



Hosts and Services Getting Started Guide

for Version 11.0



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.

February 2018

Contents

Hosts and Services Basics	9
What Is a Host	9
Setting Up a Host	10
Maintaining Hosts	10
Update Version Naming Convention	11
Maintaining Services	12
Services Implemented with the NetWitness Server	12
Running in Mixed Mode	14
Functionality Gaps Encountered During in Staggered Updates	14
Examples of Staggered Updates	14
Example 2. Multiple Decoders and Concentrators, Alternative 2	15
Example 3. Multiple Regions	16
Hosts and Services Procedures	17
Step 1. Deploy a Host	20
Step 2. Install a Service on a Host	21
Prerequisites	21
Procedure	21
Step 3. Review SSL Ports for Trusted Connections	22
Prerequisite	22
Encrypted SSL Ports	22
Step 4. Manage Access to a Service	24
Test a Trusted Connection	24
Apply Version Updates to a Host	26
Apply Updates from the Hosts View (Web Access)	27
Apply Updates from the Command Line (No Web Access)	29
Populate Local Update Repository	30
Set Up an External Repository with RSA and OS Updates	32
Create and Manage Host Groups	34
Create a Group	35
Change the Name of a Group	35
Add a Host to a Group	36

View the Hosts in a Group	36
Remove a Host from a Group	36
Delete a Group	37
Search for Hosts	37
Search for a Host	37
Find the Host that Runs a Service	38
Execute a Task From the Host Task List	39
Add and Delete a Filesystem Monitor	41
Configure the Filesystem Monitor	41
Delete a Filesystem Monitor	42
Reboot a Host	43
Shut Down and Restart a Host from the Hosts View	43
Shut Down and Restart a Host from the Host Task List	44
Set Host Built-In Clock	44
Set the Time on the Local Clock	44
Set Network Configuration	45
Specify the Network Address for a Host	46
Set Network Time Source	46
Specify the Network Clock Source	47
Set SNMP	48
Toggle SNMP Service on the Host	48
Set Syslog Forwarding	49
Set Up and Start Syslog Forwarding	49
Show Network Port Status	51
Display the Network Port Status	51
Show Serial Number	52
Show the Serial Number	52
Shut Down Host	53
Shut Down the Host	54
Stop and Start a Service on a Host	54
Stop a Service on a Host	54
Start a Service on a Host	55
Add, Replicate or Delete a Service User	56
Replication and Migration Considerations	57
Procedures	57
Add a Service User Role	60

Procedure	61
Change a Service User Password	62
Create and Manage Service Groups	63
Create a Group	64
Change the Name of a Group	65
Add a Service to a Group	65
View the Services in a Group	65
Remove a Service from a Group	65
Delete a Group	66
Duplicate or Replicate a Service Role	66
Duplicate a Service Role	67
Replicate a Role	67
Edit Core Service Configuration Files	68
Edit a Service Configuration File	68
Revert to a Backup Version of a Service Configuration File	69
Push a Configuration File to Other Services	70
Edit or Delete a Service	81
Procedures	82
Explore and Edit Service Property Tree	83
Procedures	84
Kill a Connection to a Service	85
End a Session on a Service	85
End an Active Query in a Session	86
Search for Services	86
Search for a Service	86
Filter Services by Type	87
Find the Services on a Host	89
Start, Stop or Restart a Service	90
Start a Service	90
Stop a Service	90
Restart a Service	91
View Service Details	91
Purpose of Each Service View	91
Access a Service View	91
Hosts and Services Views References	94
Hosts View	95

Workflow	95
What do you want to do?	95
Quick Look	96
Hosts Panel Toolbar	96
Groups Panel Toolbar	98
Services View	99
Workflow	99
What do you want to do?	100
Related Topics	100
Quick Look	100
Add Service or Edit Service Dialog	103
Groups Panel Toolbar	106
Services Panel Toolbar	107
Services Config View	109
Topic	113
Features	115
Edit a Service Configuration File	116
Files Tab Toolbar	117
Services Explore View	119
The Node List	120
The Monitor Panel	121
Features	123
Services Logs View	125
Services Security View	127
Roles and Service Access	128
Features	130
Role Name Panel	130
Role Information and Permissions Panel	131
Service User Roles	132
Service User Permissions	133

Features	137
SDK Meta Role Permissions Options	138
Features	140
User List Panel	140
User Definition Panel	142
Services Stats View	145
Summary Stats Section	146
Gauges	150
Timelines	150
Historical Timelines	150
Chart Stats Tray	150
Components	151
Features	153
System View	155
Services Info Toolbar	156
Features	158
Host Task Selection List	159
Service Configuration Settings	161
Appliance Service Configuration Parameters	161
Archiver Service Configuration View	161
Broker Service Configuration Parameters	163
Aggregation Configuration Parameters	164
Concentrator Service Configuration Parameters	167
Core Service Logging Configuration Parameters	168
Core Service-to-Service Configuration Parameters	170
Core Service System Configuration Parameters	171
Decoder Service Configuration Parameters	172
Decoder and Log Decoder Configuration Parameters	173
Log Decoder Service Configuration View	177

Log Decoder Service Configuration Parameters	179
REST Interface Configuration Parameters	183
NetWitness Suite Core Service system.roles Modes	184
Troubleshooting Version Updates	185

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.

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
- Concentrator
- Context Hub
- Decoder
- Event Stream Analysis

- Event Stream Analytics
- 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.

Name	Host	Services	Current Version	Update Version	Status
<input checked="" type="checkbox"/> NW Server	IP-address	8	11.0.0.0		Up-to-Date
<input type="checkbox"/> Archiver	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Broker	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Concentrator	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Decoder - Packets	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Event Stream Analysis	IP-address	3	11.0.0.0		Up-to-Date
<input type="checkbox"/> Log Decoder	IP-address	1	11.0.0.0		Up-to-Date

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 NetWitness Suite 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 NetWitness Suite 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.
Investigate	Co-located on NW Server host with the Admin server , Config server , Orchestration server , Respond server , and Security server .
Orchestration	Internal, system management service that runs on the NW Server to provision, install, and configure all services in your NetWitness Suite deployment.
Respond	Co-located on NW Server host with the Admin server , Config server , Investigate server , Orchestration server , and Security server .

Service	Purpose
Security	<p>The NetWitness Suite Security Server (Security server) manages the security infrastructure of a NetWitness Suite deployment. It handles the following security-related concerns.</p> <ul style="list-style-type: none"> • Users and the authentication accounts • Role Based Access Control (RBAC) • Deployment PKI infrastructure <p>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.</p> <p>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.</p>

Running in Mixed Mode

Functionality Gaps Encountered During in Staggered Updates

If you stagger the update, you:

- 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

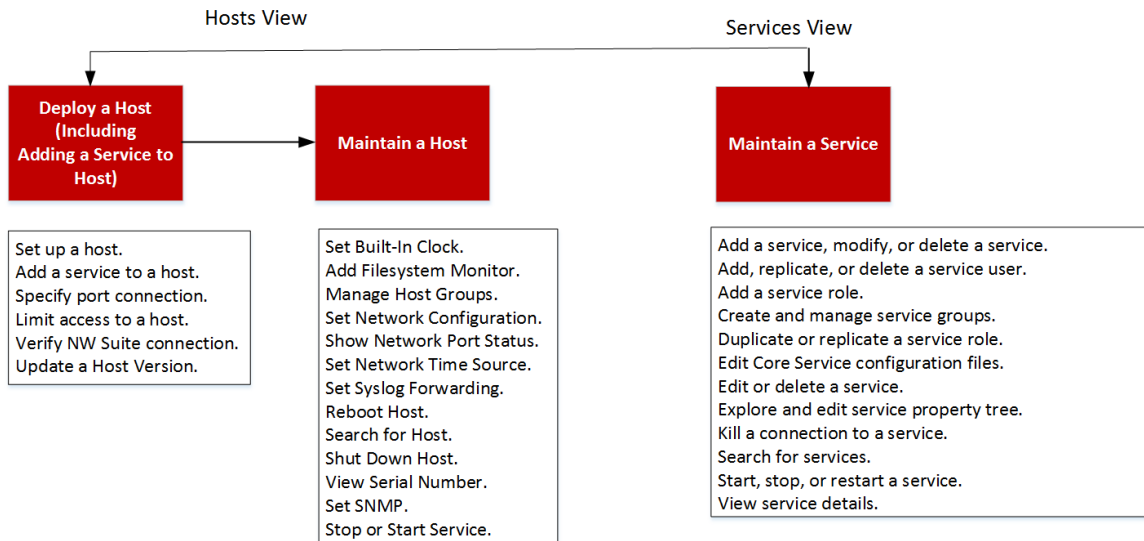
1. Update the NW Server host.
2. Update the Event Stream Analysis host.
3. Update the Malware Analysis host.
4. Update 1 Broker host, 2 Decoder hosts, and 2 Concentrator hosts.
5. Update all other hosts.

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	<p>Complete the following tasks in the order shown to set up a host.</p> <p>Step 1. Deploy a host.</p> <p>Step 2. Install a service on a host.</p> <p>Step 3. Review SSL Ports for Trusted Connections.</p> <p>Step 4. Manage access to a service.</p>

High-Level Task	Description
Maintain a Host - Basics	<p>The following maintenance tasks are not required and are shown in alphabetical order.</p> <ul style="list-style-type: none">• Apply version updates to a host.<ul style="list-style-type: none">• 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	<p>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.</p> <ul style="list-style-type: none">• 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	<p>The following procedures describe how to maintain services.</p> <ul style="list-style-type: none"> • 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*

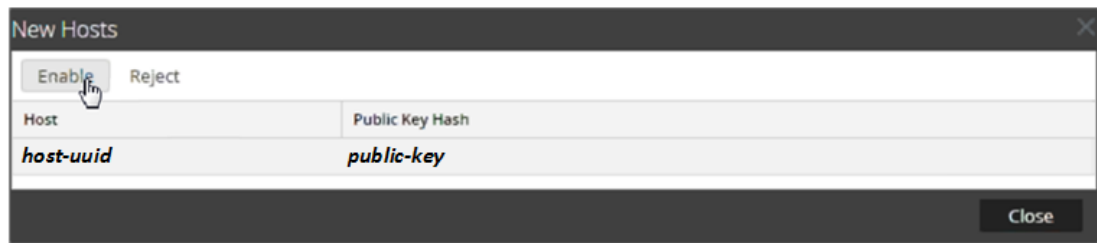
2. Go to **Administration** > **Hosts**.

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.

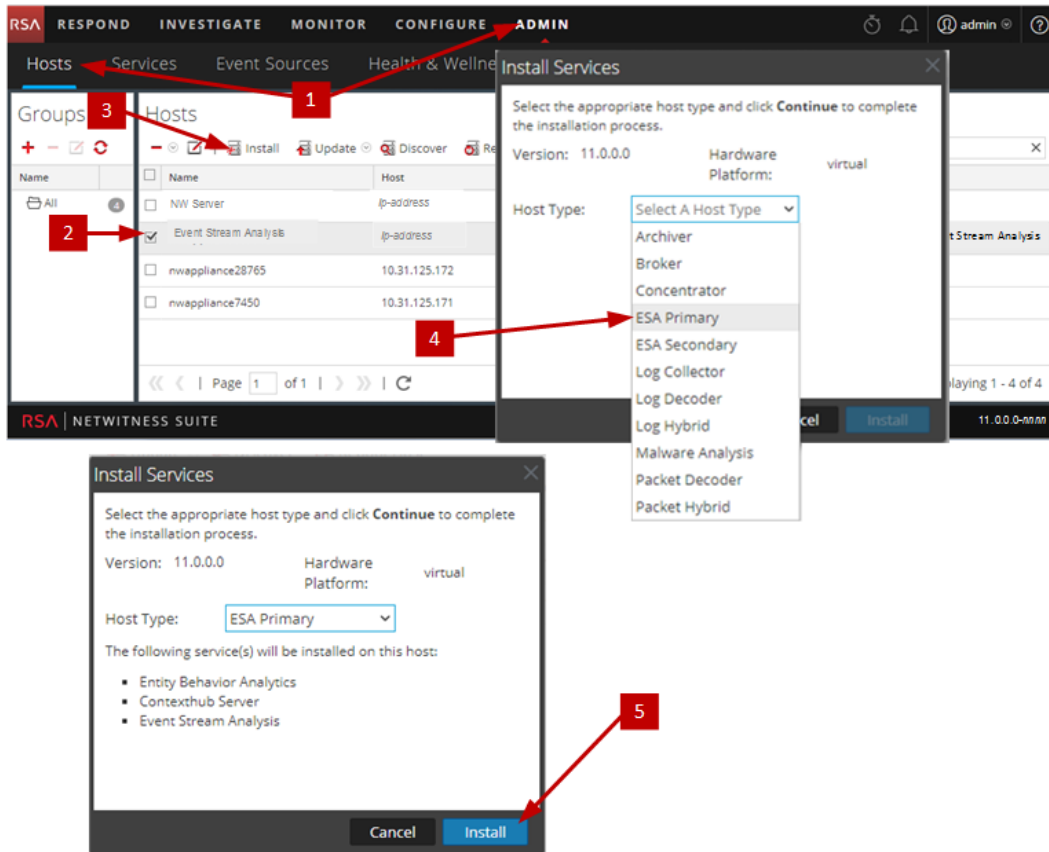
3. Click  (Install Icon) in the toolbar.

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
Archiver	50008	56008
Broker	50003	56003
Concentrator	50005	56005
Context Hub	N/A	50022
Decoder (Packets)	50004	56004
Event Stream Analysis	N/A	50030
Log Collector	50001	56001
Log Decoder	50002	56002
Malware Analysis	N/A	60007
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.

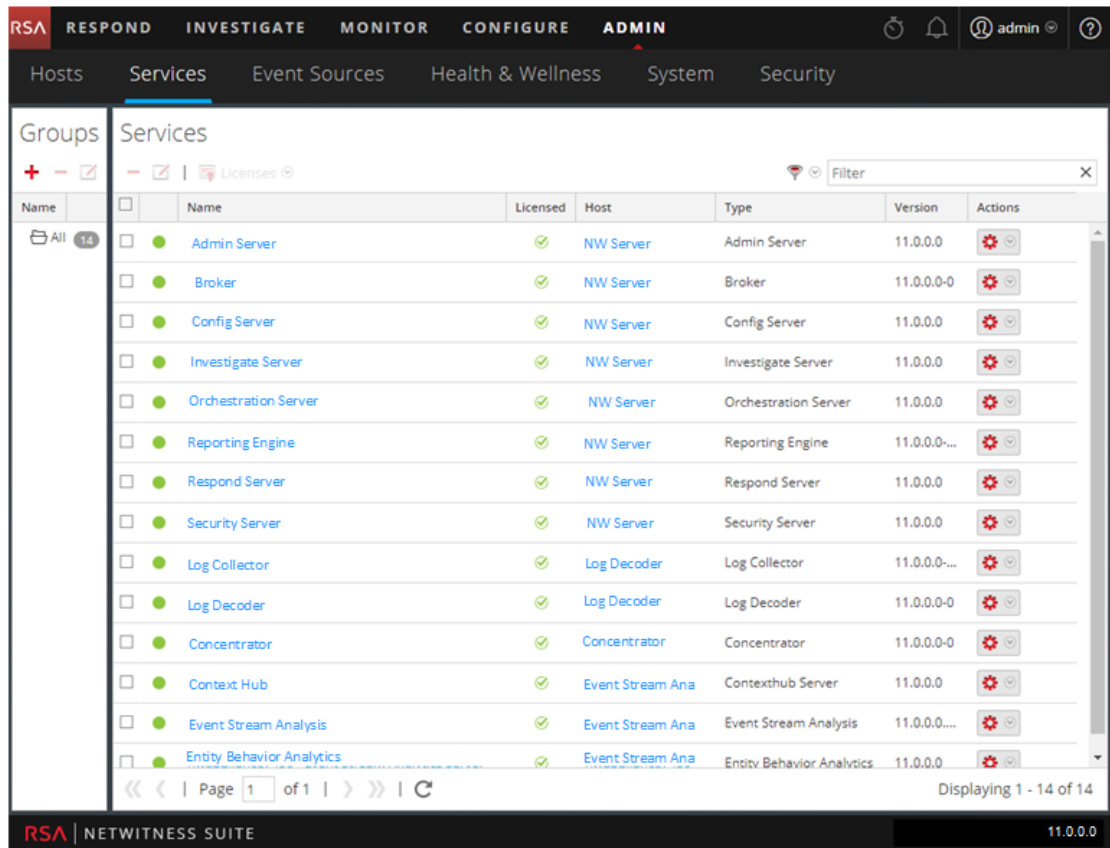
Test a Trusted Connection

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.

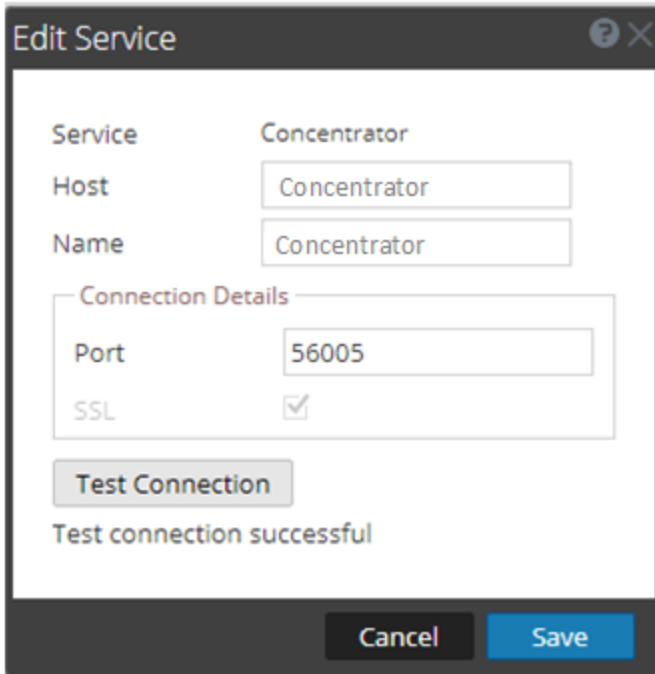


2. Select the service (for example, a Concentrator) to test and click . The **Edit Service** dialog is displayed.

The 'Edit Service' dialog box is shown. It has a title bar with a question mark and a close button. The dialog contains the following fields and controls:

- Service:** Concentrator
- Host:** Concentrator
- Name:** Concentrator
- Connection Details:**
 - Port:** 56005
 - SSL:** ☒
- Test Connection:** A button to test the connection.
- Cancel:** A button to cancel the operation.
- Save:** A button to save the changes.

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 screenshot shows a dialog box titled "Edit Service" with a question mark icon and a close button. Inside the dialog, there are several fields: "Service" is set to "Concentrator", "Host" is "Concentrator", and "Name" is "Concentrator". Below these is a section titled "Connection Details" which contains a "Port" field set to "56005" and an "SSL" checkbox that is checked. At the bottom of the dialog, there is a "Test Connection" button. Below this button, the text "Test connection successful" is displayed. At the very bottom of the dialog, there are "Cancel" and "Save" buttons.

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

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

- [Apply updates from the Host view \(Web Access\)](#)
- [Apply update from the command line \(No Web Access\)](#)

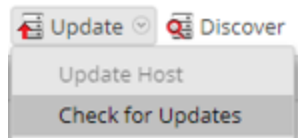
Apply Updates from the Hosts View (Web Access)

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: When you update the NetWitness Server host (also referred to as the NW Server host), NetWitness Suite backs up the System Management Service (SMS) configuration files (excluding the `wrapper.conf` file) from the `/opt/rsa/sms/conf` directory to `/opt/rsa/sms/conf_%timestamp%` directory. This is a precautionary measure for the rare occasion when you may need to restore the SMS configuration from backup. To do this, replace the files in the `/opt/rsa/sms/conf` directory with the files backed up to the `/opt/rsa/sms/conf_%timestamp%` directory after the update.

1. Log in to NetWitness Suite.
2. Make sure that the Local Update Repo is populated.
See [Populate Local Update Repo](#) for instructions.
3. Go to **ADMIN > HOSTS**.
4. (Conditional) Check for the latest updates.

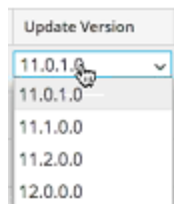


5. Select a host or hosts.

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](#).


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

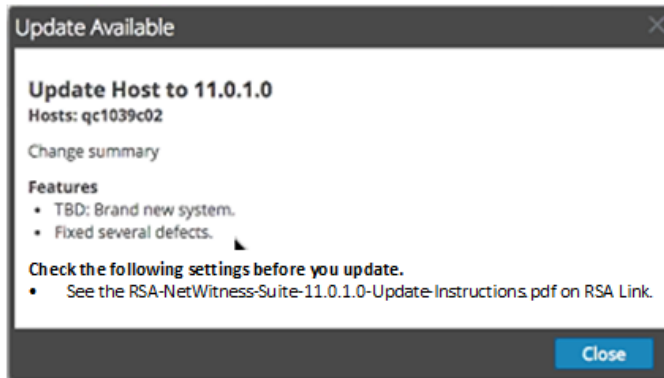
6. Select the version you want to apply from the **Update Version** column.



If you:

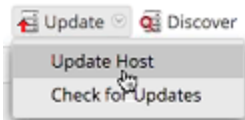
- Want to update more than one host to that version, select the checkbox to the left of the hosts. Only currently supported update versions are listed.

- 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.

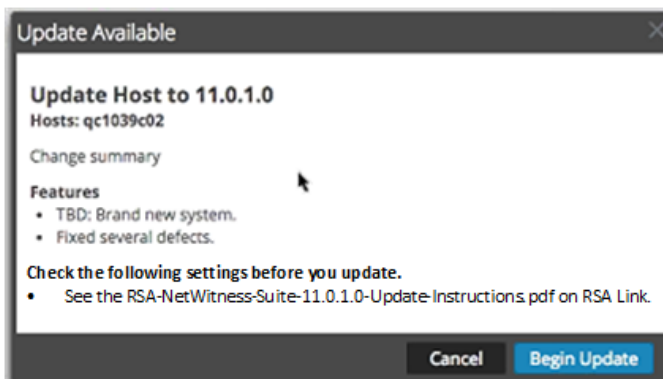


- Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show **Update Available**. By default, only supported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

7. 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 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.

See [Troubleshooting Version Updates](#) if you encounter an error when updating a host to a new version.

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, 11.0.1.0 is the version used as an example in the code strings of any 11.0 version.

1. Download .zip update package for the version you want (for example, netwitness-11.0.1.0.zip) from RSA Link (<https://community.rsa.com/>) > NetWitness Suite > RSA NetWitness Logs and Packets Downloadsto a local directory.

Note: In command line, if there are multiple updates available for a host and you want to skip an earlier update, you must download the interim updates too. For example, the host is running 11.0.0.1 and the 11.0.0.2 and 11.0.0.3 updates are available for that host. If you want to update directly to 11.0.0.3, you must:

1. Download both 11.0.0.2 and 11.0.0.3.
2. Initialize to 11.0.0.3.
3. Apply the 11.0.0.3 update to the host.

You do not need to apply 11.0.0.2 update if you set up 11.0.0.2 and 11.0.0.3 in the stage directory before you run the initialization.

2. Transfer the .zip update package file to a local directory on the to the NW Server host.
3. SSH to the NW Server host.
4. Make a tmp/upgrade/<version> staging directory for the version you want (for example, tmp/upgrade/11.0.1.0).

```
mkdir -p /tmp/upgrade/11.0.1.0
```
5. Change the directory to the staging directory.

```
cd /tmp/upgrade/11.0.1.0
```
6. Directly unzip the file from the local directory to the staging directory.

```
unzip <local directory>/netwitness-11.0.1.0.zip
```

Note: If you copied the .zip file to the created staging directory to unzip. Make sure that you delete the initial .zip file you copied to the staging location, after you extract it.

7. Initialize the update on the NW Server.

8. Apply the update to the NW Server.

```
upgrade-cli-client --init --version 11.0.1.0 --stage-dir  
/tmp/upgrade/
```

9. Restart the NW Server.

10. Apply update to each non-NW Server host.

```
upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -  
-version 11.0.1.0
```

The update is complete when the polling is completed.

11. Restart the host.

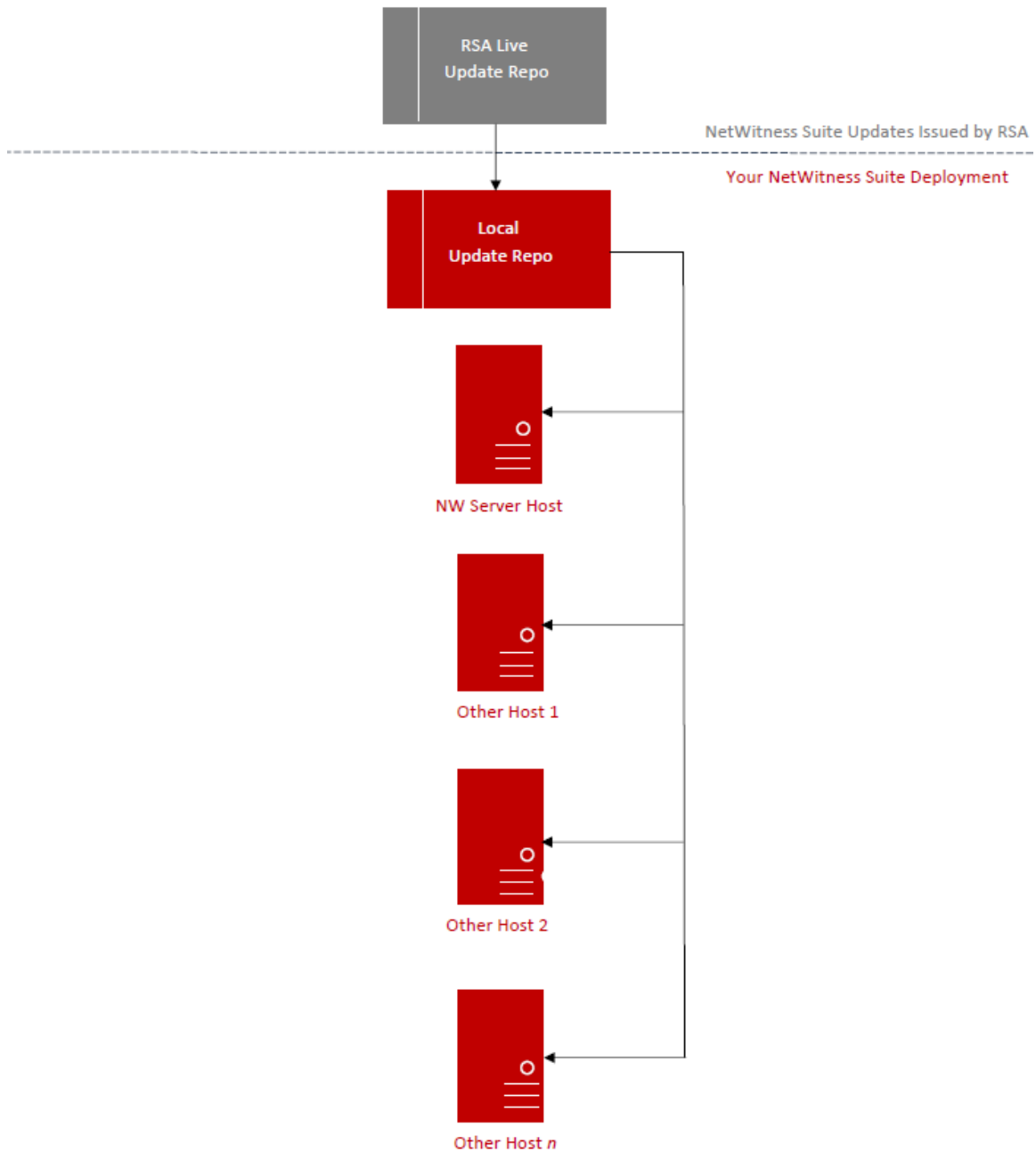
You can verify the version applied to the host with the following command:

```
upgrade-cli-client --list
```

Populate Local Update Repository

The following diagram illustrates how you obtain versions updates if your NetWitness Suite deployment has Web Access. See [Apply Updates from Command Line](#) if your NetWitness Suite deployment does not have Web Access.

RSA NetWitness Suite 11.x Version Update Workflow – 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 Security Analytics Server’s Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository.

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 for NetWitness Suite* in the *NetWitness Suite System Configuration Guide* in the help on RSA Link (<https://community.rsa.com/>).

Set Up an External Repository with RSA and OS Updates

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
```

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-11.0.0.0.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
```

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.x86_64.rpm	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.rpm	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fnserver-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.rpm	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_64.rpm	03-Oct-2017 14:07	143496
lsaf-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.el7ngx.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
nwpdextractor-11.0.0.0-6953.1.dccfe43.el7.x86_64.rpm	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el7.x86_64.rpm	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>/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.

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.

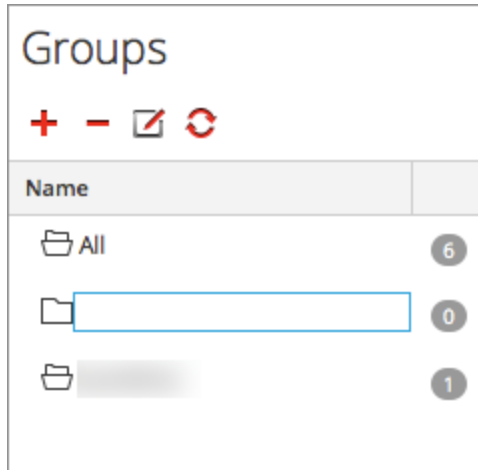
Create a Group

1. Select **ADMIN > Hosts**.

The Hosts view is displayed.

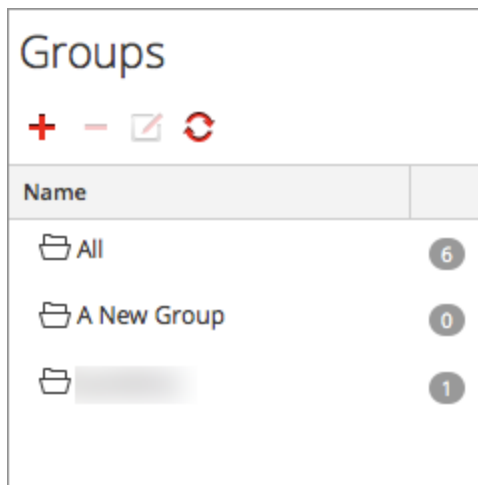
2. In the **Groups** panel toolbar, click **+**.

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.

Name	Host	Services	Current Version	Update Version	Status
<input checked="" type="checkbox"/> NW Server	IP-address	8	11.0.0.0		Up-to-Date
<input type="checkbox"/> Archiver	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Broker	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Concentrator	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Decoder - Packets	IP-address	1	11.0.0.0		Up-to-Date
<input type="checkbox"/> Event Stream Analysis	IP-address	3	11.0.0.0		Up-to-Date
<input type="checkbox"/> Log Decoder	IP-address	1	11.0.0.0		Up-to-Date

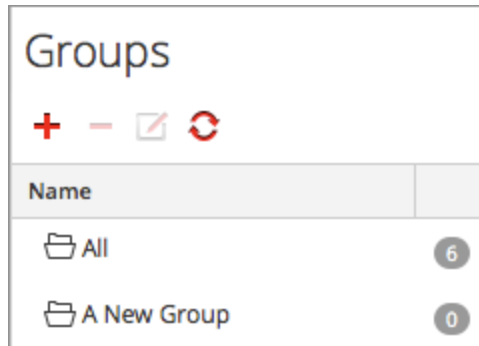
Remove a Host from a Group

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 from Group**.


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

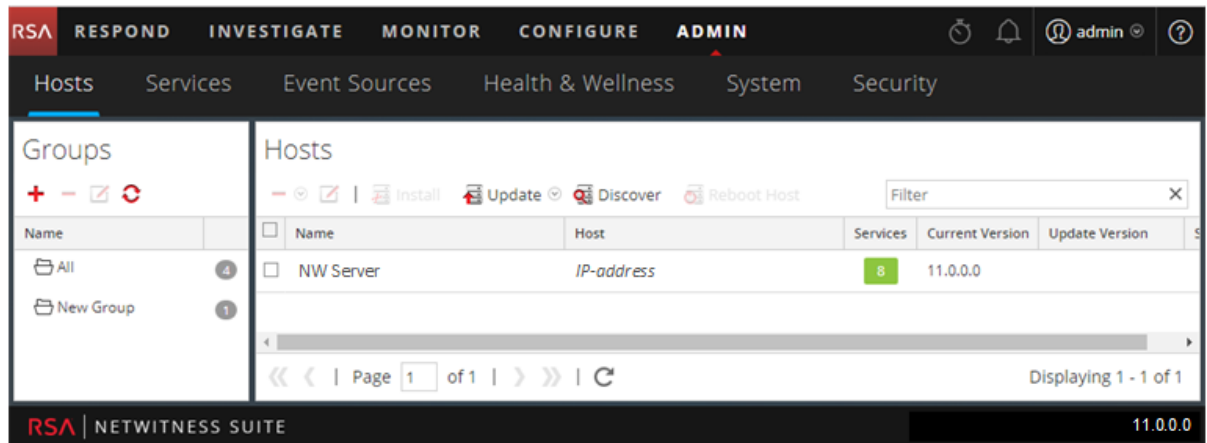
1. Select **ADMIN > Services**.
2. In the Services view, select a service. The associated host is listed in the **Host** column for that service.

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is selected, and the Services view is active. The Services view displays a list of services with the following columns: Name, Licensed, Host, Type, Version, and Actions. The services listed are:

Name	Licensed	Host	Type	Version	Actions
Admin Server	✓	NW Server	Admin Server	11.0.0.0	⚙️
Broker	✓	NW Server	Broker	11.0.0.0-0	⚙️
Config Server	✓	NW Server	Config Server	11.0.0.0	⚙️
Investigate Server	✓	NW Server	Investigate Server	11.0.0.0	⚙️
Orchestration Server	✓	NW Server	Orchestration Server	11.0.0.0	⚙️
Reporting Engine	✓	NW Server	Reporting Engine	11.0.0.0-...	⚙️
Respond Server	✓	NW Server	Respond Server	11.0.0.0	⚙️
Security Server	✓	NW Server	Security Server	11.0.0.0	⚙️
Log Collector	✓	Log Decoder	Log Collector	11.0.0.0-...	⚙️
Log Decoder	✓	Log Decoder	Log Decoder	11.0.0.0-0	⚙️
Concentrator	✓	Concentrator	Concentrator	11.0.0.0-0	⚙️
Context Hub	✓	Event Stream Ana	Contexthub Server	11.0.0.0	⚙️
Event Stream Analysis	✓	Event Stream Ana	Event Stream Analysis	11.0.0.0-...	⚙️
Entity Behavior Analytics	✓	Event Stream Ana	Entity Behavior Analytics	11.0.0.0	⚙️

The interface also shows a sidebar with 'Groups' and 'Services' sections, a search filter, and a footer indicating 'RSA | NETWITNESS SUITE' and version '11.0.0.0'.

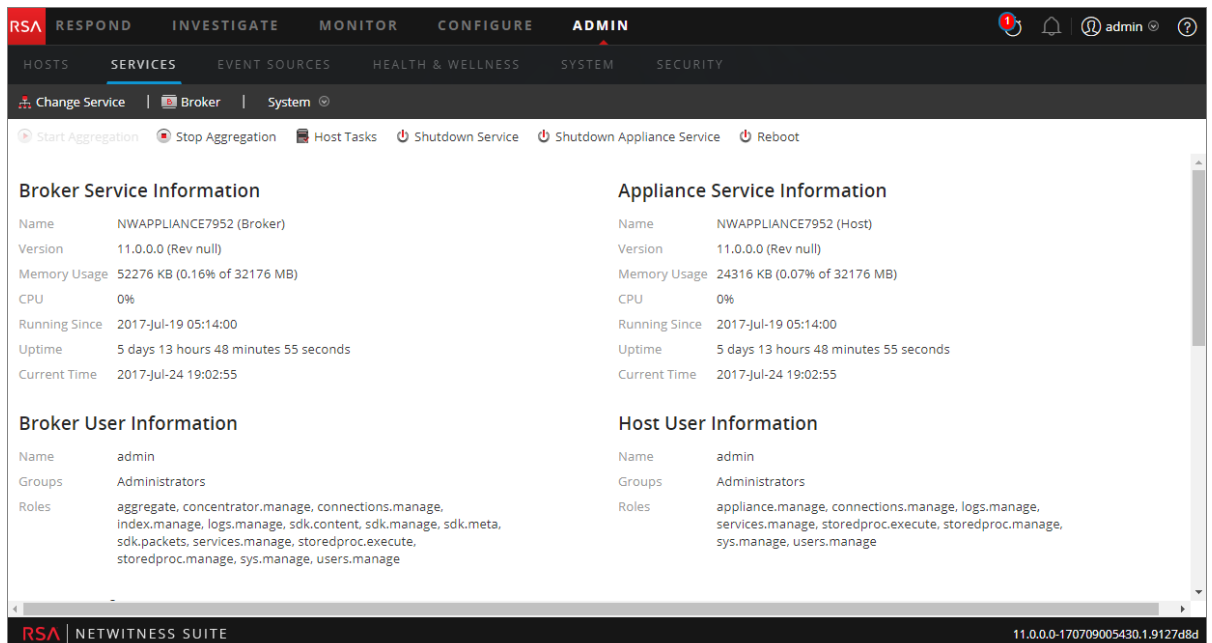
- To administer the host in the Hosts view, click the link in the **Host** column for that service. The host associated with the selected service is displayed in the Hosts view.



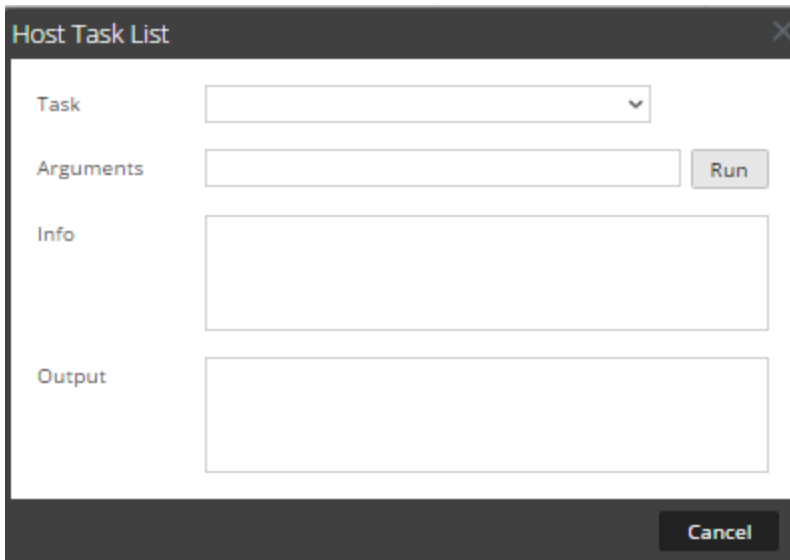
Execute a Task From the Host Task List

- Select **ADMIN > Services**.
- 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.

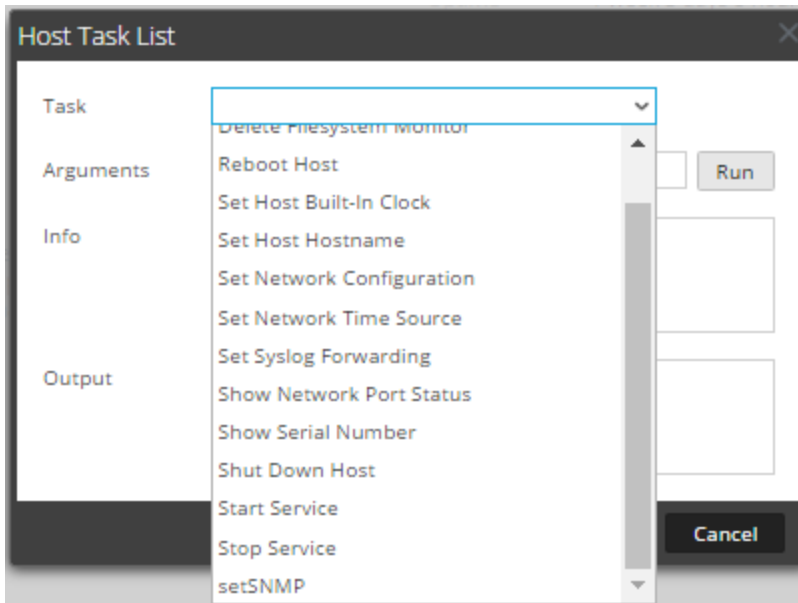


3. In the **Services System** view toolbar, click  **Host Tasks**.



The **Host Task List** dialog box is shown. It has a title bar with a close button. Inside, there are four labeled sections: **Task** with a dropdown menu, **Arguments** with a text input field and a **Run** button to its right, **Info** with a large text area, and **Output** with another large text area. At the bottom right is a **Cancel** button.

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

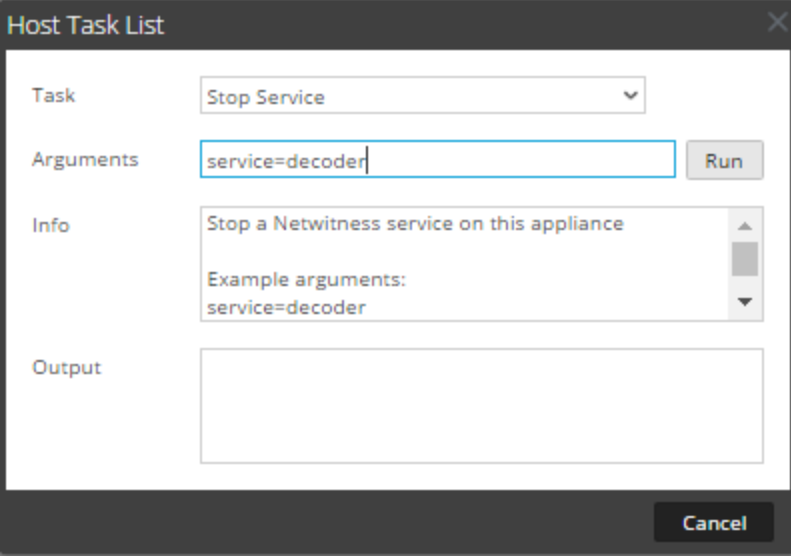


The **Host Task List** dialog box is shown with the **Task** dropdown menu open. The list of tasks includes: Delete Filesystem Monitor, Reboot Host, Set Host Built-In Clock, Set Host Hostname, Set Network Configuration, Set Network Time Source, Set Syslog Forwarding, Show Network Port Status, Show Serial Number, Shut Down Host, Start Service, Stop Service, and setSNMP. The **Run** button is visible to the right of the dropdown, and the **Cancel** button is at the bottom right.

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.

A screenshot of the 'Host Task List' dialog box. It has a title bar with a close button. Inside, there are four sections: 'Task' with a dropdown menu showing 'Stop Service'; 'Arguments' with a text input field containing 'service=decoder' and a 'Run' button to its right; 'Info' with a text area containing 'Stop a Netwitness service on this appliance' and 'Example arguments: service=decoder'; and 'Output' with an empty text area. A 'Cancel' button is at the bottom right.



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

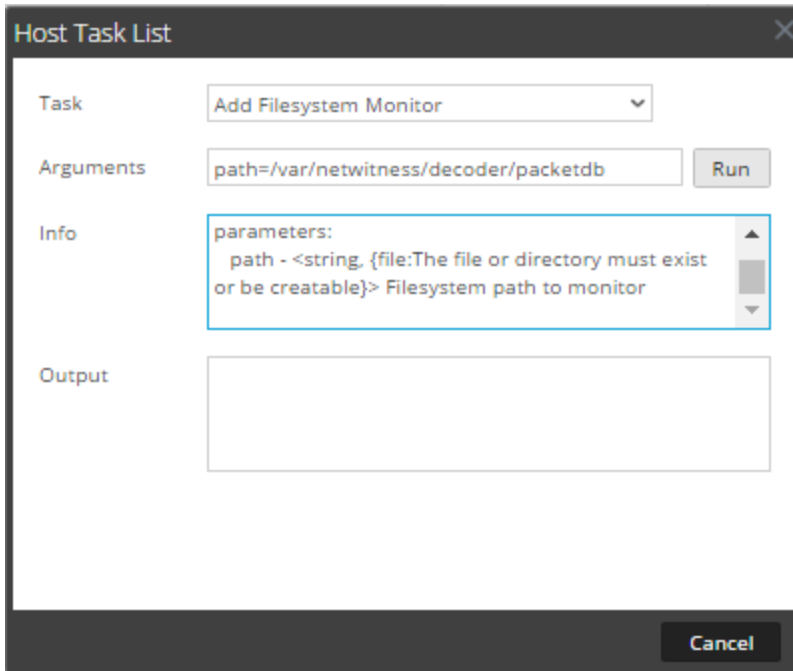
When you want a service to monitor traffic on a specific file system, you can select the service and then specify the path. Security Analytics adds a filesystem monitor. Once a file system monitor is added to a service, the service continues to monitor traffic on that path until the file system monitor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

Configure the Filesystem Monitor

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

- To identify the file system to monitor, type the path in the **Arguments** field. For example:
path=/var/netwitness/decoder/packetdb



The image shows a dialog box titled "Host Task List" with a close button (X) in the top right corner. It contains four main sections: "Task", "Arguments", "Info", and "Output". The "Task" section has a dropdown menu currently set to "Add Filesystem Monitor". The "Arguments" section has a text input field containing "path=/var/netwitness/decoder/packetdb" and a "Run" button to its right. The "Info" section is highlighted with a blue border and contains a scrollable text area with the following text: "parameters: path - <string, {file:The file or directory must exist or be creatable}> Filesystem path to monitor". The "Output" section is an empty text area. At the bottom right of the dialog is a "Cancel" button.

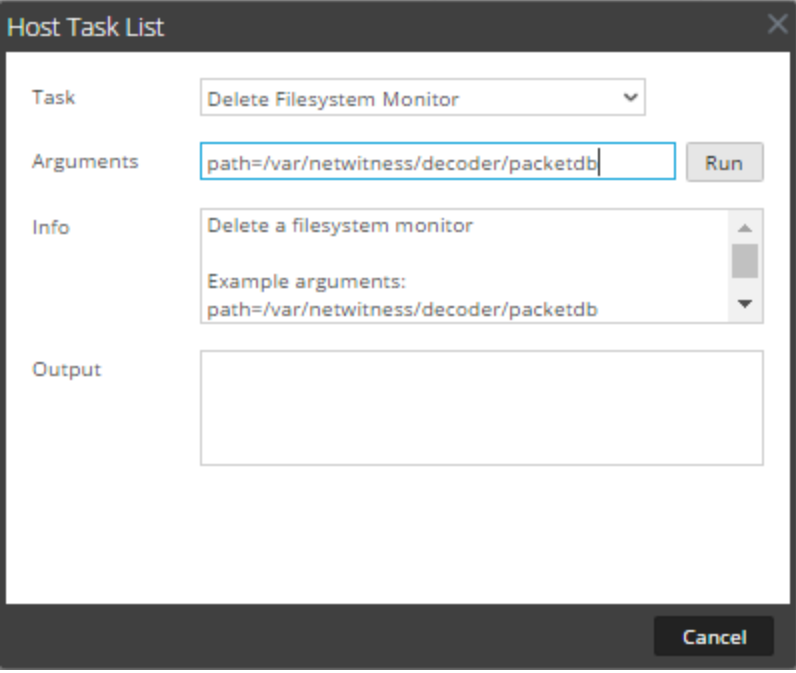
- Click **Run**.

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

- Navigate to the **Host Task List** dialog.
- 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.
- To identify the filesystem to stop monitoring, type the path in the **Arguments** field. For example:

path=/var/netwitness/decoder/packetdb

A screenshot of a 'Host Task List' dialog box. The dialog has a title bar with a close button. It contains four sections: 'Task' with a dropdown menu showing 'Delete Filesystem Monitor'; 'Arguments' with a text input field containing 'path=/var/netwitness/decoder/packetdb' and a 'Run' button; 'Info' with a text area showing 'Delete a filesystem monitor' and 'Example arguments: path=/var/netwitness/decoder/packetdb'; and 'Output' with an empty text area. A 'Cancel' button is at the bottom right.

Host Task List

Task: Delete Filesystem Monitor

Arguments: path=/var/netwitness/decoder/packetdb [Run]

Info: Delete a filesystem monitor
Example arguments:
path=/var/netwitness/decoder/packetdb

Output:

[Cancel]

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:

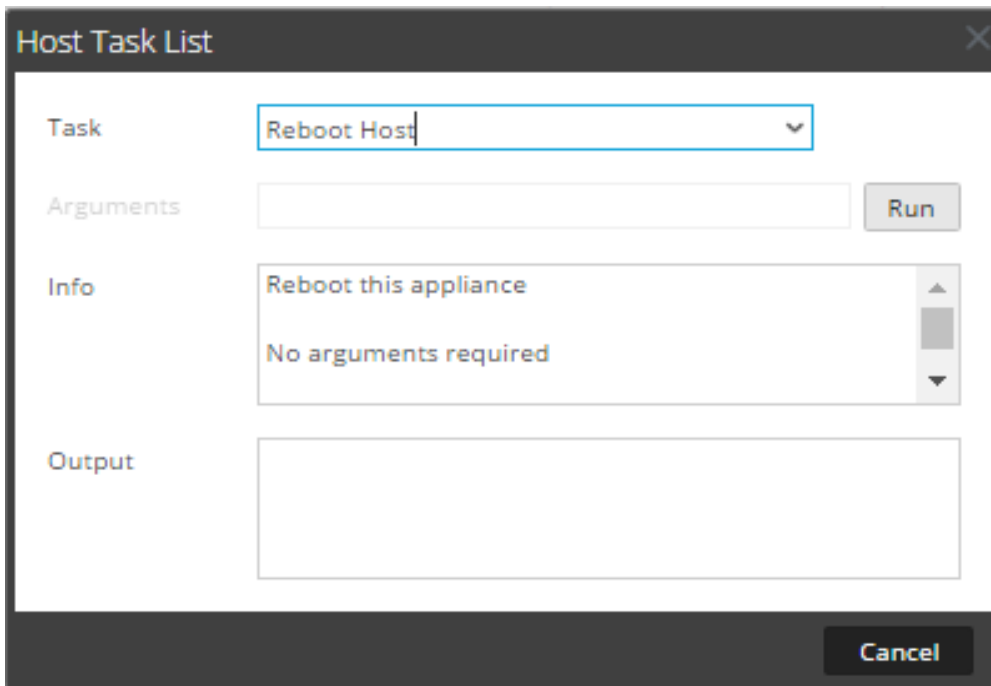
- To shut down and restart a host through an attached service, go to the Hosts view from a service in the Services view (see [Search for Hosts](#)) and then follow the *Shut Down and Restart a Host from the Hosts View* procedure below.
- To shut down the physical host without restarting, see [Shut Down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



The image shows a dialog box titled "Host Task List". It has a dark grey header bar with a close button (X) in the top right corner. The main content area is white and contains the following elements:



- Task:** A dropdown menu with "Reboot Host" selected.
- Arguments:** A text input field that is currently empty.
- Run:** A grey button with the text "Run" in white.
- Info:** A text area containing the text "Reboot this appliance" and "No arguments required".
- Output:** A large, empty text area for displaying results.
- Cancel:** A dark grey button with the text "Cancel" in white, located at the bottom right of the dialog.

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

Set Host Built-In Clock

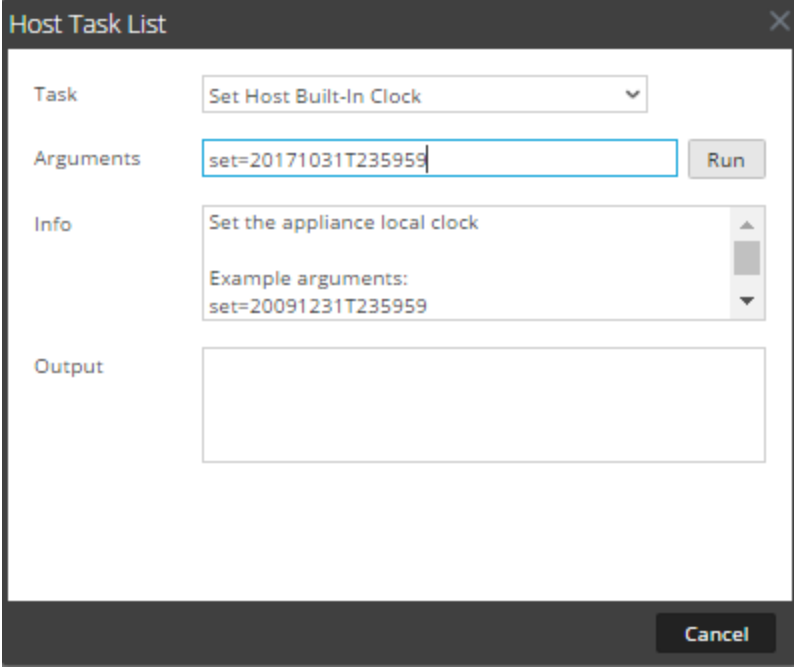
After a shutdown or battery failure, it may be necessary to set the local clock on a host. The Set Host Built-In Clock task resets the clock time.

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



The screenshot shows a window titled "Host Task List" with a close button (X) in the top right corner. Inside the window, there are four main sections: "Task", "Arguments", "Info", and "Output". The "Task" section has a dropdown menu currently showing "Set Host Built-In Clock". The "Arguments" section has a text input field containing "set=20171031T235959" and a "Run" button to its right. The "Info" section contains the text "Set the appliance local clock" and "Example arguments: set=20091231T235959". The "Output" section is a large empty text area. At the bottom right of the window is a "Cancel" button.



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

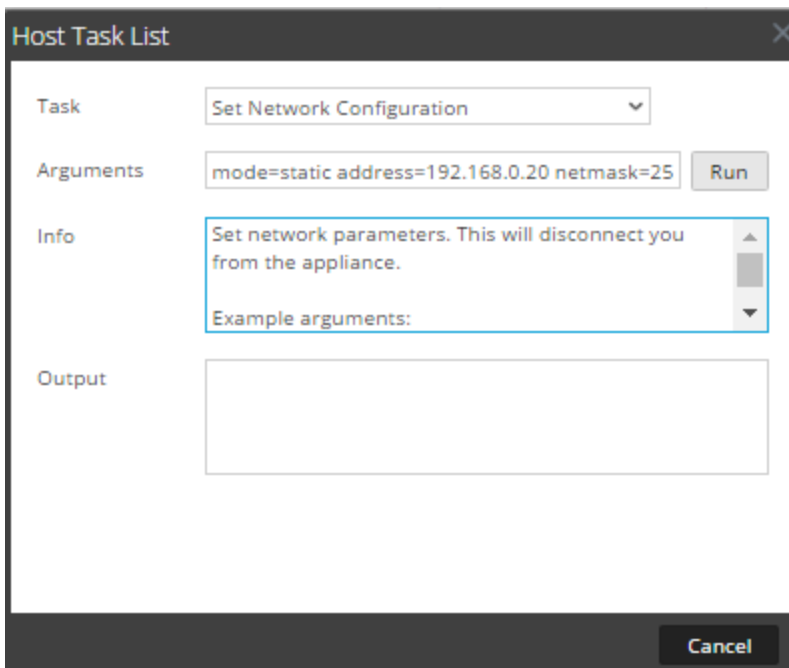
Set Network Configuration

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



Host Task List

Task: Set Network Configuration

Arguments: mode=static address=192.168.0.20 netmask=25 **Run**

Info: Set network parameters. This will disconnect you from the appliance.
Example arguments:

Output:

Cancel



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.

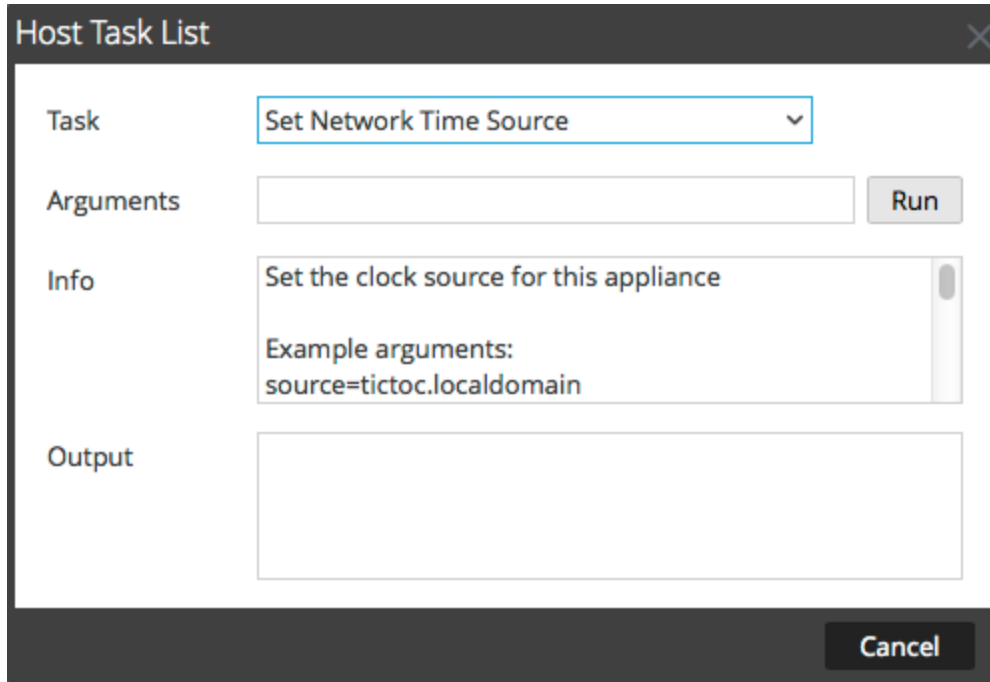
Note: If the mode is DHCP, there may be no way to determine the new address. You may have to connect to the host directly to determine the new address.

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**.

A screenshot of the 'Host Task List' dialog box. It has a dark grey header with the title 'Host Task List' and a close button. The main area is white and contains four sections: 'Task' with a dropdown menu showing 'Set Network Time Source'; 'Arguments' with a text input field and a 'Run' button; 'Info' with a text area containing 'Set the clock source for this appliance' and 'Example arguments: source=tictoc.localdomain'; and 'Output' with an empty text area. A 'Cancel' button is at the bottom right.

Host Task List

Task: Set Network Time Source

Arguments: Run

Info: Set the clock source for this appliance
Example arguments:
source=tictoc.localdomain

Output:

Cancel



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.

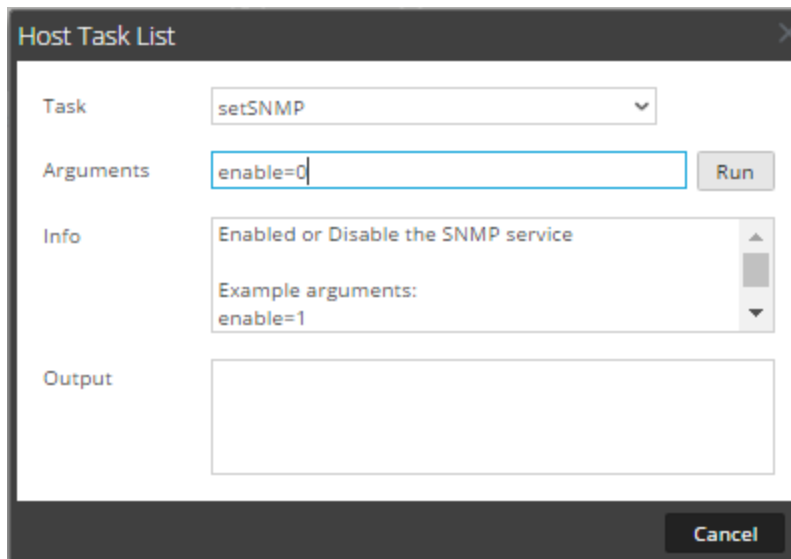
Note: If you specified a NTP clock source of **local**, the host clock serves as the clock source and the time is configured using [Set Host Built-In Clock](#).

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.

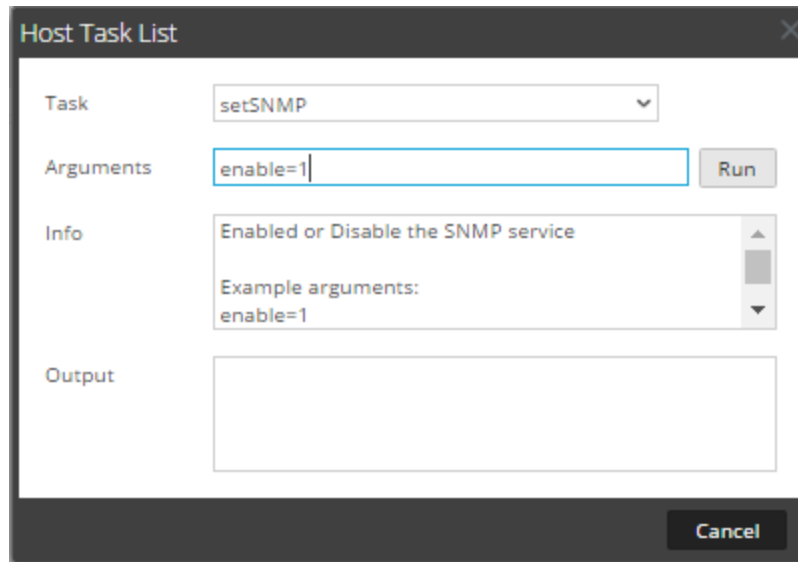
Toggle SNMP Service on the Host

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.



The image shows a screenshot of the 'Host Task List' dialog box. It has a title bar with 'Host Task List' and a close button. The dialog is divided into several sections: 'Task' with a dropdown menu showing 'setSNMP'; 'Arguments' with a text input field containing 'enable=0' and a 'Run' button; 'Info' with a text area containing 'Enabled or Disable the SNMP service' and 'Example arguments: enable=1'; and 'Output' with an empty text area. A 'Cancel' button is located at the bottom right.

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



The image shows a 'Host Task List' dialog box. It has a title bar with a close button. Inside, there are four sections: 'Task' with a dropdown menu showing 'setSNMP'; 'Arguments' with a text input field containing 'enable=1' and a 'Run' button to its right; 'Info' with a text area containing 'Enabled or Disable the SNMP service' and 'Example arguments: enable=1'; and 'Output' with an empty text area. At the bottom right is a 'Cancel' button.



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.

The screenshot shows a window titled "Host Task List". It has a "Task" dropdown menu with "Set Syslog Forwarding" selected. Below it is an "Arguments" text input field and a "Run" button. The "Info" section contains a text area with "Enable or disable syslog forwarding" and "Example arguments: host=loghost.localdomain". At the bottom is an "Output" text area and a "Cancel" button.

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.

The image shows a 'Host Task List' dialog box. It has a title bar with a close button. Inside, there are four sections: 'Task' with a dropdown menu showing 'Show Network Port Status'; 'Arguments' with an empty text box and a 'Run' button; 'Info' with a text area showing 'Show interface information' and 'No arguments required'; and 'Output' with a text area showing 'lo: link up' and 'eth0: link up'. A 'Cancel' button is at the bottom right.

Show Serial Number

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

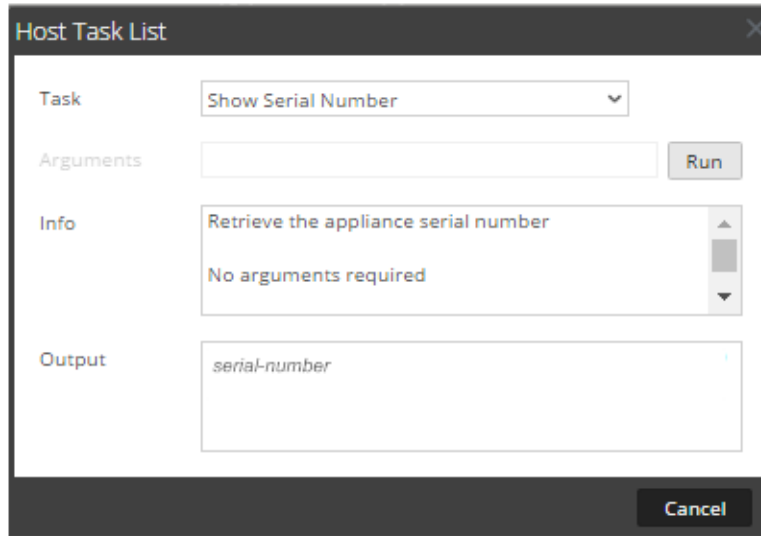
Show the Serial Number

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.



The image shows a 'Host Task List' dialog box. It has a title bar with a close button. Inside, there are four sections: 'Task' with a dropdown menu set to 'Show Serial Number'; 'Arguments' with an empty text field and a 'Run' button; 'Info' with a scrollable area containing the text 'Retrieve the appliance serial number' and 'No arguments required'; and 'Output' with a text area displaying 'serial-number'. A 'Cancel' button is at the bottom right.

Shut Down Host

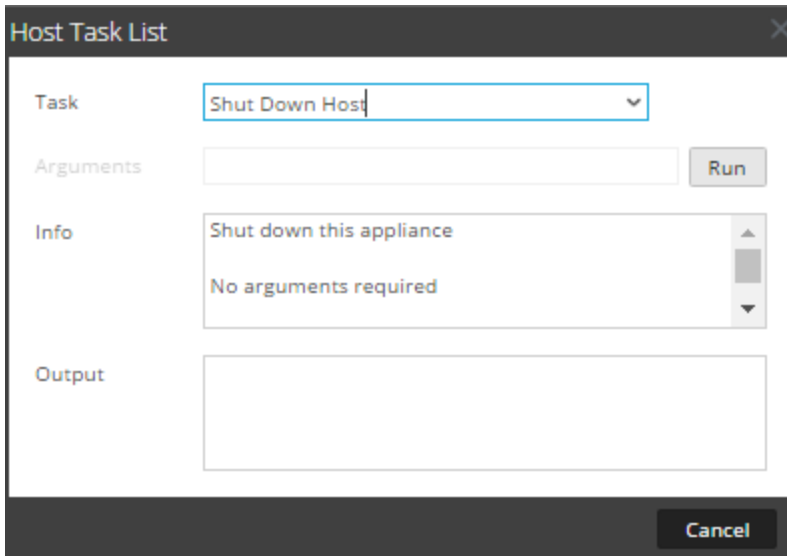
Under certain circumstances; for example, a hardware upgrade or an extended power outage that exceeds backup power capacity, it may be necessary to shut down a physical host. When you shut down a host, all services running on the host are stopped and the physical host turns off.

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

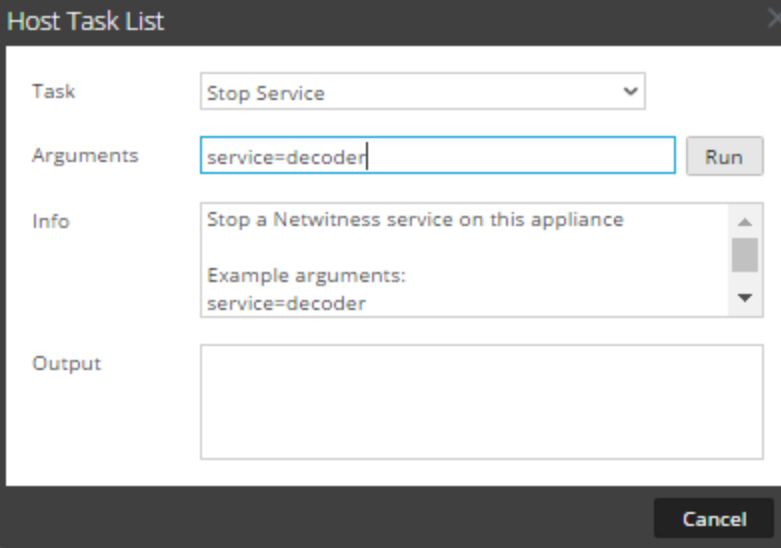
The Host Task List has two options for stopping and starting a service on a host. When you stop a service using the **Stop Service** message, all processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically.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

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



The image shows a 'Host Task List' dialog box with a dark header and a light gray body. It contains four main sections: 'Task' with a dropdown menu set to 'Stop Service'; 'Arguments' with a text input field containing 'service=decoder' and a 'Run' button to its right; 'Info' with a text area containing 'Stop a Netwitness service on this appliance' and 'Example arguments: service=decoder'; and 'Output' with an empty text area. A 'Cancel' button is located at the bottom right of the dialog.

- 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

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

service=decoder

The image shows a 'Host Task List' dialog box. It has a title bar with a close button. Inside, there are four sections: 'Task' with a dropdown menu set to 'Start Service'; 'Arguments' with a text input field containing 'service=decoder' and a 'Run' button to its right; 'Info' with a text area containing 'Start a NetWitness service on this appliance' and 'Example arguments: service=decoder'; and 'Output' with an empty text area. At the bottom right is a 'Cancel' button.

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

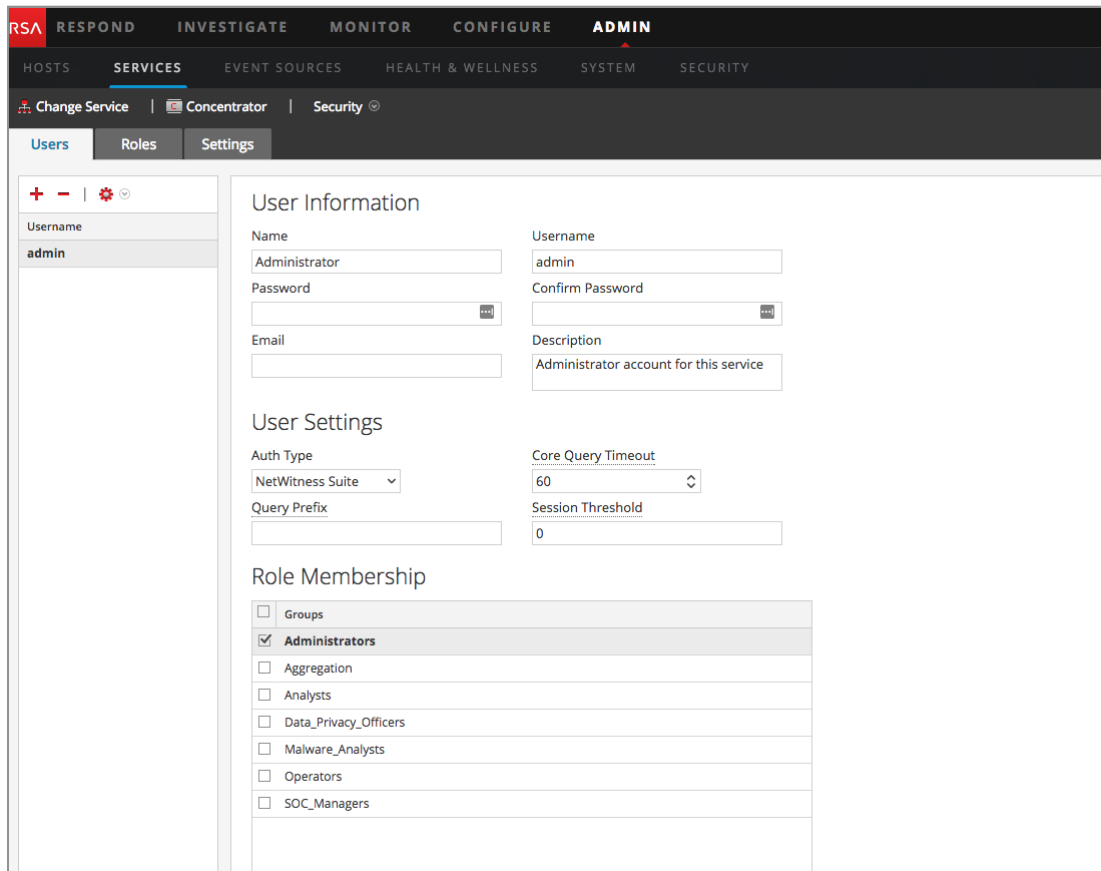
Each of the following procedures starts in the Services Security view.

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.



The screenshot shows the RSA NetWitness Suite Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The 'ADMIN' tab is active, and the 'SECURITY' sub-tab is selected. The left sidebar shows the 'Users' tab, with a list of users including 'admin'. The main content area displays the 'User Information' form for the 'admin' user. The form includes fields for Name, Username, Password, Confirm Password, Email, and Description. The 'User Settings' section includes a dropdown for 'Auth Type' (set to 'NetWitness Suite'), a 'Query Prefix' field, a 'Core Query Timeout' dropdown (set to '60'), and a 'Session Threshold' field (set to '0'). The 'Role Membership' section shows a list of roles with checkboxes, where 'Administrators' is selected.

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.

Replicate User to other services

Please enter and confirm the service user password. The entire service user account replicates to the selected services. The user password also changes on each selected service.

Password


Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	- Broker		Broker
<input type="checkbox"/>	- Conc...		Concentrator
<input type="checkbox"/>	- Archi...		Archiver
<input type="checkbox"/>	- Work...		Workbench
<input type="checkbox"/>	- Log C...		Log Collector
<input type="checkbox"/>	- Log ...		Log Decoder
<input type="checkbox"/>	- Wareh...		Warehouse C...
	NW – Malware A		Malware A

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:

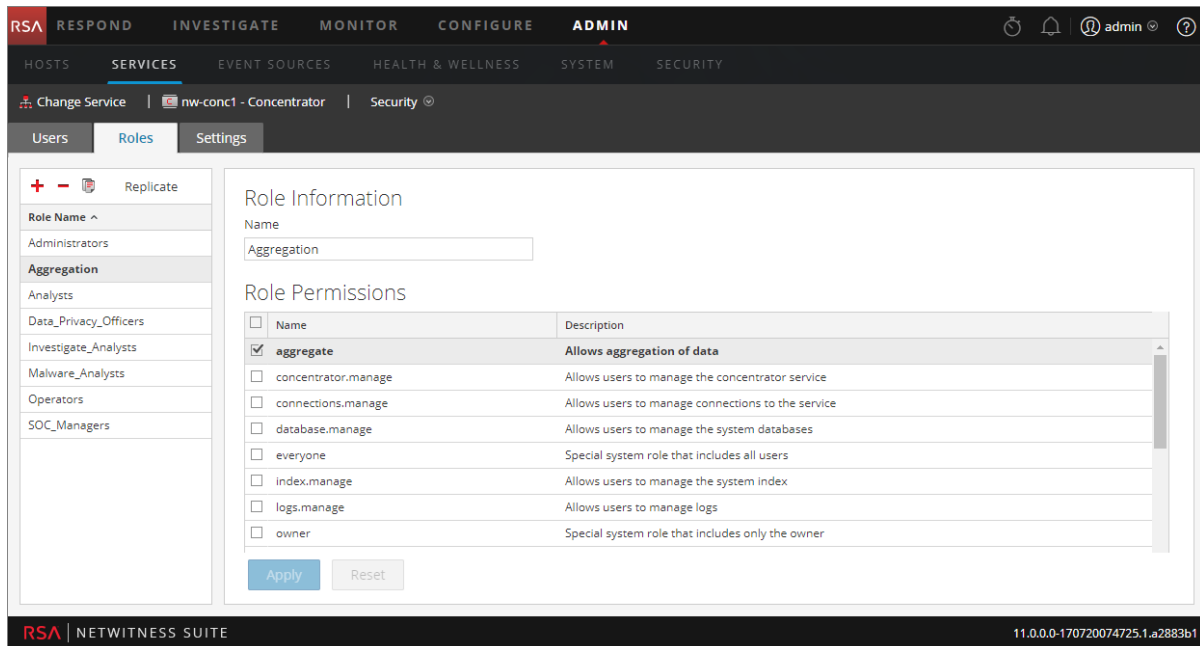
1. In NetWitness Suite, go to **ADMIN > Services**.

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**.
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

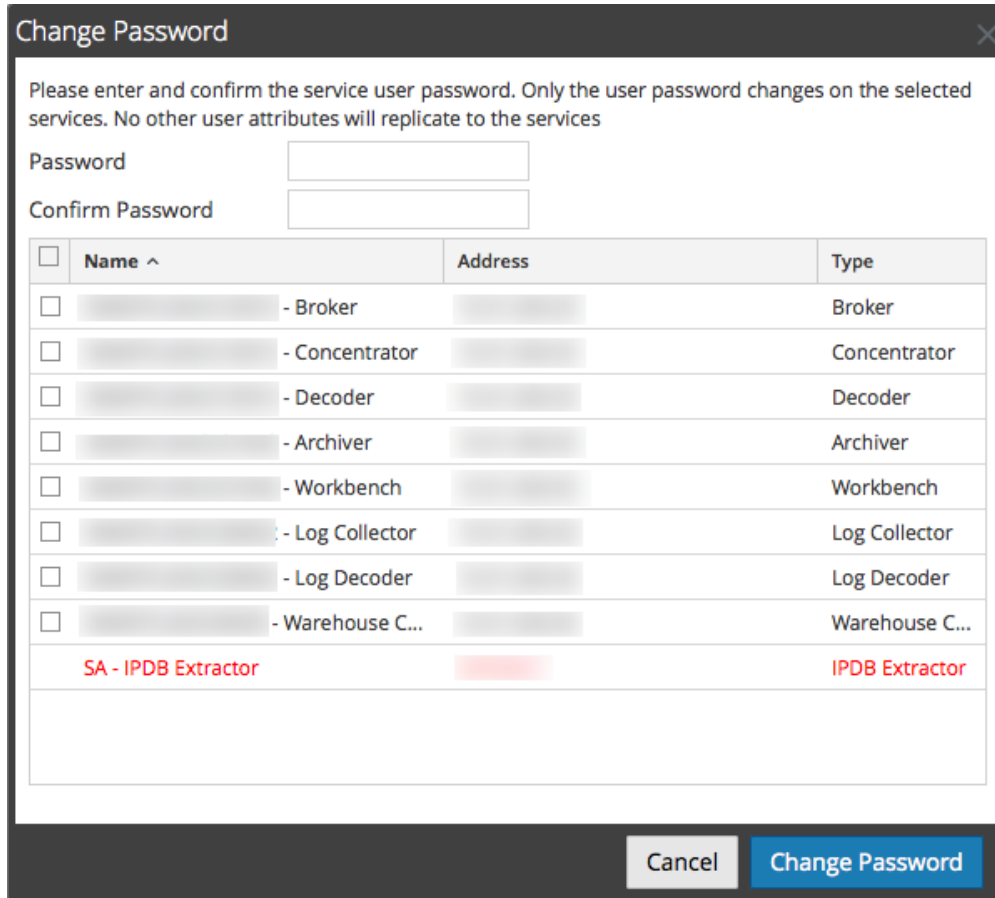
This procedure allows Administrators to change the password of a service user and replicate the new password to all Core services with that user account defined. It replicates only the password change to the Core services selected and does not replicate the entire user account. Administrators can also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



Change Password

Please enter and confirm the service user password. Only the user password changes on the selected services. No other user attributes will replicate to the services

Password

Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	- Broker		Broker
<input type="checkbox"/>	- Concentrator		Concentrator
<input type="checkbox"/>	- Decoder		Decoder
<input type="checkbox"/>	- Archiver		Archiver
<input type="checkbox"/>	- Workbench		Workbench
<input type="checkbox"/>	- Log Collector		Log Collector
<input type="checkbox"/>	- Log Decoder		Log Decoder
<input type="checkbox"/>	- Warehouse C...		Warehouse C...
	SA - IPDB Extractor		IPDB Extractor

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

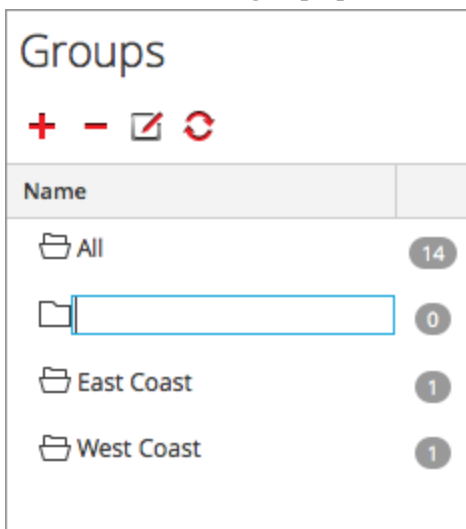
The Administration Services view provides options for creating and managing groups of services. The Services panel toolbar includes options for creating, editing, and deleting service groups. Once groups are created, you can drag individual services from the Services panel into a group.

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.

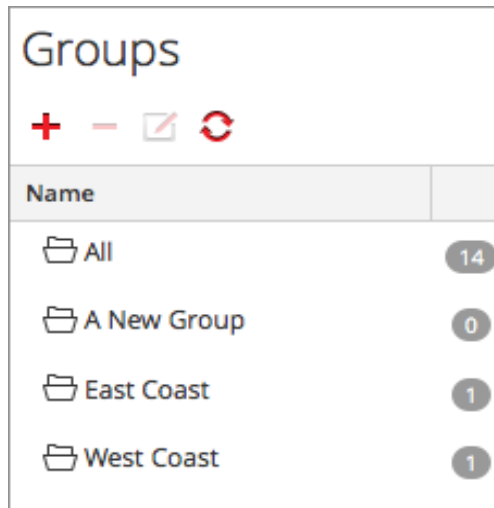
Create a Group

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.

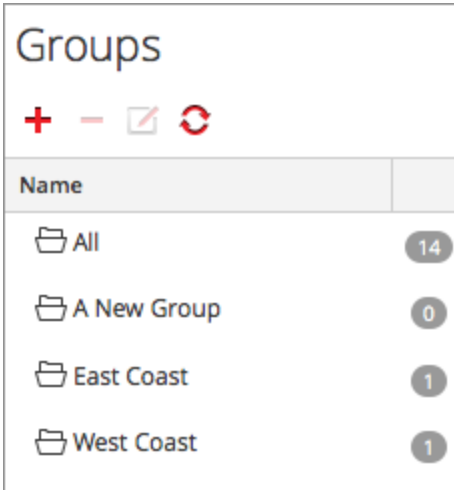
Remove a Service from a Group

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**.

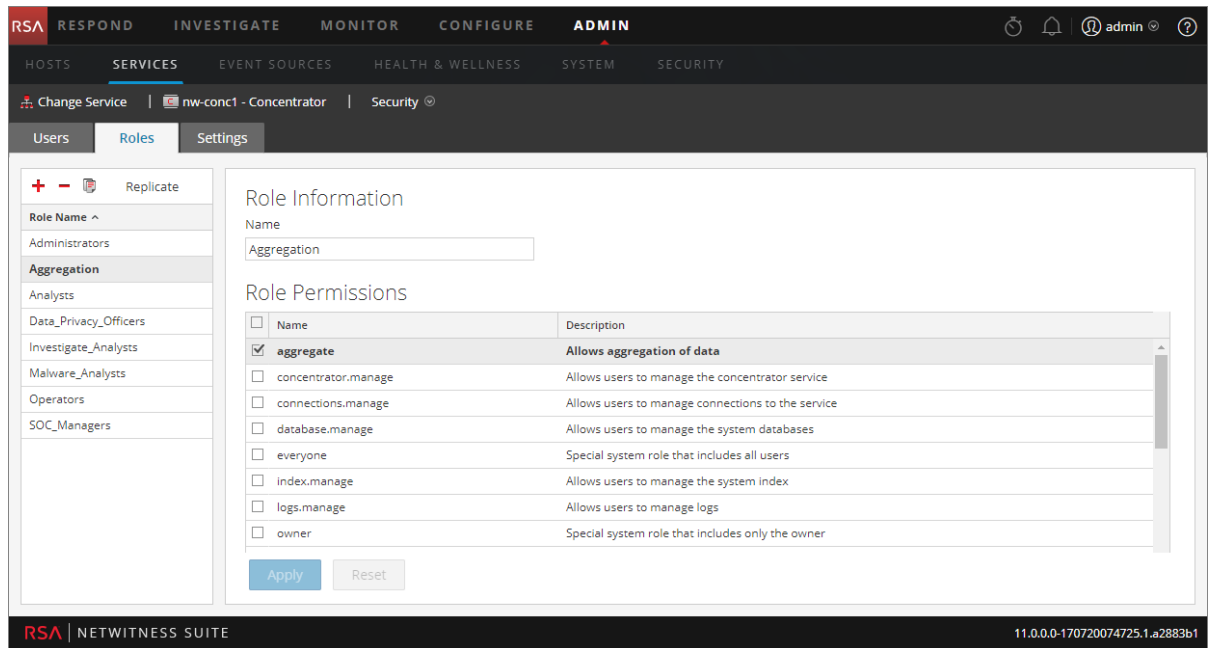
2. Select a service, then click  > **View > Security**.


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.

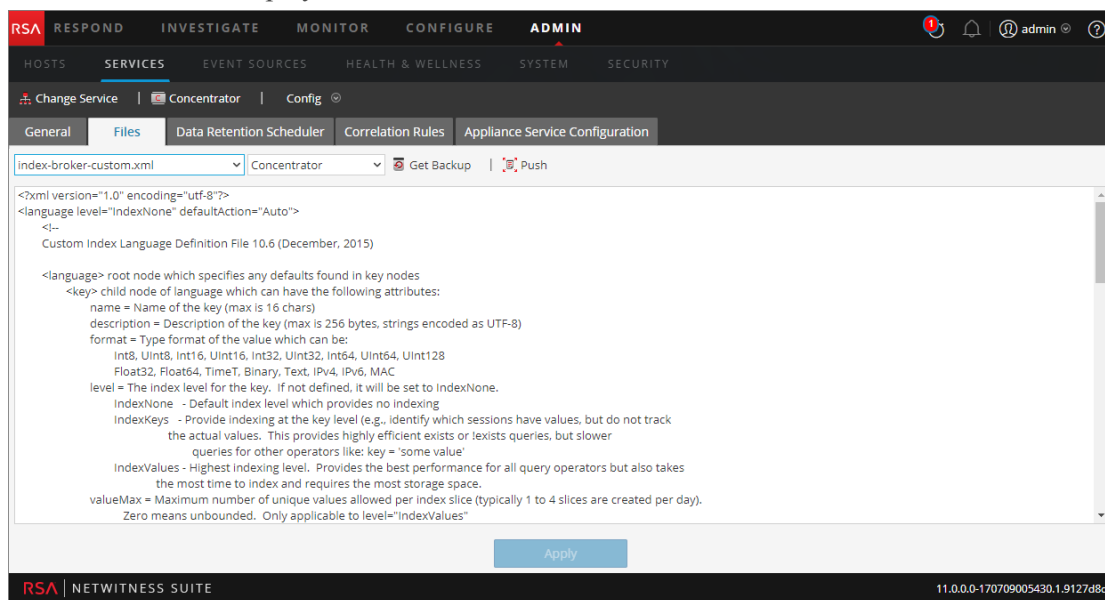
For more detail on service configuration parameters, see Service Configuration Settings.

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  **Push**. 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 .

Syntax	Description
deleteOnFinish: <bool, optional>	Delete the task when it has successfully finished.
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	<p>Add a task to run at a defined interval. For example, this message runs the /index save command every 6 hours:</p> <pre>addInter hours=6 pathname=/index msg=save</pre>

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: <pre>addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri</pre>
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 eustom.xml`

- `index-decoder.xml`, and `index-decodereustom.xml`
- `index-logdecoder.xml`, and `index-logdecodereustom.xml`
- `index-archiver.xml`, and `index-archiver eustom.xml`
- `index-workbench.xml`, and `index-workbench eustom.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>-eustom.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 `indexbroker.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	<p>Specify if the core files should be deleted after report.</p> <p>0 = No 1 = Yes</p> <p>NOTE: Until the core file is deleted, it is reported each time crashreporter is restarted.</p>

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

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  **Shutdown Service**.

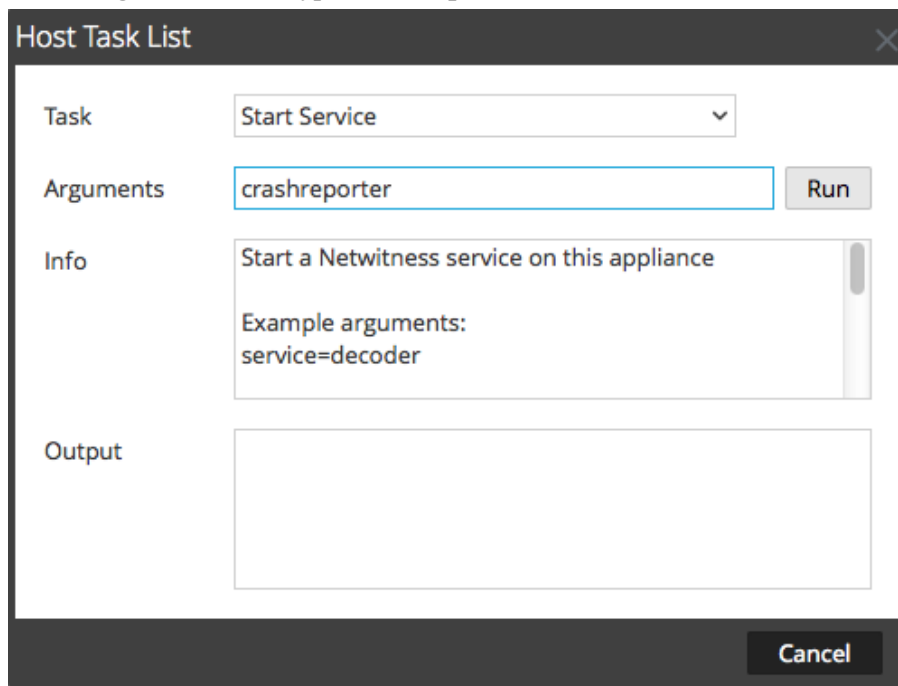
The service shuts down and restarts.

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  **Host Tasks**.
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.

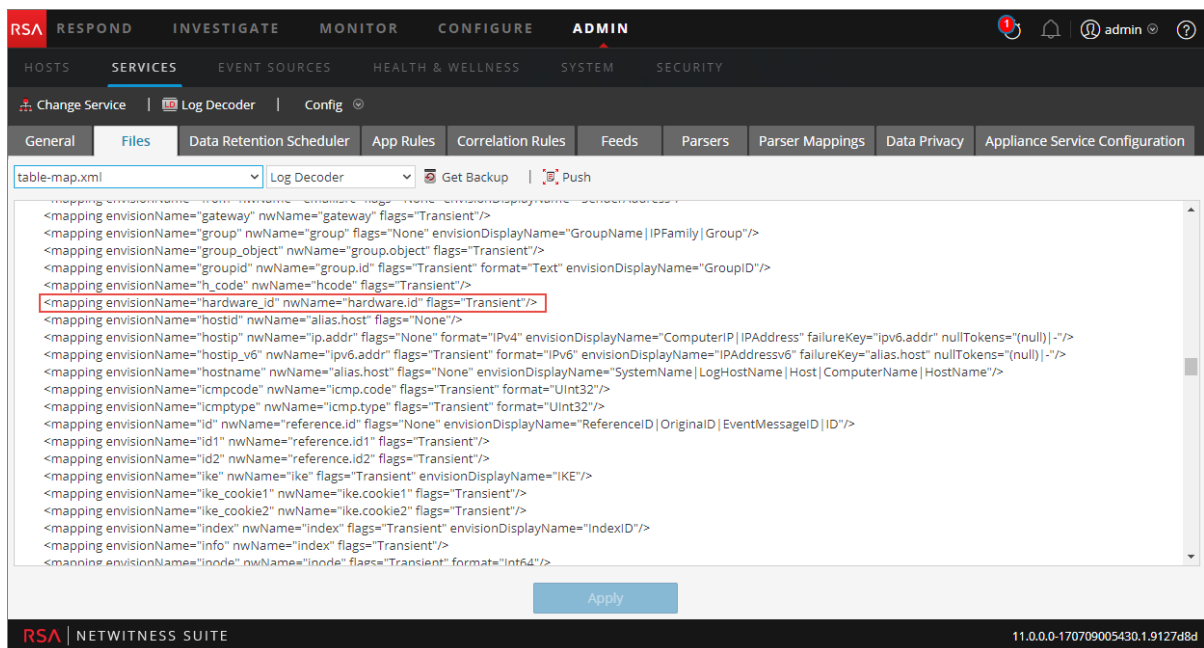
Prerequisites

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**.

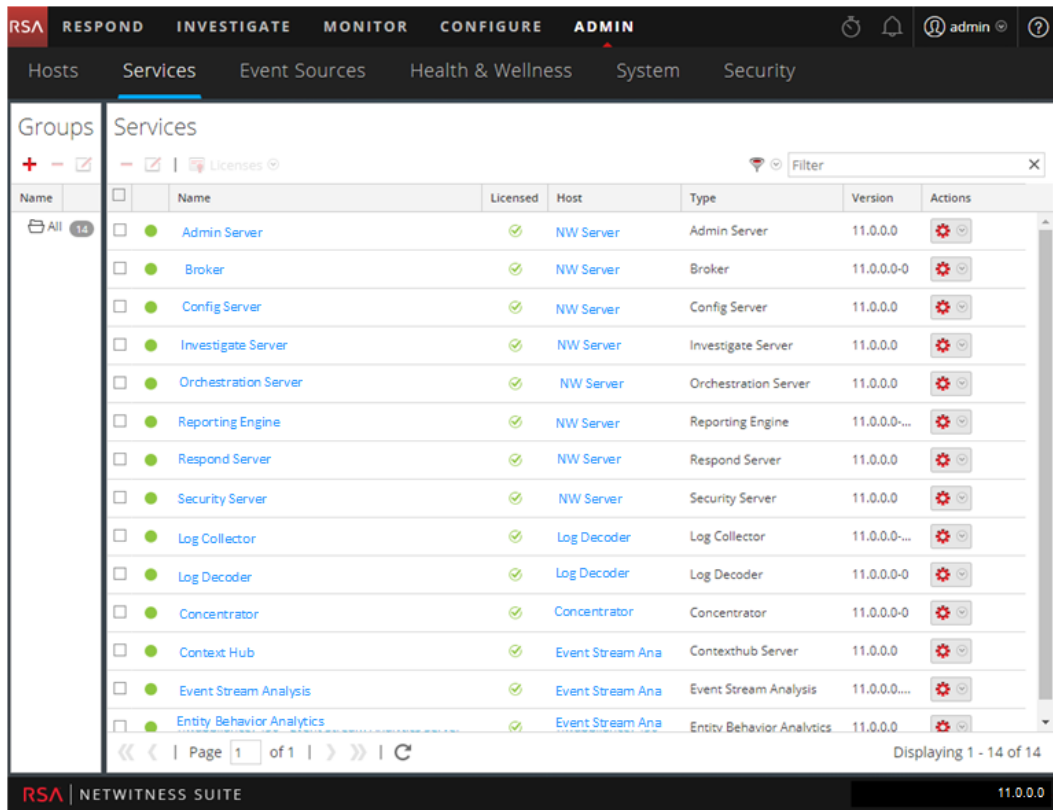
Caution: Before changing the table mapping files, carefully consider the effect of changing the index from `Transient` to `None` since it can impact the available storage and performance of the Log Decoder. For this reason, only certain meta keys are indexed out of the box. Use the `table-map-custom.xml`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

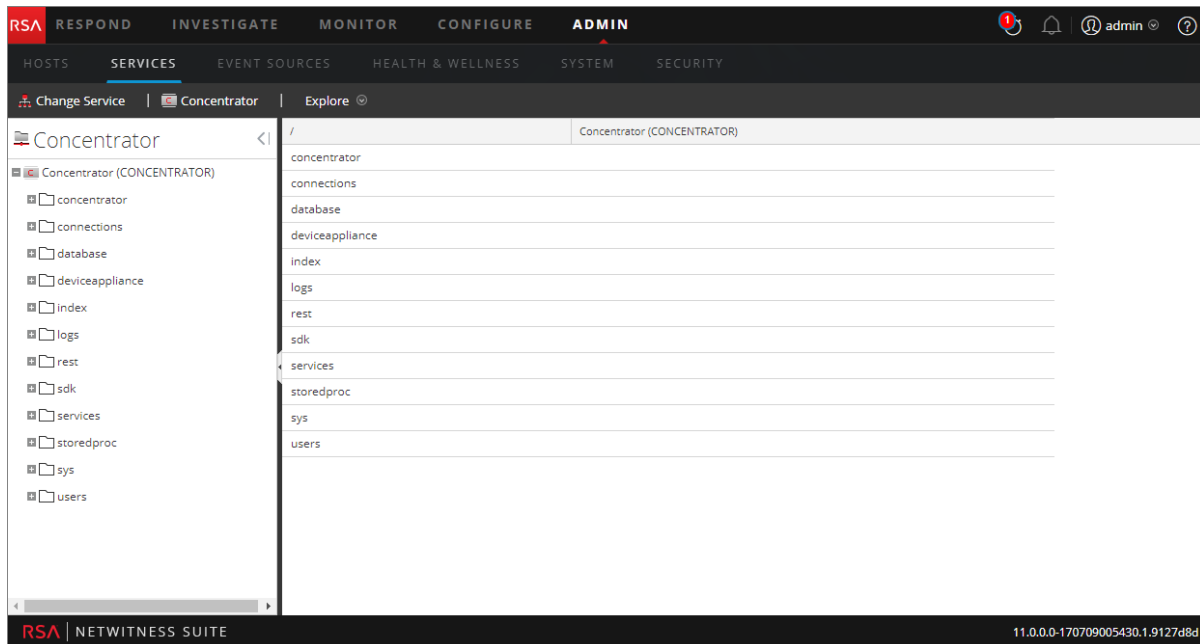
Each of the following procedures starts in the Explore view.

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.

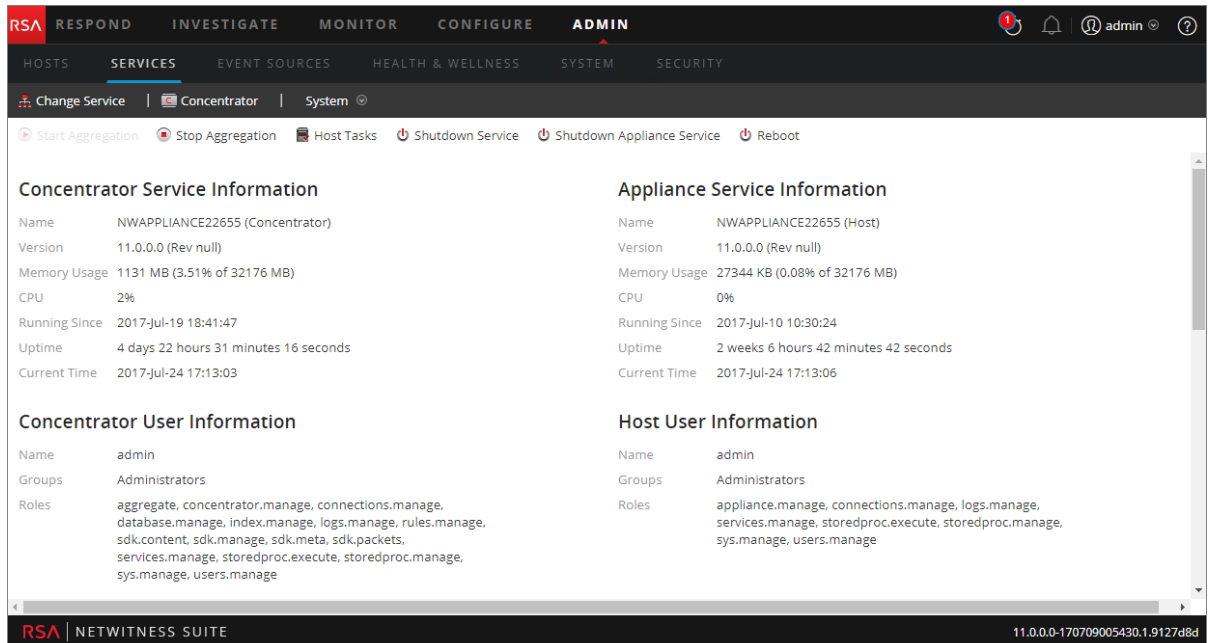
End a Session on a Service

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

The Admin Services view is displayed.

2. Select a service, and select  > **View > System**.

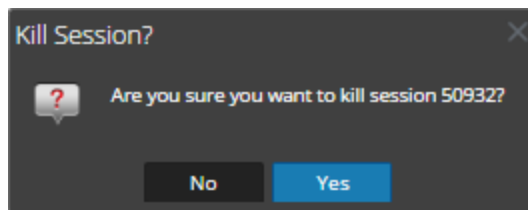
The Service System view is displayed.



The screenshot shows the NetWitness Suite Admin Services view. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is selected, and the SERVICES sub-tab is active. Below the navigation bar, there are buttons for Start Aggregation, Stop Aggregation, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into four sections: Concentrator Service Information, Appliance Service Information, Concentrator User Information, and Host User Information. Each section displays details such as Name, Version, Memory Usage, CPU, Running Since, Uptime, and Current Time. The bottom of the screen shows the RSA | NETWITNESS SUITE logo and the version number 11.0.0.0-170709005430.1.9127d8d.

3. In the **Session Information** grid at the bottom, click a *session-number*.

The following confirmation dialog is displayed.



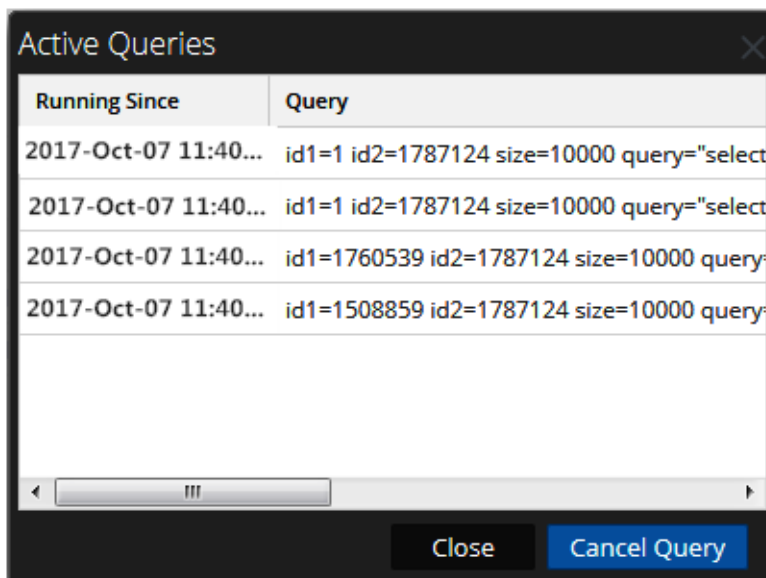
4. Click **Yes**.

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.

Services

Licenses

log

<input type="checkbox"/>		Name	Licensed	Host	Type	Version	Actions
<input type="checkbox"/>	<div><div></div></div>	Log Collector	or <div><div></div></div>	Log Decoder	Log Collector	11.0.0...	<div><div></div></div>
<input type="checkbox"/>	<div><div></div></div>	Log Decoder	or <div><div></div></div>	Log Decoder	Log Decoder	11.0.0...	<div><div></div></div>

«

<

Page 1 of 1

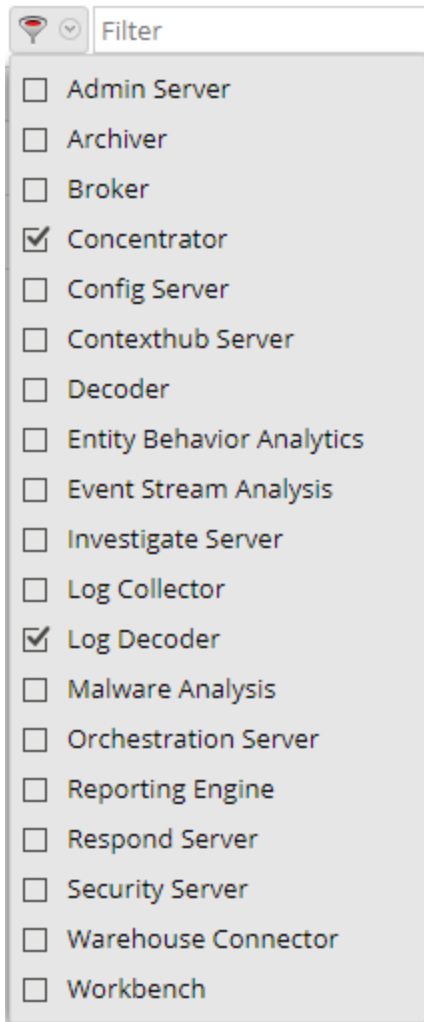
>

»

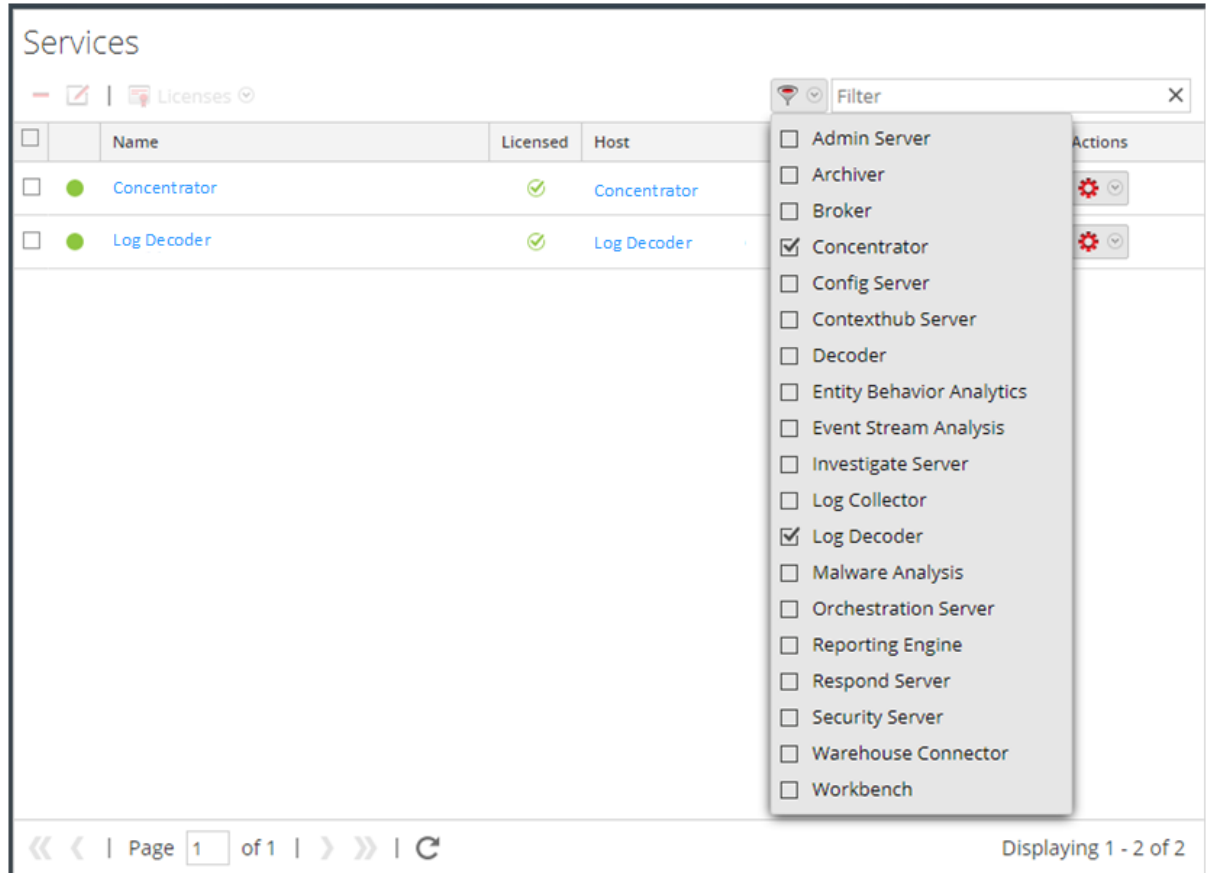
Displaying 1 - 2 of 2

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.



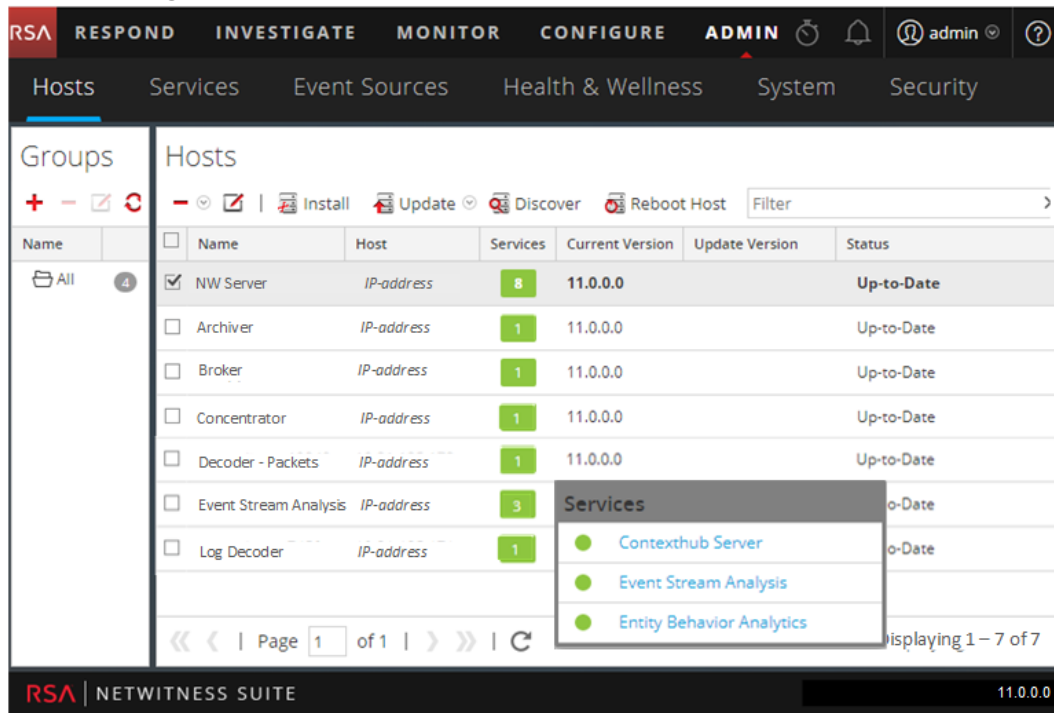
Find the Services on a Host

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.

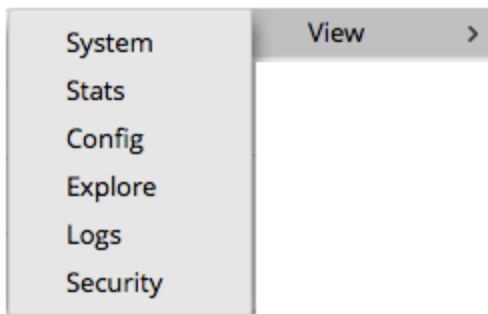
To restart a service:

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.

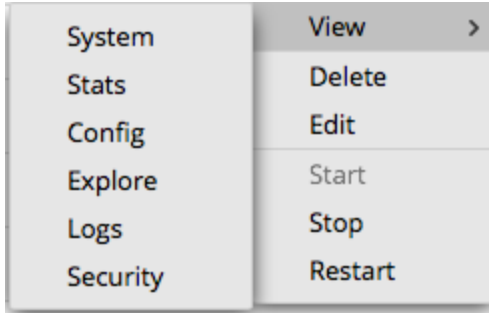
Access a Service View

To access a view for a service:

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

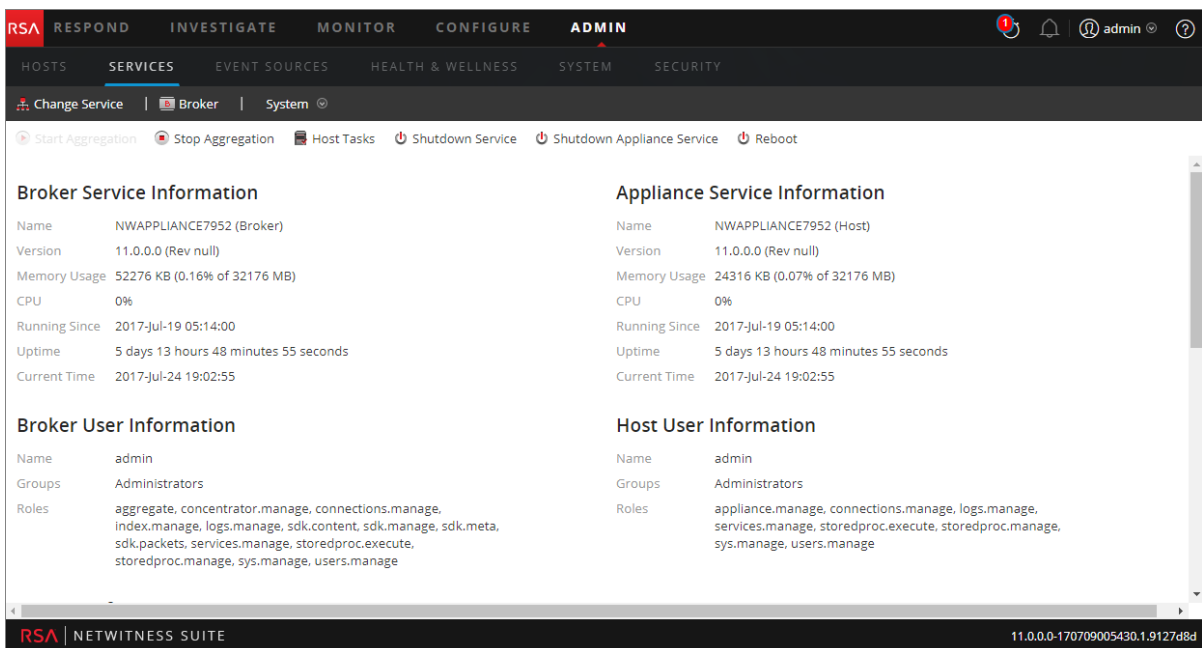
2. Select a service and click  > **View**.

The View menu is displayed.



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

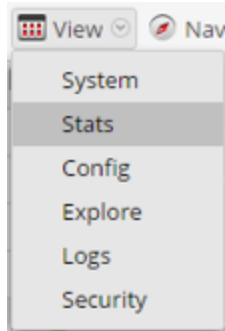
This is a System view for a Broker.



4. Use the toolbar to navigate:



- a. Click **Change Service** to select another service.
The **Administrative 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.

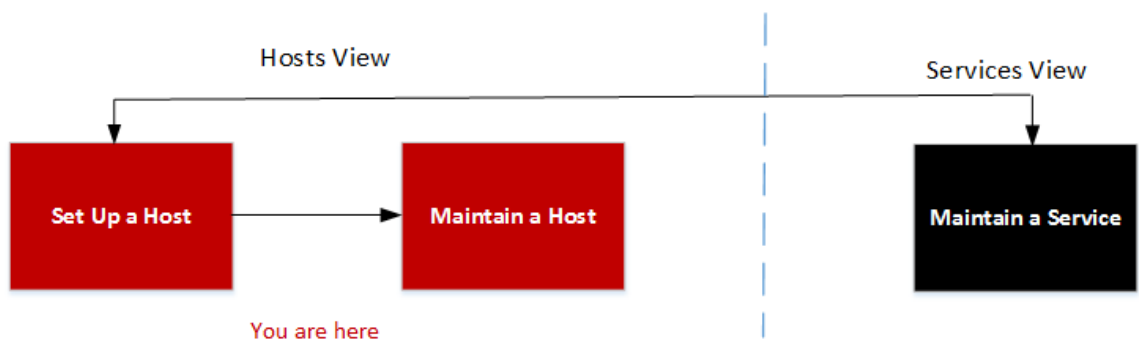
A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plug-in to enable or disable, according to the function of the host. You must configure the following Core services first:

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.

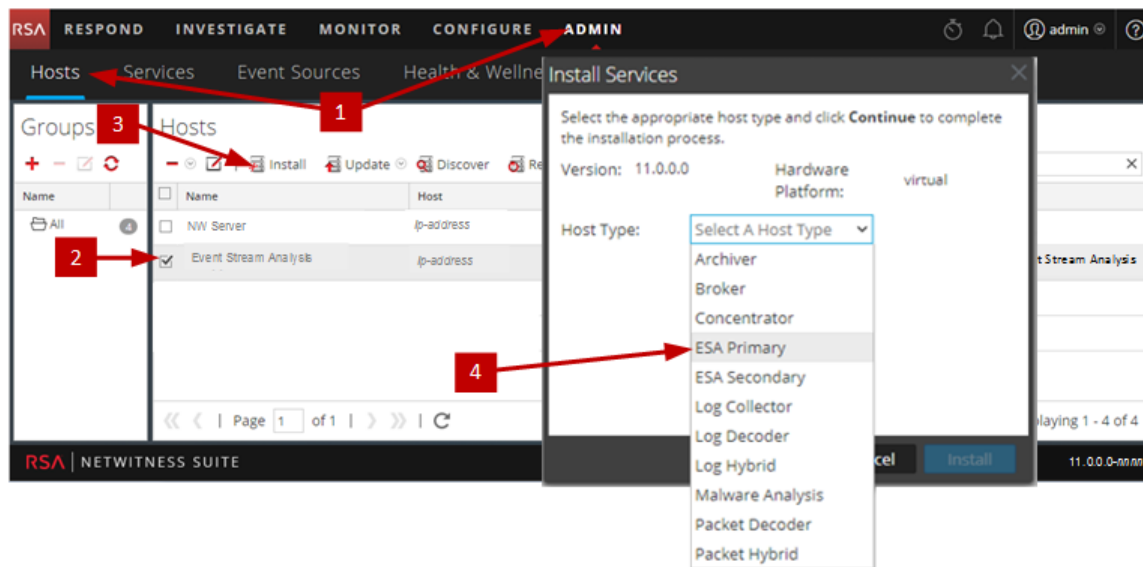


What do you want to do?


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 service to install from the **Install Services** dialog (for example, **ESA Primary**).

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 edit 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.
Update	<ul style="list-style-type: none">• 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.
Discover	<p>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.</p> <p>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.</p>
Reboot Host	Restart the host.
Install	Installs a NetWitness Suite component (service) on the selected 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.
	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

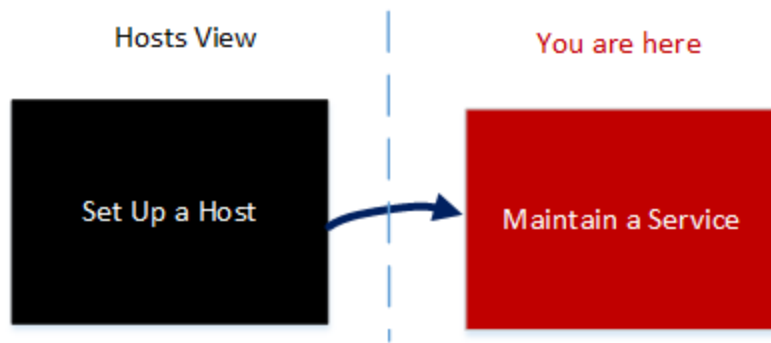
A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plug-in to enable or disable, according to the function of the host. You must configure the following Core services first:

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

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.

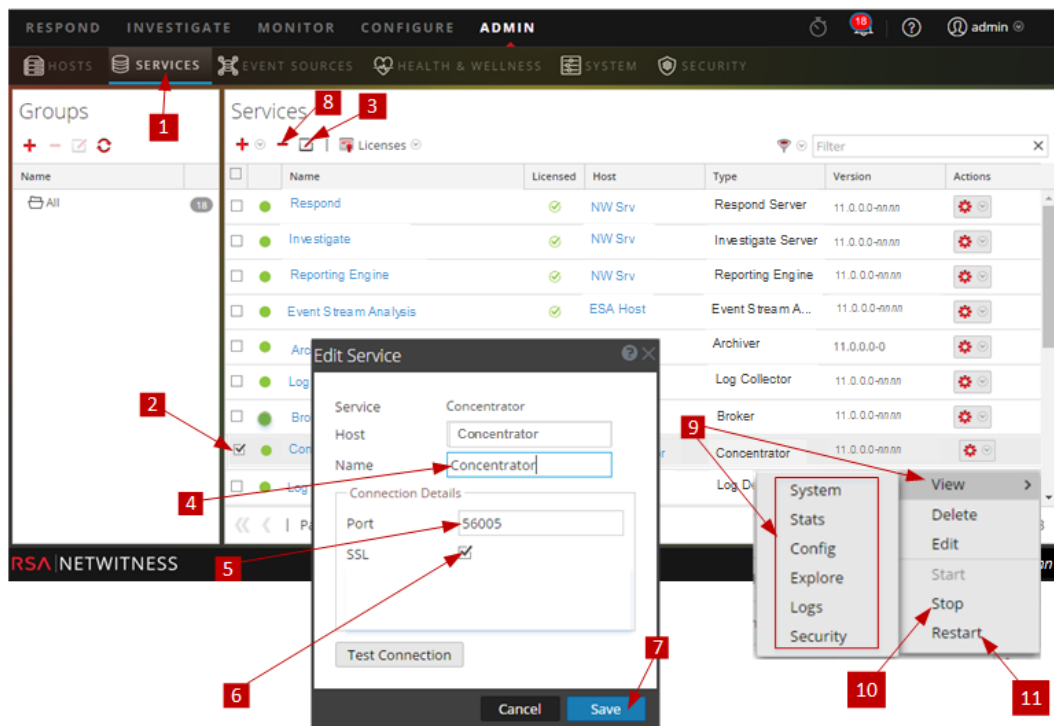
Role	I want to ...
Administrator	Maintain a service.
Administrator	Set up a host.

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

Admin Server

Archiver Service

Broker Service

Concentrator Service

Decoder Service

Event Stream Analysis Service

ESA: Context Hub Service

Investigate

Log Collector Service

Log Decoder Service

Malware Analysis Service

Reporting Engine Service

Respond Server

Warehouse Connector

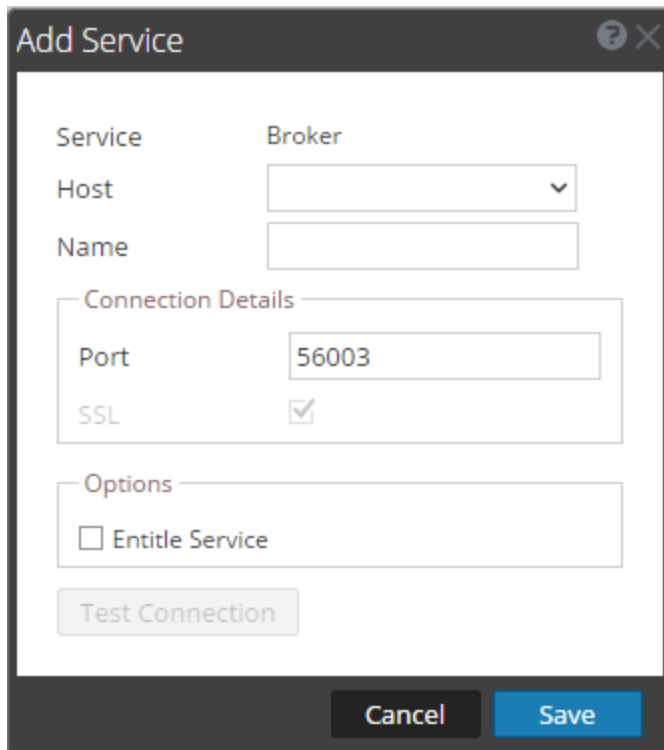
Workbench Service

Add Service or Edit Service Dialog

This topic introduces the Add Service or Edit Service dialogs accessible from the ADMIN Services view (ADMIN > Services).

NetWitness Suite services are automatically discovered in NetWitness Suite. You can manually add a service using the Add Service dialog to make services available to NetWitness Suite modules.

To access the Add Service dialog, navigate to the **ADMIN Services** view, and select **+ Add** in the **Services panel** toolbar.



The screenshot shows the 'Add Service' dialog box. It has a title bar with a question mark icon and a close button. The main content area contains the following fields and sections:

- Service** and **Broker** labels above a dropdown menu.
- Host** label above a text input field.
- Name** label above a text input field.
- Connection Details** section containing:
 - Port** label above a text input field with the value '56003'.
 - SSL** label next to a checked checkbox.
- Options** section containing:
 - Entitle Service** checkbox.
- Test Connection** button.

At the bottom of the dialog, there is a dark bar with **Cancel** and **Save** buttons.

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

The 'Edit Service' dialog box is shown. It has a title bar with 'Edit Service' and a close button. The main area contains the following fields and controls:

- Service:** A dropdown menu with 'Broker' selected.
- Host:** A text input field containing 'localhost.localdomain'.
- Name:** A text input field containing 'Broker'.
- Connection Details:** A section containing:
 - Port:** A text input field containing '56003'.
 - SSL:** A checkbox that is checked.
- Test Connection:** A button located below the 'Connection Details' section.
- Buttons:** 'Cancel' and 'Save' buttons are located at the bottom right of the dialog.

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, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.
Host	Specifies the host on which the service resides.
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.

Field or Option	Description
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 <i>Deployment Guide</i> .
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 <i>Licensing Guide</i> .
Test Connection	Clicking this button tests the connection of a service that you are adding.
Save	Clicking this button saves the new service.
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.

Groups Panel Toolbar

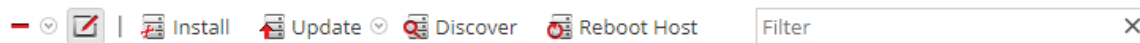
This topic introduces the features and options in **ADMIN > Services** view > **Groups** panel toolbar.

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.

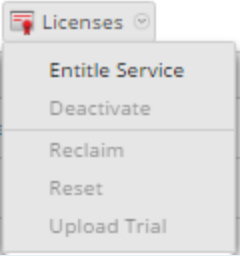
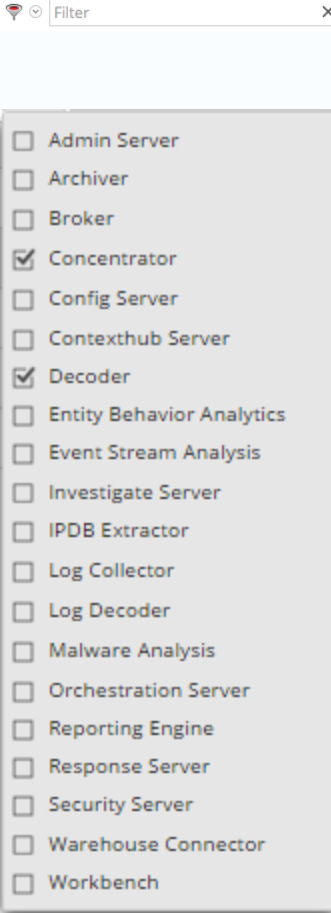
To access the Administration Services view, in **NetWitness Suite**, go to **ADMIN > Services**. The Services panel toolbar is at the top of the Services grid in the Services view.



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
	<ul style="list-style-type: none"> • Entitle Service: Assigns licenses from the local license server (LLS) to selected services (see the Overview Tab topic in the <i>Licensing Guide</i>). • 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.
	<p>Filters the services listed in Services view.</p> <p>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.</p> <p>In the Filter field, you can filter the services by Name and Host.</p> <p>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.</p>

Services Config View

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

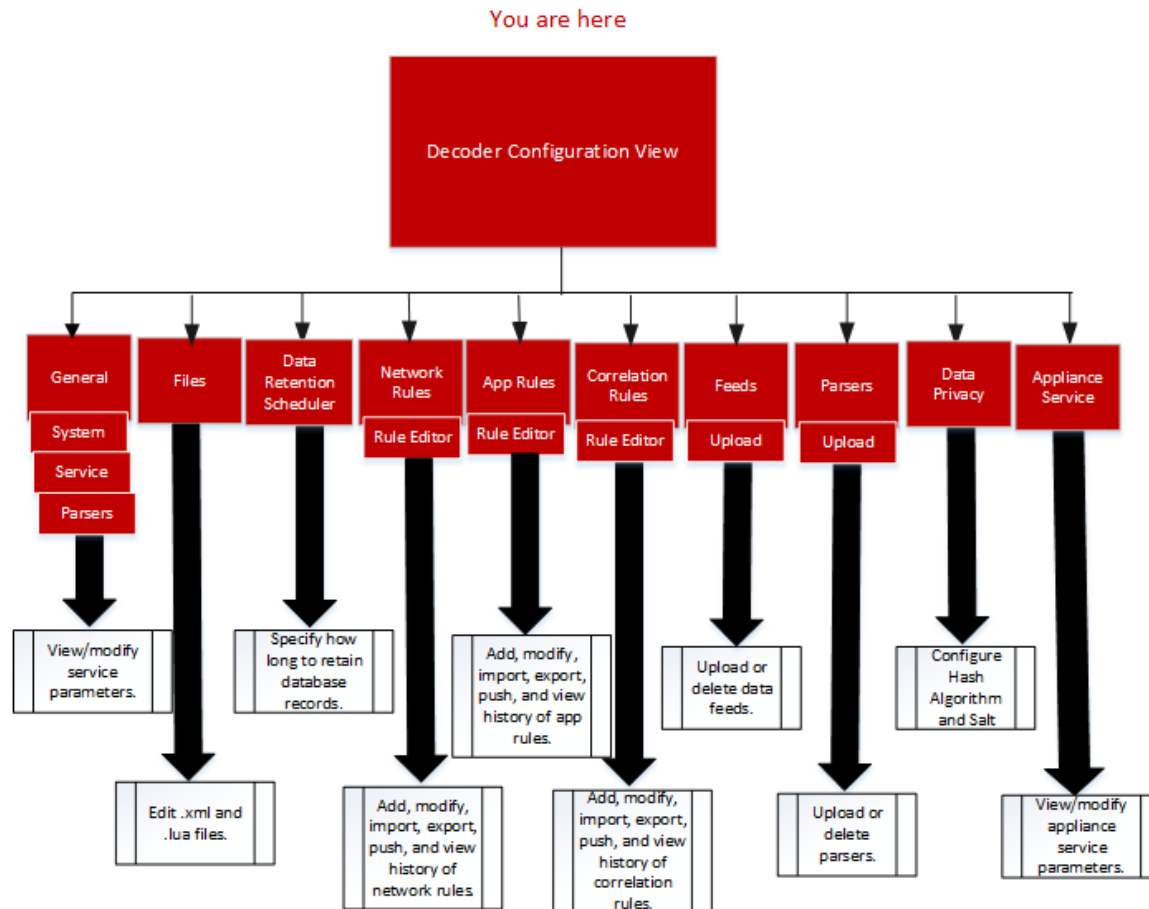
The Services Config view is one of the views available from the **Services** > Actions () menu. It provides a user interface for configuring all aspects of a Core service or NetWitness Suite service.

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, 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.

System Configuration

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

Decoder Configuration

Name	Config Value
Adapter	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_eth0 (bpf)
Cache	

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).

Name	Config Value
ALERTS	Enabled
DHCP	Enabled
DNS	Enabled
Entropy	Enabled
FeedParser	Enabled
FTP	Enabled
GeoIP	Enabled
GTalk	Enabled
H323	Enabled
HTTP	Enabled
HTTPS	Enabled

Apply

RSA | NETWITNESS SUITE 11.0.0.0-

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

Aggregate Services

+ - ✎ ⚙️ Edit Service | 🔄 Toggle Service | ▶️ Start Aggregation | ⏹️ Stop Aggregation

<input type="checkbox"/>	Address	Port	Rate	Max	Behin	Meta Fil	Filter	Meta Incl	Grouped	Status
<input type="checkbox"/>	10.25.51.110	56...	0	186	0			no		consuming
<input type="checkbox"/>	10.25.51.68	56...	0	24...	0			no		consuming

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	10000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

RSA | NETWITNESS SUITE 11.0.0.0-170801164828.1.c71c098

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, 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**.

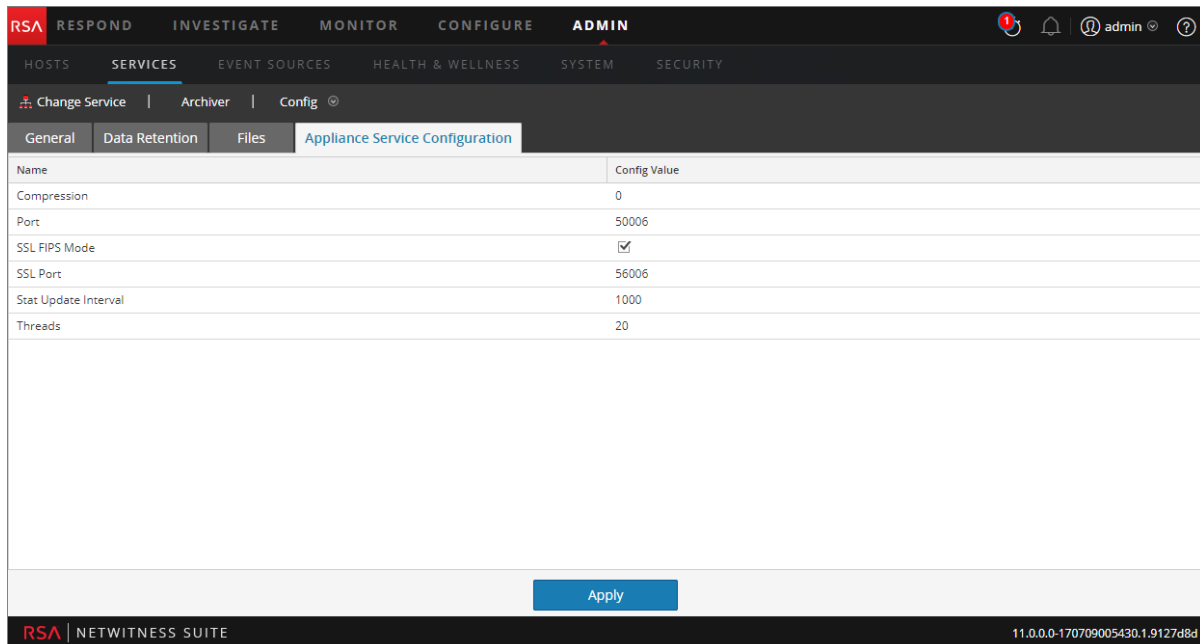
The Administration Services view is displayed.

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.



The screenshot shows the NetWitness Suite Admin console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the SERVICES section is selected. The Archiver service is chosen, and the Config view is displayed. The Appliance Service Configuration tab is active, showing a table of configuration parameters.

Name	Config Value
Compression	0
Port	50006
SSL FIPS Mode	<input checked="" type="checkbox"/>
SSL Port	56006
Stat Update Interval	1000
Threads	20

An Apply button is located at the bottom right of the configuration table.

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.

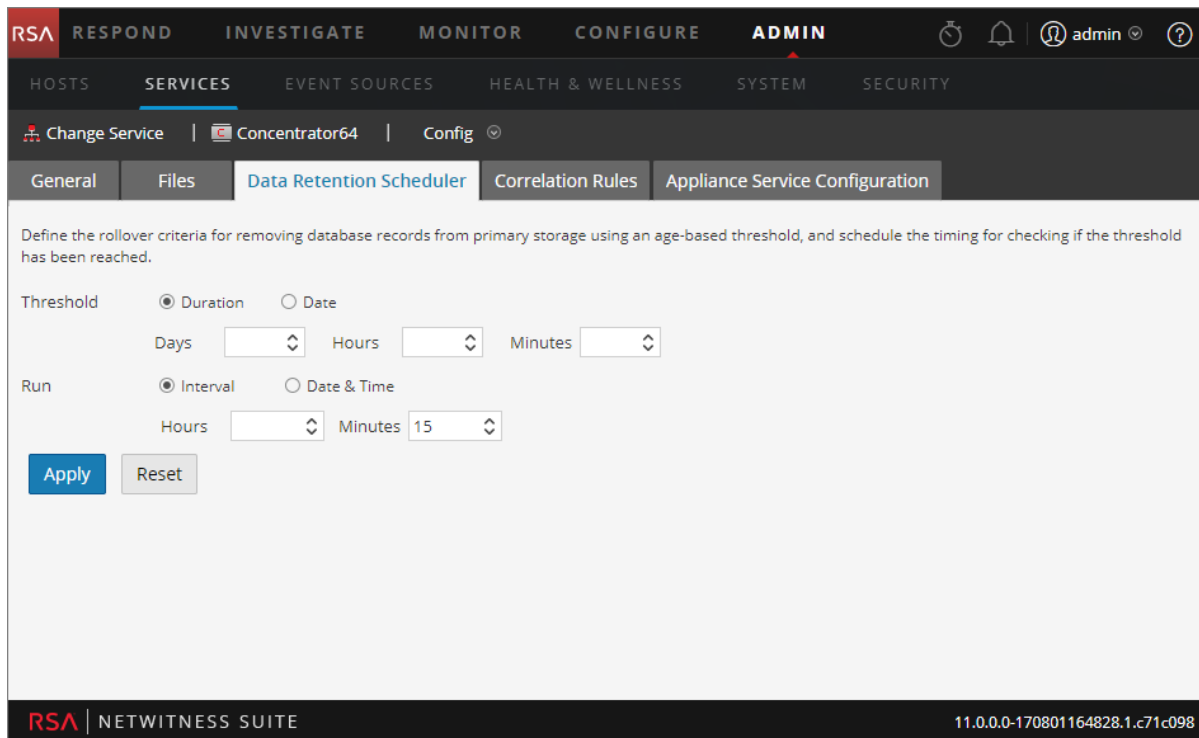
For information on the Data Retention tab for Archiver, see the **Data Retention Tab - Archiver** topic in the *Archiver Configuration Guide*.

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.



The screenshot shows the NetWitness Suite interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the SERVICES sub-tab is selected. Below this, the breadcrumb path is 'Change Service | Concentrator64 | Config'. The 'Data Retention Scheduler' tab is highlighted among other tabs like General, Files, Correlation Rules, and Appliance Service Configuration.

The main content area contains the following configuration options:

- Define the rollover criteria for removing database records from primary storage using an age-based threshold, and schedule the timing for checking if the threshold has been reached.**
- Threshold:** Radio buttons for **Duration** (selected) and **Date**. Below are input fields for Days, Hours, and Minutes.
- Run:** Radio buttons for **Interval** (selected) and **Date & Time**. Below are input fields for Hours and Minutes (set to 15).
- Buttons:** 'Apply' (blue) and 'Reset' (grey).

The footer of the interface shows 'RSA | NETWITNESS SUITE' on the left and the version '11.0.0.0-170801164828.1.c71c098' on the right.

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	<p>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.</p> <ul style="list-style-type: none">• 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	<p>The schedule for running the job that checks rollover criteria.</p> <ul style="list-style-type: none">• 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	<p>Overwrites any previous schedule for this service and applies the new settings immediately.</p> <div>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.</div>
Reset	<p>Resets the schedule to the last applied state.</p>

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**.

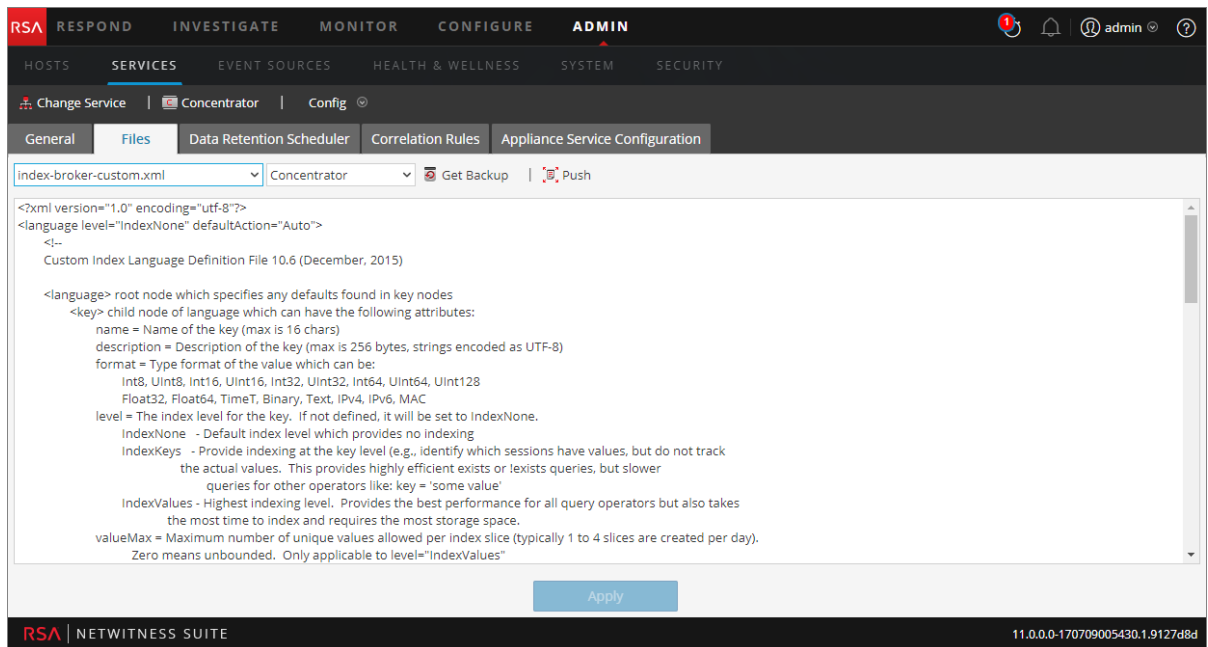
The Services Config view is displayed with the **General** tab open.

3. Click the **Files** tab.

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

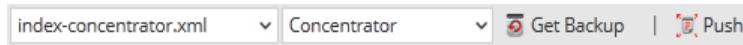
Edit a Service Configuration File

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.



Get B

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**.

Feature	Description
 Push	Displays a dialog in which you can select services of the same type and push the currently viewed file to the services.
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:

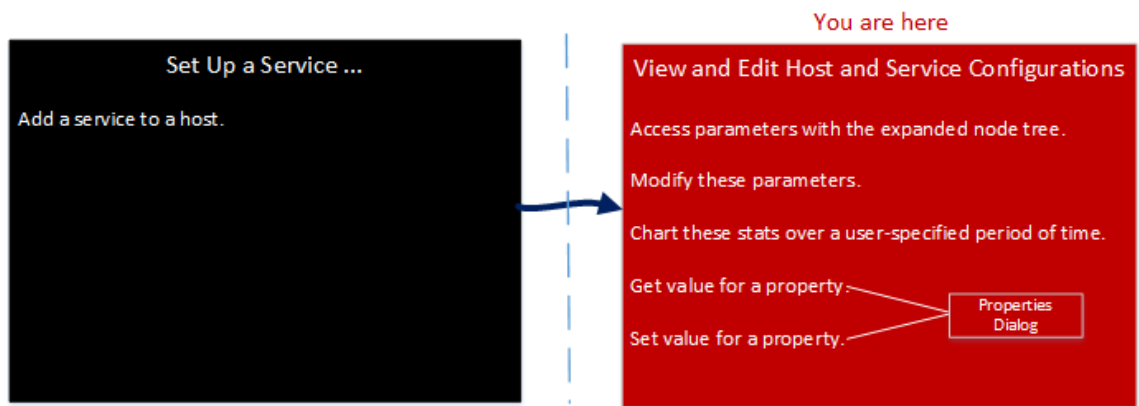
- View a directory tree showing common files for all selected services.
- Navigate down through the directory to a file.
- Open the same file for each service, and display the contents side by side.
- Select an entry in the file and edit the value.
- Apply a property value from one service to other services.

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

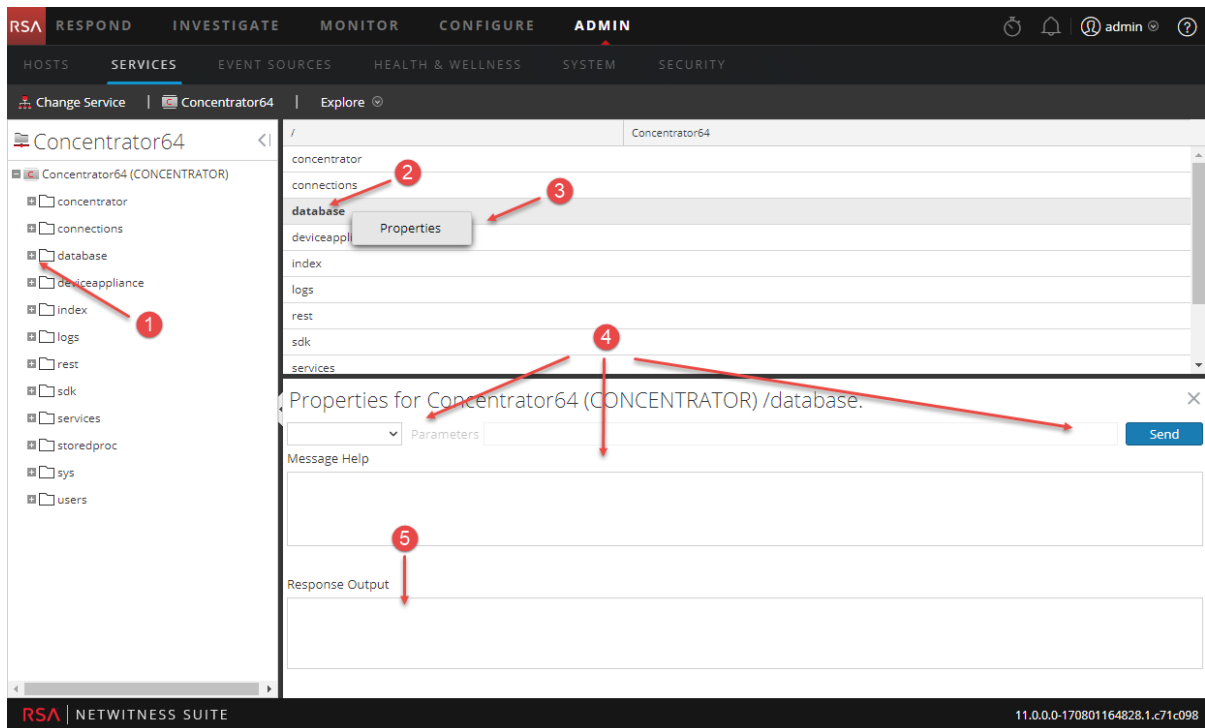
This workflow shows the tasks you perform from the Explore view.



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

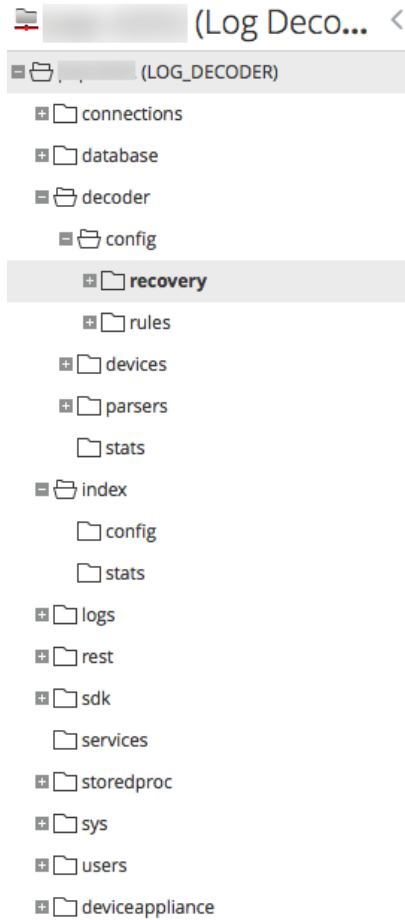
The **Services Explore View** has two main panels:

- 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:

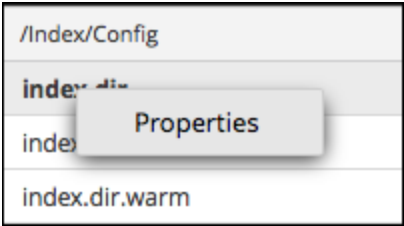
- A description of the node.
- The list of supported messages with a corresponding description.
- Security roles needed to access the messages.

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:

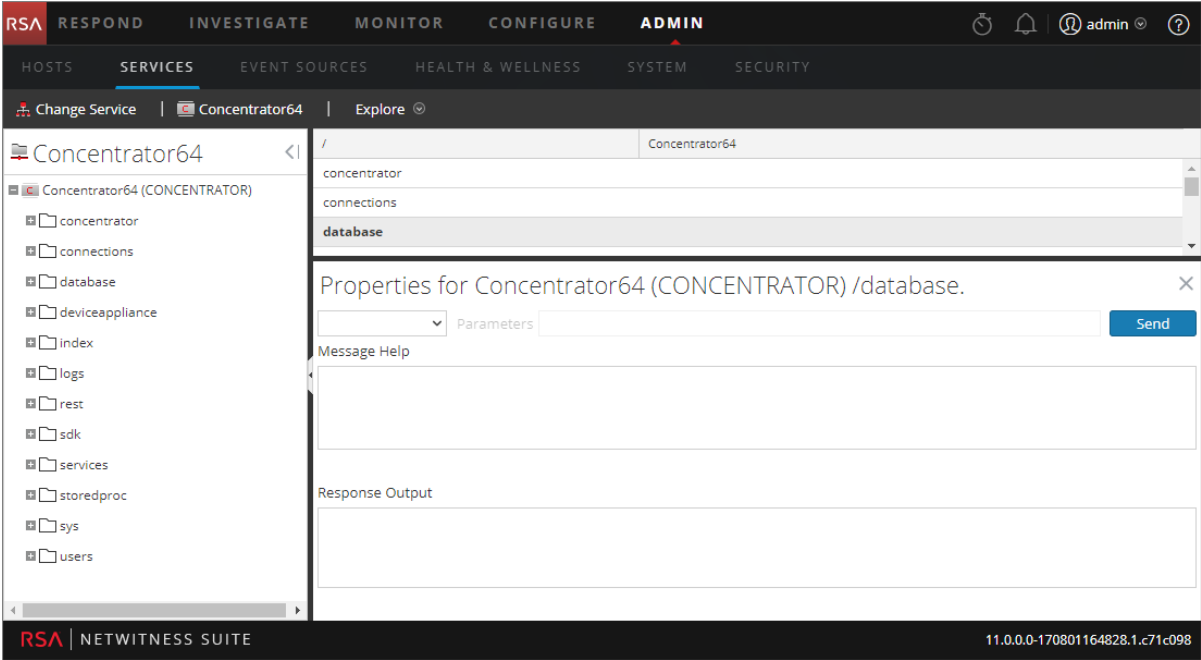
1. In **NetWitness Suite**, go to **ADMIN > Services**.
2. Select a service and select  > **View > Explore**.
3. In the **Node** list, select a file.

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.

Feature	Description
Message Help	Displays help text for the current message.
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:

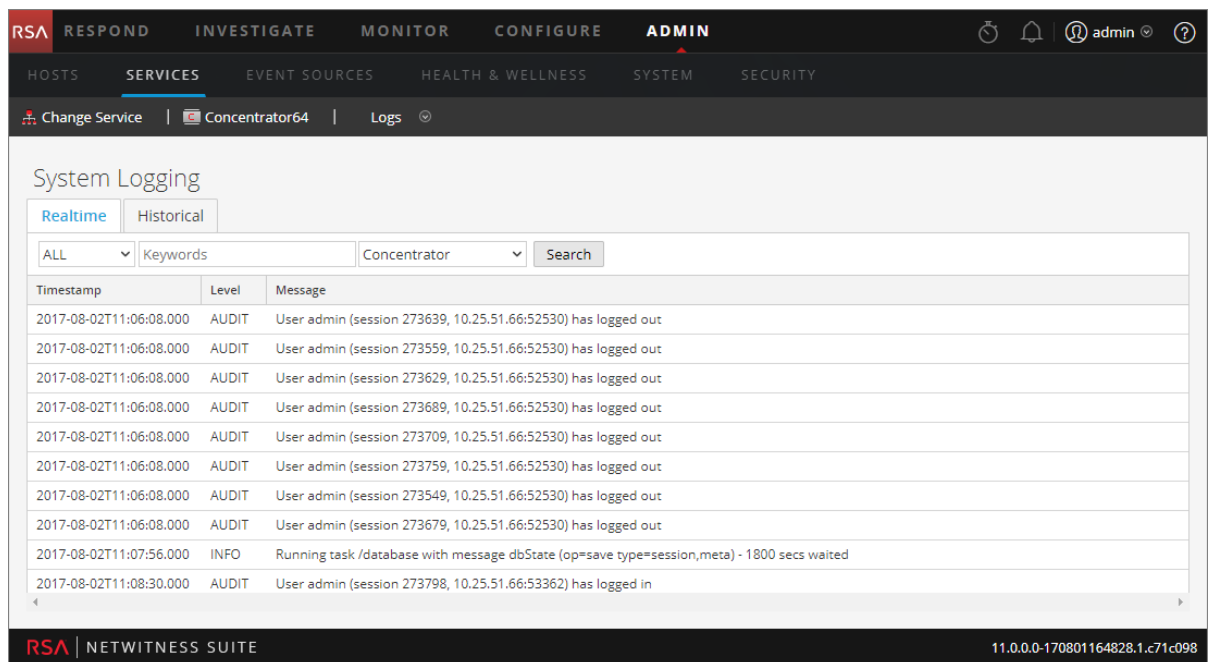
- The Services Logs view has an additional filter to select messages for the service or host.
- The System Logging panel has an additional tab for Settings.

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.



Timestamp	Level	Message
2017-08-02T11:06:08.000	AUDIT	User admin (session 273639, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273559, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273629, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273689, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273709, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273759, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273549, 10.25.51.66:52530) has logged out
2017-08-02T11:06:08.000	AUDIT	User admin (session 273679, 10.25.51.66:52530) has logged out
2017-08-02T11:07:56.000	INFO	Running task /database with message dbState (op=save type=session,meta) - 1800 secs waited
2017-08-02T11:08:30.000	AUDIT	User admin (session 273798, 10.25.51.66:53362) has logged in

The following figure shows the Services Logs view Historical tab.

System Logging

Realtime Historical

Start Date End Date ALL Keywords Concentrator Search Export

Timestamp	Level	Message
2017-08-02T11:05:38.000	AUDIT	User admin (session 273124, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273421, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273192, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273281, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273451, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273391, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273104, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273134, 10.25.51.66:52530) has logged out
2017-08-02T11:05:38.000	AUDIT	User admin (session 273182, 10.25.51.66:52530) has logged out

« | Page 200 of 200 | » | C

Displaying 9951 - 10000 of 10000

RSA | NETWITNESS SUITE 11.0.0.0-170801164828.1.c71c098

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.

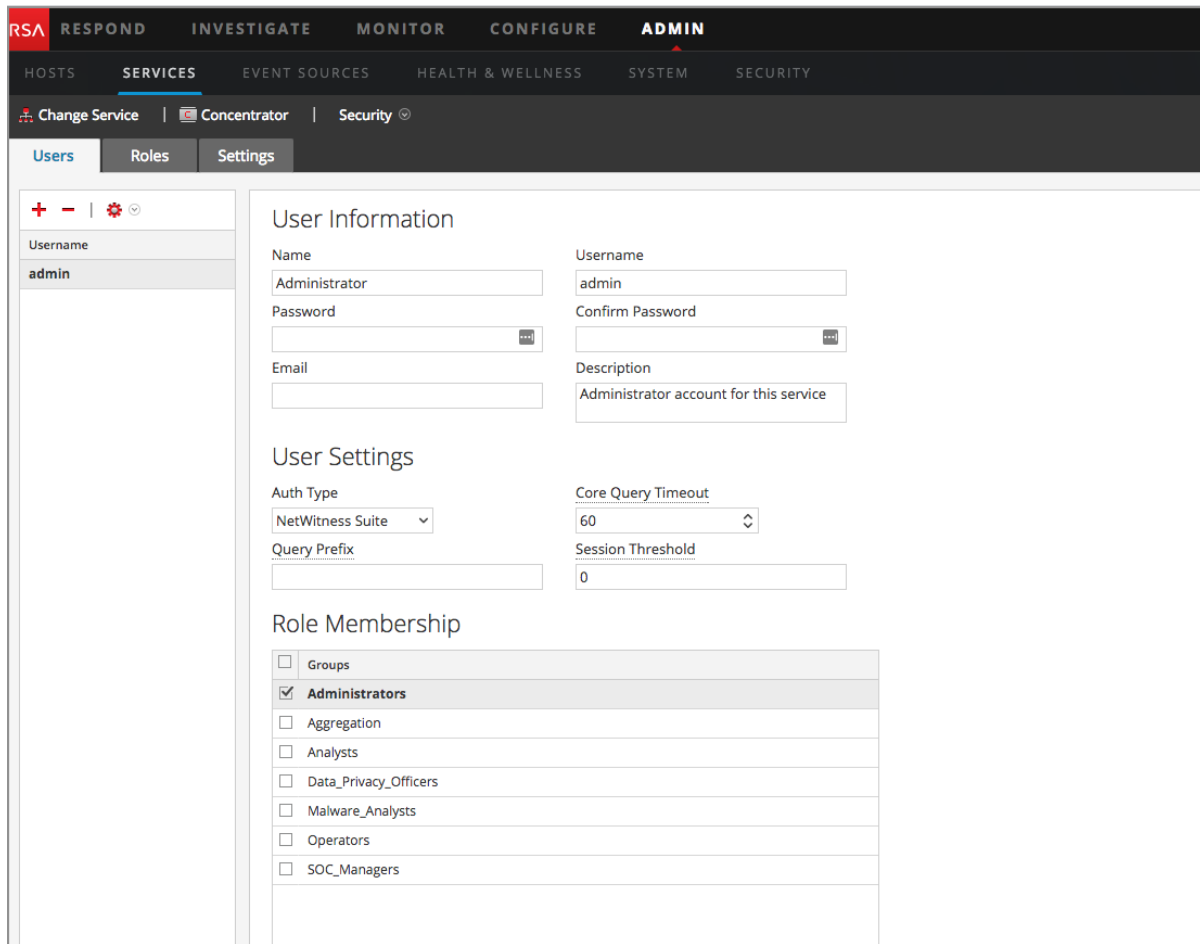
Procedures related to this tab are described in [Hosts and Services Procedures](#).

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.

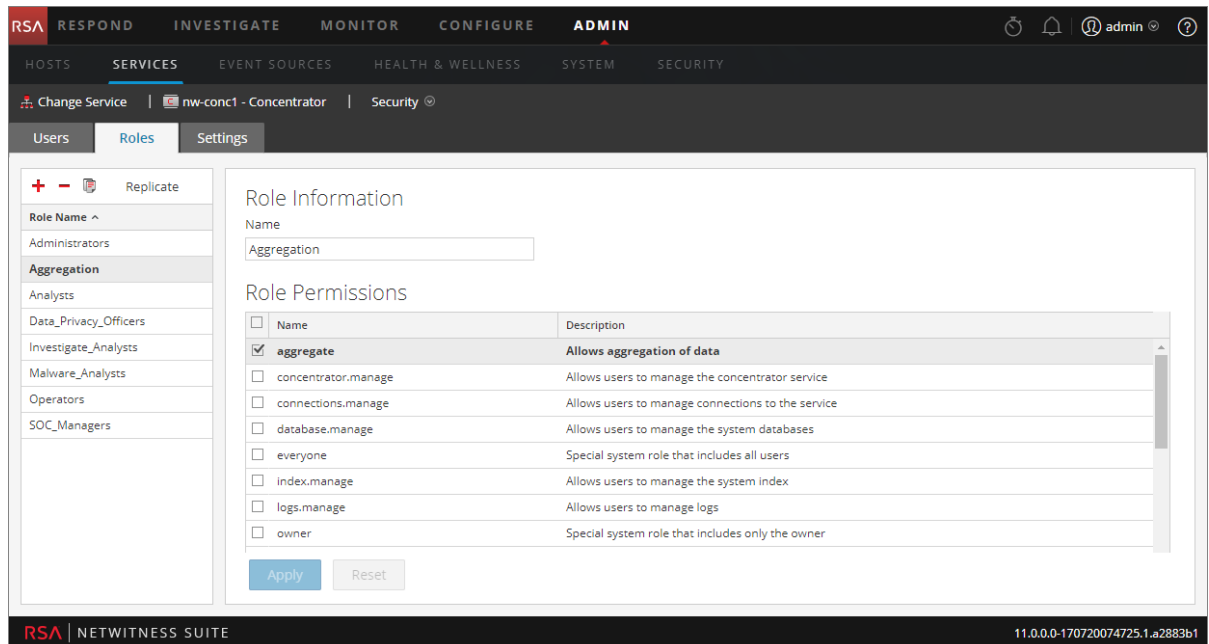
Before you can add users to roles, you need to define user roles, usually by function, and assign permissions to the roles.

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.

Replicate Role to other services

☐

Name ^

Address

Type

☐

Broker

Broker

☐

Concentrator

Concentrator

☐

Decoder

Decoder

☐

Broker

Cancel

Replicate

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	<p>You can use this role to create an Aggregation account.</p> <p>This role provides the minimum permissions necessary to perform aggregation of data. It is only available on NetWitness Suite 10.5 and later services.</p>
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	<p>Data Privacy Officer</p> <p>Data Privacy Officers have the dpo.manage permission on Decoders and Log Decoders.</p>

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

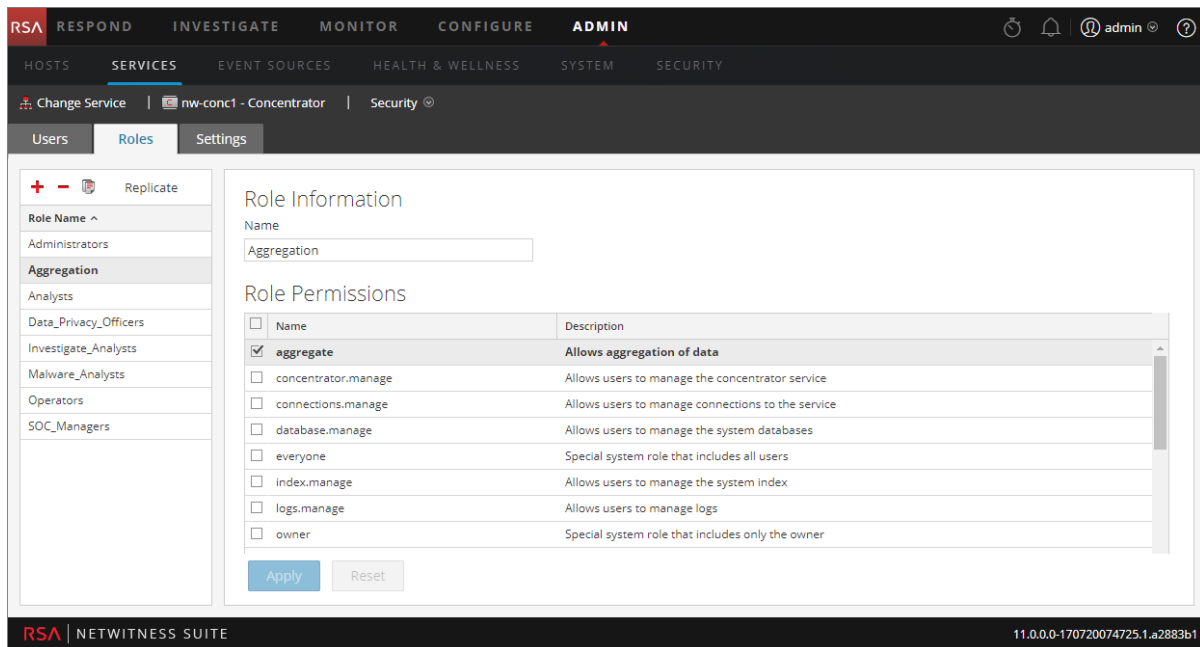
The Aggregation role is available only on NetWitness Suite 10.5 and later services and it can be used for an aggregation account. Members of this role or service users with these permissions can perform aggregation on Decoders, Concentrators, Archivers, and Brokers. The **aggregate** permission allows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

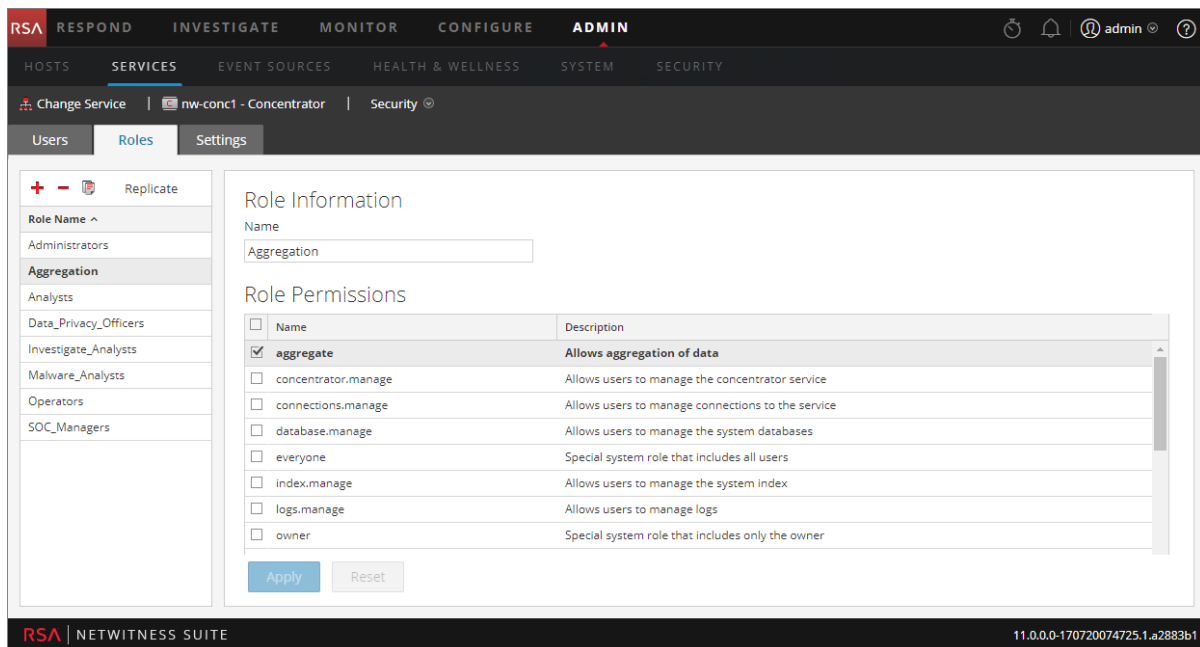
The following figure shows the permissions in the Aggregation role.



Settings Tab


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

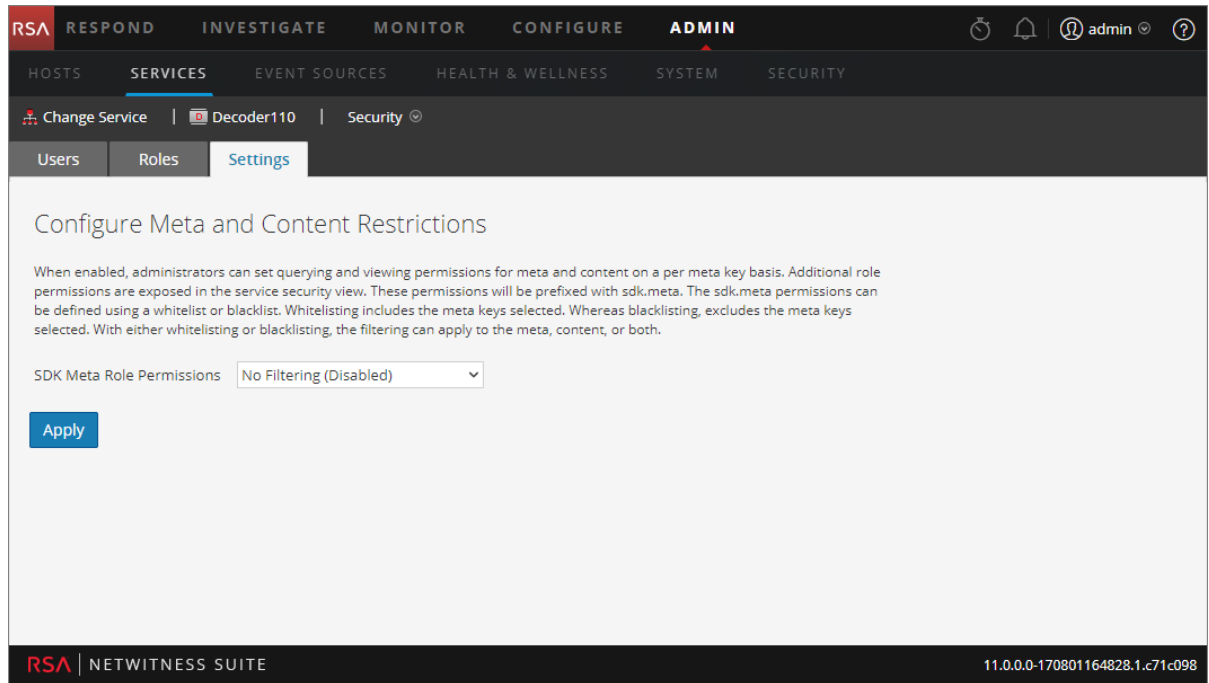
In the Services Security view Settings tab, Administrators can enable and configure system roles that define permissions on a per meta key basis for individual Brokers, Concentrators, Decoders, and Log Decoders. Configuring this feature adds configurable meta keys to the Services Security view > Roles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

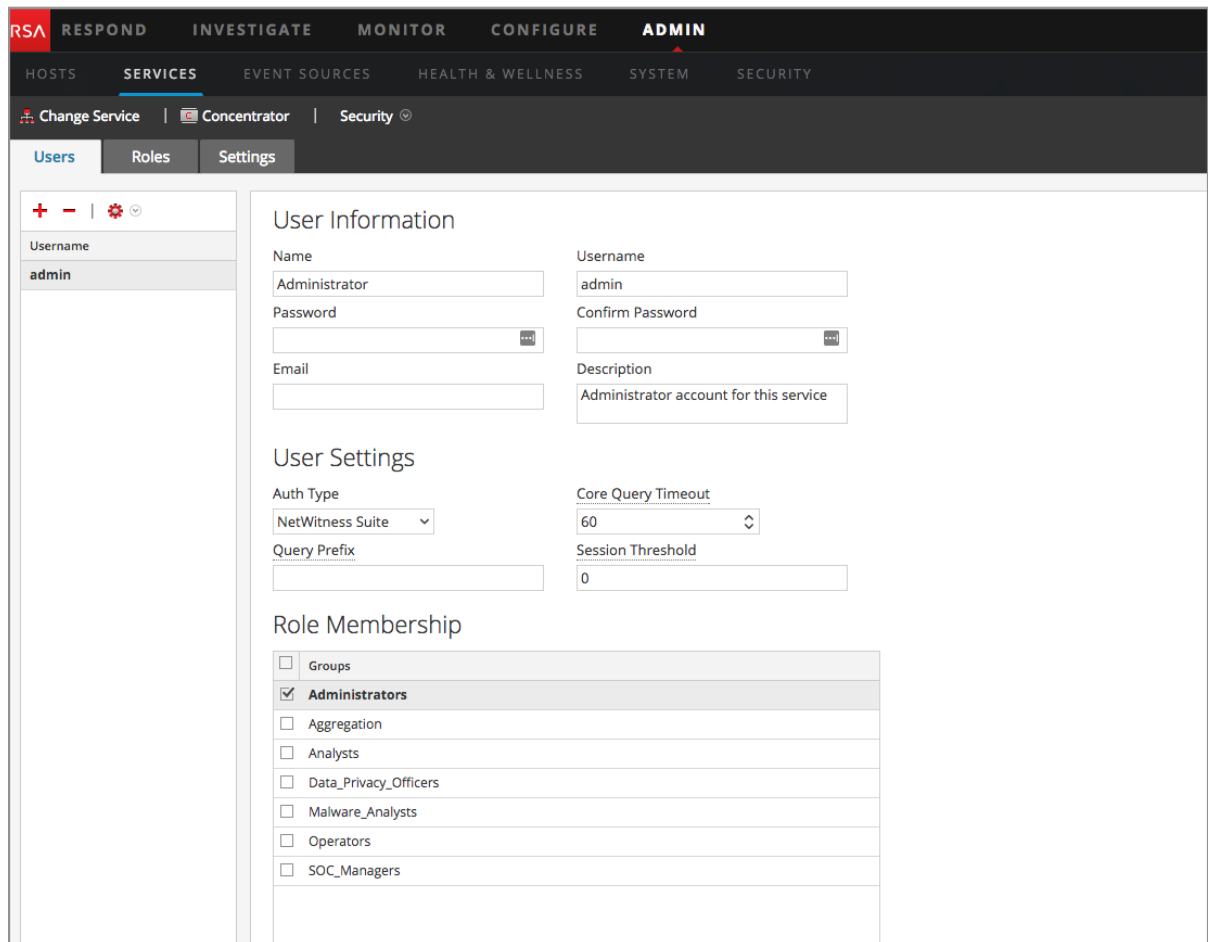
- Add user accounts.
- Change service user passwords.
- Configure user authentication properties and query handling properties for the service.
- Specify the user role membership, which specifies the roles that the user belongs to on the selected service.

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**.






The screenshot displays the NetWitness Suite web interface for managing users. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the left sidebar shows the 'SERVICES' tab selected. The main content area is titled 'Security' and contains a 'Users' tab. The 'Users' tab is active, showing a list of users on the left and a form for adding or editing a user on the right. The form is divided into three sections: 'User Information', 'User Settings', and 'Role Membership'. The 'User Information' section includes fields for Name (Administrator), Username (admin), Password, Confirm Password, Email, and Description (Administrator account for this service). The 'User Settings' section includes fields for Auth Type (NetWitness Suite), Query Prefix, Core Query Timeout (60), and Session Threshold (0). The 'Role Membership' section includes a list of roles with checkboxes, where 'Administrators' is selected.

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.
	<p>Performs one of the following actions on the selected service user account:</p> <ul style="list-style-type: none"> • 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.

Replicate User to other services

Please enter and confirm the service user password. The entire service user account replicates to the selected services. The user password also changes on each selected service.

Password

Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	- Broker		Broker
<input type="checkbox"/>	- Conc...		Concentrator
<input type="checkbox"/>	- Archi...		Archiver
<input type="checkbox"/>	- Work...		Workbench
<input type="checkbox"/>	- Log C...		Log Collector
<input type="checkbox"/>	- Log ...		Log Decoder
<input type="checkbox"/>	- Wareh...		Warehouse C...
	NW – Malware A		Malware A

Cancel

Replicate

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

Change Password

Please enter and confirm the service user password. Only the user password changes on the selected services. No other user attributes will replicate to the services

Password

Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	- Broker		Broker
<input type="checkbox"/>	- Concentrator		Concentrator
<input type="checkbox"/>	- Decoder		Decoder
<input type="checkbox"/>	- Archiver		Archiver
<input type="checkbox"/>	- Workbench		Workbench
<input type="checkbox"/>	- Log Collector		Log Collector
<input type="checkbox"/>	- Log Decoder		Log Decoder
<input type="checkbox"/>	- Warehouse C...		Warehouse C...
	SA - IPDB Extractor		IPDB Extractor

Cancel

Change Password

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.

Field	Description
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	<p>The authentication scheme for this user. The product line supports internal and external authentication.</p> <ul style="list-style-type: none">• 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 <i>System Security and User Management</i> guide.
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.

Field	Description
SA Core Query Timeout	<p>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.</p> <p>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.</p> <p>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.</p>
Session Threshold	<p>(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.</p> <p>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.</p>

Role Membership

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

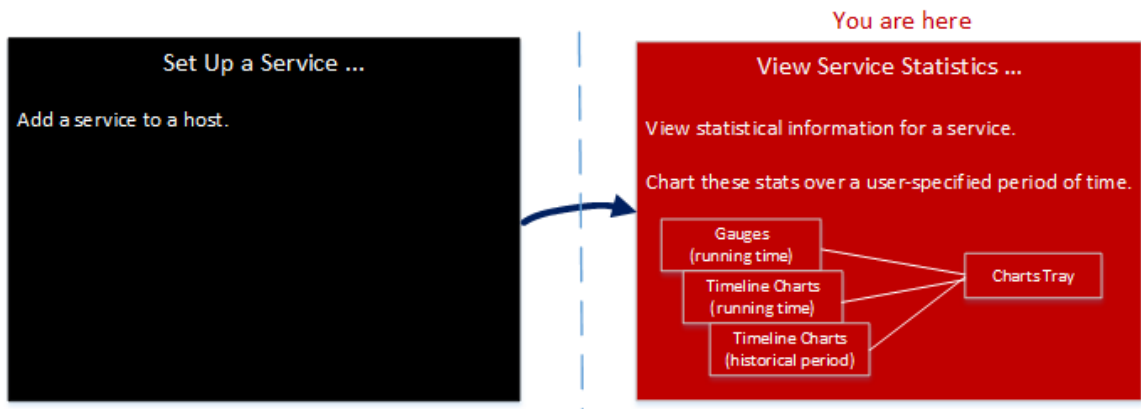
Services Stats View

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.

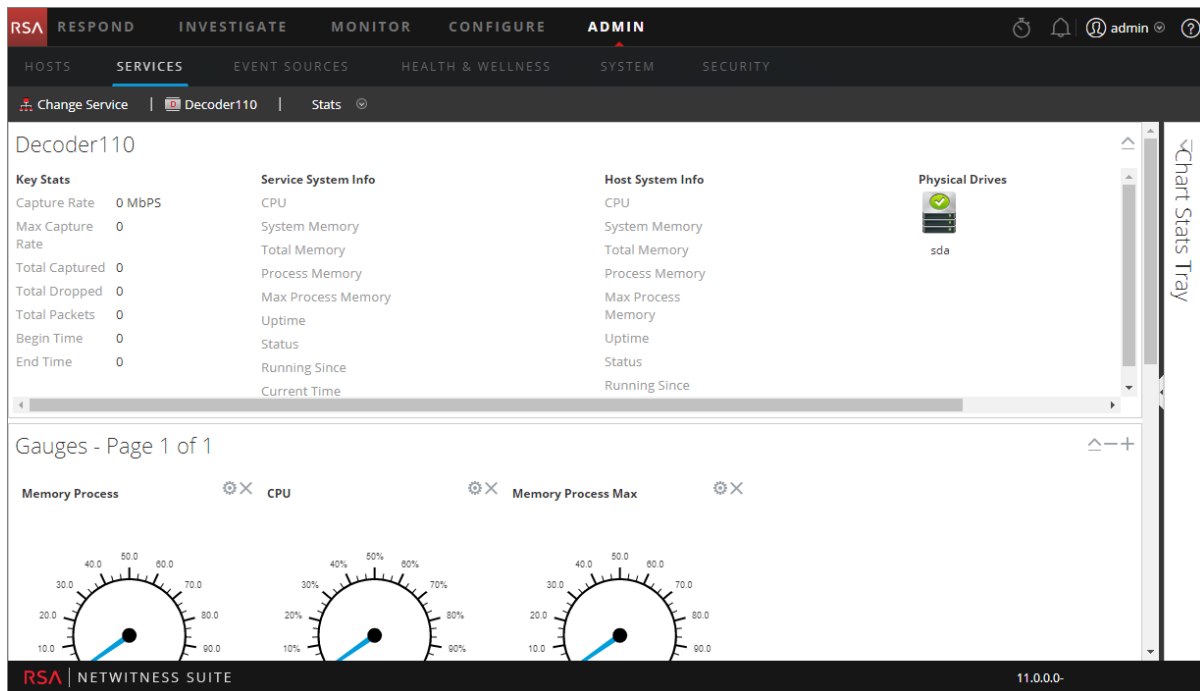


In the Stats view, you can customize the monitored statistics for individual services.

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.

Key Stats	
Capture Rate	0 MBPS
Max Capture Rate	33 MBPS
Total Captured	8.2 Million Packets
Total Dropped	0 Packets (0% loss)
Total Packets	271,941 Packets
Begin Time	2008-Feb-13 16:55:19
End Time	2015-Jan-23 05:15:47

- 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.

Key Stats				
Key Stats	Rate	Max	Behind	Status
	0	2346	0	consumir
	0	0	0	consumir
	0	26	0	consumir

Service System Info

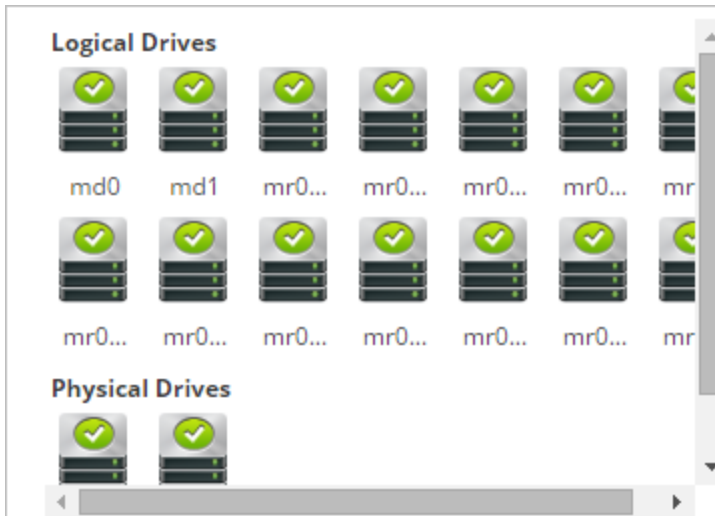
The Service System Info panel includes the percentage of CPU used by the service, the memory usage statistics (system, total, process, and maximum process), service uptime, status, running since time, and the current time.

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.

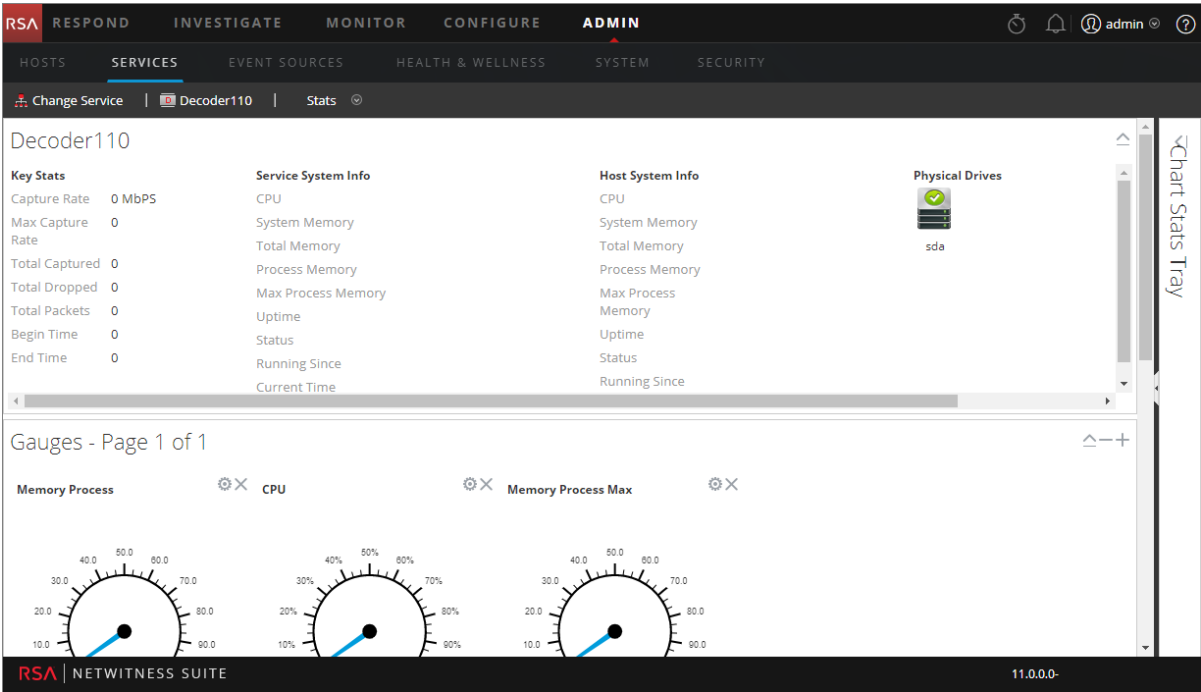
To access the Services Stats view:

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.


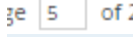



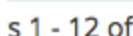
The following example shows the Services Stats view for a Decoder. The Chart Stats Tray is collapsed.



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.

Feature	Description
	Click to go to the previous page.
	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.
	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:

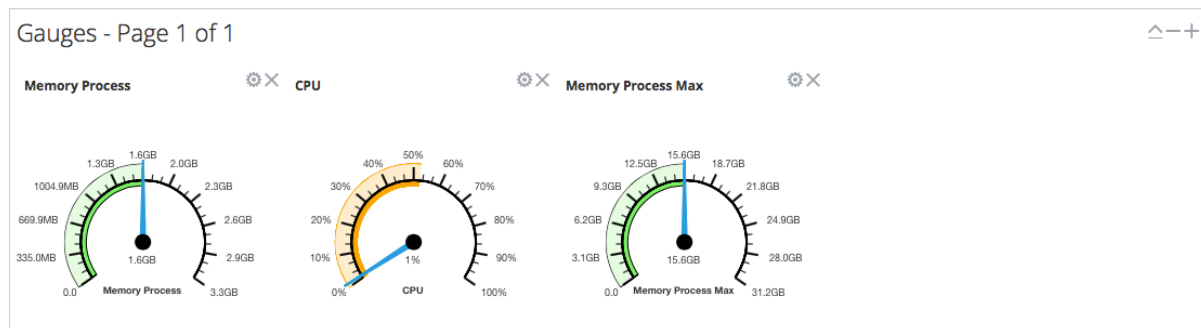
1. In the **NetWitness Suite** menu, select **ADMIN > Services**

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.

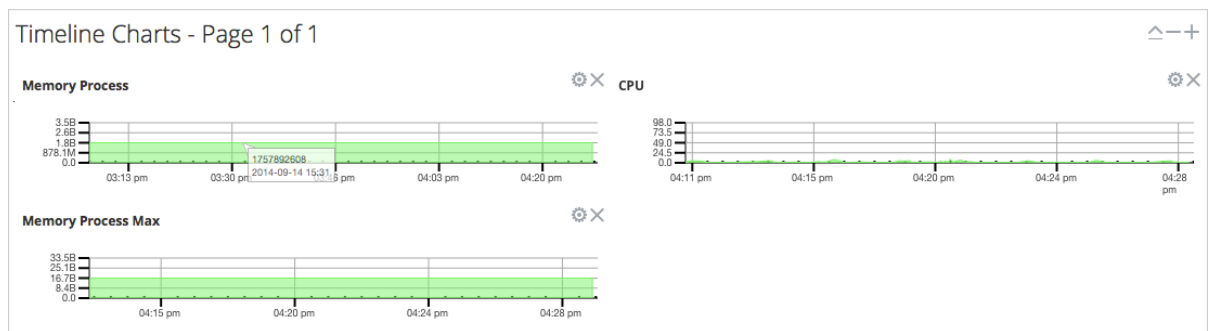
- In the Gauges title bar, you can collapse and expand the section and page forward or back.
- In each gauge, you can edit properties (⚙) and delete (✕) the gauge.

Timeline Charts

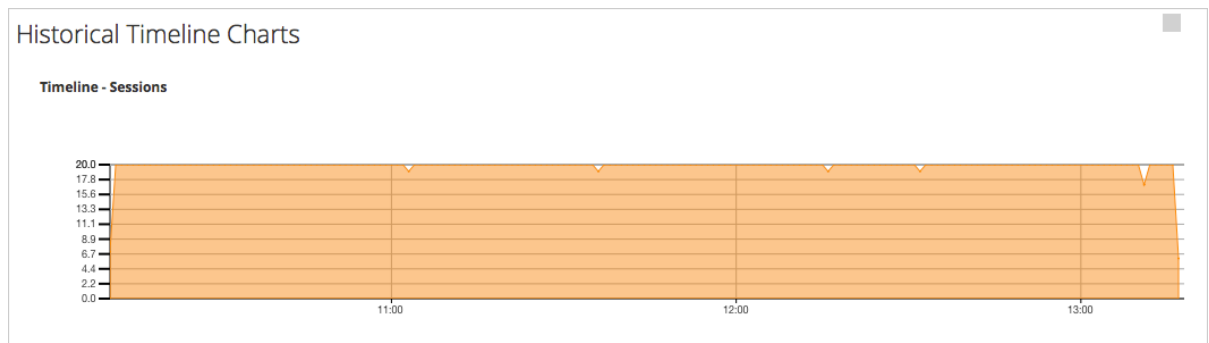
This topic describes the features of the timeline charts in the Services Stats view.

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.

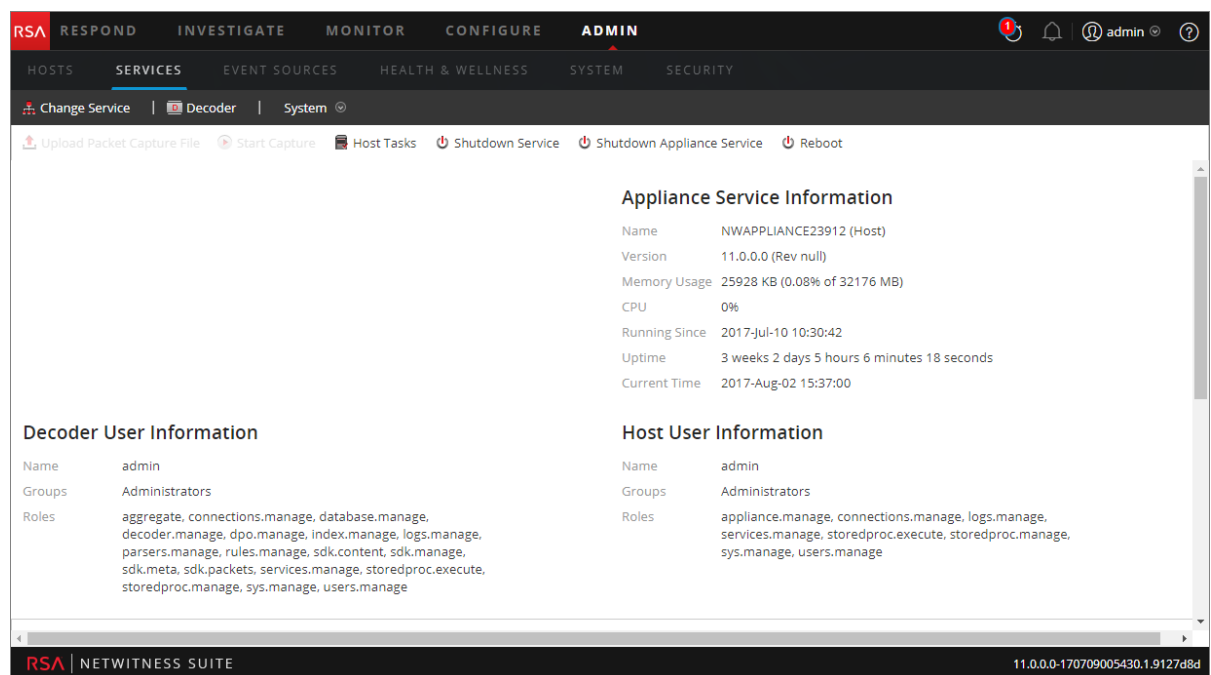
To access the Services System view for a Decoder:

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 screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is selected, and the left sidebar shows the path: ADMIN > SERVICES > SYSTEM. The main content area displays the following information:

Appliance Service Information	
Name	NWAPPLIANCE23912 (Host)
Version	11.0.0.0 (Rev null)
Memory Usage	25928 KB (0.08% of 32176 MB)
CPU	0%
Running Since	2017-Jul-10 10:30:42
Uptime	3 weeks 2 days 5 hours 6 minutes 18 seconds
Current Time	2017-Aug-02 15:37:00

Decoder User Information	
Name	admin
Groups	Administrators
Roles	aggregate, connections.manage, database.manage, decoder.manage, dpo.manage, index.manage, logs.manage, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information	
Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

The bottom of the interface shows the RSA logo and the text "NETWITNESS SUITE" on the left, and the version "11.0.0.0-170709005430.1.9127d8d" on the right.

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

The screenshot displays the RSA NetWitness Suite Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, showing sub-tabs for HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The SERVICES tab is selected, showing a toolbar with options: Change Service, Log Decoder, and System. Below the toolbar, there are four information panels:

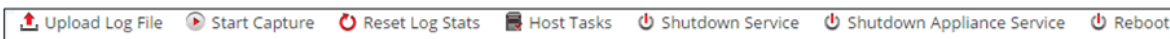
- Log Decoder Service Information:**
 - Name: NWAPPLIANCE11639 (Log Decoder)
 - Version: 11.0.0.0 (Rev null)
 - Memory Usage: 1764 MB (5.48% of 32176 MB)
 - CPU: 2%
 - Running Since: 2017-Jul-27 05:44:55
 - Uptime: 6 days 9 hours 53 minutes 30 seconds
 - Current Time: 2017-Aug-02 15:38:25
- Appliance Service Information:**
 - Name: NWAPPLIANCE11639 (Host)
 - Version: 11.0.0.0 (Rev null)
 - Memory Usage: 26808 KB (0.08% of 32176 MB)
 - CPU: 3%
 - Running Since: 2017-Jul-12 10:23:15
 - Uptime: 3 weeks 5 hours 15 minutes 11 seconds
 - Current Time: 2017-Aug-02 15:38:26
- Log Decoder User Information:**
 - Name: admin
 - Groups: Administrators
 - Roles: aggregate, connections.manage, database.manage, decoder.manage, dpo.manage, index.manage, logs.manage, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
- Host User Information:**
 - Name: admin
 - Groups: Administrators
 - Roles: appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

The bottom of the console shows the RSA NETWITNESS SUITE logo and the version 11.0.0.0.

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 <i>Decoder and Log Decoder Configuration Guide</i> .
	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 the Upload Log File to a Log Decoder topic in the <i>Decoder and Log Decoder Configuration Guide</i> .
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:

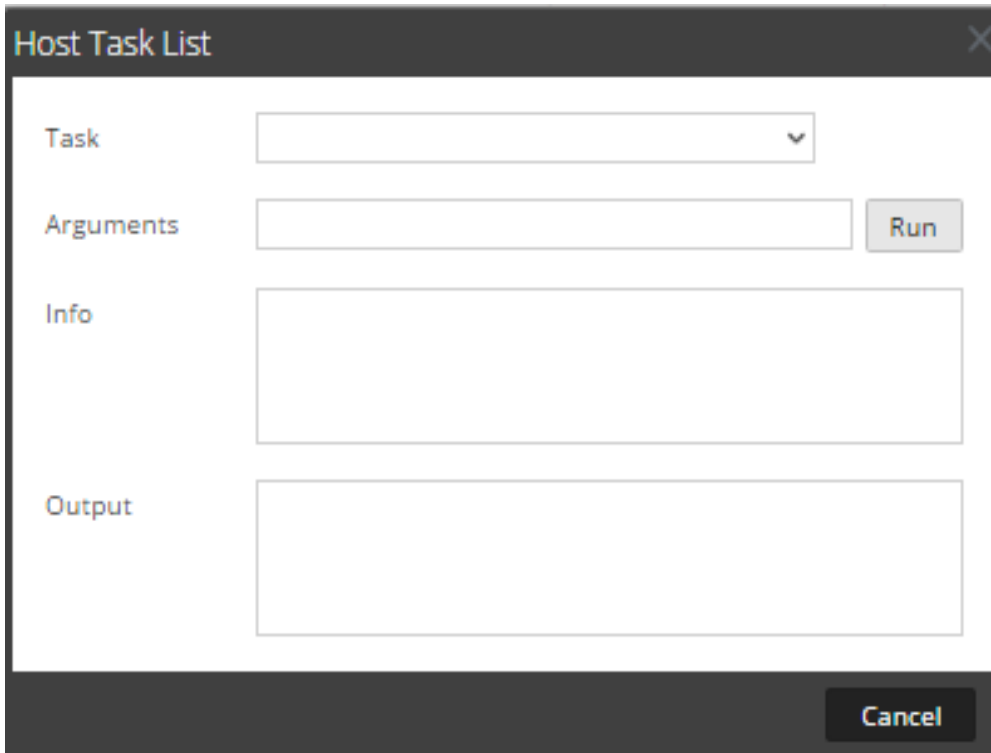
1. In **NetWitness Suite**, select **ADMIN > Services**.

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.



The Host Task List dialog box is shown. It has a title bar with the text "Host Task List" and a close button (X). The dialog contains four main sections: "Task" with a dropdown menu, "Arguments" with a text input field and a "Run" button, "Info" with a large text area, and "Output" with a large text area. A "Cancel" button is located at the bottom right.

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 <u>remains off</u> (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.

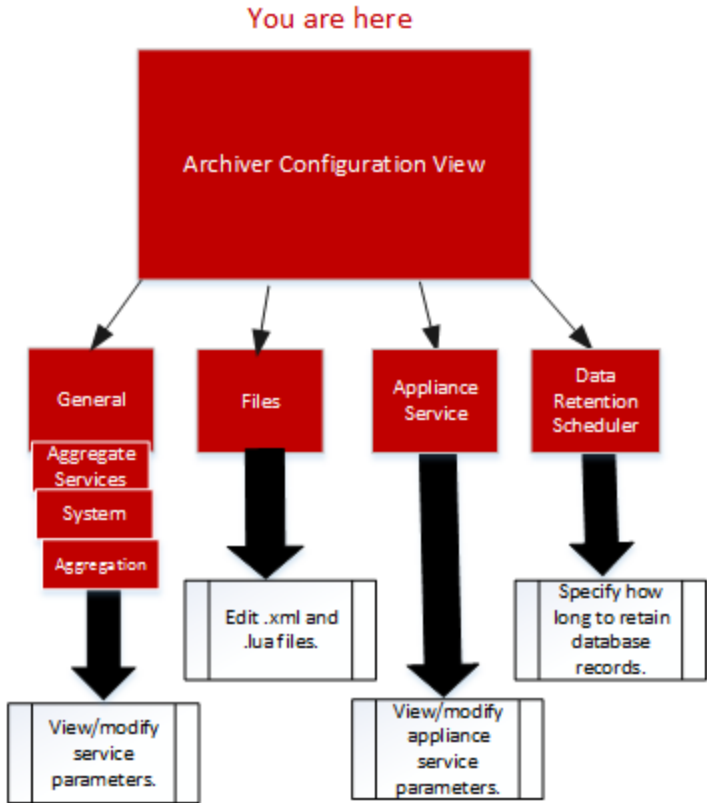
Appliance Parameter Field	Description
Logs	/logs/config, see Core Service Logging Configuration Parameters
REST	/rest/config, see REST Interface Configuration Parameters
Services	/services/<service name>/config, see Core Service-to-Service Configuration Parameters
System	/sys/config, see Core Service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



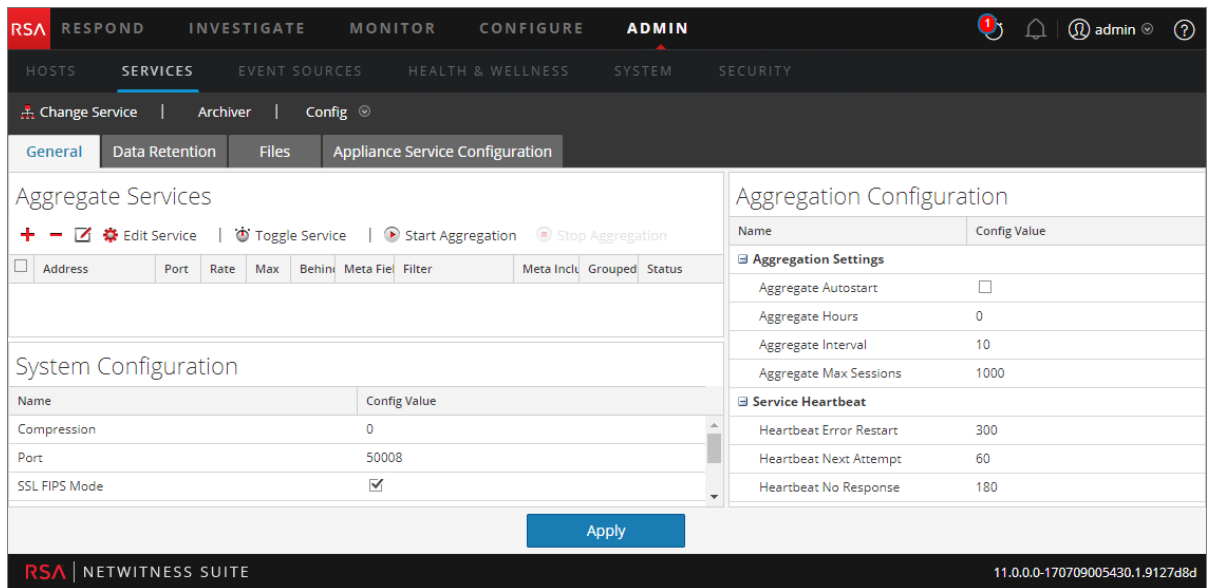
Role	I want to ...
Administrator	Configure Meta Filters for Aggregation. Refer to "(Optional) Configure Meta Filters for Aggregation" in the <i>RSA NetWitness Suite Archiver Configuration Guide</i> for instructions.
Administrator	Configure Group Aggregation. Refer to "Configure Group Aggregation" in the <i>RSA NetWitness Suite Deployment Guide</i> 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 <i>NetWitness SuiteCore Services Database Tuning Guide</i>
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.

Broker Parameter Field	Description
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 <i>NetWitness Suite Core Services Database Tuning Guide</i> 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.

Configuration Path	/concentrator/config or /archiver/config
aggregate.interval	Lists the minimum number of milliseconds before another round of aggregation is requested. Change takes effect immediately.
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.

Configuration Path	/concentrator/config or /archiver/config
export.format	Determines the file format used during data export. Change takes effect on service restart.
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.

Configuration Path	/concentrator/config or /archiver/config
heartbeat.interval	Lists the number of milliseconds between heartbeat service checks. Change takes effect immediately.
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 <i>NetWitness Suite Core Database Tuning Guide</i>
Index	/index/config refer to the Index Configuration Nodes topic in the <i>NetWitness Suite Core Database Tuning Guide</i>
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 <i>NetWitness Suite Core Database Tuning Guide</i> and NetWitness Suite Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration Parameters

Concentrator Parameter Field	Description
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.

Logs Configuration Folder	/logs/config
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.
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.

Logs Configuration Folder	/logs/config
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.

System Configuration Folder	/sys/config
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.
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 <i>NetWitness Suite Core Database Tuning Guide</i>
Index	/index/config refer to the Index Configuration Nodes topic in the <i>NetWitness Suite Core Database Tuning Guide</i>

Decoder Parameter Field	Description
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 <i>NetWitness Suite Core Database Tuning Guide</i> 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.

Decoder Configuration Path	/decoder/config
assembler.session.flush	Flushes sessions when they are complete (1) or flushes sessions when they are parsed (2). Change takes effect on service restart.
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	<p>Displays capture service specific parameters. Change takes effect on service restart.</p> <p>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.</p> <p>On Log Decoders, there is only the Log Events capture device. It accepts some optional parameters.</p> <ul style="list-style-type: none"> • 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.

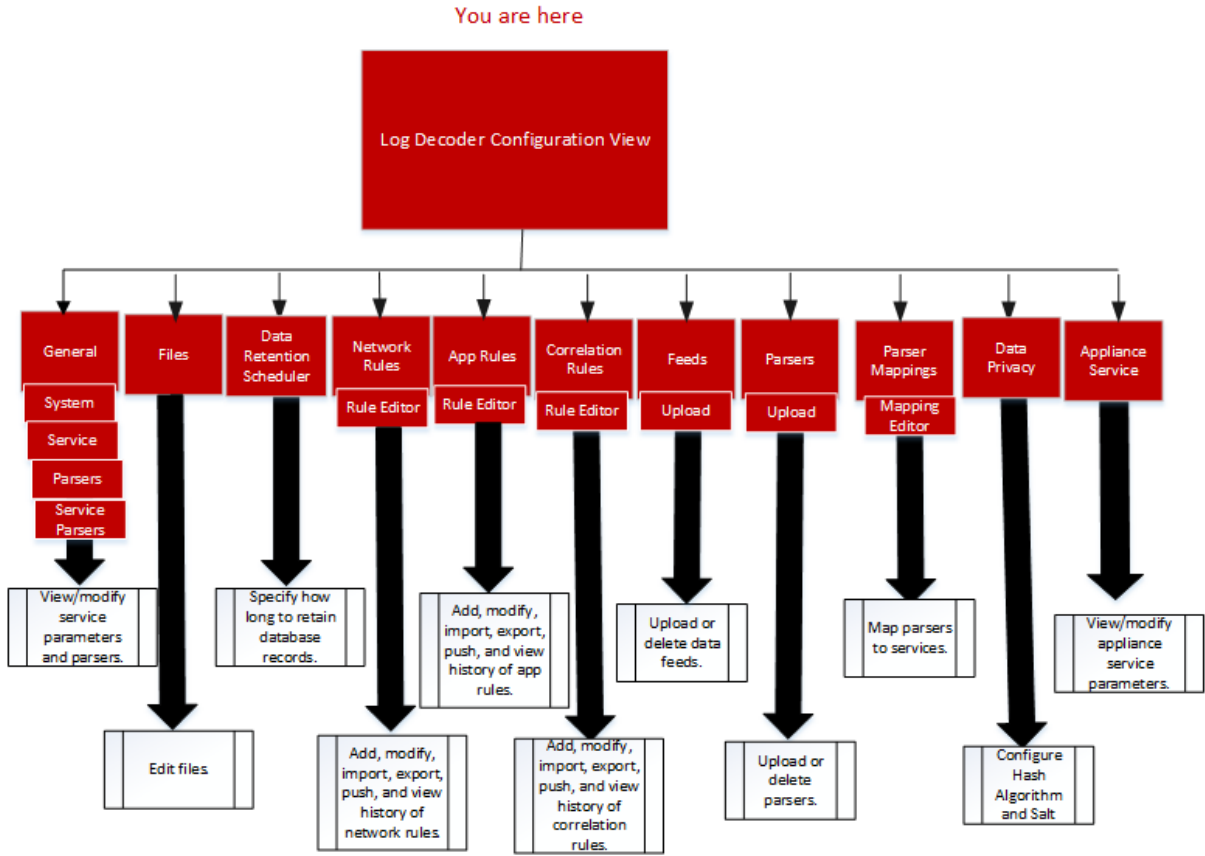
Decoder Configuration Path	/decoder/config
export.usage.max	Lists the session maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
parse.threads	Lists the number of parse threads to use for session parsing. 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 ...
------	---------------

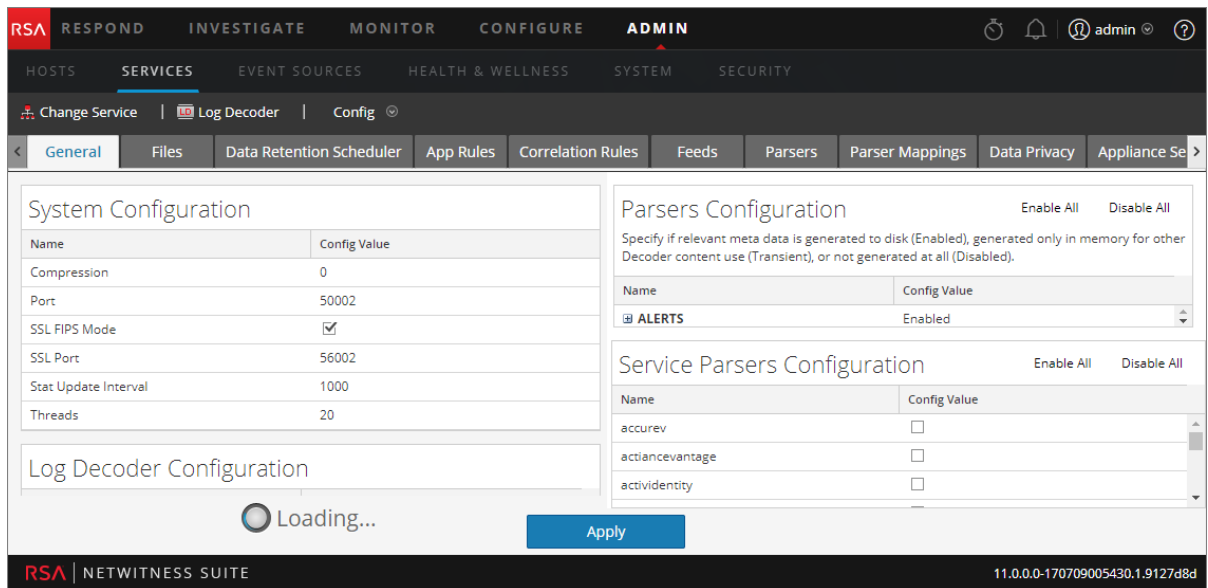
Administrator Configure Group Aggregation.

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 <i>NetWitness Suite Core Database Tuning Guide</i> .
Decoder	/decoder/config refer to Decoder and Log Decoder Configuration Parameters
Index	/index/config refer to the Index Configuration Nodes topic in the <i>NetWitness Suite Core Database Tuning Guide</i> .
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 <i>NetWitness Suite Core Database Tuning Guide</i> 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	<p>The set of device types that will be scanned for raw text tokens. By default, this is set to <code>unknown</code>, 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.</p> <p>If this field is empty, then log tokenization is disabled.</p>
token.char.classes	<p>This field controls the type of tokens that are generated. It can be any combination of the values <code>alpha</code>, <code>digit</code>, <code>space</code>, and <code>punct</code>. The default value is <code>alpha</code>.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
token.min.length	<p>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.</p>

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 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.
port	Displays the port the REST service will listen on. Change takes effect on service restart.

REST Configuration Path	/rest/config
ssl	<p>Encrypts all REST traffic using SSL, if enabled. The default 'system' means use setting from /sys/config/ssl.</p> <p>Change takes effect on service restart.</p>

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 Updates

Error Message	Failed to download because of the following errors.
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	<ol style="list-style-type: none">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)" under Apply Version Updates to a Host in the <i>NetWitness Suite Host and Services Getting Started Guide</i>.3. If you still cannot download the update file, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	Error updating <ip-address> to version <version-number>.
Problem	When you select an update version and click Update >Update Host , the download process is successful, but the update process fails.
Solution	<ol style="list-style-type: none"> 1. Try to apply it again. 2. If you still cannot apply the new version update: <ol style="list-style-type: none"> a. Monitor the following logs on NW Server as it progresses (for example, use submit the <code>tail -f</code> command string from the command line'): <pre> /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 </pre> The error will appear in one or more of these logs. b. Try to resolve the issue and reapply the version update. 3. If that did not work, try to apply the version update outside of the user interface as described in "Apply Updates from the Command Line (No Web Access)" under Apply Version Updates to a Host in the <i>NetWitness Suite Host and Services Getting Started Guide</i>. 4. If you still cannot apply the update, gather the logs from from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	Update path not supported.
Problem	You tried to apply a version update to the Legacy Windows Log Collector.
Cause	RSA does not support updates to the Legacy Windows Log Collector from the Host view.
Solution	Refer to the <i>RSA NetWitness 11.0 Legacy Windows Collection Guide</i> on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

