up Your Host Systems
- Post Backup Tasks

Task 1 - Set up an External Host for Backing up Files

You must set up an external host to use for backing up files. The host must be running CentOS 6 with connectivity through SSH to the Security Analytics stack of hosts.

Note: If you are not able to use an external host for backing up files, contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

Ensure that the host names for the systems to be backed up are resolvable on the backup host machine, either by DNS or listed in the `/etc/hosts` file.

Note: These scripts are designed to run on CentOS 6 only. You must execute these scripts on CentOS 6 machines.

There are several scripts that you run during the backup process. You must download the zip file that contains the scripts (`nw-backup-v4.0.sh`) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your Security Analytics Servers and host systems to be backed up.
- `ssh-propagate.sh`: Automates sharing keys between the systems you are backing up and the backup host system so that you are not prompted for passwords multiple times.
- `nw-backup.sh`: Performs the backup of your hosts.
- `azure-mac-retention.ps1`: Applies only if you are using AZURE. See the *AZURE Deployment Guide* on for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

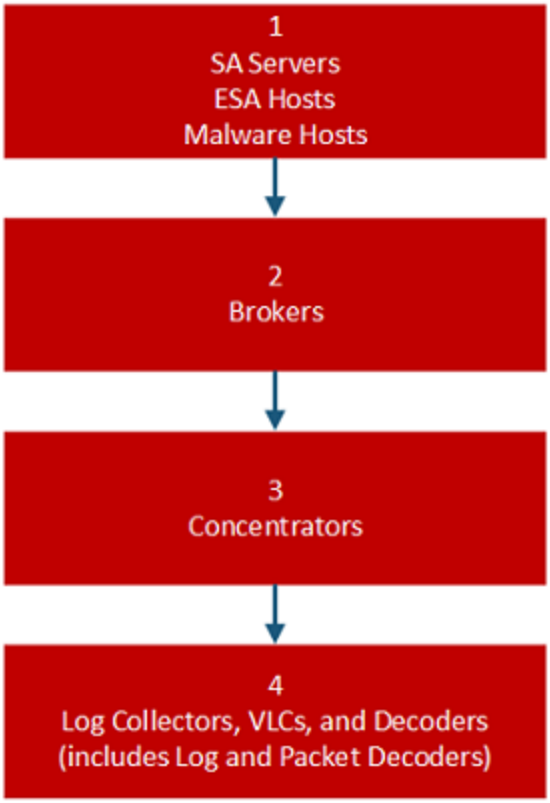
Note: If you have used the 10.6.x versions of the backup and restore scripts on your 10.6.5 hosts, you must still run all the scripts listed here.

Note: Do NOT use the scripts in the `nw-backup-v4.0.zip` file for regular backups. These scripts are specifically designed for upgrading from 10.6.5.x to 11.1.

Note: The backup scripts do not support backing up data for STIG-hardened hosts.

Task 2 - Create a List of Hosts to Back up

The script that you use to back up your files depends on the `all-systems` and `all-systems-master-copy` files, which contain a list of the hosts that you want to back up. The `all-systems-master-copy` file contains a list of all your hosts. The `all-systems` file is used for each backup session, and contains only those hosts which are being backed up for a particular session. You run the `get-all-systems.sh` script to generate these files. RSA recommends that you back up your hosts in groups, and not all at once. The recommended order and grouping of hosts for backup sessions is shown in the following diagram:



Limit each backup session to five hosts to ensure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference and then manually editing the `all-systems` file to contain specific hosts.

To generate the `all-systems` and the `all-systems-master-copy` files:

1. From the host on which you are running the backup process, make the `get-all-systems.sh` script executable by running the following command:
   ```
   chmod u+x get-all-systems.sh
   ```
2. At the root level, run the `get-all-systems.sh` script:
   ```
   ./get-all-systems.sh <IP-Address-of-SA-Admin-Server>
   ```
   You will be prompted for the password for each host system once per host.

This script saves the `all-systems` file and the `all-systems-master-copy` file to `/var/netwitness/database/nw-backup/`.

3. Validate that the `all-systems` and `all-systems-master-copy` files were generated and that they contain the right hosts.
4. Edit the `all-systems` file to contain only the systems you are backing up. You can do this by using the `all-systems-master-copy` file as a reference, and then opening the `all-systems` file in an editor (such as vi) and modifying it to include only the systems you want to back up. RSA recommends that you comment out the hosts that you do not want to back up (add the number sign (#) to the beginning of the line that contains the host that will not be backed up).
   The following examples shows how to comment out the 10.6.5 Security Analytics Server:
   `loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.5.0`
   `#nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.5.0`

   Note: If you use vi, be sure to include the path to the location of the `all-systems` file.

Here is an example of an `all-systems-master-copy` file:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.5.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.5.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.5.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.5.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.5.0
```

And here is an example of an `all-systems` file that could be used in the first backup session, where only the Security Analytics Server, ESA host, and Malware Analysis host are backed up:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

Troubleshooting Information

- Be sure to save copies of the `all-systems` and `all-systems-master-copy` files in a safe location. Follow these recommendations:
  - Do not edit the `all-systems-master-copy` file.
  - If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure that each version of the file lists only those hosts that are currently being backed up, and the other hosts are commented out.
    For more information, see Post Backup Tasks.
- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.
- The `get-all-systems.sh` script generates a list of hosts that were defined in the Security Analytics user interface. Ensure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to Security Analytics, you use the Security Analytics user interface to ensure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.

- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the Security Analytics Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the Security Analytics Server. (Any Windows Legacy Collectors or AWS Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)
- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

RSA recommends that you run the `ssh-propagate.sh` script to automate sharing keys between the backup host and the host systems.

Note: If you have SSH keys that are protected with pass phrases, you can use `ssh-agent` to save time. For more information, refer to the man page for `ssh-agent`.

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:
   `chmod u+x ssh-propagate.sh`
2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. You are prompted for the password once per host, but you will not need to enter it repeatedly later during the backup process.

Task 4 - Check for Backup Requirements for Specific Types of Hosts

After you create the `all-systems` file to use for backup, you must check to see if any of the hosts listed in the file have requirements that must be met before you run the backup process.

For All Host Types

Perform the following steps for all host types:

1. On the Security Analytics Server, place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directories will be automatically restored during the upgrade process. After upgrading to 11.1., your custom certificate files will be located in `/etc/pki/nw/trust/import`.
   You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the Security Analytics Server and run the following command strings to perform the conversions listed.
   Convert a DER file (.crt .cer .der) to PEM
   `openssl x509 -inform der -in certificate.cer -out certificate.pem`
   Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Note:** Add the following qualifier to the command string to:
> `-nocerts` convert private keys exclusively.
> `-nokeys` convert certificates exclusively.

2. Manually record any custom configurations made to CentOS 6 (for example, driver customizations) for restoration after you update to CentOS 7. Custom configurations to CentOS 6 are not automatically backed up and restored.

For ESA Hosts with Mongo Databases

The default 10.6.x Mongo database password is `netwitness`. If you have customized this password, you could encounter an error while running the backup script. You can either use your custom Mongo database password during the backup, or you could change that password back to `netwitness` before running the `nw-backup.sh` script.

1. Find out if the Mongo database password is `netwitness` or if it has been modified.
2. If it has been modified, either change it back to `netwitness`, or be sure you know what the customized password is so that you can enter it during the backup.

See "ESA Config: Change MongoDB Password for admin Account" in the *NetWitness Suite Event Stream Analysis Configuration Guide* for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for Decoder, Concentrator, or Broker hosts, stop data capture and aggregation on all the systems that you are backing up. For instructions, refer to Appendix B. Stopping and Restarting Data Capture and Aggregation

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run `prepare-for-migrate.sh`

> **Caution:** This task stops log collection so you must perform this step immediately before you upgrade to minimize the loss of event collection. Complete this task in accordance with the backup and upgrade tasks in this guide.

Prerequisites

You need the following information before you prepare LCs and VLCs for upgrade.

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.
- If you set the password for `logcollector` user for RabbitMQ, you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.
2. Submit the following command string.

   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```

   This command:

   - Stops the Puppet Agent service.
   - Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.1.
   - Stops all the collection protocols in the Log Collector service.
   - Saves the list of Plugin accounts and RabbitMQ accounts.
   - Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.
   - Waits until the Log Collector queues are empty.
   - Stops the Log Collector service.
   - Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

The `prepare-for-migrate.sh` script:

- Sends informational, warning, and error messages to the console.
- Saves a session log in the `/var/log/backup/` directory.

You must fix any of the following errors and resume the preparation. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

- Log Collector queues with events but without consumers are found.
- Unable to stop the Puppet Agent service.
- Unable to stop a collection protocol in the Log Collector service.
- Unable to block event publishers to the RabbitMQ server.
- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.
- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting.

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the Security Analytics Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.1. upgrade, you can restore RabbitMQ user accounts.

To get a list of RabbitMQ usernames and passwords, run the following command:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

To restore RabbitMQ user accounts, refer to *Task 2 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL* in **Post Upgrade Tasks**.

For Bluecoat Event Sources

Bluecoat ProxySG event sources use FTPS protocol to upload log files to the Log Collector (LC) and Virtual Log Collector (VLC). The event source documentation contains the steps to configure VSFTPD service on the LC and VLC.

- If key material exists in `/root/vsftpd/` directory in 10.6.5.x, this material area will be backed up and restored. **If the material was in another location, you must back it up and restore it manually.**
- If the `/etc/vsftpd/vsftpd.conf` file exits in 10.6.5.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

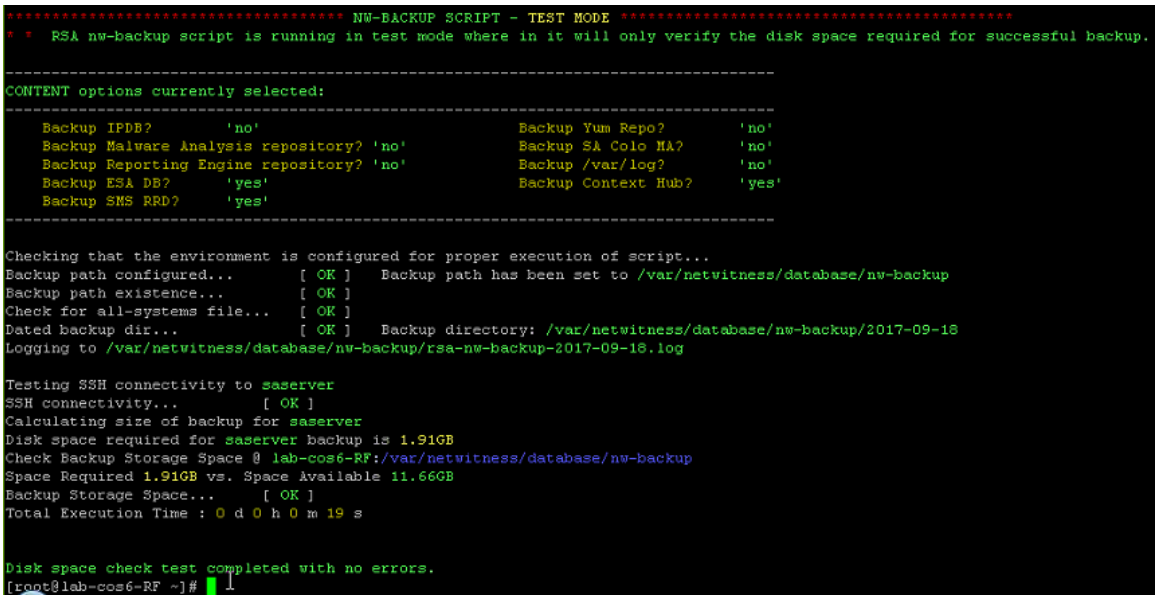
You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to ensure that you provide adequate space for the backup so that the backup captures all your data.

To check for adequate disk space:

1. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
2. Run the following command at the root directory level:
   `./nw-backup.sh -t`
   The output displays the amount of disk space that is required for the backup.

> **Note:** The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-d` option by using `-D`. Using the `-D` option will show how much space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

The following figure shows an example of the output from using the `-t` option.



Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.1.

> **Note:** The script will stop services as it runs. However, you can stop services manually before you run the script if needed.

When you run the backup script, you can choose from several options that are described in the following sections.

Usage:
`./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>`

General Options

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) - COPY`

`-b <path to write backups> : path to the location for storing backup files on a backup server.` **`For upgrading to 11.1, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

Note: Do **not** change the backup path in upgrade (-u) mode.

Note: When you run a backup with the `-u` option, all services are stopped. If you need to continue to use the 10.6.x machine after running the backup, reboot the 10.6.x system so that services are restarted.

Advanced Content Selection Options

`-c : back up Colocated Malware Analysis on SA servers. Default: (no)`

`-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)`

`-m : back up Malware Analysis File Repository. Default: (no)`

`-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)`

`-v : back up system logs (/var/log). Default: (no)`

`-y : back up YUM Web Server & RPM Repository. Default: (no)`

`-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)`

-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)

-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)

Test Options

-t : performs script test run for disk space check only. Services are not stopped and excludes execution of backup. Can be combined with (-d) or (-D) and other flags. Default: (-t)

For example, the command:
`./nw-backup.sh`
would run the backup with options as set in the Header of the script itself.
OR, the command:
`./nw-backup.sh -ue /mnt/external_backup`
would run a normal backup using the backup path defined in the script, with the following options:

-u : enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on /mnt/external_backup

For Help: ./nw-backup.sh -h

When you run the script, the following text is displayed at the top of the script:

Caution: RSA nw-backup script backs up configuration files, data, and logs on the options provided in the script. It tars the content, with options to store the backup files on the backup server, move or copy them to external storage on a mount point (USB/NFS/SMB), or SCP them back to the target host.
This backup script has been qualified on the following versions of Security Analytics:
10.6.5.x
Use of this script on any other versions of the product may not give expected results and may not be supported by RSA Customer Service.Note: All non-RSA custom files, scripts, Cronjobs and other important files should be placed in /root, /home/'user', OR /etc to be included in the backup.

To run the backup script to back up your hosts:

1. Ensure that the `all-systems` file contains only the hosts to back up. For information, see Task 2 - Create a List of Hosts to Back up.
2. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
3. Begin the backup process by running the following command at the root directory level:

```
./nw-backup.sh -u
```

Note: You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.1. Do NOT make any changes to the header of the backup script for the backup path because the path is specific to the upgrade, and that data needs to be in a specific place.

When the text "`Backup completed with no errors`" is displayed, the backup has completed successfully.

A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:
`rsa-nw-backup-2017-03-15.log`

4. When the backup has completed, to ensure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   The following archive files are created:

   For all hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

   For Security Analytics Servers:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

   For ESA Hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `<hostname-IPaddress>-controldata-mongodb.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

The archived files are located in the `/var/netwitness/database/nw-backup` directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

Post Backup Tasks

Task 1 - Save a Copy of the `all-systems` File and the Backup Tar files

Make copies of the `all-systems` file, the `all-systems-master-copy` file, and the backup tar files and put the copies in a secure location. You cannot regenerate these files after you upgrade the Security Analytics Server (specifically the Admin service) to 11.1.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.1. upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

The following files are generated on all hosts by the backup scripts:

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

In addition to the files listed above, the following files will be generated on the Security Analytics Server and ESA hosts:

- `<hostname>-<host IP address>-mongodb.tar.gz`
- `<hostname>-<host IP address>-mongodb.tar.gz.sha256`

The backup script will also generate the following `controldata-mongodb.tar.gz` files.

Note: The backup script copies the following files from all ESA hosts to the Security Analytics Server's backup path .

- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz`
- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256`

Task 3 - (Conditional) For Multiple ESA Hosts, Copy `mongodb tar` files to Primary ESA Host

If you have multiple ESA host systems in your enterprise, copy the following two files from each ESA host to the `/opt/rsa/database/nw-backup/` directory on the Primary ESA host system (the host that has the ContextHub service running on it) :

- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Task 4 - Ensure All Required Backup Files are on Each Host

Before you upgrade to 11.1., ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

Note: The default paths for backup files are:
- Security Analytics Servers:`/var/netwitness/database/nw-backup`
- ESA hosts:`/opt/rsa/database/nw-backup`
- Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256`

Required Files for ESA Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Required Files for All Other Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

Note: The following files are located in the <hostname>-<host-IP-address>-backup.tar.gz tar on all hosts:
appliance_info
service_info

Note: The paths to the location of the backup and restore files for iptables, NAT configurations, user accounts, and crontab entries are shown in the following list:
Backup paths:
`BUPATH=/opt/rsa/database/nw-backup` for the ESA Correlation Engine
`BUPATH=/var/lib/rsamalware/nw-backup` for the Malware Service
`BUPATH=/var/netwitness/database/nw-backup` for all other services
Restore locations:
`BUPATH/restore/etc/sysconfig` for Iptable rules
`BUPATH/restore/etc/sysconfig` for NAT configurations
`BUPATH/restore/etc` for Crontab entries
`BUPATH/restore/etc` for User Accounts (users are located in the `passwd` file, and groups are located in the `group` file. These are not restored during the upgrade process but can be restored manually.
`BUPATH/restore/etc/ntp.conf` for NTP configurations (must be restored using the NetWitness Suite UI)

Migrate Disk Drives from 10.6.5.x to 11.1

These instructions tell you how to upgrade virtual hosts from 10.6.5.x to 11.1.

Caution: 1) You cannot perform the migration if you have a snapshot for your VM.
2). Run the backup immediately before you upgrade hosts for each phase so that the data is not out-dated.
3.) This guide applies to virtual host upgrades exclusively. If have both physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite 11.1 Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: The machines must be in VMware ESX.

There are five tasks you must complete to migrate your Virtual Machine (VM) deployment disk drives from 10.6.5.x to 11.1:

Task 1 - Back up data in your 10.6.5.x VMs.

Task 2 - Deploy the same VM Stack in 11.1 as you have in 10.6.5.x.

Task 3 - Copy the VMDK Files and add them as a hard disk to the new VMs.

Task 4 - Retain MAC address of upgraded SA Server VM.

Task 5 - Restore backup data in 10.6.5.x to 11.1 VMs.

Task 1 - Back Up Data in 10.6.5.x VMs

1. Prepare Log Collector for the migration:
   a. Log in to the Log Collector using root credentials.
   b. Go to the `/opt/rsa/nwlogcollector/nwtools/` directory and run the following command.
      `sh prepare-for-migrate.sh --prepare`
      See Virtual Log Collector Host (VLC) for detailed instructions on how to upgrade the VLC.
2. Download the `.zip` file that contains the 10.6.5.x backup scripts from RSA Link https://community.rsa.com/docs/DOC-81514)) to the external backup host.

   Note: You must set up an external host to use for backing up files. The host must be running CentOS 6 with connectivity through SSH to the NetWitness Suite stack of hosts.
3. Run the following commands from the `nw-backup/scripts` directory (see Backup Instructions for a detailed descriptions of the backup scripts).
   `./get-all-systems.sh <SA-IP>`
   `./ssh-propagate.sh <path-to-backup-directory/all-systems>`
   `./nw-backup.sh -u`
   (if you have a Malware VM, substitute `-m -u` for `-u` in this command string (for example, `./nw-backup.sh -m -u`).

Task 2 - Deploy Same 10.6.5.x VM Stack in 11.1

You must set up the same virtual host stack in 11.1 that you had in 10.6.5.x. See the *RSA NetWitness® Suite 11.1 Virtual Host Installation Guide* for instructions.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

The following steps are the high-level steps on how to deploy an OVA host in the ESXi environment.

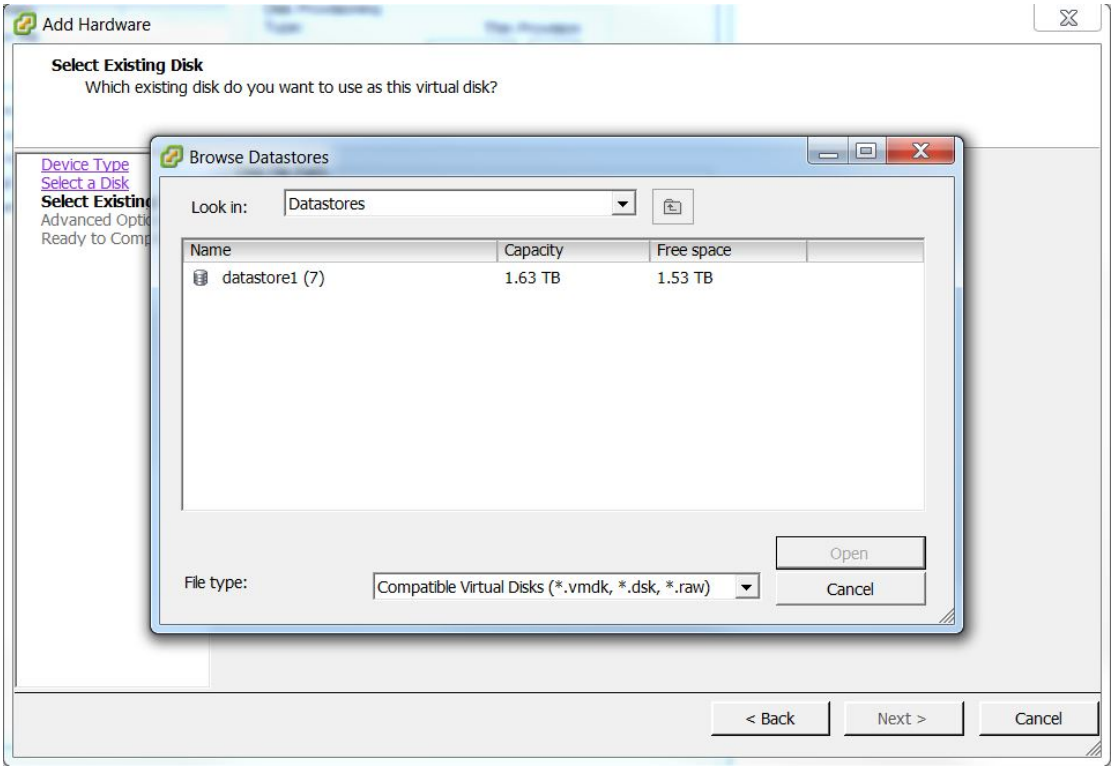
Download the 11.1 OVA, from RSA Link Download Central to a local directory.

1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.
   The Deploy OVA Template dialog is displayed.
3. Browse your local directory for the 11.1 OVAs you downloaded.
4. Select the to deploy in the virtual environment , and click **Next**.

5. Select the appropriate Configuration for the VM and click **Next**.
6. Power on the VM, go to Console, and log in to the machine.
   The VM now has the 11.1 base image required to run the Setup Program (that is, `nwsetup-tui`).

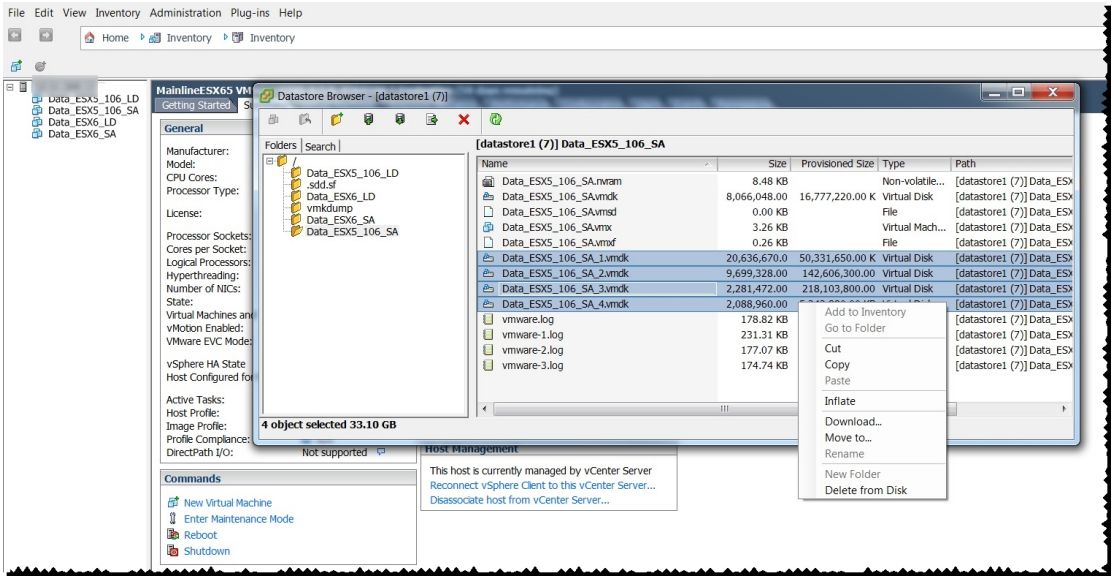
Task 3 - Copy VMDK Files and Add Them as Hard Disk to New VMs

1. Power off both the 10.6.5.x and 11.1 VMs.
2. Go to the desired ESX server, click the **Configuration** tab > **Storage**.
3. Right-click the required datastore and click **Browse Datastore**.



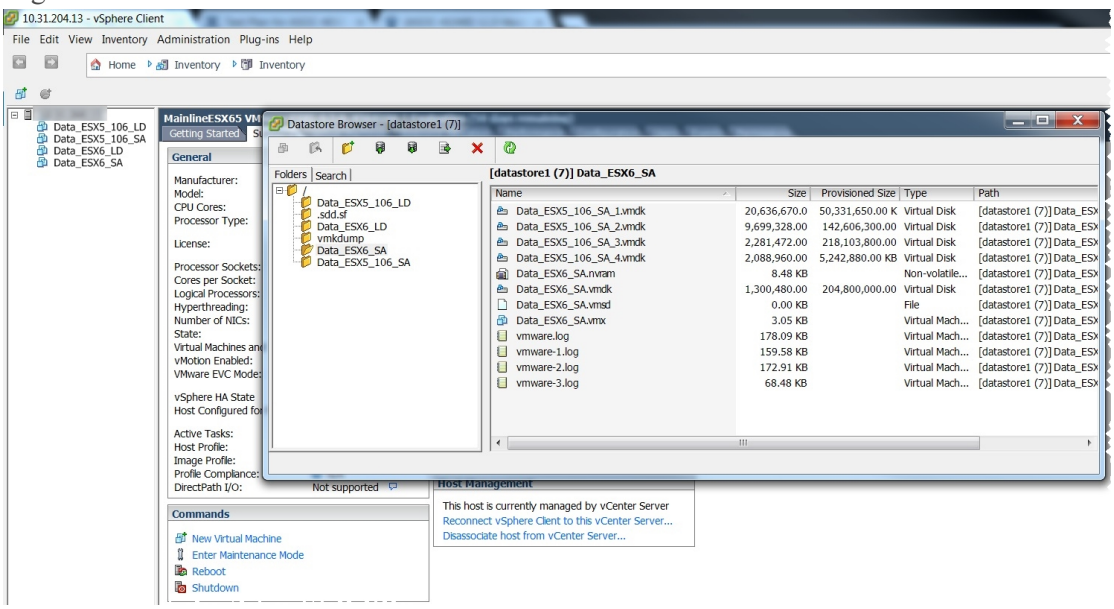
4. Navigate to the existing 10.6.5.x VM in the datastore.
5. Select all the VMDK files in the datastore, right-click, and click **Copy**.

> **Caution:** Do not copy the base VMDK file (for example, `Data_106_SA`) because it contains CentOS6.
>
> You must copy all the numbered VMDK files. For example, if the 10.6.5.x VM name is `Data_106_SA`, you would copy all the `Data_106_SA_1`, `Data_106_SA_2`, `Data_106_SA_3`, etc files.



6. Navigate to the new 11.1 VM in the datastore.

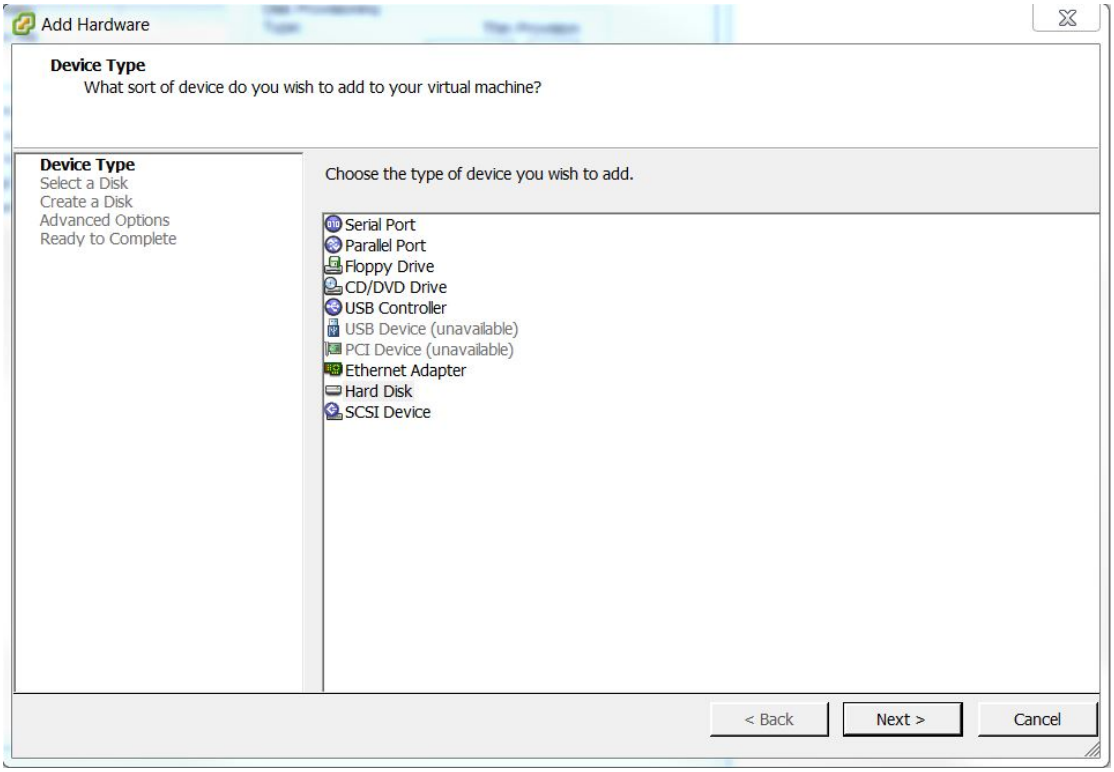
7. Right-click and click **Paste**.



> **Note:** You must wait until all the VMDK files from the previous VM are completely copied into the datastore of the new VM.

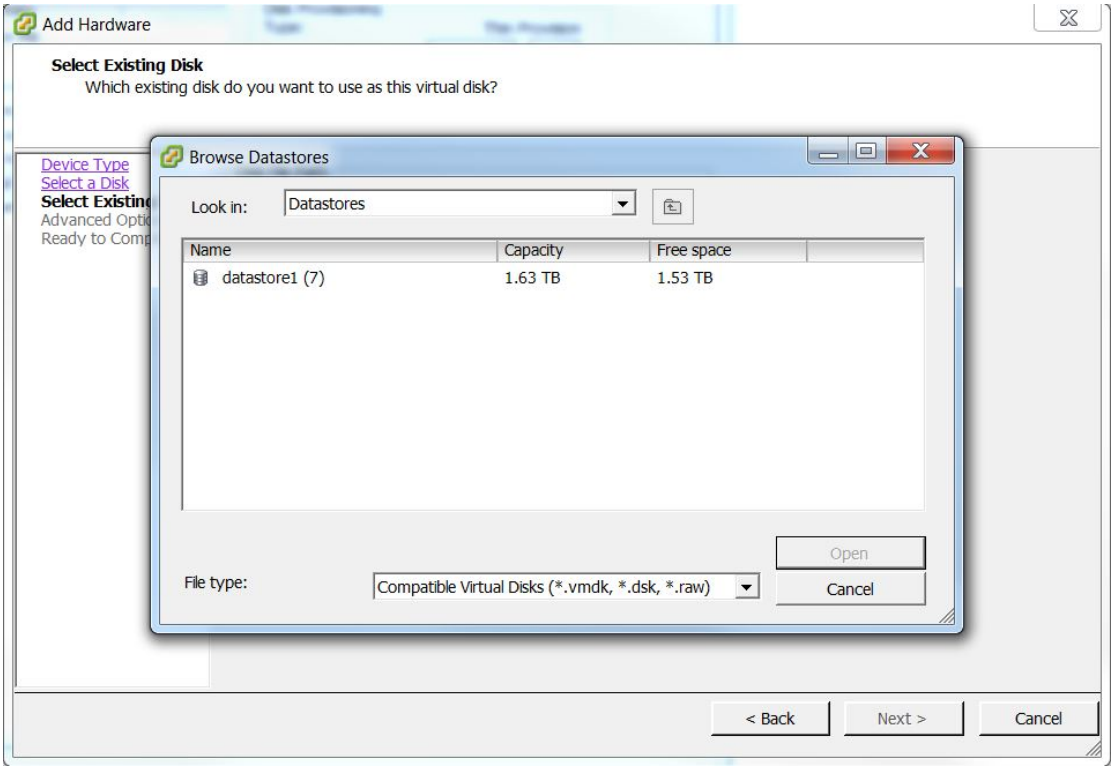
8. Select the 11.1 VM, click **Edit Settings** > **Add**.

9. In the dialog box, click **HardDisk** > **Next**.

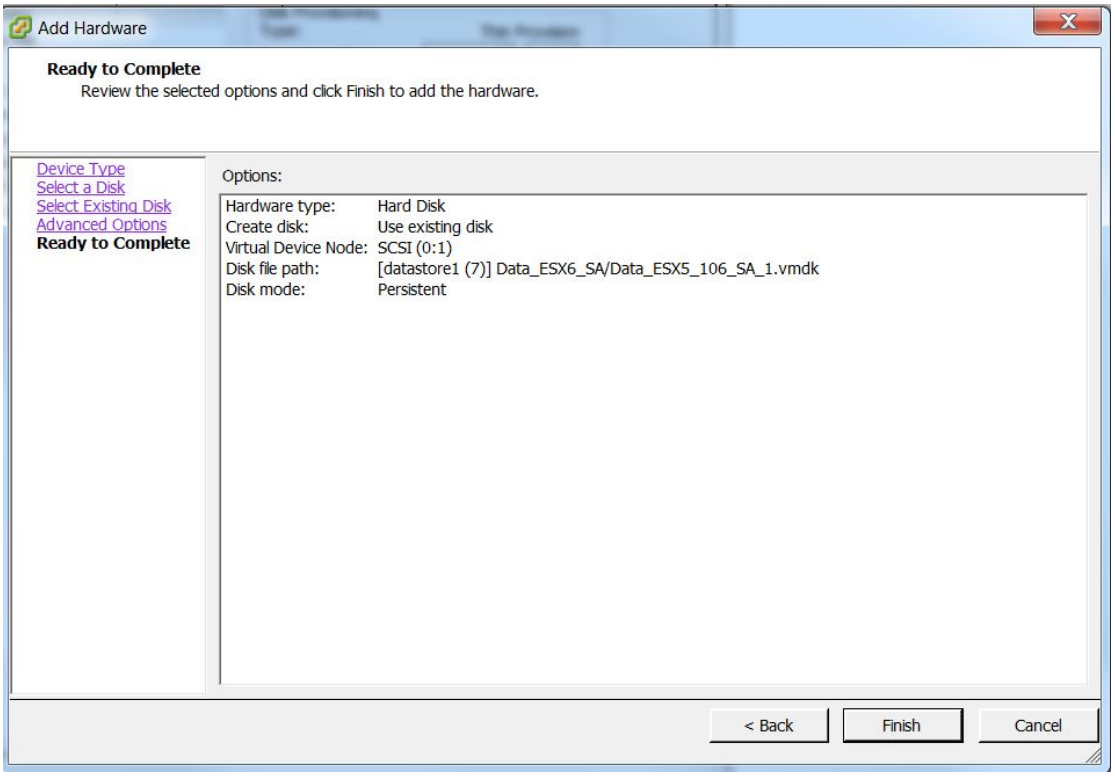


10. Click **Already existing hard disk** > **Next**.

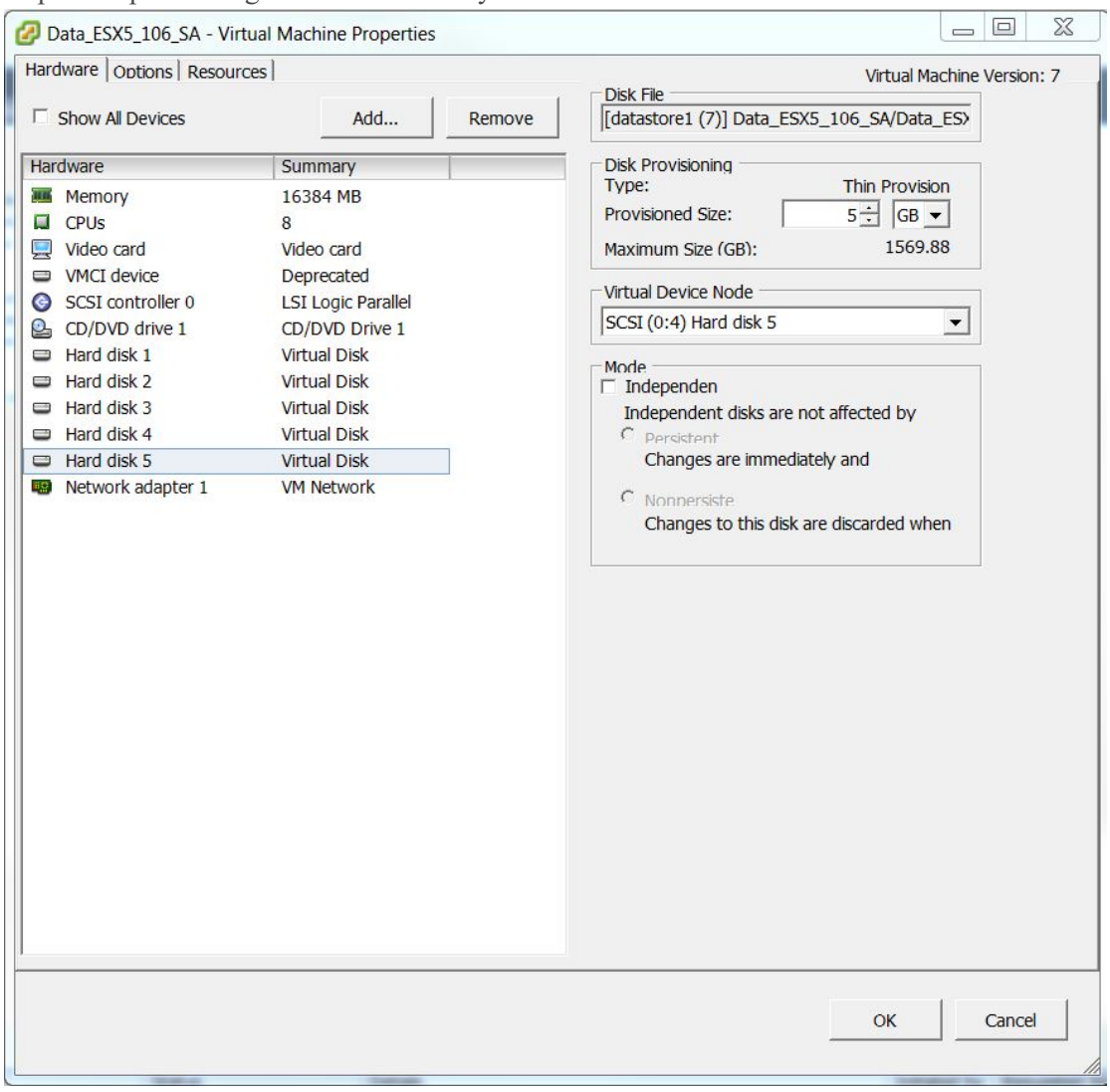
11. Click **Browse** and browse to the datastore location to which you copied the vmdk files.



12. Select the VMDK file from the 11.1 VM that you want to add as a disk.



13. Repeat steps 8 through 12 for each disk you want to add.



14. Click **OK**.

Task 4 - Retain MAC Address of Upgraded SA Server VM

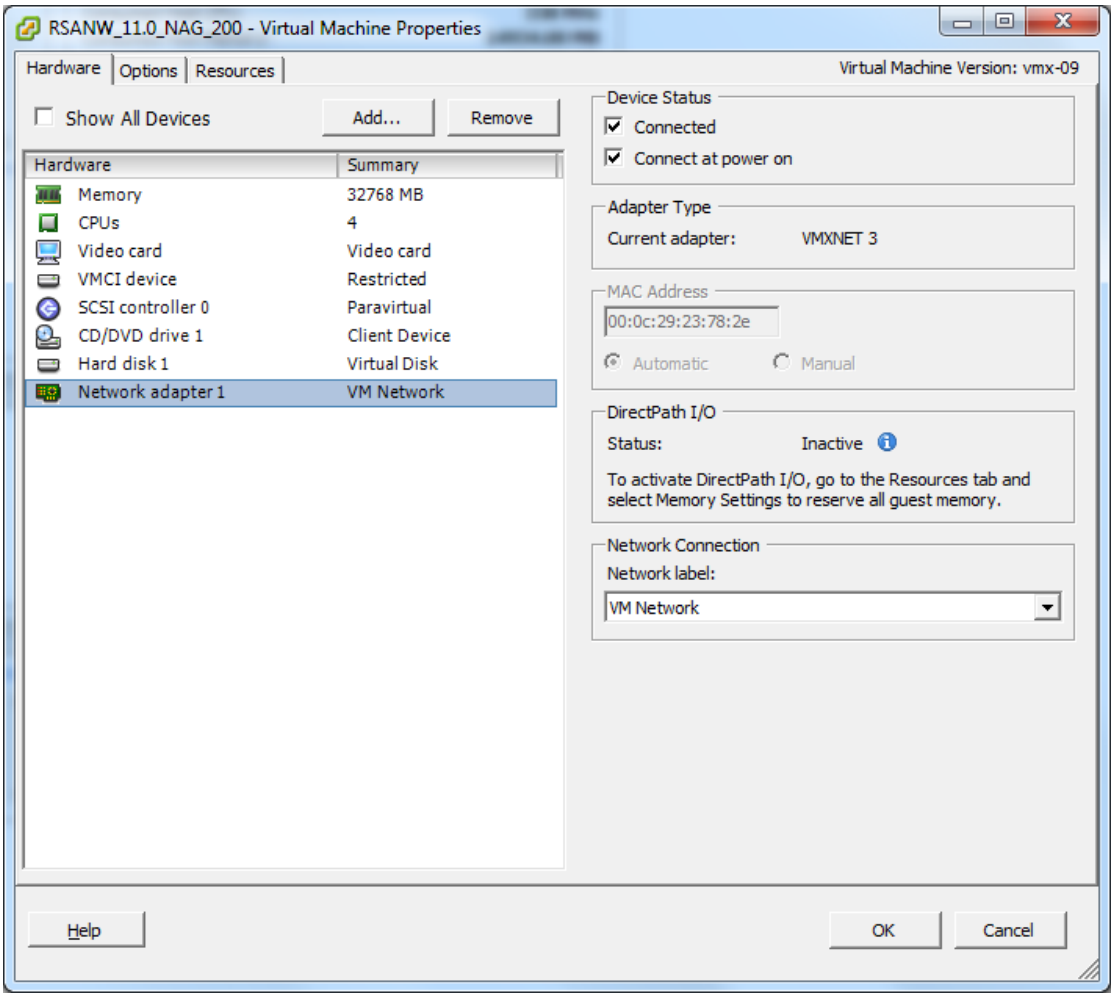
To retain the MAC address of migrated Security Analytics (SA) Server Virtual Machine (VM):

Note: These steps apply to the SA Server VM (created with "Automatic" MAC address assignment selected) to the 11.1 NetWitness Server. For VMs with a Static MAC address, you can change the MAC address by going to Edit Settings for a VM and typing in the MAC address.

1. Log in to vCenter server.

   Note: The supported versions of vCenter is 5.5 through 6.5 inclusive.

2. (Conditional) If they are powered on, **Power Off** both VMs (NetWitness 10.6.5.x and 11.1).
3. Click **Summary** tab, right-click **Datastore** and browse for the datastore location.
4. Go to the VM folder and download the `.vmx` file of 10.6.5.x and 11.1 to the local repository. By default, the VM generated with the MAC address is created in the format (as shown in the below figure).



Note: 00:0c:29:XX:YY:ZZ – 00:0c:29 is the unique identifier for an automatically generated MAC address. **00:50:56:XX:YY:ZZ – 00:50:56** is the unique identifier for a static or manually generated MAC address. This is valid only if the vCenter is not deployed. If vCenter is deployed, this MAC address denotes the unique identifier for an automatically generated MAC address.

5. Using a text editor, copy the `uuid.location` and `ethernet0.generatedAddress` values from 10.6.5.x **.vmx** file into the 11.1 **.vmx** file.

   Note: If you deployed the 10.6.5.x stack on the ESX server directly (not through VCenter), you must copy the value for `uuid.bios` in addition to `uuid.location` and `ethernet0.generatedAddress` from 10.6.5.x **.vmx** file into the 11.1 **.vmx** file.

6. Remove both the 10.6.5.x and the 11.1 VMs from inventory.

   a. Navigate to the vCenter server.

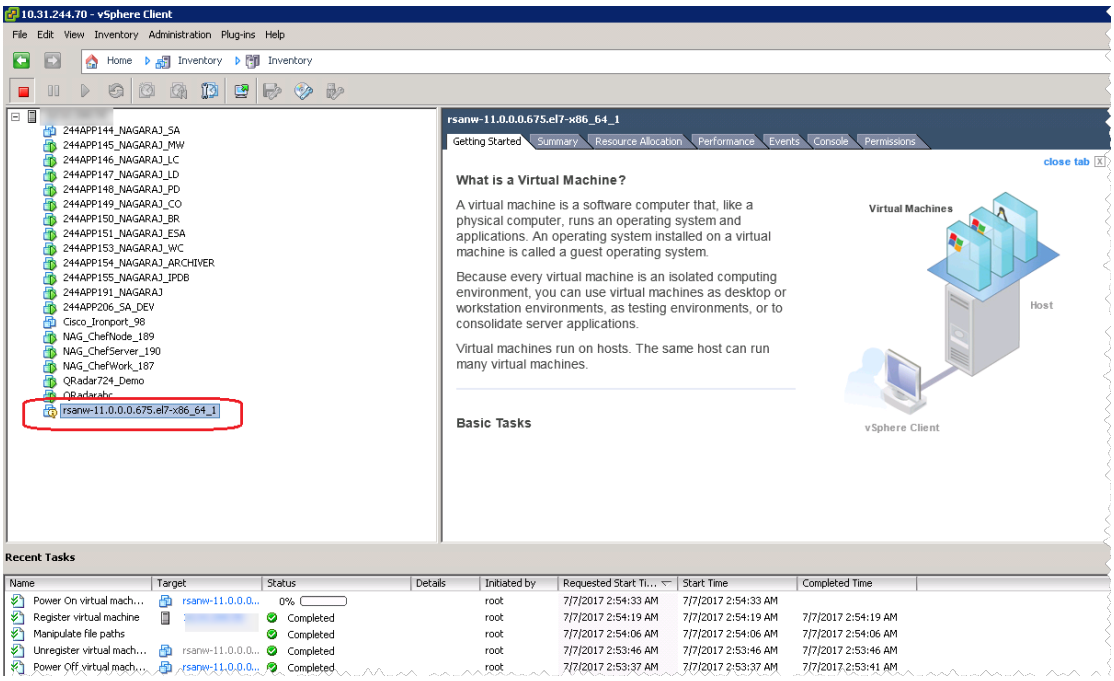
   b. Right-click both the 10.6.5.x and the 11.1 VMs.

c. Select Remove from Inventory.

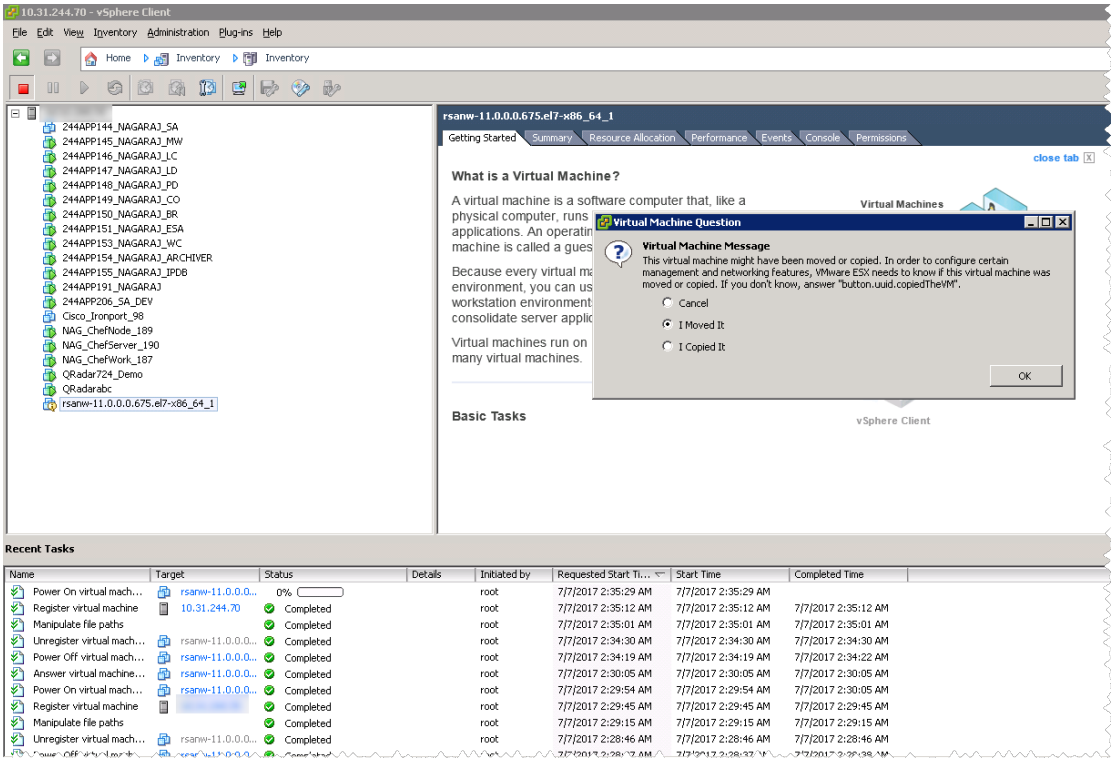
7. Upload the modified 11.1 **.vmx** file to the datastore location by replacing it with the existing **.vmx** file.

8. From the datastore, right- click the 11.1 **.vmx** file and select Add to Inventory.

9. Navigate to the vCenter server and **Power On** the 11.1 VM.
The following message is displayed.
The virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "I Copied it."



10. Right-click the VM and select **Guest** > **Answer Question**.
    The following figure is displayed.



11. Select **I Moved It**.
12. Click **OK**.
    The MAC address is retained to the MAC address from 10.6.5.x to 11.1.

Task 5 - Restore Backup Data in 10.6.5.x to 11.1 VMs

Complete the following steps to **Power On** the 11.1 VM.

1. Copy backed-up data from the `nw-backup` directory to the 11.1 VMs.
   - For the NW Server (SA Server in 10.6.5.x):

     Note: See Virtual Log Collector Host (VLC) for detailed instructions on how to upgrade the VLC.

     a. Create the `nwhome` directory under `/tmp`.

     b. Mount `VolGroup00-nwhome` on `/tmp/nwhome/`.
     ```
     mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
     ```

     c. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`.
     ```
     cp -r /tmp/nwhome/* /var/netwitness/
     ```

d. Mount `VolGroup02-redb` on `/var/netwitness/database`.
```
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

> **Note:** Make sure that the `/var/netwitness/database/nw-backup` directory exists with backup tarballs of the appliance.

e. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- For the Archiver, Broker, Concentrator, Log Decoder/Log Collector, and Packet Decoder:

> **Note:** If your 10.6.5.x Decoder or Log Decoder had multiple network interfaces:
> 1. **Power Off** the 11.1 VM 11.1 Decoder or Log Decoder VM.
> 2. Go to **Edit Settings** for the VM and add the required number of Ethernet Adapters.
> 3. **Power On** the VM.
> 4. Add the ethernet adapters before restoring the backup data.

a. Create the `nwhome` directory under `/tmp`.

b. Create a temporary mount `VolGroup00-nwhome` on `/tmp/nwhome/`.
```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

c. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`.
```
cp -r /tmp/nwhome/* /var/netwitness/
```

d. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- For Malware Analysis (Co-located Malware Not Supported in 11.1 Upgrade):

a. Create the `apps` directory under `/tmp/`.

b. Create a temporary mount `VolGroup01-apps` on `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copy the `nw-backup` directory to `/var/netwitness/`.
```
cp -r /tmp/apps/nw-backup /var/netwitness/database
```

d. Unmount `VolGroup01-apps` from `/tmp/apps/`.
```
umount /tmp/apps
```

- For Event Stream Analysis:

a. Create the `apps` directory under `/tmp/`

b. Create a temporary mount `VolGroup01-apps` on `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copy the `nw-backup` directory to `/var/netwitness`.
```
cp -r /tmp/apps/nw-backup /var/netwitness/database
```

d. Unmount `VolGroup01-apps` from `/tmp/apps/`.
```
umount /tmp/apps
```

2. Mount the disks.

Note: If you have configured any external mount points on the VMs in the stack for any of the following directories, re-mount the external mount points in place of the following mounts.

- For the NW Server:
```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Note: Make sure that the `/var/netwitness/database/nw-backup` directory exists with backup tarballs of the appliance.

- For the Log Decoder/Log Collector:

Note: The following mounts are not required for the Virtual Log Collector.

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/logdecoder/sessiondb
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/logdecoder/packetdb
```

- For the Packet Decoder:
```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/decoder/packetdb
```

- For the Concentrator:
```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
```

```
mount /dev/mapper/VolGroup01-metadb
/var/netwitness/concentrator/metadb
```

- For the Archiver:
  ```
  mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
  mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
  ```
- For the Broker:
  ```
  mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
  ```

8. Add the following mount entries to `/etc/fstab`.
   - For the NW Server:
     ```
     /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
     defaults,noatime,nosuid 1 2
     ```
   - For the Log Decoder/Log Collector:

     Note: The following mounts are not required for the Virtual Log Collector.

     ```
     /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb
     /var/netwitness/logdecoder/sessiondb xfs defaults,noatime,nosuid 1
     2
     /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
     xfs defaults,noatime,nosuid 1 2
     ```
   - For the Packet Decoder:
     ```
     /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
     xfs defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
     defaults,noatime,nosuid 1 2
     ```

```
/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb
xfs defaults,noatime,nosuid 1 2
```

- For the Concentrator:

```
/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime
1 2
/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
xfs defaults,noatime,nosuid 1 2
```

- For the Archiver:

```
/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
defaults,nosuid,noatime 1 2
/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
defaults,nosuid,noatime 1 2
```

- For the Broker:

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
defaults,nosuid,noatime 1 2
```

Set Up Virtual Hosts in 11.1

There two phases to set up your 11.1 virtual stack that you must complete in the order shown.

- Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

  Note: For Event Stream Analysis, if you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

- Phase 2 - Set Up The Rest of the Component Hosts

Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

Task 1 - Set Up 11.1 NetWitness Server

Follow the instructions under Set Up 11.1 NW Server Host.

Task 2 - Set Up 11.1 ESA

Caution: If you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.1 Non-NW Server Host to set up your ESA hosts.

1. Set up your primary ESA host through the Setup program and install **ESA Primary** on the host in the user interface on the **Admin Hosts** view.

   Note: If you have multiple ESA hosts in your enterprise, you must upgrade the ESA Primary host, where all the `mongodb` (Mongo Database) backup tar files are located, first, before you upgrade ESA Secondary hosts.

2. (Conditional) If you have a secondary ESA host, set it up through the Setup program and install **ESA Secondary** on the host in the user interface on the **Admin Hosts** view.

Task 3 - Set Up 11.1 Malware Analysis

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Task 4 - Set Up 11.1 Broker or Concentrator

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Set Up The Rest of the Component Hosts

See Appendix B. Stopping and Restarting Data Capture and Aggregation for instructions on how to stop and restart data capture and aggregation when upgrading the Decoder, Concentrator, and Log Collection hosts.

Decoder and Concentrator Hosts

1. Stop data capture and aggregation.
2. Complete the steps in Set Up 11.1 Non-NW Server Host.
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the **Backup Instructions**.
2. Stop data capture on the Log Decoder.
3. Complete the steps in Set Up 11.1 Non-NW Server Host.
4. Restart data capture on Log Decoder.

Note: After you upgrade, you will restart log collection after completing the Task 28 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task in the **Post Upgrade Tasks**

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described in the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the **Backup Instructions**.
2. Back up your 10.6.5.x VLC by editing the `all-systems` file on host where you performed the backup.

a. Make sure your `all-systems` file contents has this information before you perform this step.

```
vlc,<host-name>,<IP-address>,<UUID>,10.6.5.x
```

b. Run the following command to create backup.

```
./nw-backup.sh -u
```

See Backup Instructions for detailed procedures on how to back up the host.

3. Make sure the backup host contains the VLC backup in the following format.

```
<hostname>-<IPaddress>-root.tar.gz
<hostname>-<IPaddress>-root.tar.gz.sha256
<hostname>-<IPaddress>-backup.tar.gz
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```

4. Power off the 10.6.5.x VLC so that a new 11.1 VM can be created with the same network configuration.
5. Deploy a fresh Non-NW Server host using the 11.1 NetWitness Suite ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.5.x VLC.
This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.5.x VLC backup file.

Note: Make sure IPv6 is disabled.

a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings. Contents of `ifcfg-eth0` should be as follows.

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. Submit the following command string.

```
systemctl restart network.service
```

8. Create the backup directory.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new VLC in the `/var/netwitness/database/nw-backup` directory.
10. Complete the steps 2 through 12 inclusive in Set Up 11.1 Non-SA Server Host for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

Set Up 11.1 NW Server Host

Make sure that you have backed up 10.6.5.x data for the SA Server host. **You must follow the instructions in Backup Instructions to back up the host**.

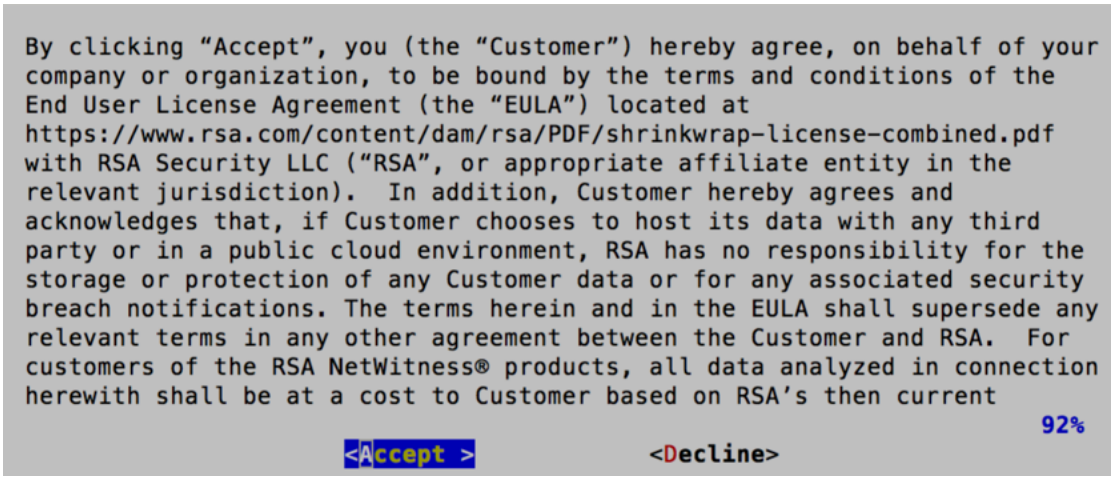
Caution: Run the backup immediately before upgrading the SA Server to 11.1 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.1.

Complete the following steps to set up the 11.1 NW Server host.

1. Log in to 11.1 NW Server VM's console and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

   Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press the Enter key to register your command response and move to the next prompt.
   2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

2. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

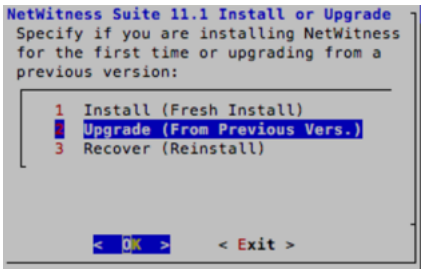
Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

3. Tab to **Yes** and press **Enter**.

Choose **No** if you already upgraded the NW Server to 11.1.

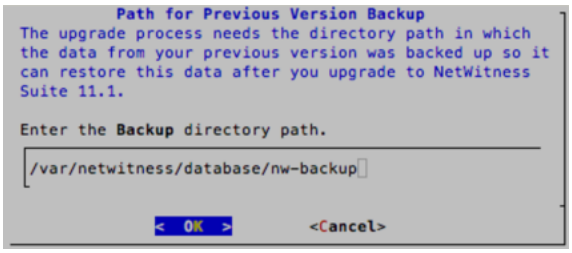
The **Install or Upgrade** prompt is displayed.

4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.



The **Backup** path prompt is displayed.

5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.



This table lists the backup and restore paths by host/service.

Host	Backup Path	Restore Path
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
All Other Hosts	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

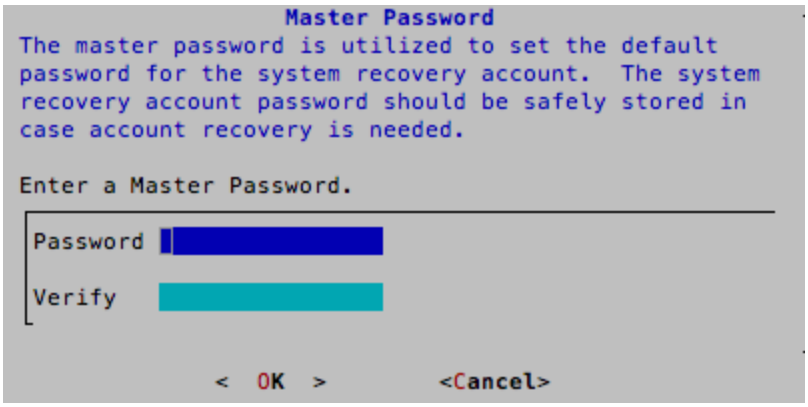
The **Master Password** prompt is displayed.

The following list of characters are supported for Master Password and Deployment Password:

- Symbols : ! @ # % ^ + ,
- Numbers : 0-9
- Lowercase Characters : a-z
- Uppercase Characters : A-Z

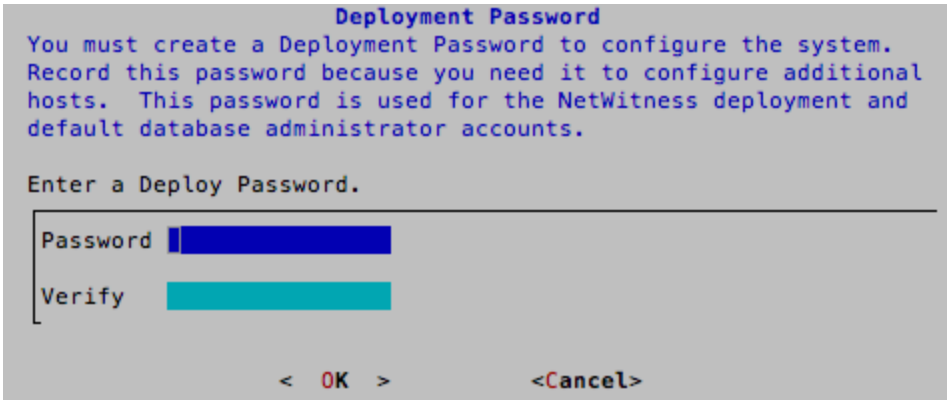
No ambiguous characters are supported for Master Password and Deployment Password. For example:
space { } [ ] ( ) / \ ' " ` ~ ; : . < > -

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



The **Deployment Password** prompt is displayed.

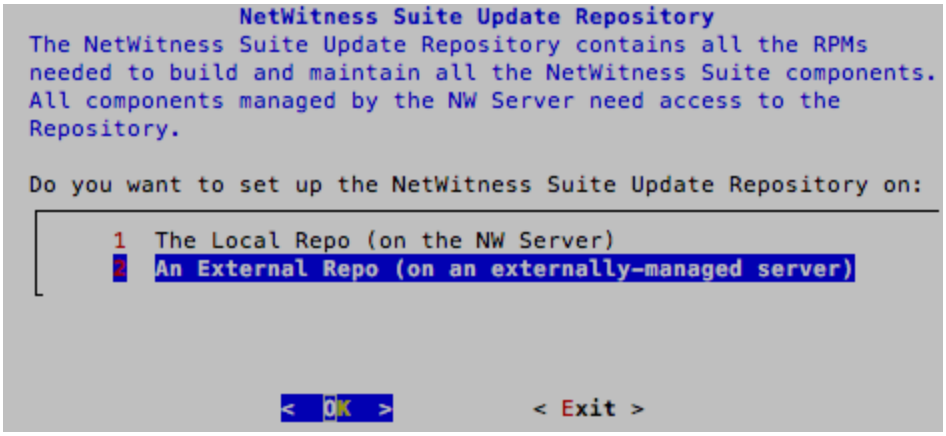
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



The **Update Repository** prompt is displayed.

You must use the same repo that you used for the NW Server hosts for all hosts.

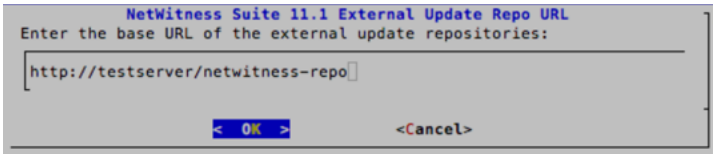
8. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.



The **External Update Repo URl** prompt is displayed.

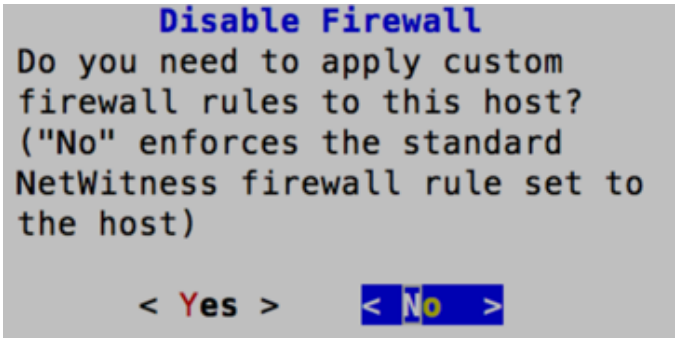
Refer to Appendix D. Create External Repository for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

9. Enter the base URL of the NetWitness Suite external repo (for example, **http:/testserver/netwitness-repo**)and click **OK**.

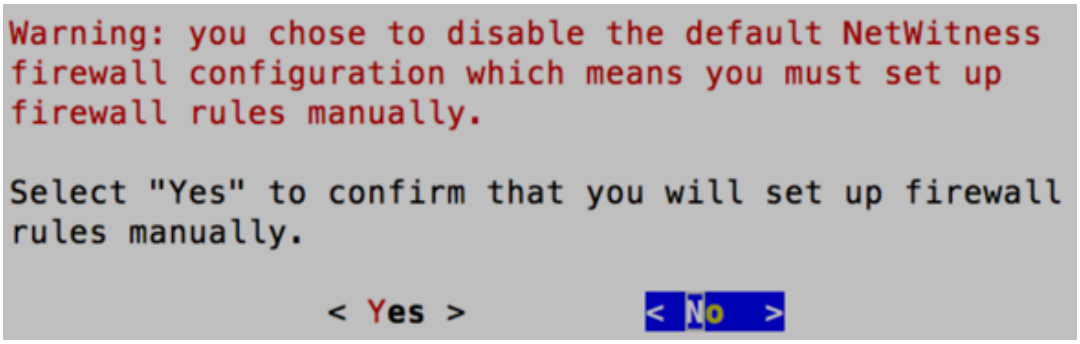


The **Disable** or use standard **Firewall** configuration prompt is displayed.

10. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

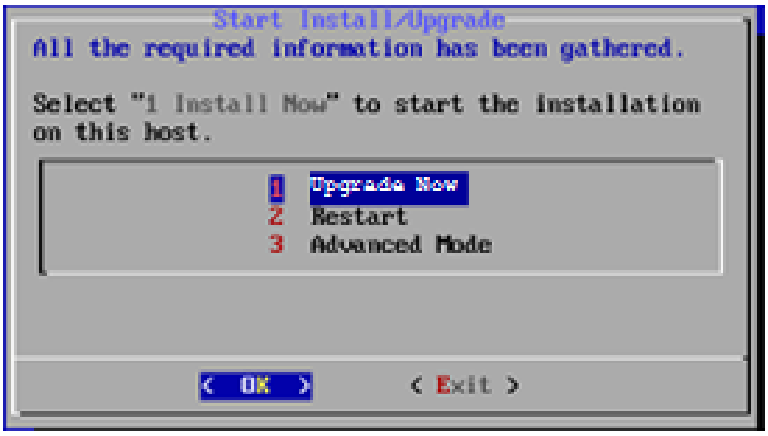


- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.



When **Installation complete** is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
      (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

12. Complete the NW Server before you upgrade any of the non-SA Server hosts to 11.1.

Set Up 11.1 Non-NW Server Host

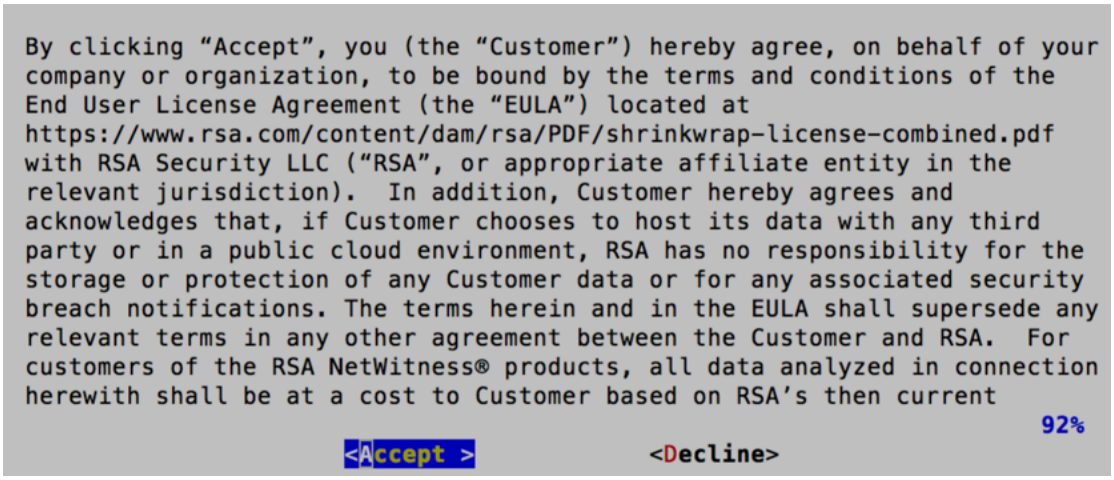
Make sure that you Back up your 10.6.5.x data for the host. **You must follow the instructions in Backup Instructions to back up the host.**

Caution: Run the backup immediately before upgrading the host to 11.1 so that the data is as recent as possible.

Complete the following steps to set up an 11.1 Non-NW Server host.

1. Log in to 11.1 non-NW Server VM console and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

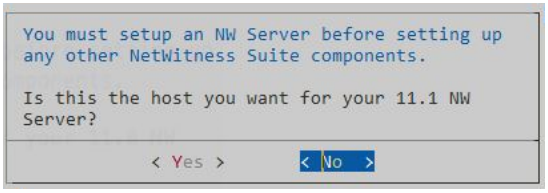
2. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

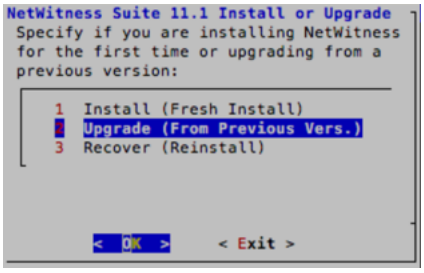
Caution: If you choose the wrong the host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

3. Tab to **No** and press **Enter**.



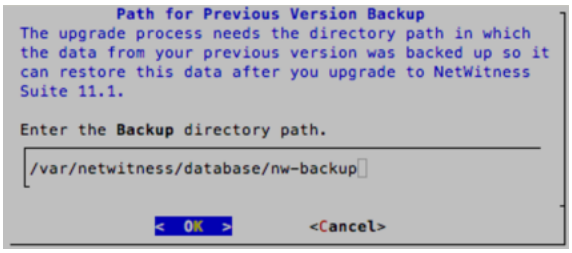
The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.



The **Backup** path prompt is displayed.

5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.



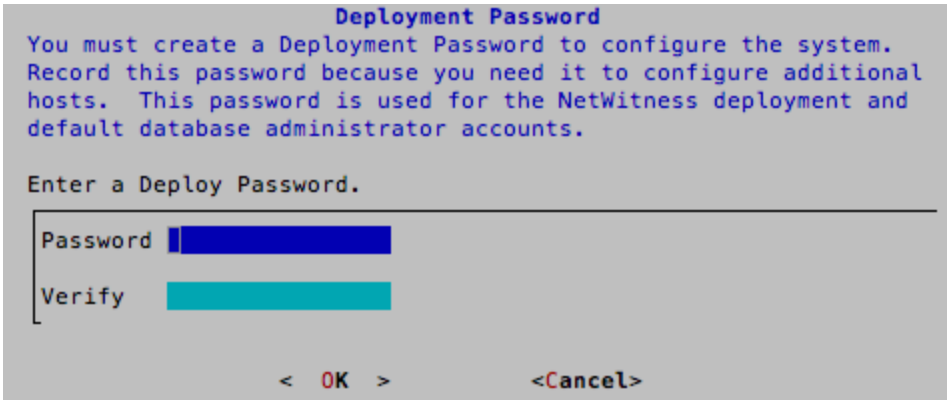
This table lists the backup and restore paths by host/service.

Host	Backup Path	Restore Path
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
All Other Hosts	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

The **Deployment Password** prompt is displayed.

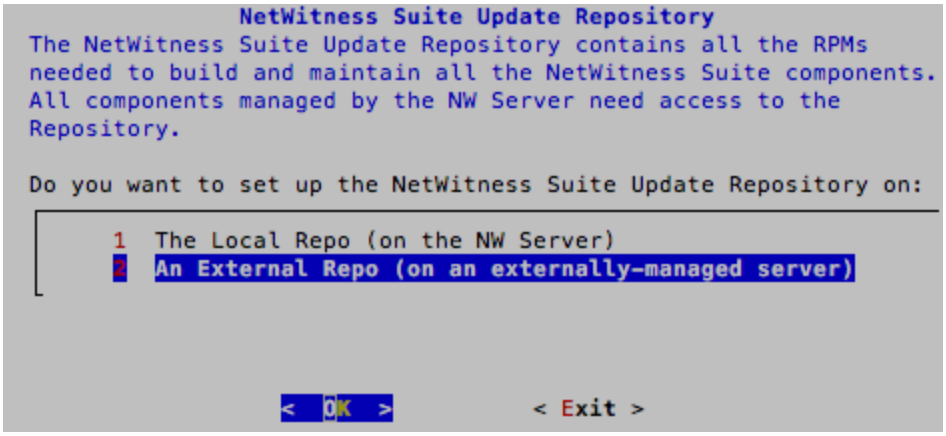
Note: You must use the same deployment password that you used when you upgraded the NW Server.

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



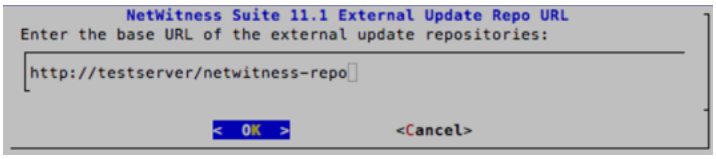
The **Update Repository** prompt is displayed.

7. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, tab to **OK**, and press **Enter**.



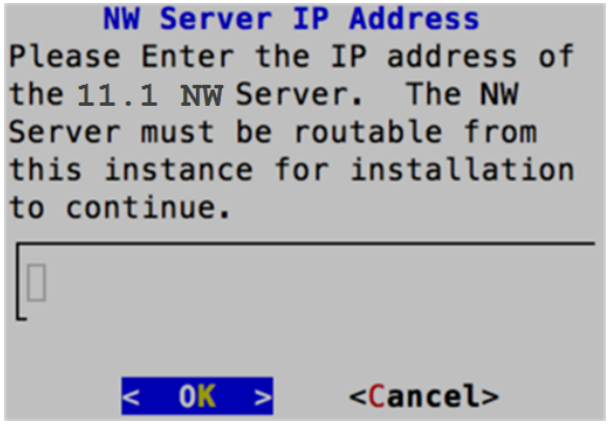
   The **External Update Repo URL** prompt is displayed.
   The repositories give you access RSA updates and CentOS updates.

8. Enter the base URL of the NetWitness Suite external repo (for example, **http://testserver/netwitness-repo**)and click **OK**. Refer to Appendix D. Create External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



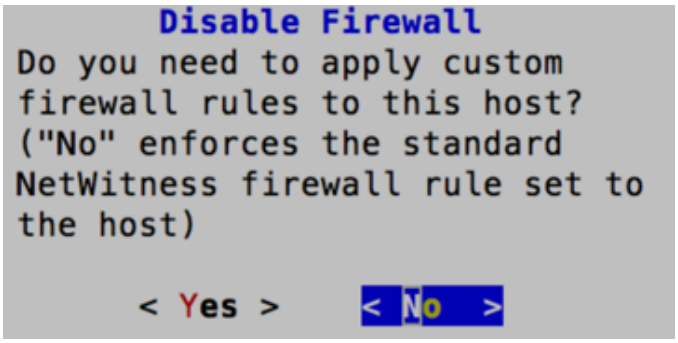
   The **NW Server IP Address** is displayed.

9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

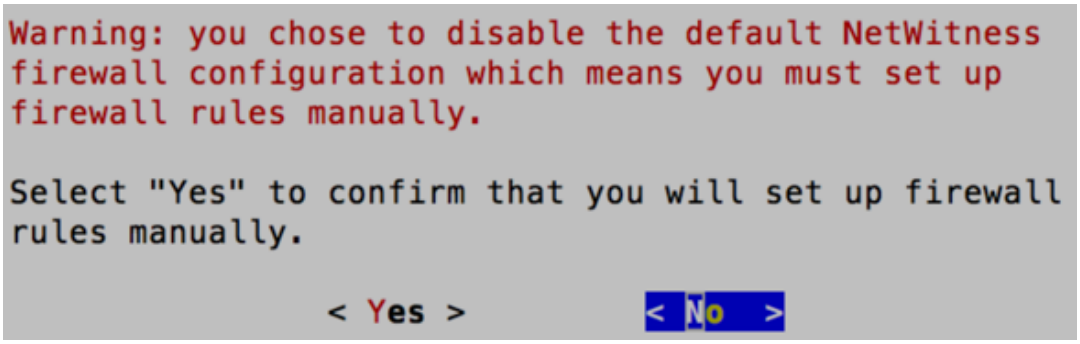


   The **Disable** or use standard **Firewall** configuration prompt is displayed.

10. Tab to **No** (default), and press Enter to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.



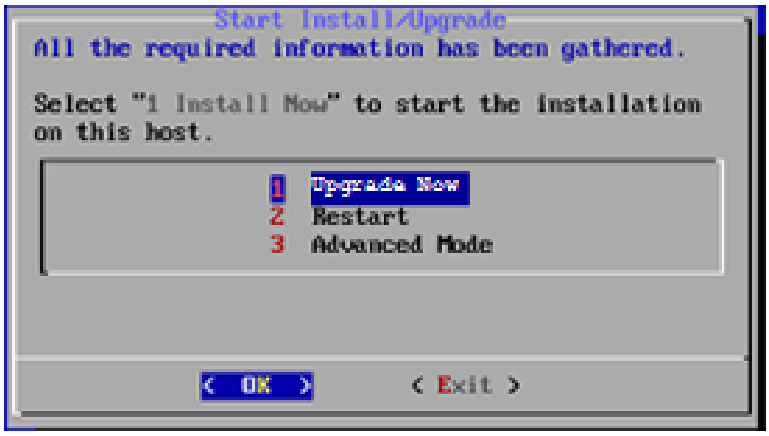
- If you select **Yes**, confirm your selection.



- If you select **No**, the standard firewall configuration is applied.

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.



When **Installation complete** is displayed, you have upgraded the host to the 11.1.

12. Install the service on this host:

    a. Log into NetWitness Suite and click **ADMIN** > **Hosts**.

    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

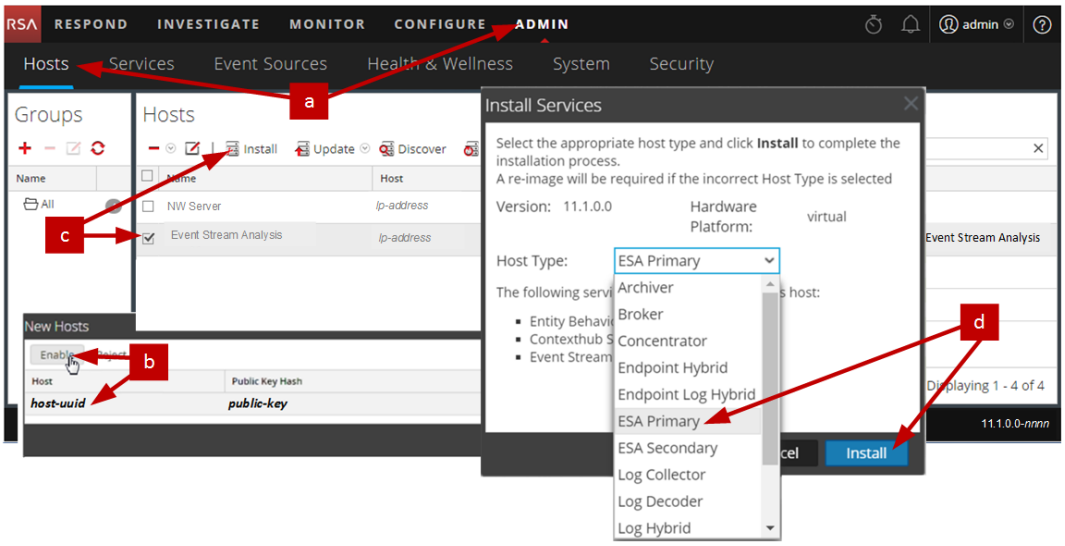
b. Click on the host in the **New Hosts** dialog and click **Enable**.

The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click Install

The **Install Services** dialog is displayed.

d. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



You have completed the upgrade of the non-NW Server host in NetWitness Suite

Note: When you upgrade a Respond host from 10.6.5.x to 11.1, it takes a period of time for Respond to come back online. This is caused by Respond indexing data while it is restored. The size of the data in the Mongo database will determine the time.

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.1. These tasks are organized by the following categories.

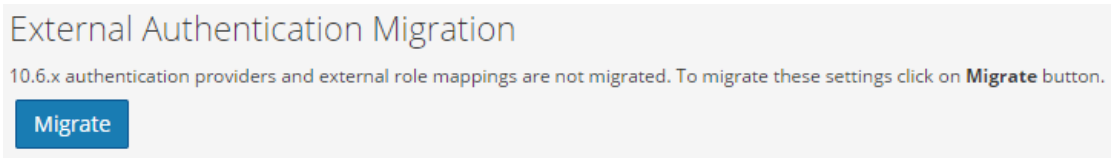
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Investigate
- Log Collection
- Reporting Engine
- Respond
- RSA NetWitness® SecOps Manager
  (RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)
- Backup

NW Server

Task 1 - Migrate Active Directory (AD)

The first time you log into the NetWitness Suite 11.1 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Suite 11.1 with your `admin user` credentials.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.

3. Click **Migrate**.
   The migration is complete and the dialog closes.

Task 2 - Modify Migrated AD Configuration to Upload Certificate

If you authenticated through Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.5.x, you must modify the migrated AD configuration to upload the Active Directory server certificate.

Complete the following procedure to modify the migrated AD configuration to upload the certificate.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** and click the **Settings** tab.
2. Under **Active Directory Settings**, select an AD configuration and click .

   The Edit Configuration dialog is displayed.
3. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
4. Click **Save**.

Task 3 - Reconfigure Pluggable Authentication Module (PAM) in 11.1

You must reconfigure PAM after you upgrade to 11.1. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite System Security and User Management Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

You can refer to your 10.6.5.x PAM configuration files in the **/etc** directory in the your 10.6.5.x backup data for guidance.

Task 4 - Restore NTP Servers

You must use the NetWitness Suite 11.1 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *RSA NetWitness® Suite System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 5 - Restore Licenses for Environments without FlexNet Operations-On Demand Access

If your environment does not have access to FlexNet Operations-On Demand, you need to re-download your NetWitness Suite licenses. Refer to "Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on how to re-download licenses. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 6 - Remap Virtual NW Server License to 10.6.5.x MAC Address

If you are upgrading a Security Analytics server running on a virtual machine, change the 11.1 NW Server virtual host to the 10.6.5.x MAC address to retain licensing. Refer to "Licensing: Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on remapping a license to a new MAC address." Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

(Conditional) Task 7 - If You Disabled Standard Firewall Config - Add Custom IPtables

During the upgrade, you have the option of using these rules or disabling them. If you disabled them, follow these instructions as a baseline to create a user-managed firewall rule sets on all the hosts for which you disabled the standard firewall configuration.

Note: You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the restore folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.
2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Reload the `iptables` and `ip6tables` services.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditional) Task 8 - Specify SSL Ports If You Never Set Up Trusted Connections

Complete this task only if you never set up Trusted Connections. You would not have set up Trusted Connections if you:

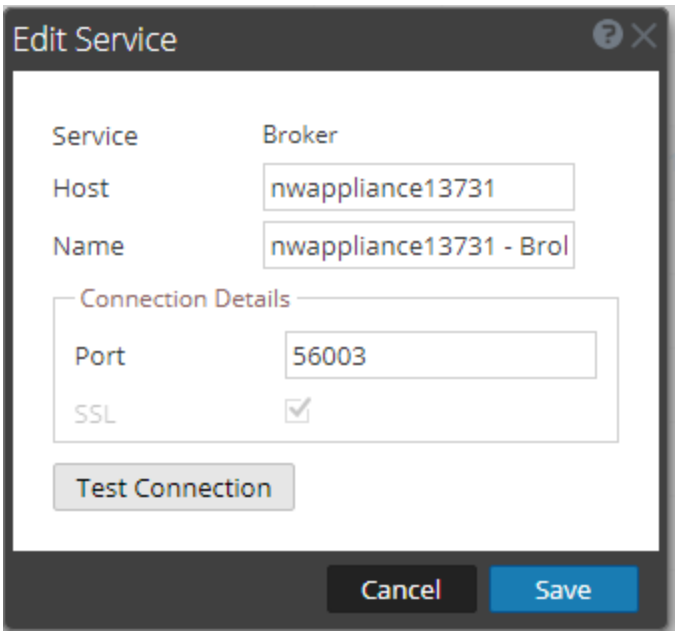
- Used the base ISO image for 10.3.2 or earlier.
- Updated the system using RPMs exclusively to get to 10.6.5.

NetWitness Suite 11.1 cannot communicate with the core services for these customers because they are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Services**.
2. Select each core service and change there ports from Non-SSL to SSL ports.

Service	Non-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

3. Click (Edit) from the **Services** view toolbar.
   The Edit Service dialog is displayed.
4. Change the port from Non-SSL to SSL as shown in the table and click **Save** (for example, change the Broker port from 50003 to 56003).



Task 9 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File

Problem: When a user updates from 10.6.5 to 11.1 and 11.0.0.0 to 11.1, if they have a global auditing set up, audit log templates are not getting updated in Logstash output conf file.

Workaround: If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click save to apply the latest Audit log configuration.

If you had global auditing configured in 11.0.x, you must complete the following procedure to apply the latest Global Auditing configuration.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications**.
   The **Global Notifications** view is displayed.
2. Click the **Servers** tab, select any syslog server.
3. Click (edit icon) and click **Save**.

RSA NetWitness® Endpoint

Task 10 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

You must reconfigure the Legacy Endpoint recurring feed due to the change in Java version. Complete the following step to fix this problem.

1. Import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness Endpoint Integration Guide* to import the certificate.
   Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint Insights

(Optional) Task 11 - Install Endpoint Hybrid or Endpoint Log Hybrid

See:

RSA NetWitness Suite 11.1 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Suite 11.1 Virtual Host Installation Guide for instructions for installation on a virtual host.

Task 12 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.
   ```
   <add key="IMVirtualHost" value="/rsa/system" />
   ```

Note: In NetWitness Suite 11.1, the virtual host is `/rsa/system`. For 10.6.5.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.
3. SSH to the NW Server and log in with `root` credentials.
4. Submit the following command to add all certificates to the truststore.
   `orchestration-cli-client --update-admin-node`
5. Submit the following command to restart the RabbitMQ server.
   `systemctl restart rabbitmq-server`
   The NetWitness Endpoint account should automatically be available on RabbitMQ.
6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Event Stream Analysis Tasks (ESA)

Task 13 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.1.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
2. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. Click **ADMIN** > **Services**, select the Context Hub service, in the action commands ( ) drop-down menu, click **View** > **Config** > **Lists** tab).
   b. Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Suite ESA Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 14 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL

If you integrate with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint, you must configure Mutually Authenticated SSL on each integrated system so that the application can authenticate itself when connecting to the RabbitMQ message bus.

Note: Use the RabbitMQ usernames and passwords that were obtained when you backed up your 10.6.5.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Suite by logging into the host and running the following `rabbitmqctl` command.

   ```
   > rabbitmqctl add_user <username> <password>
   ```

   For example:

   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

2. Set permissions for users by running the following command (use the username from step 1):

   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*",
   ".*"
   ```

   For example:

   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*",
   ".*", ".*"
   ```

Task 15 - Enable Threat - Malware Indicators Dashboard

In 11.1.0, the 10.6.5.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.5.x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.1.
2. Set datasource for new dashlets.

   See "Dashlets" in RSA Link (https://community.rsa.com/docs/DOC-81463) for a description of Dashlets in the context of NetWitness Suite.

Investigate

Task 16 - Make Sure User Roles Have Customized User Roles Have `Investigate-server` Permissions for Event Analysis Access

After you upgrade to 11.1.0.0, any customized user role does not have `investigate-server.*` permission enabled by default. Complete the following procedure to make sure that the appropriate user roles have permission to access Event Analysis.

1. Log in to NetWitness Suite 11.1.0.0 as an `Admin` user.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** .
3. Click the **Roles** tab.
4. Select the roles that need `investigate-server.*` permissions and click (edit icon).
5. Select the **Investigate-server** tab under under **Permissions**.
6. If investigate-server checkbox is not checked, check it for the users that require Event Analysis access.

7. Click **Save**.

Log Collection

Task 17 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.1 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

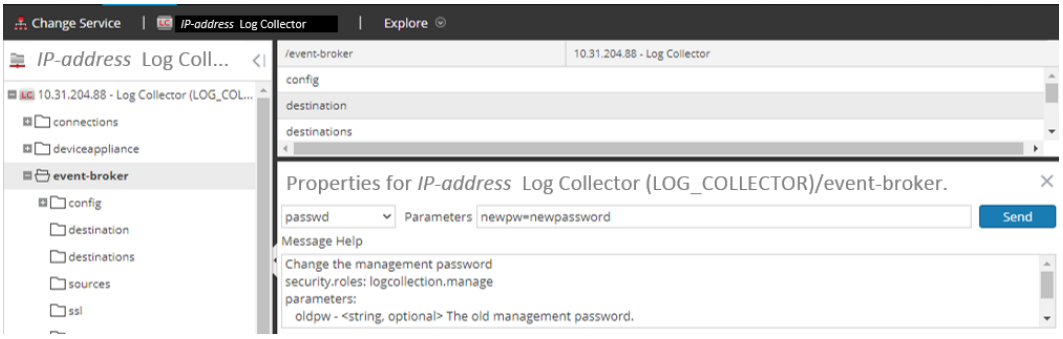
The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Update Log Collector Service RabbitMQ User Account Password

If the logcollector service RabbitMQ user account password was changed, you must reenter it after the 11.1 upgrade.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN > Services**.
2. Select the Log Collector service.
3. Click (Actions) > **View** > **Explore**.
4. Right click `event-broker` > **Properties**.

5. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders)

Task 18 - Enable FIPS Mode

FIPS is enabled on all services except Log Collector, Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder. For information about how to enable FIPS for these services, see the "Sys Maintenance: Activate or Deactivate FIPS" topic in the *RSA NetWitness® SuiteSystem Maintenance Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Reporting Engine

Task 19 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the back up you made prior to the upgrade. The Backup script backs up the 10.6.5.x CA certificates into the `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts` directory.

Complete the following procedure to restore the CA certificates in 11.1.

1. SSH to the NW Server host.
2. Export the CA certificates.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Copy the CA pem into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 20 - Restore External Storage for Reporting Engine

If you have external storage for the Reporting Engine (such as SAN or NAS for storing reports), you must restore the mount you unlinked before the upgrade. See "Reporting Engine: Add Additional Space for Large Reports" in the *RSA NetWitness® Suite Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

(Conditional) Task 21 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.1. See "Add a Role and Assign Permissions" in the *RSA NetWitness Suite System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 22 - Restore Respond Service Custom Keys

In 10.6.5.x, if you added custom key for use in the **groupBy** clause, the `alert_rules.json` file was modified. The `alert_rules.json` file contains aggregation rule schema. RSA moved the `alert_rules.json` file to the following new location: `/var/lib/netwitness/respond-server/scripts`

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.

   This directory is where the `alert_rules.json` file is restored from the 10.6.5.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.1.

   This is the new file for 11.1.

3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 23 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.1 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.x, you must:

1. Go to the to the `/opt/rsa/im/scripts` directory.
   This directory is where the following Respond service normalization scripts are restored from the 10.6.5.x backup.
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Copy any custom logic from the 10.6.5.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Suite 11.1 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
   The `alert_rules.json` file contains aggregation rule schema.

Task 24 - Add Respond Notification Settings for Custom Roles

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**CONFIGURE** > **Respond Notifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. You will also need to add permissions to your custom roles. See the "Respond Notification Settings Permissions" topic in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 25 - Manually Configure Respond Notification Settings

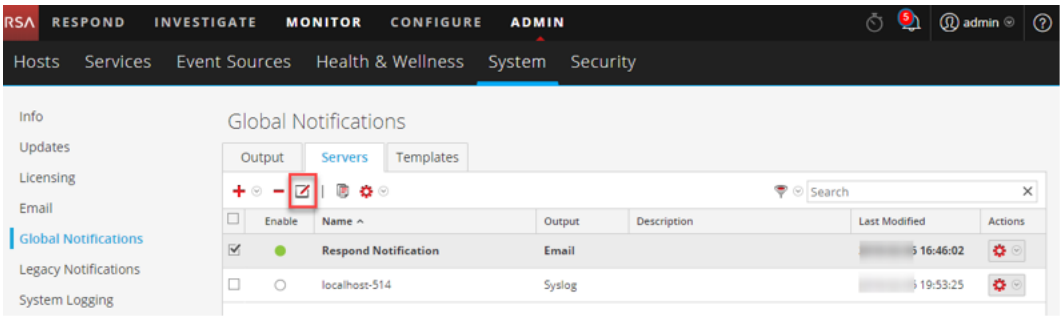
The Incident Management notification settings in NetWitness Suite 10.6.5.x to 11.1 are different from the Respond notification settings available in 11.1, so your existing 10.6.5.x to 11.1 settings will not migrate to 11.1.

NetWitness Respond notification settings enable email notifications to be sent to SOC Managers and the Analyst assigned to an incident when an incident is created or updated.

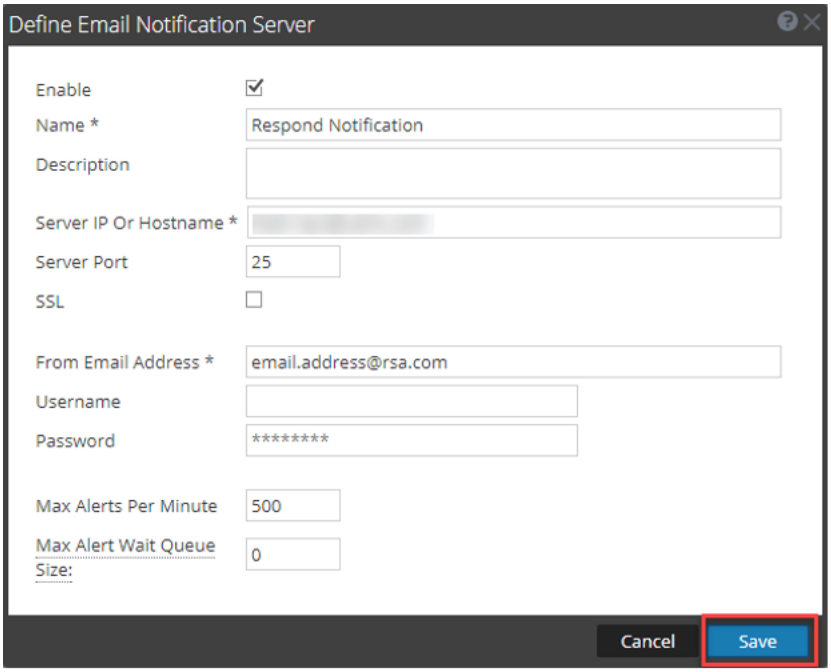
To manually configure the Respond Notification Settings, go to **CONFIGURE** > **Respond Notifications.** See the "Configure Respond Email Notification Settings" procedure in the *NetWitness Respond Configuration Guide*.

Notification Servers from 10.6.5.x to 11.1 will not display in the Email Server drop-down list. The email servers must be edited and saved in the Global Notification Servers panel (**ADMIN** > **System** > **Global Notifications** > **Server** tab).

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications** > **Server** tab.
2. Go to **CONFIGURE** > **Respond Notifications**. The Respond Notifications Settings view is displayed.
3. Notice that the email notification servers do not appear in the EMAIL SERVER drop-down list.
4. Click the **Email Server Settings** link. You will see the Global Notifications panel.
5. Click the **Servers** tab.
6. For each of your email notification servers:
   a. Select the Email notification server and click .



b. In the Define Email Notification Server dialog, click **Save**.



7. Go back to **CONFIGURE** > **Respond Notifications**. Your servers will appear in the **EMAIL SERVER** drop-down list.
   Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

Task 26 - Update Default Incident Rule Group By Values

Four of the default incident rules now use ”Source IP Address” as the Group By value. To update the default rules, change the Group By value of the following default rules to “Source IP Address”:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

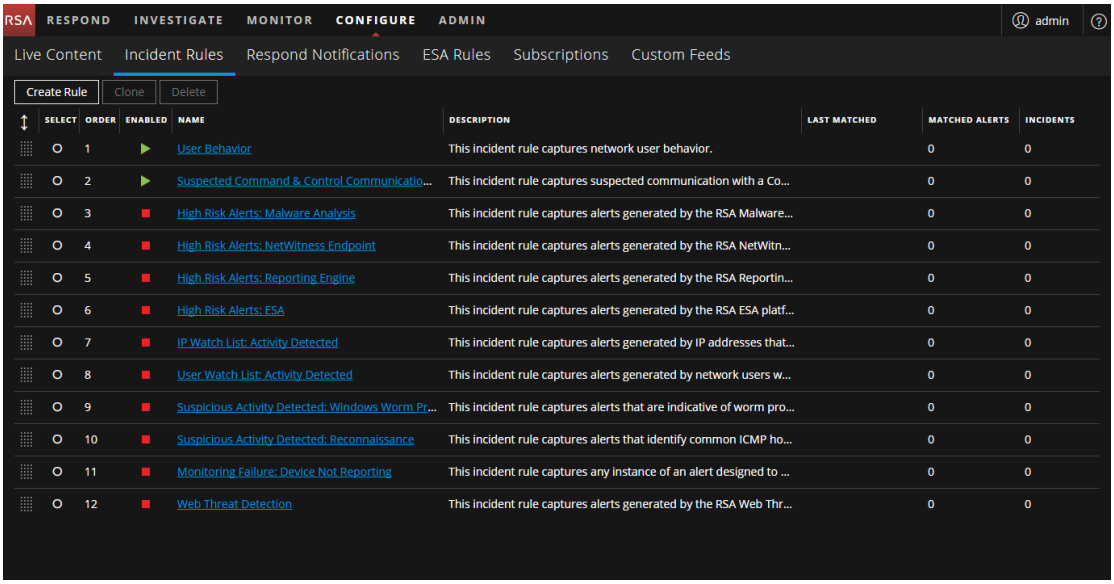
1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update. The Incident Rule Details view is displayed.
2. In the **Group By** field, select the new Group By value.
3. Click **Save** to update the rule.

Task 27 - Add Group By Field to Incident Rules

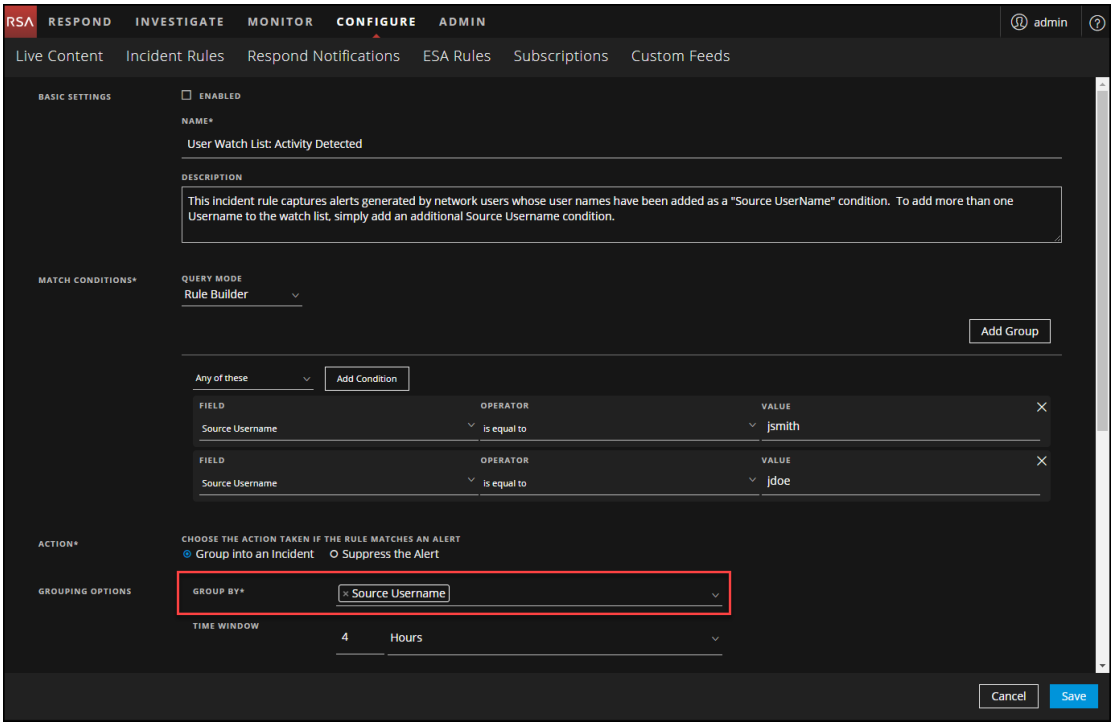
The **Group By** field is not required in 10.6.5, but it is required in 11.1. After you upgrade to 11.1, some incident rules will not have a **Group By** field, so you must add them to the rules or the rules will not work and they will not create incidents.

Complete the following steps for each incident rule:

1. In the **NetWitness Suite** 11.1 menu, select Go to **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



2. In the Group By field, verify that a Group By value is selected. If not, select a Group By value.



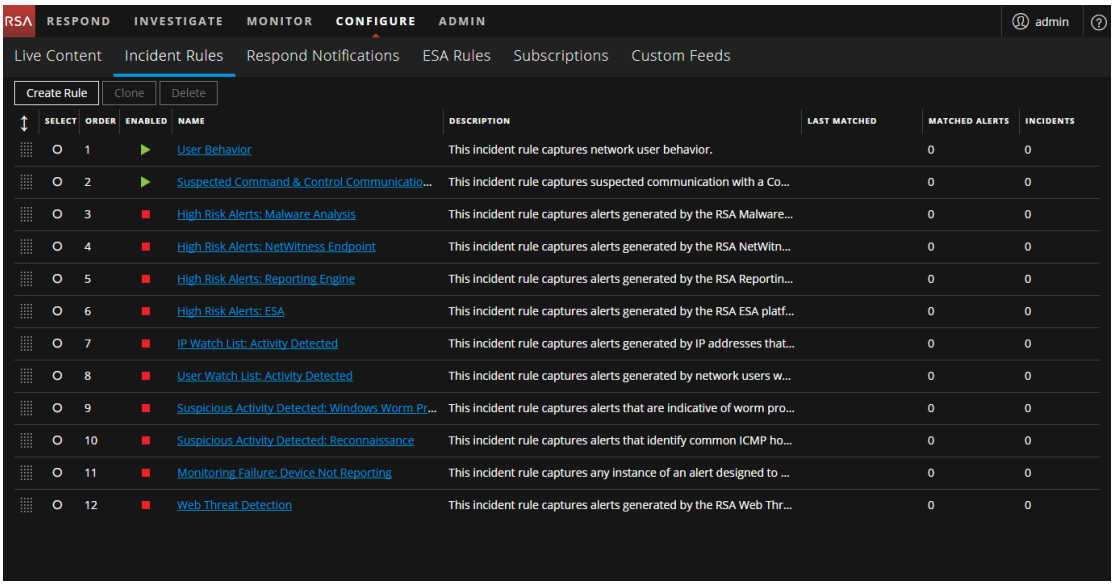
3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 28 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task

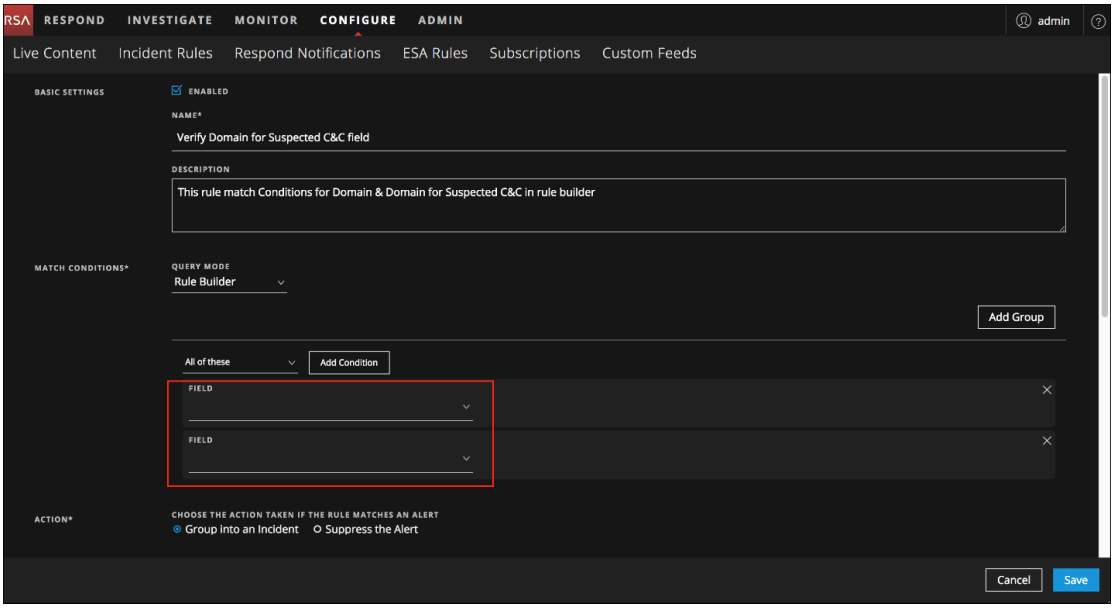
Modify the incident rules that you identified in the Task 4 - Check Aggregation Rules Match Conditions for "Domain" or "Domain for Suspected C&C" upgrade preparation task, which contained Domain or Domain for Suspected C&C in the matching conditions in rule builder, to use only Domain.

For each rule that you previously identified:

1. In the **NetWitness Suite** 11.1 menu, select **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



2. In the **Match Conditions** section, in the blank fields, select **Domain** in the drop-down list and then select the conditions that you previously identified in the pre-upgrade tasks.



3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® SecOps Manager

(RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)

Task 29 - Reconfigure NW SecOps Manager Integration

For information on how to reconfigure NW SecOps for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Backup

Task 30 - Remove Backup-Related Files from Host Local Directories

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.1 before you remove the backup-related files from the local directories on your 11.1 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.1, you must remove:

- the backup files from the local directories on the hosts.
- all the files from `nw-backup` and `restore` directories on the hosts.

Host	Backup Path	Restore Path
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
All Other Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Appendix A. Troubleshooting

This section describes solutions to problems that you may encounter during installations and upgrades. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294) .

This section has troubleshooting documentation for the following services, features, and processes.

- Command Line Interface (CLI)
- Backup Script
- Event Stream Analysis
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

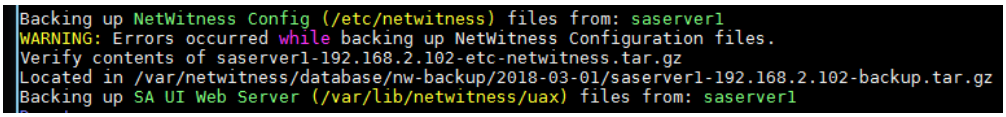
Command Line Interface (CLI)

Error Message	Command Line Interface (CLI) displays: "Orchestration failed." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Entered the wrong `deploy_admin` password in `nwsetup-tui`.
Solution	Retrieve your `deploy_admin` password password. 1. SSH to the NW Server host. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` SSH to the host that failed. 2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

Error Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Suite sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service. `systemctl restart rsa-sms`

Backup (`nw-backup` script)

Error Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the *Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Error	Backup errors caused by the `immutable` attribute setting. Here is an example of an error that can be displayed: 
Cause	If you have any files that have the immutable flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.
Solution	On the host that contains the files with the immutable flag set, run the following command to remove the immutable setting from the files: `chattr -i <filename>`

Error	Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: `/etc/sysconfig/network-scripts/ifcfg-em1` Verify contents of `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Cause	There are incorrect or duplicate entries for any one of the following fields: DEVICE, BOOTPROTO, IPADDR, NETMASK or GATEWAY, that were found from reading the primary Ethernet interface configuration file from the host being backed up.

Solution	Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format `<hostname>-<hostip>-network.info.txt`, and should contain the following entries:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1.0.0 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESA Primary host and log in.
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Submit the following command to restart ESA.
	`systemctl restart rsa-nw-esa-server`
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Suite and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Suite and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Error Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Suite and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.5.x to 11.1.0.0.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Error Message	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Appendix B. Stopping and Restarting Data Capture and Aggregation

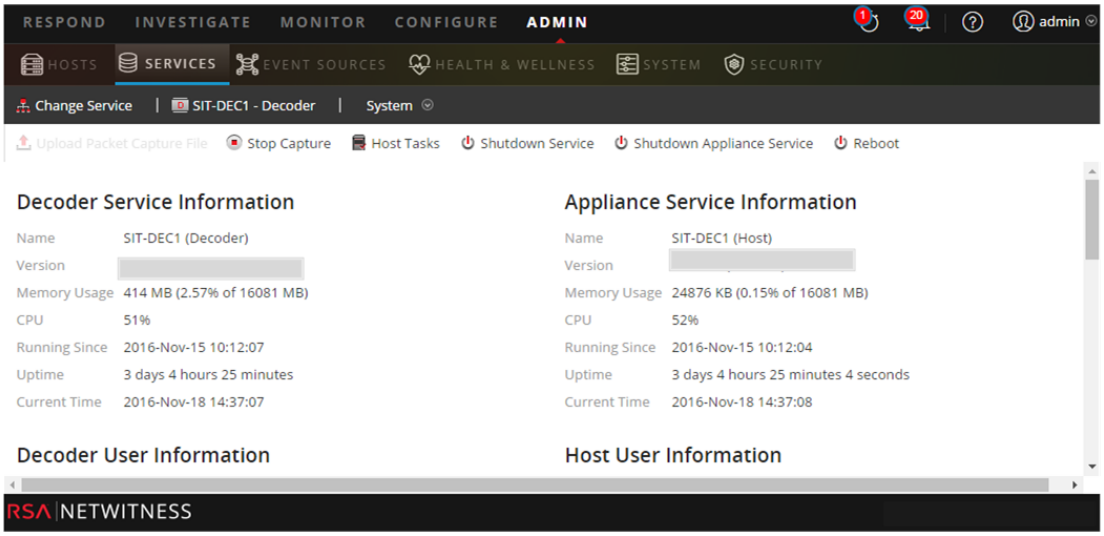
RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.1.0.0. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.



3. Under (actions), select **View** > **System**.
4. In the toolbar, click

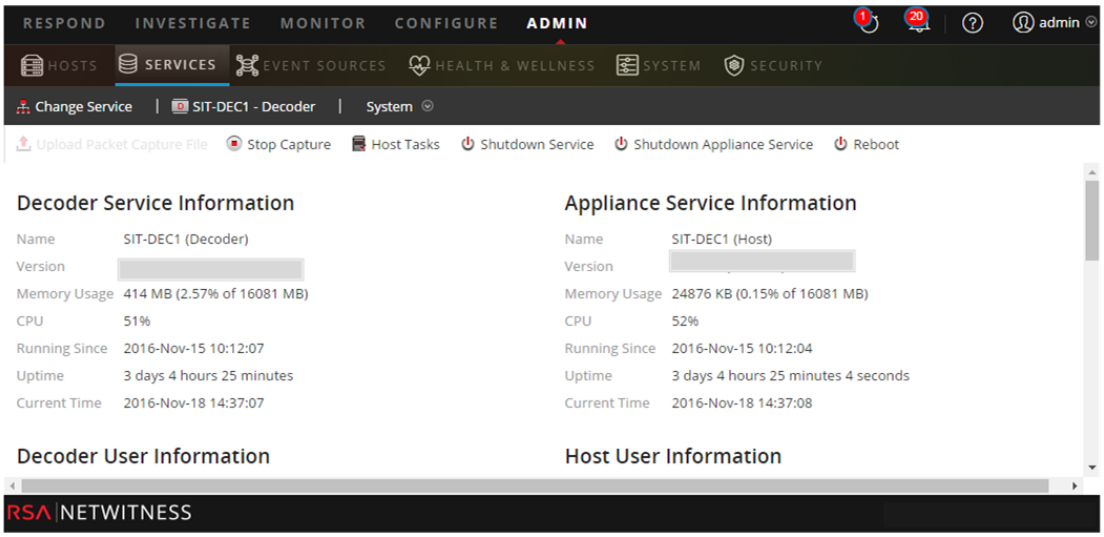
.

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.



3. Under (actions), select **View** > **System**.

4. In the toolbar, click

.

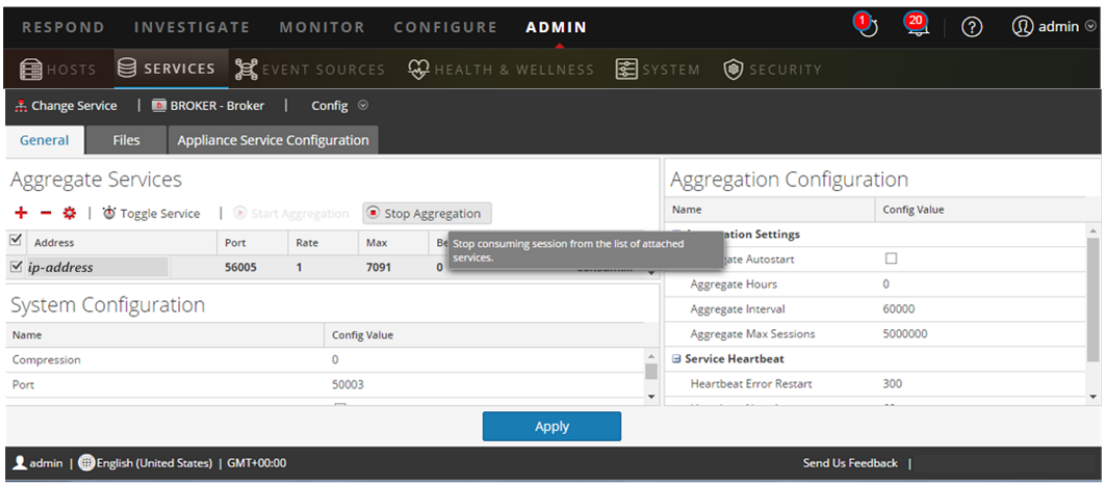
Stop Aggregation

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.

2. Select the **Broker** service.

3. Under (actions), select **View** > **Config**.

4. The **General** tab is displayed.



5. Under **Aggregated Services** click

.

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.0.0.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Log Capture

To start log capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Aggregation

To start aggregation:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. For each Concentrator and Broker service.
   a. Select the service.
   b. Under (actions), select **View** > **Config**.
   c. In the toolbar, click .

Appendix C. Using iDRAC

Many customers have remote sites with limited physical access and limited bandwidth from the administrator's desktop. If this the case, you may want to use iDRAC with the ISO Image shared out from an NFS share that is local to the devices being upgraded or installed. This also gives you the ability to use an existing NetWitness device as the sharing host.

For example, you have:

- a Concentrator and Decoder at a site in a remote geographic location.
- the bandwidth is relatively low to that site from the administrator's site.
- shipping a USB stick and arranging to have person to go plug it into the boxes while you upgrade is not practical.

In this situation, you can:

1. Install the nfs-utils rpm.
2. Configure the NFS share.
3. Configure iDRAC to connect to that share.
   Make sure that you update your iDRAC firmware Supported Windows and Linux Operating Systems. You do this by downloading and running the Dell Update Packages for supported Windows and Linux operating systems from Dell Support website at http://www.support.dell.com. For more information, see the Dell Update Package User's Guide available on the Dell Support website at http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.
4. Boot to the virtual media that contains the ISO file and continue with the upgrade.

Configure NFS Server - NFS Server config File

1. Install NFS and it’s common utilities using yum.
   ```
   yum install nfs-utils
   ```
2. Configure the NFS service to run at boot.
   ```
   chkconfig nfs on
   ```
3. Configure the rpcbind service to run at boot.
   This service is required by NFS and must be running before NFS can be started.
   ```
   chkconfig rpcbind on
   ```

4. Start the rpcbind service.
   `service rpcbind start`
5. Start the NFS service.
   `service nfs start`
6. Create a directory for our first export.
   `mkdir /exports/files`
7. Open the NFS exports file into a text editor.
   `vi /etc/exports`
8. To export the directory to everyone with read-only access, add the following line.
   `/exports/files *(ro)`
9. Save your changes and exit the editor.
   `:wq!`
10. Export the directory defined above.
    `exportfs -a`
11. Disable firewall rules while performing upgrades.
    `service iptables stop`
12. Copy install media that contains the ISO file to `/exports/files` directory.

Boot iDRAC to NFS Configuration

Note: You must verify idrac firmware is at least 1.57.57 for Series 4 (R620).

1. Log into iDRAC interface.
2. Attach media via Remote File Share.
   `<server ip>:/export/files/11.1.0.0.iso`
   For example: `10.10.10.10:/exports/files/rsa-11.1.0.0.1948.el7-usb.iso`
3. Click **Connect**.
4. Launch **Console**.
5. From **next boot** menu select **Virtual DVD/CD**.
6. Reboot device.

Appendix D. Create External Repository

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. Log in to the web server host.
2. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, `/var/netwitness` is the `web-root`, submit the following command string.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.
6. Unzip the:
   a. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

b. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will appear after you unzip the file.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD

10.6.5.x to 11.1 VirtualHost Upgrade Checklist

RSA NETWITNESS® SUITE

Task	Description	√
Prepare for Upgrade		
1.	Download **RSANW-11.1-VirtUpgradeGde.pdf** from RSA Link and review it. a. Be aware of the unsupported components and services in 11.x. b. Carefully read the sections on Event Stream Analysis (ESA) Upgrade Considerations and Investigate in Mixed Mode. c. Review the new required ports .	
2.	Be aware of the hardware, deployments, services, and features not supported in 11.1.	
3.	Perform the upgrade preparation tasks for the features you use. **Caution:** Make sure that you implement and test the new ports so that upgrade does not fail due to missing ports.	
4.	Create CentOS 6 external host to save backup tar files.	
5.	Download the `nw-backup-v4.0.zip` file from RSA Link (https://community.rsa.com/docs/DOC-81514) an extract the files to an external host.	
6.	Execute `get-all-systems.sh` and `ssh-propagate.sh` script from external host.	
7.	Preserve a copy of the `get-all-systems-master` file for future reference.	
8.	Execute `nw-backup.sh` in `TEST` mode to evaluate the space requirements from external host (for example: `nw-backup -t -l -D`).	
9.	Review the back up options for `nw-backup.sh` by displaying the help menu (`nw-backup.sh -h`) .	

Task	Description	√
Migrate Disk Drives		
10.	Back up data in 10.6.5.x virtual machines (VMs).	
11.	Download 11.1 OVA from RSA Link.	
12.	Deploy the same 10.6.5.x VM stack in 11.1.	
13.	Power off both 10.6.5 VM and 11.1 VM .	
14.	Copy VMDK files from the 10.6.5 and add them to 11.1 OVA deployed in step 12.	
15.	Retain the MAC Address of upgraded SA Server VM.	
16.	Remove 10.6.5 VM from inventory (Do not delete the VM).	
17.	Power on 11.1 VM.	
18.	Mount the file system from VMDK.	
19.	Restore Backup data in 10.6.5.x to 11.1 VMs.	
Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts		
20.	Update the contents of the `all-systems` so they consist of SA, ESA's, MA and Broker/Concentrator backup data.	
21.	Reset the Mongo Database admin password to 'netwitness' if it contains special characters .	
22.	Execute `nw-backup.sh` with `-u` flag for all Phase 1 hosts and confirm that it completes with no errors.	
23.	If your environment has multiple ESA appliances, designate a primary ESA (Where the Context Hub service is running) and copy `mongodb.tar.gz.*` files from the secondary ESAs to designated primary ESA default backup path.	
24.	Confirm that backup tar files are saved locally and remotely.	
25.	Set up the 10.6.5.x SA Server host to 11.1 NW Server host by running the `nwsetup-tui` program on the host.	
26.	Install the ESA, Malware Analysis, and Broker or Concentrator services in the NetWitness 11.1 User Interface.	

Task	Description	√
Phase 2 - Upgrade All Other Hosts		
27.	Update the contents of the `all-systems` so they consist of Phase 2 host backup data.	
28.	Execute `nw-backup.sh` in `TEST` mode to evaluate the space requirements from external host (for example: `nw-backup -t -l -D`).	
29.	Execute `nw-backup.sh` with `-u` flag for all Phase 2 hosts and confirm that it completes with no errors.	
30.	Confirm that backup tar files are saved locally and remotely.	
31.	Set up the all othe hosts host to 11.1 NW Server host by running the `nwsetup-tui` program on the host.	
32.	Install the host service in the NetWitness 11.1 User Interface:	
Preform Post Upgrade Adjustments		
33.	Perform the post upgrade tasks for the features you use.	

Revision History

Revision	Date	Description	Author
1.0	20-Apr-18	General Availability(GA)	IDD

RSA NETWITNESS® SUITE

AWS Upgrade Guide

Incomplete Preliminary Review Draft - Do Not Distribute

for Version 11.1.0.0

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **9**

CentOS6 to CentOS7 Upgrade 9

RSA NetWitness® Suite 11.1 Upgrade Path 10

Hardware, Deployments, Services, and Features Not Supported in 11.1 10

Event Stream Analysis (ESA) Upgrade Considerations 10

User Attribute and Role Changes Affecting Investigate 11

Contact Customer Support 12

Upgrade Preparation Tasks **13**

Global 13

Task 1 - Review Core Ports and Open Firewall Ports 13

Task 2 - Record Your 10.6.5.x admin user Password 14

Task 3 - Create a Backup of /etc/fstab File 14

Reporting Engine 14

(Conditional) Task 4 - Unlink External Storage 14

Respond and Incident Management 15

(Conditional) Task 5 – Disable Incident Management Data Retention 15

Backup Instructions **16**

Task 1 - Set up an External Host for Backing up Files 17

Task 2 - Create a List of Hosts to Back up 19

Troubleshooting Information 20

Task 3 - Set up Authentication Between Backup and Target Hosts 22

Task 4 - Check for Backup Requirements for Specific Types of Hosts 22

For All Host Types 22

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation 23

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh 23

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords 25

For Bluecoat Event Sources 25

Task 5 - Check for Adequate Space for the Backup 25

Task 6 - Back up Your Host Systems 26

Post Backup Tasks 29

Task 1 - Save a Copy of the all-systems File and the Backup Tar files 29
Task 2 - Ensure Required Backup Files Were Generated 29
Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host 30
Task 4 - Ensure All Required Backup Files are on Each Host 30

Migrate Disk Drives from 10.6.5.x to 11.1 33

Task 1 - Backup the 10.6.5.x EC2 appliance 33
(Optional)Task 2 - Run the backup script to take backup data of 10.6.5.x instance 34
Task 3 - Stop the instances and detach volumes from 10.6.5.x instances 35
Task 4 - Note the IP addresses of 10.6.5.x instances and then terminate the EC2 instances 37
Task 5 - (IP retention) Create 11.1 instances using 11.1 AMI. 37
Task 6 - Attach volumes to the corresponding 11.1 instance 38
Task 7 - Restore backup data in 10.6.5.x to 11.1 Instances (Data Restoration) 39
Task 8 Run nwsetup-tui script. 41

Set Up Virtual Hosts in 11.1 42

Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts 42
Task 1 - Set Up 11.1 NetWitness Server 42
Task 2 - Setup 11.1 ESA 42
Task 3 - Set Up 11.1 Malware Analysis 42
Task 4 - Set Up 11.1 Broker or Concentrator 43
Phase 2 - Set Up The Rest of the Component Hosts 43
Decoder and Concentrator Hosts 43
Log Decoder Host 43
Virtual Log Collector Host 43
Set Up 11.1 NW Server Host 45
Set Up 11.1 Non-NW Server Host 50

Update or Install Legacy Windows Collection 55

Post Upgrade Tasks 56

Global Tasks 56
Task 1 - Remove Backup-Related Files from Host Local Directories 56
Task 2 - Restore NTP Servers 57
Task 3 - Restore Licenses for Environments without FlexNet Operations-On Demand Access 57

(Conditional) Task 5 - If You Disabled Standard Firewall Config - Add Custom IPtables 57
(Conditional) Task 6 - Specify SSL Ports If You Never Set Up Trusted Connections 58
NetWitness Endpoint 59
Task 7 - Reconfigure Endpoint Alerts Via Message Bus 59
Event Stream Analysis Tasks (ESA) 60
Task 8 - Reconfigure Automated Threat Detection for ESA 60
Task 9 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL 60
Task 10 - Enable Threat - Malware Indicators Dashboard 61
Log Collection 61
Task 11 - Reset Stable System Values for Log Collector after Upgrade 61
(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 12 - Enable FIPS Mode 62
Reporting Engine 62
Task 13 - Restore the CA certificates for External Syslog Servers for Reporting Engine .. 62
(Conditional) Task 14 - Restore External Storage for Reporting Engine 63
Respond 63
Task 15 - Restore Respond Service Custom Keys 63
Task 16 - Restore Customized Respond Service Normalization Scripts 64
(Conditional) Task 17 - Enable Disabled 10.6.5.x Incident Management Data Retention .64
(Conditional) Task 18 - Restore Custom Analysts Roles 65
NetWitness SecOps Manager 65
Task 19 -Reconfigure NW SecOps Manager Integration 65
Security 65
Task 20 - Migrate Active Directory (AD) 65
Task 21 - Modify Migrated AD Configuration to Upload Certificate 65
Task 22. Address Authentication Failure in 11.1 66
Task 23 - Reconfigure Pluggable Authentication Module (PAM) in 11.1 66

Appendix A. Troubleshooting 67

11.1 Setup Program (nwsetup-tui) 68
Backup (nw-backup script) 69
Event Stream Analysis 69
General 70
Log Collector Service (nwlogcollector) 71
NW Server 73
Reporting Engine Service 73

Appendix B. Stopping and Restarting Data Capture and Aggregation ... 74

Stop Data Capture and Aggregation ... 74

Start Data Capture and Aggregation ... 75

Revision History ... 77

Introduction

The instructions in this guide apply to the upgrade of AWS for RSA NetWitness Suite 10.6.5.x to 11.1.0.0 exclusively. See the *RSA NetWitness Suite Physical Host Upgrade Guide* for instructions on how to upgrade your 10.6.5.x physical hosts to 11.1. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents. This document assumes that the appliances are in AWS cloud.

NetWitness Suite 11.1 is a major release that affects all products in the NetWitness Suite suite. The components of the suite are the NetWitness Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Entity Behavior Analytics, Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, and Workbench.

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.1 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.1 platform environment has been improved greatly to accommodate current and future physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Suite 11.1 Upgrade Path

The supported Upgrade path for RSA NetWitness® Suite 11.1 is Security Analytics 10.6.5.x. If you are running a version of NetWitness Suite that is prior to 10.6.5.x, you must update to 10.6.5.x before you can upgrade to 11.1. See the *RSA Security Analytics 10.6.5 Update Guide* on RSA Link.

Caution: There is a known issue if you have Active Directory users configured in 10.6.5.x. You have two options to address this issue:
• Apply the 10.6.4.2 patch before you back up your data for the 11.1 upgrade.

Note: If you are updating from 11.0 to 11.1, see to the *Update Guide for Version 11.01 to 11.1* on RSA link.

Hardware, Deployments, Services, and Features Not Supported in 11.1

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.1.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.0.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.1, your custom policy is not present. In its place, there is the out-of-the-box Context hub Server Monitoring Policy in the user interface, which is specific for version 11.1.
- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Suite 11.1, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.0, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.4.x has been removed.

Caution: If you do not use Incident Management in 10.6.4.x, carefully consider whether or not to upgrade to version 11.0.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.1.

In your 10.6.4.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.0.
- Multiple ESA hosts configured to use Incident Management – The system will continue to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.4.x, you can upgrade to version 11.0.
- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.0.

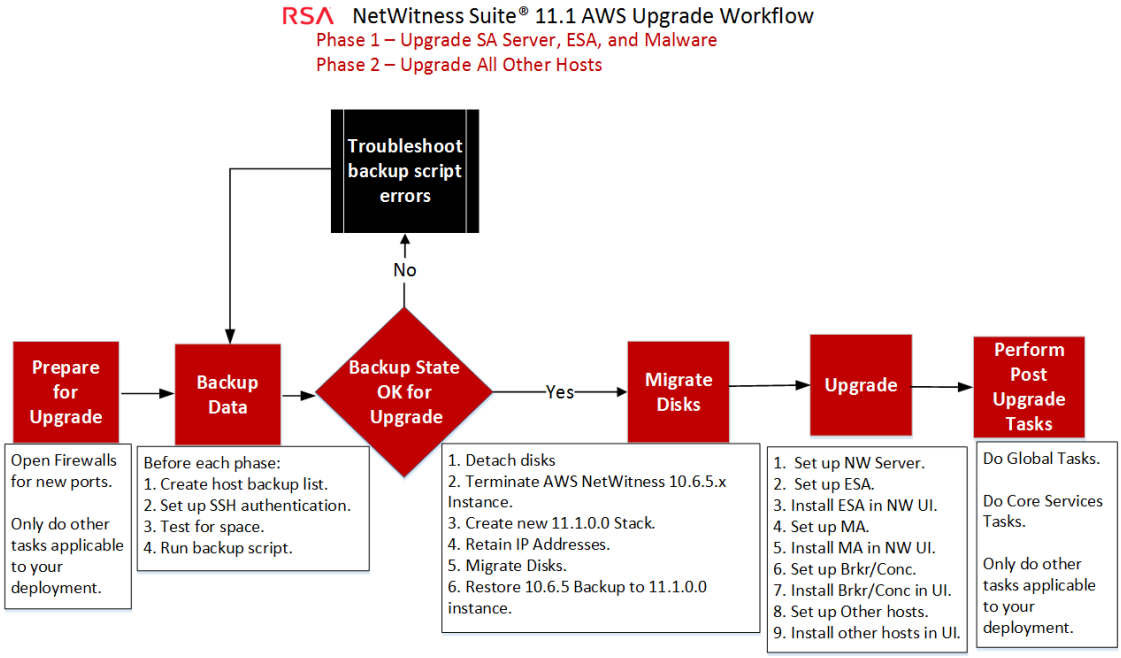
Note: If you did not use Incident Management in 10.6.4.x, you cannot view the 10.6.4.x ESA alerts in the 11.0 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.0 that will allow Respond to view them. See the *ESA Alert Migration Instructions for 10.6.4.x to 11.0* knowledge base article (https://community.rsa.com/docs/DOC-81680) in RSA Link for instructions on how to run this script.

User Attribute and Role Changes Affecting Investigate

The following changes affect how NetWitness Suite 11.1 handles user and role attributes in the Investigate component.

- User Attributes
  When you upgrade to 11.1, the user attributes (query prefix, session timeout, and query threshold) available in SA 10.6.5.x no longer exist. The same attributes are available at the role level for use.
- User and Role Attributes (Query Prefix) is not applicable to Investigate Event Analysis. The user and role attributes, most importantly the query prefix, do not apply to the new Investigate Event Analysis. Any user can modify the URL in browser to access data that should be

restricted from viewing even when query prefix is applied.



Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Suite 11.1.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.1. These tasks are organized by the following categories.

- Global
- Reporting Engine
- Respond and Incident Management

Global

You must complete these tasks regardless of how you deploy NetWitness Suite and which components you use.

Task 1 - Review Core Ports and Open Firewall Ports

The following table lists new ports in 11.1.

Caution: Make sure that the new ports are implemented and tested before upgrading so that upgrade does not fail due to missing ports.

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 27017	MongoDB

ESA Host

Source Host	Destination Host	Destination Ports	Comments
NW Server, NW Endpoint, ESA Secondary	ESA Primary	TCP 27017	MongoDB

All NetWitness Suite core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® Suite Deployment Guide* in case you need to reconfigure NetWitness Suite services and firewalls. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 2 - Record Your 10.6.5.x `admin user` Password

Record your 10.6.5.x `admin user` password. You will need it to complete the upgrade.

Task 3 - Create a Backup of `/etc/fstab` File

Copy the `/etc/fstab` file from all VMs to your local machine (backup host or remote machine).

Note: You need this file to restore a VM with external storage mounts.

Reporting Engine

(Conditional) Task 4 - Unlink External Storage

If the Reporting Engine has external storage [such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports] you must perform the following steps to unlink the storage.

In these steps:

- `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
- `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.
2. Stop the Reporting Engine service.
   ```
   stop rsasoc_re
   ```
3. Switch to `rsasoc` user.
   ```
   su rsasoc
   ```
4. Change to the Reporting Engine the home directory.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. Unlink the `resultstore` directory mounted to external storage.
   ```
   unlink /externalStorage/resultstore
   ```
6. Unlink the `formattedReports` directory mounted to external storage.
   ```
   unlink /externalStorage/formattedReports
   ```

Respond and Incident Management

(Conditional) Task 5 – Disable Incident Management Data Retention

Complete the following procedure to disable Incident Management data retention jobs in 10.6.5.x

1. Log in to RSA Security Analytics 10.6..x.
2. Go to **Incident Management** > **Configure** > **Retention Scheduler**.
3. Uncheck the **Enable data retention scheduler** checkbox and click **Apply**.

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from 10.6.5.x releases to 11.1.0.0.

Note: It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.1.0.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types

Caution: 1) These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the NetWitness Server
- Standalone Warehouse Connector

2) There is a known issue if you have Active Directory users configured in 10.6.5.x. You have two options to address this issue:
• Apply the 10.6.5.2 patch before you back up your data for the 11.1 upgrade.
• If you failed to apply the 10.6.5.2 patch, you can apply the 11.0.0.1 patch immediately after you upgrade to 11.1.

The following types of hosts can be backed up and are automatically restored during the upgrade process:

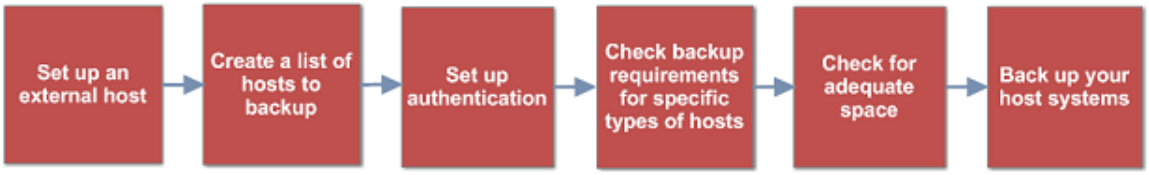
- **NetWitness Server** (may include Malware Analysis, NetWitness Respond, Health and Wellness, and Reporting Engine)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and NetWitness Respond database)
- **Concentrator**
- **Log Decoder**
- **Packet Decoder**
- **Virtual Log Collector**

The following types of files are automatically backed up but must be restored manually after the upgrade process:

- PAM configuration files: For information about restoring the PAM configuration files, refer to "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.1.0.0", in the "Global" section of the Post Upgrade Tasks.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of Post Upgrade Tasks.

Note: If you have problems during the backup or upgrade processes and you lose data, you can recover the data and start the process again. For information about recovering lost data, see "Recover Data After System Failure" in the *System Maintenance Guide*.

The following diagram shows the high-level task flow of the steps you perform to back up your hosts.



The following sections describe each of these tasks:

- Task 1 - Set up an External Host for Backing up Files
- Task 2 - Create a List of Hosts to Back up
- Task 3 - Set up Authentication Between Backup and Target Hosts
- Task 4 - Check for Backup Requirements for Specific Types of Hosts
- Task 5 - Check for Adequate Space for the Backup
- Task 6 - Back up Your Host Systems
- Post Backup Tasks

Task 1 - Set up an External Host for Backing up Files

You must set up an external host to use for backing up files. The host must be running Centos 6 with connectivity through SSH to the NetWitness Suite stack of hosts.

Ensure that the host names for the systems to be backed up are resolvable on the backup host machine, either by DNS or listed in the `/etc/hosts` file.

Note: These scripts are designed to run on CentOS 6 only. You must execute these scripts on CentOS 6 machines.

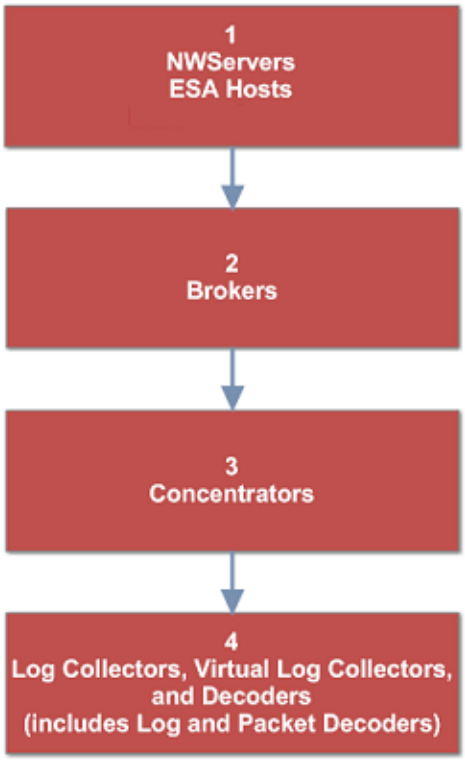
There are several scripts that you run during the backup process.You must download the zip file that contains the scripts `(nw-backup-v4.0.sh)` from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your NetWitness Servers and host systems to be backed up.
- `ssh-propagate.sh`: Automates sharing keys between the systems you are backing up and the backup host system so that you are not prompted for passwords multiple times.
- `nw-backup.sh`: Performs the backup of your hosts.

Note: The backup scripts do not support backing up data for STIG-hardened hosts.

Task 2 - Create a List of Hosts to Back up

The script that you use to back up your files depends on the `all-systems` and `all-systems-master-copy` files, which contain a list of the hosts that you want to back up. The `all-systems-master-copy` file contains a list of all your hosts. The `all-systems` file is used for each backup session, and contains only those hosts which are being backed up for a particular session. You run the `get-all-systems.sh` script to generate these files. RSA recommends that you back up your hosts in groups, and not all at once. The recommended order and grouping of hosts for backup sessions is shown in the following diagram:



Limit each backup session to five hosts to ensure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference and then manually editing the `all-systems` file to contain specific hosts.

To generate the `all-systems` and the `all-systems-master-copy` files:

1. From the host on which you are running the backup process, make the `get-all-systems.sh` script executable by running the following command:
   ```
   chmod u+x get-all-systems.sh
   ```
2. At the root level, run the `get-all-systems.sh` script:
   ```
   ./get-all-systems.sh <IP-Address-of-NetWitness-Admin-Server>
   ```
   You will be prompted for the password for each host system once per host.

This script saves the `all-systems` file and the `all-systems-master-copy` file to `/var/netwitness/database/nw-backup/`.

3. Validate that the `all-systems` and `all-systems-master-copy` files were generated and that they contain the right hosts.
4. Edit the `all-systems` file to contain only the systems you are backing up. You can do this by using the `all-systems-master-copy` file as a reference, and then opening the `all-systems` file in an editor (such as vi) and modifying it to include only the systems you want to back up.

> **Note:** If you use vi, be sure to include the path to the location of the `all-systems` file.

Here is an example of an `all-systems-master-copy` file:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

And here is an example of an `all-systems` file based on the `all-systems-master-copy` file that could be used in the first backup session:

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
```

Troubleshooting Information

- Be sure to save copies of the `all-systems` and `all-systems-master-copy` files in a safe location. Follow these recommendations:

  - Do not edit the `all-systems-master-copy` file.
  - If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure to remove pre-existing entries from the file so that the file contains only those hosts that are currently being backed up.
    For more information, see Post Backup Tasks.

- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.

- The `get-all-systems.sh` script generates a list of hosts that were defined in the NetWitness Suite user interface. Ensure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to NetWitness Suite, you use the NetWitness Suite user interface to ensure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.

- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the NetWitness Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the NetWitness Server. (Any Windows Legacy Collectors or AWS Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)
- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

RSA recommends that you run the `ssh-propagate.sh` script to automate sharing keys between the backup host and the host systems.

Note: If you have SSH keys that are protected with pass phrases, you can use `ssh-agent` to save time. For more information, refer to the man page for `ssh-agent`.

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:
   `chmod u+x ssh-propagate.sh`
2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. You are prompted for the password once per host, but you will not need to enter it repeatedly later during the backup process.

Task 4 - Check for Backup Requirements for Specific Types of Hosts

After you create the `all-systems` file to use for backup, you must check to see if any of the hosts listed in the file have requirements that must be met before you run the backup process.

For All Host Types

Perform the following steps for all host types:

1. On the NetWitness Server, place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directories will be automatically restored during the upgrade process. After upgrading to 11.1.0.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`.
   You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the NetWitness Server and run the following command strings to perform the conversions listed.
   Convert a DER file (.crt .cer .der) to PEM
   `openssl x509 -inform der -in certificate.cer -out certificate.pem`
   Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Note:** Add the following qualifier to the command string to:
> `-nocerts` convert private keys exclusively.
> `-nokeys` convert certificates exclusively.

2. Manually record any custom configurations made to CentOS 6 (for example, driver customizations) for restoration after you update to CentOS 7. Custom configurations to CentOS 6 are not automatically backed up and restored.

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for Decoder, Concentrator, or Broker hosts, stop data capture and aggregation on all the systems that you are backing up. For instructions, refer to Appendix B. Stopping and Restarting Data Capture and Aggregation

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run `prepare-for-migrate.sh`

> **Caution:** This task stops log collection so you must perform this step immediately before you upgrade to minimize the loss of event collection. Complete this task in accordance with the backup and upgrade tasks in this guide.

Prerequisites

You need the following information before you prepare LCs and VLCs for upgrade.

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.
- If you set the password for `logcollector` user for RabbitMQ , you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.
2. Submit the following command string.

   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```

   This command:

- Stops the Puppet Agent service.
- Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.1.0.0.
- Stops all the collection protocols in the Log Collector service.
- Saves the list of Plugin accounts and RabbitMQ accounts.
- Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.
- Waits until the Log Collector queues are empty.
- Stops the Log Collector service.
- Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

The `prepare-for-migrate.sh` script:

- Sends informational, warning, and error messages to the console.
- Saves a session log in the `/var/log/backup/` directory.

You must fix any of the following errors and resume the preparation. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

- Log Collector queues with events but without consumers are found.
- Unable to stop the Puppet Agent service.
- Unable to stop a collection protocol in the Log Collector service.
- Unable to block event publishers to the RabbitMQ server.
- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.
- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the NetWitness Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.1.0.0 upgrade, you can restore RabbitMQ user accounts.

To get a list of RabbitMQ usernames and passwords, run the following command:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

To restore RabbitMQ user accounts, refer to *Task 2 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL* in Post Upgrade Tasks.

For Bluecoat Event Sources

Bluecoat ProxySG event sources use FTPS protocol to upload log files to the Log Collector (LC) and Virtual Log Collector (VLC). The event source documentation contains the steps to configure VSFTPD service on the LC and VLC.

- If key material exists in `/root/vsftpd/` directory in 10.6.5.x, this material area will be backed up and restored. **If the material was in another location, you must back it up and restore it manually.**
- If the `/etc/vsftpd/vsftpd.conf` file exits in 10.6.5.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to ensure that you provide adequate space for the backup so that the backup captures all your data.

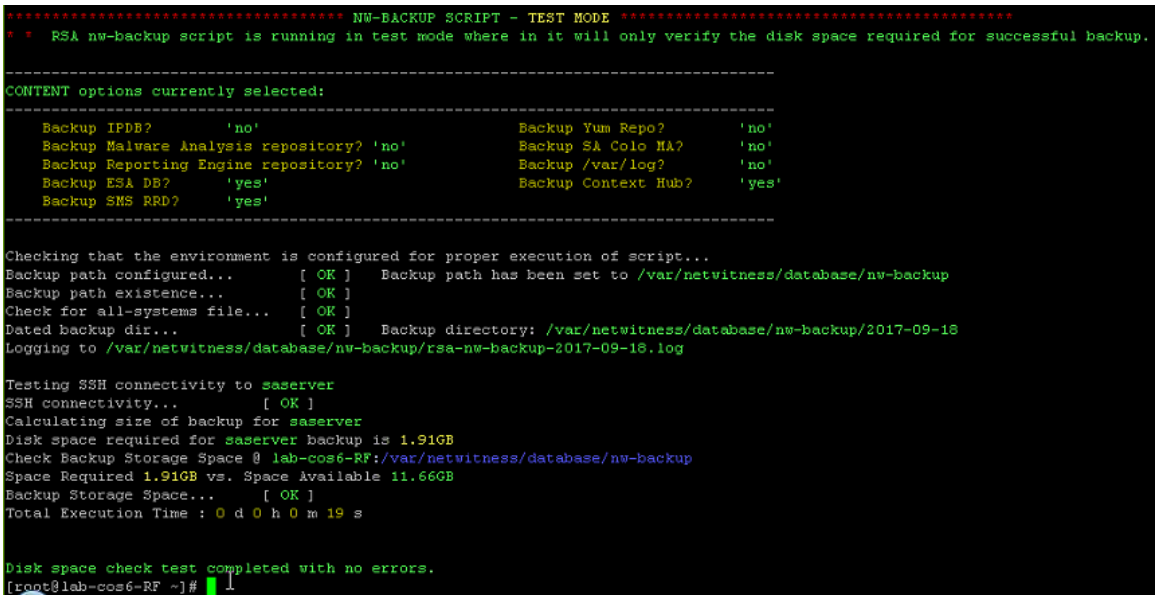
To check for adequate disk space:

1. Make the backup script executable by running the following command:
   ```
   chmod u+x nw-backup.sh
   ```
2. Run the following command at the root directory level:
   ```
   ./nw-backup.sh -t
   ```
   The output displays the amount of disk space that is required for the backup.

   Note: The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-d` option by using `-D`. Using the `-D` option will show how much

space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

The following figure shows an example of the output from using the `-t` option.



Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.1.0.0.

Note: The script will stop services as it runs. However, you can stop services manually before you run the script if needed.

When you run the backup script, you can choose from several options that are described in the following sections.

Usage:
`./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>`

General Options

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)

-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)

-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)

-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)

-x : move all backup files to an external mount point. Default: (no) -COPY

-b <path to write backups> : path to the location for storing backup files on a backup server. **For upgrading to 11.1, please use the default location!** Default: (/var/netwitness/database/nw-backup)

Note: Do **not** change the backup path in upgrade (-u) mode.

Advanced Content Selection Options

-c : back up Colocated Malware Analysis on SA servers. Default: (no)

-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)

-m : back up Malware Analysis File Repository. Default: (no)

-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)

-v : back up system logs (/var/log). Default: (no)

-y : back up YUM Web Server & RPM Repository. Default: (no)

-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)

-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)

-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)

Test Options

-t : performs script test run for disk space check only. Services are not stopped and excludes execution of backup. Can be combined with (-d) or (-D) and other flags. Default: (-t)

For example, the command:
`./nw-backup.sh`
would run the backup with options as set in the Header of the script itself.
OR, the command:
`./nw-backup.sh -ue /mnt/external_backup`
would run a normal backup using the backup path defined in the script, with the following options:

```
-u : enables the upgrade flag to run backup for upgrading to 11.1. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

When you run the script, the following text is displayed at the top of the script:

Caution:
```
RSA nw-backup script backs up configuration files, data, and
logs on the options provided in the script. It tars the content, with
options to store the backup files on the backup server, move or copy
them to external storage on a mount point (USB/NFS/SMB), or SCP them
back to the target host.
This backup script has been qualified on the following versions of
Security Analytics:
10.6.5.x
Use of this script on any other versions of the product may not give
expected results and may not be supported by RSA Customer
Service.Note: All non-RSA custom files, scripts, Cronjobs and other
important files should be placed in /root, /home/'user', OR /etc to be
included in the backup.
```

To run the backup script to back up your hosts:

1. Ensure that the `all-systems` file contains only the hosts to back up. For information, see Task 2 - Create a List of Hosts to Back up.
2. Make the backup script executable by running the following command:
   ```
   chmod u+x nw-backup.sh
   ```
3. Begin the backup process by running the following command at the root directory level:
   ```
   ./nw-backup.sh -u <additional options as needed>
   ```

   Note: You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.1.0.0.

   When the text "`Backup completed with no errors`" is displayed, the backup has completed successfully.

   A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:
   ```
   rsa-nw-backup-2017-03-15.log
   ```
4. When the backup has completed, to ensure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:
   ```
   tar -tzvf hostname-ip-address-backup.tar.gz
   ```
   The following archive files are created:

   For all hosts:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

For NetWitness Servers:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

For ESA Hosts:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

<hostname-IPaddress>-controldata-mongodb.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

The archived files are located in the /var/netwitness/database/nw-backup directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

Post Backup Tasks

Task 1 - Save a Copy of the all-systems File and the Backup Tar files

Make copies of the all-systems file, the all-systems-master-copy file, and the backup tar files and put the copies in a secure location. You cannot regenerate these files after you upgrade the NetWitness Server (specifically the Admin service) to 11.1.0.0.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.1.0.0 upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

The following files are generated on all hosts by the backup scripts:

- all-systems
- all-systems-master-copy

- appliance_info
- service_info
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

In addition to the files listed above, the following files will be generated on NetWitness Server and ESA hosts:

- <*hostname*>-<*host IP address*>-mongodb.tar.gz
- <*hostname*>-<*host IP address*>-mongodb.tar.gz.sha256

The backup script will also generate the following controldata-mongodb.tar.gz files.

Note: The backup script copies the following files from all ESA hosts to the NetWitness Server host's backup path .

- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz
- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256

Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host

If you have multiple ESA host systems in your enterprise, copy the following two files from each ESA host to the /opt/rsa/database/nw-backup/ directory on the Primary ESA host system (the host that has the ContextHub service running on it) :

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Task 4 - Ensure All Required Backup Files are on Each Host

Before you upgrade to 11.1.0.0, ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

Note: The default paths for backup files are:
- NetWitness Server hosts:`/var/netwitness/database/nw-backup`
- ESA hosts:`/opt/rsa/database/nw-backup`
- Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256`

Required Files for ESA Hosts

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Required Files for All Other Hosts

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Note: The following files are located in the `<hostname>-<host-IP-address>-backup.tar.gz` tar on all hosts:
`appliance_info`
`service_info`

Note: The paths to the location of the backup and restore files for iptables, NAT configurations, user accounts, and crontab entries are shown in the following list:
Backup paths:
`BUPATH=/opt/rsa/database/nw-backup` for the ESA Correlation Engine
`BUPATH=/var/lib/rsamalware/nw-backup` for the Malware Service
`BUPATH=/var/netwitness/database/nw-backup` for all other services
Restore locations:
`BUPATH/restore/etc/sysconfig` for Iptable rules
`BUPATH/restore/etc/sysconfig` for NAT configurations
`BUPATH/restore/etc` for Crontab entries
`BUPATH/restore/etc` for User Accounts (users are located in the `passwd` file, and groups are located in the `group` file. These are not restored during the upgrade process but can be restored manually.
`BUPATH/restore/etc/ntp.conf` for NTP configurations (must be restored using the NetWitness Suite UI)

Migrate Disk Drives from 10.6.5.x to 11.1

These instructions tell you how to upgrade virtual hosts from 10.6.5.x to 11.1.

Caution: 1.) Run the backup immediately before you upgrade hosts for each phase so that the data is not out-dated.
2.) This guide applies to AWS host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite 11.0 Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

There are five tasks you must complete to migrate from 10.6.5.x to 11.1:

Task 1 - Backup the 10.6.5.x EC2 appliance

(Optional)Task 2 - Run the backup script to take backup data of 10.6.5.x instance

Task 3 - Stop the instances and detach volumes from 10.6.5.x instances

Task 4 - Note the IP addresses of 10.6.5.x instances and then terminate the EC2 instances

Task 5 - (IP retention) Create 11.1 instances using 11.1 AMI.

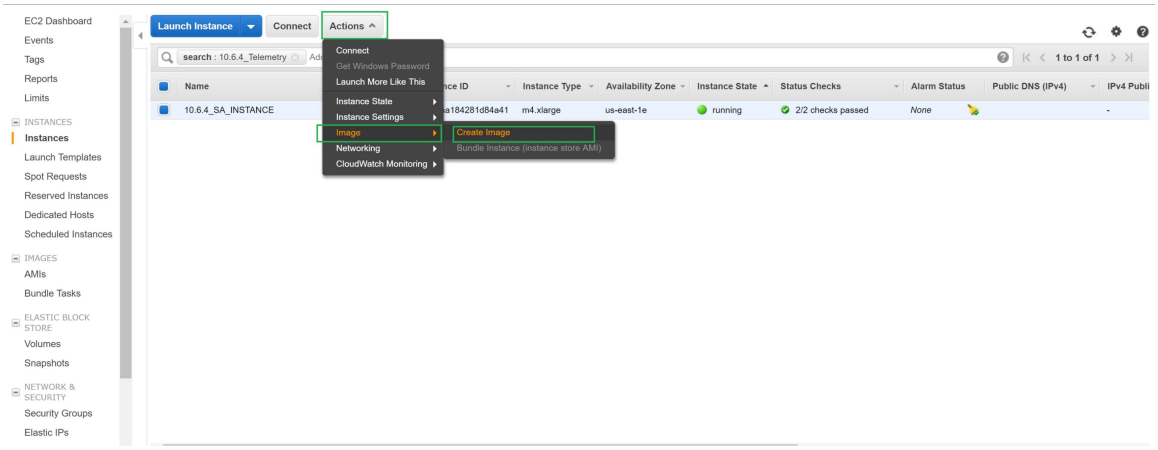
Task 6 - Attach volumes to the corresponding 11.1 instance

Task 7 - Restore backup data in 10.6.5.x to 11.1 Instances (Data Restoration)

Task 8 Run nwsetup-tui script.

Task 1 - Backup the 10.6.5.x EC2 appliance

Select the 10.6.5.x EC2 Instance and navigate to Actions. Click Image and then select Create Image.



(Optional)Task 2 - Run the backup script to take backup data of 10.6.5.x instance

Note: If you have not taken a backup of the 10.6.5.x instance, follow these steps, otherwise skip to Task 3 - Stop the instances and detach volumes from 10.6.5.x instances.

If the stack contains Log Collector then prepare **Log Collector** for the migration:

1. Navigate to `/opt/rsa/nwlogcollector/nwtools/` and run the below command:

```
sh prepare-for-migrate.sh --prepare
```

2. Download backup scripts from GitHub: https://github.rsa.lab.emc.com/asoc/nw-backup (maintenance-11.0) and place it anywhere in a computer running an RPM-based Linux distribution (RHEL or CentOS for example) with a large amount of free hard drive space. In many cases the SA server will suffice. Now, navigate to `scripts` directory inside '`nw-backup-master`' and run the following commands:

```
./get-all-systems.sh <SA server-IP>
```

```
./ssh-propagate.sh <path-to-backup-directory/all-systems>
```

```
./nw-backup.sh -u
```

Its safe to copy a backup of the tar balls created at `/var/netwitness/database`, in some safe location (not mandatory).

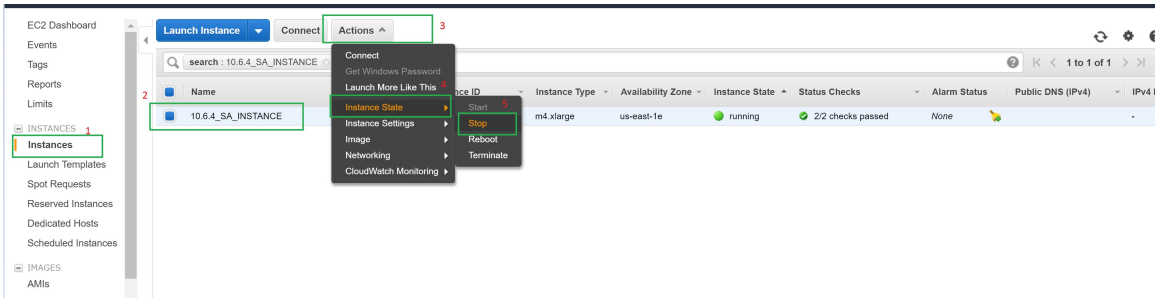
Before starting the restore process, if you have ESA deployment then copy the files `<hostname>-<IP>-controldata-mongodb.tar.gz` & `<hostname>-<IP>-controldata-mongodb.tar.gz.sha256` from the location `/opt/rsa/database/nw-backup` of ESA VM to `/var/netwitness/database/nw-backup/` of SA VM.

```
root@ip-172-24-184-59 ~]# ./nw-backup.sh -u
------------------------------------------------------------------------
Starting execution of NW-BACKUP script in UPGRADE backup mode
------------------------------------------------------------------------
WARNING: For UPGRADE backups, services must be stopped and all externally mounted disks (DACs) must be unmounted.
         If you prefer to stop the services and unmount the external partions manually, exit out of the script by typing
         (CTRL-C) within 30 seconds, otherwise the services will be automatically stopped, all externally mounted
         filesystems will be unmounted, and the script will proceed with the UPGRADE backup process.

NOTE: The easiest way to remount and restart the services on a host is to perform a reboot of the host.

The script will continue in 30 seconds...

--------------------------------------------------------------------------------
OUTPUT options currently selected:
--------------------------------------------------------------------------------
    Path to files on backup system:           '/var/netwitness/database/nw-backup'
    Copy backup files locally to each system?  'yes'
    Performing backup in upgrade mode?         'yes'
--------------------------------------------------------------------------------
CONTENT options currently selected:
--------------------------------------------------------------------------------
    Backup IPDB?          'no'                    Backup Yum Repo?        'no'
    Backup Malware Analysis repository? 'no'      Backup SA Colo MA?      'no'
    Backup Reporting Engine repository? 'yes'     Backup /var/log?        'no'
    Backup ESA DB?        'yes'                   Backup Context Hub?     'yes'
    Backup SMS RRD?       'yes'
--------------------------------------------------------------------------------

Checking that the environment is configured for proper execution of script...
OS Version...                 [ OK ]
Backup path configured...     [ OK ]   Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence...      [ OK ]
Check for all-systems file... [ OK ]
Updated backup dir...         [ OK ]   Backup directory: /var/netwitness/database/nw-backup/2017-12-08
SA Version check ...          [ OK ]

********************** NW-BACKUP SCRIPT - UPGRADE MODE ******************************
******** UPGRADE IS ONLY SUPPORTED FOR SA VERSION 10.6.4.0 AND HIGHER***************** *
*  RSA nw-backup script backs up configuration files, data, and logs based           * *
*  on the options provided in the script.  It tars the content and leaves a          * *
*  copy of tars on the host for consumption by the upgrade process.  It also         * *
*  provides an option to back up the tars to an external mount point (USB/NFS).      * *
*                                                                                    * *
*    NOTE: The following systems and services are NOT supported for restore          * *
*    for the 11.0.0.0 upgrade:                                                       * *
*              - Malware-Analysis (Co-located on SA server)                          * *
*              - IPDB Extractor (Co-located on SA Server & Standalone)               * *
*              - Warehouse Connector (Standalone)                                    * *
*              - All-in-one Servers                                                  * *
*                                                                                    * *
*  Note: All non-RSA custom files, scripts, Cronjobs and other important files       * *
*  should be placed in /root, /home/'user', OR /etc to be included in the backup.    * *
************************************************************************************ *
**************************************************************************************
```

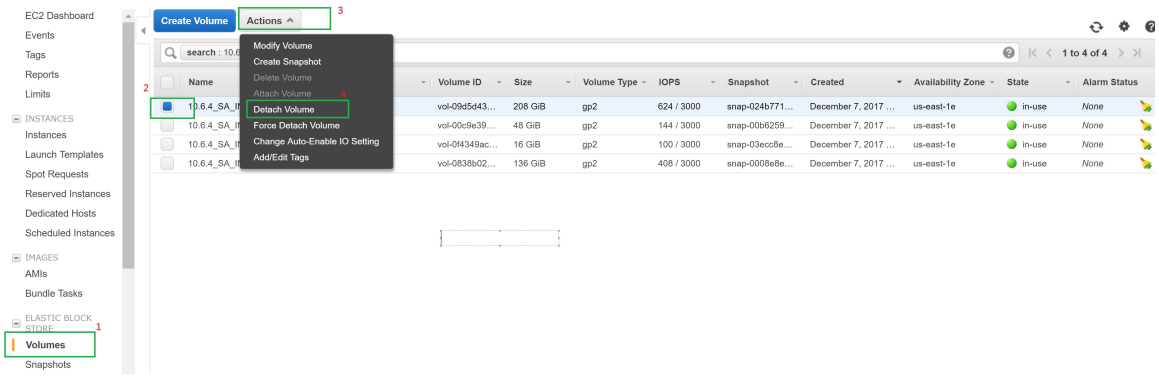
Task 3 - Stop the instances and detach volumes from 10.6.5.x instances

Note: If detach fails, do a forced detach on the volume.

Select the 10.6.5.x EC2 instance and navigate to Actions and then click Stop.



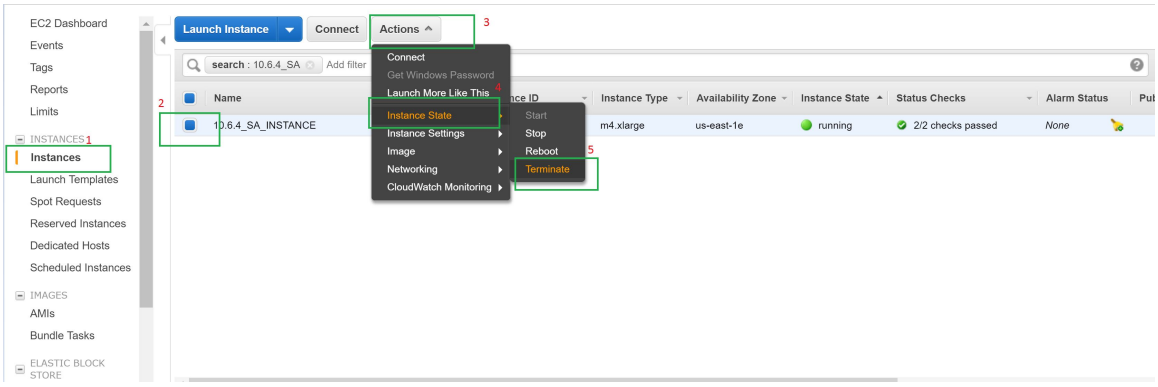
Click on Volumes and then select the 10.6.5.x instance volumes to detach Actions and then select Detach Volume.


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Create Volume
Actions
Modify Volume
Create Snapshot
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Change Auto-Enable IO Setting
Add/Edit Tags
1 to 4 of 4
Name
Volume ID
Size
Volume Type
IOPS
Snapshot
Created
Availability Zone
State
Alarm Status
vol-09d5d43...
208 GiB
gp2
624 / 3000
snap-024b771...
December 7, 2017 ...
us-east-1e
in-use
None
vol-00c9e39...
48 GiB
gp2
144 / 3000
snap-00b6259...
vol-0f4349ac...
16 GiB
100 / 3000
snap-03ecc8e...
vol-0838b02...
136 GiB
408 / 3000
snap-0008e8e...

Task 4 - Note the IP addresses of 10.6.5.x instances and then terminate the EC2 instances

Note: Termination is required to free the IP address.

1. Click on Instances and then select the Instance.
2. Click Actions and navigate to Instance State.
3. Click Terminate

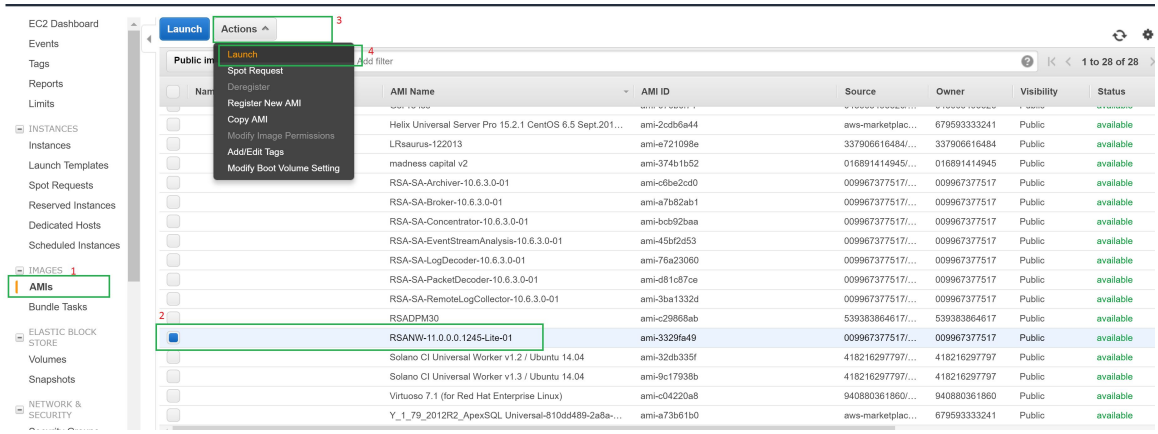


Task 5 - (IP retention) Create 11.1 instances using 11.1 AMI.

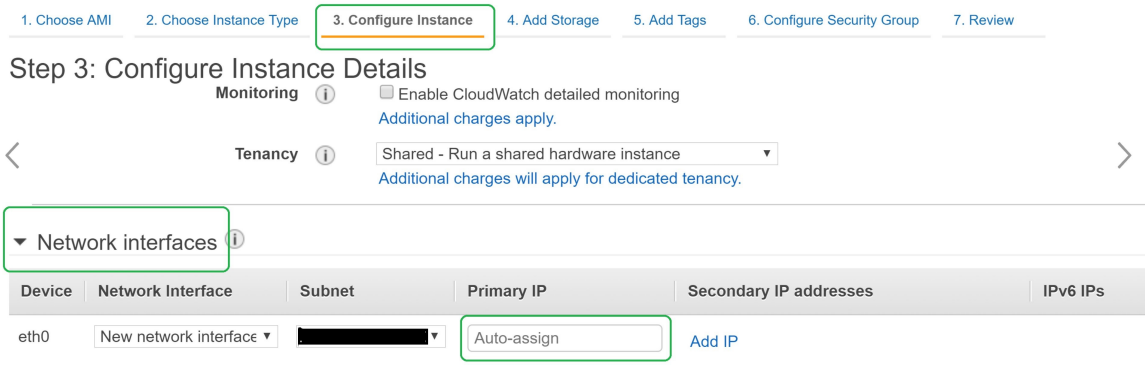
1. During the creation of EC2 instance, provide the IP address from task4. Click on AMIs and select 11.0 AMI.

Note: Refer to the *AWS Deployment Guide for version 11.0* for installing RSA NetWitness Suite11.0.0.0

2. Click Actions and then click Launch.



3. Assign the retained IP for the appropriate instances (IP retention). For example, If 10.6.1.xSA instance IP is 172.24.184.63 . Then assign the same IP(172.24.184.63) for 11.1 Instance.



Note: To deploy components other than NW, select the image(RSANW-11.0.0.0.1245-Lite-01) which is available under community AMIs section.

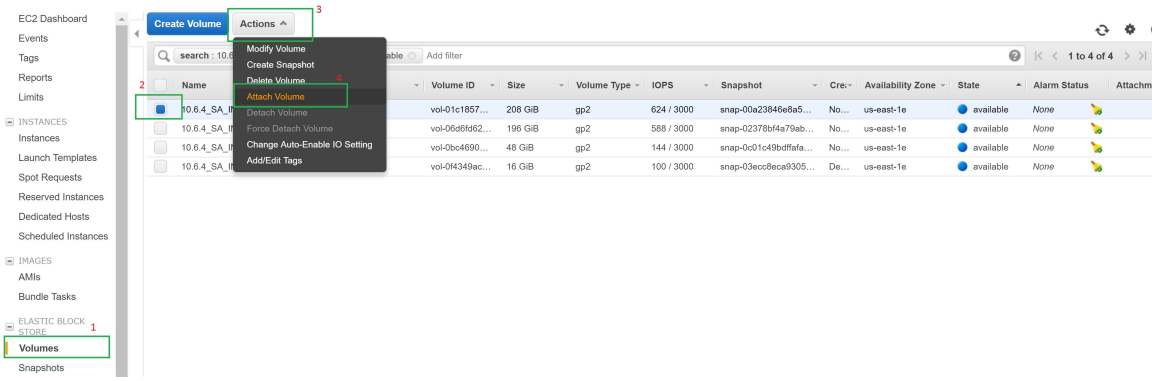
Task 6 - Attach volumes to the corresponding 11.1 instance

After NW 11.1 instance is deployed, stop the 11.0 instance and attach the available 10.6.1.x volumes (except the 'OS disk') to 11.1 instances.

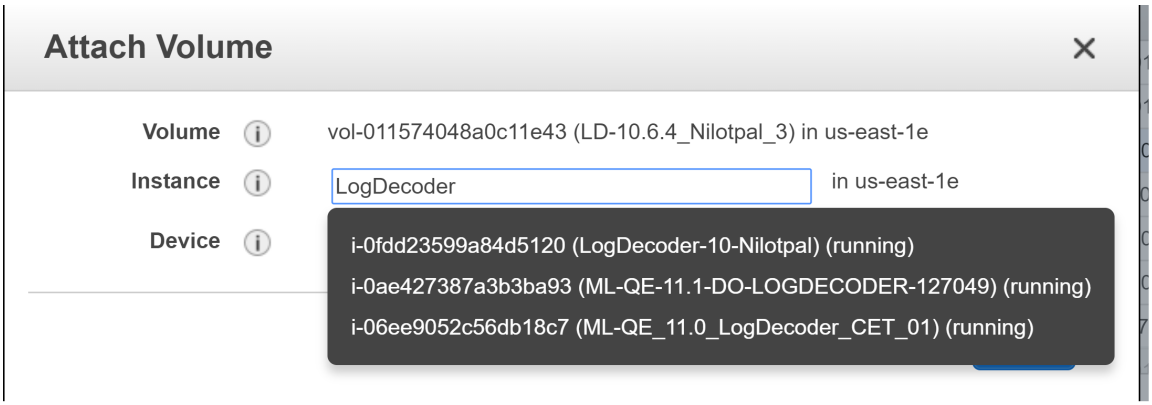
1. Click on Volumes.

2. Select the 10.6.5.x instance volume to attach.

3. Click Actions and then select Attach Volume.



4. Enter the 11.1 instance ID to which the volume has to be attached.



5. Power ON all the 11.1 instances once all the disks are attached.

Task 7 - Restore backup data in 10.6.5.x to 11.1 Instances (Data Restoration)

Execute the following steps for copying the backup data on SA, LD/LC, PD, Concentrator, Archiver, Broker:

1. Create a directory under `/tmp/` by the name `nwhome`.
2. Mount `VolGroup00-nwhome` on `/tmp/nwhome/` and make sure `/var/netwitness/database/` directory is present.

```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

3. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`.
4. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`

```
umount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

Follow these steps for **ESA**:

1. Create a directory under `/tmp/` by the name `apps`.
2. Mount `VolGroup01-apps` temporarily on `/tmp/apps/`

```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
```

3. Copy nw-backup directory from here to `/var/netwitness`

```
cp -r /tmp/apps/database/nw-backup /var/netwitness
```

4. Unmount VolGroup01-apps from `/tmp/apps/`

umount /tmp/apps

5. Add the following entries in `/etc/fstab` for `mounts`:(Disk Mounting) and then run mount -a

For SA:

/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs defaults,noatime,nosuid 1 2

For LogDecoder/LogCollector:

/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4 defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb xfs defaults,noatime,nosuid 1 2

For PacketDecoder:

dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4 defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb xfs defaults,noatime,nosuid 1 2

For Concentrator:

/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4 defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime 1 2

/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb xfs defaults,noatime,nosuid 1 2

For Archiver:

/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs defaults,nosuid,noatime 1 2

/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs defaults,nosuid,noatime 1 2

For Broker:

/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs defaults,nosuid,noatime 1 2

6. Then run mount command

   ```
   mount -a
   ```

Task 8 Run nwsetup-tui script.

Note: Please provide appropriate host names for all the 11.1 instances after launching. (for 10.6.5.x instance names refer all-systems-master-copy file, which contains 10.6.5.x instance names with IP address)

Execute the command to set the hostname: `hostnamectl set-hostname <hostname>`

Login to SA Sever CLI and run `nwsetup-tui` script for rest of the process completion.

Run 'nwsetup-cli' on rest of the components for Bootstrap and Orchestration. For more information, refer to the Set Up Virtual Hosts in 11.1 section.

Set Up Virtual Hosts in 11.1

There two phases to set up your 11.1 virtual stack that you must complete in the order shown.

- Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

  Note: For Event Stream Analysis, if you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.5 and they will not be available until the warm up completes.

- Phase 2 - Set Up The Rest of the Component Hosts

Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

Task 1 - Set Up 11.1 NetWitness Server

Follow the instructions under Set Up 11.1 NW Server Host.

Task 2 - Setup 11.1 ESA

Caution: If you had C2 modules enabled in 10.6.4.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.0 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.1 Non-NW Server Host to set up your ESA hosts.

1. Set up your primary ESA host through the Setup program and install **ESA Primary** on the host in the user interface on the **Admin Hosts** view.

   Note: If you have multiple ESA hosts in your enterprise, you must upgrade the ESA Primary host, where all the `mongodb` (Mongo Database) backup tar files are located, first, before you upgrade ESA Secondary hosts.

2. (Conditional) If you have a secondary ESA host, set it up through the Setup program and install **ESA Secondary** on the host in the user interface on the **Admin Hosts** view.

Task 3 - Set Up 11.1 Malware Analysis

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Task 4 - Set Up 11.1 Broker or Concentrator

Follow the instructions under Set Up 11.0 Non-NW Server Host.

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Set Up The Rest of the Component Hosts

See Appendix B. Stopping and Restarting Data Capture and Aggregation for instructions on how to stop and restart data capture and aggregation when upgrading the Decoder, Concentrator, and Log Collection hosts.

Decoder and Concentrator Hosts

1. Stop data capture and aggregation.
2. Complete the steps in Set Up 11.1 Non-NW Server Host.
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the *Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh* in the **Backup Instructions**.
2. Stop data capture on the Log Decoder.
3. Complete the steps in Set Up 11.1 Non-NW Server Host.
4. Restart data capture on Log Decoder.

Note: After you upgrade, you will restart log collection after completing the Task 11 - Reset Stable System Values for Log Collector after Upgrade in the **Post Upgrade Tasks**

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described in the *Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh*.
2. Back up your 10.6.5.x VLC by editing the `all-systems` file on host where you performed the backup.
   a. Make sure your `all-systems` file contents has this information before you perform this step.
   `vlc,<host-name>,<IP-address>,<UUID>,10.6.5.0`

b. Run the following command to create backup.

```
./nw-backup.sh -u
```

See Backup Instructions for detailed procedures on how to back up the host.

3. Make sure the backup host contains the VLC backup in the following format.

```
<hostname>-<IPaddress>-root.tar.gz
<hostname>-<IPaddress>-root.tar.gz.sha256
<hostname>-<IPaddress>-backup.tar.gz
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```

4. Power off the 10.6.5.x VLC so that a new 11.1 VM can be created with the same network configuration.
5. Deploy a fresh Non-NW Server host using the 11.0 NetWitness Suite ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.5.x VLC.
This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.5.x VLC backup file.

Note: Make sure IPv6 is disabled.

a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings. Contents of `ifcfg-eth0` should be as follows.

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. Submit the following command string.

```
systemctl restart network.service
```

8. Create the backup directory.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new VLC in the `/var/netwitness/database/nw-backup` directory.
10. Complete the steps 2 through 12 inclusive in Set Up 11.1 Non-SA Server Host for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

Set Up 11.1 NW Server Host

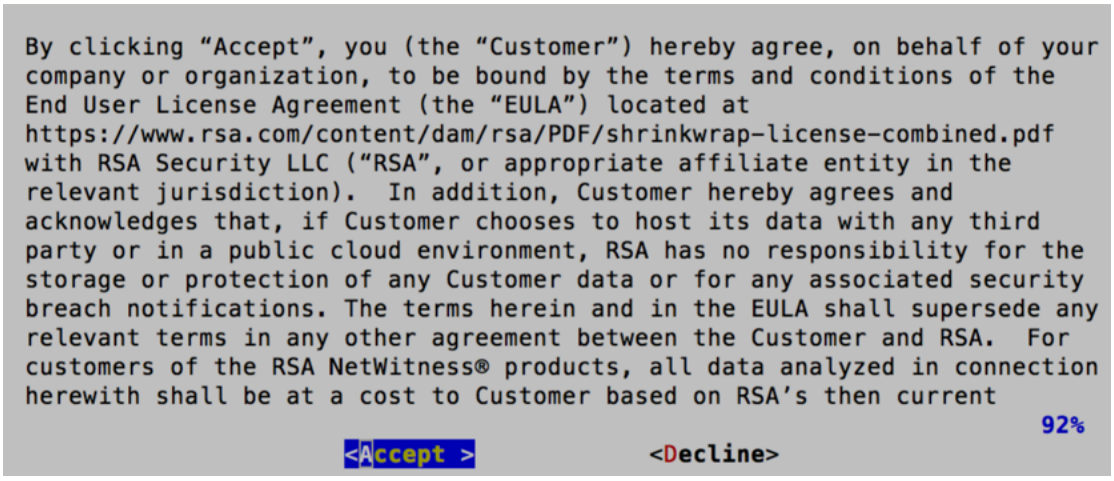
Make sure that you have backed up 10.6.5.x data for the SA Server host. **You must follow the instructions in** Backup Instructions **to back up the host.**

Caution: Run the backup immediately before upgrading the SA Server to 11.1 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.1.

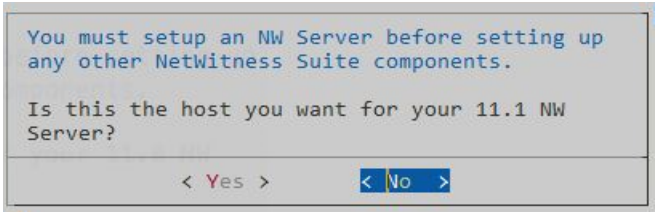
Complete the following steps to set up the 11.1 NW Server host.

1. Power on the NW Server VM and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

   Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press the Enter key to register your command response and move to the next prompt.
   2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

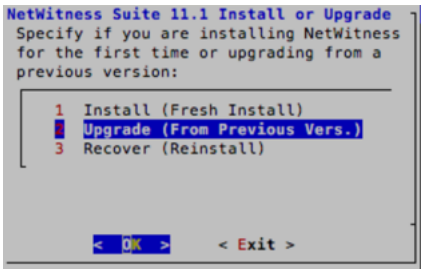


Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

3. Tab to **Yes** and press **Enter**.

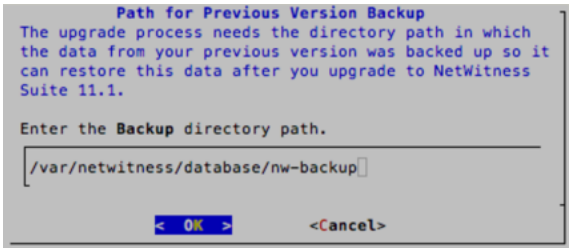
   Choose No if you already upgraded the NW Server to 11.1.

   The Install or Upgrade prompt is displayed.



4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.

   The backup path prompt is displayed.



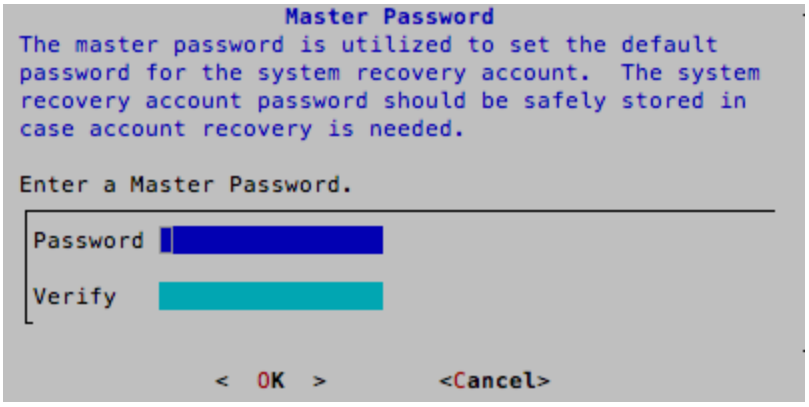
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.

   The Master Password prompt is displayed.

   The following list of characters are supported for Master Password and Deployment Password:

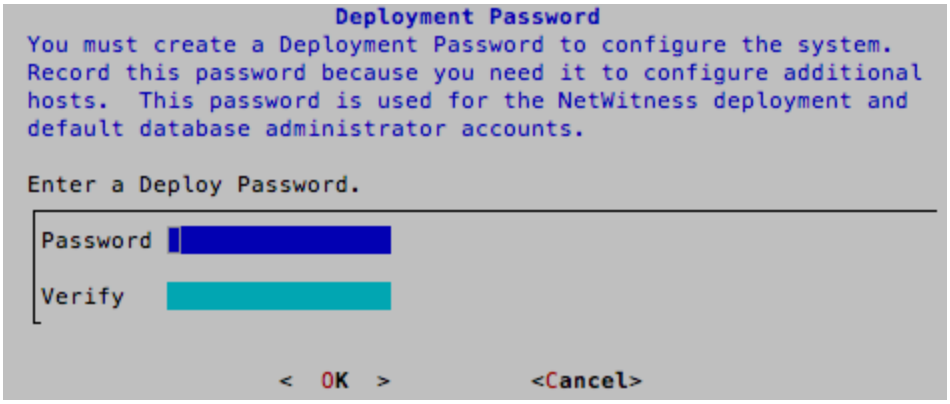
   - Symbols : ! @ # % ^ + ,
   - Numbers :0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z

No ambiguous characters are supported for Master Password and Deployment Password (for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -.



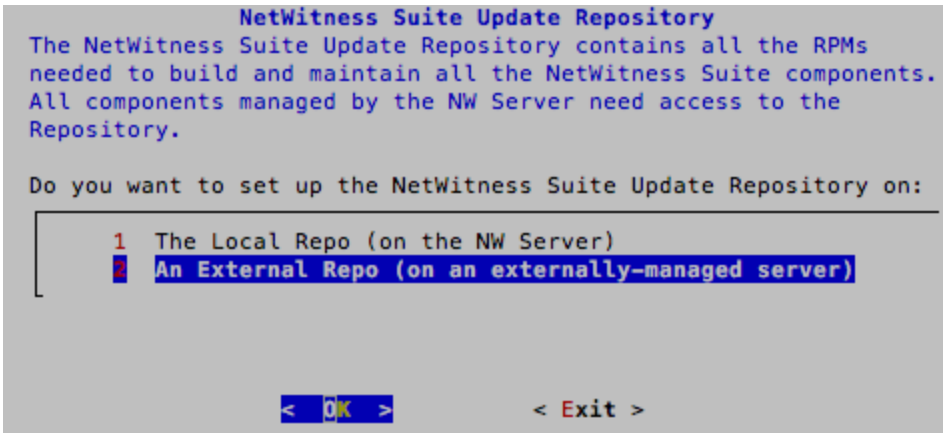
6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   The Deployment Password prompt is displayed.



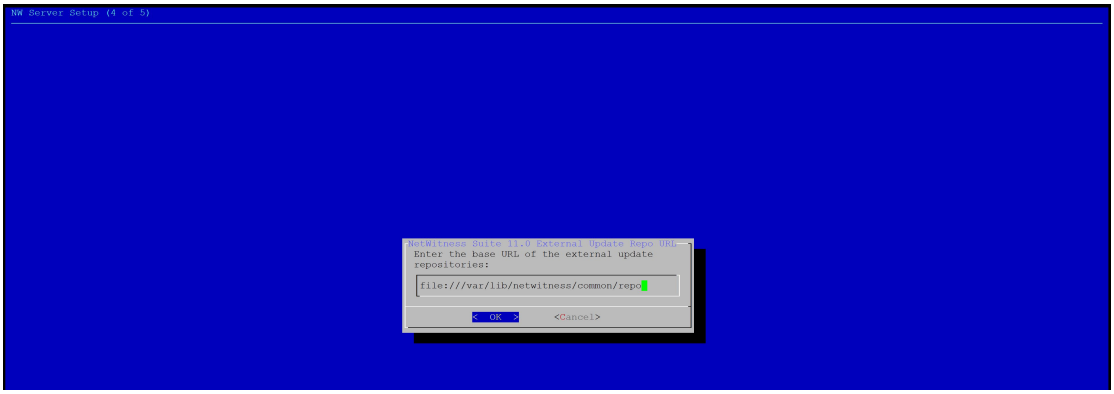
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   The Update Repo prompt is displayed.



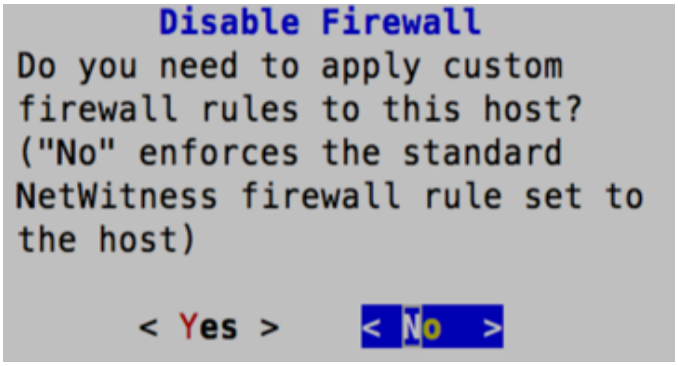
   You must use the same repo that you used for the NW Server hosts for all hosts.

8. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.



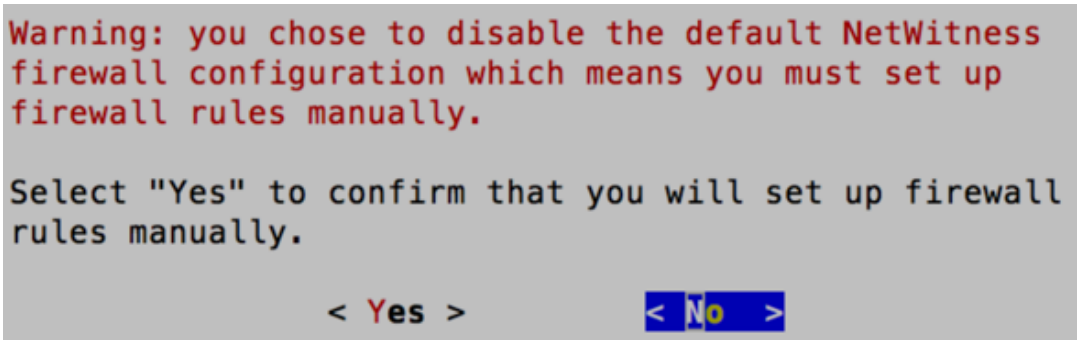
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *Hosts and Services Getting Started Guide for Version 11.1* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

9. Enter the base URL of the NetWitness Suite external repo and click **OK**.
The disable or use standard firewall configuration prompt is displayed.



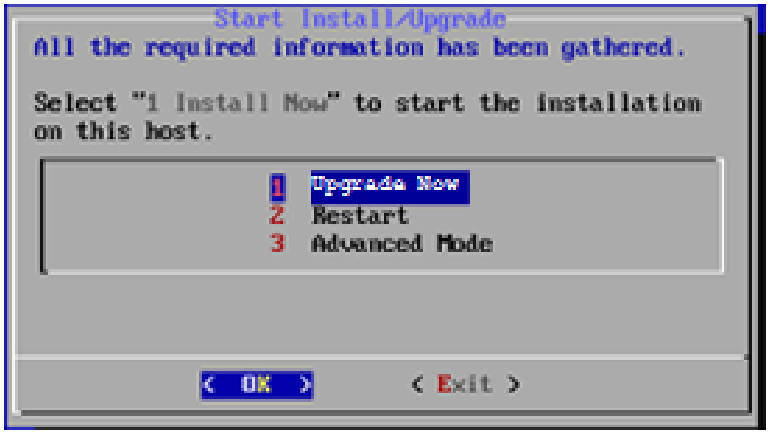
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- If you select Yes, confirm your selection.



- If you select No, the standard firewall configuration is applied.

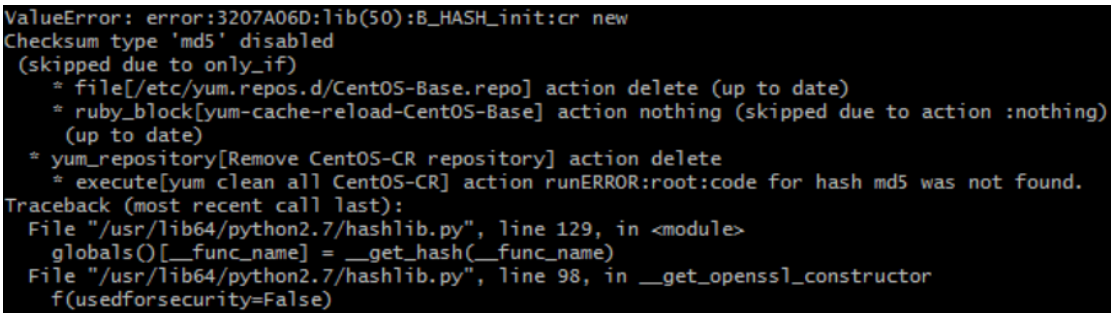
The start upgrade prompt is displayed.



11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.

When "Installation complete" is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.



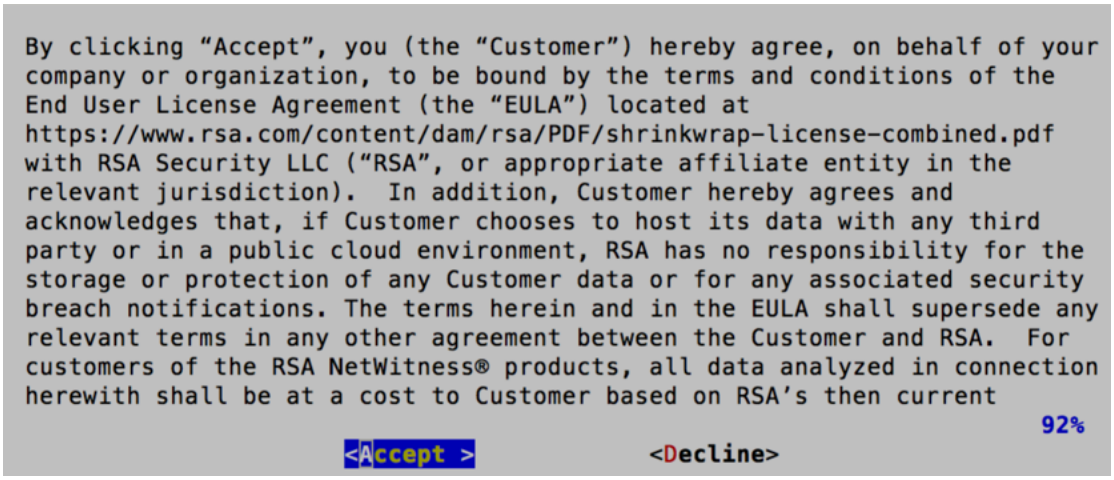
Set Up 11.1 Non-NW Server Host

Make sure that you Back up your 10.6.5.x data for the host. You must follow the instructions in Backup Instructions to back up the host.

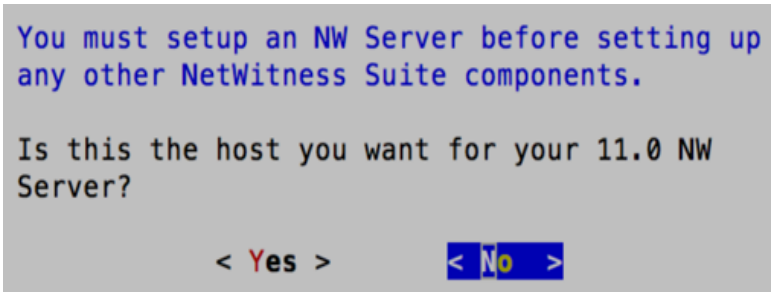
Caution: Run the backup immediately before upgrading the host to 11.1 so that the data is as recent as possible.

Complete the following steps to set up an 11.1 Non-NW Server host.

1. **Power On** the non-NW Server VM and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

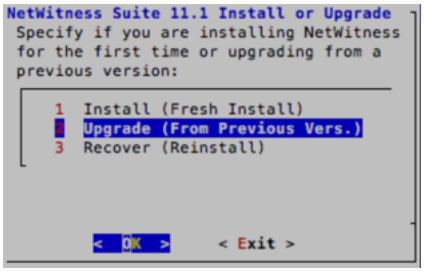


2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

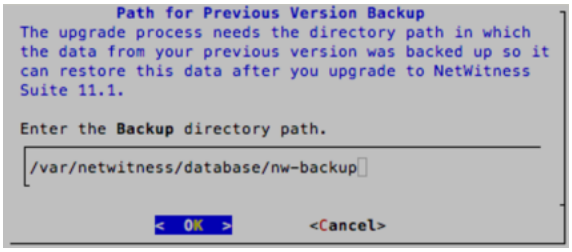


Caution: If you choose the wrong the host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

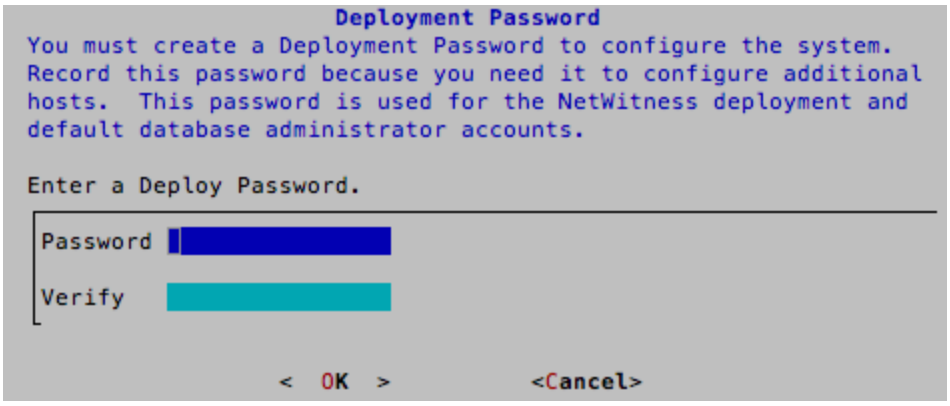
3. Tab to **No** and press **Enter**.
   The Install or Upgrade prompt is displayed.



4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.
   The backup path prompt is displayed.



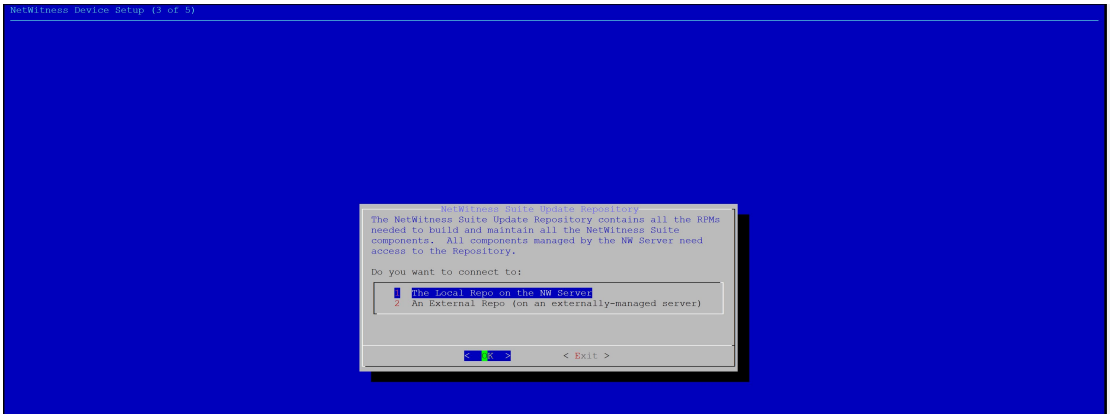
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.
   The Deployment Password prompt is displayed.



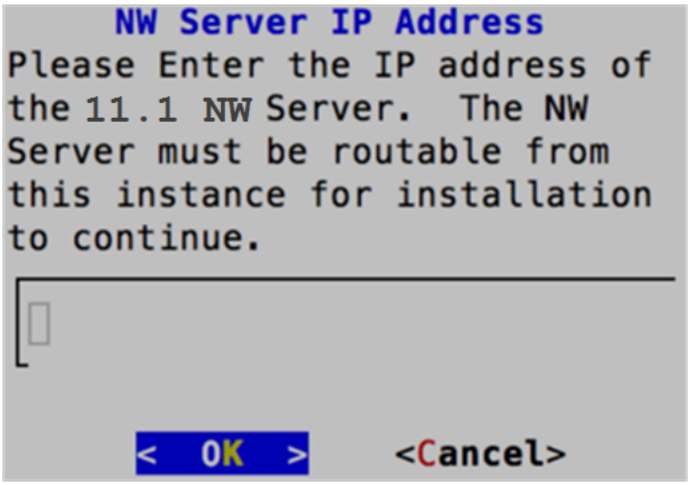
> **Note:** You must use the same deployment password that you used when you upgraded the NW Server.

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

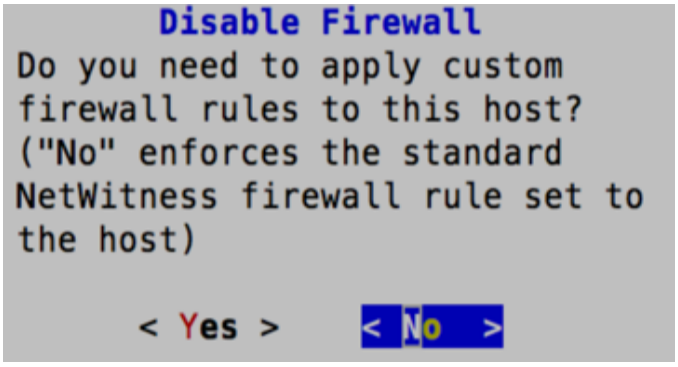
The Update Repo prompt is displayed.



7. Use the down and up arrows to select **1 The Local Repo on the NW Server**, tab to **OK**, and press **Enter**.
8. The NW Server IP Address is displayed.

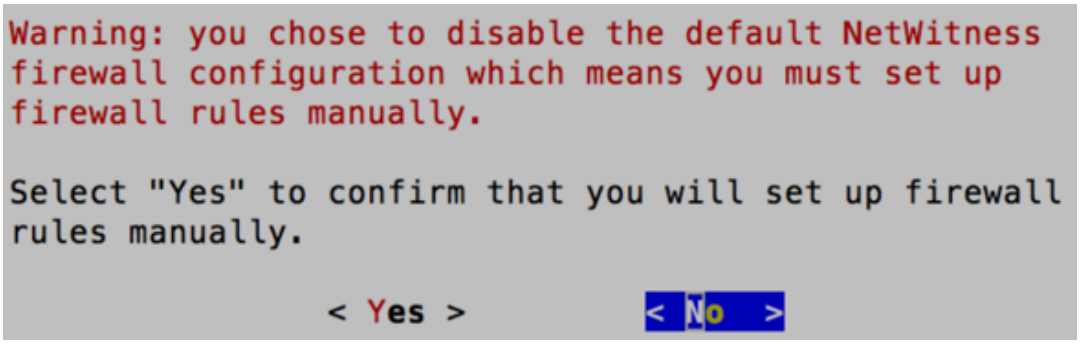


9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.
   The disable or use standard firewall configuration prompt is displayed.



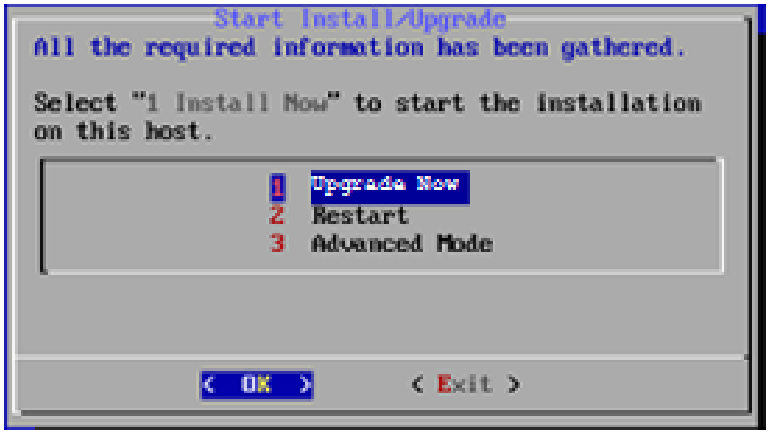
10. Tab to **No**, and press Enter to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

    - If you select **Yes**, confirm your selection.

    - If you select **No**, the standard firewall configuration is applied.

    The start upgrade prompt is displayed.

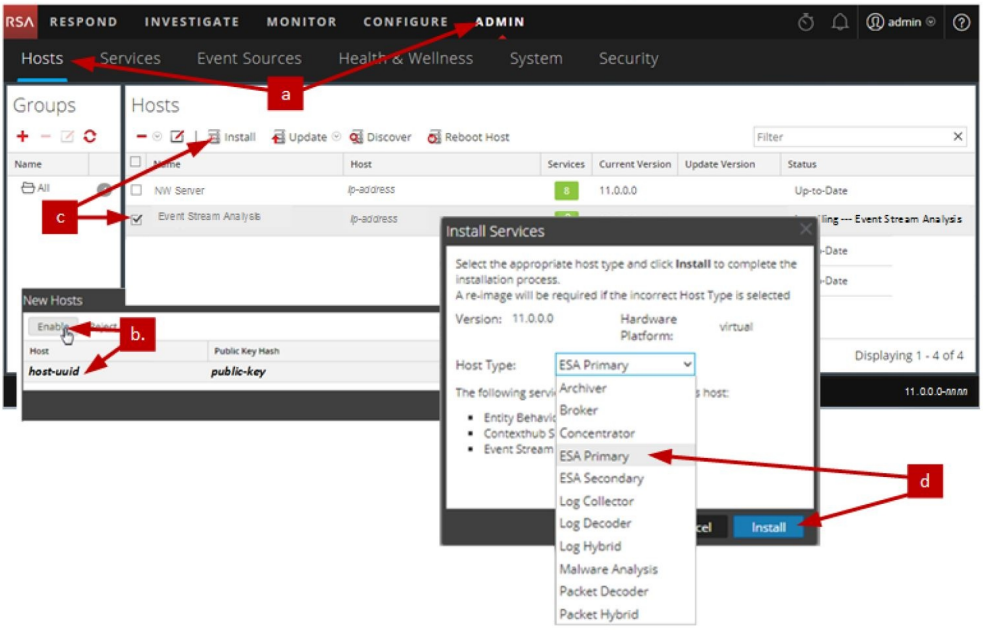
11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.
    When "Installation complete" is displayed, you have upgraded the host to the 11.1.

Once 'nwsetup-cli' script ran successfully on all the components, follow the below steps to complete NW 11.1 Upgrade or Migration:

1. Log into NetWitness Suite. (Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Suite Login screen)
2. Click ADMIN > Hosts. The New Hosts dialog is displayed with the Hosts view grayed out in the background. Note: If the New Hosts dialog is not displayed, click Discover in the Hosts view toolbar.
3. Click on the host in the New Hosts dialog and click Enable. The New Hosts dialog closes and the host is displayed in the Hosts view.

4. Select that host (for example, ESA Primary) and click The Install Services dialog is displayed.

   e. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.1 Legacy Windows Collection Guide* on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.1. These tasks are organized by the following categories.

- Global
- NetWitness Endpoint
  RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, and 4.4 only for NetWitness Suite 11.1.
- Event Stream Analysis
- Log Collection
- Reporting Engine
- Respond
- NetWitness SecOps Manager
- Security

Global Tasks

Task 1 - Remove Backup-Related Files from Host Local Directories

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.1 before you remove the backup-related files from the local directories on your 11.1 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.1, you must remove:

- the backup files from the local directories on the hosts.
- all the files from `nw-backup` and `restore` directories on the hosts.

Host	Backup Path	Restore Path
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`

Host	Backup Path	Restore Path
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
All Other Hosts	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

Task 2 - Restore NTP Servers

You must use the NetWitness Suite 11.1 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *RSA NetWitness® Suite 11.1 System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 3 - Restore Licenses for Environments without FlexNet Operations-On Demand Access

If your environment does not have access to FlexNet Operations-On Demand, you need to re-download your NetWitness Suite licenses. Refer to "Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on how to re-download licenses. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

(Conditional) Task 5 - If You Disabled Standard Firewall Config - Add Custom IPtables

During the upgrade, you have the option of using these rules or disabling them. If you disabled them, follow these instructions as a baseline to create a user-managed firewall rule sets on all the hosts for which you disabled the standard firewall configuration.

Note: You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the restore folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.
2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Reload the `iptables` and `ip6tables` services.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditional) Task 6 - Specify SSL Ports If You Never Set Up Trusted Connections

Complete this task only if you never set up Trusted Connections. You would not have set up Trusted Connections if you:

- Used the base ISO image for 10.3.2 or earlier.
- Updated the system using RPMs exclusively to get to 10.6.5.

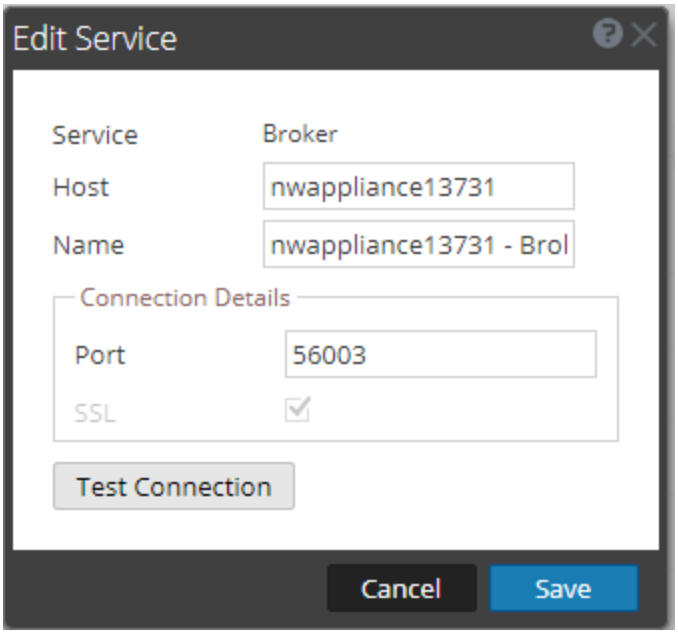
NetWitness Suite 11.1 cannot communicate with the core services for these customers because they are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. Log in to NetWitness Suite
2. Go to **ADMIN** > **Services**.
3. Select each core service and change there ports from Non-SSL to SSL ports.

Service	Non-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

4. Click (Edit) from the **Services** view toolbar.
   The Edit Service dialog is displayed.

5. Change the port from Non-SSL to SSL as shown in the table and click **Save**(for example, change the Broker port from 50003 to 56003).



NetWitness Endpoint

Task 7 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite 11.1, the virtual host is `/rsa/system`. For 10.6.5.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.
3. SSH to the NW Server and log in with `root` credentials.
4. Submit the following command to add all certificates to the truststore.
   `orchestration-cli-client --update-admin-node`
5. Submit the following command to restart the RabbitMQ server.
   `systemctl restart rabbitmq-server`
   The NetWitness Endpoint account should automatically be available on RabbitMQ.

6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Event Stream Analysis Tasks (ESA)

Task 8 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.1.

1. Log in to NetWitness Suite 11.1
2. Click **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
3. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. Click **ADMIN**> **Services**, select the Context Hub service, in the action commands ( ) drop-down menu, click **View** > **Config** > **Lists** tab).
   b. Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Suite ESA Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 9 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL

If you integrate with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint, you must configure Mutually Authenticated SSL on each integrated system so that the application can authenticate itself when connecting to the RabbitMQ message bus.

Note: Use the RabbitMQ usernames and passwords that were obtained when you backed up your 10.6.5.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Suite by logging into the host and running the following `rabbitmqctl` command.

```
> rabbitmqctl add_user <username> <password>
```

For example:

```
> rabbitmqctl add_user wtd-incidents incidents
```

2. Set permissions for users by running the following command (use the username from step 1):
   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*",
   ".*"
   ```
   For example:
   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*",
   ".*", ".*"
   ```

Task 10 - Enable Threat - Malware Indicators Dashboard

In 11.1.0, the 10.6.5.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.5x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.1.
2. Set datasource for new dashlets.

   See "Dashlets" in the RSA Link (https://community.rsa.com/docs/DOC-81463).

Log Collection

Task 11 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.1 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

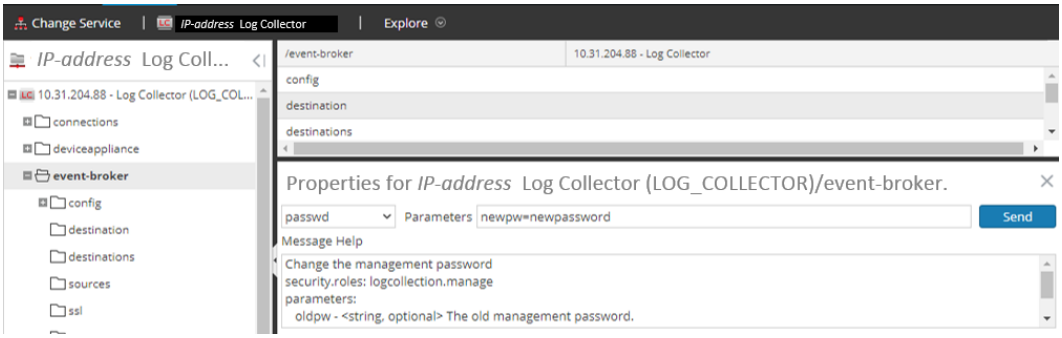
The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Update Log Collector Service RabbitMQ User Account Password

If the logcollector service RabbitMQ user account password was changed, you must reenter it after the 11.1 upgrade.

1. Log in to NetWitness Suite.
2. Go to **ADMIN > Services**.
3. Select the Log Collector service.
4. Click (Actions) > **View** > **Explore**.

5. Right click `event-broker` > **Properties**.
6. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 12 - Enable FIPS Mode

FIPS is enabled on all services except Log Collector Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder. For information about how to enable FIPS for these services, see the "Sys Maintenance: Activate or Deactivate FIPS" topic in the *RSA NetWitness® SuiteSystem Maintenance Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Reporting Engine

Task 13 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the back up you made prior to the upgrade. The Backup script backs up the 10.6.5.x CA certificates into the `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts` directory.

Complete the following procedure to restore the CA certificates in 11.1.

1. SSH to the NW Server host.
2. Export the CA certificates.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Copy the CA pem into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 14 - Restore External Storage for Reporting Engine

If you have external storage for the Reporting Engine (such as SAN or NAS for storing reports), you must restore the mount you unlinked before the upgrade. See "Reporting Engine: Add Additional Space for Large Reports" in the *RSA NetWitness® Suite Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

Task 15 - Restore Respond Service Custom Keys

In 10.6.5.x, if you added custom key for use in the groupBy clause, the `alert_rules.json` file was modified. The `alert_rules.json` file contains aggregation rule schema. RSA moved the `alert_rules.json` file to the following new location: `/var/lib/netwitness/respond-server/scripts`

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.

   This directory is where the `alert_rules.json` file is restored from the 10.6.5.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.1.

   This is the new file for 11.1.

3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 16 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.1 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.x, you must:

1. Go to the to the `/opt/rsa/im/scripts` directory.
   This directory is where the following Respond service normalization scripts are restored from the 10.6.5.x backup.
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Copy any custom logic from the 10.6.5.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Suite 11.1 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
   The `alert_rules.json` file contains aggregation rule schema.

(Conditional) Task 17 - Enable Disabled 10.6.5.x Incident Management Data Retention

Complete the following procedure to enable the Incident Management data retention jobs you disabled prior to upgrade.

1. Log in to RSA NetWitness® Suite.
2. Go to **ADMIN** > **Services** and select the **Respond server**.
3. Click the (Actions), **View** > **Explore**.
4. Go to the `respond/dataretention` node.
5. Set the `enable` parameter to `true`.

(Conditional) Task 18 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.1. See *Adding Roles and Assigning Permissions for the Roles* in the *RSA NetWitness Suite Warehouse Analytics Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

NetWitness SecOps Manager

Task 19 -Reconfigure NW SecOps Manager Integration

For information on how to reconfigure NW SecOps for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

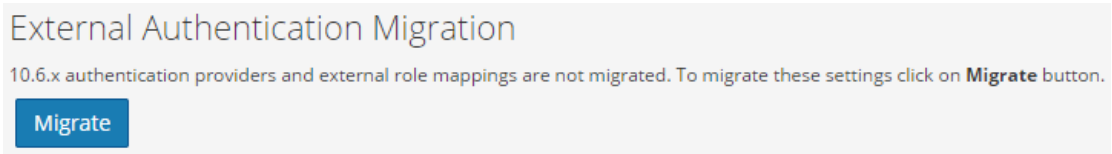
Security

Task 20 - Migrate Active Directory (AD)

The first time you log into the NetWitness Suite 11.1 User Interface, you must click on the Migrate button to complete the migration of AD.

Caution: If you did not upgrade from 10.6.4.2, you must apply the 11.0.0.1 patch immediately before you first log into NetWitness Suite 11.1 and migrate Active Directory. You do not need to apply the 11.0.0.1 patch if you upgraded to 11.1 from 10.6.4.2.

1. Log in to NetWitness Suite with your `admin user` credentials.
2. Click **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.



3. Click **Migrate**.
   The migration is complete and the dialog closes.

Task 21 - Modify Migrated AD Configuration to Upload Certificate

If the you used a self-signed certificate in Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.4.x, you must modify the migrated AD configuration to upload the certificate (either the self-signed cert or the CA cert).

Complete the following procedure to modify the migrated AD configuration to upload the certificate (either the self-signed cert or the CA cert).

1. Log in to NetWitness Suite.
2. Go to **ADMIN** > **Security** and click the **Settings** tab.
3. Under **Active Directory Settings**, select an AD configuration and click .
   The Edit Configuration dialog is displayed.
4. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
5. Click **Save**.

Task 22. Address Authentication Failure in 11.1

Users cannot log in to NetWitness Suite User Interface after you upgrade to 11.1 because the Interface cannot retrieve user account information from MongoDB.

- Apply the 11.0.0.1 patch to fix this issue immediately after you upgrade to 11.1.

Task 23 - Reconfigure Pluggable Authentication Module (PAM) in 11.1

You must reconfigure PAM after you upgrade to 11.1. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite System Security and User Management Guide*for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

You can refer to your 10.6.5.x PAM configuration files in the **/etc** directory in the your 10.6.5.x backup data for guidance.

Appendix A. Troubleshooting

This section describes problems that you may encounter during the upgrade with solutions. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve any upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294)

This section has troubleshooting documentation for the following services, features, and processes.

- 11.1 Setup Program (`nwsetup-tui`)
- Backup
- Event Stream Analysis
- General
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

11.1 Setup Program (nwsetup-tui)

Problem	Host Setup Program (nwsetup-tui) exits and creates the following error message in /var/log/netwitness/bootstrap/launch/security-server/security-server.log: <yyyy-mm-dd hh:mm:ss,nnn> [main] ERROR SystemOperation|Service startup failed. Running in safe mode org.h2.jdbc.JdbcSQLException: The database is read only [90097-193] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) ... at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnection(AbstractDriverBasedDataSource.java:159) at com.rsa.asoc.security.upgrade.legacy.MigrationDatabase.<init>(MigrationDatabase.java:113)
Cause	The H2 database needs write permission to complete the host setup.
Solution	From the NW Server command line, provide write permission to H2.db, restart the NW Server, and restart nwsetup-tui Setup Program. chmod o+w /var/lib/netwitness/uax/db/platform.h2.db systemctl restart rsa-nw-security-server.service nwsetup-tui

Backup (`nw-backup` script)

Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the the *RSA NetWitness® Suite Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESAPrimary host and log in.
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Submit the following command to restart ESA .
	`systemctl restart rsa-nw-esa-server`
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

General

Logs referred to in this section are posted to `/var/log/install/install.log` on the NW Server Host.

Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Suite sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service using below command. `systemctl restart rsa-sms`

Message	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt is nGB` `<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.`
Cause	Low or insufficient disk space allocated for the SMS service.
Solution	RSA recommends that you provide a minimum of 10 GB of disk space for the SMS service to run optimally.

Problem	After you run the Setup Program for a non-NW Server host, you must go in to the UI, enable the host, and install the service on the host from the Hosts View. If you see "Install error View Details" in the **Status** column of the Hosts view, the host lost connectivity due to network issues.
Solution	Re-install the service on the host from the Hosts view.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Suite and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Message	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Suite and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents..

Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Suite and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the sa.log. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.5 to 11.1.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Message	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

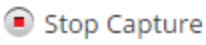
Appendix B. Stopping and Restarting Data Capture and Aggregation

RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.1. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

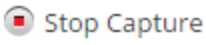
1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
   

3. Under (actions), select **View** > **System**.
4. In the toolbar, click

   .

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.
   

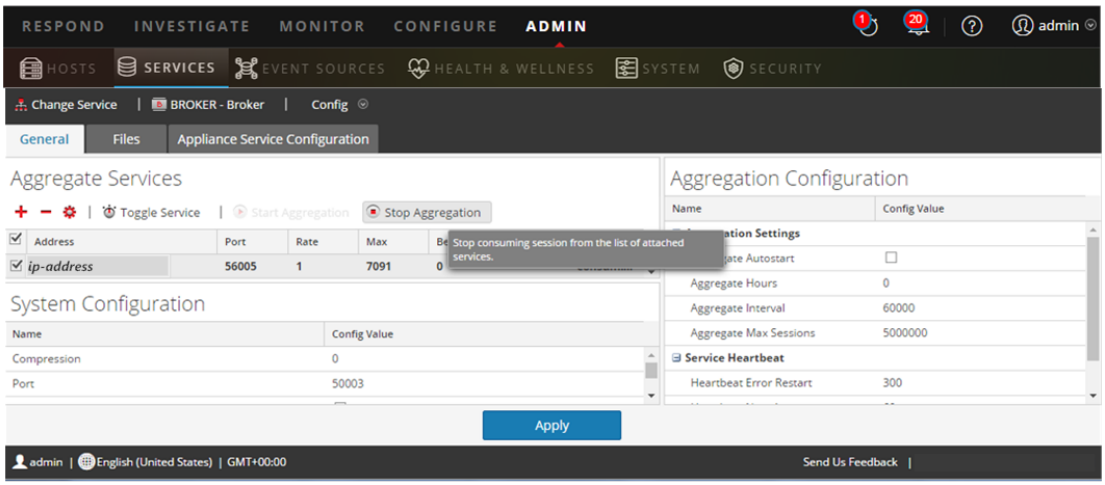
3. Under (actions), select **View** > **System**.
4. In the toolbar, click

   .

Stop Aggregation

1. Log in to NetWitness Suite
2. Go to **ADMIN** > **Services**.

3. Select the **Broker** service.
4. Under (actions), select **View** > **Config**.
5. The **General** tab is displayed.



6. Under **Aggregated Services** click

.

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.

Start Packet Capture

To start packet capture:

1. Login to **NetWitness Suite**.
2. Go to **ADMIN** > **Services**.
   The Services view is displayed.
3. Select each **Decoder** service.
4. Under (actions), select **View** > **System**.
5. In the toolbar, click

.

Start Log Capture

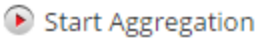
To start log capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click

.

Start Aggregation

1. Log in to **.**NetWitness Suite.
2. Go to **ADMIN** > **Services**.
3. Select the **Broker** service.
4. Under (actions), select **View** > **Config**.
5. The **General** tab is displayed.
6. Under **Aggregated Services** click 

.

Revision History

Revision	Date	Description	Author
1.0	29-Mar-2018	Release to RSA Link	IDD

RSA NETWITNESS® SUITE

Azure Upgrade Guide

for Version 11.1.0.0

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

Introduction **7**

CentOS6 to CentOS7 Upgrade 7

RSA NetWitness® Suite 11.1 Upgrade Path 8

Hardware, Deployments, Services, and Features Not Supported in 11.1 8

Event Stream Analysis (ESA) Upgrade Considerations 9

Upgrade Phases 9

Investigate in Mixed Mode 10

Contact Customer Support 13

Upgrade Preparation Tasks **14**

Global 14

Task 1 - Review Core Ports and Open Firewall Ports 14

Task 2 - Record Your 10.6.5.x admin user Password 15

Task 3 - Create a Backup of /etc/fstab File 15

Reporting Engine 15

(Conditional) Task 4 - Unlink External Storage 15

Backup Instructions **16**

Task 1 - Set up an External Host for Backing up Files 17

Task 2 - Create a List of Hosts to Back up 19

Troubleshooting Information 20

Task 3 - Set up Authentication Between Backup and Target Hosts 22

Task 4 - Check for Backup Requirements for Specific Types of Hosts 22

For All Host Types 22

For Concentrator, or Broker Hosts: Stop Data Capture and Aggregation 23

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh 23

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords 25

For Bluecoat Event Sources 25

Task 5 - Check for Adequate Space for the Backup 25

Task 6 - Back up Your Host Systems 26

Post Backup Tasks 29

Task 1 - Save a Copy of the all-systems File and the Backup Tar files 29

Task 2 - Ensure Required Backup Files Were Generated 29
Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host 30
Task 4 - Ensure All Required Backup Files are on Each Host 30

Migrate Disk Drives from 10.6.5.x to 11.1 33

Prerequisites: 33
Task 1 - Deploy NW 11.1 VM 35
Task 2 - Delete Virtual Machine and OS disk resource of NW 10.6.5 VM 35
Task 3 - Install Azure PowerShell modules on a local Windows machine 37
Task 4 - IP Retention: Run the PowerShell script 37
Task 5 - Perform Disk Migration 39
Task 6 - Data Restoration 40
Task 7 - Delete all NW 11.1 Deployment 'Network interface' Resources 42

Set Up Virtual Hosts in 11.1 43

Phase 1 - Set Up NW Server, Event Stream Analysis, and Broker or Concentrator Hosts 43
Task 1 - Set Up 11.1 NetWitness Server 43
Task 2 - Setup 11.1 ESA 43
Task 3 - Set Up 11.1 Broker or Concentrator 43
Phase 2 - Set Up The Rest of the Component Hosts 44
Concentrator Hosts 44
Log Decoder Host 44
Virtual Log Collector Host 44
Set Up 11.1 NW Server Host 46
Set Up 11.1 Non-NW Server Host 51

Update or Install Legacy Windows Collection 56

Post Upgrade Tasks 57

Global Tasks 57
Task 1 - Remove Backup-Related Files from Host Local Directories 57
Task 2 - Restore NTP Servers 58
Task 3 - Restore Licenses for Environments without FlexNet Operations-On Demand Access 58
Task 4 - Remap Virtual NW Server License to 10.6.5.x MAC Address 58
(Conditional) Task 5 - If You Disabled Standard Firewall Config - Add Custom IPtables 58
(Conditional) Task 6 - Specify SSL Ports If You Never Set Up Trusted Connections 59

NetWitness Endpoint 60
Task 7 - Reconfigure Endpoint Alerts Via Message Bus 60
Event Stream Analysis Tasks (ESA) 61
Task 8 - Reconfigure Automated Threat Detection for ESA 61
Task 9 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL 61
Task 10 - Enable Threat - Malware Indicators Dashboard 62
Log Collection 62
Task 11 - Reset Stable System Values for Log Collector after Upgrade 62
(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 12 - Enable FIPS Mode 63
Reporting Engine 63
Task 13 - Restore the CA certificates for External Syslog Servers for Reporting Engine ..63
(Conditional) Task 14 - Restore External Storage for Reporting Engine 64
Respond 64
Task 15 - Restore Respond Service Custom Keys 64
Task 16 - Restore Customized Respond Service Normalization Scripts 65
(Conditional) Task 18 - Restore Custom Analysts Roles 65
NetWitness SecOps Manager 65
Task 19 -Reconfigure NW SecOps Manager Integration 65
Security 66
Task 20 - Migrate Active Directory (AD) 66
Task 21 - Modify Migrated AD Configuration to Upload Certificate 66
Task 23 - Reconfigure Pluggable Authentication Module (PAM) in 11.1 66

Appendix A. Troubleshooting 68

11.1 Setup Program (nwsetup-tui) 69
Backup (nw-backup script) 70
Event Stream Analysis 70
General 71
Log Collector Service (nwlogcollector) 72
NW Server 74
Reporting Engine Service 74

Appendix B. Stopping and Restarting Data Capture and Aggregation ..75

Stop Data Capture and Aggregation 75
Start Data Capture and Aggregation 77

Revision History **78**

Introduction

The instructions in this guide apply to the upgrade of Azure for RSA NetWitness Suite 10.6.5.x to 11.1.0.0 exclusively. See the *RSA NetWitness Suite Physical Host Upgrade Guide* for instructions on how to upgrade your 10.6.5.x physical hosts to 11.1. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents. This document assumes that the appliances are in Azure cloud.

NetWitness Suite 11.1 is a major release that affects all products in the NetWitness Suite in Azure. The components of the suite are the NetWitness Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Entity Behavior Analytics, Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, and Workbench.

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.1 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.1 platform environment has been improved greatly to accommodate current and future, physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Suite 11.1 Upgrade Path

The supported Upgrade path for RSA NetWitness® Suite 11.1 is Security Analytics 10.6.5.x. If you are running a version of NetWitness Suite that is prior to 10.6.5.x, you must update to 10.6.5.x before you can upgrade to 11.1. See the *RSA Security Analytics 10.6.5 Update Guide* (https://community.rsa.com/docs/DOC-85119) on RSA Link.

For updating from RSA NetWitness® Suite 11.0.0.0 to RSA NetWitness® Suite 11.1.0.0, please see the *Update Guide from 11.0.x to 11.1.0.0 Guide*.

Hardware, Deployments, Services, and Features Not Supported in 11.1

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.1.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- IPDB service
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.1.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.1.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.1, your custom policy is not present. In its place, there is the out-of-the-box Context hub Server Monitoring Policy in the user interface, which is specific for version 11.1.
- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)
- Malware Analysis
- Packet Decoder

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Suite 11.1, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.1, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.5.x has been removed.

Caution: If you do not use Incident Management in 10.6.5.x, carefully consider whether or not to upgrade to version 11.1.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.1.

In your 10.6.5.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.1.
- Multiple ESA hosts configured to use Incident Management – The system will continue to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.5.x, you can upgrade to version 11.1.
- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.1.

Upgrade Phases

RSA recommends that you stagger host upgrades as described in this section. The update to CentOS7 and the need of a physical or iDRAC access cause the 11.1 upgrade to take more time than most upgrades.

Caution: If you stagger the upgrade, you:
• must upgrade the hosts in Phase 1 first, in the order shown.
• may not have all the features operational until you update your entire deployment.
• will not have service administrative features available until you upgrade all the hosts in your deployment.

Phase 1

You perform Phase 1 first and you must upgrade the hosts in the following order:

1. Security Analytics Server host
2. Event Stream Analysis hosts
3. Broker hosts (if you do not have a Broker, upgrade your Concentrator hosts)
   The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2

Upgrade the rest of your hosts.

In Phase 2, (other than Log Collection hosts with downstream event destinations) there is no technical reason to upgrade your hosts in the following order. RSA recommends that you follow the order in Phase 2 to reduce:

- functionality loss during investigation.
- downtime that results in the loss of packet and log capture.

1. Concentrator hosts
2. Archiver hosts
3. Log Collection hosts - Log Collectors on Log Decoder hosts (LDs), Virtual Log Collectors (VLCs) and Legacy Windows Collectors (LWCs)
   Before you upgrade a log collection host , you must prepare it for the upgrade. Part of this preparation ensures that no event data remains in the queues. This requires you to keep the downstream destinations of event data (Log Collectors, Virtual Log Collectors and Log Decoders) up and functioning properly.

   If you have event data destinations downstream from the Log Decoder, you must prepare and upgrade log collectors in the following order.

   a. LDs (one LD at a time)

   b. VLCs and LWCs

   If you do not have event data destinations, downstream from the Log Decoder, you can prepare and upgrade multiple LDs, VLCs, and LWCs together.
4. All other hosts

See "Running in Mixed Mode" under "The Basics" in the RSA 11.1 *NetWitness Suite Hosts and Services Getting Started Guide* for:

- Functionality gaps encountered while running in this mode.
- Examples of staggered upgrades.

Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.1 and some are still on 10.6.x. This happens when you upgrade to 11.1 in phases.

Note: You must follow the host upgrade sequence as shown in Upgrade Phases to ensure complete Investigate functionality. The 11.1 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.0 to access the Event Analysis View.

After you upgrade all services to 11.1, when an analyst conducts an investigation, Role-Based Access Control (RBAC) of downloads works consistently to limit access to restricted data.

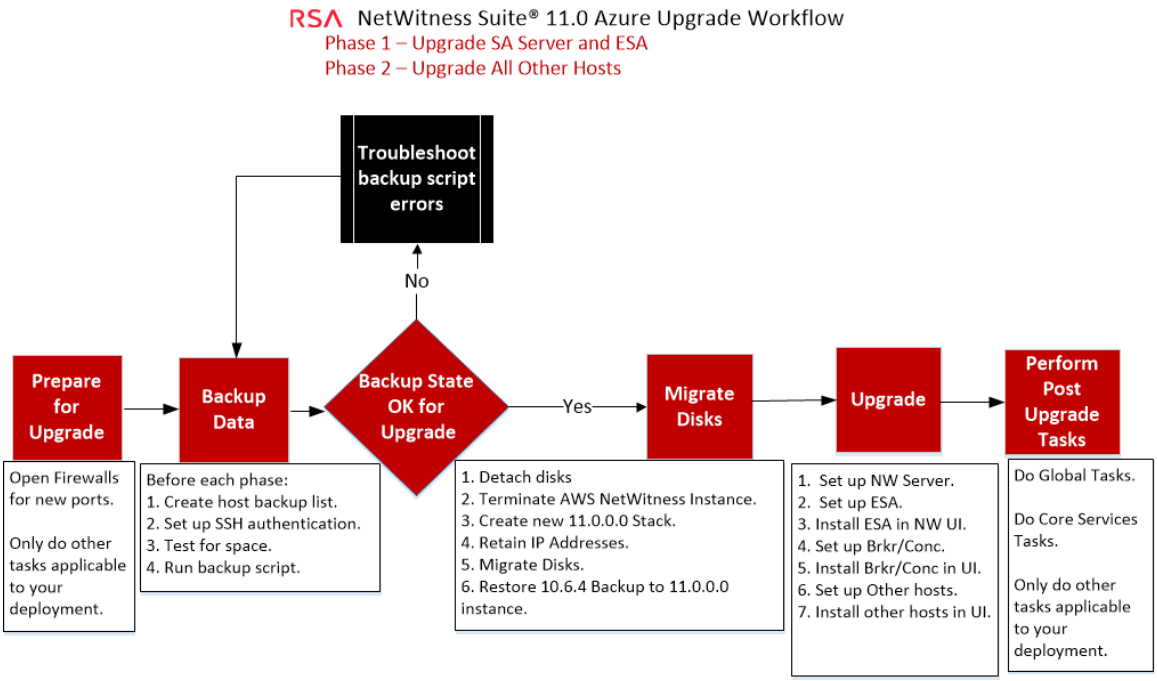
In mixed mode (that is, some services are upgraded to 11.1 and some are still on 10.6.x), when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads.

If the `sdk.packets` setting has not been disabled on the 10.6.x services, analysts with SDK meta and roles permissions in place to restrict viewing and reconstructing an event's content can download the PCAP of an event that has content restrictions. Other types of downloads appear to download, then generate errors due to insufficient permissions, and the data is still protected.

During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.1, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NetWitness Server is on version 11.1 connected to services at a lower version.

Connecting Service Version	Affected View	User Role	Can See	Can Download Successfully	Can Download with Errors
11.1 Broker -> 10.x Concentrator	Events View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst		PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload
	Event Reconstruction View	Admin			Files archive is downloaded but cannot unzip
11.1 Broker -> 11.1 Concentrator	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items		Files archive is downloaded but cannot unzip
	Event Reconstruction View				PCAPs and logs are downloaded as zero bytes



Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Suite 11.1.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.1. These tasks are organized by the following categories.

- Global
- Reporting Engine
- Respond and Incident Management

Global

You must complete these tasks regardless of how you deploy NetWitness Suite and which components you use.

Task 1 - Review Core Ports and Open Firewall Ports

The following table lists new ports in 11.1.

Caution: Make sure that the new ports are implemented and tested before upgrading so that upgrade does not fail due to missing ports.

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 27017	MongoDB

ESA Host

Source Host	Destination Host	Destination Ports	Comments
NW Server, NW Endpoint, ESA Secondary	ESA Primary	TCP 27017	MongoDB

All NetWitness Suite core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® Suite Deployment Guide* in case you need to reconfigure NetWitness Suite services and firewalls. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 2 - Record Your 10.6.5.x `admin user` Password

Record your 10.6.5.x `admin user` password. You will need it to complete the upgrade.

Task 3 - Create a Backup of `/etc/fstab` File

Copy the `/etc/fstab` file from all VMs to your local machine (backup host or remote machine).

Note: You need this file to restore a VM with external storage mounts.

Reporting Engine

(Conditional) Task 4 - Unlink External Storage

If the Reporting Engine has external storage [such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports] you must perform the follow steps to unlink the storage.

In these steps:

- `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
- `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.
2. Stop the Reporting Engine service.
   ```
   stop rsasoc_re
   ```
3. Switch to `rsasoc` user.
   ```
   su rsasoc
   ```
4. Change to the Reporting Engine the home directory.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. Unlink the `resultstore` directory mounted to external storage.
   ```
   unlink /externalStorage/resultstore
   ```
6. Unlink the `formattedReports` directory mounted to external storage.
   ```
   unlink /externalStorage/formattedReports
   ```

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from 10.6.5.x releases to 11.1.0.0.

Note: It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.1.0.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types

Caution: 1) These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the NetWitness Server
- Standalone Warehouse Connector

The following types of hosts can be backed up and are automatically restored during the upgrade process:

- **NetWitness Server** (may include Malware Analysis, NetWitness Respond, Health and Wellness, and Reporting Engine)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and NetWitness Respond database)
- **Concentrator**
- **Log Decoder** (including Local LogCollector and Warehouse Connector, if installed)
- **Virtual Log Collector**

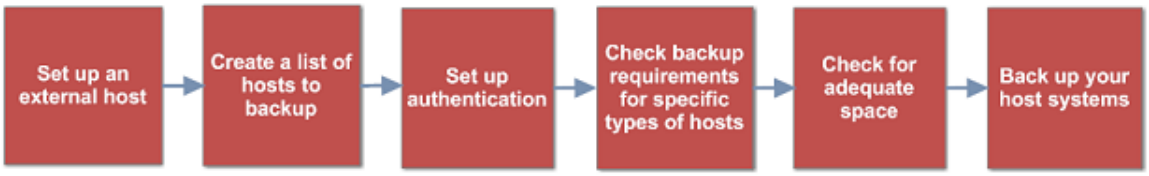
The following types of files are automatically backed up but must be restored manually after the upgrade process:

- PAM configuration files: For information about restoring the PAM configuration files, refer to "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.1.0.0", in the "Global" section of the Post Upgrade Tasks.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-`

`backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of Post Upgrade Tasks.

Note: If you have problems during the backup or upgrade processes and you lose data, you can recover the data and start the process again. For information about recovering lost data, see "Recover Data After System Failure" in the *System Maintenance Guide*.

The following diagram shows the high-level task flow of the steps you perform to back up your hosts.



The following sections describe each of these tasks:

- Task 1 - Set up an External Host for Backing up Files
- Task 2 - Create a List of Hosts to Back up
- Task 3 - Set up Authentication Between Backup and Target Hosts
- Task 4 - Check for Backup Requirements for Specific Types of Hosts
- Task 5 - Check for Adequate Space for the Backup
- Task 6 - Back up Your Host Systems
- Post Backup Tasks

Task 1 - Set up an External Host for Backing up Files

You must set up an external host to use for backing up files. The host must be running Centos 6 with connectivity through SSH to the NetWitness Suite stack of hosts.

Ensure that the host names for the systems to be backed up are resolvable on the backup host machine, either by DNS or listed in the `/etc/hosts` file.

Note: These scripts are designed to run on CentOS 6 only. You must execute these scripts on CentOS 6 machines.

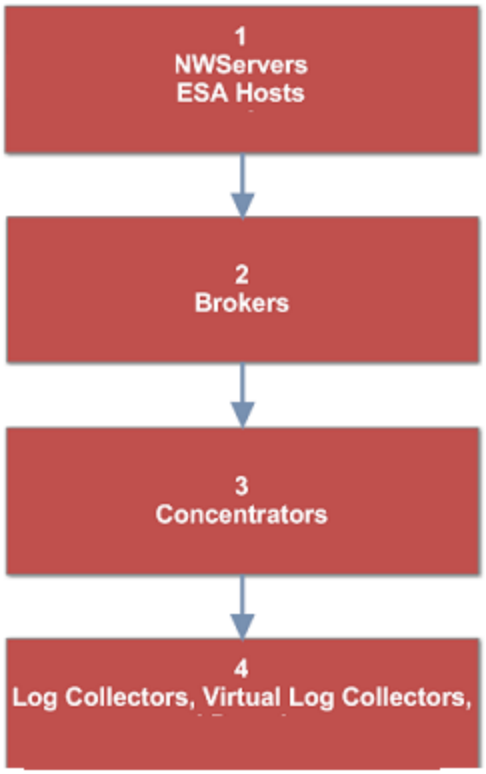
There are several scripts that you run during the backup process. You must download the zip file that contains the scripts (`nw-backup-v3.0.zip`) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Click the **RSA NetWitness Logs & Packets 11.1 Backup Script (nw-backup-v3.0.sh)** link and extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your NetWitness Servers and host systems to be backed up.
- `ssh-propagate.sh`: Automates sharing keys between the systems you are backing up and the backup host system so that you are not prompted for passwords multiple times.
- `nw-backup.sh`: Performs the backup of your hosts.

Note: The backup scripts do not support backing up data for STIG-hardened hosts.

Task 2 - Create a List of Hosts to Back up

The script that you use to back up your files depends on the `all-systems` and `all-systems-master-copy` files, which contain a list of the hosts that you want to back up. The `all-systems-master-copy` file contains a list of all your hosts. The `all-systems` file is used for each backup session, and contains only those hosts which are being backed up for a particular session. You run the `get-all-systems.sh` script to generate these files. RSA recommends that you back up your hosts in groups, and not all at once. The recommended order and grouping of hosts for backup sessions is shown in the following diagram:



Limit each backup session to five hosts to ensure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference and then manually editing the `all-systems` file to contain specific hosts.

To generate the `all-systems` and the `all-systems-master-copy` files:

1. From the host on which you are running the backup process, make the `get-all-systems.sh` script executable by running the following command:
   ```
   chmod u+x get-all-systems.sh
   ```
2. At the root level, run the `get-all-systems.sh` script:
   ```
   ./get-all-systems.sh <IP-Address-of-NetWitness-Admin-Server>
   ```
   You will be prompted for the password for each host system once per host.

This script saves the `all-systems` file and the `all-systems-master-copy` file to `/var/netwitness/database/nw-backup/`.

3. Validate that the `all-systems` and `all-systems-master-copy` files were generated and that they contain the right hosts.
4. Edit the `all-systems` file to contain only the systems you are backing up. You can do this by using the `all-systems-master-copy` file as a reference, and then opening the `all-systems` file in an editor (such as vi) and modifying it to include only the systems you want to back up.

> **Note:** If you use vi, be sure to include the path to the location of the `all-systems` file.

Here is an example of an `all-systems-master-copy` file:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.4.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.4.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.4.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.4.0
```

And here is an example of an `all-systems` file based on the `all-systems-master-copy` file that could be used in the first backup session:

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
```

Troubleshooting Information

- Be sure to save copies of the `all-systems` and `all-systems-master-copy` files in a safe location. Follow these recommendations:
  - Do not edit the `all-systems-master-copy` file.
  - If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure to remove pre-existing entries from the file so that the file contains only those hosts that are currently being backed up.
    For more information, see Post Upgrade Tasks.

- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.
- The `get-all-systems.sh` script generates a list of hosts that were defined in the NetWitness Suite user interface. Ensure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to NetWitness Suite, you use the NetWitness Suite user interface to ensure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.
- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the NetWitness Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the NetWitness Server. (Any Windows Legacy Collectors or Azure Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)
- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

RSA recommends that you run the `ssh-propagate.sh` script to automate sharing keys between the backup host and the host systems.

Note: If you have SSH keys that are protected with pass phrases, you can use `ssh-agent` to save time. For more information, refer to the man page for `ssh-agent`.

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:
   `chmod u+x ssh-propagate.sh`
2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. You are prompted for the password once per host, but you will not need to enter it again later during the backup process.

Task 4 - Check for Backup Requirements for Specific Types of Hosts

After you create the `all-systems` file to use for backup, you must check to see if any of the hosts listed in the file have requirements that must be met before you run the backup process.

For All Host Types

Perform the following steps for all host types:

1. On the NetWitness Server, place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directories will be automatically restored during the upgrade process. After upgrading to 11.1.0.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`.
   You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the NetWitness Server and run the following command strings to perform the conversions listed.
   Convert a DER file (.crt .cer .der) to PEM
   `openssl x509 -inform der -in certificate.cer -out certificate.pem`
   Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Note:** Add the following qualifier to the command string to:
> `-nocerts` convert private keys exclusively.
> `-nokeys` convert certificates exclusively.

2. Manually record any custom configurations made to CentOS 6 (for example, driver customizations) for restoration after you update to CentOS 7. Custom configurations to CentOS 6 are not automatically backed up and restored.

For Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for Concentrator, or Broker hosts, stop data capture and aggregation on all the systems that you are backing up. For instructions, refer to Appendix B. Stopping and Restarting Data Capture and Aggregation

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run `prepare-for-migrate.sh`

> **Caution:** This task stops log collection so you must perform this step immediately before you upgrade to minimize the loss of event collection. Complete this task in accordance with the backup and upgrade tasks in this guide.

Prerequisites

You need the following information before you prepare LCs and VLCs for upgrade.

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.
- If you set the password for `logcollector` user for RabbitMQ , you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.
2. Submit the following command string.
   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```
   This command:

- Stops the Puppet Agent service.
- Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.1.0.0.
- Stops all the collection protocols in the Log Collector service.
- Saves the list of Plugin accounts and RabbitMQ accounts.
- Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.
- Waits until the Log Collector queues are empty.
- Stops the Log Collector service.
- Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

The `prepare-for-migrate.sh` script:

- Sends informational, warning, and error messages to the console.
- Saves a session log in the `/var/log/backup/` directory.

You must fix any of the following errors and resume the preparation. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

- Log Collector queues with events but without consumers are found.
- Unable to stop the Puppet Agent service.
- Unable to stop a collection protocol in the Log Collector service.
- Unable to block event publishers to the RabbitMQ server.
- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.
- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the NetWitness Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.1.0.0 upgrade, you can restore RabbitMQ user accounts.

To get a list of RabbitMQ usernames and passwords, run the following command:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

To restore RabbitMQ user accounts, refer to *Task 2 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL* in Post Upgrade Tasks.

For Bluecoat Event Sources

Bluecoat ProxySG event sources use FTPS protocol to upload log files to the Log Collector (LC) and Virtual Log Collector (VLC). The event source documentation contains the steps to configure VSFTPD service on the LC and VLC.

- If key material exists in `/root/vsftpd/` directory in 10.6.5.x, this material area will be backed up and restored. **If the material was in another location, you must back it up and restore it manually.**
- If the `/etc/vsftpd/vsftpd.conf` file exits in 10.6.5.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to ensure that you provide adequate space for the backup so that the backup captures all your data.

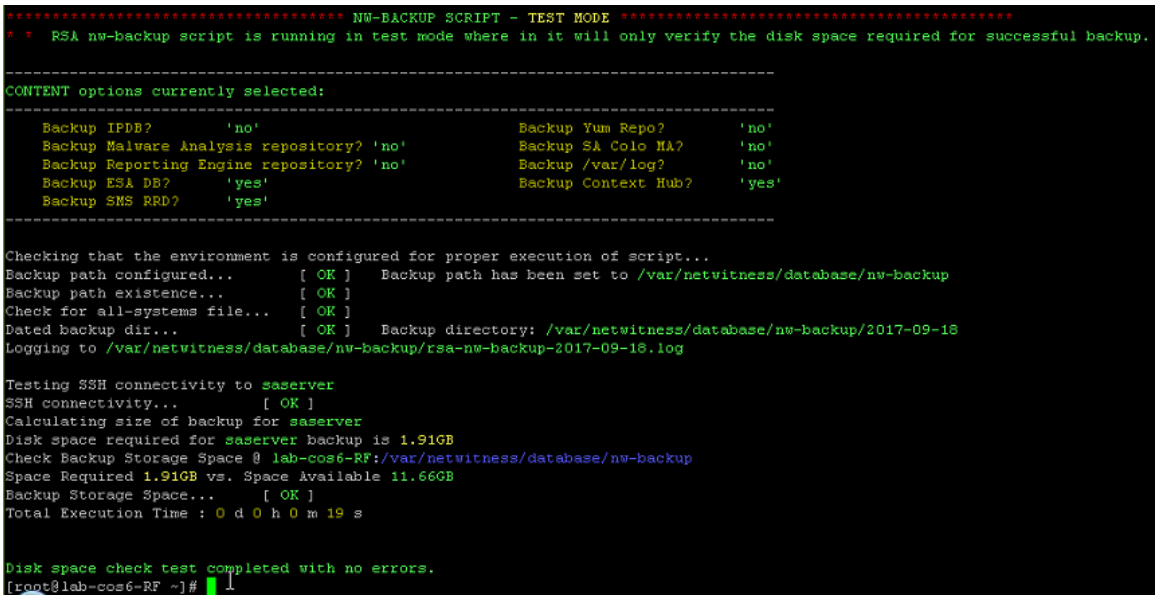
To check for adequate disk space:

1. Make the backup script executable by running the following command:
   ```
   chmod u+x nw-backup.sh
   ```
2. Run the following command at the root directory level:
   ```
   ./nw-backup.sh -t
   ```
   The output displays the amount of disk space that is required for the backup.

   Note: The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-d` option by using `-D`. Using the `-D` option will show how much

space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

The following figure shows an example of the output from using the `-t` option.



Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.1.0.0.

Note: The script will stop services as it runs. However, you can stop services manually before you run the script if needed.

When you run the backup script, you can choose from several options that are described in the following sections.

Usage:

```
./nw-backup.sh [-u -t -d -D -u -l -x -e <external-mnt> -b <backup file path>
```

General Options

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)

-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)

-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)

-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)

-x : move all backup files to an external mount point. Default: (no) -COPY

-b <path to write backups> : path to the location for storing backup files on a backup server. **For upgrading to 11.0, please use the default location!** Default: (/var/netwitness/database/nw-backup)

Note: Do **not** change the backup path in upgrade (-u) mode.

Advanced Content Selection Options

-c : back up Colocated Malware Analysis on SA servers. Default: (no)

-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)

-m : back up Malware Analysis File Repository. Default: (no)

-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)

-v : back up system logs (/var/log). Default: (no)

-y : back up YUM Web Server & RPM Repository. Default: (no)

-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)

-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)

-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)

Test Options

-t : performs script test run for disk space check only. Services are not stopped and excludes execution of backup. Can be combined with (-d) or (-D) and other flags. Default: (-t)

For example, the command:
`./nw-backup.sh`
would run the backup with options as set in the Header of the script itself.
OR, the command:
`./nw-backup.sh -ue /mnt/external_backup`
would run a normal backup using the backup path defined in the script, with the following options:

```
-u : enables the upgrade flag to run backup for upgrading to 11.1. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

When you run the script, the following text is displayed at the top of the script:

```
Caution: RSA nw-backup script backs up configuration files, data, and
logs on the options provided in the script. It tars the content, with
options to store the backup files on the backup server, move or copy
them to external storage on a mount point (USB/NFS/SMB), or SCP them
back to the target host.
This backup script has been qualified on the following versions of
Security Analytics:
10.6.3.x and 10.6.4.x
Use of this script on any other versions of the product may not give
expected results and may not be supported by RSA Customer
Service.Note: All non-RSA custom files, scripts, Cronjobs and other
important files should be placed in /root, /home/'user', OR /etc to be
included in the backup.
```

To run the backup script to back up your hosts:

1. Ensure that the `all-systems` file contains only the hosts to back up.
2. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
3. Begin the backup process by running the following command at the root directory level:
   `./nw-backup.sh -u <additional options as needed>`

   Note: You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.1.0.0.

   When the text "`Backup completed with no errors`" is displayed, the backup has completed successfully.

   A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:
   `rsa-nw-backup-2017-03-15.log`
4. When the backup has completed, to ensure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   The following archive files are created:

   For all hosts:

   `<hostname-IPaddress>-root.tar.gz`

<hostname-IPaddress>-backup.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

For NetWitness Servers:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

For ESA Hosts:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

<hostname-IPaddress>-controldata-mongodb.tar.gz

tar checksum files

<hostname-IPaddress>-network.info.txt

The archived files are located in the /var/netwitness/database/nw-backup directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

Post Backup Tasks

Task 1 - Save a Copy of the all-systems File and the Backup Tar files

Make copies of the all-systems file, the all-systems-master-copy file, and the backup tar files and put the copies in a secure location. You cannot regenerate these files after you upgrade the NetWitness Server (specifically the Admin service) to 11.1.0.0.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.1.0.0 upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

The following files are generated on all hosts by the backup scripts:

- all-systems
- all-systems-master-copy
- appliance_info

- service_info
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

In addition to the files listed above, the following files will be generated on NetWitness Server and ESA hosts:

- <*hostname*>-<*host IP address*>-mongodb.tar.gz
- <*hostname*>-<*host IP address*>-mongodb.tar.gz.sha256

The backup script will also generate the following controldata-mongodb.tar.gz files.

Note: The backup script copies the following files from all ESA hosts to the NetWitness Server host's backup path .

- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz
- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256

Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host

If you have multiple ESA host systems in your enterprise, copy the following two files from each ESA host to the /opt/rsa/database/nw-backup/ directory on the Primary ESA host system (the host that has the ContextHub service running on it) :

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Task 4 - Ensure All Required Backup Files are on Each Host

Before you upgrade to 11.1.0.0, ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

Note: The default paths for backup files are:
- NetWitness Server hosts:/var/netwitness/database/nw-backup
- ESA hosts:/opt/rsa/database/nw-backup

Required Files for NetWitness Servers

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256

Required Files for ESA Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Required Files for All Other Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz

- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Note: The following files are located in the `<hostname>-<host-IP-address>-backup.tar.gz` tar on all hosts:
`appliance_info`
`service_info`

Note: The paths to the location of the backup and restore files for iptables, NAT configurations, user accounts, and crontab entries are shown in the following list:
Backup paths:
`BUPATH=/opt/rsa/database/nw-backup` for the ESA Correlation Engine
`BUPATH=/var/lib/rsamalware/nw-backup` for the Malware Service
`BUPATH=/var/netwitness/database/nw-backup` for all other services
Restore locations:
`BUPATH/restore/etc/sysconfig` for Iptable rules
`BUPATH/restore/etc/sysconfig` for NAT configurations
`BUPATH/restore/etc` for Crontab entries
`BUPATH/restore/etc` for User Accounts (users are located in the `passwd` file, and groups are located in the `group` file. These are not restored during the upgrade process but can be restored manually.
`BUPATH/restore/etc/ntp.conf` for NTP configurations (must be restored using the NetWitness Suite UI)

Migrate Disk Drives from 10.6.5.x to 11.1

These instructions tell you how to upgrade Azure NetWitness VMs from 10.6.5.x to 11.1.0.0 on Azure Cloud Platform.

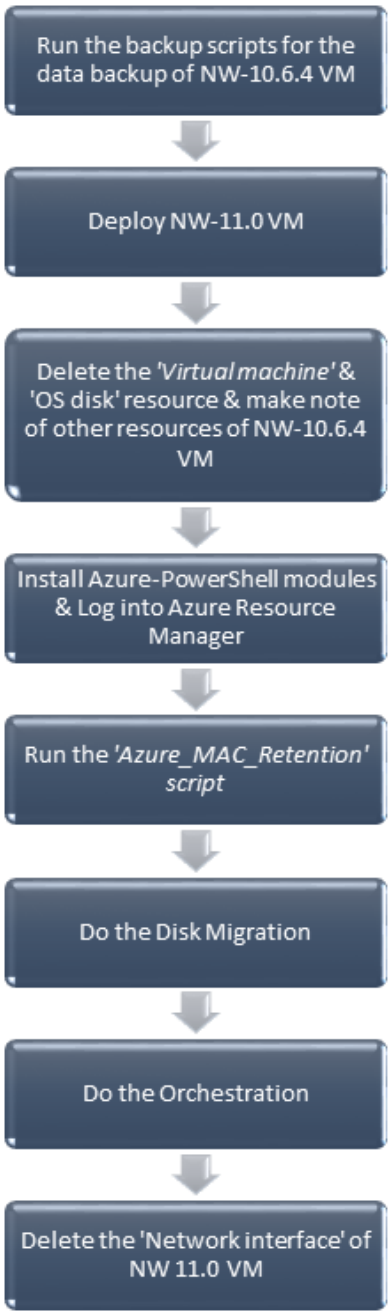
Prerequisites:

- Download and install the latest version of Azure PowerShell from https://github.com/Azure/azure-powershell/releases on a Windows machine.
- Upload the same latest version of Azure modules in automation account. [https://docs.microsoft.com/en-us/azure/automation/automation-update-azure-modules]

Note: Azure PowerShell 4.4.1 was used for qualification.

Note: Both versions of VMs must be on the same Virtual Network and Resource Group for the migration.

Caution: 1) You cannot perform the migration if you have a snapshot for your VM.
2). Run the backup immediately before you upgrade hosts for each phase so that the data is not out-dated.
3.) This guide applies to virtual host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.



Complete the following tasks to migrate your Virtual Machine (VM) deployment disk drives from 10.6.5.x to 11.1:

Task 1 - Deploy NW 11.1 VM

Task 2 - Delete Virtual Machine and OS disk resource of NW 10.6.5 VM

Task 3 - Install Azure PowerShell modules on a local Windows machine

Task 4 - IP Retention: Run the PowerShell script

Task 5 - Perform Disk Migration

Task 6 - Data Restoration

Task 1 - Deploy NW 11.1 VM

1. Deploy NW 11.1 VMs. [Refer to the Azure deployment guide for v 11.1.0.0.
2. Power OFF all the NW 10.6.5 and 11.1 VMs.
3. In the Azure Portal, navigate to Virtual machines.
4. Click on the <Name_of_the_VM>.
5. Click Overview and then click Stop.

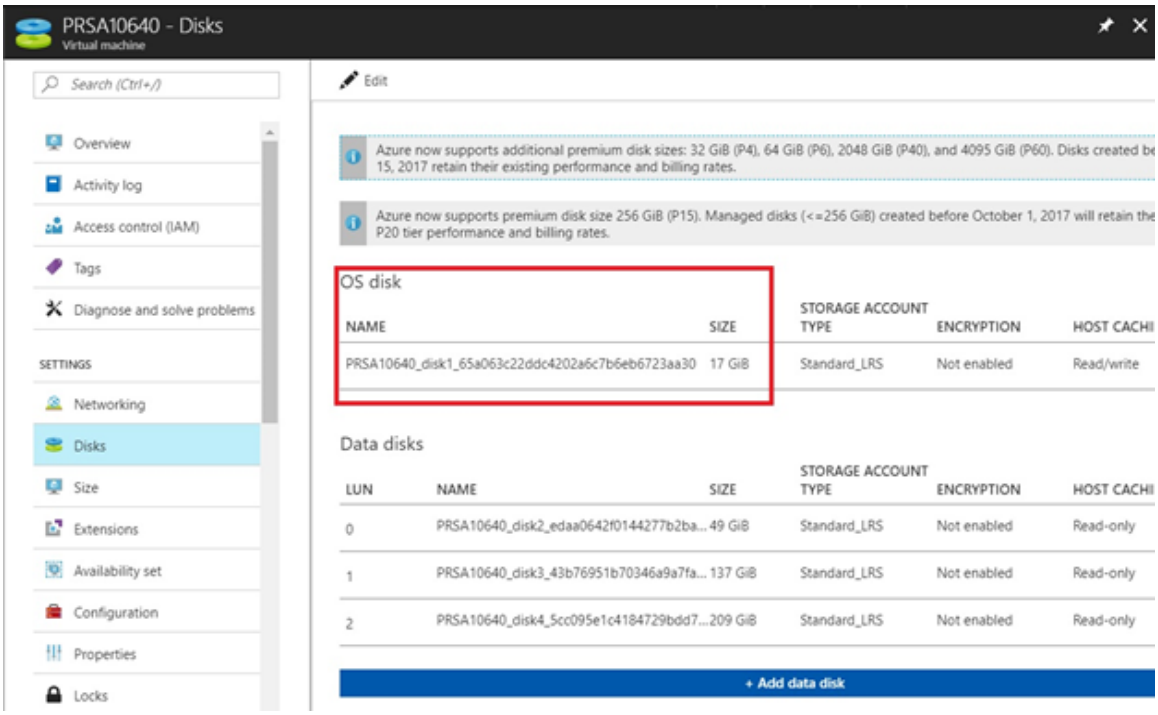
Task 2 - Delete Virtual Machine and OS disk resource of NW 10.6.5 VM

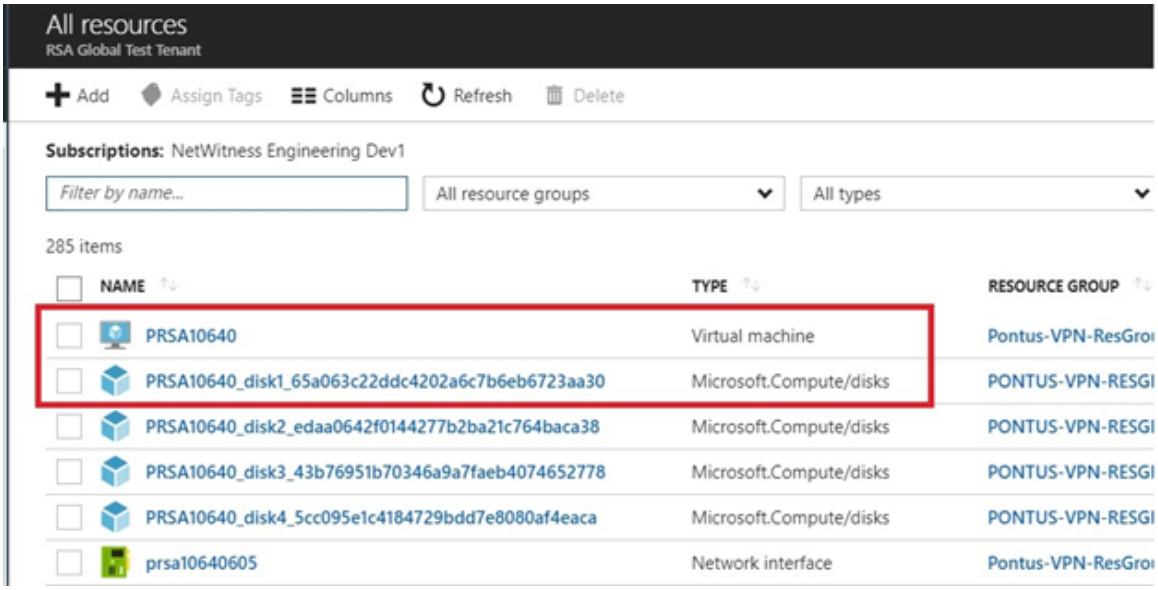
Note the other resources like Data disks and Network Interface.

1. Delete the ‘Virtual machine’ and the 'OS disk' (usually disk1 of VM) resource of NW 10.6.5 VM and make a note of these Network interface and Data disks.

Note: Delete only these 2 resources and retain all other resources of NW 10.6.5 VMs like 'Network interface', 'Network security group' and 'Data disks') and make a note of these 'Network interface' and 'Data disks'.

2. In the Azure Portal, navigate to All resources. Select the Name_of_NW_10.6.5_VM.
3. Click Delete.


PRSA10640 - Disks
Virtual machine
Search (Ctrl+/)
Edit
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Networking
Disks
Size
Extensions
Availability set
Configuration
Properties
Locks
Azure now supports additional premium disk sizes: 32 GiB (P4), 64 GiB (P6), 2048 GiB (P40), and 4095 GiB (P60). Disks created be
15, 2017 retain their existing performance and billing rates.
Azure now supports premium disk size 256 GiB (P15). Managed disks (<=256 GiB) created before October 1, 2017 will retain the
P20 tier performance and billing rates.
OS disk
NAME
SIZE
STORAGE ACCOUNT TYPE
ENCRYPTION
HOST CACHI
PRSA10640_disk1_65a063c22ddc4202a6c7b6eb6723aa30
17 GiB
Standard_LRS
Not enabled
Read/write
Data disks
LUN
NAME
SIZE
STORAGE ACCOUNT TYPE
ENCRYPTION
HOST CACHI
0
PRSA10640_disk2_edaa0642f0144277b2ba...
49 GiB
Standard_LRS
Not enabled
Read-only
1
PRSA10640_disk3_43b76951b70346a9a7fa...
137 GiB
Standard_LRS
Not enabled
Read-only
2
PRSA10640_disk4_5cc095e1c4184729bdd7...
209 GiB
Standard_LRS
Not enabled
Read-only
+ Add data disk


All resources
RSA Global Test Tenant
Add
Assign Tags
Columns
Refresh
Delete
Subscriptions: NetWitness Engineering Dev1
Filter by name...
All resource groups
All types
285 items
NAME
TYPE
RESOURCE GROUP
PRSA10640
Virtual machine
Pontus-VPN-ResGro
PRSA10640_disk1_65a063c22ddc4202a6c7b6eb6723aa30
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk2_edaa0642f0144277b2ba21c764baca38
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk3_43b76951b70346a9a7faeb4074652778
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk4_5cc095e1c4184729bdd7e8080af4eaca
Microsoft.Compute/disks
PONTUS-VPN-RESGI
prsa10640605
Network interface
Pontus-VPN-ResGro

Task 3 - Install Azure PowerShell modules on a local Windows machine

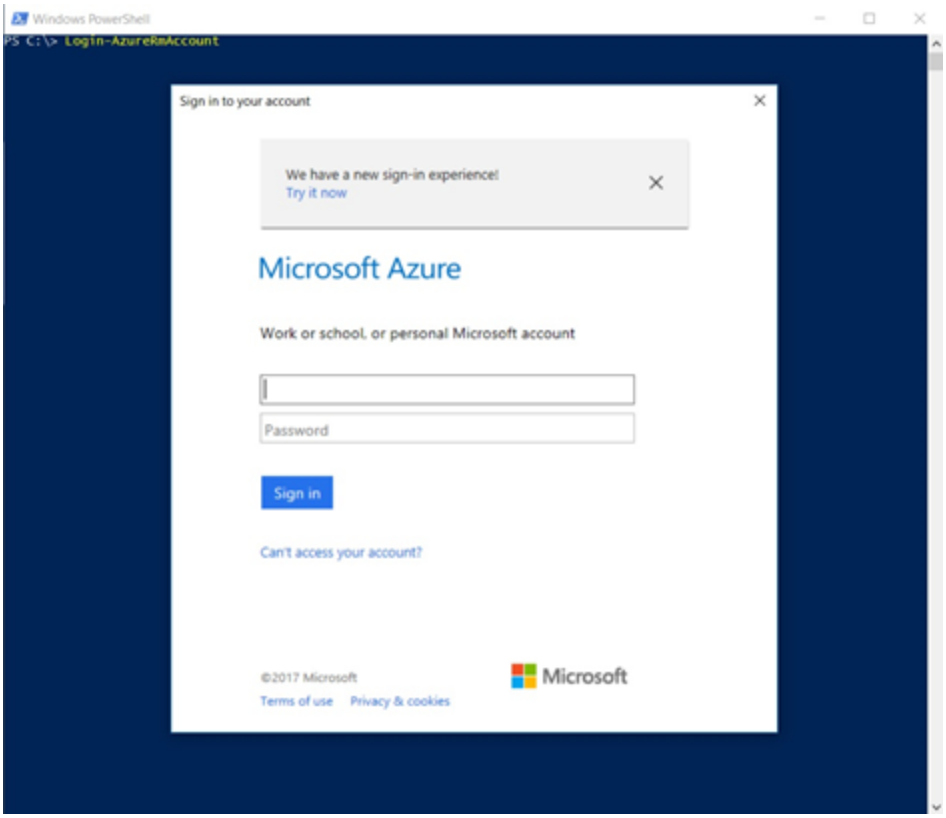
Install the Azure PowerShell modules on a local Windows machine and Login to Azure Resource Manager.

Navigate to Azure PowerShell on the Windows machine where you have installed the Azure PowerShell modules and log in to Azure Resource Manager using the below command

Note: Make sure you have followed the steps mentioned in the Prerequisites section above before executing the below command.

```
Login-AzureRmAccount
```

Login using the Azure credentials in the window that appears.



Task 4 - IP Retention: Run the PowerShell script

Run the PowerShell script for MAC retention for all NW Components. MAC address and IP retention:

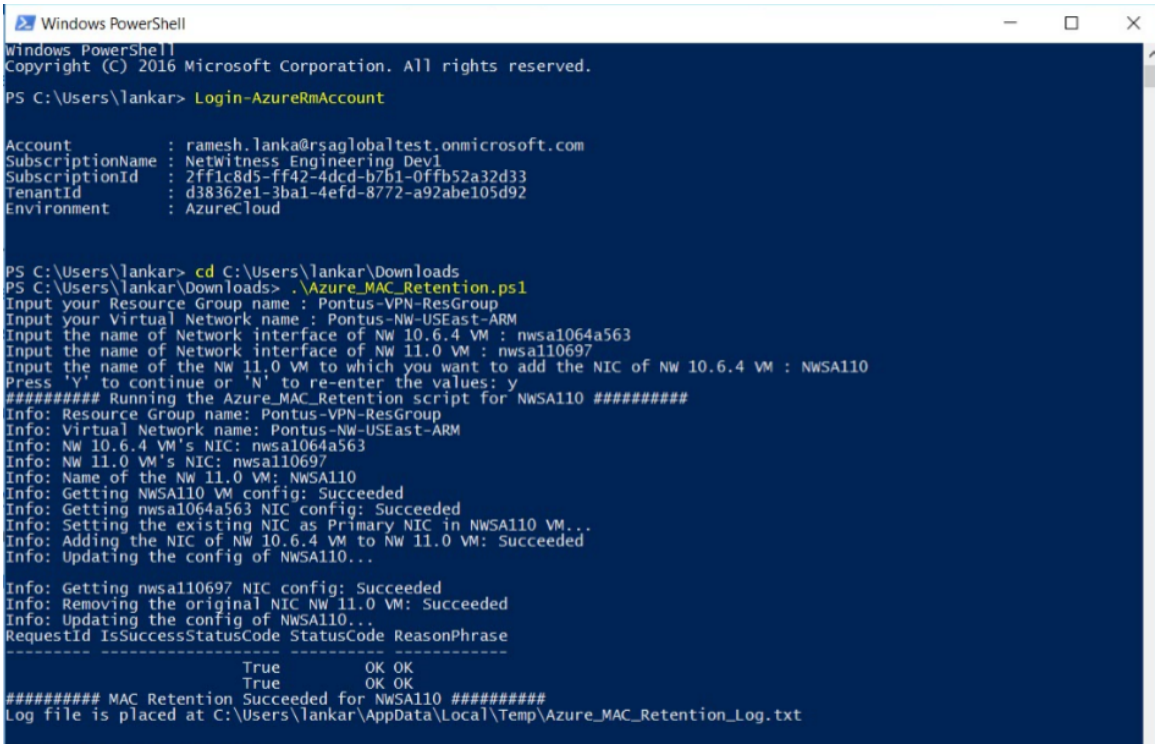
MAC address and IP are bound to the 'Network interface' resource of a VM.

The Azure portal doesn't allow us to

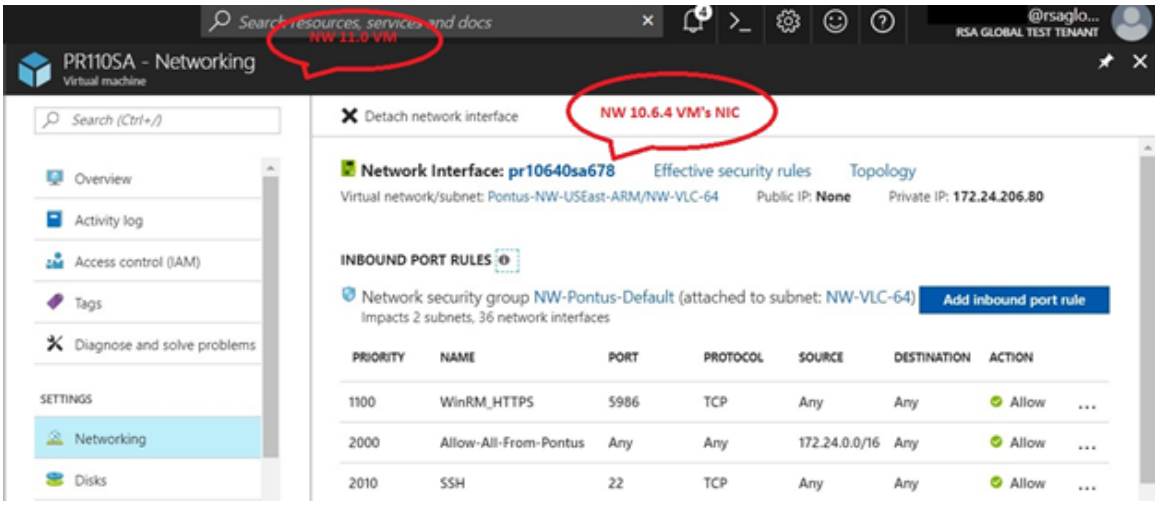
- Specify an existing network interface to add when creating the VM
- Create a VM with multiple network interfaces
- Specify a name for the network interface (the portal creates the network interface with a default name)

This can be achieved using the Azure PowerShell. [https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm]

Click here to download and run the script by providing the requested parameters on the Windows machine installed with Azure PowerShell to retain the 'Network interface' from NW 10.6.5 VM to 11.1 VM.



You should be able to see NW 10.6.5 VM's NIC attached to 11.1 VM under 'Networking' settings after successful execution of the script.

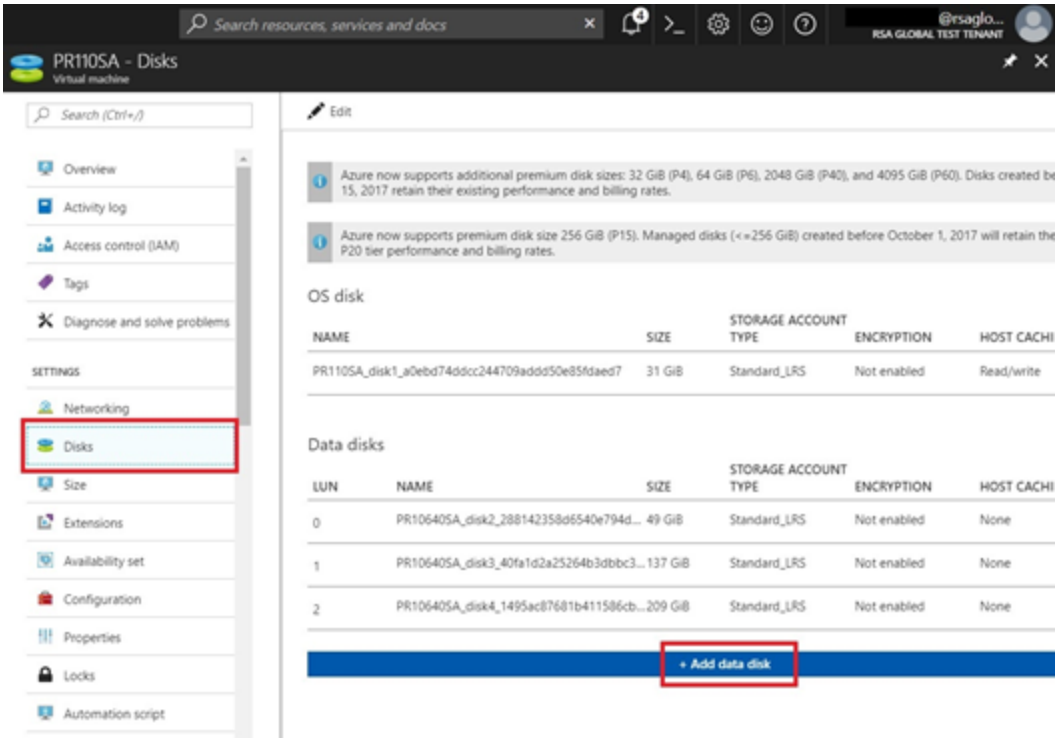


Task 5 - Perform Disk Migration

Add all the disks (except the 'OS disk') of NW 10.6.5 VM to the corresponding NW 11.1 VM under the ‘Disks’ settings.

In Azure Portal, navigate to Virtual machines and then Name_of_the_11.1_VM. Click **Disks** and then click + **Add data disk**. Select all disks of corresponding NW-10.6.5 VM which you had noted down earlier in the dropdown list that appears.

Click **Save**.



Power ON the NW 11.1 VM and login with the credentials provided during VM deployment and set the root password as netwitness.

Task 6 - Data Restoration

Copy NW 10.6.5 VM's backed up data (nw-backup) to NW 11.1 VM.

Note: Do the Data Restoration for SA Server first followed by other components

For SA, LD/LC, Virtual Log Collector, Concentrator, Archiver, Broker:

1. Create a directory under `/tmp/` by the name `nwhome`.
2. Mount `VolGroup00-nwhome` on `/tmp/nwhome/`.

```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

3. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`

```
cp -R /tmp/nwhome/* /var/netwitness/
```

4. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`

```
umount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

For ESA:

1. Create a directory under `/tmp/` by the name apps.
2. Mount `VolGroup01-apps` temporarily on `/tmp/apps/`

```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
```

3. Copy `nw-backup` directory from here to `/var/netwitness`

```
cp -r /tmp/apps/database/nw-backup /var/netwitness
```

4. Unmount `VolGroup01-apps` from `/tmp/apps/`

```
umount /tmp/apps/
```

Perform disk mounting by running the below commands:

For NW Server:

```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Add below entries for these mounts in `/etc/fstab`:

```
/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs defaults,noatime,nosuid 1 2
```

For LogDecoder/LogCollector:

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
```

mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb

mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb

mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector

mount /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb

Add below entries for these mounts in `/etc/fstab`:

/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4 defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb xfs defaults,noatime,nosuid 1 2

For Virtual LogCollector:

mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector

Add below entry for these mounts in `/etc/fstab`:

```
/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs defaults,noatime,nosuid 1 2
```

For Concentrator:

mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator

mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb

mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index

mount /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb

Add below entries for these mounts in `/etc/fstab`:

/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4 defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime 1 2

/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb xfs defaults,noatime,nosuid 1 2

For Archiver:

mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver

mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench

Add below entries for these mounts in `/etc/fstab`:

/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs defaults,nosuid,noatime 1 2

/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs defaults,nosuid,noatime 1 2

For Broker:

mount /dev/mapper/VolGroup01-broker /var/netwitness/broker

Add below entry for these mounts in `/etc/fstab`:

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
defaults,nosuid,noatime 1 2
```

Task 7 - Delete all NW 11.1 Deployment 'Network interface' Resources

1. In Azure Portal, go to All resources.
2. Click on <Name_of_NW_11.1_Network_interface> and select Delete.

Set Up Virtual Hosts in 11.1

There two phases to set up your 11.1 virtual stack that you must complete in the order shown.

- Phase 1 - Set Up NW Server, Event Stream Analysis, and Broker or Concentrator Hosts

  Note: For Event Stream Analysis, if you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

- Phase 2 - Set Up The Rest of the Component Hosts

Phase 1 - Set Up NW Server, Event Stream Analysis, and Broker or Concentrator Hosts

Task 1 - Set Up 11.1 NetWitness Server

Follow the instructions under Set Up 11.1 NW Server Host.

Task 2 - Setup 11.1 ESA

Caution: If you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.1 Non-NW Server Host to set up your ESA hosts.

1. Set up your primary ESA host through the Setup program and install **ESA Primary** on the host in the user interface on the **Admin Hosts** view.

   Note: If you have multiple ESA hosts in your enterprise, you must upgrade the ESA Primary host, where all the `mongodb` (Mongo Database) backup tar files are located, first, before you upgrade ESA Secondary hosts.

2. (Conditional) If you have a secondary ESA host, set it up through the Setup program and install **ESA Secondary** on the host in the user interface on the **Admin Hosts** view.

Task 3 - Set Up 11.1 Broker or Concentrator

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Set Up The Rest of the Component Hosts

See Appendix B. Stopping and Restarting Data Capture and Aggregation for instructions on how to stop and restart data capture and aggregation when upgrading the Decoder, Concentrator, and Log Collection hosts.

Concentrator Hosts

1. Stop data capture and aggregation.
2. Complete the steps in Set Up 11.1 Non-NW Server Host.
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh.
2. Stop data capture on the Log Decoder.
3. Complete the steps in Set Up 11.1 Non-NW Server Host.
4. Restart data capture on Log Decoder.

   Note: After you upgrade, you will restart log collection after completing the Task 11 - Reset Stable System Values for Log Collector after Upgrade in the **Post Upgrade Tasks**

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described in the Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh.
2. Back up your 10.6.5.x VLC by editing the `all-systems` file on host where you performed the backup.

   a. Make sure your `all-systems` file contents has this information before you perform this step.

   ```
   vlc,<host-name>,<IP-address>,<UUID>,10.6.5.0
   ```

   b. Run the following command to create backup.

```
./nw-backup.sh -u
```

See Backup Instructions for detailed procedures on how to back up the host.

3. Make sure the backup host contains the VLC backup in the following format.

```
<hostname>-<IPaddress>-root.tar.gz
<hostname>-<IPaddress>-root.tar.gz.sha256
<hostname>-<IPaddress>-backup.tar.gz
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```

4. Power off the 10.6.5.x VLC so that a new 11.1 VM can be created with the same network configuration.
5. Deploy a fresh Non-NW Server host using the 11.1 NetWitness Suite ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.5.x VLC.
   This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.5.x VLC backup file.

   Note: Make sure IPv6 is disabled.

   a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings. Contents of `ifcfg-eth0` should be as follows.

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

   b. Submit the following command string.

```
systemctl restart network.service
```

8. Create the backup directory.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new VLC in the `/var/netwitness/database/nw-backup` directory.
10. Complete the steps 2 through 12 inclusive in Set Up 11.1 Non-SA Server Host for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

Set Up 11.1 NW Server Host

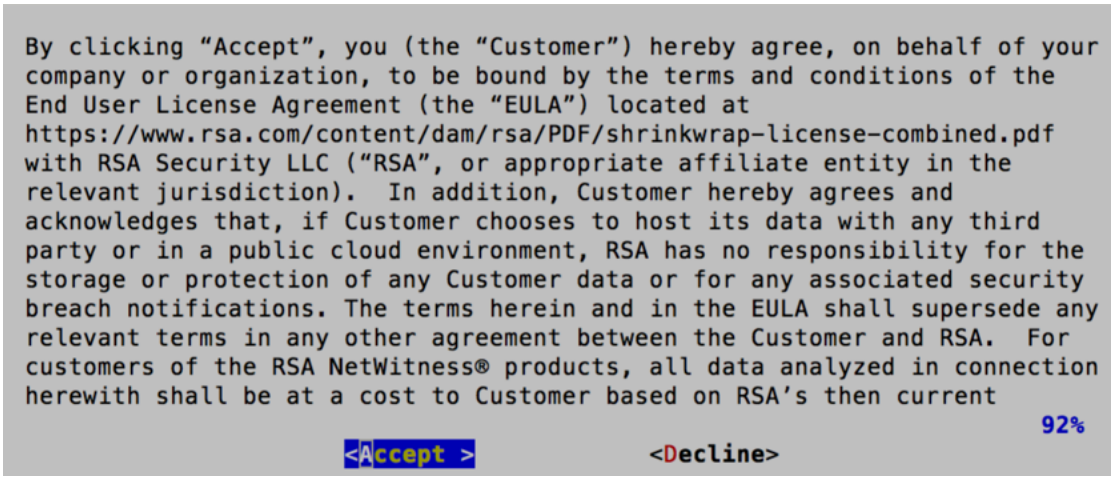
Make sure that you have backed up 10.6.5.x data for the SA Server host. **You must follow the instructions in** Backup Instructions **to back up the host.**

Caution: Run the backup immediately before upgrading the SA Server to 11.1 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.1.

Complete the following steps to set up the 11.1 NW Server host.

1. Power on the NW Server VM and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

   Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press the Enter key to register your command response and move to the next prompt.
   2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

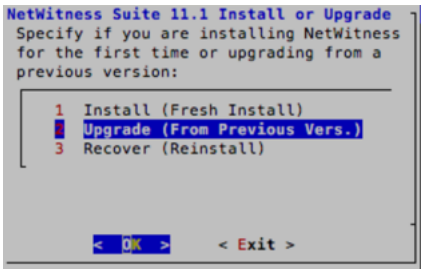
2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

3. Tab to **Yes** and press **Enter**.

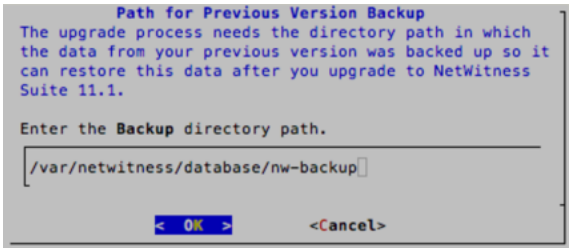
   Choose No if you already upgraded the NW Server to 11.1.

   The Install or Upgrade prompt is displayed.



4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.

   The backup path prompt is displayed.



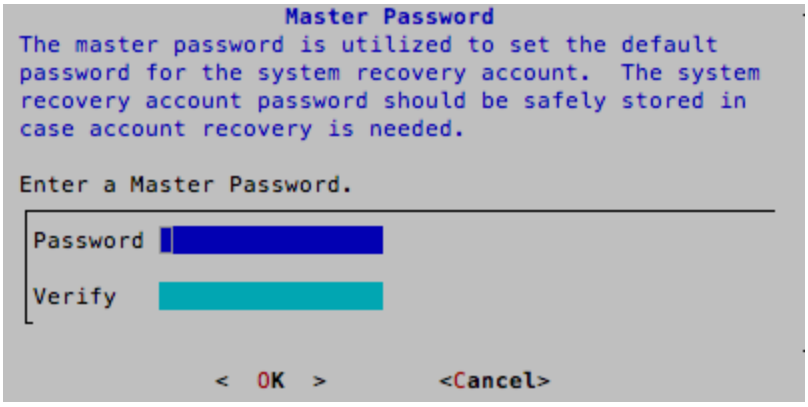
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.

   The Master Password prompt is displayed.

   The following list of characters are supported for Master Password and Deployment Password:

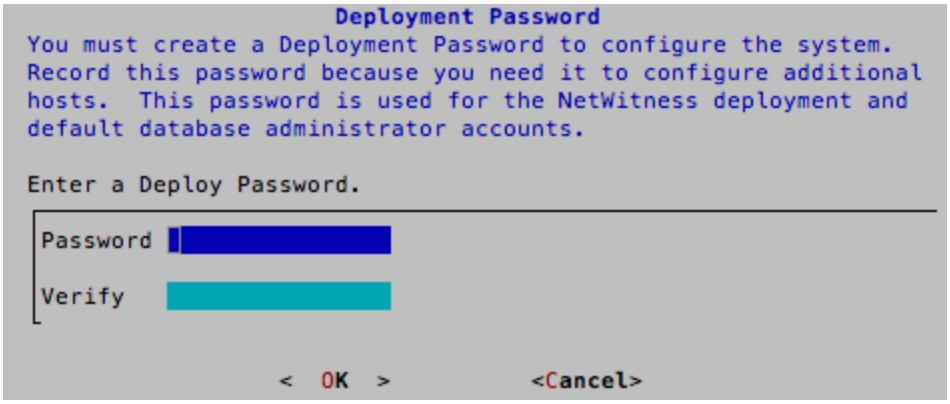
   - Symbols : ! @ # % ^ +,
   - Numbers :0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z

No ambiguous characters are supported for Master Password and Deployment Password (for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -).



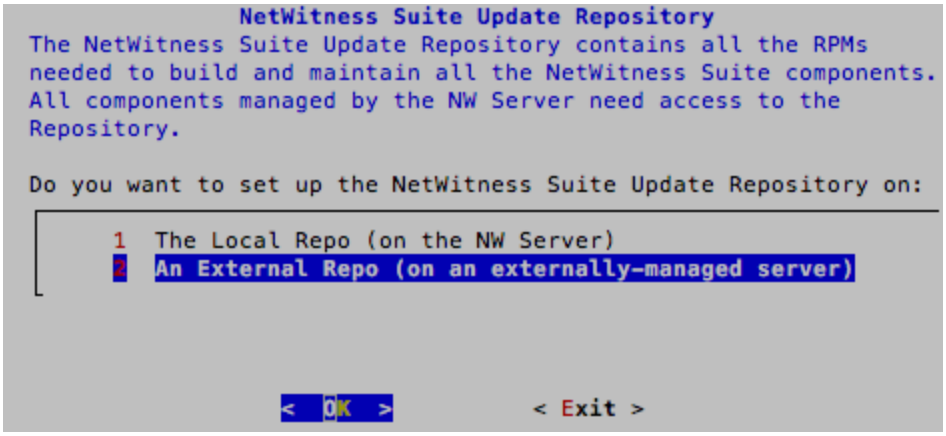
6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   The Deployment Password prompt is displayed.



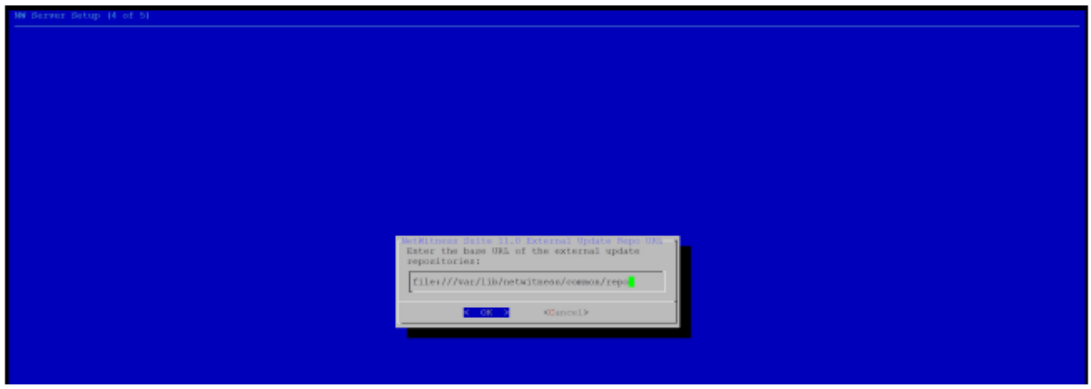
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   The Update Repo prompt is displayed.



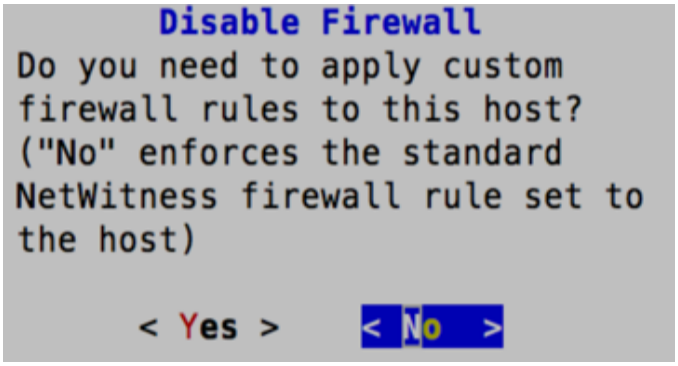
   You must use the same repo that you used for the NW Server hosts for all hosts.

8. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.



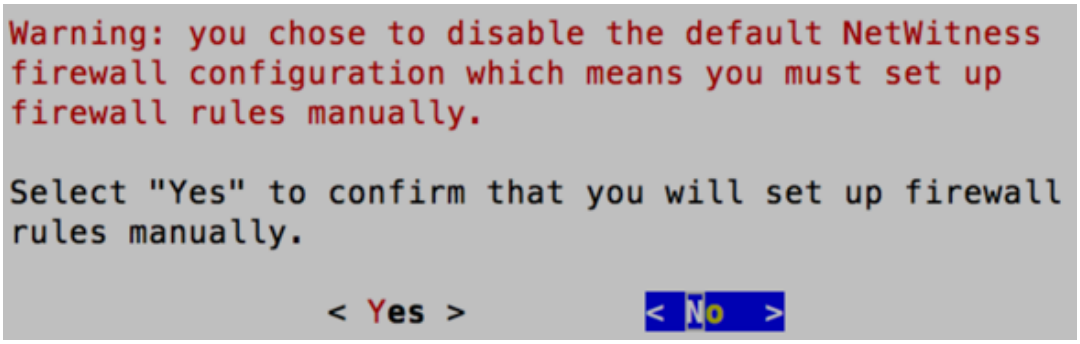
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite 11.1 Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

9. Enter the base URL of the NetWitness Suite external repo and click **OK**.
The disable or use standard firewall configuration prompt is displayed.



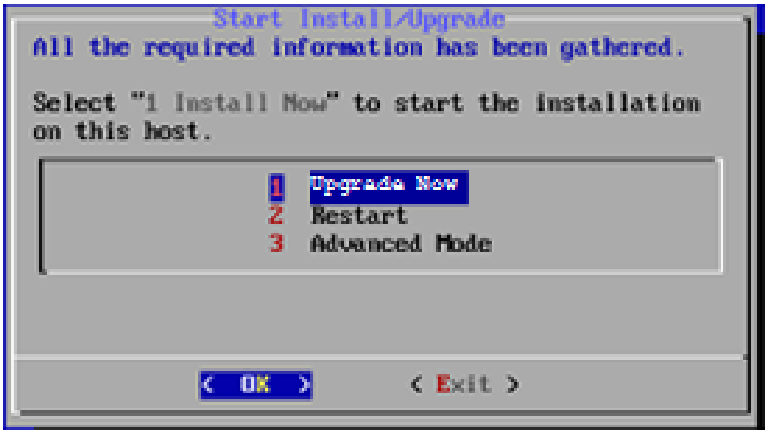
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- If you select Yes, confirm your selection.



- If you select No, the standard firewall configuration is applied.

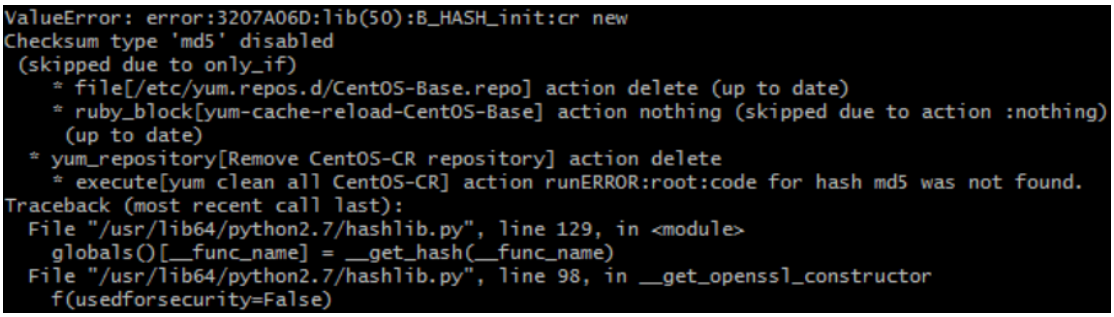
The start upgrade prompt is displayed.



11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.

    When "Installation complete" is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

> **Note:** Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.



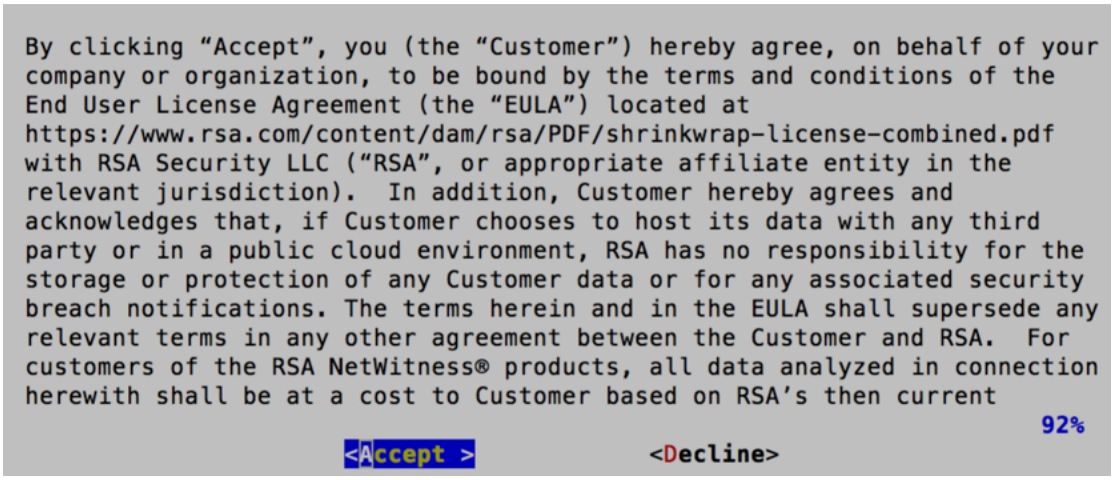
Set Up 11.1 Non-NW Server Host

Make sure that you Back up your 10.6.5.x data for the host. **You must follow the instructions in** Backup Instructions **to back up the host.**

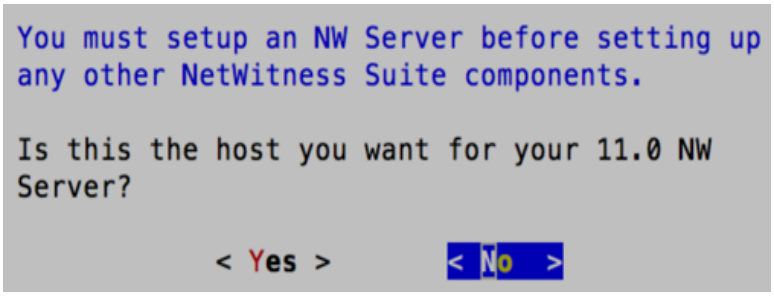
Caution: Run the backup immediately before upgrading the host to 11.1 so that the data is as recent as possible.

Complete the following steps to set up an 11.1 Non-NW Server host.

1. **Power On** the non-NW Server VM and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

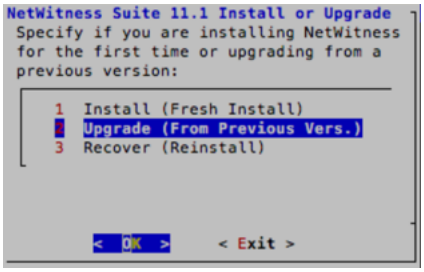


2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

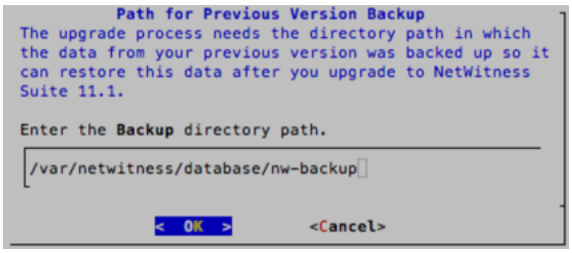


Caution: If you choose the wrong the host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

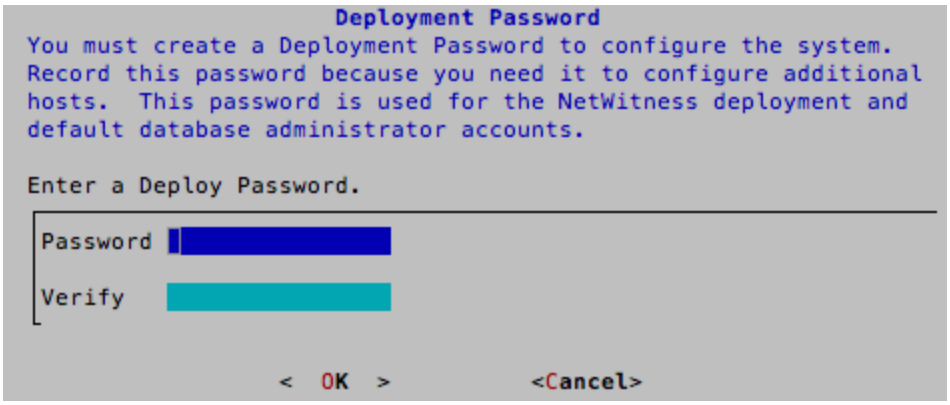
3. Tab to **No** and press **Enter**.
   The Install or Upgrade prompt is displayed.



4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.
   The backup path prompt is displayed.



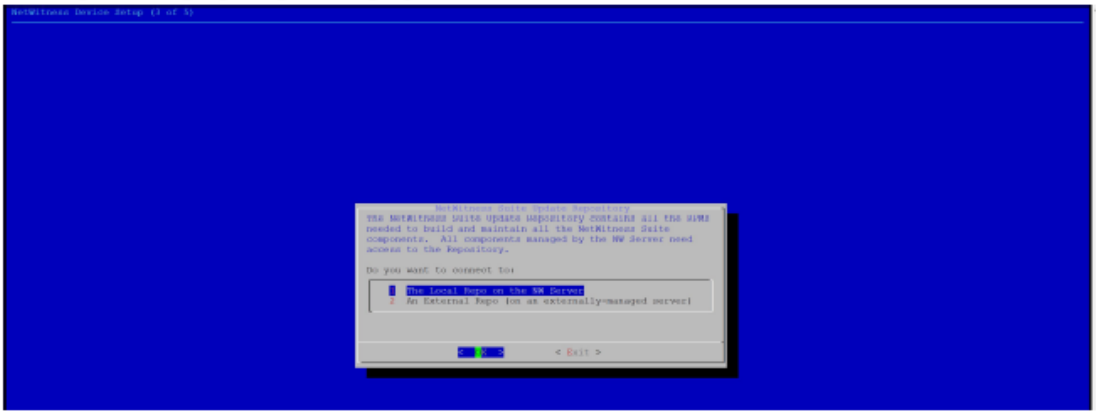
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.
   The Deployment Password prompt is displayed.



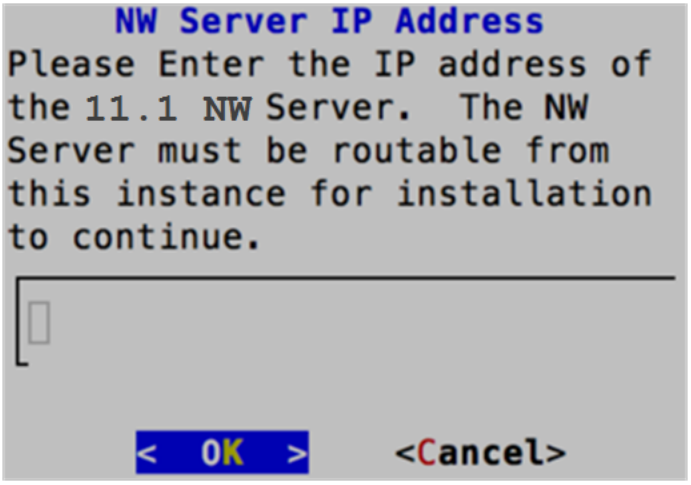
> **Note:** You must use the same deployment password that you used when you upgraded the NW Server.

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

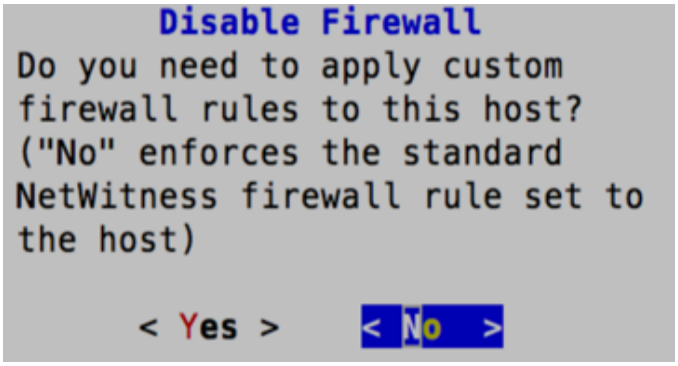
The Update Repo prompt is displayed.



7. Use the down and up arrows to select the **2 The Local Repo (on the NW Server)**, tab to **OK**, and press **Enter**.
8. Enter the base URL of the NetWitness Suite external repo and click **OK**.
   The NW Server IP Address is displayed.

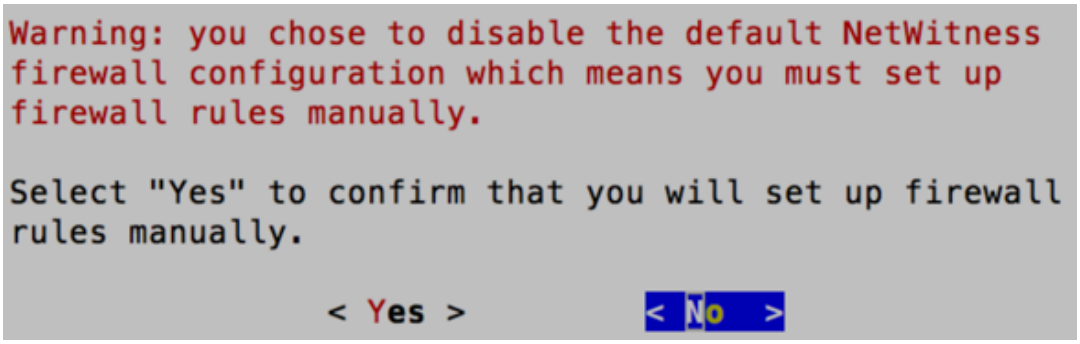


9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.
   The disable or use standard firewall configuration prompt is displayed.



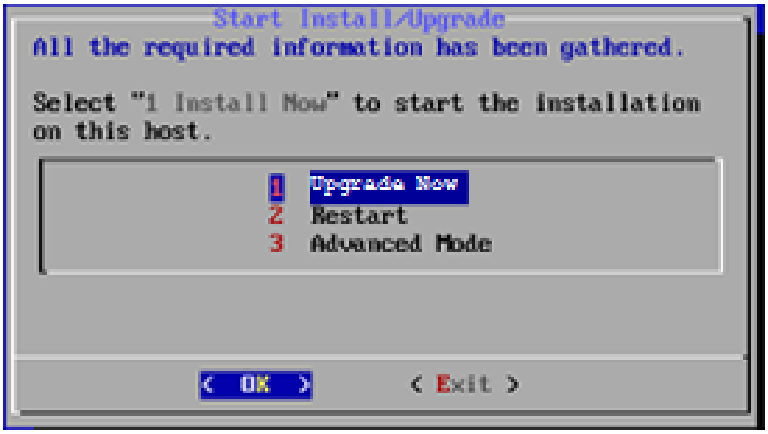
10. Tab to **No**, and press Enter to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

    - If you select **Yes**, confirm your selection.

    - If you select **No**, the standard firewall configuration is applied.

    The start upgrade prompt is displayed.

11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.
    When "Installation complete" is displayed, you have upgraded the host to the 11.1.

12. Install the service on this host:

    a. Log into NetWitness Suite.
    Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Suite Login screen

    b. Click **ADMIN** > **Hosts**.
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

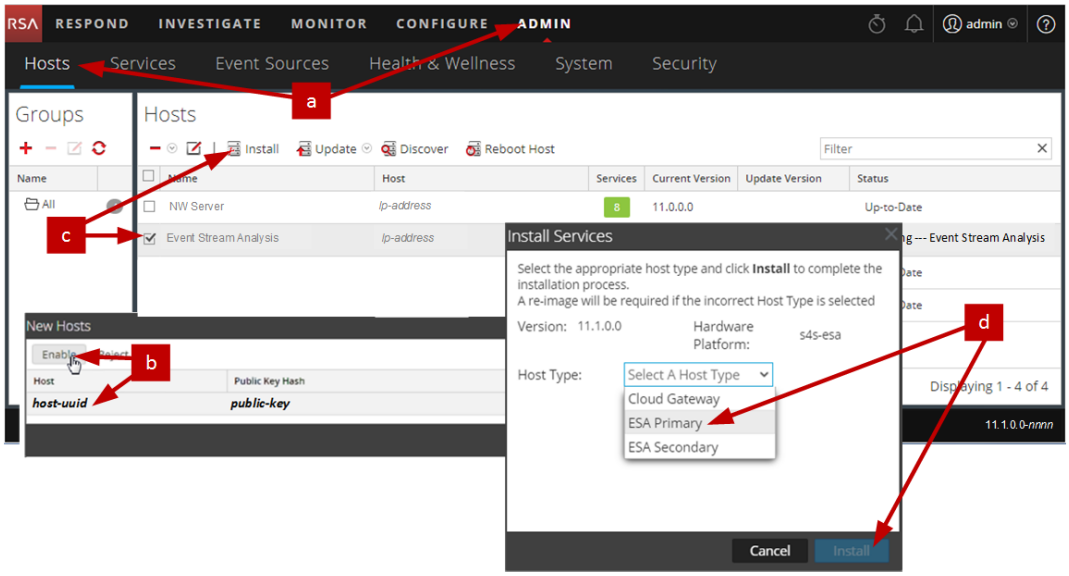
    > **Note:** If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

    c. Click on the host in the **New Hosts** dialog and click **Enable**.
    The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

d. Select that host (for example, **Event Stream Analysis**) and click Install

The **Install Services** dialog is displayed.

e. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



You have completed the upgrade of the non-NW Server host in NetWitness Suite

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.1 Legacy Windows Collection Guide* on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.1. These tasks are organized by the following categories.

- Global
- NetWitness Endpoint
  RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, and 4.4 only for NetWitness Suite 11.1.
- Event Stream Analysis
- Log Collection
- Reporting Engine
- Respond
- NetWitness SecOps Manager
- Security

Global Tasks

Task 1 - Remove Backup-Related Files from Host Local Directories

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.1 before you remove the backup-related files from the local directories on your 11.1 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.1, you must remove:

- the backup files from the local directories on the hosts.
- all the files from `nw-backup` and `restore` directories on the hosts.

Host	Backup Path	Restore Path
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Host	Backup Path	Restore Path
NW Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
All Other Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Task 2 - Restore NTP Servers

You must use the NetWitness Suite 11.1 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *RSA NetWitness® Suite 11.1 System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 3 - Restore Licenses for Environments without FlexNet Operations-On Demand Access

If your environment does not have access to FlexNet Operations-On Demand, you need to re-download your NetWitness Suite licenses. Refer to "Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on how to re-download licenses. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 4 - Remap Virtual NW Server License to 10.6.5.x MAC Address

If you are upgrading a Security Analytics server running on a virtual machine, change the 11.1 NW Server virtual host to the 10.6.5.x MAC address to retain licensing. Refer to "Licensing: Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on remapping a license to a new MAC address." Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

(Conditional) Task 5 - If You Disabled Standard Firewall Config - Add Custom IPtables

During the upgrade, you have the option of using these rules or disabling them. If you disabled them, follow these instructions as a baseline to create a user-managed firewall rule sets on all the hosts for which you disabled the standard firewall configuration.

Note: You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the restore folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.
2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Reload the `iptables` and `ip6tables` services.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditional) Task 6 - Specify SSL Ports If You Never Set Up Trusted Connections

Complete this task only if you never set up Trusted Connections. You would not have set up Trusted Connections if you:

- Used the base ISO image for 10.3.2 or earlier.
- Updated the system using RPMs exclusively to get to 10.6.5.

NetWitness Suite 11.1 cannot communicate with the core services for these customers because they are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

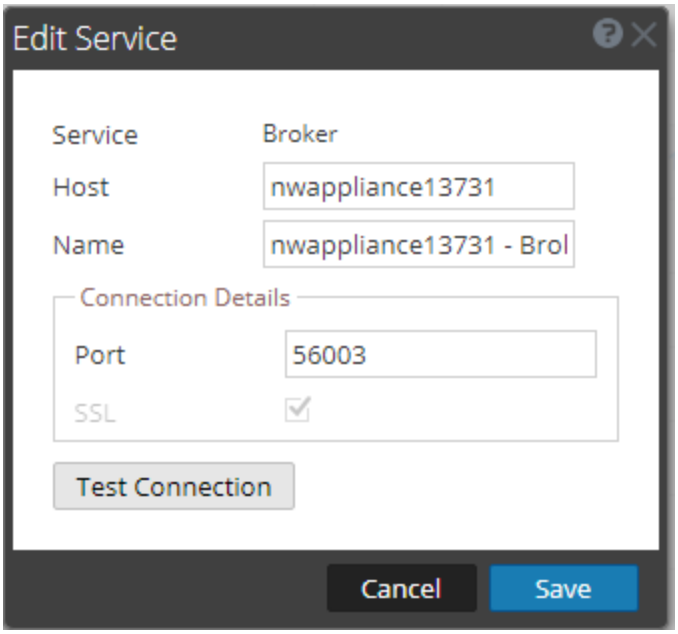
1. Log in to NetWitness Suite
2. Go to **ADMIN** > **Services**.
3. Select each core service and change there ports from Non-SSL to SSL ports.

Service	Non-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

4. Click (Edit) from the **Services** view toolbar.

   The Edit Service dialog is displayed.

5. Change the port from Non-SSL to SSL as shown in the table and click **Save**(for example, change the Broker port from 50003 to 56003).



NetWitness Endpoint

Task 7 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite 11.1, the virtual host is `/rsa/system`. For 10.6.5.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.
3. SSH to the NW Server and log in with `root` credentials.
4. Submit the following command to add all certificates to the truststore.
   `orchestration-cli-client --update-admin-node`
5. Submit the following command to restart the RabbitMQ server.
   `systemctl restart rabbitmq-server`
   The NetWitness Endpoint account should automatically be available on RabbitMQ.

6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Event Stream Analysis Tasks (ESA)

Task 8 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.1.

1. Log in to NetWitness Suite 11.1
2. Click **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
3. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. Click **ADMIN**> **Services**, select the Context Hub service, in the action commands ( ) drop-down menu, click **View** > **Config** > **Lists** tab).
   b. Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Suite ESA Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 9 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL

If you integrate with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint, you must configure Mutually Authenticated SSL on each integrated system so that the application can authenticate itself when connecting to the RabbitMQ message bus.

Note: Use the RabbitMQ usernames and passwords that were obtained when you backed up your 10.6.5.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Suite by logging into the host and running the following `rabbitmqctl` command.

```
> rabbitmqctl add_user <username> <password>
```

For example:

```
> rabbitmqctl add_user wtd-incidents incidents
```

2. Set permissions for users by running the following command (use the username from step 1):
   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*",
   ".*"
   ```
   For example:
   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*",
   ".*", ".*"
   ```

Task 10 - Enable Threat - Malware Indicators Dashboard

In 11.0, the 10.6.5.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.5.x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.1.
2. Set datasource for new dashlets.

   See "Dashlets" in the RSA Link (https://community.rsa.com/docs/DOC-81463).

Log Collection

Task 11 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.0 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

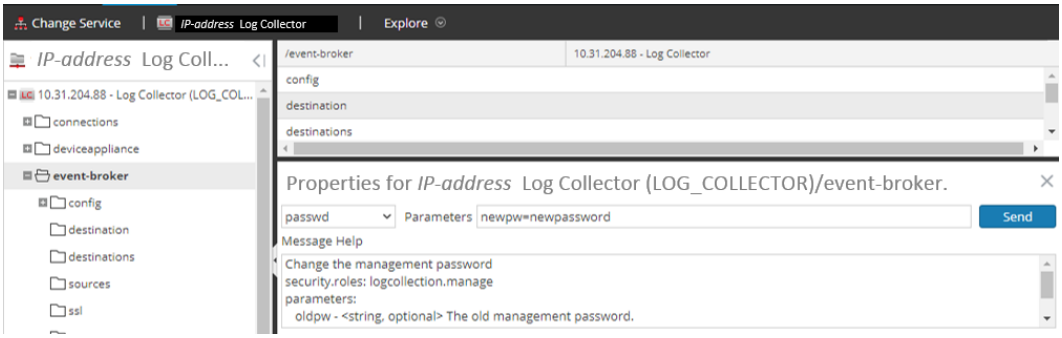
The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Update Log Collector Service RabbitMQ User Account Password

If the logcollector service RabbitMQ user account password was changed, you must reenter it after the 11.0 upgrade.

1. Log in to NetWitness Suite.
2. Click **ADMIN > Services**.
3. Select the Log Collector service.
4. Click (Actions) > **View** > **Explore**.

5. Right click `event-broker` > **Properties**.
6. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 12 - Enable FIPS Mode

FIPS is enabled on all services except Log Collector Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder. For information about how to enable FIPS for these services, see the "Sys Maintenance: Activate or Deactivate FIPS" topic in the *RSA NetWitness® SuiteSystem Maintenance Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Reporting Engine

Task 13 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the back up you made prior to the upgrade. The Backup script backs up the 10.6.5.x CA certificates into the `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts` directory.

Complete the following procedure to restore the CA certificates in 11.1.

1. SSH to the NW Server host.
2. Export the CA certificates.
   `keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file`
3. Copy the CA pem into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 14 - Restore External Storage for Reporting Engine

If you have external storage for the Reporting Engine (such as SAN or NAS for storing reports), you must restore the mount you unlinked before the upgrade. See "Reporting Engine: Add Additional Space for Large Reports" in the *RSA NetWitness® Suite Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

Task 15 - Restore Respond Service Custom Keys

In 10.6.5.x, if you added custom key for use in the groupBy clause, the `alert_rules.json` file was modified. The `alert_rules.json` file contains aggregation rule schema. RSA moved the `alert_rules.json` file to the following new location:
`/var/lib/netwitness/respond-server/scripts`

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.

   This directory is where the `alert_rules.json` file is restored from the 10.6.5.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.0.

   This is the new file for 11.0.

3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 16 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.0 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.x, you must:

1. Go to the to the `/opt/rsa/im/scripts` directory.
   This directory is where the following Respond service normalization scripts are restored from the 10.6.5.x backup.
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Copy any custom logic from the 10.6.5.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Suite 11.0 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
   The `alert_rules.json` file contains aggregation rule schema.

(Conditional) Task 18 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.1. See *Adding Roles and Assigning Permissions for the Roles* in the *RSA NetWitness Suite Warehouse Analytics Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

NetWitness SecOps Manager

Task 19 -Reconfigure NW SecOps Manager Integration

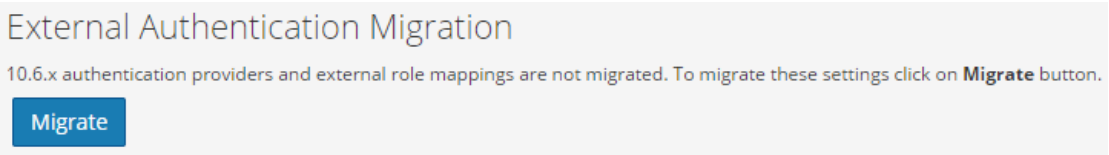
For information on how to reconfigure NW SecOps for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Security

Task 20 - Migrate Active Directory (AD)

The first time you log into the NetWitness Suite 11.1 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Suite with your `admin user` credentials.
2. Click **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.



3. Click **Migrate**.
   The migration is complete and the dialog closes.

Task 21 - Modify Migrated AD Configuration to Upload Certificate

If the you used a self-signed certificate in Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.5.x, you must modify the migrated AD configuration to upload the certificate (either the self-signed cert or the CA cert).

Complete the following procedure to modify the migrated AD configuration to upload the certificate (either the self-signed cert or the CA cert).

1. Log in to NetWitness Suite.
2. Click **ADMIN** > **Security** and click the **Settings** tab.
3. Under **Active Directory Settings**, select an AD configuration and click .
   The Edit Configuration dialog is displayed.
4. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
5. Click **Save**.

Task 23 - Reconfigure Pluggable Authentication Module (PAM) in 11.1

You must reconfigure PAM after you upgrade to 11.1. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite System Security and User Management Guide*for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

You can refer to your 10.6.5.x PAM configuration files in the **/etc** directory in the your 10.6.5.x backup data for guidance.

Appendix A. Troubleshooting

This section describes problems that you may encounter during the upgrade with solutions. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve any upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294)

This section has troubleshooting documentation for the following services, features, and processes.

- 11.1 Setup Program (`nwsetup-tui`)
- Backup
- Event Stream Analysis
- General
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

11.1 Setup Program (nwsetup-tui)

Problem	Host Setup Program (nwsetup-tui) exits and creates the following error message in /var/log/netwitness/bootstrap/launch/security-server/security-server.log: <yyyy-mm-dd hh:mm:ss,nnn> [main] ERROR SystemOperation|Service startup failed. Running in safe mode org.h2.jdbc.JdbcSQLException: The database is read only [90097-193] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) ... at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnection(AbstractDriverBasedDataSource.java:159) at com.rsa.asoc.security.upgrade.legacy.MigrationDatabase.<init>(MigrationDatabase.java:113)
Cause	The H2 database needs write permission to complete the host setup.
Solution	From the NW Server command line, provide write permission to H2.db, restart the NW Server, and restart nwsetup-tui Setup Program. chmod o+w /var/lib/netwitness/uax/db/platform.h2.db systemctl restart rsa-nw-security-server.service nwsetup-tui

Backup (`nw-backup` script)

Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the the *RSA NetWitness® Suite Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESAPrimary host and log in.
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Submit the following command to restart ESA .
	`systemctl restart rsa-nw-esa-server`
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

General

Logs referred to in this section are posted to `/var/log/install/install.log` on the NW Server Host.

Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Suite sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service using below command. `systemctl restart rsa-sms`

Message	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt is nGB` `<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.`
Cause	Low or insufficient disk space allocated for the SMS service.
Solution	RSA recommends that you provide a minimum of 10 GB of disk space for the SMS service to run optimally.

Problem	After you run the Setup Program for a non-NW Server host, you must go in to the UI, enable the host, and install the service on the host from the Hosts View. If you see "Install error View Details" in the **Status** column of the Hosts view, the host lost connectivity due to network issues.
Solution	Re-install the service on the host from the Hosts view.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Suite and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Message	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Suite and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents..

Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Suite and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the sa.log. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.5 to 11.1.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Message	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Appendix B. Stopping and Restarting Data Capture and Aggregation

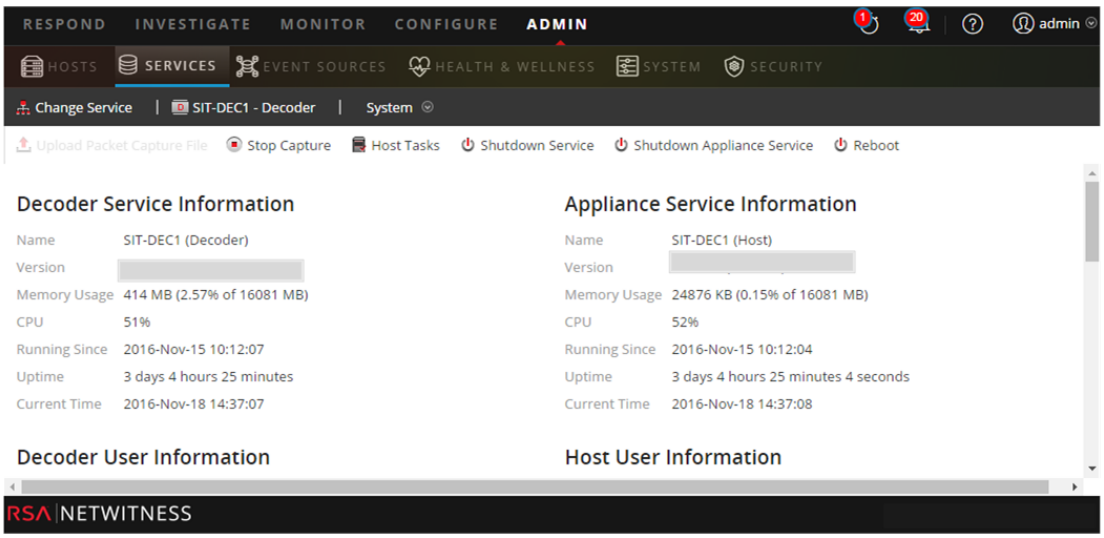
RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.1. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

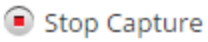
Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.



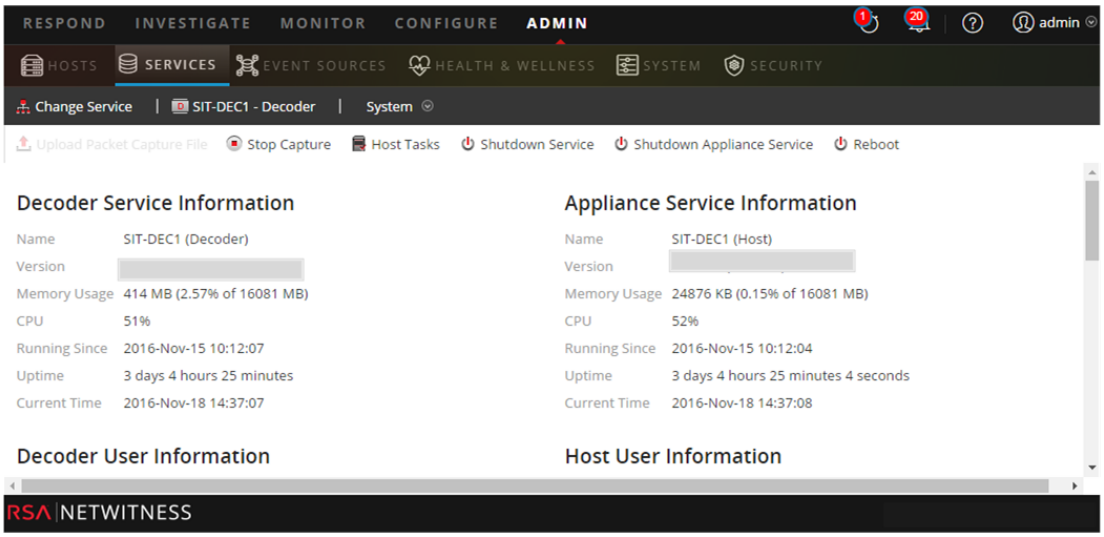
3. Under (actions), select **View** > **System**.
4. In the toolbar, click  .

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.



3. Under (actions), select **View** > **System**.

4. In the toolbar, click

.

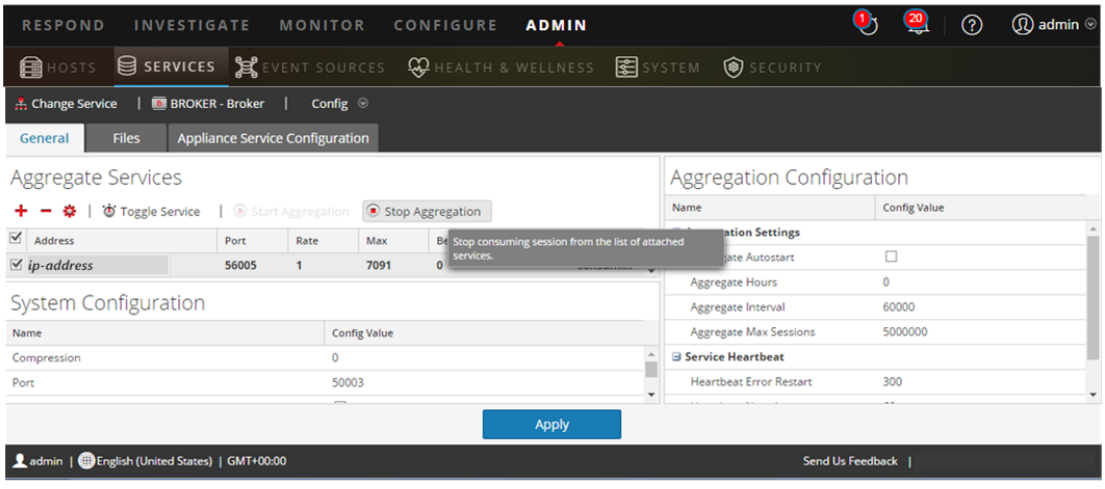
Stop Aggregation

1. Log in to NetWitness Suite and go to **ADMIN** > **Services**.

2. Select the **Broker** service.

3. Under (actions), select **View** > **Config**.

4. The **General** tab is displayed.



5. Under **Aggregated Services** click

.

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Log Capture

To start log capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click .

Start Aggregation

During the upgrade from 10.6.5.x to 11.1, the Broker Service is restarted and this automatically starts aggregation.

Revision History

Revision	Date	Description	Author
1.0	16-Mar-18	Release to Operations	IDD

RSA NETWITNESS® SUITE

Update Guide

for Version 11.0.x to 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2018

Contents

Introduction **5**

Update Path 5

Running in Mixed Mode 5

Update Preparation Tasks **6**

General 6

Task 1 - Review Core Ports and Open Firewall Ports 6

Task 2- Back Up Malware Analysis Configuration File to Another Directory 6

Task 3 - Stop Data Capture and Aggregation 7

Task 4 - Make Sure That deploy_admin User Credentials Are Still Valid (Not Expired) 9

Reporting Engine 10

Task 5 - Configure Reporting Engine for Out-of-the-Box Charts 10

Respond 10

Task 6 - (Conditional) Restore Respond Service Custom Keys 10

Task 7 - Back Up Customized Respond Service Normalization Scripts 10

Task 8 - (Conditional - For Azure Stack) 11

Update Tasks **12**

Apply Updates from the Hosts View (Web Access) 12

Task 1. Populate Local Repo or Set Up an External Repo 12

Task 2. Apply Updates from the Hosts View to Each Host 13

Apply Updates from the Command Line (No Web Access) 16

Update or Install Legacy Windows Collection **17**

Post Update Tasks **18**

General 18

Task 1 - Start Data Capture and Aggregation 18

NW Server 20

Task 2 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File 20

(Conditional) Task 3 - Reconfigure PAM Radius Authentication 20

RSA NetWitness® Endpoint 20

Task 4 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed 20
RSA NetWitness® Endpoint Insights 21
(Optional) Task 5 - Install Endpoint Hybrid or Endpoint Log Hybrid 21
Event Stream Analysis 21
(Conditional) Task 6 - Reconfigure the “Suspected Command and Control Communication By Domain” Aggregation Rule for Automated Threat Detection 21
Respond 22
Task 7 - (Conditional) Get the Latest Version of the Aggregation Rule Schema and Restore any Respond Service Custom Keys 22
Task 8 - Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts 23
Task 9 - Add Respond Notification Settings Permissions 23
Task 10 - Update Default Incident Rule Group By Values 24
Appendix A. Troubleshooting Version Installations and Updates 25
Appendix B. Populate Local Repo 32
Appendix C. Set Up External Repo 35
Revision History 38

Introduction

RSA NetWitness® Suite11.1.0.0 provides fixes for all products in the suite. The components of the suite are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, and Security sever), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.

Note: The Reporting Engine is installed on the NW Server host, Workbench is installed on the Archiver host, Warehouse Connector can be installed on the Decoder host or Log Decoder host.

The instructions in this guide apply to both physical and virtual hosts (including AWS and Azure Public Cloud) unless stated to the contrary.

Update Path

The following update paths are supported for NetWitness Suite 11.1.0.0:

- 11.0.0.0 to 11.1.0.0
- 11.0.0.1 to 11.1.0.0
- 11.0.0.2 to 11.1.0.0
- 10.6.5.x to 11.1.0.0

  Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

  See the *RSA NetWitness Suite 10.6.5.x to 11.1 Physical Host Upgrade Guide* and *RSA NetWitness Suite 10.6.5.x to 11.1 Virtual Host Upgrade Guide* for instructions on how to upgrade 10.6.5.x to 11.1.0.0.

Running in Mixed Mode

Running in mixed mode occurs when some services are updated to the latest version and some services are on older versions. See "Running in Mixed Mode" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for further information.

Update Preparation Tasks

Complete the following tasks to prepare for the update to NetWitness Suite 11.1.0.0. These tasks are organized by the following categories.

General

Reporting Engine

Respond

General

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.1.0.0.

Caution: Make sure that the new ports are implemented and tested before updating so that update does not fail due to missing ports.

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5672	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

Task 2- Back Up Malware Analysis Configuration File to Another Directory

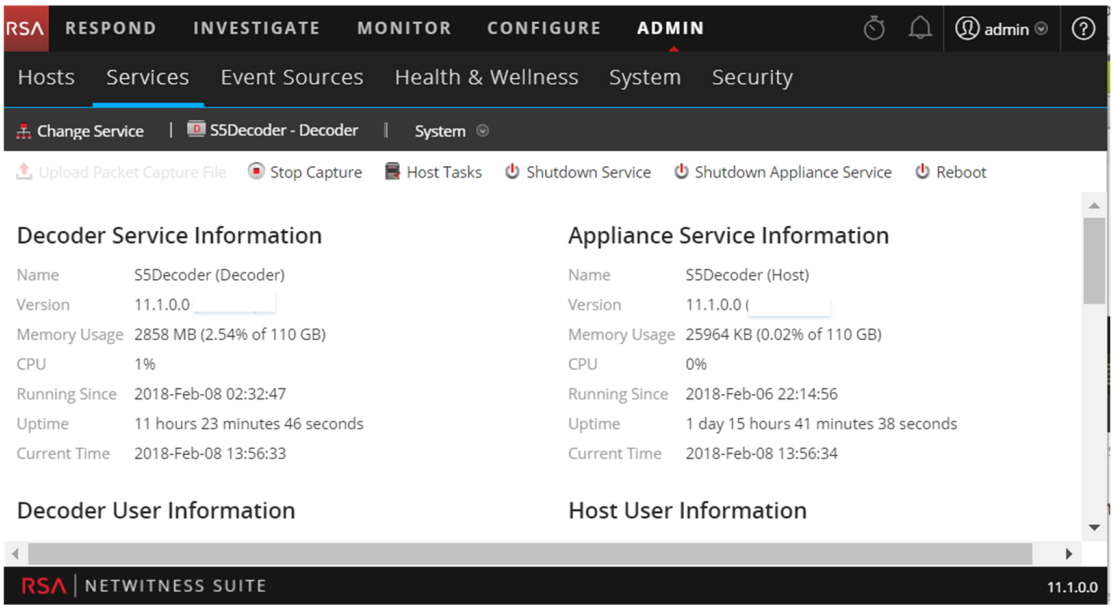
1. Make a backup of the following file to another, safe directory.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`
   You need to retrieve your custom parameter values from this backup after you update the Malware Analysis host to 11.1.0.0. The update creates a new configuration file with all the parameters set to the default values.
2. Delete the following file.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`

Task 3 - Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite 11.0.x and go to **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.



3. Under (actions), select **View** > **System**.
4. In the toolbar, click

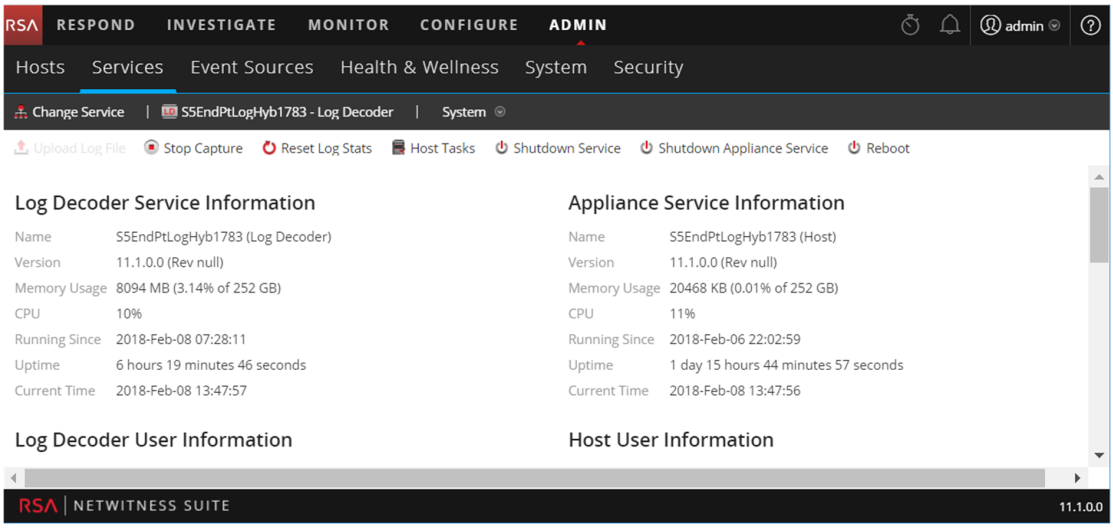
.

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite 11.0.x and go to **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.



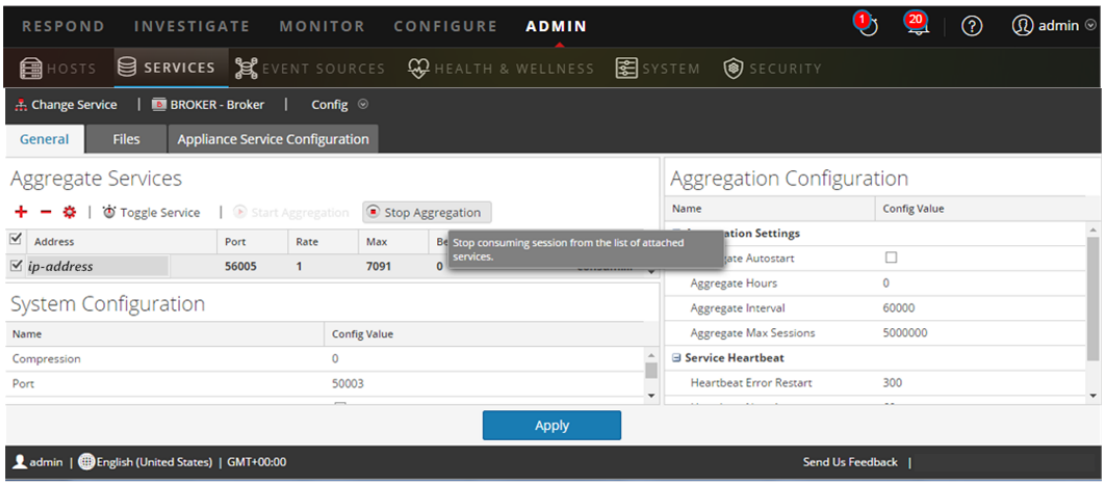
3. Under (actions), select **View** > **System**.

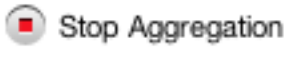
4. In the toolbar, click

.

Stop Aggregation

1. Log in to NetWitness Suite 11.0.x and go to **ADMIN** > **Services**.
2. Select the **Broker** service.
3. Under (actions), select **View** > **Config**.
4. The **General** tab is displayed.



5. Under **Aggregated Services** click 

.

Task 4 - Make Sure That `deploy_admin` User Credentials Are Still Valid (Not Expired)

You must have valid (not exipred) `deploy_admin` user credentials to update to 11.1.

Part I. Verify Expiration Status of `deploy_admin` User Credentials

Complete the following procedure to determine if the `deploy_admin` user credentials have expired.

1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
2. Make sure that the `deploy_admin` has not expired.
   - If they are still valid, you can proceed with the update.
   - If they have expired , complete Part II of this task.

(Conditional) Part II. Reset Expired `deploy_admin` User Credentials

Complete the following procedure to reset expired `deploy_admin` user credentials.

1. Select the `deploy_admin` and click **Reset Password**.
2. (Conditional) If NetWitness Suite allows you to enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
   a. Enter the expired `deploy_admin` password.
   b. Uncheck the Force password change on next login checkbox.
   c. Click **Save**.
3. (Conditional) If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the Reset Password dialog, complete the following steps.
   a. Reset `deploy_admin` to use a new password.
   b. On all the NW Server host and all other hosts on 11.x, run the following command using the new `deploy_admin` password.
   `/opt/rsa/saTools/bin/set-deploy-admin-password`
   c. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

Reporting Engine

Task 5 - Configure Reporting Engine for Out-of-the-Box Charts

For Out-of-the-Box charts to run after the update, you must configure the default data source on the Reporting Engine Configuration page before you perform the update. If you do not perform this task, you must manually set up the data source after the update. For more information on Reporting Engine data sources, see the *NetWitness Suite11.1 Reporting Engine Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

At this point, you can proceed to the update instructions.

Respond

Task 6 - (Conditional) Restore Respond Service Custom Keys

If you added custom keys in `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` for use in the groupBy Clause in 11.0, copy and save the custom keys in a file.

Task 7 - Back Up Customized Respond Service Normalization Scripts

RSA re-factored Respond service normalization scripts are stored in the `/var/lib/netwitness/respond-server/scripts` directory in 11.1.0.0. You need to back them up in 11.0.x before you update to 11.1.0.0 so you can restore them in 11.1.0.0 as described in the Respond Post Update Tasks.

1. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
2. Back up the following files:

   ```
   data_privacy_map.js
   normalize_alerts.js
   normalize_core_alerts.js
   normalize_ecat_alerts.js
   normalize_ma_alerts.js
   normalize_wtd_alerts.js
   utils.js
   ```

3. (Conditional) If you have any custom logic added in 11.0.x or any previous release, copy and save this logic from the backed up scripts so you can restore it in 11.1.0.0.

Task 8 - (Conditional - For Azure Stack)

Populate the Repo with the additional packages.

1. If using a local repository, extract the Azure Zip from the following steps on the Admin server:

a. Run as root: `mkdir -p /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

b. Unzip to the above directory: `unzip nw-azure-11.1-extras.zip -d /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

2. If you are using external repo, follow these steps:

a. After setting up the 11.1.0.0 content on the external repo, unzip the nw-azure-11.1-extras.zip to the external repo directory's <base-directory>11.1.0.0/OS/other folder.

b. Run createrepo from the external repository's 11.1.0.0/OS directory.

Update Tasks

Complete the following tasks to update NetWitness Suite 11.0.x.x to 11.1.0.0.

There are two methods you can use to apply version updates to a host.

Note: If you plan to use an update repository (repo) for NetWitness Suite 11.1.0.0 that is different from the repo you have set up now for 11.0.x.x , refer to Appendix C. Set Up External Repo for instructions.

- Apply updates from the Host view (Web Access)
- Apply update from the command line (No Web Access)

Apply Updates from the Hosts View (Web Access)

There are two tasks you must complete to apply updates from the Hosts view:

- Task 1. Populate Local Repo or Set Up an External Repo - make sure that you have the latest version updates .
- Task 2. Apply updates from the Hosts View to each host.

Task 1. Populate Local Repo or Set Up an External Repo

When you set up your NW Server in 11.1.0.0, you select the Local Repo or an external repo. The Hosts view retrieves version updates from the repo you selected.

If you selected the Local Repo, you do not need to set it up, but you must make sure that it is populated with the latest version updates. See Appendix B. Populate Local Repo for instructions on how populate it with version update.

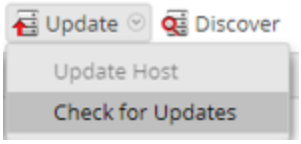
If you selected an External Repo, you must set it up. See Appendix C. Set Up External Repo for instructions on how to set up an external repo.

Task 2. Apply Updates from the Hosts View to Each Host

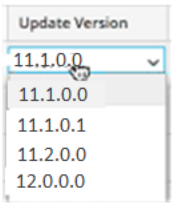
The Hosts view displays the software version updates available in your Local Update Repository and you choose and apply the updates you want from the Host view.

This procedure tells you how to update a host to a new version of NetWitness Suite.

1. Log in to NetWitness Suite.
2. Go to **ADMIN > HOSTS**.
3. (Conditional) Check for the latest updates.



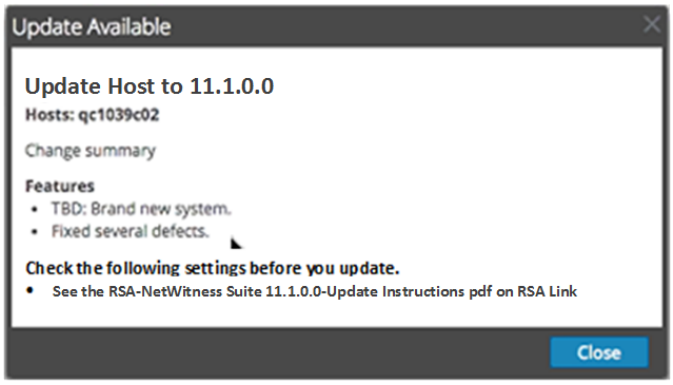
4. Select a host or hosts.
   You must update the NW Server to latest version first. You can update the other hosts in any sequence you prefer, but RSA recommends that you follow the guidelines in "Running in Mixed Mode" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for further information.
   Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected hosts.
5. Select the version you want to apply from the **Update Version** column.



   If you:

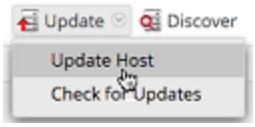
   - Want to update more than one host to that version, after you update the NW Server host, select the checkbox to the left of the hosts. Only currently supported update versions are listed.
   - Want to view a dialog with the major features in the update and information on the updates click the information icon ( ) to the right of the update version number. The

following is an example of this dialog.

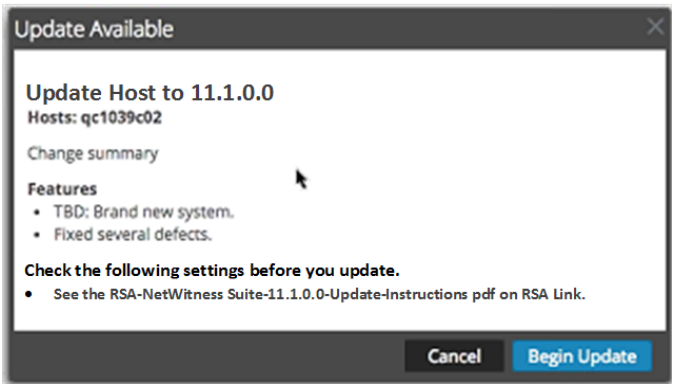


- Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show Update Available. By default, only supported updates for the selected host are displayed.

6. Click **Update > Update Host** from the toolbar.



A dialog is displayed with information on the selected update. Click **Begin Update**.



The **Status** column tells you what is happening in each of the following stages of the update:

- Stage 1 - **Downloading update packages** - downloads the repository artifacts to the NW Server applicable to the services on the host you chose.
- Stage 2 - **Configuring update packages** - configures update files in to correct format.
- Stage 3 - **Update in progress** - updates host to new version.

7. When you see **Update in progress**, refresh the browser.
   This may send you to the NetWitness Log In screen. If this happens, log in and navigate

back to the Host view.

After the host is updated, NetWitness Suite prompts you to **Reboot Host**.

8. Click **Reboot Host** from the toolbar.

   NetWitness Suite shows the status as **Rebooting...** until the host comes back online. After the host comes back online, the **Status** shows **Up-to-Date**. Contact Customer Care if the host does not come back online.

Note: If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates.

Apply Updates from the Command Line (No Web Access)

If your RSA NetWitness Suite deployment does not have Web access, complete the following procedure to apply a version update.

1. Download `.zip` update package for the version you want (for example, `netwitness-11.1.0.0.zip`) from RSA Link to a local directory.
2. SSH to the NW Server host.
3. Make a `tmp/upgrade/<version>` staging directory for the version you want (for example, `tmp/upgrade/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Unzip the package into the staging directory you created (for example, `tmp/upgrade/11.1.0.0`).
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Initialize the update on the NW Server.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Apply the update to the NW Server.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Log in to NetWitness Suite and reboot the NW Server host in the Host View.
8. Apply update to each non-NW Server host.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   The update is complete when the polling is completed.
9. Log in to NetWitnesss Suite and reboot the host in the Host View.
   You can verify the version applied to the host with the following command:
   ```
   upgrade-cli-client --list
   ```

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Update Tasks

Complete the following tasks after you update to NetWitness Suite 11.1.0.0.

- General
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Respond

General

These tasks apply to all NetWitness Suite 11.1.0.0 customers.

Task 1 - Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.0.0.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under (actions), select **View** > **System**.
4. In the toolbar, click

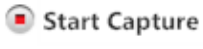
.

Start Log Capture

To start log capture:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.

3. Under (actions), select **View** > **System**.

4. In the toolbar, click 

.

Start Aggregation

To start aggregation:

1. In the **NetWitness Suite** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. For each Concentrator and Broker service.
   a. Select the service.
   b. Under (actions), select **View** > **Config**.
   c. In the toolbar, click

.

NW Server

Task 2 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File

Problem: When a user updates from 11.0.0.0 to 11.1.0.0, if they have global auditing set up, audit log templates are not getting updated in Logstash output conf file.

Workaround: If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click save to apply the latest Audit log configuration.

If you had global auditing configured in 11.0.x, you must complete the following procedure to apply the latest Global Auditing configuration.

1. In the **NetWitness Suite** menu, select **ADMIN** > **System** > **Global Notifications**.
   The **Global Notifications** view is displayed.
2. Click the **Servers** tab, select any syslog server.
3. Click (edit icon) and click **Save**.

(Conditional) Task 3 - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.0.x.x using the `pam_radius` package, you must reconfigure it in 11.1.0.0 using the `pam_radius_auth package` to achieve better performance. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite 11.1 System Security and User Management Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint

Task 4 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

You must reconfigure the Legacy Endpoint recurring feed due to the change in Java version. Complete the following step to fix this problem.

- Import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness 11.1 Endpoint Integration Guide* to import the certificate.
  Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint Insights

(Optional) Task 5 - Install Endpoint Hybrid or Endpoint Log Hybrid

See:

RSA NetWitness Suite 11.1 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Suite 11.1 Virtual Host Installation Guide for instructions for installation on a virtual host.

Event Stream Analysis

These tasks apply to NetWitness Suite 11.1.0.0 customers using Event Stream Analysis.

(Conditional) Task 6 - Reconfigure the "Suspected Command and Control Communication By Domain" Aggregation Rule for Automated Threat Detection

In 11.0, the "Suspected Command & Control Communication By Domain" aggregation rule Group By condition "Domain by Suspected C&C" was not functioning as expected and had to be changed to "Domain" to aggregate alerts and enable incidents to be created for "Suspected C&C." The "Domain by Suspected C&C" condition works correctly in 11.1.0.0 and should be used as the Group By condition for the "Suspected Command & Control Communication By Domain" aggregation rule (known as incident rule in 11.1.0.0).

If you changed the "Suspected Command & Control Communication By Domain" aggregation rule Group By condition to "Domain" for 11.0, you will need to change it back to "Domain by Suspected C&C" for 11.1.0.0.

1. Log in to NetWitness Suite 11.1.0.0.
2. Go to **CONFIGURE** > **Incident Rules**.
3. In the Incident Rules list, locate the Suspected Command & Control Communication by Domain rule and click the link in the NAME field to open it.
4. In the Incident Rule Details view Grouping Options section, set the Group By field to Domain for Suspected C&C and click Save.

For more information, see the NetWitness Suite Automated Threat Detection Guide and the

"Configure ESA Analytics" section of the NetWitness Suite ESA Configuration Guide. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

Task 7 - (Conditional) Get the Latest Version of the Aggregation Rule Schema and Restore any Respond Service Custom Keys

Complete the following procedure to get the latest version of the Aggregation Rule Schema and restore any Respond service custom keys.

1. Delete the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file.
2. Restart the Respond server to get the latest version of the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file.
   ```
   systemctl restart rsa-nw-respond-server
   ```
3. If you added custom keys in `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the groupBy clause for 11.0, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys that you previously saved as an Update Preparation task.

Note: New Group By fields have been added to Respond in 11.1.0.0. The new Group By fields will not be visible in the NetWitness Suite user interface if you do not get the latest version of the file from the server.

Task 8 - Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts

RSA re-factored Respond service normalization scripts in the `/var/lib/netwitness/respond-server/scripts` directory in 11.1.0.0. You must replace the old versions.

Before the update to 11.1.0.0, you backed up the following files from the `/var/lib/netwitness/respond-server/scripts` directory.

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

Complete the following procedure to get the latest version of the normalization scripts.

1. After backing up the files listed above, delete the `/var/lib/netwitness/respond-server/scripts` directory and its contents.
2. Restart the Respond server.

   ```
   systemctl restart rsa-nw-respond-server
   ```

3. (Conditional) Edit the new files to include any custom logic from the 11.0 scripts that were backed up.

Note: The following files changed with the 11.1.0.0 release:

```
normalize_alerts.js
normalize_core_alerts.js
normalize_ma_alerts.js
```

Task 9 - Add Respond Notification Settings Permissions

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**CONFIGURE** > **Respond Notifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. You will also need to add permissions to your custom roles. See the "Respond Notification Settings Permissions" topic in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 10 - Update Default Incident Rule Group By Values

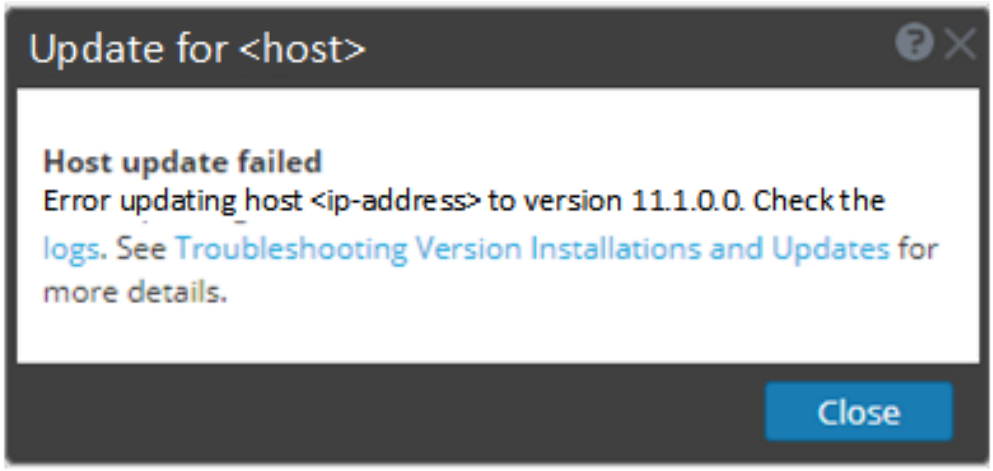
Four of the default incident rules now use “Source IP Address” as the Group By value. To update the default rules, change the Group By value of the following default rules to “Source IP Address”:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update. The Incident Rule Details view is displayed.
2. In the **Group By** field, select the new Group By value.
3. Click **Save** to update the rule.

Appendix A. Troubleshooting Version Installations and Updates

This section describes the error messages displayed in the **Hosts** view when it encounters problems updating host versions and installing services on hosts in the **Hosts** view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.

Solution	1. **Try to apply the version update to the host again**.
	Often this is all you need to do.
	2. If you still cannot apply the new version update:
	a. Monitor the following logs on NW Server as it progresses (for example, use submit the `tail -f` command string from the command line'):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error will appear in one or more of these logs.

b. Try to resolve the issue and reapply the version update.

- Cause 1 - `deploy_admin` password has expired.
  Solution - Reset your `deploy_admin` password .
  Complete the following steps to resolve Cause 1.

  1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
  2. Select the `deploy_admin` and click **Reset Password**.
  3. (Conitional) If NetWitness Suite does not allow you to expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.

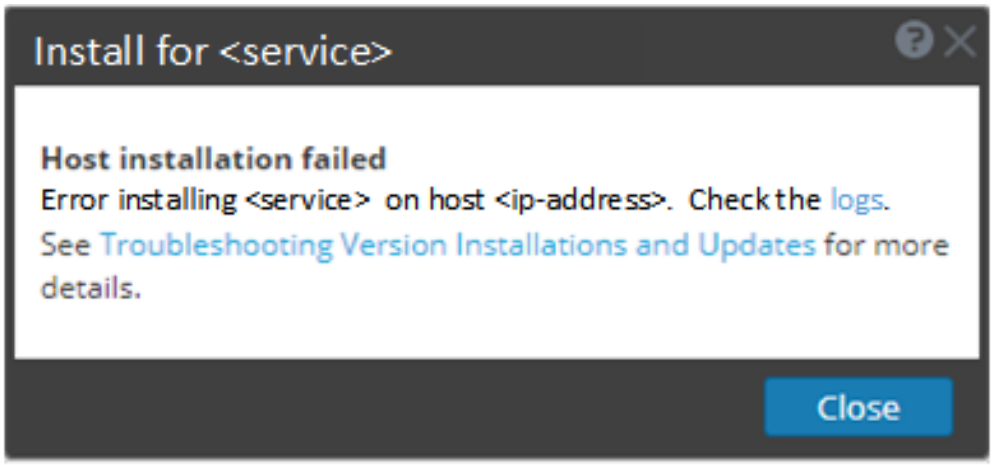
     a. Reset `deploy_admin` to use a new password.

     b. On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`

- Cause 2 -The `deploy_admin` password was changed on NW Server host but not changed on non-NW Server hosts.
  Complete the following step to resolve Cause 2.

  - On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.
    `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

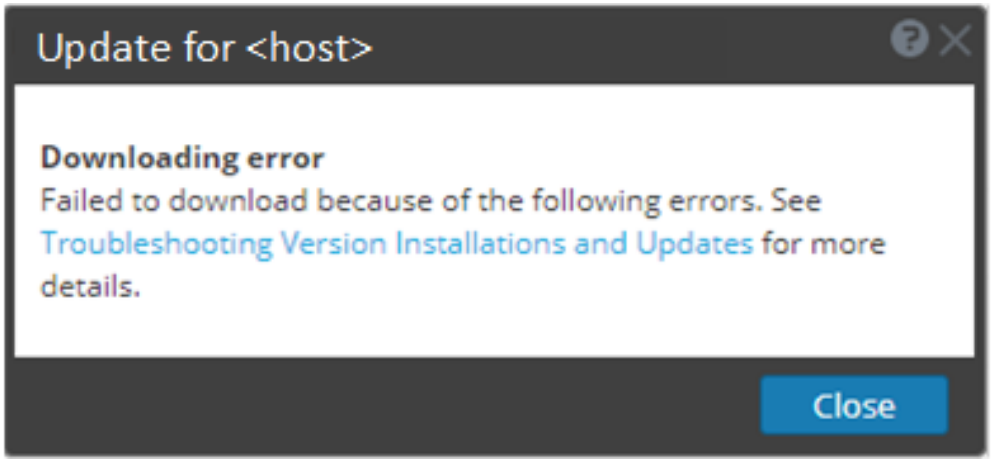
Error Message	
Problem	When you select a host and click **Install** the install service process fails.

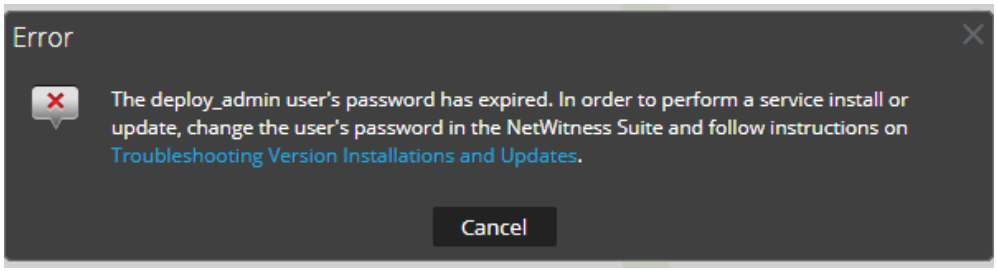
Solution	1. **Try to install the service again.**.
	Often this is all you need to do.
	2. If you still cannot install the service:
	a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error will appear in one or more of these logs.
	b. Try to resolve the issue and reinstall the service.
	• Cause 1 - Entered the wrong`deploy_admin` password in the nwsetup-tui.
	Solution - Retrieve your `deploy_admin` password.
	Complete the following steps to resolve Cause 1.
	1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
	2. Select the `deploy_admin` and click **Reset Password**.

3. (Conitional) If NetWitness Suite does not allow you to expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
   a. SSH to the NW Server host.
      ```
      security-cli-client --get-config-prop --prop-hierarchy
      nw.security-client --prop-name
      platform.deployment.password -quiet
      ```
   b. SSH to the host that failed installation/orchestration.
   c. Run the nwsetup-tui again using correct `deploy_admin` password.

- Cause 2 -The `deploy_admin` password has expired.
  Complete the following step to resolve Cause 2.
  1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
  2. Select the `deploy_admin` and click **Reset Password**.
  3. (Conditional) If NetWitness Suite allows you enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
     a. Enter the expired `deploy_admin` password.
     b. Uncheck the Force password change on next login checkbox.
     c. Click **Save**.
  4. (Conditional) If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the Reset Password dialog, complete the following steps.
     a. Reset `deploy_admin` to use a new password.
     b. On all the NW Server host and all other hosts on 11.x, run the following command using the new `deploy_admin` password.
        ```
        /opt/rsa/saTools/bin/set-deploy-admin-password
        ```
     c. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Problem	When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete.
Cause	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
Solution	1. Try to download it again. 2. If the download still fails, try to download it outside of NetWitness Suite as described in Apply Updates from the Command Line (No Web Access). 3. If you still cannot download the update file, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	
Cause	The `deploy_admin` user password has expired.
Solution	Reset your `deploy_admin` password password. 1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab. 2. Select the **deploy_admin** and click **Reset Password**. • If NetWitness Suite allows you to enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps. a. Enter the expired `deploy_admin` password. b. Uncheck the **Force password change on next login** checkbox. c. Click **Save** • If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the **Reset Password** dialog. a. On the NW Server host and all other hosts on 11.x , run the following command using the new `deploy_admin` password. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

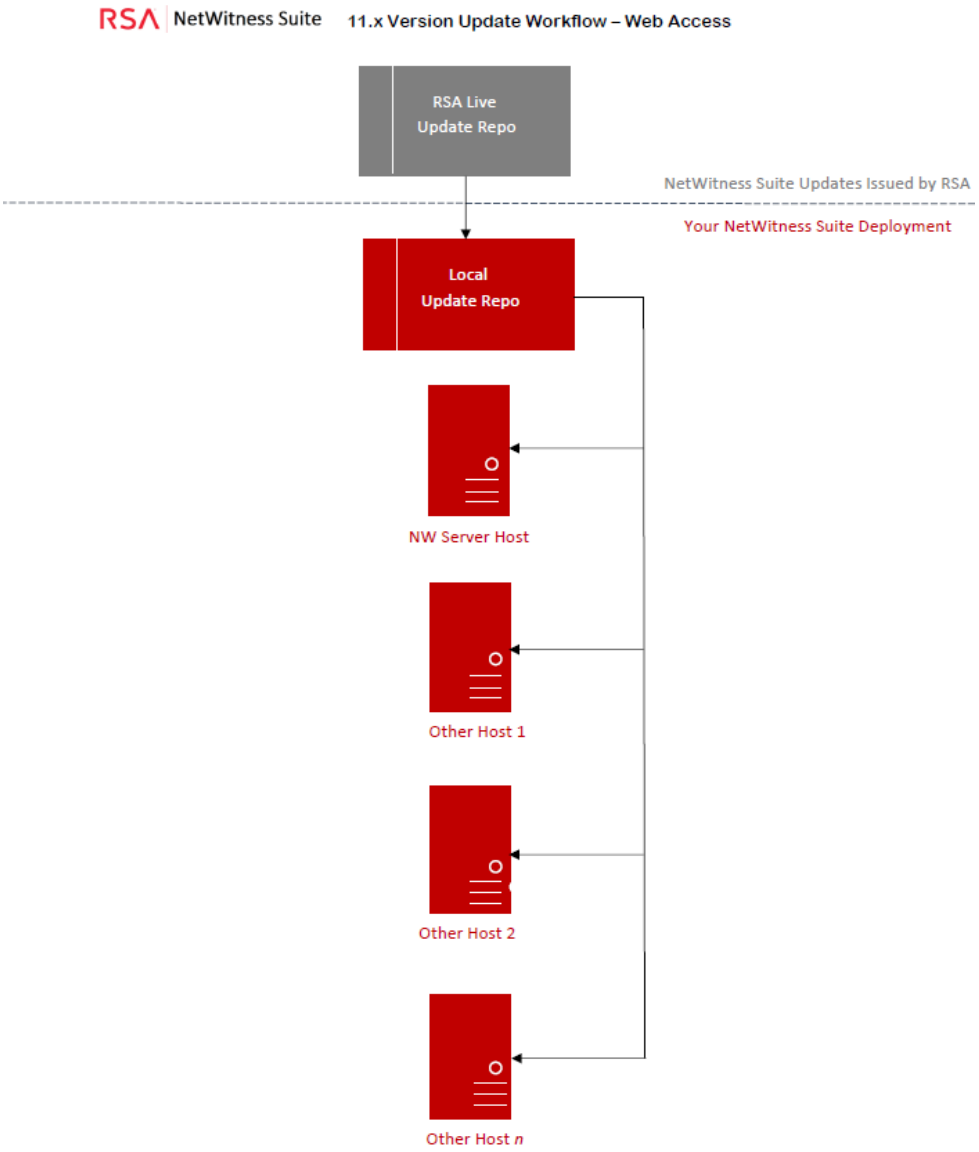
Error Message	The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error: `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgument Exception::Version '11.0.0.n' is not supported`
Problem	After you update the NW Server host to 11.1, the only update path for the non-NW Server hosts is 11.1. If you try to update any non-NW Server host to an 11.0.0.n patch (for example from 11.0.0.0 to 11.0.0.3), you will get this error.

Solution	You have two options: • Update the non-NW Server host to 11.1, or • Do not update the non-NW Server host (keep it at its current version).

Appendix B. Populate Local Repo

NetWitness Suite sends version updates to the Local Update Repository from the Live Update Repository. Access to the Live Update Repository requires and uses the Live Account credentials configured under **ADMIN > SYSTEM > Live**. In addition, you must check the `Automatically download information about new updates every day` checkbox under **ADMIN > SYSTEM > Updates** to populate the Local Repo daily.

The following diagram illustrates how you obtain version updates if your NetWitness Suite deployment has Web Access.



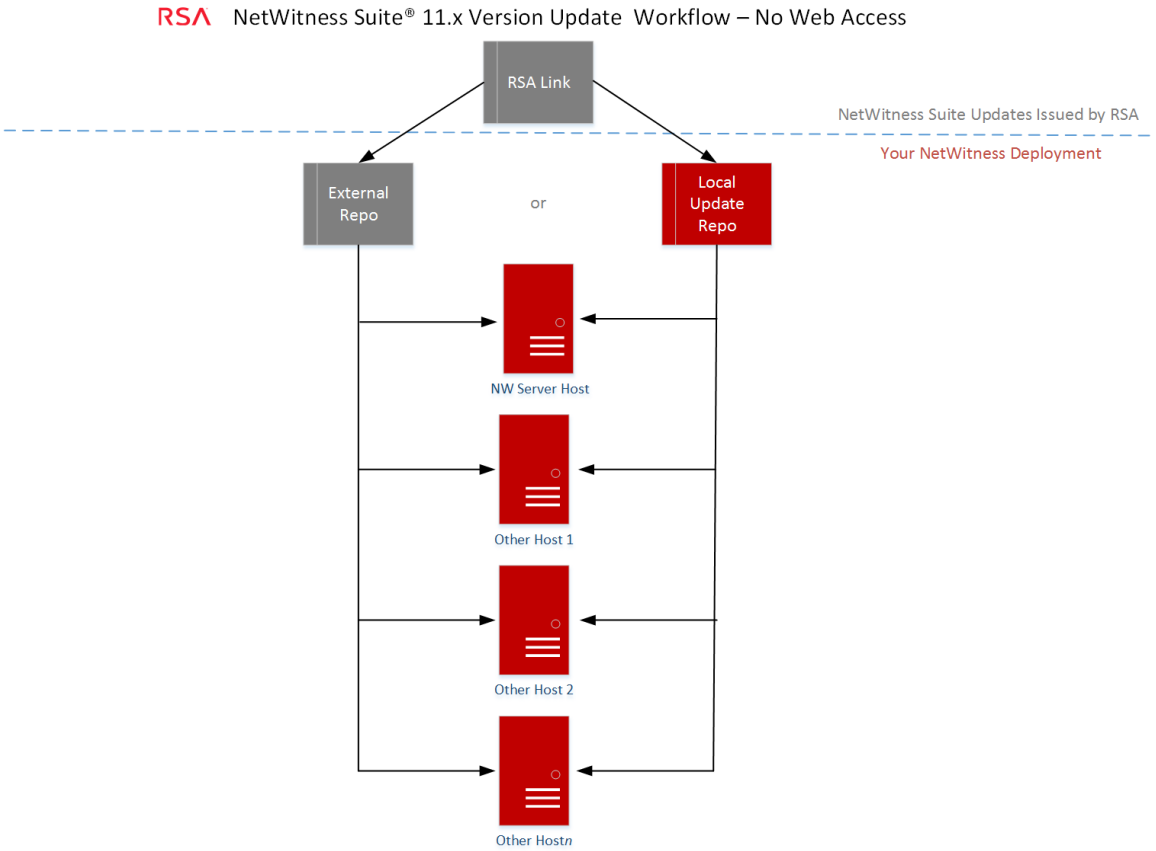
Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 7 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your NW Server Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository. Alternatively you can use an External Repo as described in "Set Up an External Repo."

To connect to the Live Update Repository, Navigate to the **ADMIN > SYSTEM** view, select **Live** in the options panel and ensure that credentials are configured (**Connection** light should be green). If it is not green, click **Sign In** and connect.

Note: If you need to use proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. Refer to "Configure Proxy forNetWitness Suite" in the *NetWitness Suite 1.1 System Configuration Guide*.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

See "Apply Updates from Command Line" if your NetWitness Suite deployment does not have Web Access.

The following diagram illustrates how you obtain version updates if your NetWitness Suite deployment does not have Web Access.



Appendix C. Set Up External Repo

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step If you have an external repo and you want to override it.
   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/platform/netwitness/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
        See for the instructions.
   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/platform/netwitness/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
        The instructions are in the "Apply Updates from the Command Line" under topic.
2. Set up the external repo.
   a. Log in to the web server host
   b. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo`under `web-root` of the web server. For example, /var/netwitness is the web-root, submit the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`

d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

e. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.

```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

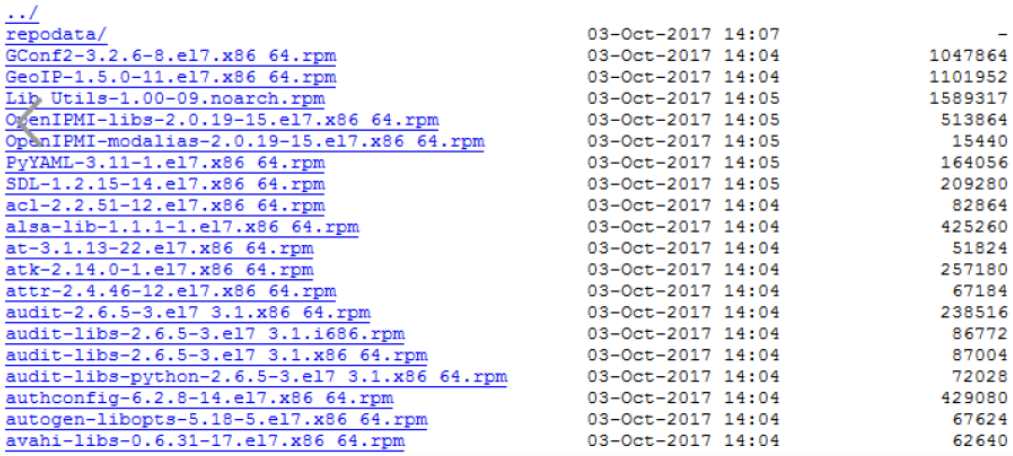
Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.

f. Unzip the:

1. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
```

The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.



../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will

appear after you unzip the file.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

g. (Conditional - For Azure) Follow these steps for Azure update

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`

iv. `createrepo .`

h. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD
1.1	12-Mar-17	Change to note at the start of the Update Tasks concerning an external repository.	IDD
1.2	12-Apr-18	Added "Task 4 - Make Sure That `deploy_admin` User Credentials Are Still Valid (Not Expired)" to the Update Preparation Tasks.	IDD

RSA NETWITNESS® SUITE

Windows Legacy Collection Configuration

for Version 11.x

RSA

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

NetWitness Legacy Windows Collection Update & Installation Instructions **4**

Setup Requirements **5**

Update the RSA NetWitness® Suite Legacy Windows Collector from 10.6.x to 11.x **7**

Fresh Install 11.x Legacy Windows Collector **11**

Troubleshooting for Fresh or Upgrade Install **15**

Logs to Examine for Information 15

Issues with the Lockbox 15

(Optional) Backup and Restore Legacy Windows Collector **16**

For Version 10.6.4 16

Backup 16

Restore 17

For Upgrading from 10.6.4 to NetWitness 11.x 17

Restore the Windows Legacy Collection Backup after Upgrade 17

Revert Windows Legacy Collection from 11.x Back to 10.6.4 18

Add a Windows Legacy Collector Host and Service in RSA NetWitness® Suite **19**

NetWitness Legacy Windows Collection Update & Installation Instructions

The RSA NetWitness® Suite Legacy Windows collection collects event data from multiple Windows Event Source domains.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

This document contains the following sections:

- Setup Requirements
- Update the RSA NetWitness® Suite Legacy Windows Collector from 10.6.x to 11.x
- Fresh Install 11.x Legacy Windows Collector
- Troubleshooting for Fresh or Upgrade Install
- (Optional) Backup and Restore Legacy Windows Collector
- Add a Windows Legacy Collector Host and Service in RSA NetWitness® Suite

Setup Requirements

This section provides the RSA NetWitness® Suite Legacy Windows Collector Setup requirements.

Caution: If you are installing or updating to version 11.x, in order to use the Security Analytics Legacy Windows Collector with NetWitness, you need to first install the following windows updates:

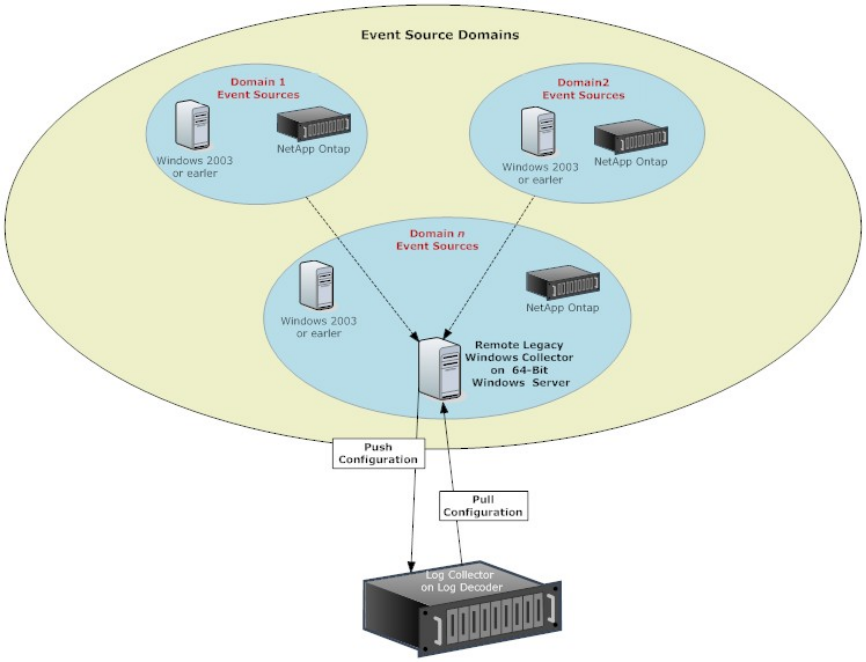
• KB2919355
• KB2919442
• KB2999226
• KB3173424

If these updates are not installed, you will get an error message, and the Legacy Windows Collector will not be installed.

To set up the RSA NetWitness ® Suite Legacy Windows Collector, you need:

- Any physical or virtual Windows 2008 R2 SP1 64-Bit Server that can reach the Windows 2003 event source domains.
- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.

Important! Do not install the Legacy Windows Collector on a domain controller.


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

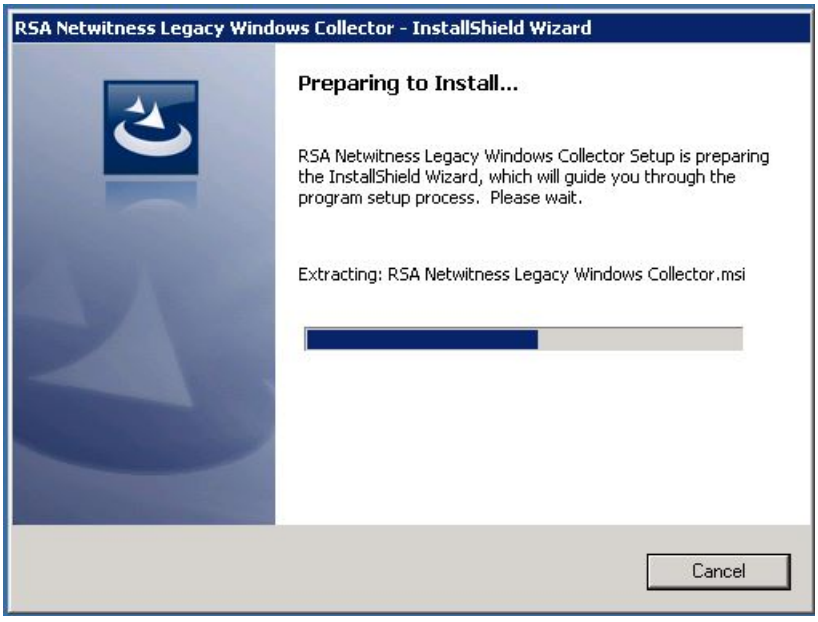
Update the RSA NetWitness® Suite Legacy Windows Collector from 10.6.x to 11.x

This section tells you how to update RSA NetWitness Suite 10.6.x Legacy Windows Collector to 11.

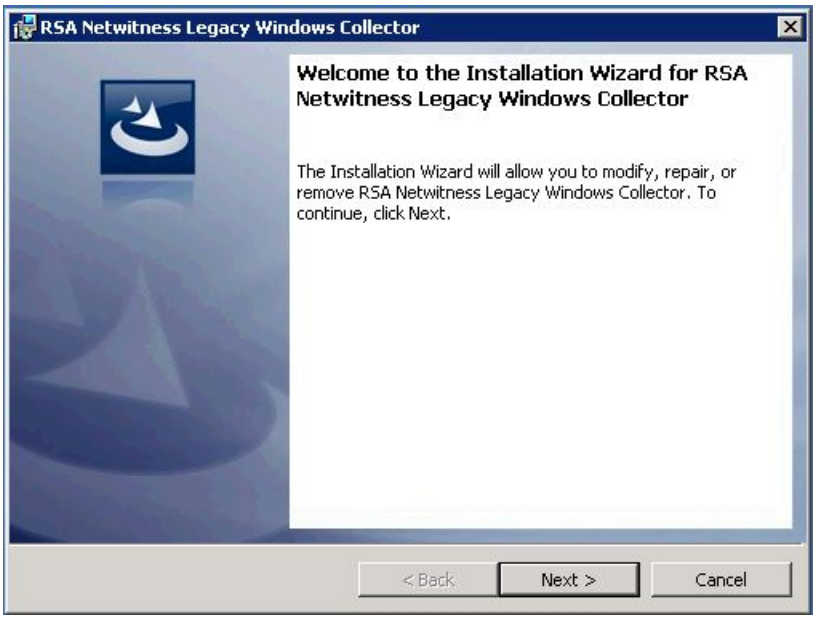
To update the RSA NetWitness® Suite 10.6.x Legacy Windows Collector to 11 on a Windows 2008 R2 SP1 64-Bit server:

1. Navigate to https://community.rsa.com/docs/DOC-83034 on RSA link. Click **RSA NetWitness Logs & Packets 11.x - Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Log on to a Windows 2008 machine.
4. Copy **NWLegacyWindowsCollector-*version-number*.exe** to the Windows 2008 server.
5. Right click on **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

   The Preparing to Install…. page of update installation wizard is displayed.

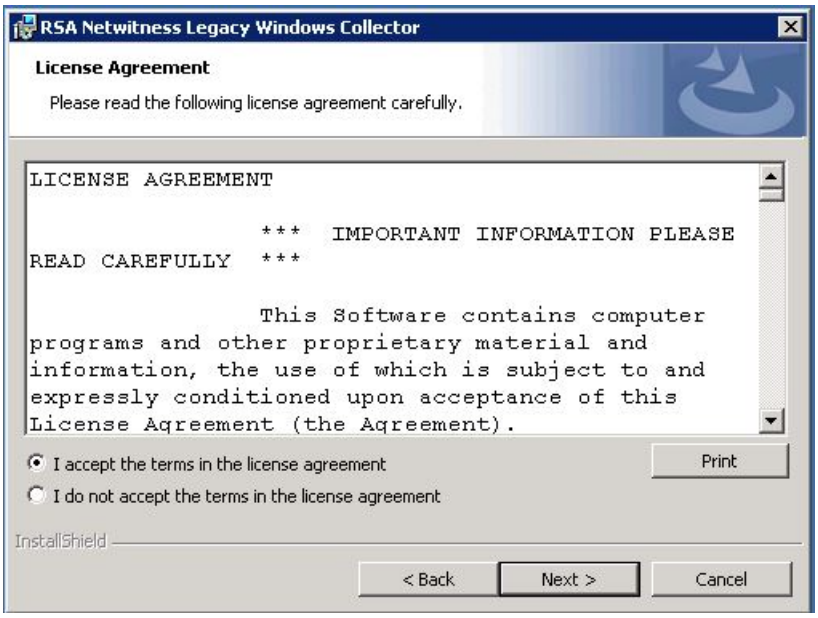


   After the update installation program extracts RSA NetWitness® Suite Legacy Windows Collector installation files, the **Welcome** page is displayed.



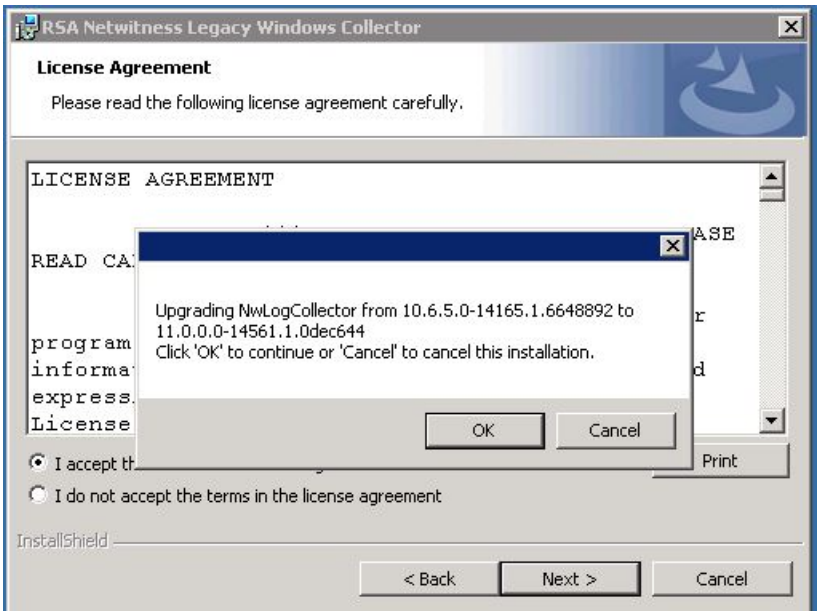
6. Click **Next**.

   The License Agreement page is displayed.



7. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

   Before it starts the update, the wizard asks if you want to continue or cancel the installation of the update.



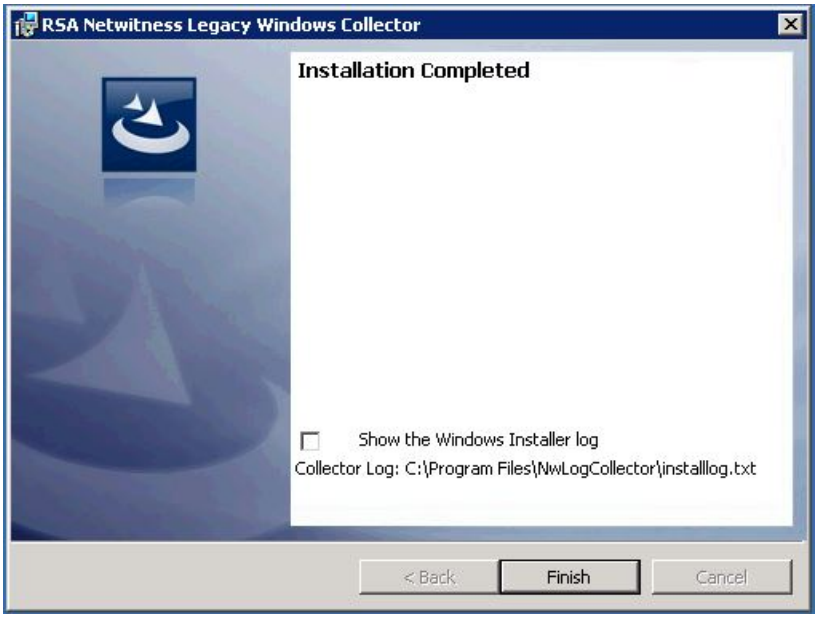
8. Click **OK** to continue installing the update.
9. Click Install.

   The Installation screens for the Legacy Windows Collector page is displayed.

After the update installation completes, the **Next** button becomes active.

10. Click **Next**.

    The Installation Completed page is displayed.



11. (Optional) If you want to review a log of the update installation, select the **Show the Windows Installer** log checkbox.
12. Click **Finish**.
13. Reboot the machine.

This completes the update of the Legacy Windows Collector to RSA NetWitness Suite 11.x.

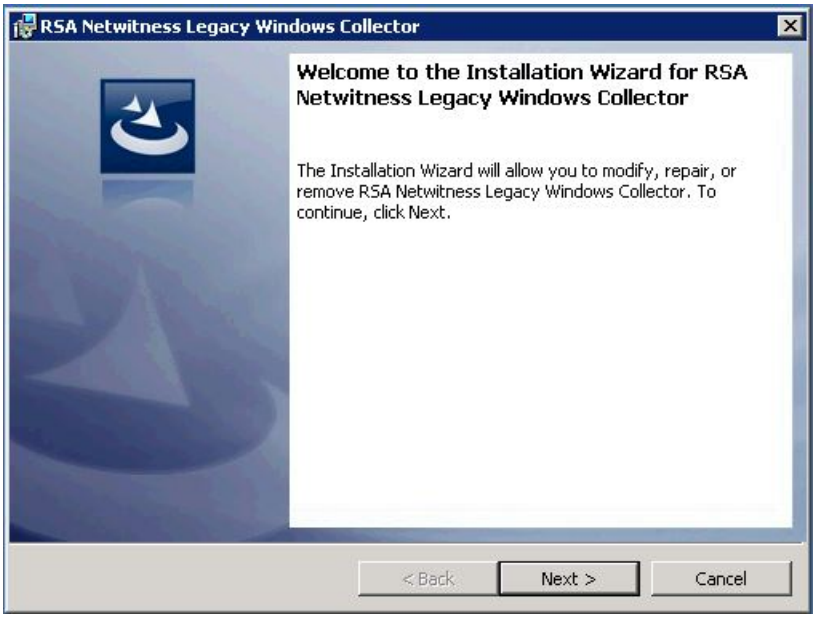
Fresh Install 11.x Legacy Windows Collector

This section describes how to install the 11.x Legacy Windows Collector on a Windows 2008 R2 SP1 64-Bit server

To install the RSA NetWitness Suite Legacy Windows Collector on a Windows 2008 R2 SP1 64-Bit server:

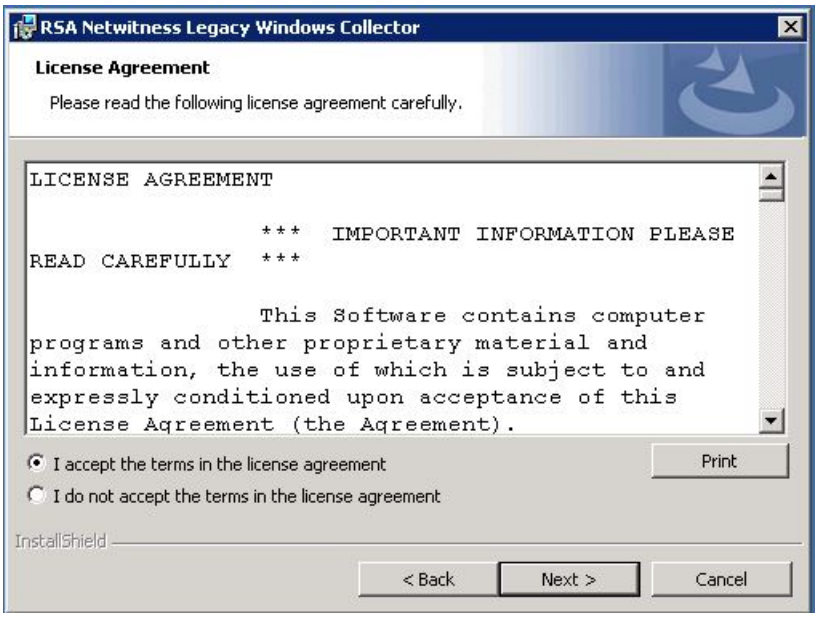
1. Navigate to https://community.rsa.com/docs/DOC-83034 on RSA link. Click **RSA NetWitness Logs & Packets 11.x - Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Copy the **NWLegacyWindowsCollector-*version-number*.exe** to the Windows 2008 server.
4. Right click on the **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

   The **Welcome** page of installation wizard is displayed.



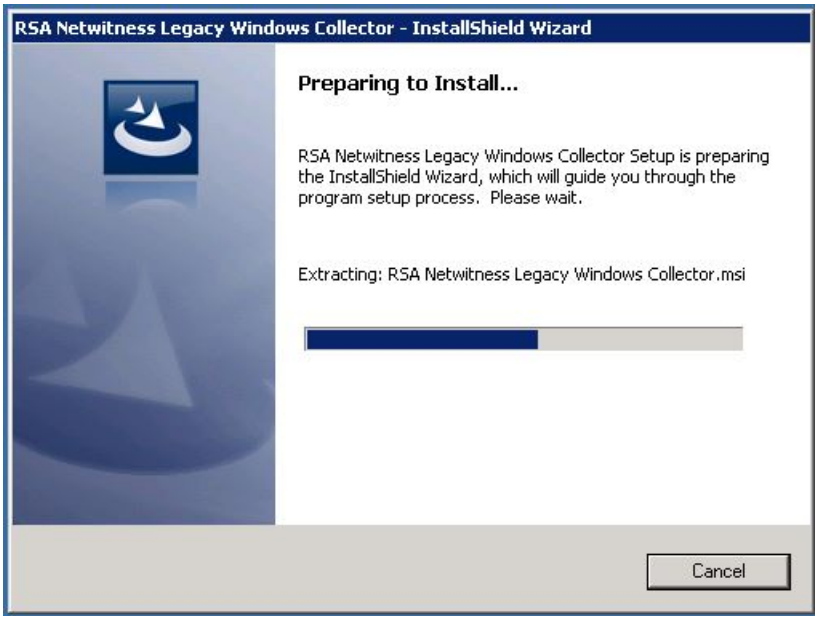
5. Click **Next**.

   The License Agreement page is displayed.



6. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

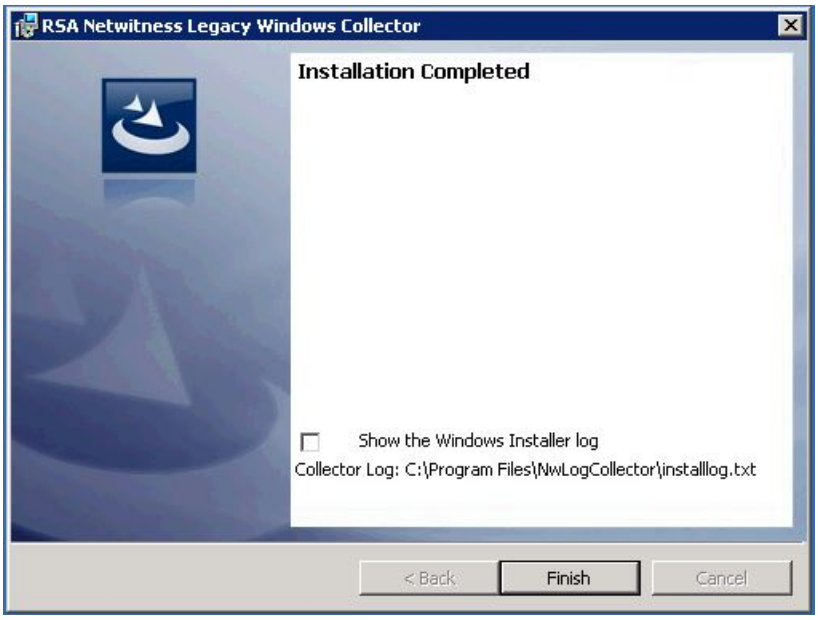
   The Ready to Install the Program page is displayed.



7. Click **Install**.

   The Installation screens for the Legacy Windows Collector page are displayed.

The Installation Completed page is displayed.



8. (Optional) If you want to review a log of the installation, select the **Show the Windows Installer** log checkbox.
9. Click **Finish**.
10. Reboot the machine.

This completes the installation of the 11.x Legacy Windows Collector. Please refer to the **Windows Legacy and NetApp Collection Configuration Guide** on RSA Link for instructions on how to configure Legacy Windows collection in RSA NetWitness Suite.

Troubleshooting for Fresh or Upgrade Install

Logs to Examine for Information

Refer to the following log files if you need to troubleshoot problems:

- `%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log`
- `%systemDrive%\Program Files\NwLogCollector\installlog.txt`

Run `C:\Program Files\NwLogCollector\ziplogfiles.vbs` to generate the ***hostname***`_WLCversion_timestamp.zip` that contains all the log files and other information needed for troubleshooting.

Issues with the Lockbox

When you create a lockbox password on a new Windows Legacy Collector, you might see the following error:

failed to set secure storage password: failed to create lockbox: The Lockbox or cryptography library could not be found.

This can occur if you are running Windows Legacy Collector version 11.x.

If you encounter this issue, download and install both of the following redistributable packages:

- Visual C++ 2010: https://www.microsoft.com/en-us/download/details.aspx?id=14632
- Visual C++ 2012: https://www.microsoft.com/en-us/download/details.aspx?id=30679

(Optional) Backup and Restore Legacy Windows Collector

This section tells you how to backup and restore the Legacy Windows Collector.

Note: You only need to do this if you are changing the Windows VM where you run the Windows Legacy Collector.

For Version 10.6.4

For the 10.6.4 version of the RSA NetWitness Suite Legacy Windows Collector, there are manual scripts provided for performing backup and install:

- WLC-Backup.bat
- WLC-Restore.bat

These files are available for download from RSA Link at the following location: https://community.rsa.com/docs/DOC-71397.

Backup

To backup the Legacy Windows Collector:

1. Download the backup and restore scripts from RSA Link to the Windows Legacy Collector.
2. On the Windows Legacy Collector, open a command prompt window, and navigate to the folder where you saved the scripts.
3. Run the command for creating a backup:
   - Backup configuration files: `WLC-Backup.bat config`
   - Backup run-time files: `WLC-Backup.bat runtime`

   Note: Only backup the run-time files if you have already started collection.

   The backup folders are created in **C:\Program Files\NwLogCollector**.

   The file names are as follows:

   - Config-bkup_***timestamp***.zip
   - Runtime-bkup_***timestamp***.zip

Restore

To restore a previously created backup for the Legacy Windows Collector:

1. On the Windows Legacy Collector, open a command prompt window, and navigate to the folder where you saved the scripts.
2. Run the following command for restoring a backup:
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
3. Once the restore is completed, set the lockbox SSV to use the password that you created during 10.6.4 setup.
   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.
   b. From the left navigation pane, expand **logcollection** > **properties** > **crypto**.
   c. Run the following command: `op=setssv pw=password_for_10.6.x_lockbox`, and hit **Send**.

For Upgrading from 10.6.4 to NetWitness 11.x

During upgrade to RSA NetWitness Suite 11.x, the backup script for the Windows Legacy Collector is invoked automatically, and creates the 10.6.4 configuration and run-time backups. After the 11.x installation is completed, run the Restore script to restore the configuration and run-time files for the updated Windows Legacy Collection.

Restore the Windows Legacy Collection Backup after Upgrade

To restore the Windows Legacy Collection setup on a newly upgraded RSA NetWitness Suite 11 platform:

1. On the Windows Legacy Collector, open a command prompt window.
2. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
3. Run the following commands for restoring a backup:
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
4. Once the restore is completed, set the lockbox SSV to use the password that you created during 10.6.4 setup.

a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.

b. From the left navigation pane, expand **logcollection > properties > crypto**.

c. Run the following command: `op=setssv pw=`***`password_for_10.6.x_lockbox`***, and hit **Send**.

Revert Windows Legacy Collection from 11.x Back to 10.6.4

To revert the Windows Legacy Collection setup from 11.x back to 10.6.4:

1. Uninstall the 11.x Setup. Note the location of the backup folder created by the system during the uninstall procedure.
2. Install the 10.6.4 version of the Windows Legacy Collector.
3. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
4. Run the Restore script from backup folder present in **C:\Program Files\NwLogCollector** to restore the configuration and run-time setup on the 10.6.4 Windows Legacy Collector.
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
5. Once the restore is completed, set the lockbox SSV to use the password that you created during 10.6.4 setup.

   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.

   b. From the left navigation pane, expand **logcollection > properties > crypto**.

   c. Run the following command: `op=setssv pw=`***`password_for_10.6.x_lockbox`***, and hit **Send**.

Add a Windows Legacy Collector Host and Service in RSA NetWitness® Suite

For this version of the Windows Legacy Collector, RSA has provided a script that replaces the manual steps of adding a Windows Legacy Collector host and service in the NetWitness UI.

To create a Windows Legacy Collector Host and Service in NetWitness:

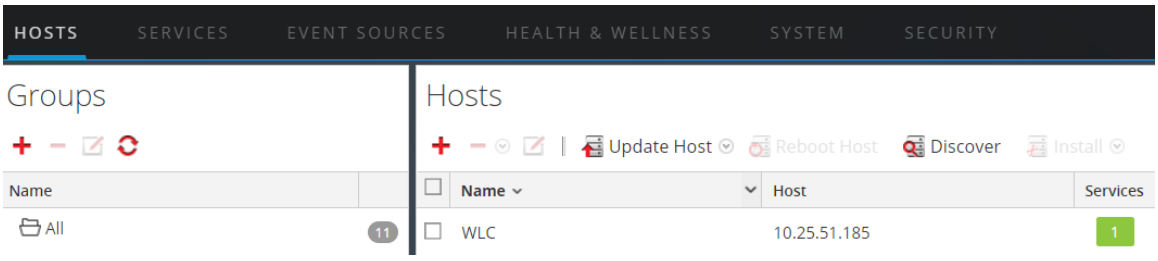
1. SSH to your NetWitness server.
2. Run the following command:

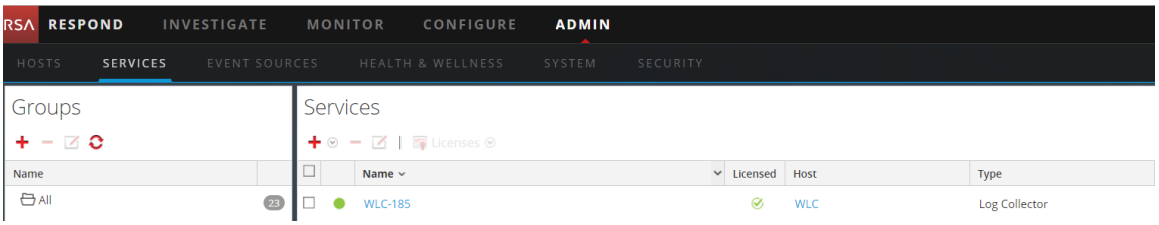
   wlc-cli-client --host-display-name ***hostDisplayName*** --service-display-name **serviceDisplayName** --host ***WLChostIPAddress*** --port 50101 --use-ssl false

   The parameters are explained below:

   - **--host-display-name**: the name for the host as it is displayed in the NetWitness Hosts page
   - ***--service-display-name***: the name for the host as it is displayed in the NetWitness Services page
   - **--host**: the IP address for the Windows Legacy Collector
   - **--port**: the port NetWitness uses to communicate with the Windows Legacy Collector. The recommended value is 50101.
3. You will be prompted to supply the following information:
   - **Windows Log Collector REST Username** and **Windows Log Collector REST Password**: you must supply admin credentials for the Windows Legacy Collector.
   - **Security Server Username** and **Security Server Password**: you must supply admin credentials for RSA NetWitness Suite.

When you complete this procedure, you should see the Windows Legacy Collector Host and Service as shown in the following screenshots.




RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
23
Services
Licenses
Name
Licensed
Host
Type
WLC-185
WLC
Log Collector