NetWitness® Platform

Version 12.5.1

Hosts and Services Getting Started Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2024

Contents

Hosts and Services Basics **8**

What Is a Host? 8

What Is a Category? 8

What Is a Service? 9

Setting Up a Host 12

Maintaining Hosts 12

Update Version Naming Convention 12

Maintaining Services 13

Services Implemented with the NetWitness Server 13

Running in Mixed Mode 15

Functionality Gaps Encountered During in Staggered Updates 15

Examples of Staggered Updates 15

Example 1. Multiple Network Decoders and Concentrators, Alternative 1 15

Example 2. Multiple Network Decoders and Concentrators, Alternative 2 16

Example 3. Multiple Regions 16

Hosts and Services Set Up Procedures **18**

Step 1. Deploy a Host 18

Step 2. Install a Service on a Host 19

Step 3. Review SSL Ports for Trusted Connections 20

Encrypted SSL Ports 20

Step 4. Manage Access to a Service 20

Test a Trusted Connection 20

Hosts and Services Maintenance Procedures **24**

Apply Version Upgrades to a Host 26

Pre-Stage Host 26

Create and Manage Host Groups 27

Create a Group 28

Change the Name of a Group 28

Add a Host to a Group 28

View the Hosts in a Group 28

Remove a Host from a Group 29

Delete a Group 29

Search for Hosts 29

Search for a Host 30

Find the Host that Runs a Service 30

Execute a Task From the Host Task List ... 30
Add and Delete a Filesystem Monitor ... 33
Configure the Filesystem Monitor ... 33
Delete a Filesystem Monitor ... 34
Reboot a Host ... 34
Shut Down and Restart a Host from the Hosts View ... 35
Shut Down and Restart a Host from the Host Task List ... 35
Set Host Built-In Clock ... 35
Set the Time on the Local Clock ... 36
Set Network Time Source ... 36
Specify the Network Clock Source ... 37
Set SNMP ... 38
Toggle SNMP Service on the Host ... 38
Set Syslog Forwarding ... 39
Set Up and Start Syslog Forwarding ... 39
Show Network Port Status ... 41
Display the Network Port Status ... 41
Show Serial Number ... 41
Show the Serial Number ... 42
Shut Down Host ... 42
Shut Down the Host ... 43
Stop and Start a Service on a Host ... 43
Stop a Service on a Host ... 43
Start a Service on a Host ... 44
Add, Replicate, or Delete a Service User ... 45
Add a User Role to a Service ... 48
Change a Service User Password ... 50
Create and Manage Service Groups ... 52
Create a Group ... 52
Change the Name of a Group ... 53
Add a Service to a Group ... 53
View the Services in a Group ... 53
Remove a Service from a Group ... 54
Delete a Group ... 54
Duplicate or Replicate a Service Role ... 54
Duplicate a Service Role ... 55
Replicate a Role ... 56
Edit Core Service Configuration Files ... 56
Edit a Service Configuration File ... 57
Revert to a Backup Version of a Service Configuration File ... 57

Push a Configuration File to Other Services 58
Edit a Service Index File 58
Index and Custom Index Files 59
Configure the Task Scheduler 59
Scheduler File 59
Scheduler Task Syntax 59
Task Line Parameters 60
Messages 60
Sample Task Line 61
Enable the Crash Reporter Service 61
The crashreporter.cfg File 61
Configure the Crash Reporter Service 63
Start and Stop the Crash Reporter Service 64
Maintain the Table Map Files 64
Prerequisites 65
Edit or Delete a Service 66
Edit a Service 67
Delete a Service 68
Edit Service Hierarchy Timeout Settings 68
Explore and Edit Service Property Tree 69
Display or Edit a Service Property 69
Send a Message to a Node 70
Terminate a Connection to a Service 70
Terminate a Session on a Service 70
Terminate an Active Query in a Session 71
Search for Services 72
Search for a Service 72
Filter Services by Type 73
Find the Services on a Host 74
Start, Stop, or Restart a Service 75
Start a Service 75
Stop a Service 75
Restart a Service 75
View Service Details 76
Purpose of Each Service View 76
Access a Service View 76
View Topology Details 78
Centralized Service Configuration via Policy 79
Creating Groups and Policies 80
Create a Group 80

Create a Policy ... 81
Managing Groups and Policies ... 82
View a Group ... 82
Delete a group ... 82
Edit a Group ... 82
Filter Groups ... 83
Delete a Policy ... 83
Revert a Policy ... 84
Clone a Policy ... 84
Edit a Policy ... 84
View a Policy ... 85
Filter Policies ... 85
Hosts and Services Views References ... 86
Hosts View ... 87
Services View ... 92
Edit Service Dialog ... 99
Services Config View ... 102
Services Config View - Appliance Service Configuration Tab ... 105
Services Config View - Data Retention Scheduler Tab ... 107
Services Config View - Files Tab ... 110
Services Explore View ... 113
Services Explore View - Properties Dialog ... 116
Services Logs View ... 119
Services Security View ... 122
Services Security View - Users Tab ... 125
Services Security View - Roles Tab ... 131
Services Security View - Service User Roles and Permissions ... 133
Services Security View - Aggregation Role ... 136
Services Security View - Settings Tab ... 137
Services Stats View ... 141
Services Stats View - Chart Stats Tray ... 146
Services Stats View - Gauges ... 149
Services Stats View - Timeline Charts ... 150
Services System View ... 153
Services Topology View ... 156
Services System View - Host Task List Dialog ... 158
Service Configuration Settings ... 161
Aggregation Configuration Parameters ... 161
Appliance Service Configuration Parameters ... 163
Archiver Service Configuration View ... 163

Broker Service Configuration Parameters ... 165
Concentrator Service Configuration Parameters ... 166
Core Service Logging Configuration Parameters ... 166
Core Service-to-Service Configuration Parameters ... 167
Core Service System Configuration Parameters ... 168
Decoder Configuration Parameters ... 169
Network Decoder Service Configuration Parameters ... 172
Log Decoder Service Configuration Parameters ... 172
REST Interface Configuration Parameters ... 175
NetWitness Platform Core Service system.roles Modes ... 175
Centralized Service Configuration via Policy Settings ... 177
Centralized Service Configuration – Groups Tab ... 177
Create Group Dialog ... 179
Define Group Dialog ... 180
Assign Policy Dailog ... 183
Centralized Service Configuration – Policies Tab ... 186
Create Policy ... 188
Define Policy Settings ... 190
Assign to Group ... 192
Troubleshooting Version Installations and Updates ... 194
deploy_admin User Password Has Expired Error ... 195
Downloading Error ... 196
Error Deploying Version <version-number> Missing Update Packages ... 197
Upgrade Failed Error ... 197
External Repo Update Error ... 199
Host Installation Failed Error ... 199
Host Update Failed Error ... 200
Missing Update Packages Error ... 201
OpenSSL 1.1.x ... 202
Patch Update to Non-NW Server Error ... 202
Reboot Host After Update from Command Line Error ... 203
Reporting Engine Restarts After Upgrade ... 203
Log Collector Service (nwlogcollector) ... 205
NW Server ... 206
Orchestration ... 207
Reporting Engine Service ... 207
Event Stream Analysis ... 207

Hosts and Services Basics

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

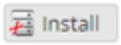
- Tasks you must complete to set up hosts and services in your network
- Additional procedures that you complete based on the long-term and daily, operational needs of your enterprise
- Reference topics that describe the user interface

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

What Is a Host?

A host is the machine on which a service runs and can be a physical or virtual machine. See the "NetWitness Detailed Host Deployment Diagram" in the *NetWitness Deployment Guide* for an illustration of how hosts are deployed.

What Is a Category?

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

. The following table lists each category and the services it installs. See the "NetWitness Detailed Host Deployment Diagram" in the *NetWitness Deployment Guide* for an illustration of how hosts are deployed.

Category	Services Installed
Analyst UI	Investigate Server, Broker, NetWitness UI, Reporting Engine, Respond Server
Archiver	Workbench and Archiver
Broker	Broker
Concentrator	Concentrator
Endpoint	Endpoint Server
Endpoint Broker	Endpoint Broker Server
Endpoint Log Hybrid	Log Collector, Log Decoder, Endpoint Server, and Concentrator
ESA Primary	Contexthub Server and ESA Correlation

Category	Services Installed
ESA Secondary	ESA Correlation
Log Collector	Log Collector
Log Decoder	Log Collector and Log Decoder
Log Hybrid	Log Collector, Log Decoder, and Concentrator
Log Hybrid - Retention	Log Collector and Log Decoder (deployed on NetWitness Series 6 Hybrid hardware with Log Hybrid-Retention Optimization)
Malware Analysis	Malware Analysis and Broker
Network Decoder	Decoder (Packets)
Network Hybrid	Concentrator and Network Decoder
New Health and Wellness	Metrics Server
UEBA	UEBA
Warehouse Connector	Warehouse Connector

What Is a Service?

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

You must configure the following Core services first:

- Network Decoder
- Concentrator
- Broker
- Log Decoder

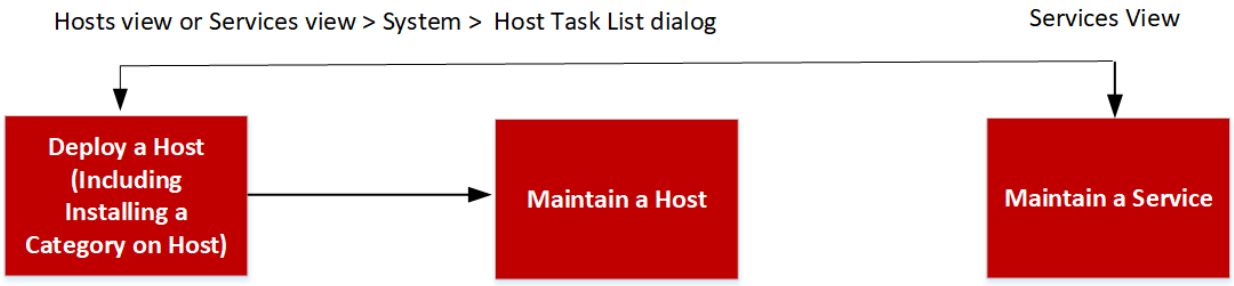
All the services are listed below and each service except the Log Collector has its own guide or shares a guide in the *Host and Services Configuration Guides* section of the NetWitness documentation page on NetWitness Community at https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation. 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*.

Services	Notes
NW Server	

Services	Notes
Admin Config Content Integration Investigate License Orchestration Reporting Engine Respond Security	Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server Resides within the NW Server
Response Actions	Resides within the NW Server
Analyst UI	
Broker Investigate Server NetWitness UI Reporting Engine Respond Server	Implemented with the Analyst UI Implemented with the Analyst UI Implemented with the Analyst UI Implemented with the Analyst UI Implemented with the Analyst UI
Archiver	
Archiver Workbench	Core Service
Broker	
Broker	Core Service
Concentrator	
Concentrator	Core Service
Endpoint	
Endpoint Server	
Endpoint Broker	
Endpoint Broker Server	
Endpoint Log Hybrid	
Log Collector Log Decoder Endpoint Server Concentrator	Core Service Core Service Core Service
ESA Primary	
Contexthub ESA Correlation	

Services	Notes
ESA Secondary	
ESA Correlation	
Log Collector	
Log Collector	Core Service
Log Decoder	
Log Collector Log Decoder	Core Service
Log Hybrid	
Log Collector Log Decoder Concentrator	Core Service Core Service
Log Hybrid - Retention	Deployed on Series 6 Hybrid hardware with Log Hybrid-Retention Optimization.
Log Collector Log Decoder	Core Service
Malware Analysis	
Malware Analysis Broker	Core Service
Network Decoder	
Decoder (Packets)	Core Service
Network Hybrid	
Concentrator Network Decoder	Core Service Core Service
New Health and Wellness	
Metrics Server	
UEBA	
UEBA	
Warehouse Connector	
Warehouse Connector	Command line installation

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. For information about ports and a comprehensive list of ports for all services, see "Network Architecture and Ports" in the *Deployment Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.



Setting Up a Host

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

Maintaining Hosts

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

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

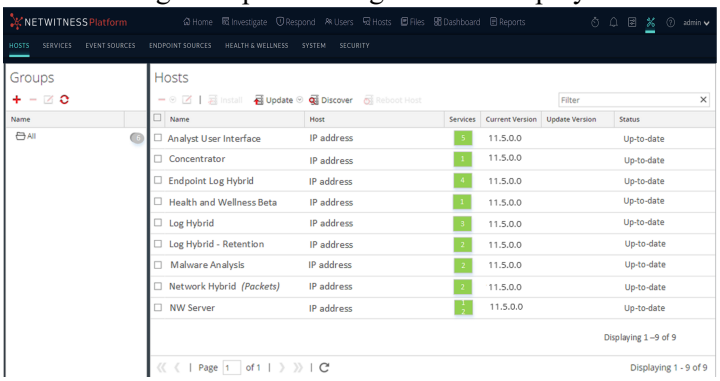
Update Version Naming Convention

You use the Hosts view to apply the latest version updates from your Hosts and Services Maintenance Procedures. 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 apply the following version to the host.

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

NetWitness supports multiple versions in your deployment. For more information, see Running in Mixed Mode. 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.

The following example is a single version deployment with all hosts updated to 11.5.0.0.



Maintaining Services

You use the Services view (**(Admin) > Services**) 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 list 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.
- Content, Investigate, Respond, and Source functionality.

Caution: You do not need to configure these services to deploy NetWitness. 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.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897).

Service	Purpose
Admin	The Administration (Admin) Server is the back-end service for administrative tasks in the NetWitness User Interface (UI). It abstracts authentication, global preferences management, and authorization support for the UI. The Admin server requires the Config server and the Security server to be online to perform its role.
Config	The Configuration (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.

Service	Purpose
Content	The Content server manages the NetWitness provided and user-created parser rules. For more information on parser management, search for "parsers" in NetWitness Community.
Integration	The Integration Server manages interactions with external systems. The service handles the following outbound or inbound channels. • REST API Gateway - gateway to external REST clients that assigns calls to the NetWitness Application Programming Interface (API). • Notifications Dispatcher - centralized dispatcher for all outbound notifications originating in the NetWitness deployment.
Investigate	The Investigate server supports Investigate and Malware Analysis functionality. For more information see the *NetWitness Investigate User Guide*.
Orchestration	The Orchestration server provisions, installs, and configures all services in your NetWitness deployment.
Respond	The Respond server supports Respond functionality. For more information see the *NetWitness Respond Configuration Guide*.
Security	The NetWitness Security Server (**Security server**) manages the security infrastructure of a NetWitness deployment. It handles the following security-related concerns. • Users and the authentication accounts • Role Based Access Control (RBAC) • Deployment PKI infrastructure A NetWitness deployment has users with authentication accounts. Independent of how you verify the identity of the analyst (for example, Active Directory), NetWitness must maintain the user state, which is not provided by all authentication providers (for example, last login time, failed login attempts, and roles). The concept of a user is separate from the identify associated with the user and the **Security server** maintains these as separate User and Account entities. In addition to the out-of-the-box local NetWitness accounts available to all NetWitness deployments, the server supports external authentication providers. The **Security server** also implements RBAC by managing Role and Permission entities. Permissions can be assigned to roles and roles to users. Together these enable a flexible authorization policy for the deployment. The server also manages generation of cryptographically secure tokens that encode the applicable authorization for a user. These tokens form the basis for deployment-wide authorization.
Source	The Source server is reserved for future use and will provide a centralized location to configure sources (for example, Endpoints and Log Sources).
Response Actions	Response Actions Server is introduced in 12.4 to integrate the third-party tools with NetWitness Platform.

Running in Mixed Mode

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

Functionality Gaps Encountered During in Staggered Updates

If you stagger the update, you:

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

Examples of Staggered Updates

In the following examples, all the hosts are on 11.4.0.0 and you want to stagger the host updates to version 11.4.1.0.

Example 1. Multiple Network Decoders and Concentrators, Alternative 1

In this example, the 11.4.0.0 deployment includes one NW Server host, two Network Decoder hosts, two Concentrator hosts, one Archiver host, one Broker host, one Event Stream Analysis host, one Endpoint Log Hybrid host, and one Malware Analysis host.

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

NetWitness recommends that you update the Sessions 2 and 3 hosts in the order listed.

Session 1: Update Essential Hosts

1. Update the NetWitness Server host.
2. Update the Event Stream Analysis host.
3. Update the Endpoint Log Hybrid host.
4. Update the Malware Analysis host.
5. Update the Broker host.

Session 2: Update Other Hosts

1. Update the two Network Decoder hosts.
2. Update the two Concentrator hosts and the Archiver host.

Session 3: Update Other Hosts

1. Update all other hosts.

Example 2. Multiple Network Decoders and Concentrators, Alternative 2

In this example, the 11.4.0.0 deployment includes one NW Server host, two Network Decoder hosts, two Concentrator hosts, one Broker host, one Event Stream Analysis host, one Endpoint Log Hybrid host and one Malware Analysis host.

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

NetWitness recommends that you update the Sessions 2 and 3 hosts in the order listed.

Session 1: Update Essential Hosts

1. Update the NetWitness Server host.
2. Update the Event Stream Analysis host.
3. Update the Endpoint Log Hybrid host.
4. Update the Malware Analysis host.
5. Update the Broker host.

Session 2: Update Other Hosts

1. Update one Network Decoder host and one Concentrator host.

Note: It does not matter which of the Network Decoder hosts or which of the Concentrator hosts you update first.

Time elapses during which NetWitness processes a significant amount of data.

Session 3: Update Other Hosts

1. Update the second Network Decoder host and the second Concentrator host.
2. Update all Log Decoder hosts before you update Virtual Log Collectors.
3. Update all other hosts.

Example 3. Multiple Regions

In this example, the 11.4.0.0 deployment includes one NW Server host, one Event Stream Analysis host, one Endpoint Log Hybrid host, one Malware Analysis host. Additionally, there are two sites, each with two Network Decoders, two Concentrators, and one Broker, for a total of four Network Decoder hosts, four Concentrator hosts, and two Broker hosts.

Session 1: Update Essential Hosts and Site 1

1. Update the NW Server host.
2. Update the Event Stream Analysis host.
3. Update the Endpoint Log Hybrid host.
4. Update the Malware Analysis host.
5. Update one Broker host, two Network Decoder hosts, and two Concentrator hosts.

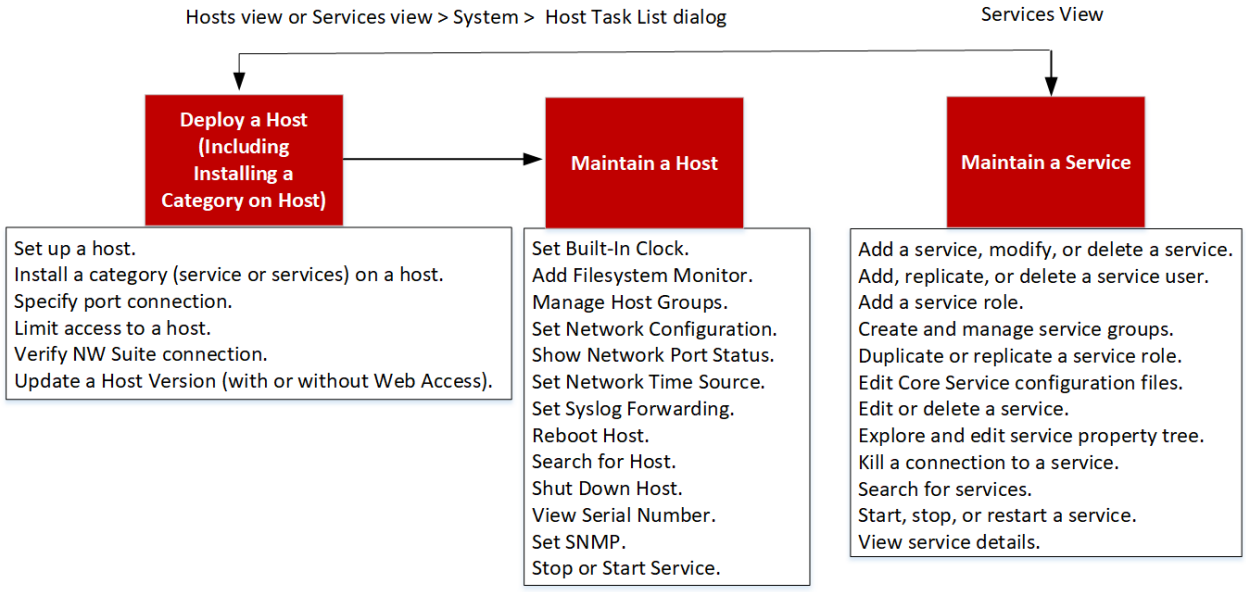
Session 2: Update Other Hosts and Site 2

1. Update the second Broker host.
2. Update the two remaining Network Decoder hosts.

3. Update the two remaining Concentrator hosts.
4. Update all the other hosts.

Hosts and Services Set Up 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 deployment. This topic contains information about basic procedures. For additional procedures, see Hosts and Services Maintenance Procedures.



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

Step 1. Deploy a Host

Caution: If you include "." in a host name, the host name must also include a valid domain name.

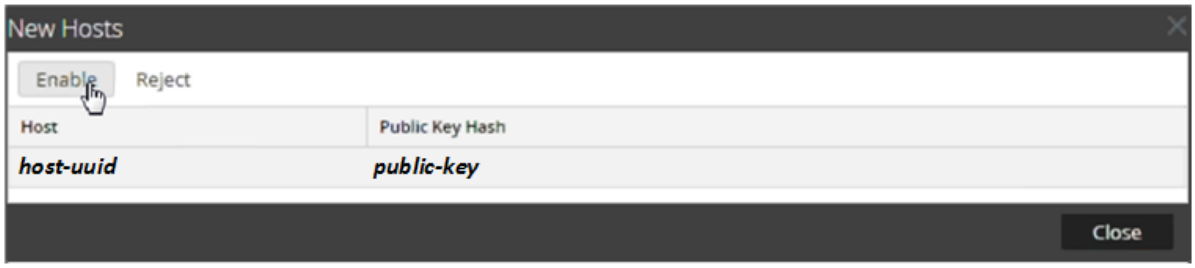
1. Deploy a host.

   You can deploy a physical host (NetWitness Appliance), virtual host on-prem, a virtual in AWS, a virtual host in Azure, or a virtual host on Google Cloud Platform. See the following guides for instructions on how to deploy hosts.

   - *Physical Host Installation Guide*
   - *Virtual Host Installation Guide*
   - *AWS Installation Guide*

- *Azure Installation Guide*
- *GCP Installation Guide*

2. Go to **(Admin) > 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**.

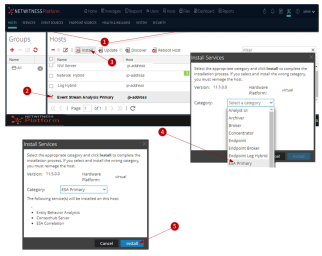


5. Select the host you enabled.
   The host is displayed in the Hosts view. At this point, you can install a service on the host.

Step 2. Install a Service on a Host

Perform the following steps to install a service on a host.

1. In NetWitness, go to **(Admin) > Hosts**.
   The Hosts view is displayed.
2. Select the host on which you want to install the service (for example, **Event Stream Analysis**).
3. Click Install in the toolbar.
   The Install Services dialog is displayed.
4. Select a service from the **Category** drop-down list (for example, **ESA Primary**).
5. Click Install in the Install Services dialog.



6. A pop-up listing all the services already installed on this host is displayed. If there are no services

installed, this pop-up will not be displayed.

7. Click **Yes** to install the new service.

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.

Encrypted SSL Ports

By default, trusted connections are established with two settings:

- SSL is enabled.
- Core service is connected to an encrypted SSL port.

Each NetWitness 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.

For information about ports and a comprehensive list of ports for all services, see "Network Architecture and Ports" in the *Deployment Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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 Core service. Instead, users who have been authenticated by the server can access the service without entering another password.

Test a Trusted Connection

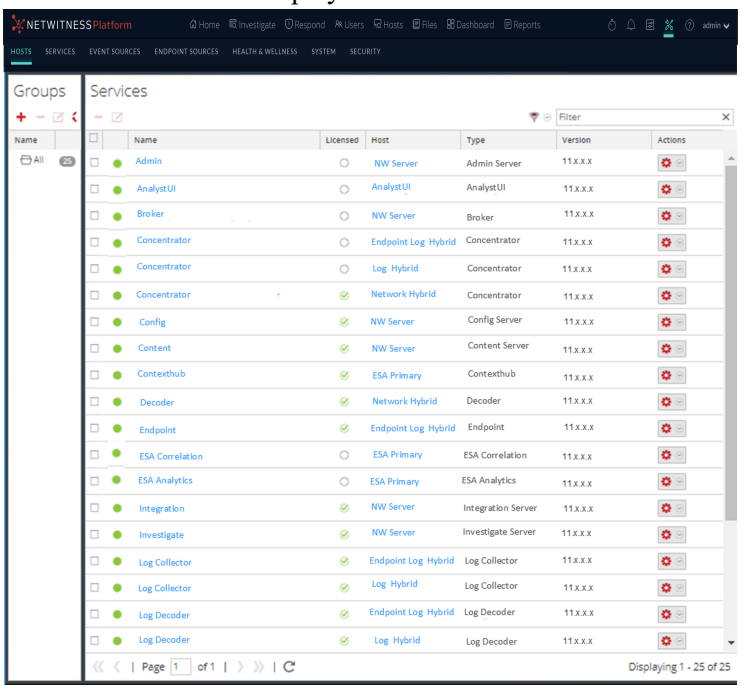
Prerequisites

1. The administrator must assign a role to the user.
   For more information, see "Add a User and Assign a Role" in the *System Security and User Management Guide*.

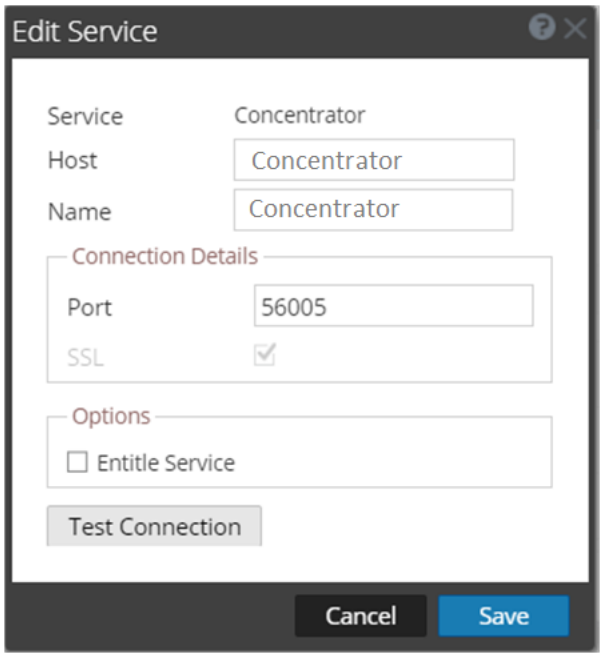
2. The user must:
   - Log in to NetWitness for the server to authenticate the user.
   - Have access to the service.

Procedure

1. In NetWitness, go to **(Admin) > Services**.
   The Services view is displayed.

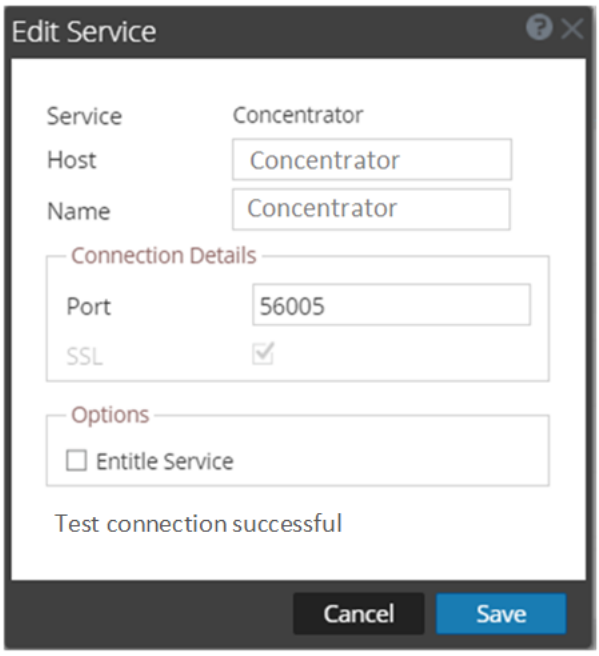


2. Select the checkbox of the service (for example, a Concentrator) to test and click  .
   The **Edit Service** dialog is displayed.



Note: The Options box will only display if the selected service is not licensed. A licensed service is denoted by a  in the Services view.

3. Remove the username to test the connection without credentials.
4. Click **Test Connection**.

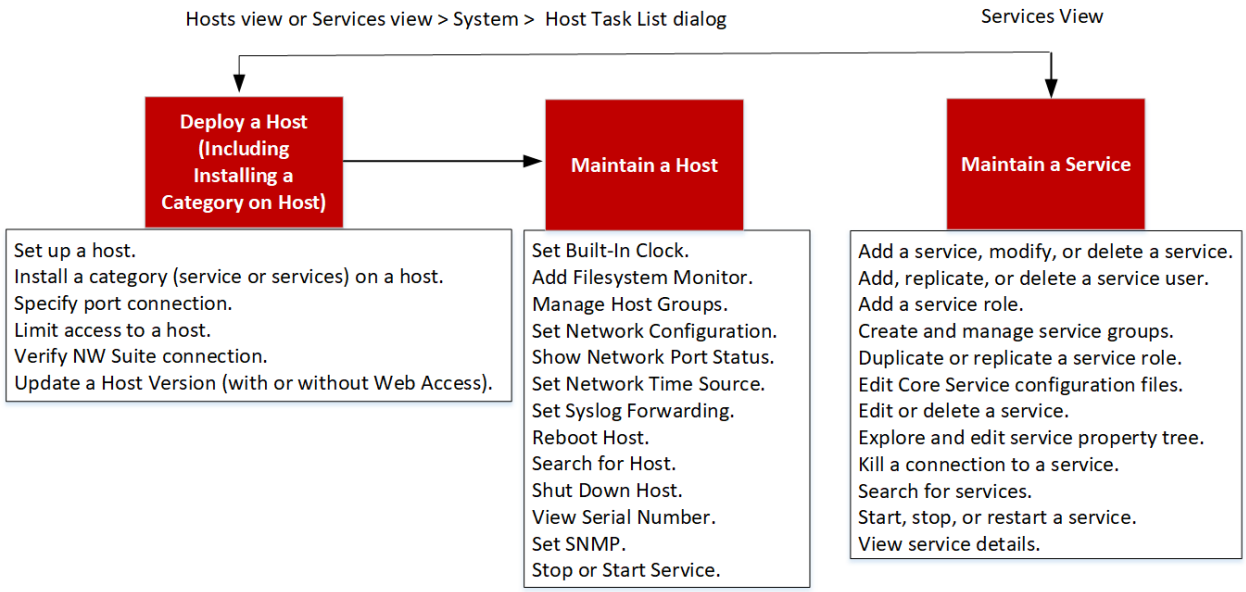


The message `Test connection successful` confirms the trusted connection is established. The previously authenticated user can access the service without typing a username and password on the service.

5. Click **Save**.

Hosts and Services Maintenance 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 deployment.



High-Level Task	Description
Maintain a Host - Basics	The following maintenance tasks are shown in alphabetical order. • Apply Version Upgrades to a Host • Create and Manage Host Groups • Search for Hosts • Set Network Time Source • Show Network Port Status • Show Serial Number • Shut Down Host • Stop and Start a Service on a Host

High-Level Task	Description
Maintain a Host from the Host Task List Dialog	You use the Host Task List dialog to manage tasks that relate to a host and its communications with the network. Several service and host configuration options are available for Core hosts. • Execute a Task From the Host Task List • Add and Delete a Filesystem Monitor • Reboot a Host • Set Host Built-In Clock • Set Network 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
Maintain a Service	The following procedures describe how to maintain services. • Add, Replicate, or Delete a Service User • Add a User Role to a Service • 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 • Terminate a Connection to a Service • Search for Services • Start, Stop, or Restart a Service • View Topology Details • Services System View • Centralized Service Configuration via Policy

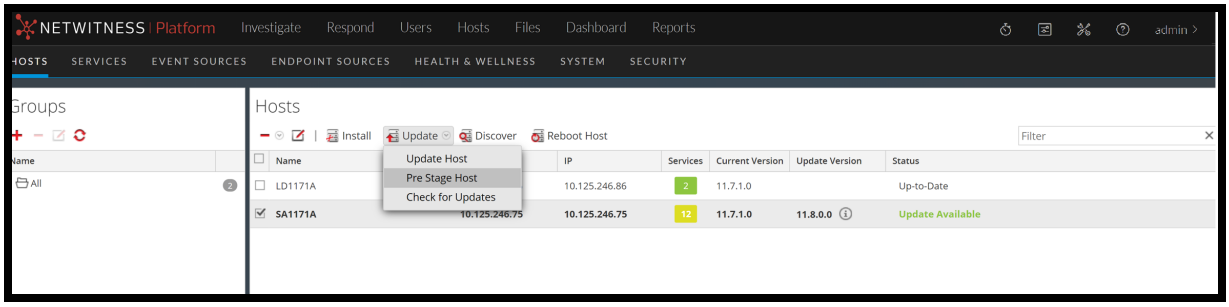
Apply Version Upgrades to a Host

Upgrade guides are available for all supported versions of NetWitness. Refer to the upgrade guide for the latest version in the *Install and Upgrade* section of the NetWitness documentation page on NetWitness Link.

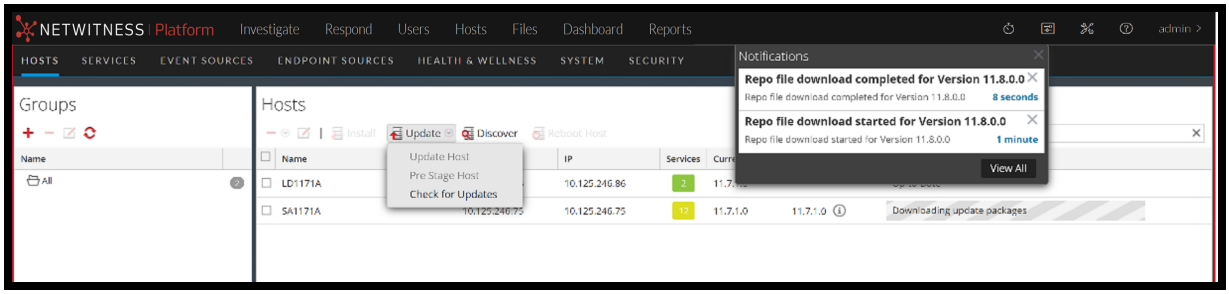
Pre-Stage Host

Note: The **Pre Stage Host** option is enabled for upgrade on the Admin Server. This option will be available after you upgrade to 11.7.1 and can be used to upgrade to versions later than 11.7.1.

1. Go to  > Hosts.
2. Click **Update** > **Check for Updates**.
   All possible update versions will displayed in the Versions drop-down list.
3. Click **Update** > **Pre Stage Host** and select the version in the update version column.
   A confirmation message for downloading the files is displayed.



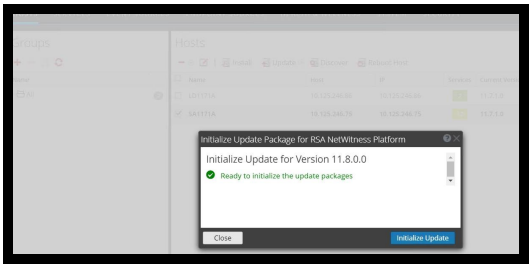
4. Click **Yes** to download the upgrade packages to the repo.
5. Verify the status of the download in the notifications tray as shown below.
   The **Pre Stage Host** and **Upgrade Host** will be disabled until pre stage is completed.



Note: The current version and the update version in the UI will be the same during the pre stage as it is not the actual update. This is because only the repo files are downloaded and no actual upgrade is done. The version will change only after upgrade.

6. If the download is successful, **Check for Updates** again to start the initialization.

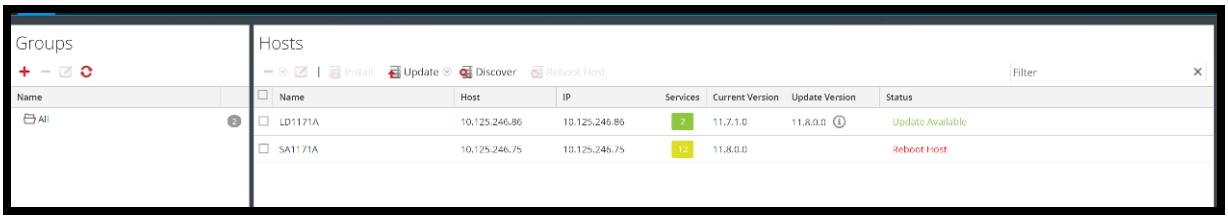
7. Click on **Initialize Update**.
   The initialization of the package will take some time as the files are large and will need to be unzipped.



IMPORTANT: Pre Stage Repo preparation steps from 1 to 4 can be performed at any time. However, from steps 5 to 8 the upgrade process begins and you must NOT reboot the host or restart the jetty server during this time as it will corrupt the .ZIP files.

8. Check the status of initialization in the notifications tray.

9. After the initialization is completed successfully, click **Update** > **Update Host.**
   After the host is updated, you will be prompted to reboot the host.



10. Set up the host and reboot the host.

Create and Manage Host Groups

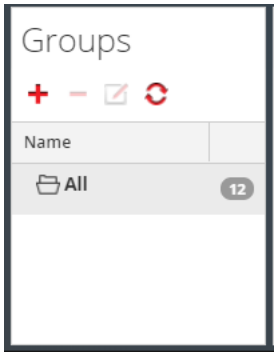
The Hosts view provides options for creating and managing groups of hosts. The Groups panel toolbar includes options for creating, editing, and deleting host groups. Once groups are created, you can drag individual hosts from the Hosts panel into a group.

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:

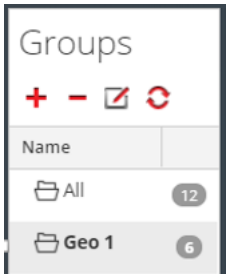
- Group different categories to make it easier to configure and monitor all Brokers, Network Decoders, or Concentrators.
- Group hosts that are part of the same data flow; for example, a Broker, and all associated Concentrators and Network Decoders.
- Group hosts according to their geographic region 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, `Geo 1`) and press **Enter**.
   The group is created as a folder in the tree. The number next to the group indicates the number of hosts in that group.



Change the Name of a Group

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

Add a Host to a Group

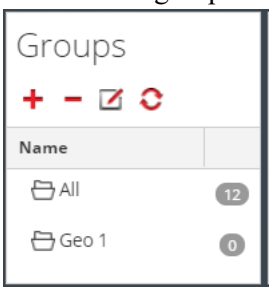
In the Hosts view **Hosts** panel, select a host and drag the host to a group folder in the Groups panel. The host is added to the group.

View the Hosts in a Group

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

Remove a Host from a Group

1. In the Hosts view **Groups** panel, select the group that contains the host that you want to remove. The hosts in that group appear in the Hosts panel.
2. In the **Hosts** panel, select one or more hosts that you want to remove from the group, and in the toolbar, select − > **Remove from Group**.
   The selected hosts are removed from the group, but are not removed from the NetWitness 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 `Geo 1` does not contain any hosts, because all the hosts in that group are 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 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 hosts in use for various purposes. Instead of scrolling through the host list, you can quickly filter the host list to locate the hosts that you want to administer.

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

Search for a Host

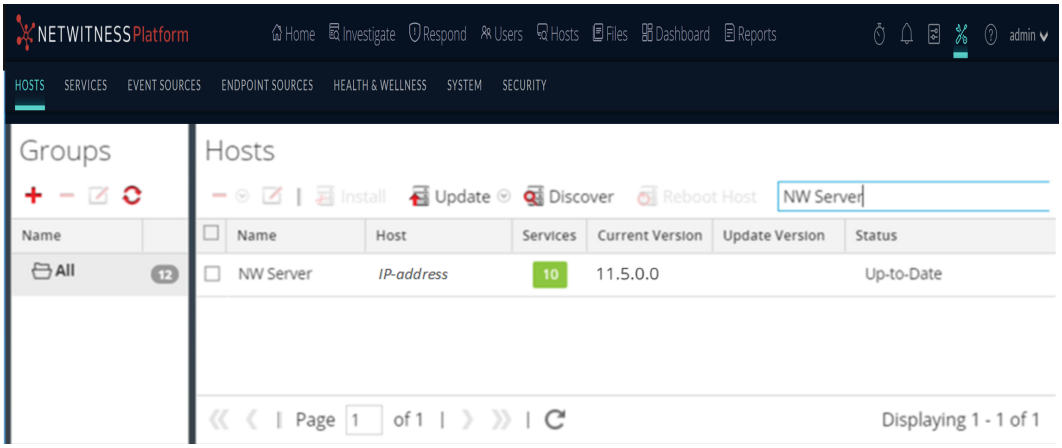
1. Select **(Admin) > Hosts**.
2. In the **Hosts** panel toolbar, type a host **Name** or **Hostname** in the **Filter** field.

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

Find the Host that Runs a Service

1. Select **(Admin) > Services**.
2. In the **Services** view, select a service. The associated host is listed in the Host column for that service.
3. To administer the host in the Hosts view, click the link in the **Host** column for that service. The host associated with the selected service is displayed in the Hosts view.

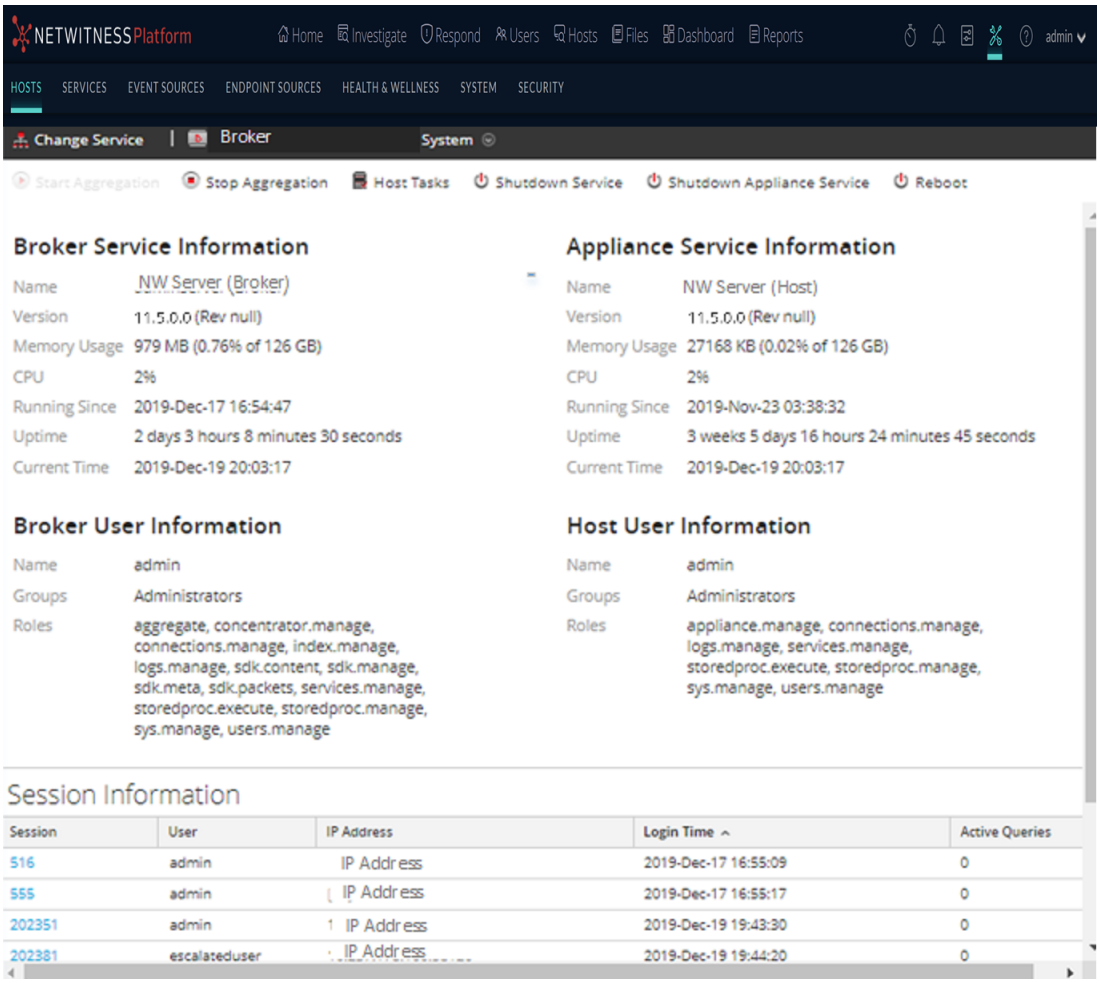


Execute a Task From the Host Task List

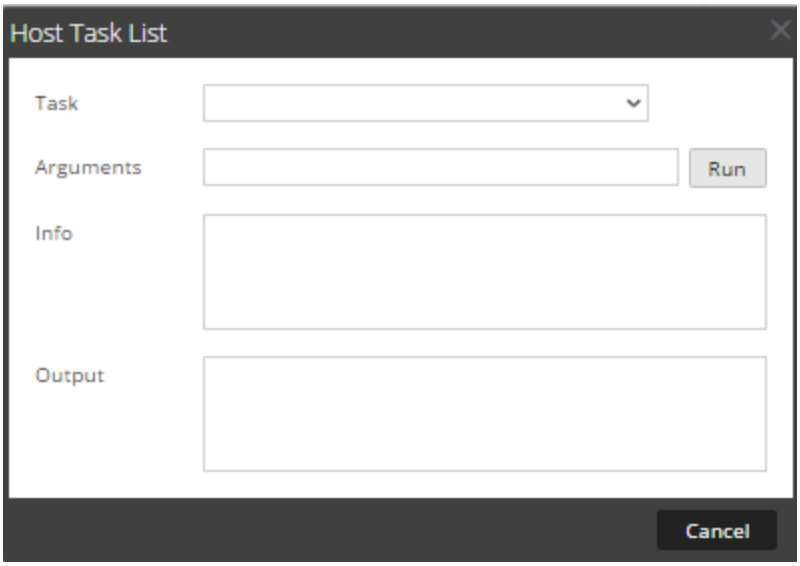
1. Select **(Admin) > Services**.
2. In the **Services** list, select a service and click **> View > System**.

   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.

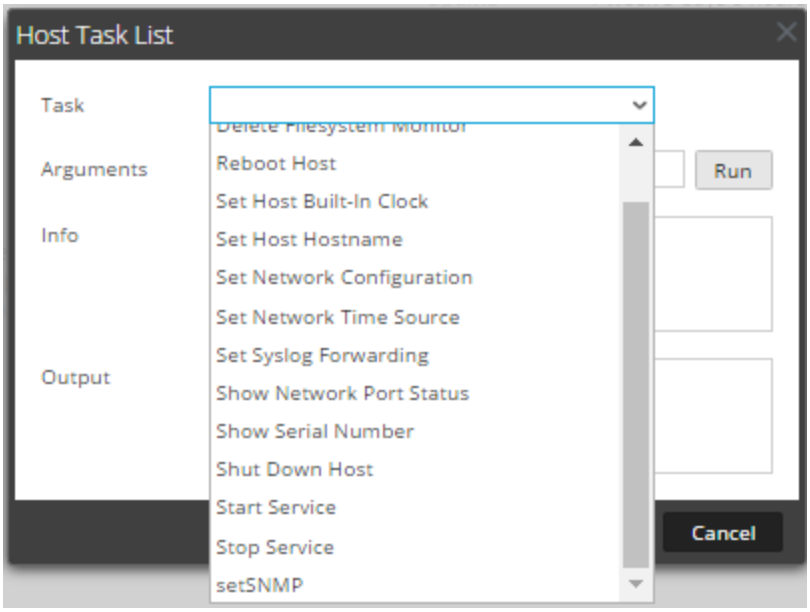
   The System view for the service is displayed below.



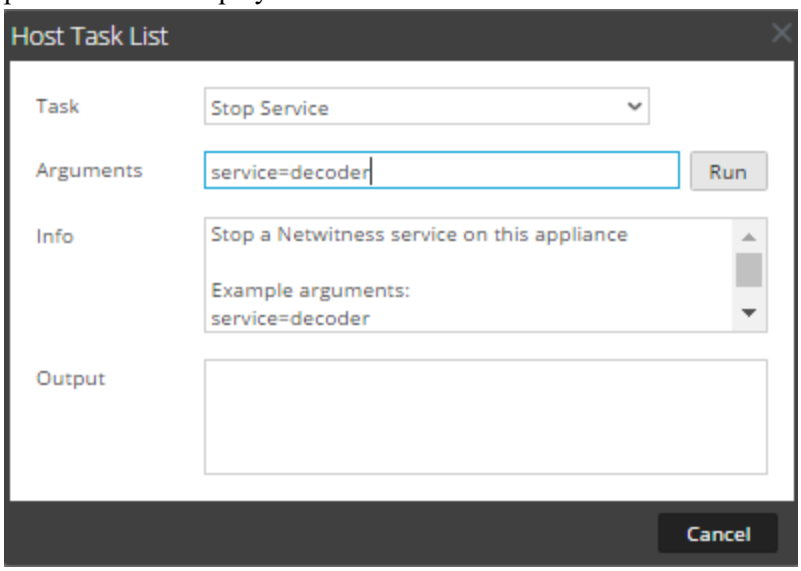
3. In the **Services System** view toolbar, click Host Tasks.



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



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



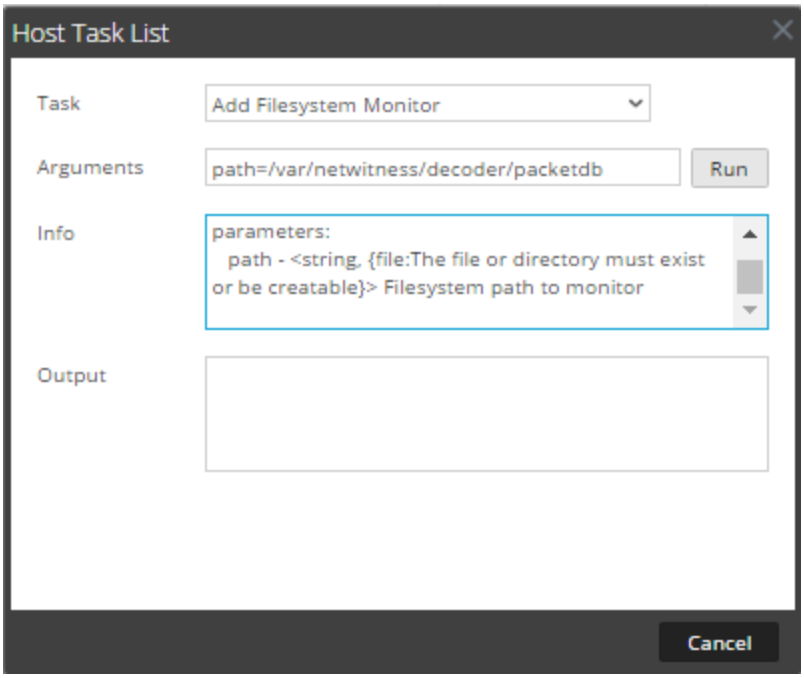
6. Type arguments if necessary and click **Run**.
The command executes and the result is displayed in the Output section.

Add and Delete a Filesystem Monitor

When you want a service to monitor traffic on a specific file system, you can select the service and then specify the path. NetWitness Platform 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

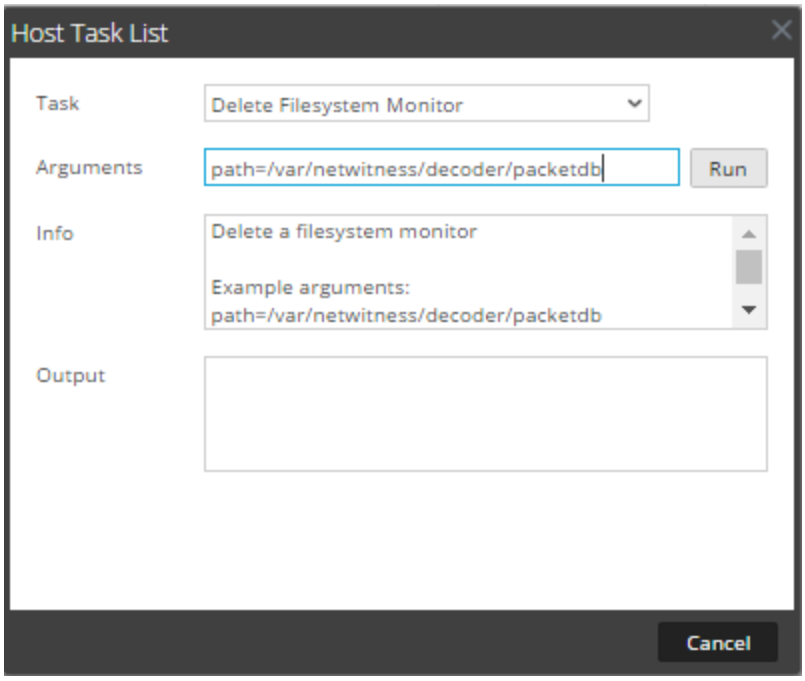
1. Select  **(Admin) > Services**.
2. In the **Services** list, select a service and click  **> View > System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Add Filesystem Monitor**.
   In the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



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

Delete a Filesystem Monitor

1. Select **(Admin) > Services**.
2. In the **Services** list, 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 **Delete Filesystem Monitor**.
   In the Info area, a brief explanation of the task and the task arguments is displayed.
5. To identify the filesystem to stop monitoring, type the path in the **Arguments** field. For example:
   `path=/var/netwitness/decoder/packetdb`



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

Reboot a Host

Under certain conditions, you must 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.

NetWitness Platform also offers other options for shutting down a host:

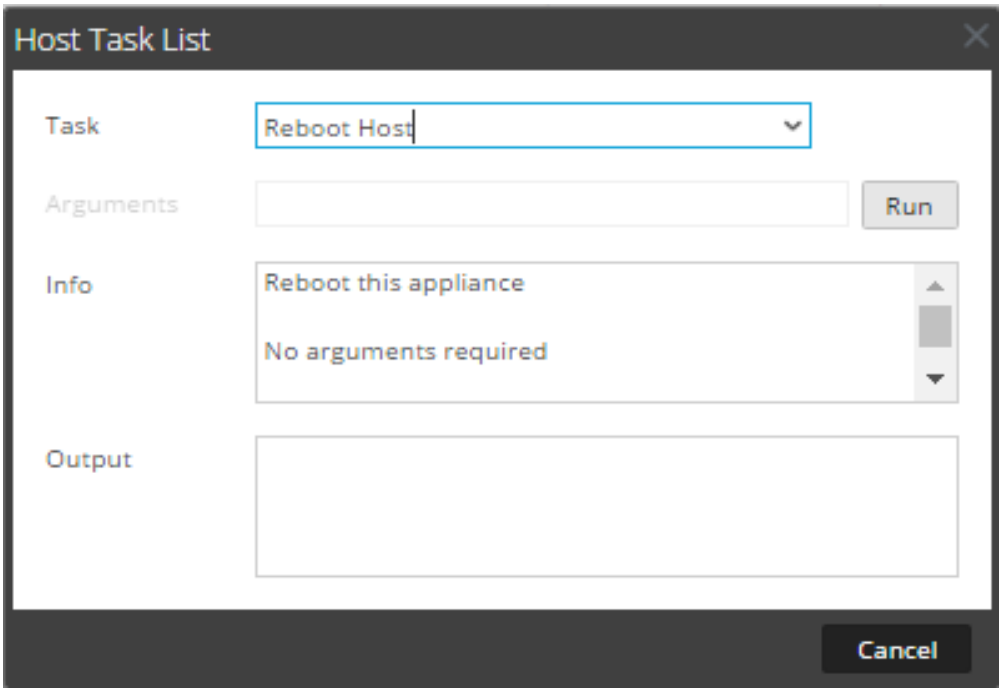
- To shut down and restart a host through an attached service, go to the Hosts view from a service in the Services view (see Search for Hosts) and then follow the Shut Down and Restart a Host from the Hosts View procedure below.
- To shut down the physical host without restarting, see Shut Down Host.

Shut Down and Restart a Host from the Hosts View

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

Shut Down and Restart a Host from the Host Task List

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



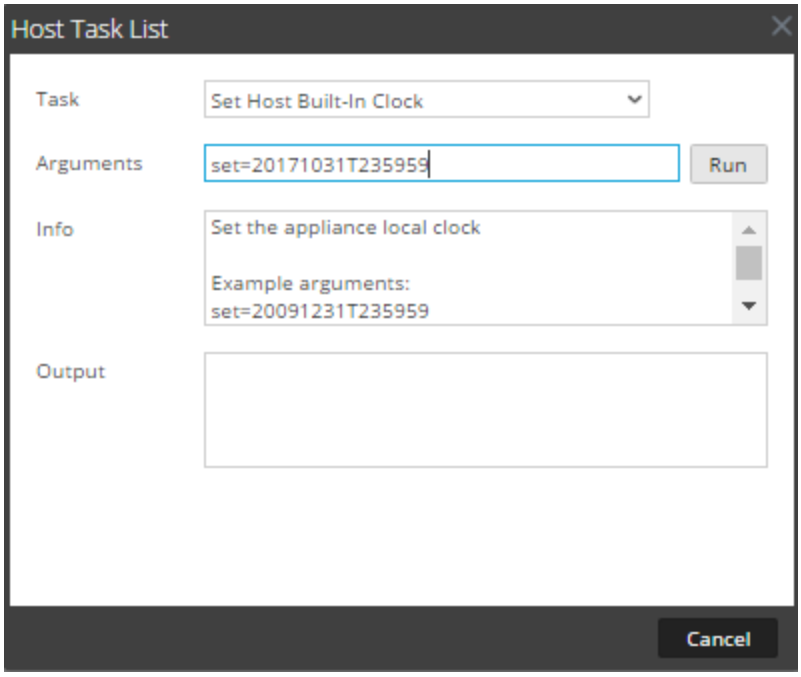
5. Click **Run**.
   The host is rebooted and the result is displayed in the Output area.

Set Host Built-In Clock

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

Set the Time on the Local Clock

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



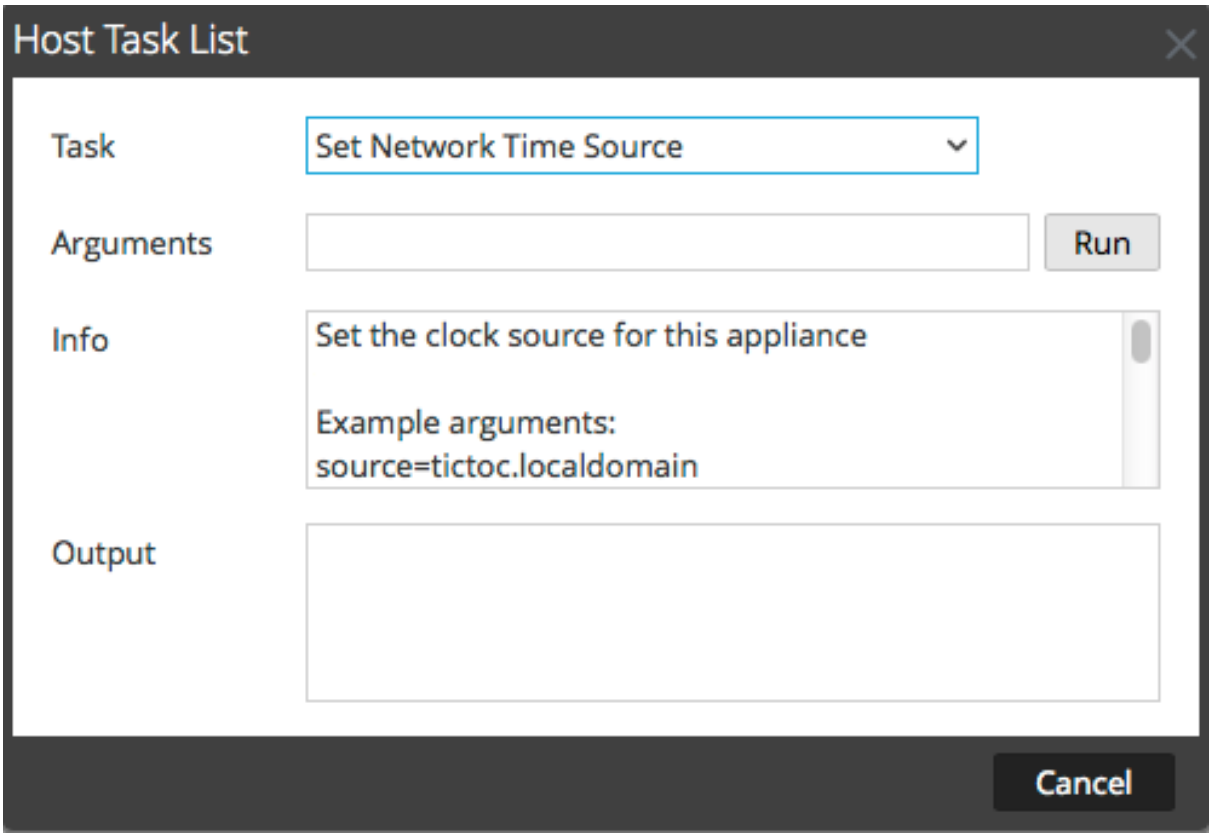
6. Click **Run**.
   The clock is set to the specified time and a message is displayed in the Output area.

Set Network Time Source

When setting the clock source for a host, set the hostname or address of an Network Time Protocol (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** list, select a service and click **> View > System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Set Network Time Source**.



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

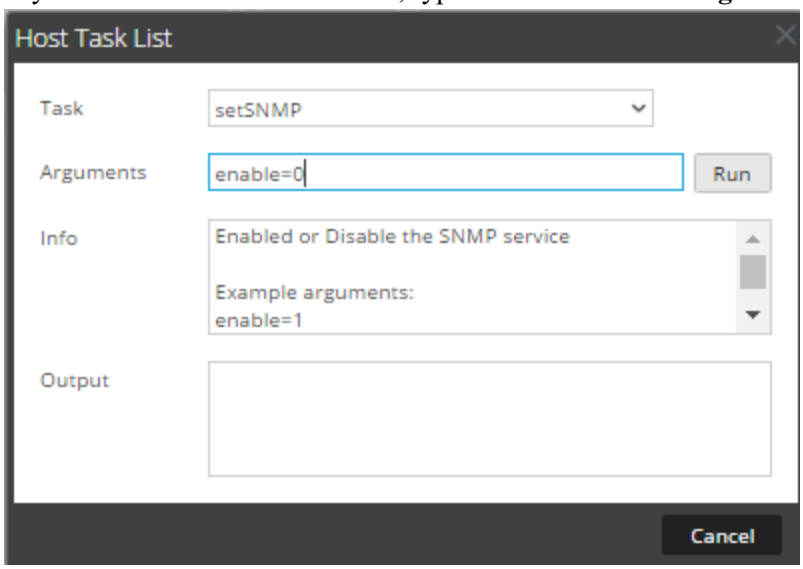
Note: If you specified a NTP clock source of **local**, the host clock serves as the clock source and the time is configured using Set Host Built-In Clock.

Set SNMP

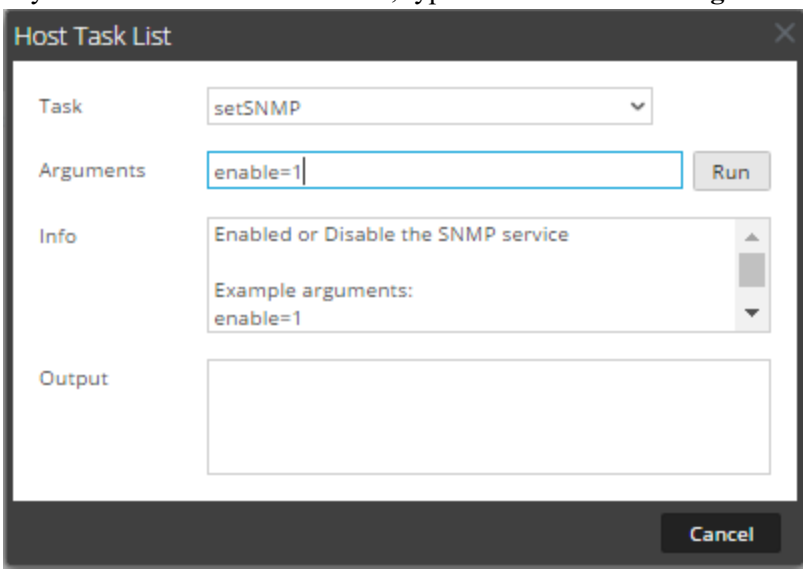
The Set SNMP task in the Host Task List enables or disables the SNMP service on a host. For a host to receive SNMP notifications, enable the SNMP service. If you are not using SNMP for NetWitness notifications, it is not necessary to enable the service.

Toggle SNMP Service on the Host

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



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



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

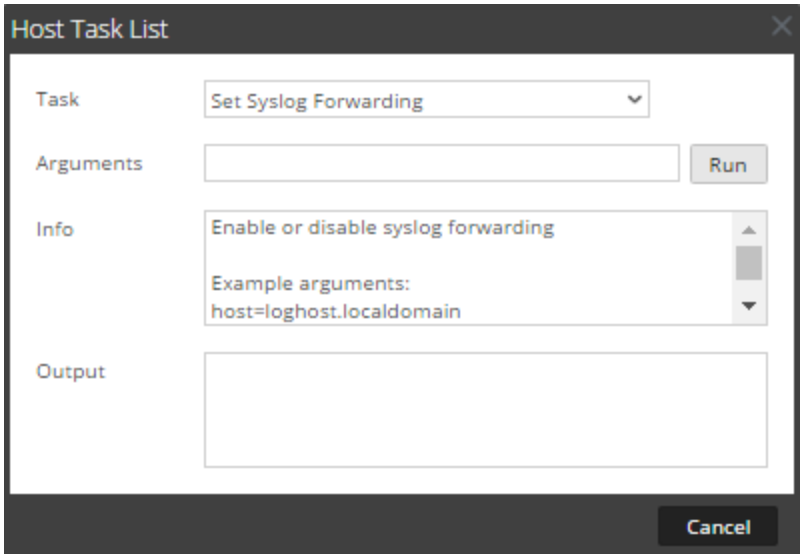
Set Syslog Forwarding

You can configure Syslog forwarding to forward the operating system logs of your NetWitness 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** list, select a service and click  **> View > System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.

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



5. In the **Arguments** field, do any one of the following.

   - To enable syslog forwarding, specify any one of the following formats:
     `host=<loghost>.<localdomain>` (for example, `host=syslogserver.local`).

     `host=<loghost>.<localdomain>:<port>` (for example, `host=syslogserver.local:514`).

     `host=<IP>` (for example, `host=10.31.244.244`).

     `host=<IP>:<port>` (for example, `host=10.31.244.244:514`).

     The following table lists the parameters used to enable syslog forwarding.

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.

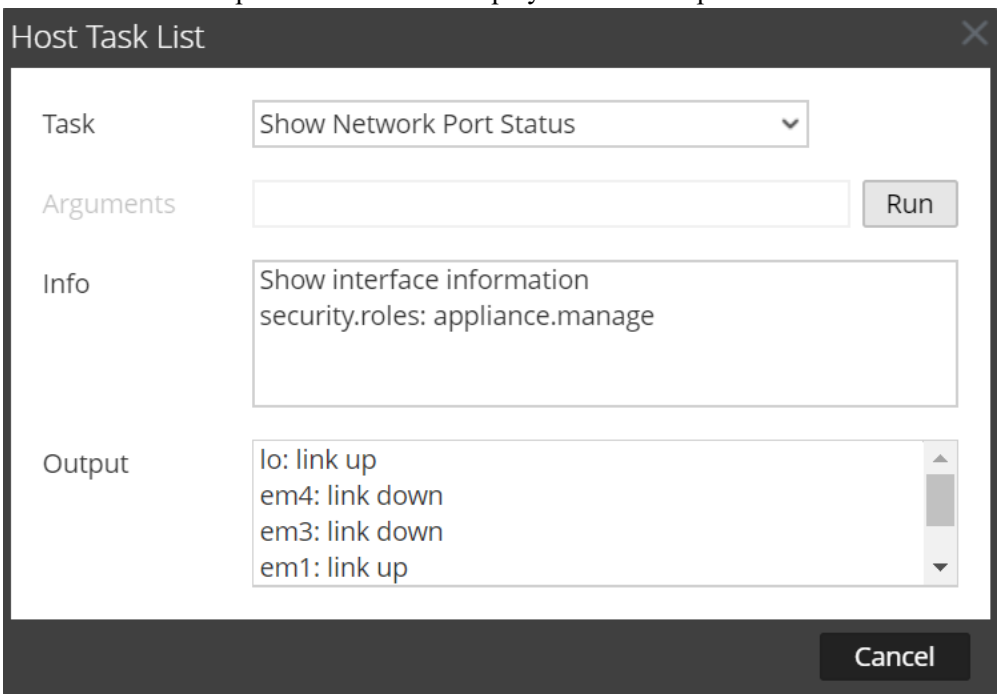
Note: You can now log in to the remote syslog server and verify if the messages are being received from the NetWitness services configured for syslog forwarding.

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** list, 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. No arguments are required for this task. Click **Run**.
   The status for each port on the host is displayed in the Output area.

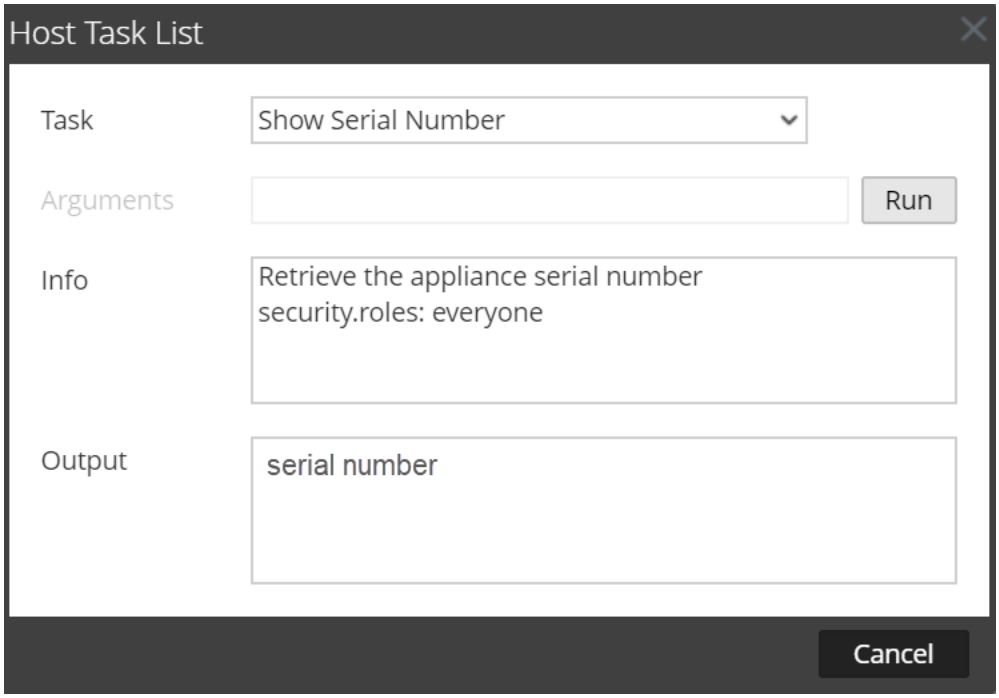


Show Serial Number

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

Show the Serial Number

1. Select **(Admin) > Services**.
2. In the **Services** list, select a service and click **> View> System**.
   The System view for the service is displayed.
3. In the **Services System** view toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Show Serial Number**.
   In the Info area, a brief explanation of the task and the task arguments is displayed.
5. No arguments are required for this task. Click **Run**.
   The serial number of the selected host is displayed in the Output area.



Shut Down Host

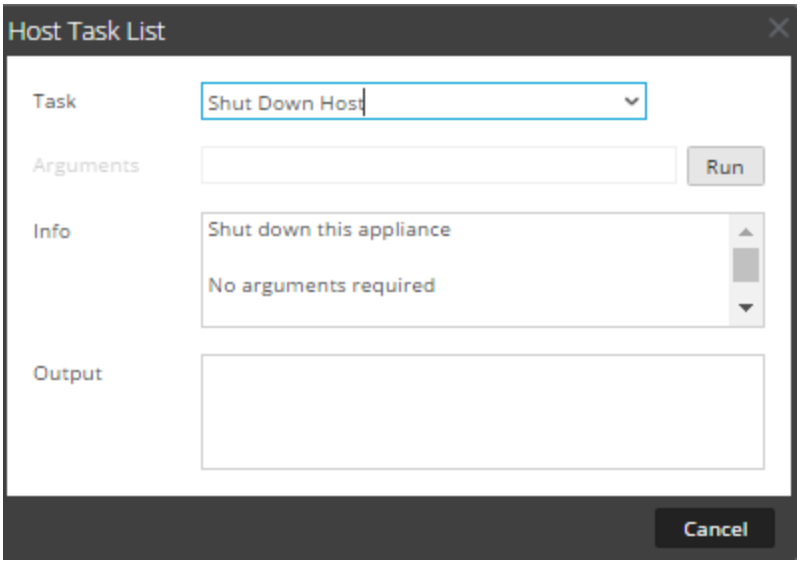
Under certain circumstances (for example, a hardware upgrade or an extended power outage that exceeds backup power capacity), it may be necessary to shut down a physical host. When you shut down a host, all services running on the host are stopped and the physical host turns off.

The physical host does not restart automatically. Use the power switch to restart the host. Once the physical host restarts, the host and services are configured to restart automatically.

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

Shut Down the Host

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



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

Stop and Start a Service on a Host

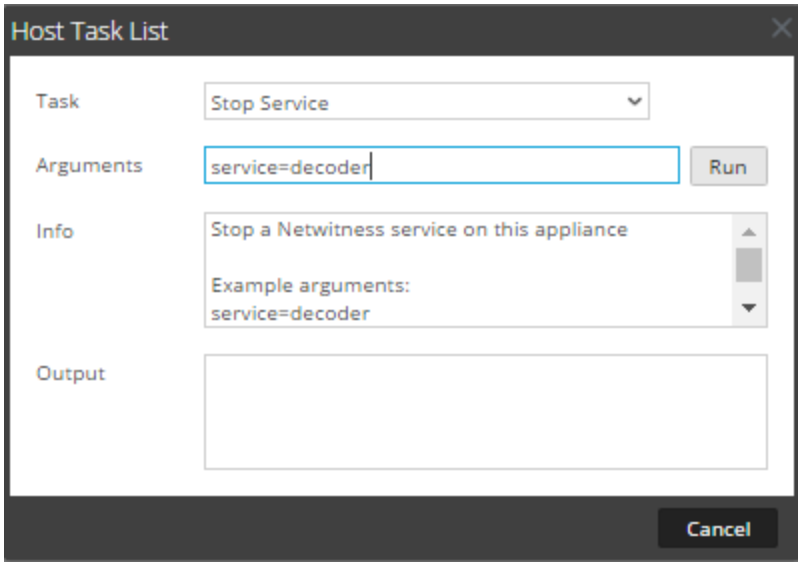
The Host Task List has two options for stopping and starting a service on a host. When you stop a service using the **Stop Service** message, all processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically.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

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

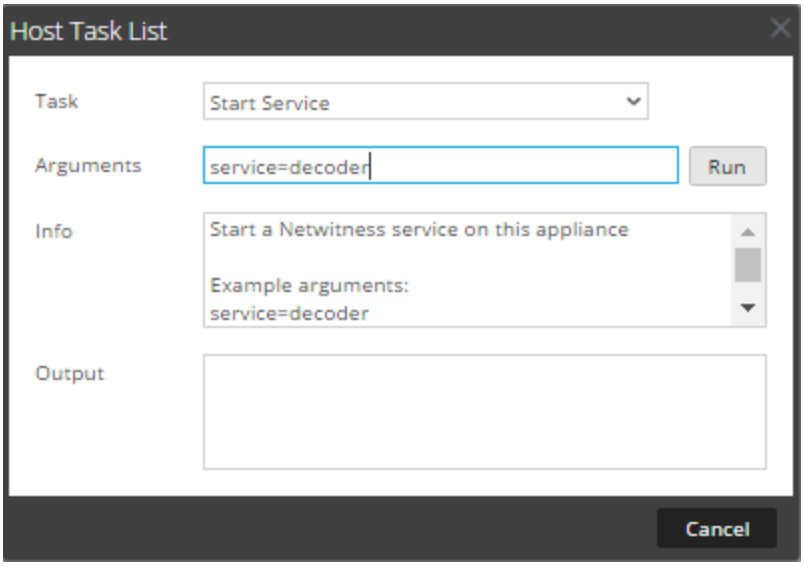


6. To execute the task, click **Run**.
   The service stops and the status is displayed in the Output area. All processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically.

Start a Service on a Host

1. Select **(Admin) > Services**.
2. In the **Services** list, 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 **Start Service**.
   The task is displayed in the Task field, and information about the task is displayed in the Info area.

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



6. To execute the task, click **Run**.
   The service 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" in *System Security and User Management Guide*.

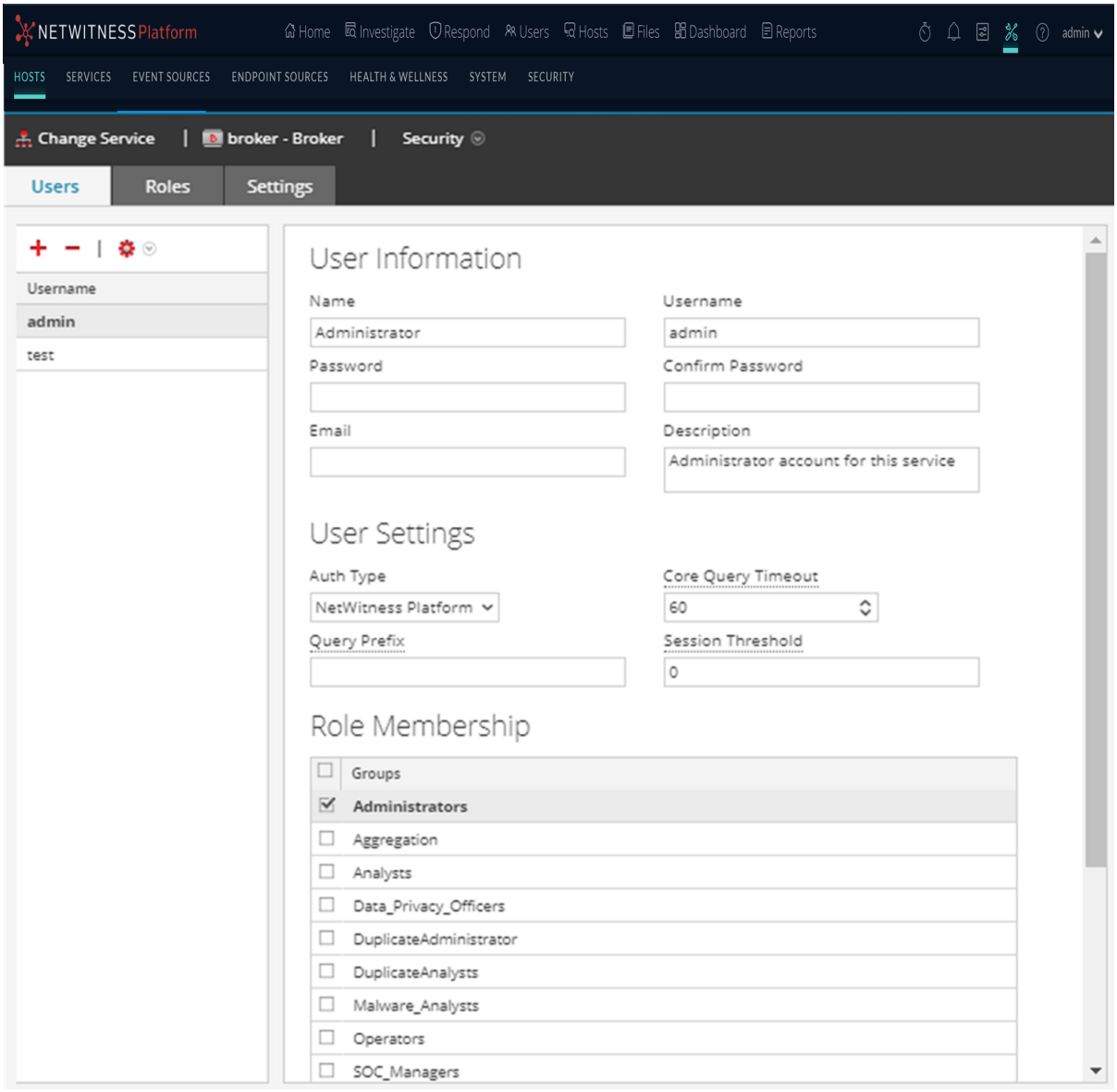
For each service user, you can:

- 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.

To navigate to the Services Security view:

1. In NetWitness, 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.



Add a Service User

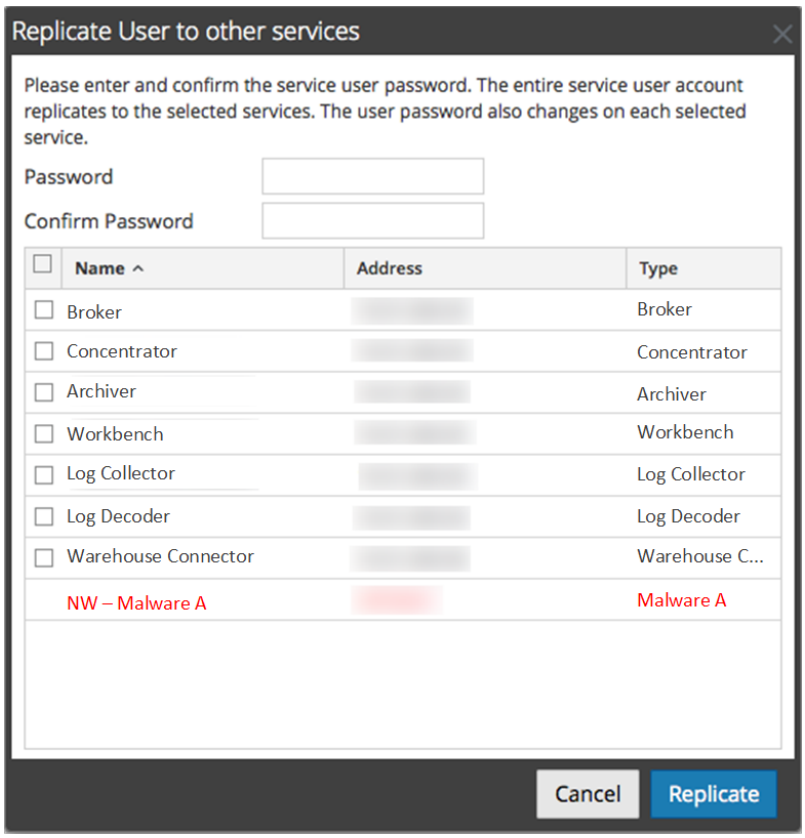
1. On the **Users** tab, click .
2. Type the user name to access the service, then press **Enter**.
   The User Information section displays the user name and the rest of the fields are available for editing.

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
   - **Email** address
   - **Description** of the user
5. In the User Settings section, select the following information:
   - **Authentication Type**
     - If NetWitness authenticates the user, select **NetWitness**.
     - If Active Directory or PAM is configured on NetWitness Server to authenticate the user, select **External**.
   - **Core Query Timeout** is the maximum number of minutes a user can run a query on the service. This field applies to NetWitness 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**.

Replicate a User to Other Services

Note: The **admin** user cannot be replicated to other services.

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



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

Delete a Service User

1. On the **Users** tab, select the **Username** and click −.
   NetWitness requests confirmation that you want to delete the selected user.
2. To confirm, click **Yes**.

Add a User Role to a Service

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

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to metadata and session content
Analysts	Access to metadata and session content but not to configurations

Role	Permission
SOC_Managers	Same access as Analysts and additional permissions to handle incidents
Malware_ Analysts	Access to malware events and to metadata and session content
Data_Privacy_ Officers	Access to metadata and session content and configuration options that manage obfuscation and viewing of sensitive data within the system (see *Data Privacy Management Guide*).

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

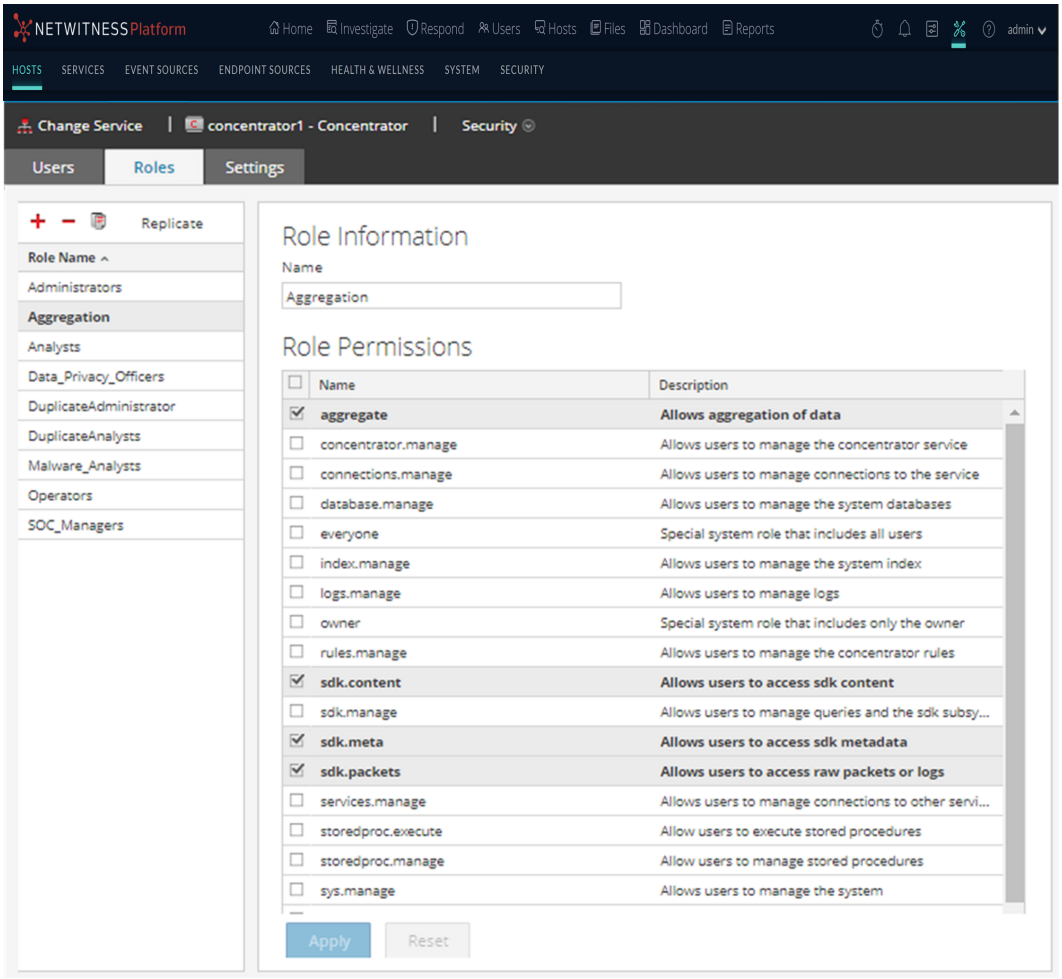
- **Service** user or users that requires a new set of permissions.
- **Custom role on NetWitness Server** because trusted connections require that the same custom role exists both on the server and on each service the custom role will access. The names must be identical. For example, if you add a Junior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

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

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

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

3. Select the **Roles** tab and click .
   The Services Security view is displayed and five pre-configured roles are already listed.



4. Click , type the **Role Name** and press **Enter**.
   The Role Name is displayed above a list of **Role Permissions**.
5. Select each permission the role will have on the service.
6. Click **Apply**.

You can add service users to the role in the **Users** tab.

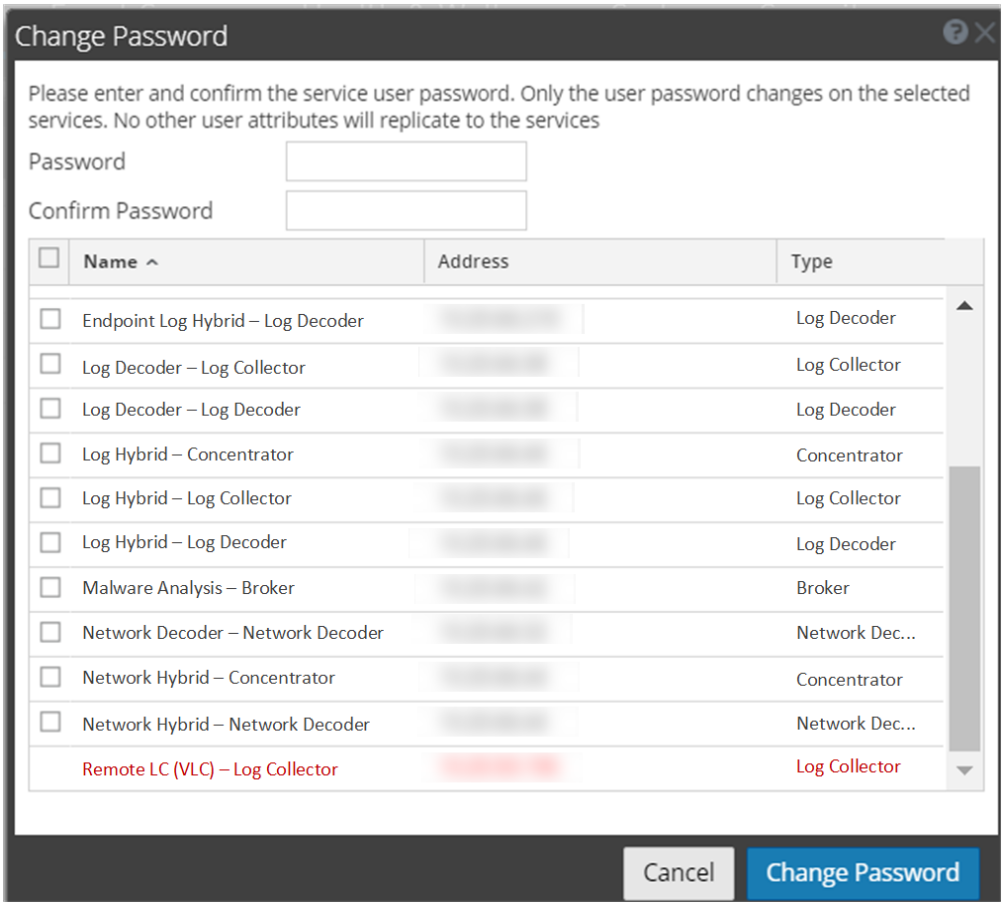
Change a Service User Password

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, go to **(Admin) > Services**.
   The Admin 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 **Change Password** dialog is displayed.



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

IMPORTANT: If you change the admin password on a NetWitness service that is used as a Reporting Engine data source, you must remove and then re-add the service as a data source. For details, see "Configure the Data Sources" topic in the *Reporting Engine Configuration Guide for NetWitness Platform 12.x Guide*.

Create and Manage Service Groups

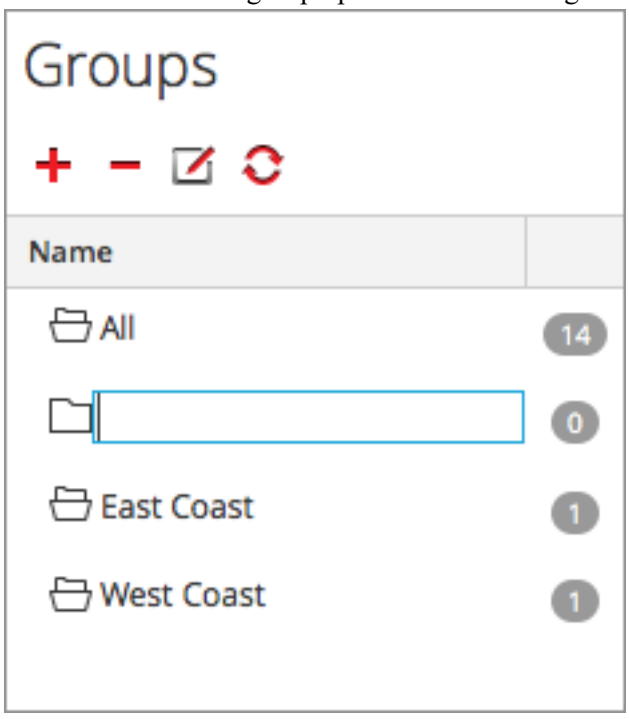
The Admin Services view provides options to create and manage groups of services. The Services list toolbar includes options to create, edit, and delete service groups. Once groups are created, you can drag individual services from the Services panel into a group.

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, Network Decoders, or Concentrators.
- Group services that are part of the same data flow; for example, a Broker, and all associated Concentrators and Network 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.

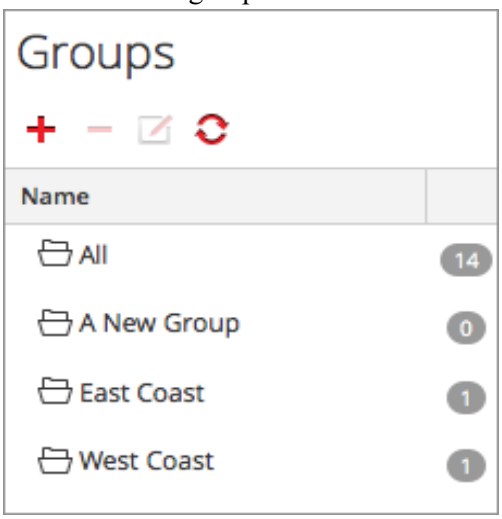
Create a Group

1. In NetWitness, go to  **(Admin) > Services**.
   The Admin 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.
The service is added to the group.

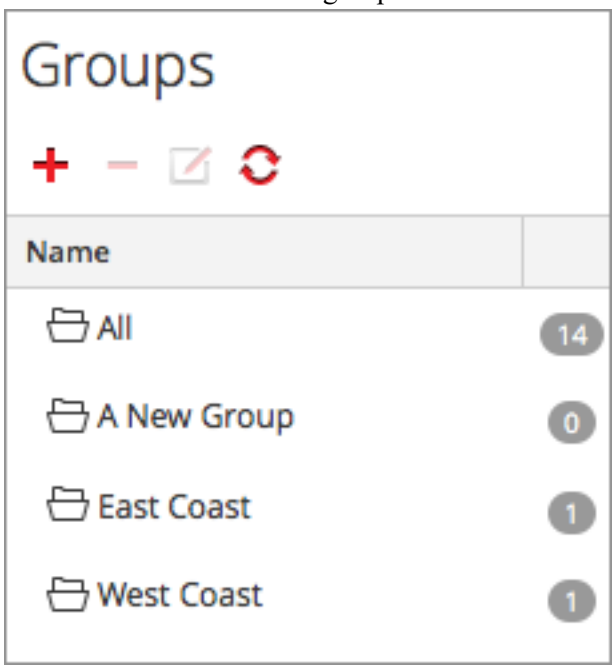
View the Services in a Group

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 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 are removed from the group.
   In the following example, the service group called **A New Group** does not contain any services, because the service in that group is 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 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.

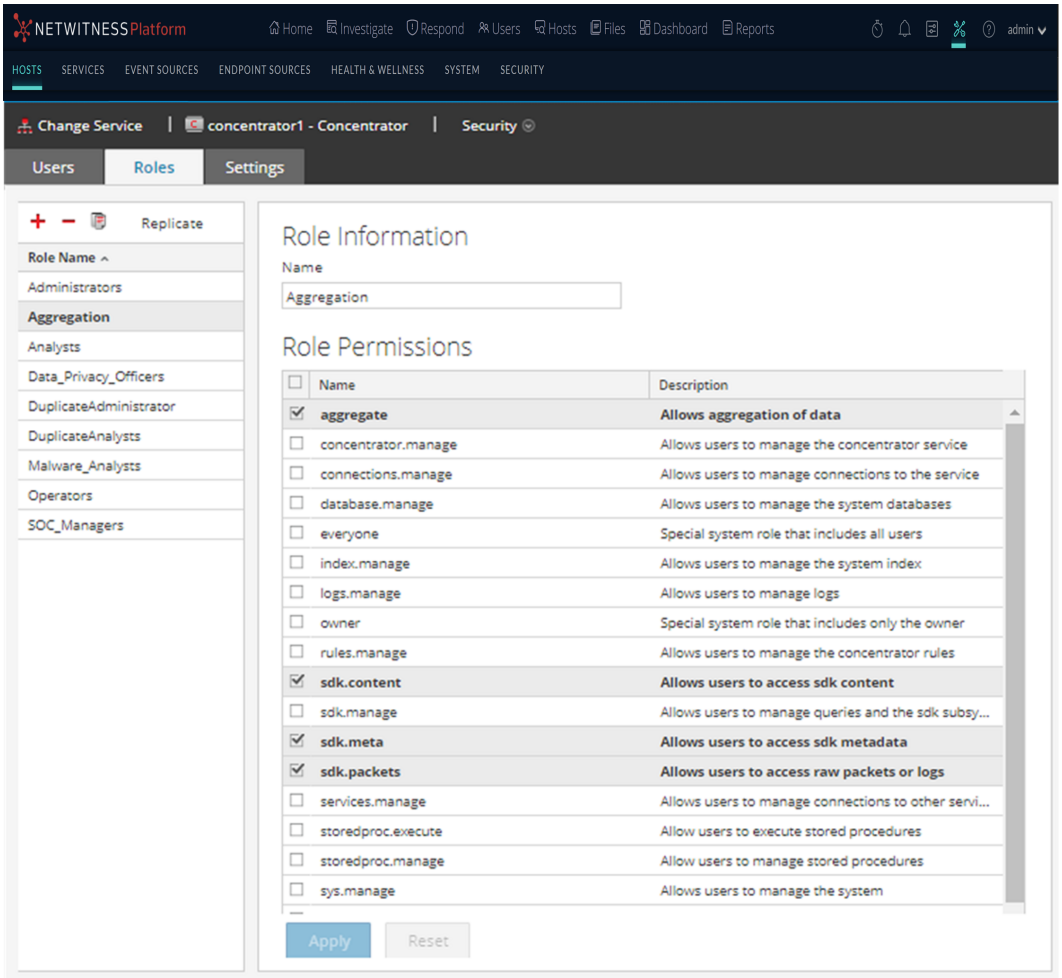
The quick way to add an existing role to other services is to replicate the role. For example, you could replicate the `JuniorAnalysts` role that exists on a Broker to a Concentrator and Log Decoder.

To navigate to the Services Security view:

1. In NetWitness, 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.

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**.

Edit Core Service Configuration Files

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

- View and edit a service configuration file that the NetWitness 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:

- The NetWitness file (`netwitness`). This is preconfigured and does not require editing.
- The service index file (`index-<service>`). This is preconfigured and may require editing.
  See Edit a Service Index File for more information.
- The scheduler file (`scheduler`). The scheduler service is optional and requires editing.
  See Configure the Task Scheduler for more information.
- The crash reporter file (`crashreporter`). The crash reporter service is optional and requires editing.
  See Enable the Crash Reporter Service for more information.
- The feed definitions file (`feed-definitions`). This file is optional and may require editing.
  See "Feed Definitions File" in the *Decoder Configuration Guide* for more information.

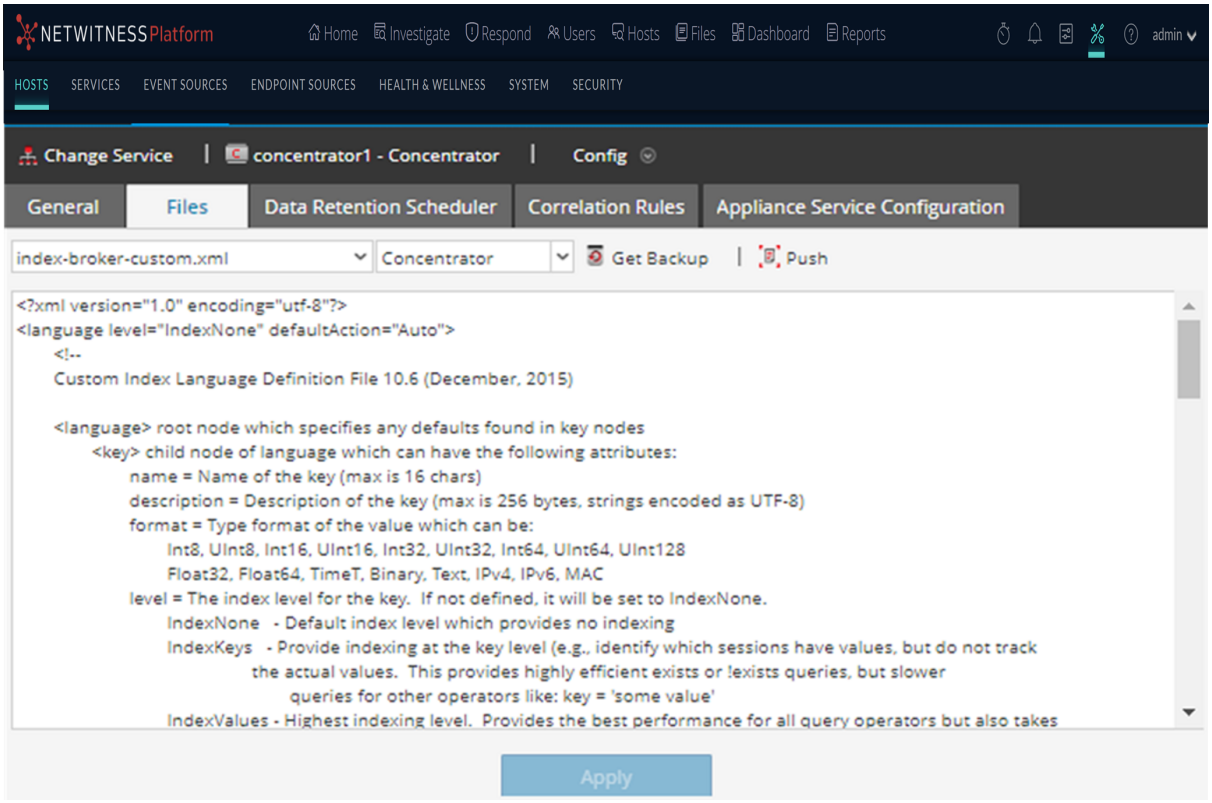
In addition, the Network Decoder has files that configure parsers, feed definitions, and a wireless LAN adapter. There is also the table mapping file provided by NetWitness, `table-map.xml`, which is an important part of the Log Decoder.

Note: The default values in these configuration files are 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.

Edit a Service Configuration File

To edit a file:

1. In NetWitness, go to **(Admin) > Services**.
2. In the Services list, select a service.
3. Select **> View > Config**.
   The Service Config view is displayed with the General tab open.
4. Click the **Files** tab.
   cThe 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.



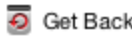
7. Edit the file and click **Apply**.

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

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

The configuration file is pushed to all selected services.

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 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 NetWitness 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-custom.xml`
- `index-decoder.xml`, and `index-decodereustom.xml`
- `index-logdecoder.xml`, and `index-logdecodereustom.xml`

- index-archiver.xml, and index-archiver-custom.xml
- index-workbench.xml, and index-workbench-custom.xml

Index and Custom Index Files

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

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

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

Some common applications for editing the index file are:

- To add new custom meta keys to add new fields to the NetWitness 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 Core database query performance as described in the *NetWitness Core Database Tuning Guide*.

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

Configure the Task Scheduler

Scheduler File

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

Scheduler Task Syntax

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

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

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

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

In each task line, these guidelines apply:

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

Task Line Parameters

The following task line parameters are accepted by the scheduler.

Syntax	Description
daysOfWeek: <string, optional, {enum-any:sun|mon|tue|wed|thu|fri|sat|all}>	The days of week to execute a task. The default value is all.
deleteOnFinish: <bool, optional>	Delete the task when it has successfully finished.
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 because service start, **0** = unlimited (default).

Messages

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

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

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

Sample Task Line

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

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

Enable the Crash Reporter Service

The Crash Reporter is an optional service for NetWitness 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 NetWitness for analysis. The results are forwarded to NetWitness Support for any further action.

The information package sent to NetWitness 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 Network Decoders, Concentrators, Brokers, and hosts.

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.
`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 to determine if the core is still being written.
`cyclewaittime=10`	Define the number of minutes to wait between search cycles

Setting	Description
`deletecores=1`	Specify if the Core files should be deleted after report. 0 = No 1 = Yes **Note:** Until the Core file is deleted, it is reported each time crashreporter is restarted.
`deletereportdir=1`	Specify if the report directory should be deleted after the report. Useful to view ore reports on box. 0 = No 1 = Yes **Note:** If not deleted, the directory will be included in each subsequent package.
`debug=1`	Specify whether debugging messages are turned on or off in the `crashreporter` logging output. 0 = No 1 = Yes
`posturl=https://www.netwitnesslive.com/crash...ter/submit.php`	Define the webserver post URL.
`postpackages=0`	Specify if the packages should be posted to the webserver. 0 = No 1 = Yes
`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:

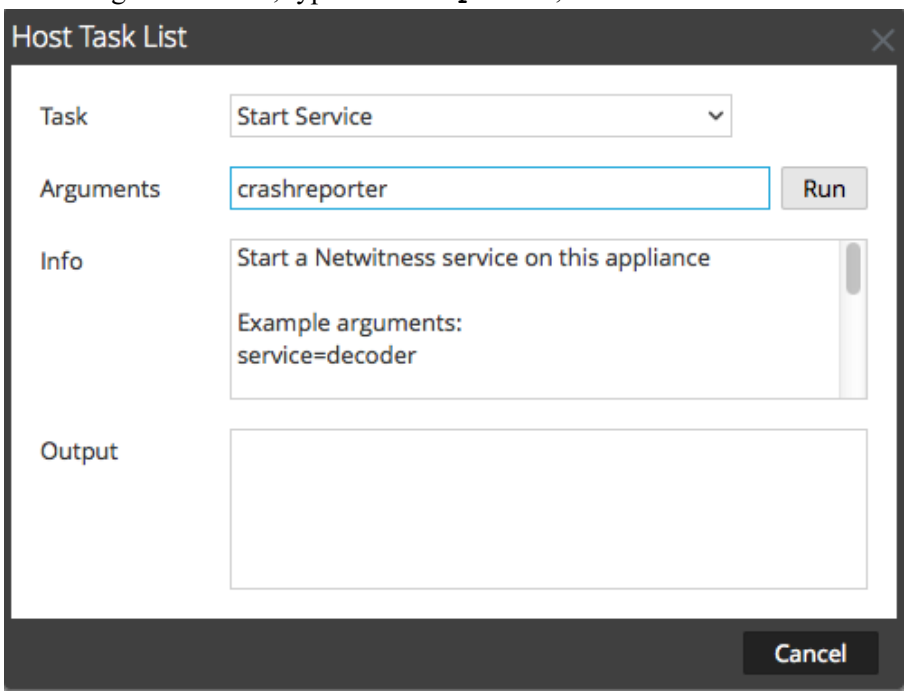
1. Select **(Admin) > Services**.
2. Select a service and click **> View > Config**.
3. Select the **Files** tab.
4. Edit `crashreporter.cfg`.

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 NetWitness, `table-map.xml`, is a very important 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`.

Note: 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 Services, which NetWitness updates as required. If you make changes to the `table-map.xml` file, they can be overwritten during a content or service upgrade.

The table map and custom table map files have two purposes:

- To translate the variables used in the Log Parsers to NetWitness meta key names
- To tell the system which keys to move onto the Concentrator.

For example, look at the out-of-the-box Palo Alto log parser, and examine one of its meta keys: `stransaddr`. This key represents the source translated address. If we look in the `table-map.xml`file we can see that this variable is listed as `Transient`:

```
<mapping envisionName="stransaddr" nwName="stransaddr" flags="Transient"
format="Text" />
```

Because this variable is listed as, `Transient`, it never moved to the Concentrator. In fact, if you look at all the metadata that we parse from that log in the Concentrator, it is not listed as an available key.

Assume we change the value in the `table-map-custom.xml`file to the following:

```
<mapping envisionName="stransaddr" nwName="stransaddr" flags="None"
format="Text" />
```

In this case, the key-value pair would get copied to the Concentrator, and from there you can choose whether or not to index it.

In the`table-map.xml`file, 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.

IMPORTANT: 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.

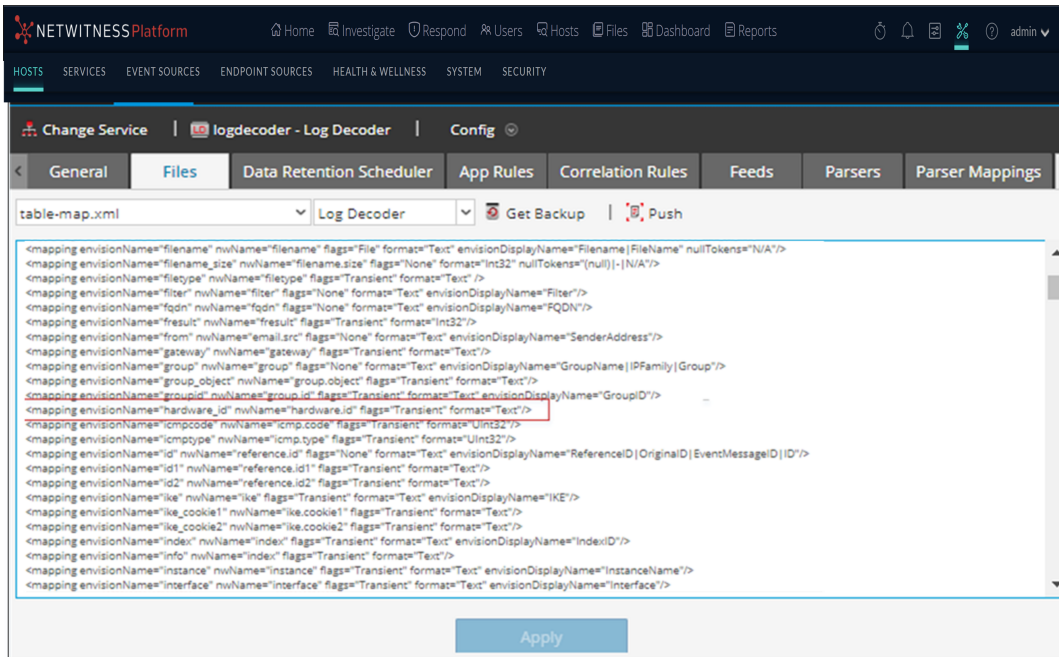
Prerequisites

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`.

To verify and update the table mapping file:

1. Go to  **(Admin) > Services**.
2. In the Services list, 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` file:
   `<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**.

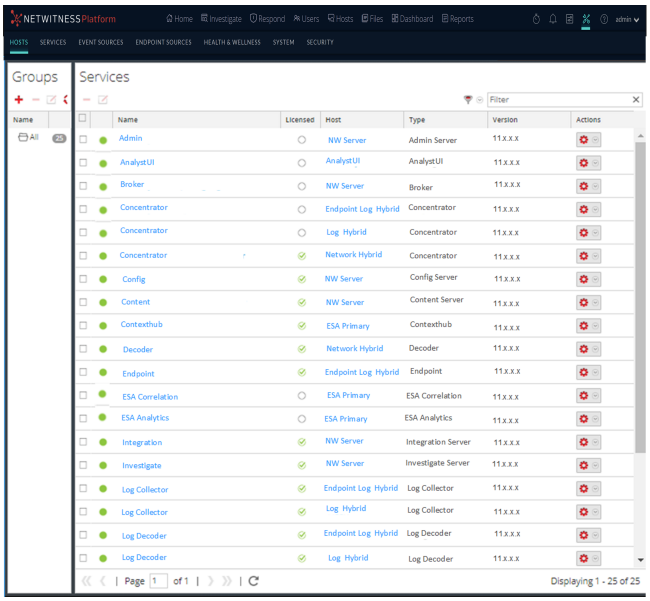
Caution: Before changing the table mapping files, carefully consider the effect of changing the index from `Transient` to `None` because it can impact the available storage and performance of the Log Decoder. For this reason, only certain meta keys are indexed out-of-the-box. Use the `table-map-custom.xml` 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 deleting a service that you no longer need.

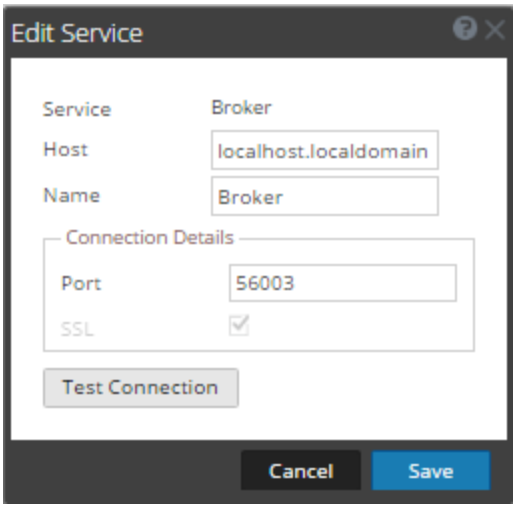
Each of the following procedures starts in the Services view.

To navigate to the Services view, in NetWitness, go to **(Admin) > Services**.



Edit a Service

1. In the Services view, select a service and either 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.
   - **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. Click **Save**.

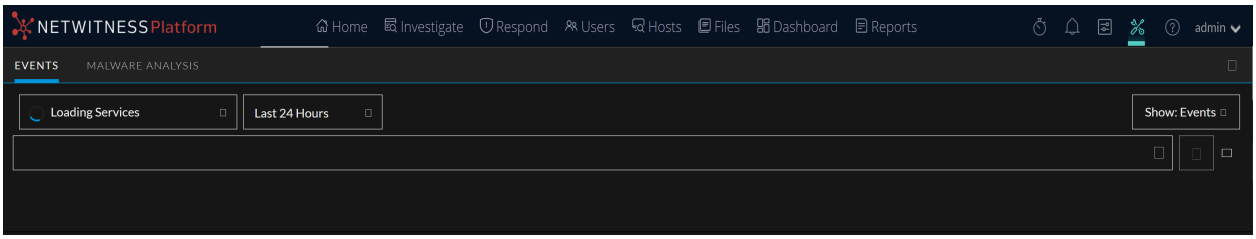
Delete a Service

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

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

Edit Service Hierarchy Timeout Settings

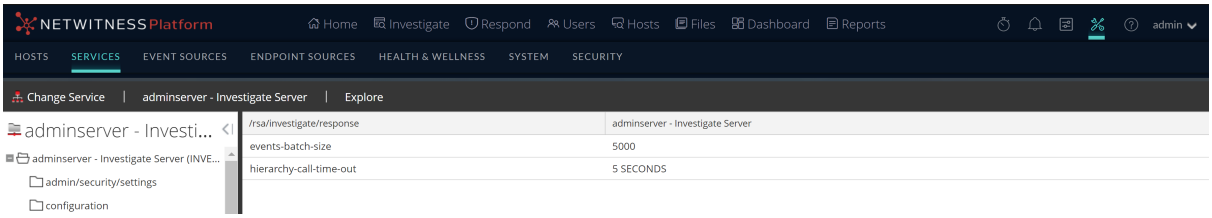
The **Investigate** > **Events** page may take longer than expected to load if the list of services to load has Core hosts that are switched off adversely. In such scenarios, NetWitness Platform users can customize the hierarchy-call-time-out parameter. This customization will allow the Services to load quickly before the request is timed out. The default value is 5 seconds.



To reduce the Service Hierarchy Timeout:

1. In NetWitness Platform, select **(Admin) > Services** > **Investigate Server** > **Explore** > **Investigate/response**.
2. In the **hierarchy-call-time-out** field, provide the time in seconds. The default time is set to 5 seconds. The time taken to load service hierarchy from Core Services will be a factor of customized ***hierarchy-call-time-out*** times the ***number of offline/in-accessible services***.

Note: The duration it takes for NetWitness Platform to load Services is the result of the total time it takes to communicate with all services present in a deployment. This load time may vary due to several factors, such as inaccessible services, stale connections, or incorrect host connection status in the cache due to a host being improperly switched off.



Explore and Edit Service Property Tree

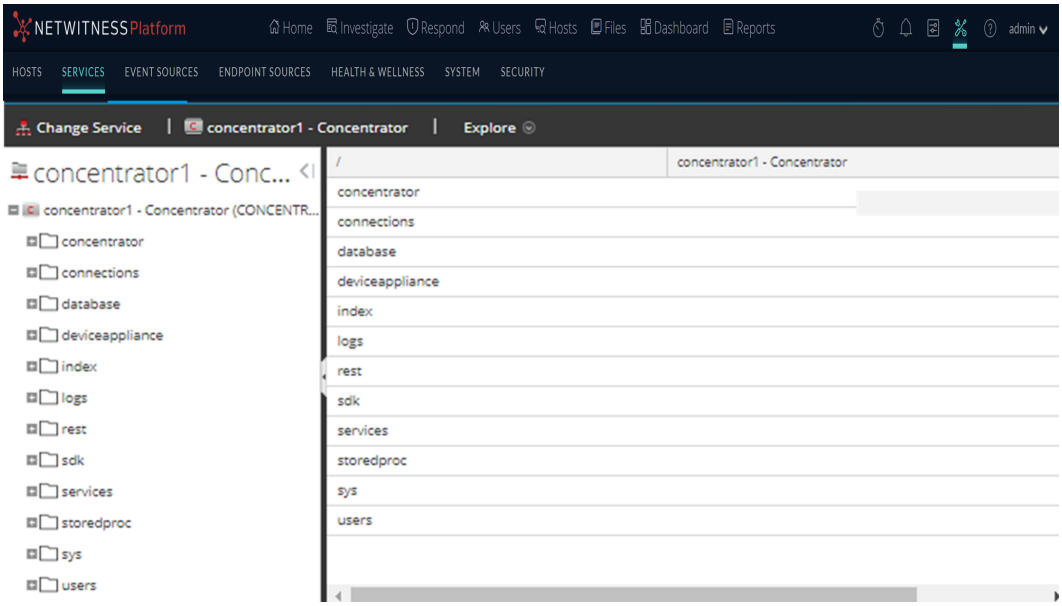
You have advanced access and control of service functionality in the Services Explore view, which consists of two parts. The Node list displays service functionality in a tree structure of folders. The Monitor panel displays properties of the folder or file selected in the Nodes list.

Each of the following procedures starts in the Explore view.

To navigate to the Explore view:

1. In NetWitness, 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.



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

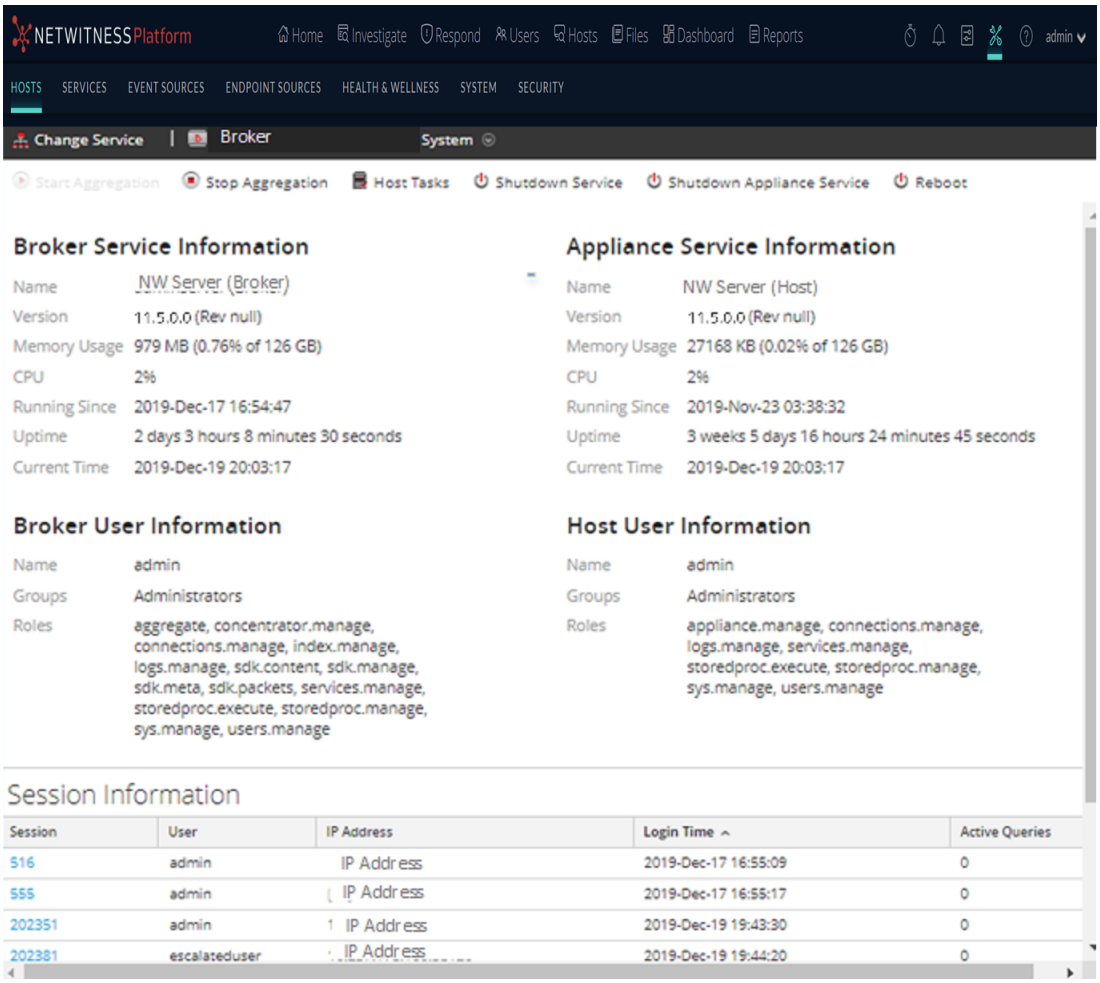
1. In the Properties dialog, select a message type from the drop-down list. Options vary according to the file selected in the Node list.
   A description of the selected message type is displayed in the **Message Help** field.
2. (Optional) If the message requires them, type the **Parameters**.
3. Click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

Terminate 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 terminate the session and the active queries in a session.

Terminate a Session on a Service

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



3. In the **Session Information** list at the bottom, click a session number from the Session column.

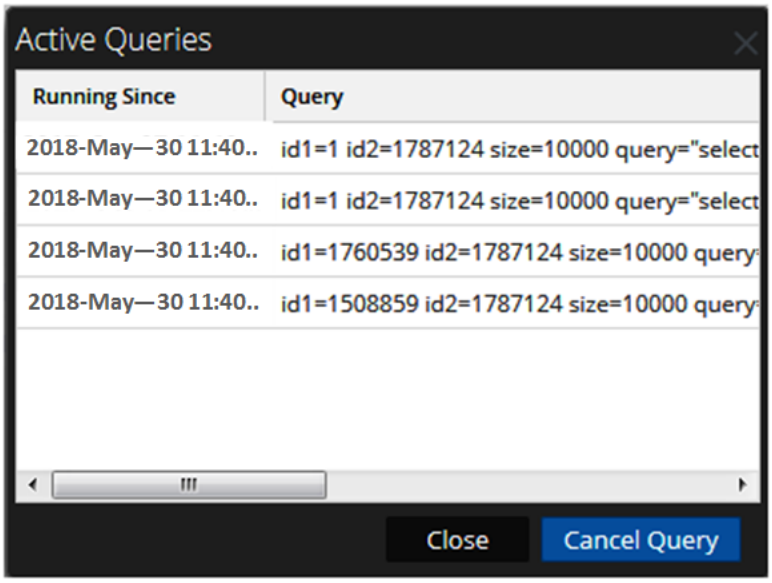
   The confirmation dialog is displayed.

4. Click **Yes**.

Terminate an Active Query in a Session

1. Scroll down to the **Sessions** list.
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**.

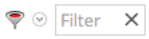
   The query stops and the Active Queries column is updated.

Search for Services

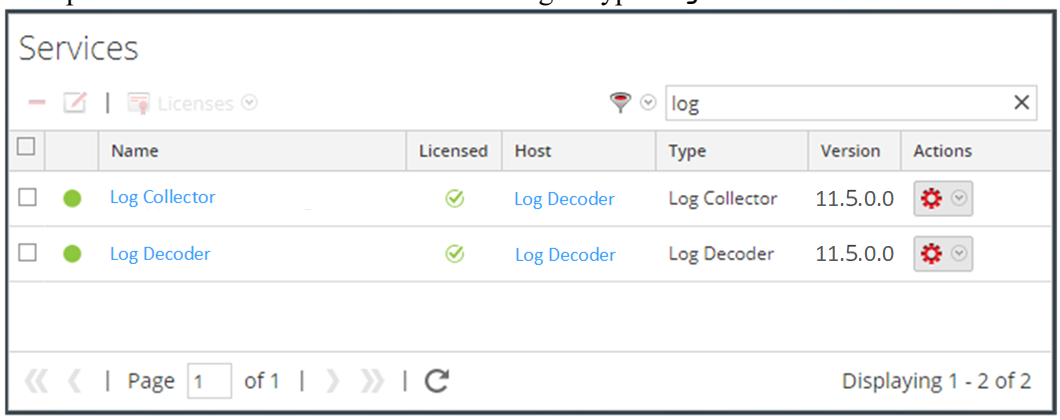
You can search for services from the list of services in the Services view. The Services view enables you to quickly filter the list of services by Name, Host, and Service Type. You can use the Filter drop-down menu and the Filter field separately or at the same time to filter the Services view.

Search for a Service

1. In NetWitness, go to **(Admin) > Services**.
2. In the **Services** list toolbar, type a service **Name**, **Host**, or service **Type** in the **Filter** field.

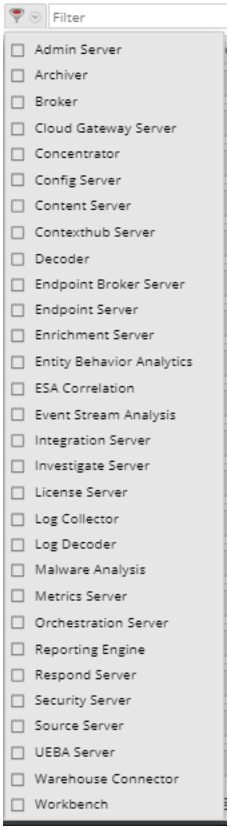
   

   The Services panel lists the services that match the names entered in the Filter field. The following example shows the search results after starting to type **log** in the filter field.

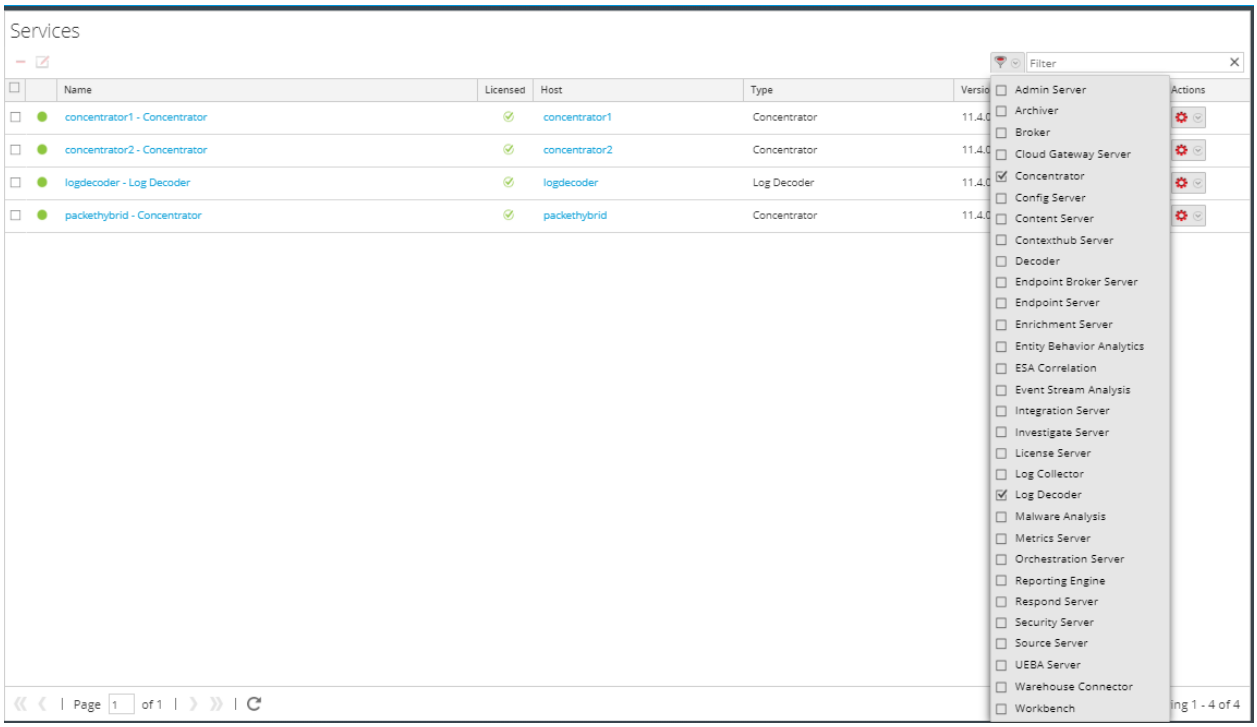


Filter Services by Type

1. In NetWitness, go to **(Admin) > Services**.
2. In the Services view, click and select the service types that you want 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.



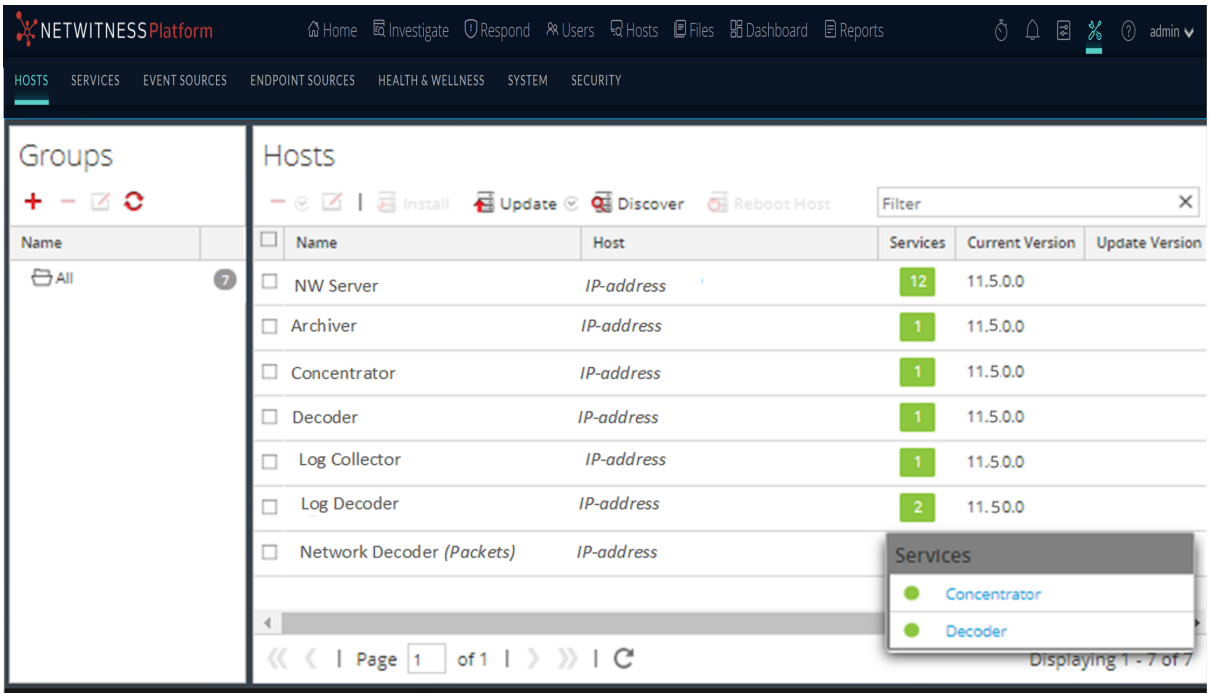
Find the Services on a Host

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, 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 two services on the selected host are listed after clicking the box containing the number 2.



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, go to **(Admin) > Services**.

Start a Service

1. 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 displays a message.

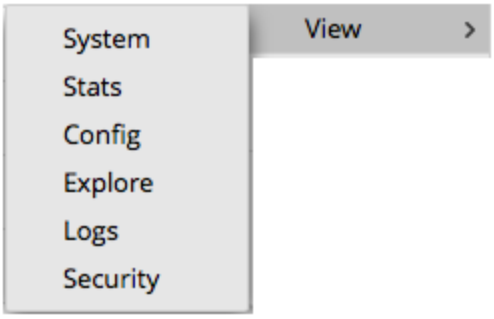
To restart a service:

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

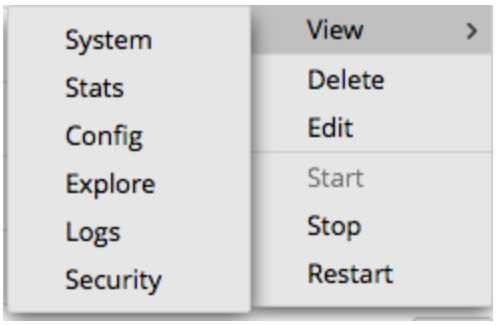
Each view displays a functional piece of a service and is described in detail in its own section:

- Services System View shows a summary of service, appliance service, service user, host user, 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 NetWitness Platform Core user accounts for aggregation, thick client users, and REST API users.

Access a Service View

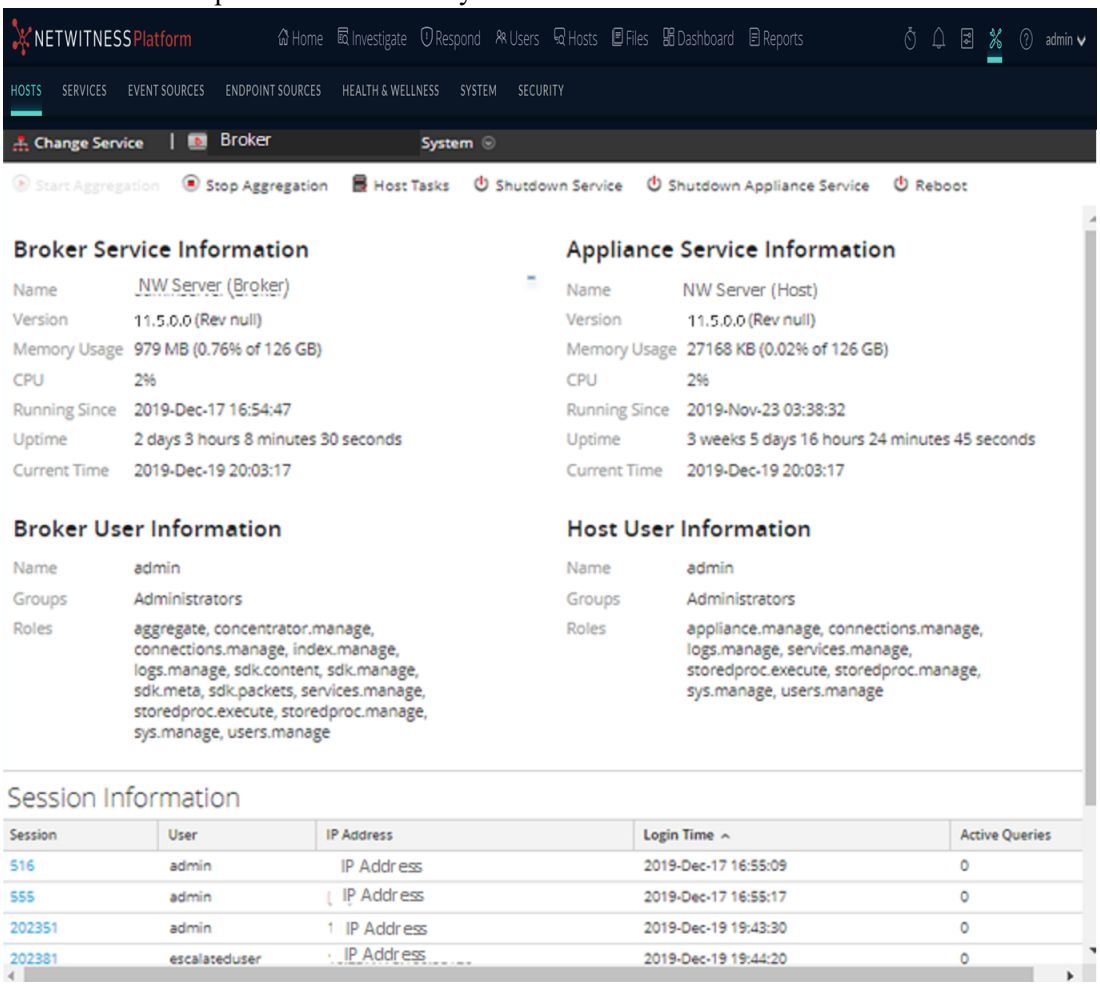
To access a view for a service:

1. In NetWitness, go to **(Admin) > Services**.
2. Select a service and click > **View**.
   The View menu is displayed.

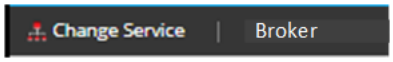


3. From the options on the left, select a view.

   Below is an example of the Services System view for a Broker.



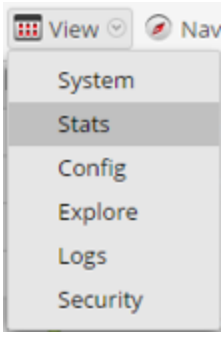
4. Use the toolbar to navigate:



   a. Click **Change Service** to select another service.
      The Administrate Service dialog is displayed.

   b. Select the checkbox to the left of the service that you want.

c. Select the view that you want for the service you selected in the View drop-down list.



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

View Topology Details

Note: This feature is supported in 11.7 and later.

Note: To view the **Service Topology Tab**, you must ensure this feature is enabled under **Admin Server** > **Explorer** > **Feature**> **service-topology-feature**.

Administrators and analysts can view all the NetWitness core services in a hierarchical layout depicting the collection and aggregation of the services in your deployment. This visualization displays the topology for Broker, Concentrator, Log Decoder, Packet Decoder, Hybrids, ESA and Log Collector and provides insights on which:

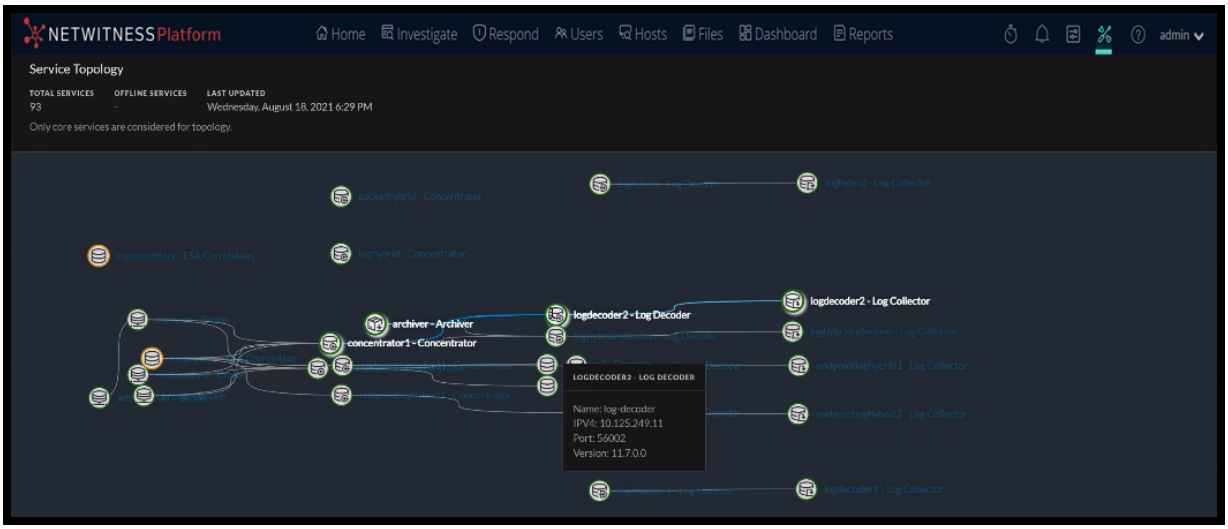
- Broker aggregates from the Concentrators.
- Concentrator aggregates from the Log Decoders.
- Log Decoder receives data from the Log Collectors.
- Log Collector sending data to other Log Collectors and vice-veNetWitness and the direction of the data flow.

Note: Services such as Reporting Engine, Malware Analysis, UEBA, Endpoint Server, Cloud Link Service, and Warehouse connector are not supported.

The topology is automatically refreshed once in 3 hours. You can click on any node to view the details.

To view the Topology:

1. Click > **Service Topology.**
2. Do one of the following:
   - Scroll horizontally to view the complete topology.
   - Click **Search** and enter the service name to locate a specific service. The specific service will be highlighted in blue color in the hierarchical layout.
3. Click on the node to view the details.
   For more information, see Services Topology View topic.



Centralized Service Configuration via Policy

Note: The information in this section applies to NetWitness Platform Version 11.7 and Later.

Centralized Service Configuration allows you to manage the configuration of services in your environment efficiently. The Decoder, Concentrator, and Log Decoder deployed in your environment may be large in number and geographically distributed. Managing common configurations across the services can be time consuming. With Centralized Service Configuration, you can centrally create a policy of common configuration settings and apply the policy to a set of groups.

Groups

A group is a set of services based on the service type Decoder, Concentrator, and Log Decoder. You can create a group and assign policy to it based on your requirement. For example, group all the 10G Decoder services or group services within a geographical area. For more information on creating groups, see Creating Groups and Policies.

Policies

A Policy is a set of service configurations that you can apply to a set of groups. This allows you to efficiently manage the service settings. Once you create a customized policy, you can assign it to a group.

Benefits of Centralized Service Configuration

- Apply customized settings in one step to any number of services
- Centrally restart all services within a group (when needed) to apply changes
- Indicates when an action is required, such as service restart, failed publication, or Out of Compliance services
- Clone policy to quickly create similar policies with minor changes

- Quickly revert changes to a policy in case of issues
- Groups of the same service type can be created based on similar hardware profiles or other criteria
- Add configuration items to policies in order to customize settings. Any settings which are not in the policy will be left as default
- (For version 11.7.1 and Later) Reconfigure 10G Network Decoders from the Policy UI. Administrators can quickly create 10G policies for each Decoder group based on the hardware profile
- (For version 11.7.1 and Later) Clone policy from an existing service, to save policy transition time for existing users

Creating Groups and Policies

Create a Group

You can create a group with one or more services and assign one policy to it. Atleast one service is required to publish a group.

To create a group:

1. Go to  (**CONFIGURE**) > **Policies**.
2. In the left panel, click **Groups**.
3. In the tool bar, click  .
4. In the New Group panel, do the following:
   - Enter the name of the group.
   - Enter a description for the group.
   - Select the type of service for the group.
5. Click **Next**.
6. In the Define Group, click  to assign services to the group.

Note: A service is disabled if it is assigned to another group.

7. Click **Next**.
8. In the Assign Policies, click  to assign one policy to a group. Make sure that the policy and group is of same service type.
9. Do any one of the following:
   - Click **Save and Publish** to save and publish the policy.

     The Publish and Restart Services dialog is displayed only if some settings require a service restart for the changes to take effect. In the Publish and Restart Services dialog, do any one of the following:

- To publish and restart the services immediately, click **Publish & Restart**.
- To publish and restart the services later, click **Publish & Restart Later**. In this case you must restart the services manually.
- To cancel the restart dialog, click **Cancel**.

The settings that do not require restart will be applied immediately.

- Click **Save and Close** to save the settings.

Create a Policy

You can create a policy and assign it to one or more groups.

To create a policy:

1. Go to **(CONFIGURE)** > **Policies**.
2. Click **Policies**.
   The available policies are displayed.
3. Click + Create New to add a new policy.
4. In the New Policy panel, do the following:
   - Select the policy type from the drop-down list.
   - Enter a unique policy name.
   - Enter a description for the policy.
   - Select the service type for the policy from the drop-down list.
   - (For version 11.7.1 and Later) Select the service from which you want to clone the settings.
5. Click **Next**.
6. Do any one of the following:
   - Customize the settings for the policy based on your requirement, for example, in the Database setting, click and change the Policy value to sha256 or change the byte range to 10 MB.

     Note: (For version 11.7.1 and Later) If you have preferred to clone from existing service, the setting values are populated automatically from the selected service on customize settings section. You can also add or modify the settings based on your requirement.
   - (For version 11.7.1 and Later) To configure 10g Settings:
     - Click **10g Settings**.
     - Select the Decoder service to fetch the settings.
     - Click **Done**.
7. In the Group List, click to assign groups to the policy. The policy and group should be of same service type.

Note: A group is disabled if another policy of the same type is already assigned to this group.

8. Do any one of the following:
   - Click **Save and Publish** to save and publish the policy.

     The Publish and Restart Services dialog is displayed only if some settings require a service restart for the changes to take effect. In the Publish and Restart Services dialog, do any one of the following:

     - To publish and restart the services immediately, click **Publish & Restart Now**.
     - To publish and restart the services later, click **Publish & Restart Later**. In this case you must restart the services manually.
     - To cancel the restart dialog, click **Cancel**.

     The settings that do not require restart will be applied immediately.
   - Click **Save and Close** to save and return to the Policies view.

Managing Groups and Policies

View a Group

To view properties of the selected group:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Groups**. The available groups are displayed.
3. Click a row to view details about the selected group in the right panel.

Delete a group

You can delete one or more groups. Once a group is deleted, the services and policies in the group will no longer displays the deleted group details.

To delete a group:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Groups**. The available groups are displayed.
3. Select one or more groups and click **Delete**.

The confirmation message is displayed.

Edit a Group

You can edit the properties of the group at any point in time. The service type cannot be edited. The status of the updated group is unpublished if you change the service or policies in a group. If you just change the group name and description the status remains published (if it is already published).

To edit a group:

1. Go to (**CONFIGURE**) > **Policies**.
2. Click **Groups**. The available groups are displayed.
3. Select a group and click **Edit**.

Note: You cannot edit the service type.

4. Make the required changes in the group.
5. Do any one of the following:
   - Click **Save and Publish** to save and publish the policy.
     The policy will be listed under the published category.
   - Click **Save and Close** to save the settings and return to the Groups view.

Filter Groups

The Filters Panel allows you to filter the list of displayed groups, based on the service type:

- Decoder
- Log Decoder
- Concentrator

Additionally, you can filter based on publication status or service status:

- **Published**: Groups that are published.
- **Unpublished**: Groups that are saved but not published.
- **Failed**: Groups that are failed to publish.
- **N/A**: Groups for which publication status is not applicable.
- **Service Require Restart**: The services associated with the group that require restart.

The Filters panel can be hidden or displayed:

- To display if hidden, click in the toolbar.
- To hide, click at the top-right of the panel.

Delete a Policy

To delete a policy:

1. Go to (**CONFIGURE**) > **Policies**.
2. Click **Policies**. The available policies are displayed.
3. Select one or more policies and in the **More Actions** drop-down list in the tool bar, click **Delete**.

The delete dialog is displayed.

Note: The services associated with this policy still require a restart if the restart is pending.

4. Click **Delete** to permanently delete the selected policies.

The deletion will take effect immediately.

Revert a Policy

You can revert a policy to the previously published version for a maximum of 5 times. Once a policy is reverted you cannot get back to the newer version and you must publish a policy.

Note: The revert is disabled if there is no previously published version.

To revert a policy:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Policies**. The available policies are displayed.
3. Select a policy and in the **More Actions** drop-down list in the tool bar, click **Revert**.
   All changes made to policy will be discarded and reverted to the previously published version. You must publish the policy once it is reverted.

Note: If there are any missing settings in the previously published version, then a default value is set for those settings.

Clone a Policy

You can clone only one policy at a time. Once cloned, all the settings from the old policy is copied to the new policy.

To clone a policy:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Policies**. The available policies are displayed.
3. Select a policy to clone and in the More actions drop-down list in the tool bar, click **Clone**.

The policy is cloned successfully.

Edit a Policy

You can edit the settings of the policies. The service type and policy type cannot be edited. Once the policy is edited the changes in the policy is reflected upon saving the policy. The updated settings are applied to the service if published.

After saving and before publishing the publication status of the changed policy is set to Unpublished if any settings is changed.

To edit a policy:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Policies**. The available policies are displayed.

3. Select a policy and click **Edit**.
4. Make the required changes in policy.

Note: You cannot edit service type and policy type.

5. Do any one of the following:
   - Click **Save and Publish** to save and publish the policy.
     The policy will be listed under the published category.
   - Click **Save and Close** to save the settings and return to the Policies view.

View a Policy

To view a policy:

1. Go to  (**CONFIGURE**) > **Policies**.
2. Click **Policies**. The available policies are displayed.
3. Click a row to view details about the selected policy in the right panel.

Filter Policies

The Filters Panel allows you to filter the list of displayed policies, based on the policy status and service type:

- **Published**: Policies that are published.
- **Unpublished**: Policies that are saved but not published.
- **Failed**: Policies that are failed to publish.
- **N/A**: Policies for which publication status is not applicable.

The Filters panel can be hidden or displayed:

- To display if hidden, click  in the toolbar.
- To hide, click  at the top-right of the panel.

Hosts and Services Views References

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

The Admin module pulls NetWitness 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
- Services System View

Hosts View

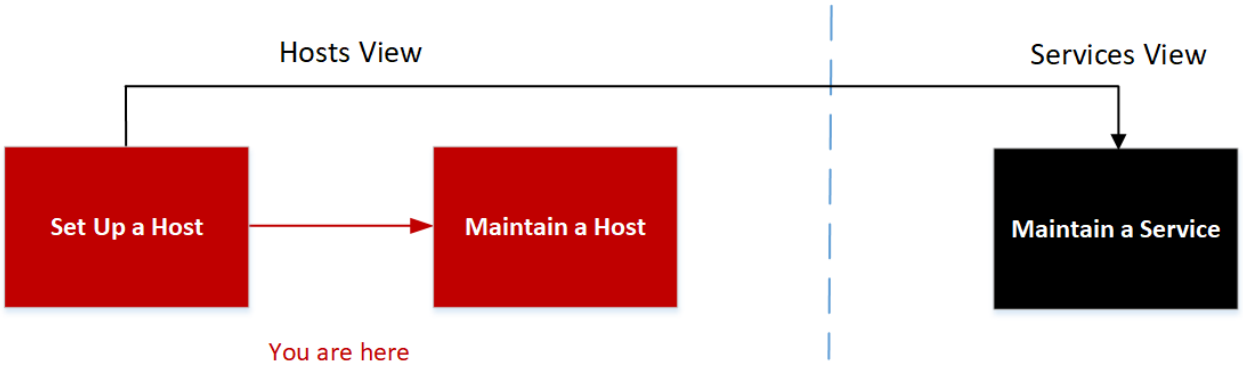
You set up and maintain the physical or virtual machine on which NetWitness services run in the Hosts view.

IMPORTANT: For help with resolving errors you receive during version installation and update, see Troubleshooting Version Installations and Updates .

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 Core services first. 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 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 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?

User Role	I want to...	Documentation
Administrator	set up a host.*	Setting Up a Host
Administrator	maintain a host.*	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	apply version updates to a host.*	Apply Version Upgrades to a Host

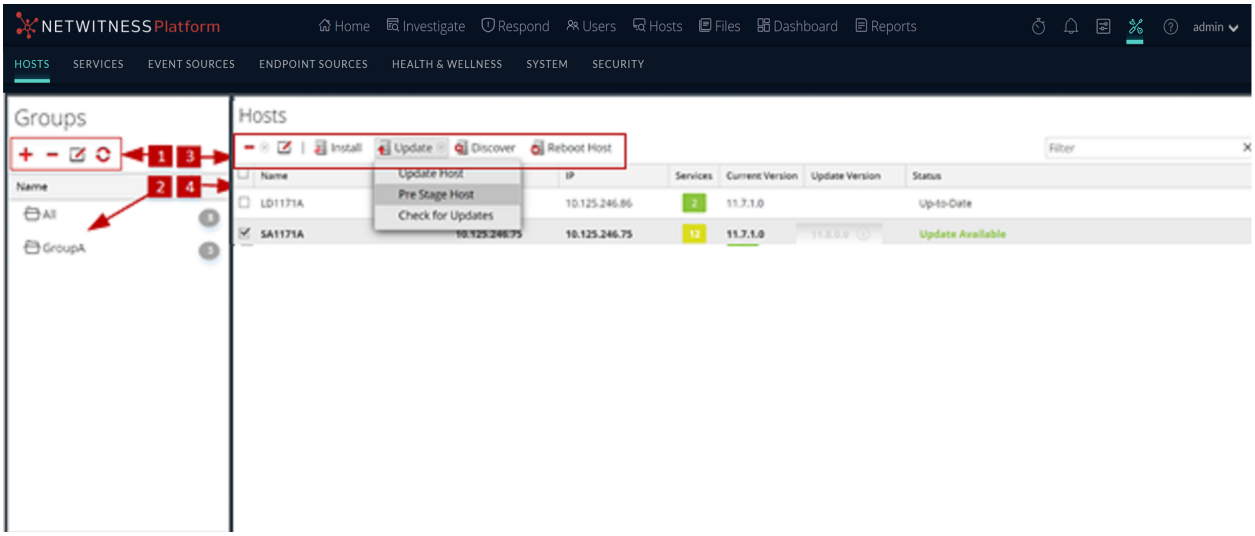
* You can perform these tasks in the current view.

Related Topics:

- Services View
- Hosts and Services Set Up Procedures
- Hosts and Services Maintenance Procedures

Quick Look

This is an example of the Hosts view.



1 Groups Panel Toolbar - Provides options to work with host groups in the list.
2 Groups Panel - Lists all host groups currently in your deployment.
3 Hosts List Toolbar - Provides options to work with the Hosts list.
4 Hosts List - Lists all hosts currently in your deployment.

Groups Panel Toolbar

Feature	Description
+	Displays a new row in the Groups panel in which you enter the name of a new group.
−	Asks for confirmation that you want to delete the group. You can confirm or cancel the deletion.
✎	Opens the field for renaming the selected preexisting group. You can also double click on the group name in the Groups panel to rename the group. Changes take effect immediately.
↻	Refreshes the Groups panel to reflect the changes and goes back to the All group view. Changes take effect immediately.

Groups Panel

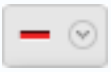
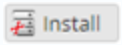
The Groups panel provides a logical way to organize hosts, such as by function, geography, or project. Once hosts are grouped, it is easier to perform operations on multiple hosts by interacting with each host in a group rather than individual hosts from an non-grouped list. You can drag a host from the Hosts list to add it to a group. A host may belong to more than one group.

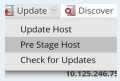
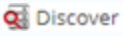
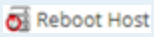
Note: In NetWitness Live, groups can subscribe to resources while individual hosts cannot.

Column Title	Description
Name	The host groups are displayed in the Groups panel. The number next to each group name displays the number of hosts that added to the group.

Hosts List Toolbar

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

Feature	Description
	This drop-down list displays two options. • **Remove Host**: Deletes the selected host from both the host group and the Hosts list altogether. All related services will be removed as well. • **Remove From Group**: Removes the selected host from the host group. The Host will still be available in the Hosts list. Changes take effect immediately.
	Opens the Edit Host dialog in which you edit a host or service identification and basic communication settings. See Step 1. Deploy a Host for more information.
	Opens the Install Services dialog from which you can install a service on a deployed host. See Step 2. Install a Service on a Host for more information.

Feature	Description
	This drop-down list displays three options. • **Update Host**: Updates the selected hosts with the version you select in the Update Version column. • **Pre-Stage Host:** Pre-stage the upgrade repository by downloading the required packages without affecting the system. • **Check for Updates**: Checks the Local Update Repo for the latest updates available from NetWitness. Changes take effect immediately. See Apply Version Upgrades to a Host for more information.
	Most of the time, the Discovery function completes automatically and you do not need to click  . For a fresh installation, click Discover to access the Provision dialog box so you can complete the provisioning phase. After the provisioning phase, NetWitness automatically discovers services running on the host and you do not need to click Discover.
	Restarts the host immediately.
	Entering a Name or Host here filters the list. This field allows you to quickly find a particular host.

Hosts List

Column	Description
☐	Select the host by clicking the corresponding checkbox in this column. To select all of the hosts, select the checkbox in the header.
Name	Displays the name of the host that was given when the host was installed. This column is organized in alphabetical order by default. Click the Name column title to view in reverse alphabetical order.
Host	Displays the IP address of each host.
Services	Displays the number of services added to the host.
Current Version	Displays the version that the host is currently on.
Update Version	Displays a drop-down list of versions that the user can upgrade to. See Apply Version Upgrades to a Host for more information.

Column	Description
Status	Displays whether or not the host is upgraded to the most current version. If the host is on the most current version, then the Status displays "Up-to-Date".

Services View

You set up and maintain the NetWitness services in the Services view. In 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.
- Sort services by name and host.
- Filter services by type, 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.

Services	Notes
NW Server	
Admin	Resides within the NW Server
Config	Resides within the NW Server
Content	Resides within the NW Server
Integration	Resides within the NW Server
Investigate	Resides within the NW Server
License	Resides within the NW Server
Orchestration	Resides within the NW Server
Reporting Engine	
Respond	Resides within the NW Server
Security	Resides within the NW Server
Response Actions	Resides within the NW Server
Analyst UI	
Broker	Implemented with the Analyst UI
Investigate Server	Implemented with the Analyst UI
NetWitness UI	Implemented with the Analyst UI
Reporting Engine	Implemented with the Analyst UI
Respond Server	Implemented with the Analyst UI
Archiver	
Archiver	Core Service
Workbench	
Broker	
Broker	Core Service

Services	Notes
Concentrator	
Concentrator	Core Service
Endpoint	
Endpoint Server	
Endpoint Broker	
Endpoint Broker Server	
Endpoint Log Hybrid	
Log Collector Log Decoder Endpoint Server Concentrator	Core Service Core Service Core Service
ESA Primary	
Contexthub ESA Correlation	
ESA Secondary	
ESA Correlation	
Log Collector	
Log Collector	Core Service
Log Decoder	
Log Collector Log Decoder	 Core Service
Log Hybrid	
Log Collector Log Decoder Concentrator	 Core Service Core Service
Log Hybrid - Retention	Deployed on Series 6 Hybrid hardware with Log Hybrid-Retention Optimization.
Log Collector Log Decoder	 Core Service
Malware Analysis	
Malware Analysis Broker	 Core Service
Network Decoder	

Services	Notes
Decoder (Packets)	Core Service
Network Hybrid	
Concentrator Network Decoder	Core Service Core Service
New Health and Wellness	
Metrics Server	
UEBA	
UEBA	
Warehouse Connector	
Warehouse Connector	Command line installation

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. For information about ports and a comprehensive list of ports for all services, see "Network Architecture and Ports" in the *Deployment Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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 deployment.



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.*	Maintaining Services

* You can perform these tasks in the current view.

Related Topics

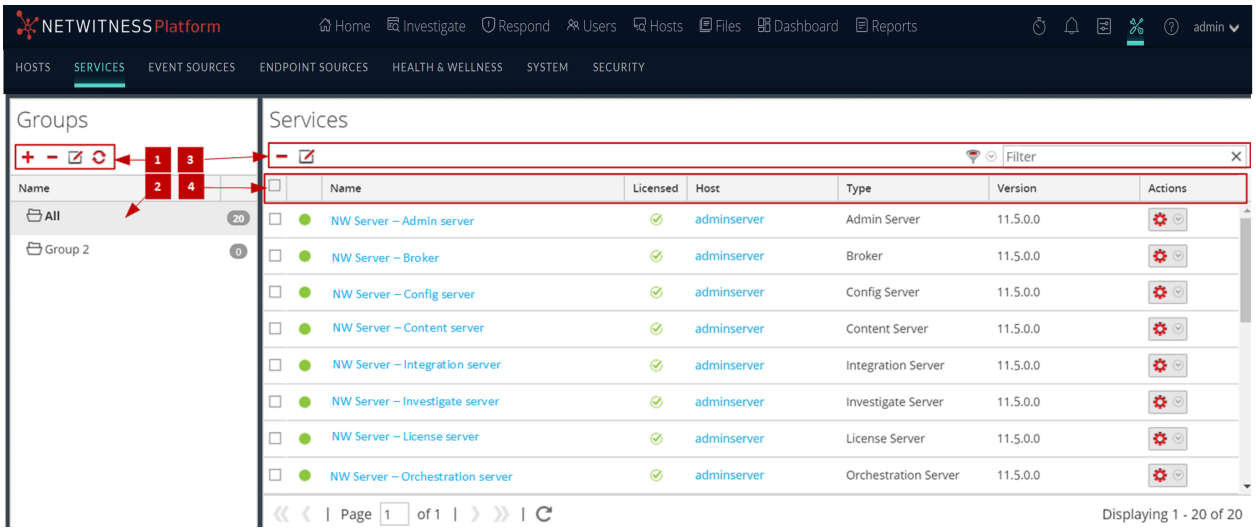
- View Topology Details
- Hosts View
- Hosts and Services Set Up Procedures
- Hosts and Services Maintenance Procedures

See the following NetWitness guides for detailed information on individual services. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Archiver Configuration Guide
Broker and Concentrator Configuration Guide
Context Hub Configuration Guide
Decoder Configuration Guide
Endpoint Configuration Guide
Event Stream Analysis (ESA) Configuration Guide
Malware Analysis Configuration Guide
Log Collection Configuration Guide
Malware Analysis Configuration Guide
Reporting Engine User Guide
NetWitness Respond Configuration Guide
NetWitness UEBA User Guide
Workbench Configuration Guide
Warehouse Connector Configuration Guide
Response Actions Configuration Guide

Quick Look

This is an example of the Services view.



1 Groups Panel Toolbar - Provides options to work with service groups in the list.
2 Groups Panel - Lists all service groups currently in your deployment.
3 Services List Toolbar - Provides options to work with the Services list.
4 Services List - Lists all services currently in your deployment.

Groups Panel Toolbar

Feature	Description
	Displays a new row in the Groups panel in which you enter the name of a new group.
	Asks for confirmation that you want to delete the group. You can confirm or cancel the deletion.
	Opens the field for renaming the selected preexisting group. You can also double click on the group name in the Groups panel to rename the group. Changes take effect immediately.
	Refreshes the Groups panel to reflect the changes and goes back to the All group view. Changes take effect immediately.

Groups Panel

The Groups panel provides a logical way to manage groups of services, such as by function, geography, or project. After you create a group, you can drag individual services from the Services panel into the group. A service may belong to more than one group.

Column Title	Description
Name	The service groups are displayed in the Groups panel. The number next to each group name displays the number of hosts that added to the group.

Services List Toolbar

This topic introduces the options in Services list toolbar to add, remove, edit, and get a license for services. You can also filter the services listed in the Services list.

To access the Admin Services view, in NetWitness, go to **(Admin) > Services.** The Services list toolbar is at the top of the Services list in the Services view.

Feature	Description
+	Adds a service for your deployment of NetWitness to manage. See Step 2. Install a Service on a Host.
−	Deletes a service from your deployment of NetWitness. See Edit or Delete a Service.
	Edits service identification and basic communication settings.
Filter	Filters the services listed in Services view. In the Filter drop-down list, you can filter the services by one or more selected service types. In the Filter field, you can filter the services by Name and Host. You can use the Filter drop-down list and the Filter field at the same time to filter the services listed in the Services view.

Services List

Column	Description
☐	Select the service by clicking the corresponding checkbox in this column. To select all of the services, select the checkbox in the header.
Online/Offline Indicator	Displays ● if the service is online. Displays ● if the service is offline.
Name	Displays the name of the service that was given when the service was installed. This column is organized in alphabetical order by default. Click the Name column title to view in reverse alphabetical order.
Licensed	Displays ✓ if the service is licensed. Displays ● if the service is not licensed. If one or more services are not licensed, a red banner will appear at the top of the screen that will prompt you to fix this. One or more services are not licensed. For more information, see License Details
Host	Displays the host name that the service belongs to.
Type	Displays the service type.
Version	Displays the version that the service is currently on.

Column	Description
Actions	Use drop-down list to: • Navigate to the different service views (System, Stats, Config, Explore, Logs, Security) See View Topology Details for more information. • Delete, edit, start, stop, and restart a service. See Start, Stop, or Restart a Service for more information.

Topics

- Edit Service Dialog
- Services Config View
- Services Explore View
- Services Logs View
- Services Security View
- Services Stats View
- Services System View

Edit Service Dialog

NetWitness services are automatically discovered in NetWitness.

You can use the Edit Service dialog to modify services. To access the Edit Service dialog, go to **(Admin) > Services** and click in the **Services** list toolbar.

Workflow



What do you want to do?

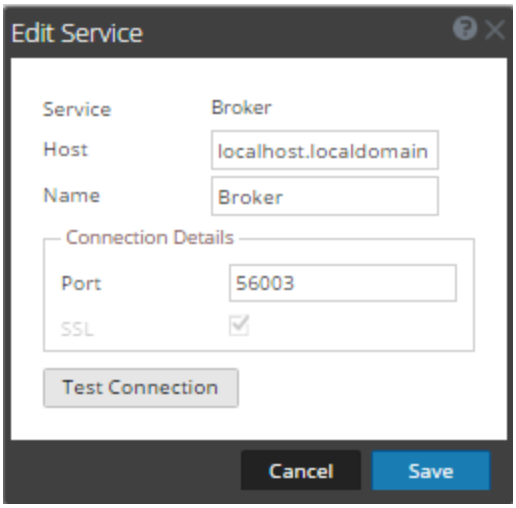
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	edit a service.*	Edit a Service

* You can perform these tasks in the current view.

Related Topics:

- Services View
- Hosts and Services Set Up Procedures
- Hosts and Services Maintenance Procedures

Quick Look



The following list 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, Network Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.
Host	Specifies the host on which the service resides.
Name	Specifies the name used to identify the service, for example, **Broker**. An understandable naming convention can make administrative tasks easier. Some administrators find it convenient to use the hostname or IP address (specified in the **Host** field) for the **Name** as well.
Port	Specifies the port used to communicate with this service. The default port, based on the selected service type in the **Service** field, is autofilled here. If you select **SSL** below, this port becomes an SSL port. If you do not select **SSL**, it becomes a non-SSL port. You can customize this port by opening a firewall for the port that you add. For information about ports, see "Network Architecture and Ports" in the *Deployment Guide*.
SSL	Indicates that NetWitness uses SSL for communications with this service.
Username	Specifies the username 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`.
Test Connection	Tests the connection of a service that you are adding.
Cancel	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.

Field or Option	Description
Save	Adds a new service or saves changes to existing service.

Services Config View

The Services Config view is one of the views available from the **(Admin) > Services >** . It provides a user interface for configuring all aspects of a Core service or NetWitness 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, Concentrators, Network Decoders, Log Decoders, and Archivers) or service (for example, Reporting Engine, IPDB Extractor, Log Collector, and Warehouse Connector).

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	configure an Archiver service.	See *Archiver Configuration Guide*.
Administrator	configure a Broker service.	See *Broker and Concentrator Configuration Guide*.
Administrator	configure a Concentrator service.	See *Broker and Concentrator Configuration Guide*.
Administrator	configure a Context Hub service.	See *Context Hub Configuration Guide*.
Administrator	configure an Endpoint Broker service.	See *Endpoint Configuration Guide*.

User Role	I want to...	Documentation
Administrator	configure an Endpoint Log Hybrid service.	See *Endpoint Configuration Guide*.
Administrator	configure an ESA Primary service.	See *ESA Configuration Guide*.
Administrator	configure an ESA Secondary service.	See *ESA Configuration Guide*.
Administrator	configure a Log Collector service.	See *Log Collection Configuration Guide*.
Administrator	configure a Log Decoder service.	See *Decoder Configuration Guide*
Administrator	configure a Malware Analysis service.	See *Malware Analysis User Guide*.
Administrator	configure a Network Decoder service.	See *Decoder Configuration Guide*.
Administrator	configure a Reporting Engine service.	See *Reporting Engine Configuration Guide*.
Administrator	configure a Respond service.	See *NetWitness Respond Configuration Guide*.
Administrator	configure a UEBA service.	See *NetWitness UEBA User Guide*.
Administrator	configure a Warehouse Connector service.	See *Warehouse Connector Configuration Guide*.
Administrator	configure a Workbench service.	See *Workbench Configuration Guide*.

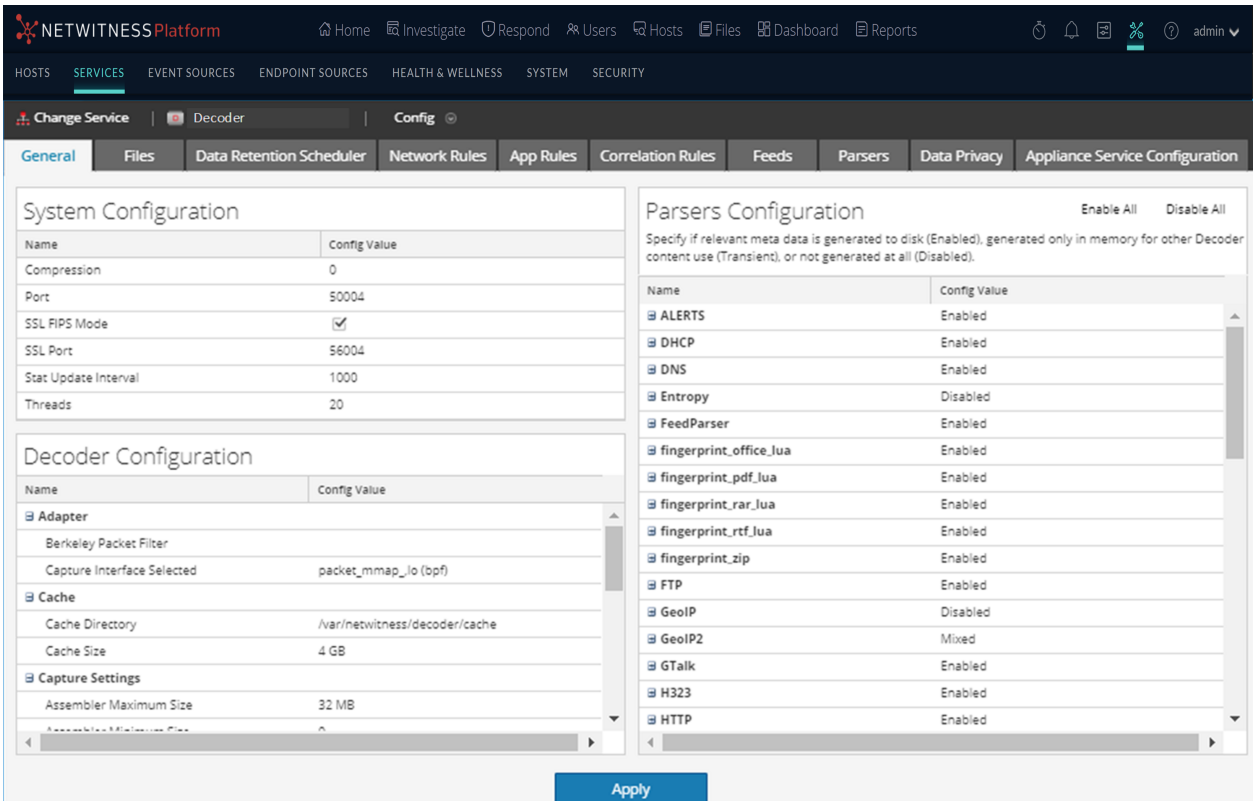
Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Related Topics

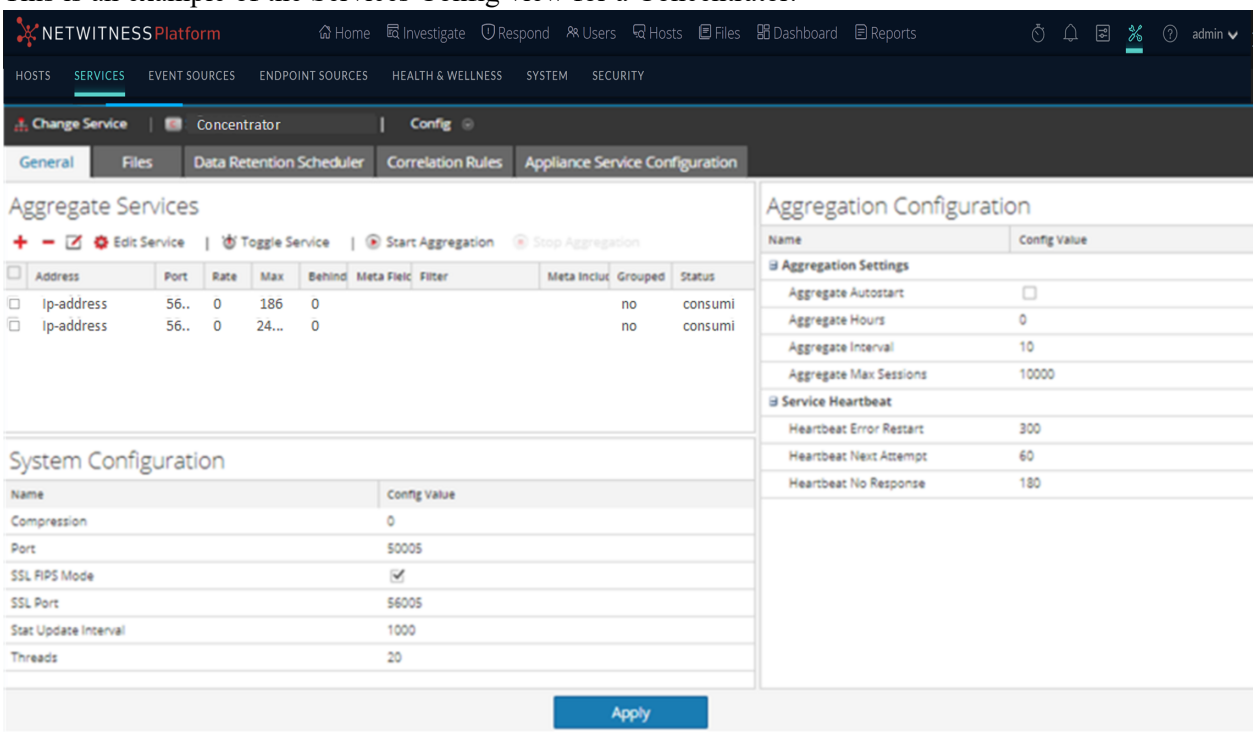
- Edit Service Dialog
- Services Explore View
- Services Logs View
- Services Security View
- Services Stats View
- Services System View
- Services View

Quick Look

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



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



Note: Although both examples show the Services Config view, the tabs and panels are different for each. Refer to the respective guides for detailed instructions on how to configure a particular Services Config view.

Topics

- Services Config View - Appliance Service Configuration Tab
- Services Config View - Data Retention Scheduler Tab
- Services Config View - Files Tab

Services Config View - Appliance Service Configuration Tab

The Appliance Service Configuration tab appears in the Services Config view for the Archiver, Broker, Concentrator, IPDB Extractor, Network Decoder, Log Collector, and Log Decoder services.

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

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.*	Maintaining Services
Administrator	view or modify appliance service parameters.*	See "Services Config View - Appliance Service Configuration Tab" in the *Hosts and Services Getting Started Guide for Version 10.x*and prior.

User Role	I want to...	Documentation
Administrator	specify how long to retain database records.	See "Configure Data Retention" in the *Data Privacy Management Guide*. For information about the Data Retention tab for Archiver, see "Data Retention Tab - Archiver" in the *Archiver Configuration Guide*.
Administrator	edit `.xml` and `.lua` files.	Edit Core Service Configuration Files

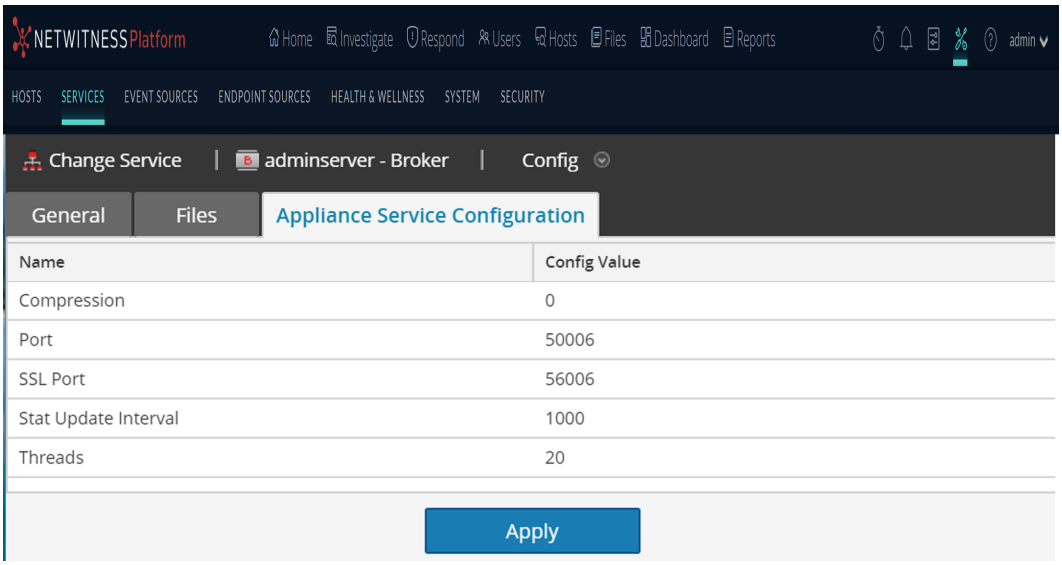
* You can perform these tasks in the current view.

Related Topics

- Services Config View - Data Retention Scheduler Tab
- Services Config View - Data Retention Scheduler Tab
- Services Config View - Files Tab
- Services Config View

Quick Look

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



The following list describes the configuration values for this tab.

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). For detailed instructions, see "Activate or Deactivate FIPS" in the *System Maintenance Guide*.	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.

Services Config View - Data Retention Scheduler Tab

The Data Retention Scheduler tab appears in the Services Config view for the Network Decoder, Log Decoder, and Concentrator.

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

Note: If additional customization is necessary, use the Scheduler under the Files tab in the Services Config view. For example, if you have storage available to save the RAW data versus the metadata, use `Capacity` as the threshold and to set different thresholds per database (metadata versus packet).

Workflow



What do you want to do?

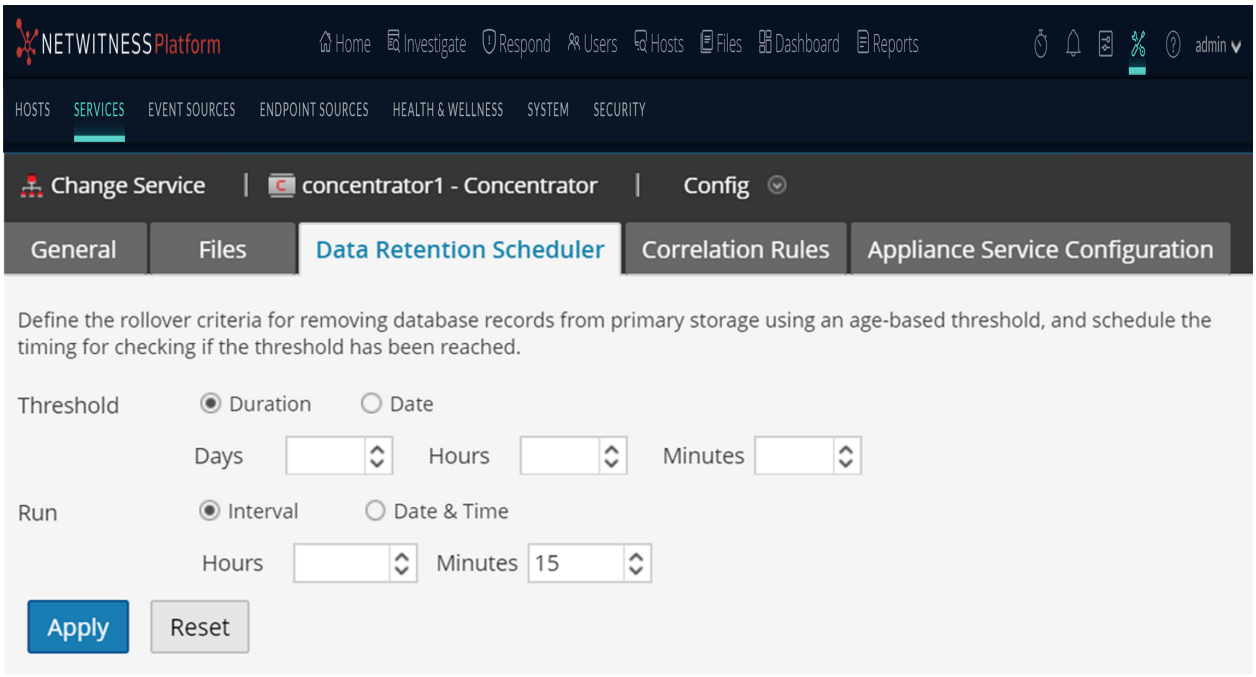
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.*	Maintaining Services
Administrator	view or modify appliance service parameters.	See "Services Config View - Appliance Service Configuration Tab" in the *Hosts and Services Getting Started Guide for Version 10.x* and prior.
Administrator	specify how long to retain database records.*	See "Configure Data Retention" in the *Data Privacy Management Guide*. For information about the Data Retention tab for Archiver, see "Data Retention Tab - Archiver" in the *Archiver Configuration Guide*.
Administrator	edit `.xml` and `.lua` files.	Edit Core Service Configuration Files

Related Topics

- Services Config View - Appliance Service Configuration Tab
- Services Config View - Files Tab
- Services Config View

Quick Look

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



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

Parameter	Description
Threshold	The threshold is based on the age of the data, the amount of time the data was stored or the date on which the data was stored. The date is from the database file, not from the actual session time. • **Duration**: The duration of time that data can be stored before removal. Specifies the number of days (365 maximum), hours (24 maximum), and minutes (60 maximum) that have elapsed since the time stamp on the data. • **Date**: The removal of data based on the date of the timestamp. Specifies the monthly date and time in the and fields.
Run	The schedule for running the job that checks rollover criteria. • **Interval**: Schedule the database check to occur at a regular interval. Specifies the hours and minutes between the scheduled checks. • **Date and Time**: Schedule the database check to occur at a regular day and time. Specifies the day from the drop-down list and the system clock time in `hh:mm:ss` format. Possible values for day are `Everyday`, `Weekdays`, `Weekends`, and `Custom`, where `Custom` allows you to select one or more specific days of the week.

Parameter	Description
Apply	Overwrites any previous schedule for this service and applies the new settings immediately. **Caution:** After you apply these settings, when the threshold is met the system deletes the old data from the database and you can no longer access it.
Reset	Resets the schedule to the last applied state.

Services Config View - Files Tab

The Files tab appears in the Services Config view for Archivers, Brokers, Concentrators, Log Decoders, and Network Decoders.

In the Files tab, you can edit service configuration files as text files. The files you can edit vary depending upon the type of service you are configuring. The following files are common to all Core services.

- The NetWitness file (`netwitness`)
- The service index file (`index-<service>`)
- The scheduler file (`scheduler`)
- The crash reporter file (`crashreporter`)
- The feed definitions file (`feed-definitions`)

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

Note: The default values in the configuration files cover most common situations. You may need to edit configuration parameters and values for optional services, such as the crash reporter or scheduler. Do not change these values in the Files tab unless you understand networks and the factors that affect the way services collect and parse data.

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

Workflow



What do you want to do?

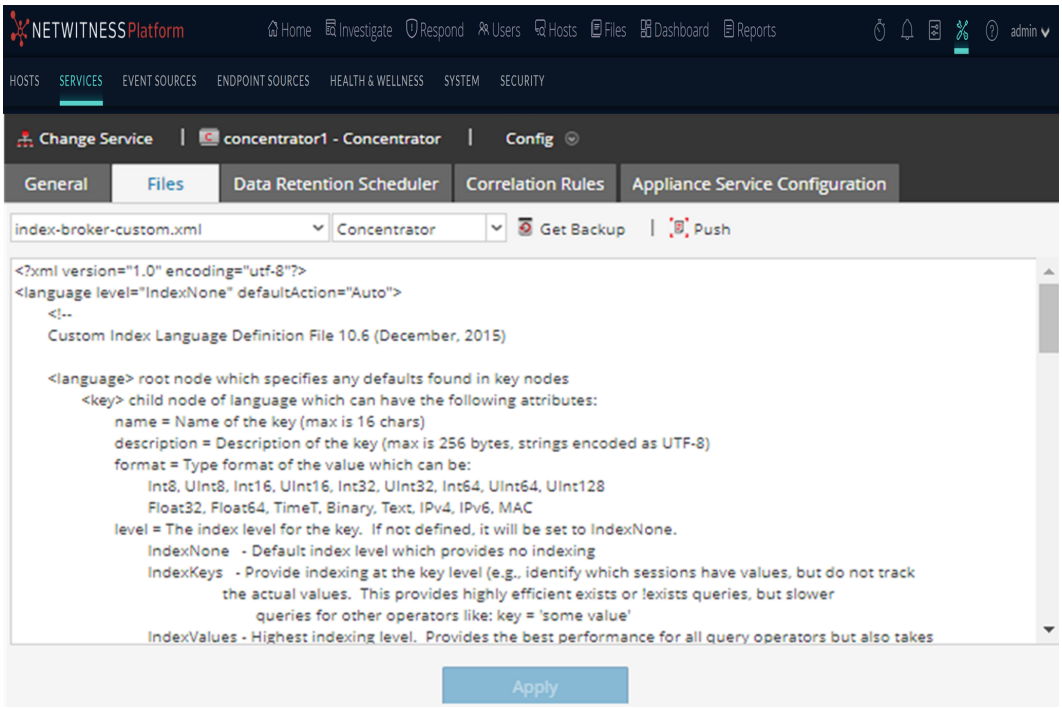
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.*	Maintaining Services
Administrator	view or modify appliance service parameters.	See "Services Config View - Appliance Service Configuration Tab" in the *Hosts and Services Getting Started Guide for Version 10.x*and prior.
Administrator	specify how long to retain database records.	See "Configure Data Retention" in the *Data Privacy Management Guide*. For information about the Data Retention tab for Archiver, see "Data Retention Tab - Archiver" in the *Archiver Configuration Guide*.
Administrator	edit `.xml` and `.lua` files.*	Edit Core Service Configuration Files

Related Topics

- Services Config View - Data Retention Scheduler Tab
- Services Config View - Data Retention Scheduler Tab
- Services Config View

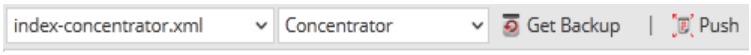
Quick Look

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 Backup	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**.
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 and creates a backup file.

Services Explore View

You can use the NetWitness Services Explore view (**(Admin) > Services**, **> View > Explore**) to display and edit both host and service configurations.

The Services Explore view offers advanced access and control of all NetWitness hosts and services. All services expose their functionality through a treelike series of nodes, similar to the Windows Explorer view of a Windows 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.

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

Workflow



What do you want to do?

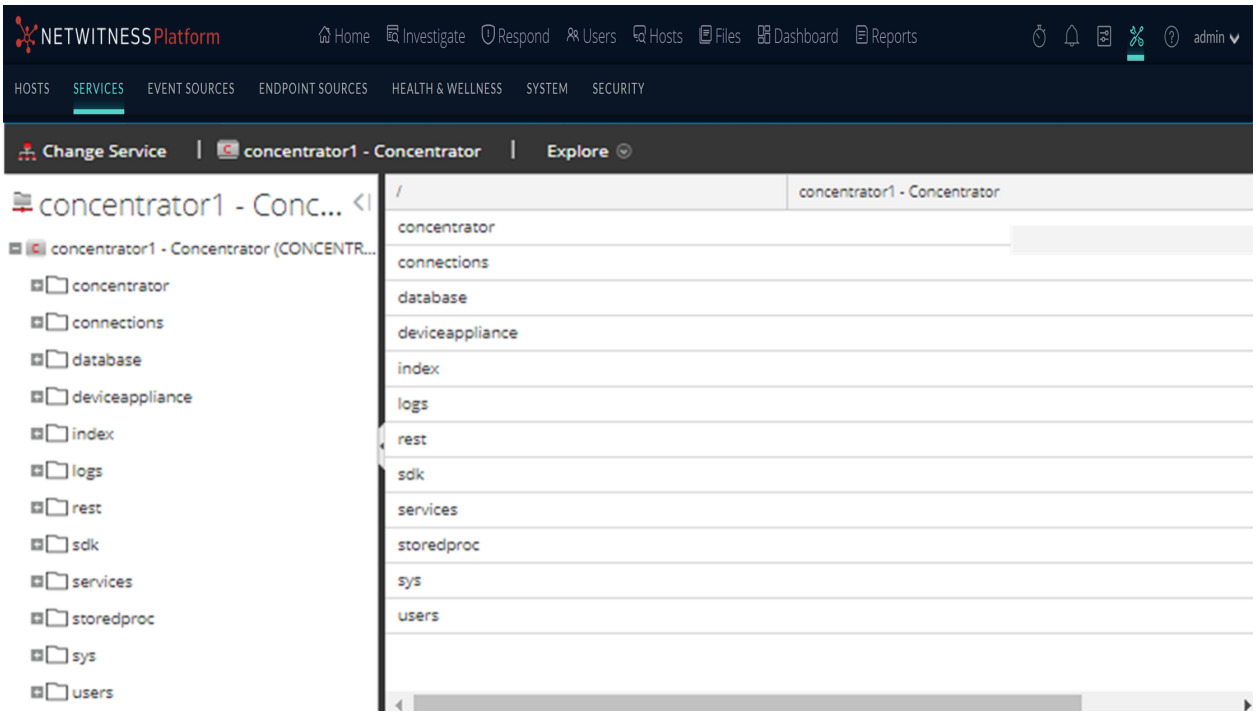
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	view and edit host and service configurations.*	Explore and Edit Service Property Tree

* You can perform these tasks in the current view.

Related Topics

- View Topology Details
- Edit Service Dialog
- Services Config View
- Services Logs View
- Services Security View
- Services Stats View
- Services System View
- Services View

Quick Look



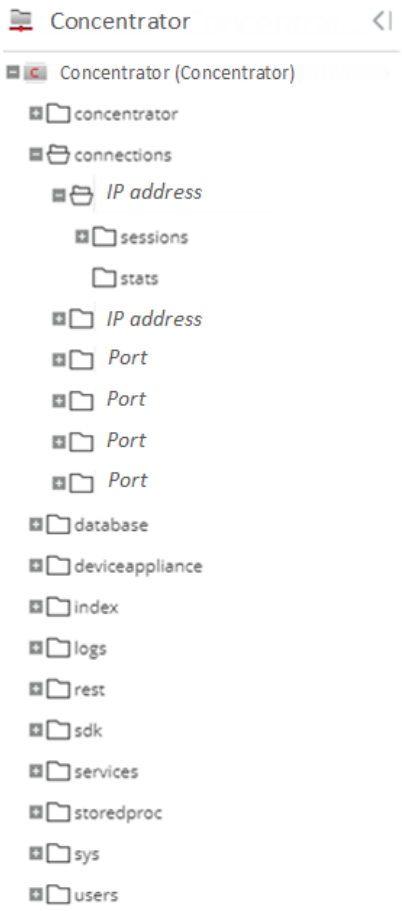
The Services Explore View has two main panels:

- The Node list
- The Monitor panel

You can right-click on a file to access the Properties for the file. See Services Explore View - Properties Dialog for more information.

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 address or port in the list 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 or received, bytes sent or received, and other values 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:

- Click the value and type a new value
- Send a `set` message in the Properties dialog

/index/config	Concentrator
index.dir	/var/netwitness/concentrator/index=2.89 TB
index.dir.cold	
index.dir.warm	
index.slices.open	42
page.compression	huffhybrid
reindex.enable	true
save.session.count	auto

Topics

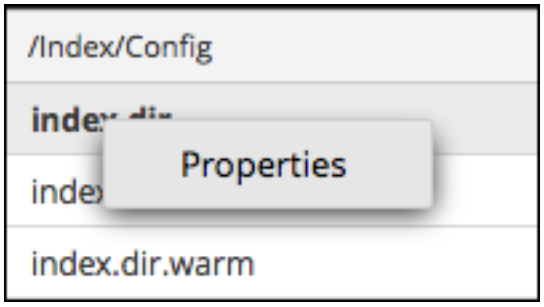
- View Topology Details

Services Explore View - Properties Dialog

You can use the Services Explore view > Properties dialog to perform the following tasks.

- Send messages to a system node
- Retrieve values for a property for multiple services
- Set values for a property for multiple services

Right-click any file in the Node list or Monitor panel to display the Properties context menu.



When you select `Properties` from the Node list or Monitor panel context menu, the Properties dialog opens below the Monitor panel. All nodes have support help that contains the following information.

- 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 dashboard or view.

Workflow



What do you want to do?

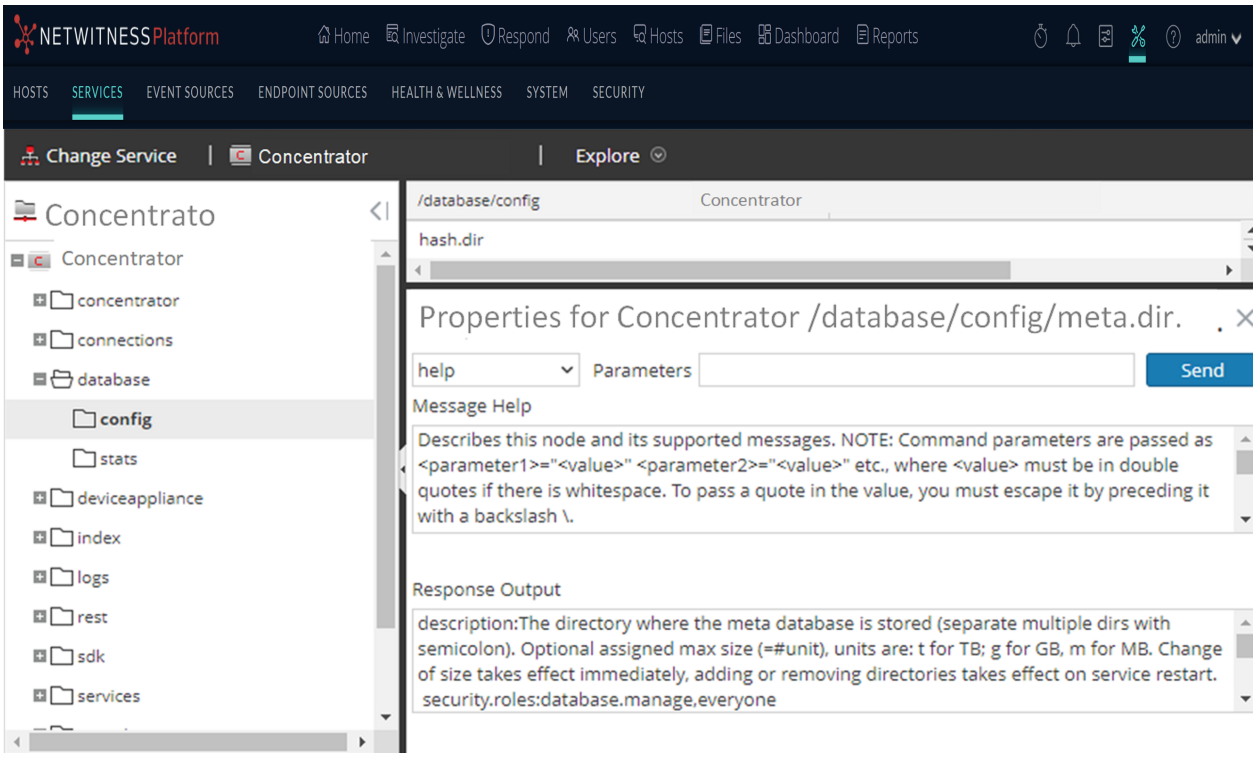
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	send messages to a system node.*	Explore and Edit Service Property Tree
Administrator	retrieve values for a property for multiple services.*	Explore and Edit Service Property Tree
Administrator	set values for a property for multiple services.*	Explore and Edit Service Property Tree

* You can perform these tasks in the current view.

Related Topics

- Services Explore View

The following example shows the Properties dialog with information in Message Help displayed.



The Properties dialog has the following features.

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

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 (**(Admin) > System tab > System Logging**) 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.

For a complete description of NetWitness logging features in the System Logging panel, see "Monitor Health and Wellness of NetWitness Platform" in the *System Maintenance Guide*.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	view and search the logs for a specific service.*	See "Monitor Health and Wellness of NetWitness Platform" in the *System Maintenance Guide*

* You can perform these tasks in the current view.

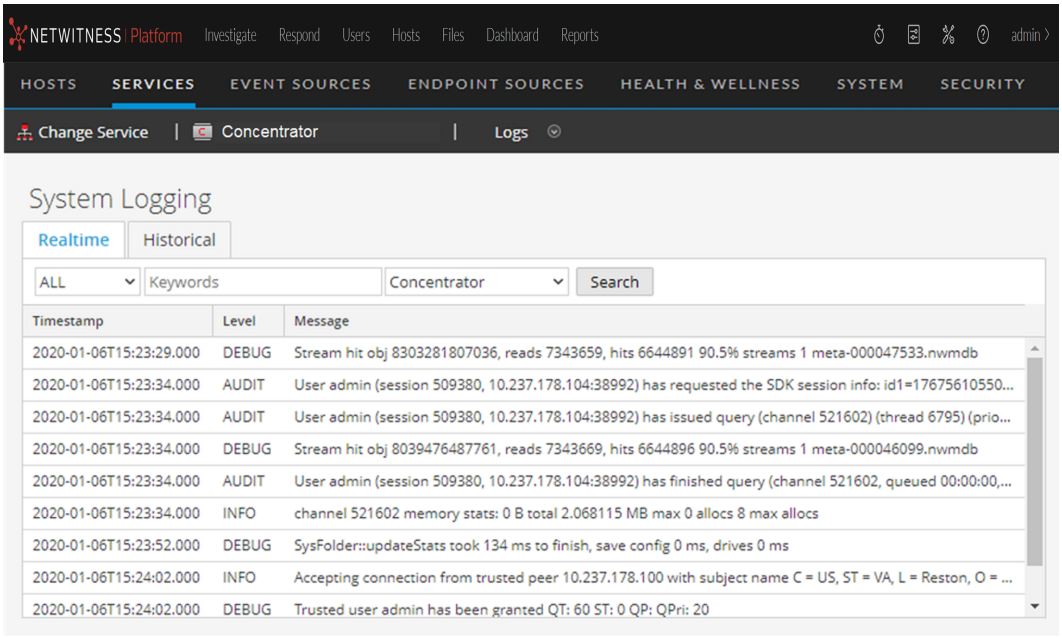
Related Topics

- Edit Service Dialog
- Services Config View
- Services Explore View
- Services Security View
- Services Stats View

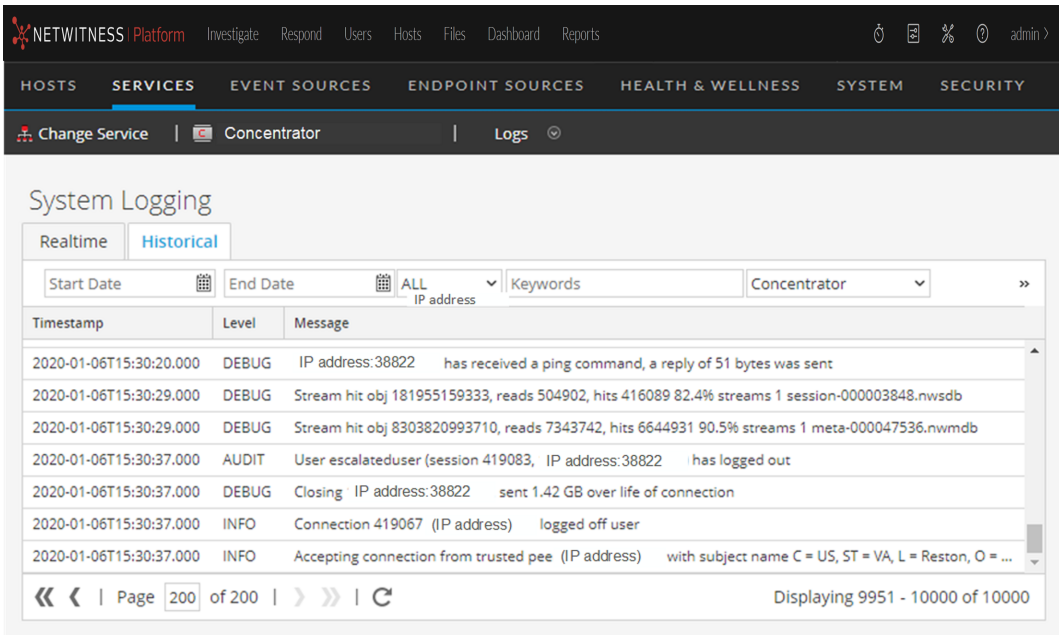
- Services System View
- Services View

Quick Look

The following figure shows the Services Logs view Realtime tab.



The following figure shows the Services Logs view Historical tab.



Feature	Description
Realtime tab	This is the monitor mode of the service log. For more information, see "System Logging - Realtime Tab" in the *System Maintenance Guide*.
Historical tab	This is a searchable view of the service log. For more information, see "System Logging - Historical Tab" in the *System Maintenance Guide*.

Services Security View

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

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

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	manage configuration of users, roles, and role permissions.*	See the *System Security and User Management Guide*.

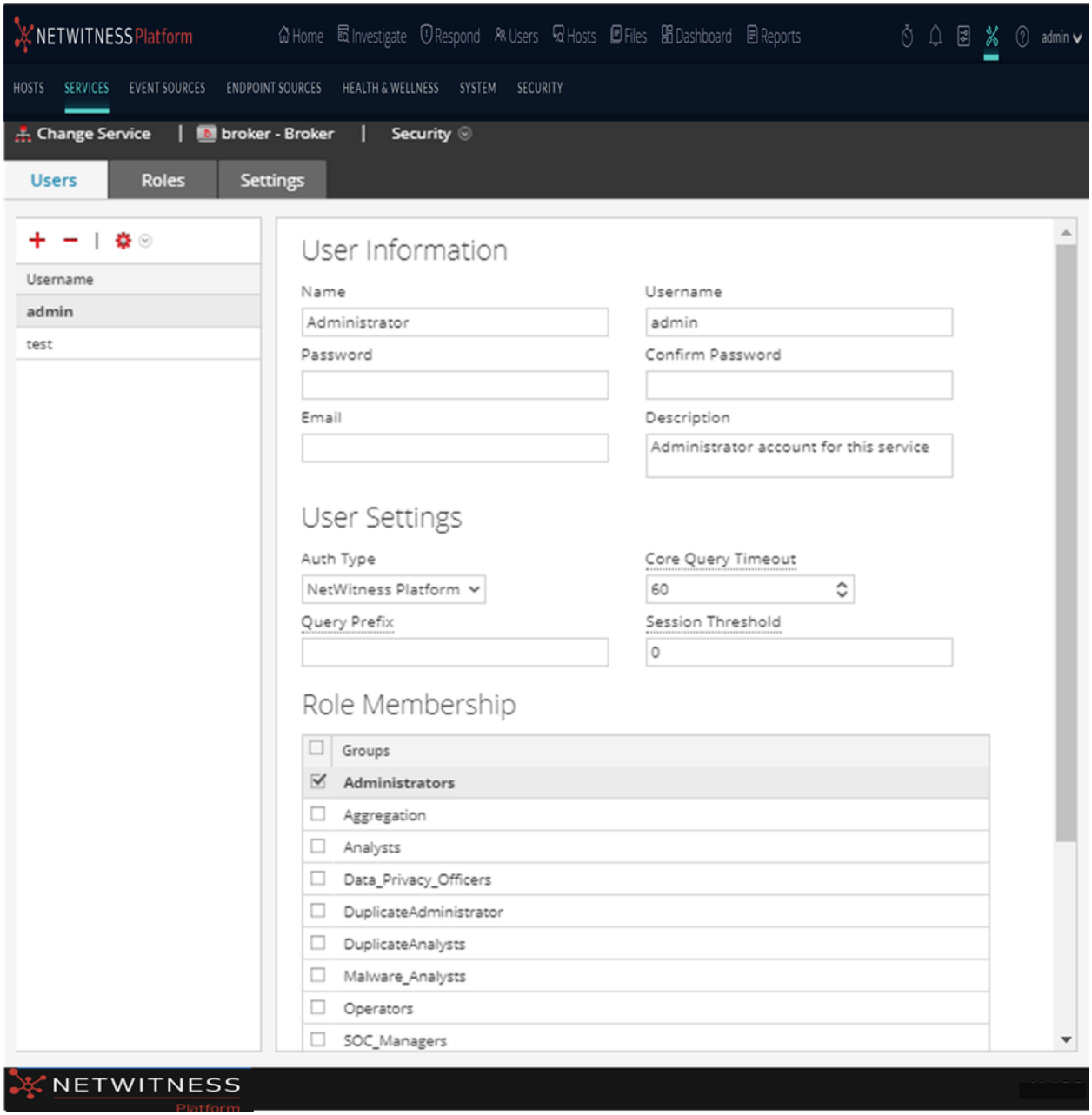
* You can perform these tasks in the current view.

Related Topics

- Add, Replicate, or Delete a Service User
- Add a User Role to a Service
- Change a Service User Password
- Duplicate or Replicate a Service Role

- Edit Service Dialog
- Services Config View
- Services Explore View
- Services Logs View
- Services Stats View
- Services System View
- Services View

Quick Look



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

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 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.

- In the Roles tab, you can create roles and assign permissions to the roles for a selected service.

Topics

- Services Security View - Users Tab
- Services Security View - Roles Tab
- Services Security View - Settings Tab

Services Security View - Users Tab

In the Services Security view Users tab, you can 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 version 10.4 or later NetWitness Core services that utilize trusted connections, it is no longer necessary to create NetWitness Core user accounts for users that log on through the web client. You only need to create NetWitness Core user accounts for aggregation, thick client users, and REST API users.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services

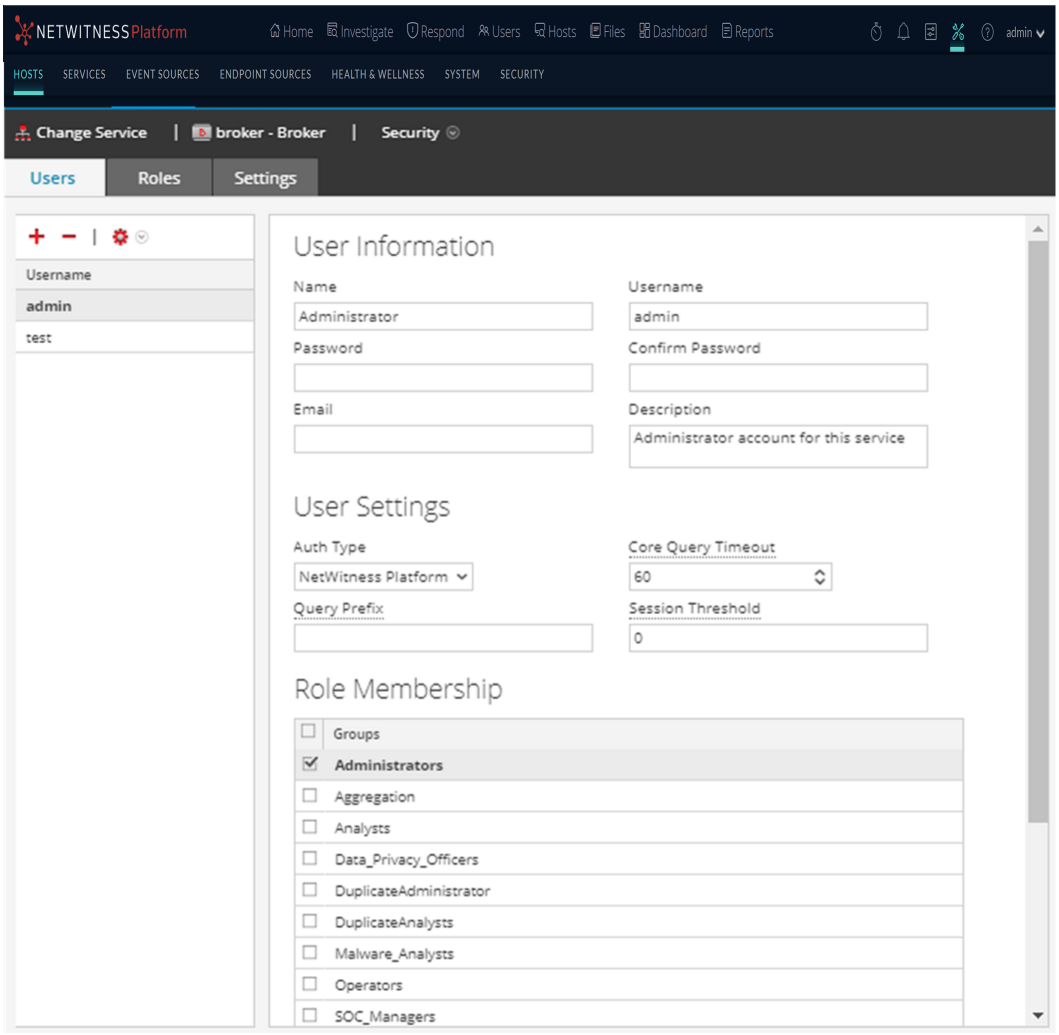
User Role	I want to...	Documentation
Administrator	add user accounts.*	Add, Replicate, or Delete a Service User
Administrator	change service user passwords.*	Change a Service User Password
Administrator	configure user authentication properties and query handling properties for the service.*	See "Verify Query and Session Attributes per Role" in the *System Security and User Management Guide*.
Administrator	specify the user role membership (roles that the user belongs to on the selected service).*	See "Add a User and Assign a Role" in the *System Security and User Management Guide*.

* You can perform these tasks in the current view.

Related Topics

- Services Security View - Roles Tab
- Services Security View - Settings Tab
- Services Security View

Quick Look



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

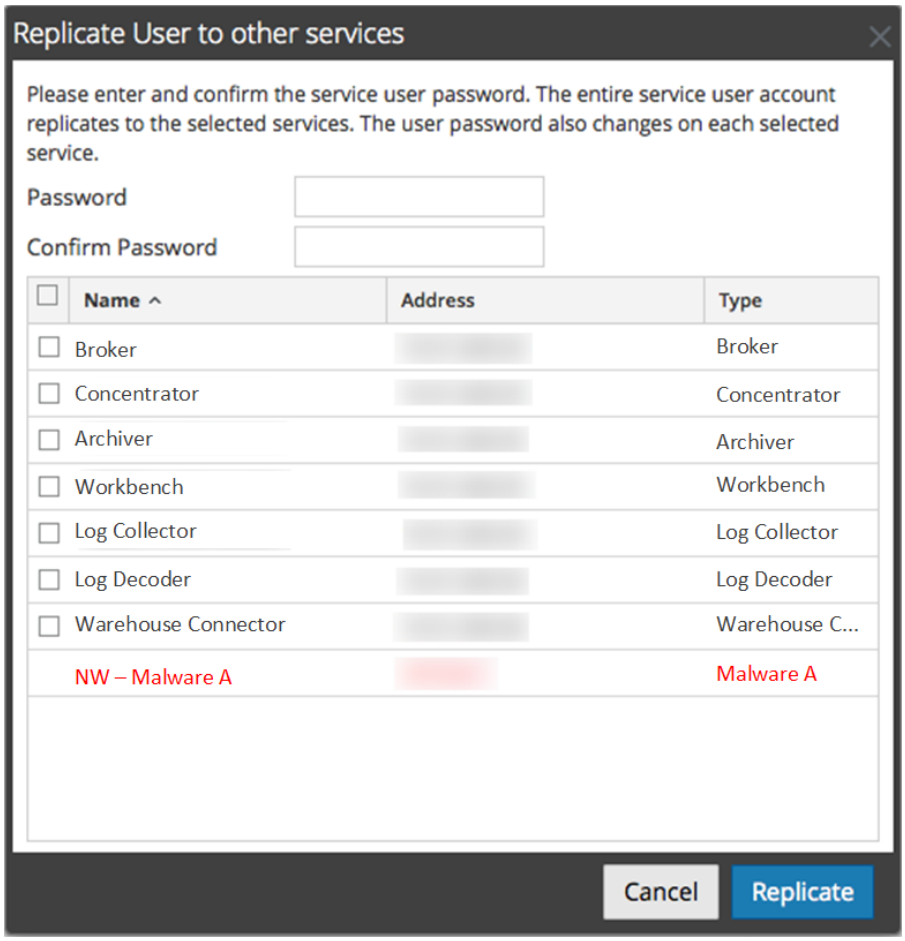
User List Panel

The User List panel has the following features.

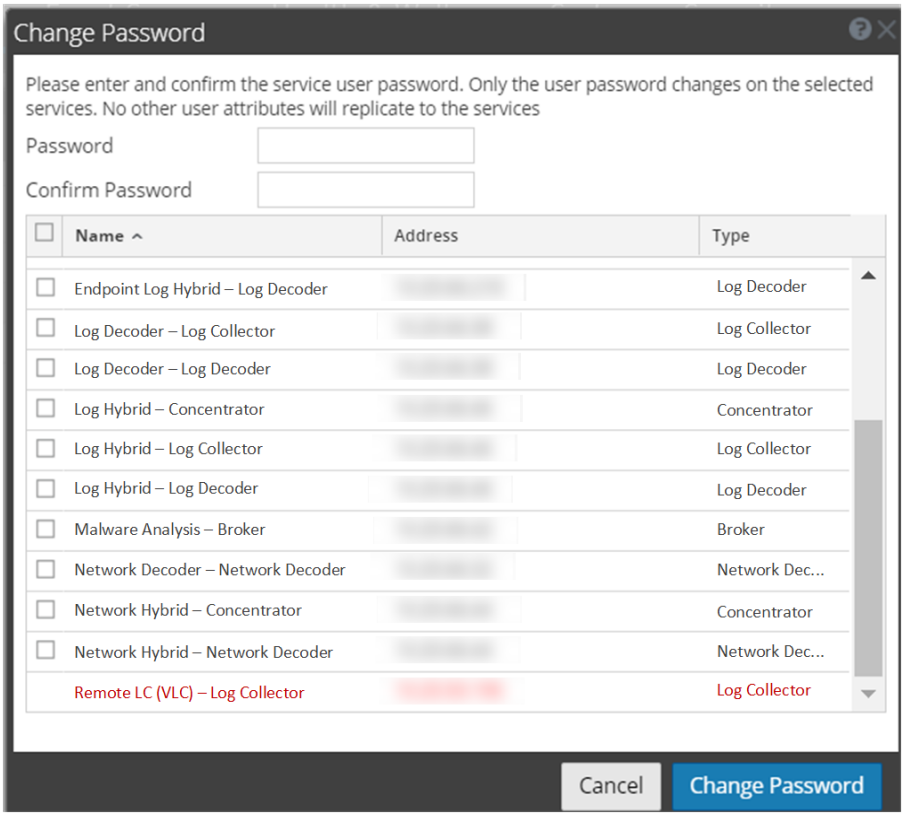
Feature	Description
+	Adds a new user to the current service.
−	Deletes the selected users from the service.

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

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



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



User Definition Panel

The User Definition panel has three sections:

- User Information identifies the user as created in the Admin Services 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 at the bottom of the panel:

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

User Information

The User Information section has the following features.

Field	Description
Name	The name of the user.
Username	The username that this user enters to log in to the service. This is the NetWitness username generated when the administrator added the user and the associated credentials in the Admin Services Security view.

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

User Settings

The User Settings section has the following features.

Field	Description
Auth Type	The authentication scheme for this user. The product line supports internal and external authentication. • **NetWitness Platform** 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 Admin Services Security view 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 "Configure PAM Login Capability" in the *System Security and User Management Guide*.
Core Query Timeout	**Note:** This field was previously known as "SA Core Query Timeout" and does not appear for 10.4 and earlier service versions. NetWitness version 10.4 and earlier services use "Query Level" instead. Specifies the maximum number of minutes a user can run a query on the service. If this value is set to **0**, the query timeout is not enforced for the user on the service.
Query Prefix	(Optional) Restricts query results seen by the user by appending the query syntax to every query. For example, adding the query prefix `email != 'ceo@company.com'` prevents those email results from showing up in the sessions.
Session Threshold	(Optional) Controls the behavior of the application when scanning meta values to determine session counts. If any meta value has a session count that is above the set threshold, the determination of the true session count stops when the threshold is reached. If a threshold is set for a session, the Navigate view (INVESTIGATE > Navigate) shows that the threshold was reached and the percentage of query time used to reach the threshold.

Role Membership

The Role Membership section shows a list of all roles. The checkbox next to a role is selected for the roles that a user is a member of for the selected service.

Services Security View - Roles Tab

The Services Security view 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 Add a User Role to a Service.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	define user roles.*	Add a User Role to a Service
Administrator	assign permissions to the roles.*	See "Add a Role and Assign Permissions" in the *System Security and User Management Guide*.
Administrator	add a user role to a service.*	See "Add a Role and Assign Permissions" in the *System Security and User Management Guide*.

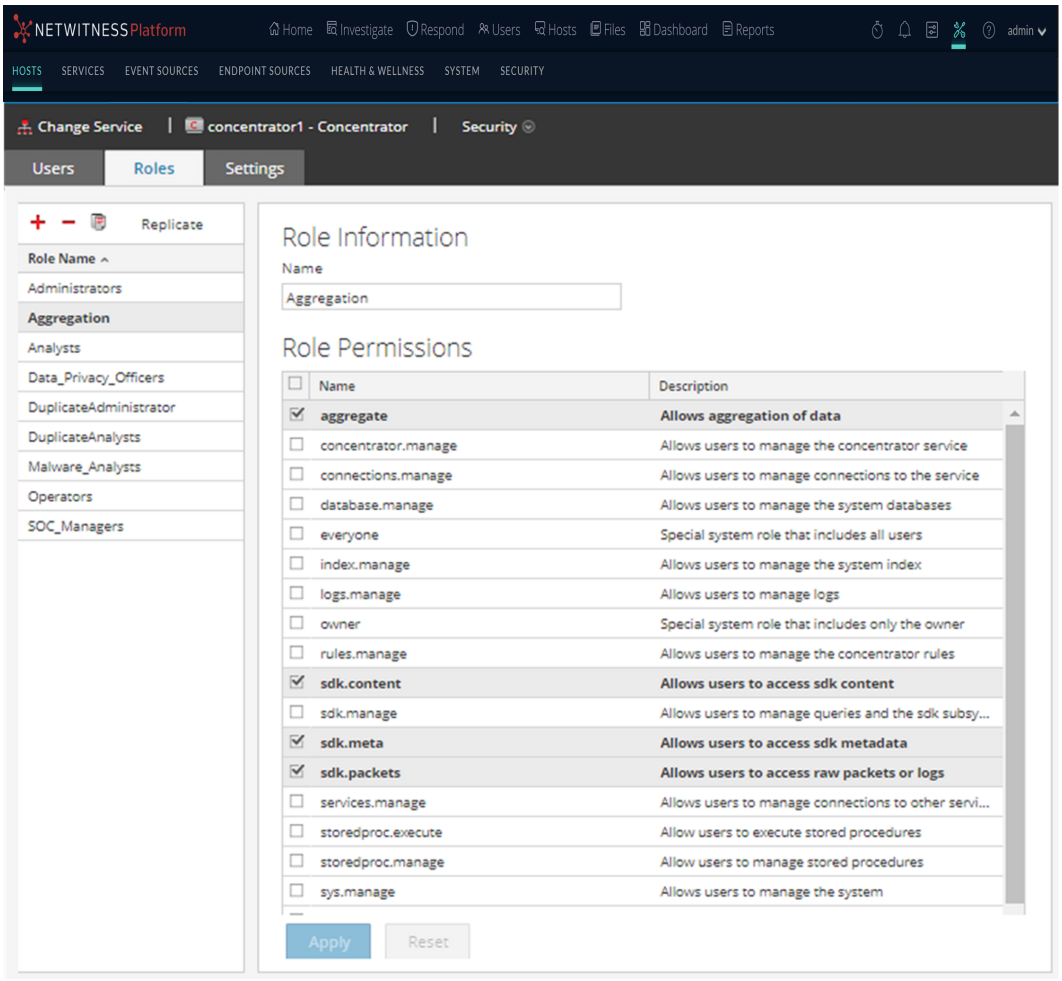
* You can perform these tasks in the current view.

Related Topics

- Duplicate or Replicate a Service Role
- Duplicate or Replicate a Service Role
- Services Security View - Users Tab

- Services Security View - Settings Tab
- Services View

Quick Look



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.

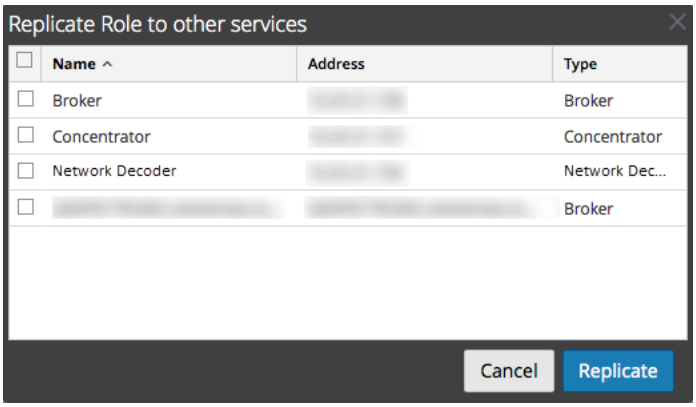
Role Name Panel

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`.

Feature	Description
Replicate	Pushes a role and its assigned permissions to other services. After you select a role and click **Replicate**, the Replicate Role to other services dialog is displayed. In the dialog, you can select the services where you want to replicate the role.

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



Role Information and Permissions Panel

The Role Information and Permissions panel defines role permissions.

There are two buttons:

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

Topics

- Services Security View - Service User Roles and Permissions
- Services Security View - Aggregation Role

Services Security View - 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 service user roles included with NetWitness to assign user permissions.

Related Topics

- Services Security View - Aggregation Role
- Services Security View - Roles Tab

Service User Roles

NetWitness has the following pre-configured service user roles.

Role	Assigned Permissions	Personnel/Account
Administrators	All permissions	NetWitness System Administrator

Aggregation	`aggregate`
	`sdk.content`
	`sdk.meta`
	`sdk.packets`
		You can use this role to create an Aggregation account.
		This role provides the minimum permissions necessary to perform aggregation of data. It is only available on NetWitness version 10.5 and later services.

Analysts, Malware_ Analysts, and SOC_ Managers	`sdk.meta`
	`sdk.content`
	`sdk.packets`
	`storedproc.execute`
		Users can use specific applications, run queries and view content for purposes of analysis.

Data_Privacy_ Officers	`sys.manage`
	`users.manage`
	`sdk.meta`
	`sdk.content`
	`sdk.packets`
	`sdk.manage`
	`logs.manage`
	`database.manage`
	`index.manage`
	`dpo.manage`
		Data Privacy Officer
		Data Privacy Officers have the `dpo.manage` permission on Network Decoders and Log Decoders.

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. 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.
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 Network 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.

Services Security View - Aggregation Role

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

Related Topics

- Services Security View - Service User Roles and Permissions
- Services Security View - Roles Tab

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

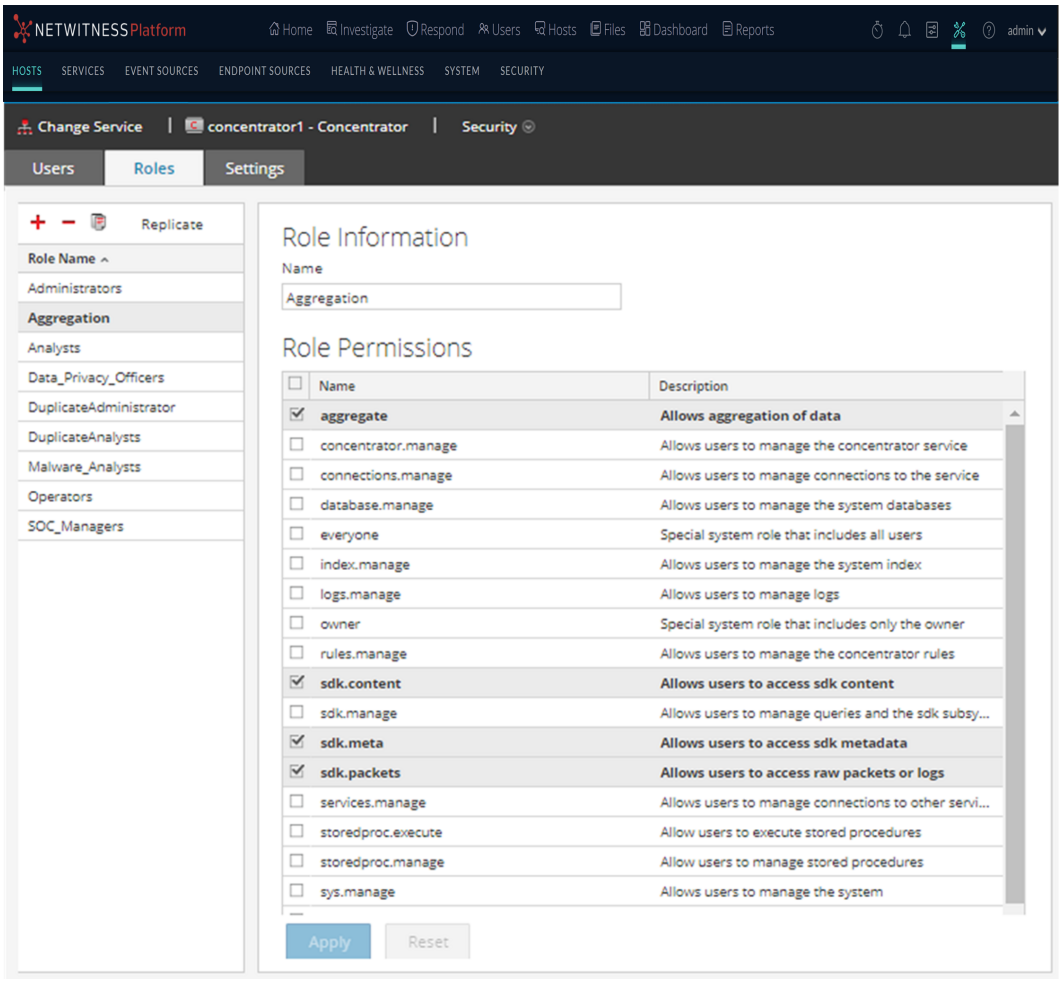
The Aggregation role is available only on NetWitness version 10.5 and later services and it can be used for an aggregation account. Members of this role or service users with these permissions can perform aggregation on Network Decoders, Concentrators, Archivers, and Brokers. The aggregate permission 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) > > **View** > **Security** > **Roles** tab.

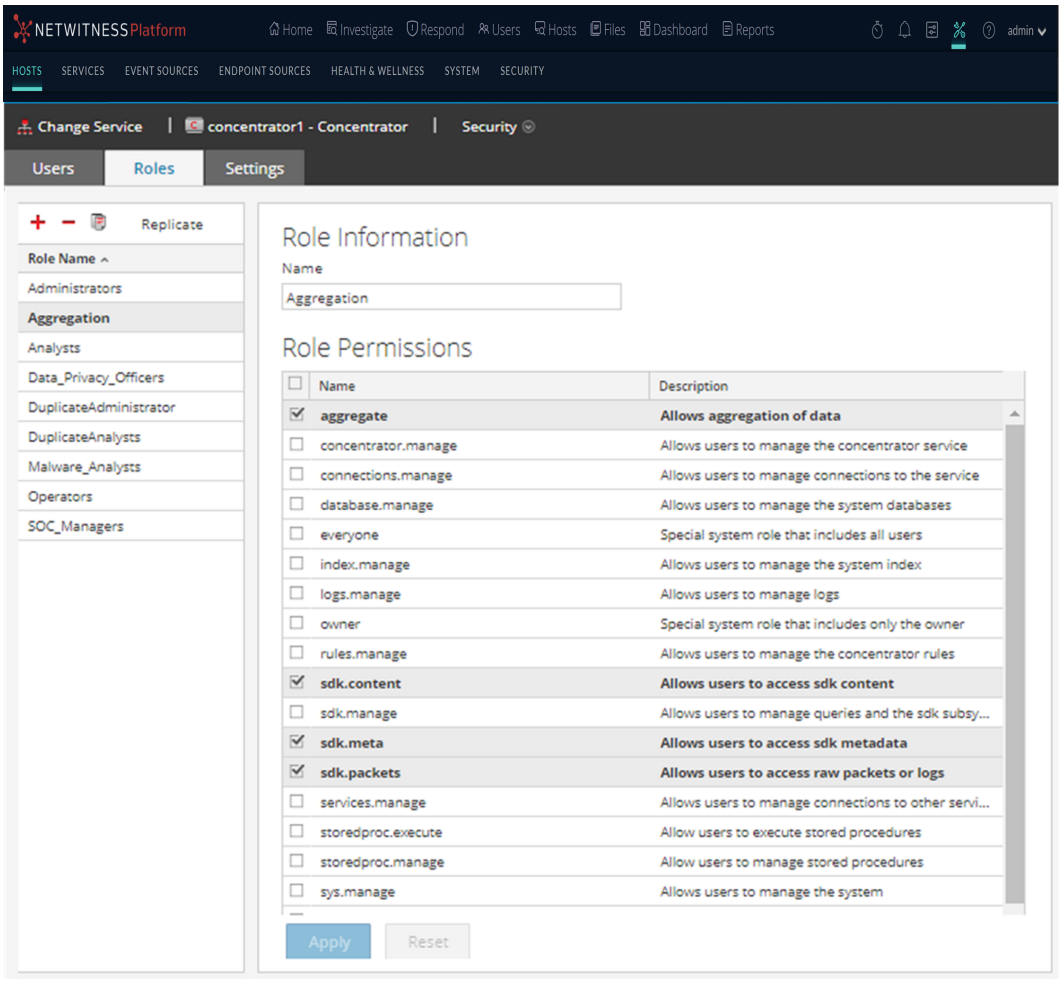
Procedures related to roles are described in Hosts and Services Maintenance Procedures. Services Security View - Service User Roles and Permissions provides detailed information on the pre-configured roles.

The following figure shows the permissions in the Aggregation role.



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, Network 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 metadata and content to privileged users. See the *Data Privacy Management Guide* for more information.

Workflow



What do you want to do?

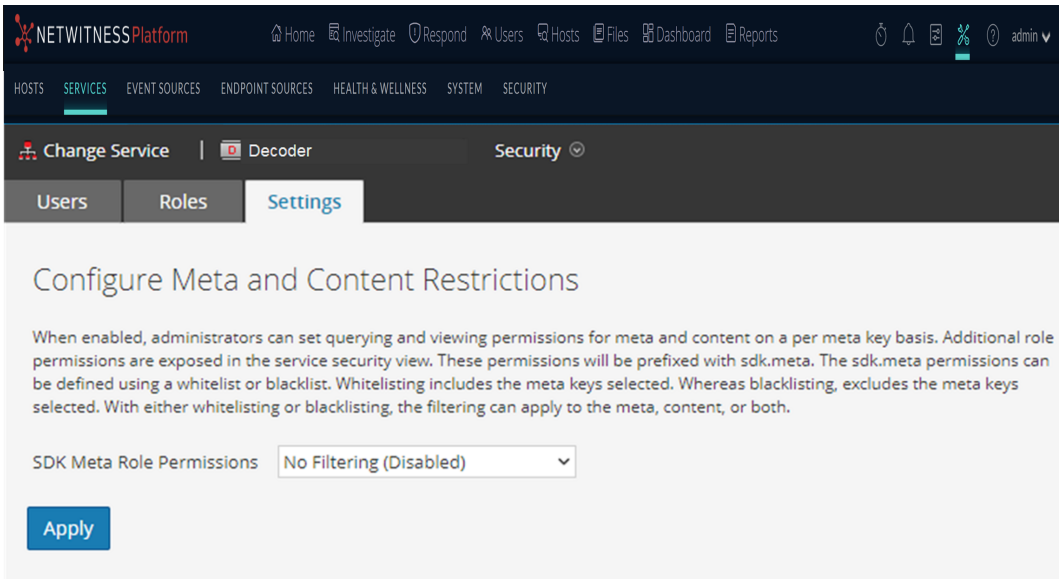
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	enable and configure system roles that define permissions on a per meta key basis for individual Brokers, Concentrators, Network Decoders, and Log Decoders.*	See the *System Security and User Management Guide* for more information.

* You can perform these tasks in the current view.

Related Topics

- Services Security View - Users Tab
- Services Security View - Roles Tab
- Services Security View

Quick Look



The Settings 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 metadata 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 metadata and content	Metadata and content for the specified SDK meta roles are white listed, or visible to users assigned the system role.
2	Whitelist only metadata	Metadata 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 metadata and content	Metadata and content for the specified SDK meta roles are black listed, or not visible to users assigned the system role.
5	Blacklist only metadata	Metadata 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.

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



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	monitor the status and operations of a service.*	See the *System Maintenance Guide*.
Administrator	chart statistical information for a service over a user-specified period of time.*	See the *System Maintenance Guide*.

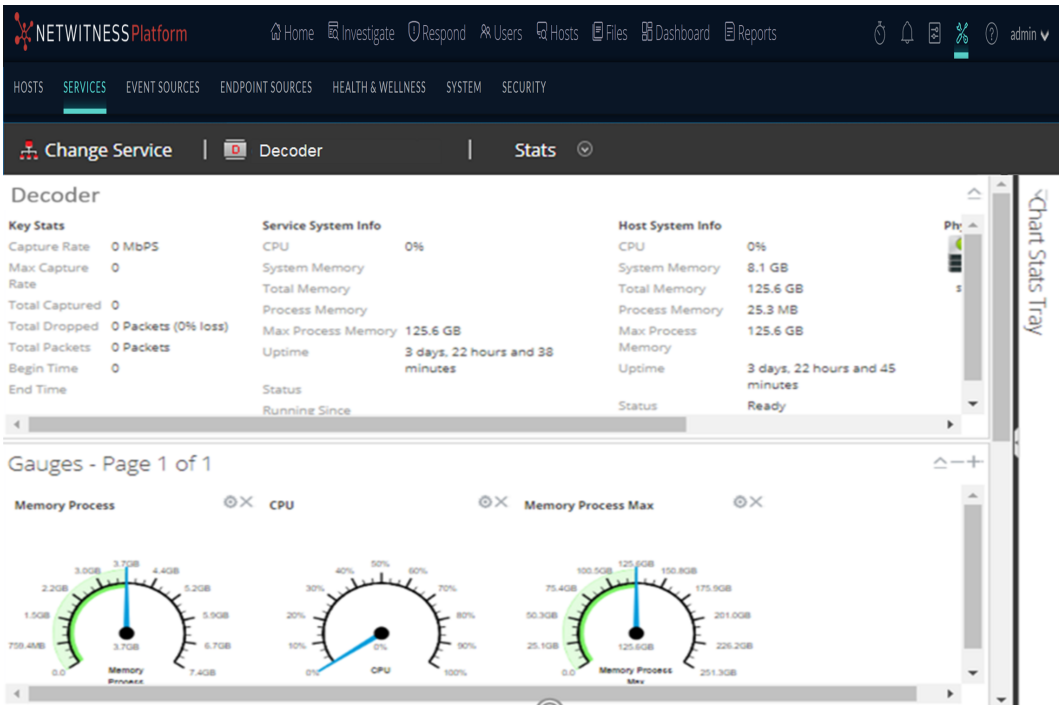
* You can perform these tasks in the current view.

Related Topics

- Edit Service Dialog
- Services Config View
- Services Explore View
- Services Logs View
- Services Security View
- Services System View
- Services View

Quick Look

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



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

- Summary Stats
- Gauges
- Timeline Charts
- Historical Timeline Charts
- Chart Stats Tray

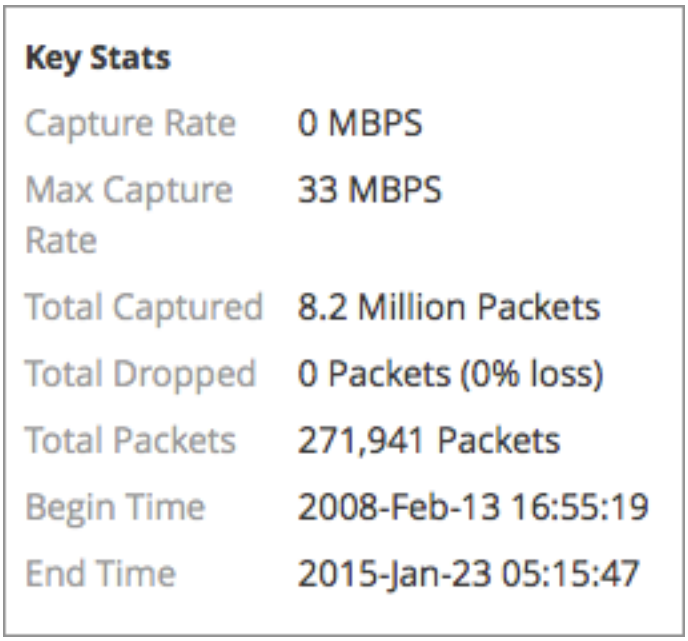
Summary Stats Section

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: Key Stats, Service System Info, Host System Info, Logical Drives, and Physical Drives. The **Key Stats** panel displays different statistics for different types of services. The remaining four panels in the Summary Stats section are the same for all types of services.

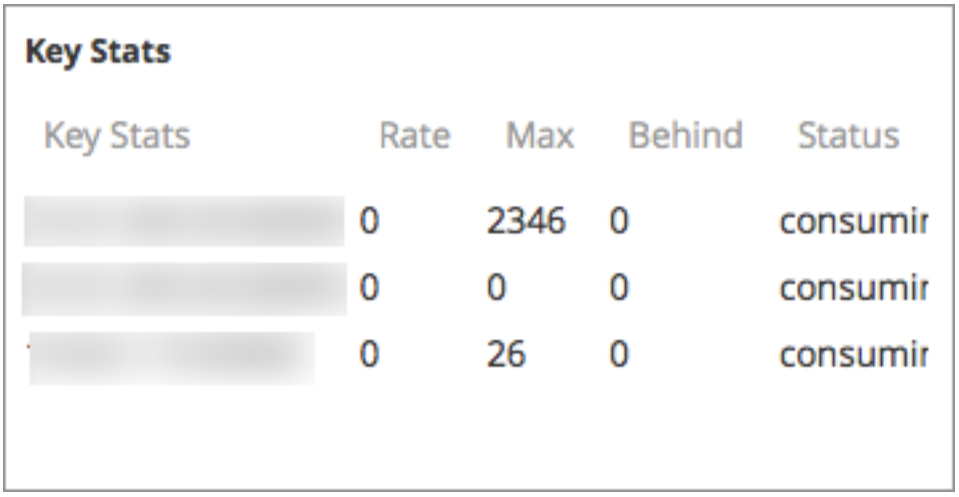
Key Stats

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

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

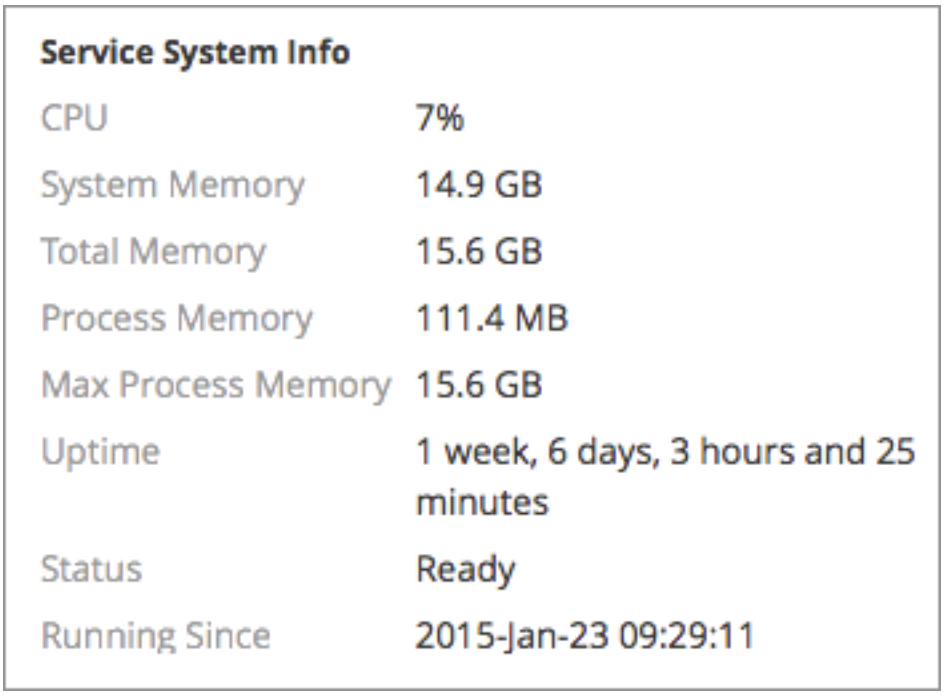


- A **Broker** or **Concentrator** aggregates data from multiple services. Therefore, the key statistics for all aggregate services are presented in a list. The columns in the list provide the service name, the capture rate, the maximum capture rate, the number of sessions behind (that need to be aggregated),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



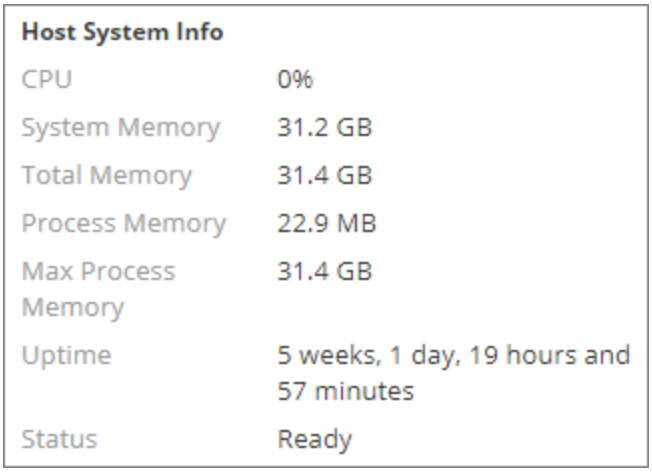
Service System Info

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



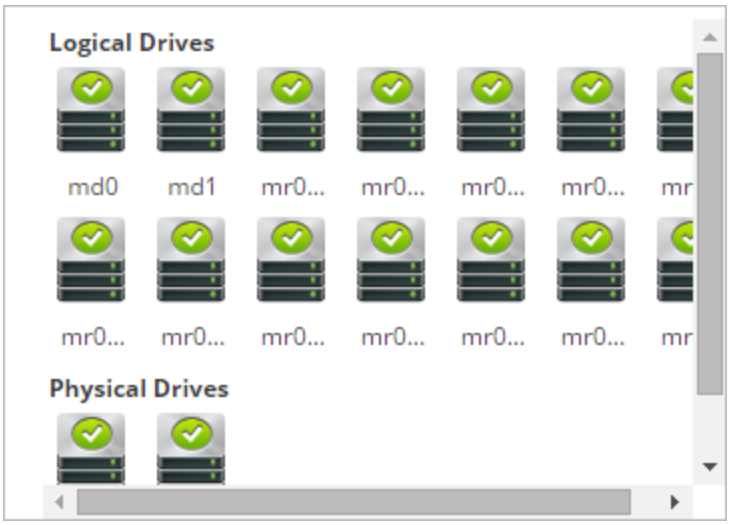
Host System Info

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



Logical Drives and Physical Drives

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



Drive Types and Status

Drive Type	Description	Comments	Status Options
`sd`	SCSI block device	Directly connected SAS, SATA MegaRAID volumes.	Green: OK Red: FAIL
`ld`	MegaRAID Logical Volume	Defined in BIOS or with MegaCLI tool.	Green: OK Yellow: DEGRADED/BUILDING Red: FAIL
`pd`	MegaRAID Physical Disks	Not directly exposed to Linux.	Green: OK Red: FAIL
`md`	Linux software RAID Volume		Green: OK Yellow: DEGRADED/BUILDING Red: FAIL

Gauges

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

Timeline Charts

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 Services Stats View - Timeline Charts for details on configuring timelines.

Historical Timeline Charts

Historical timeline charts display statistics for session size, sessions, and packets in a historical timeline. This is the same for all types of services. Only the display name, begin date, and end date. See Services Stats View - 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 Services Stats View - Chart Stats Tray for a detailed description.

Topics

- Services Stats View - Chart Stats Tray
- Services Stats View - Gauges
- Services Stats View - Timeline Charts

Services Stats View - Chart Stats Tray

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.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	customize the monitored statistics for individual services.*	See the *System Maintenance Guide*.

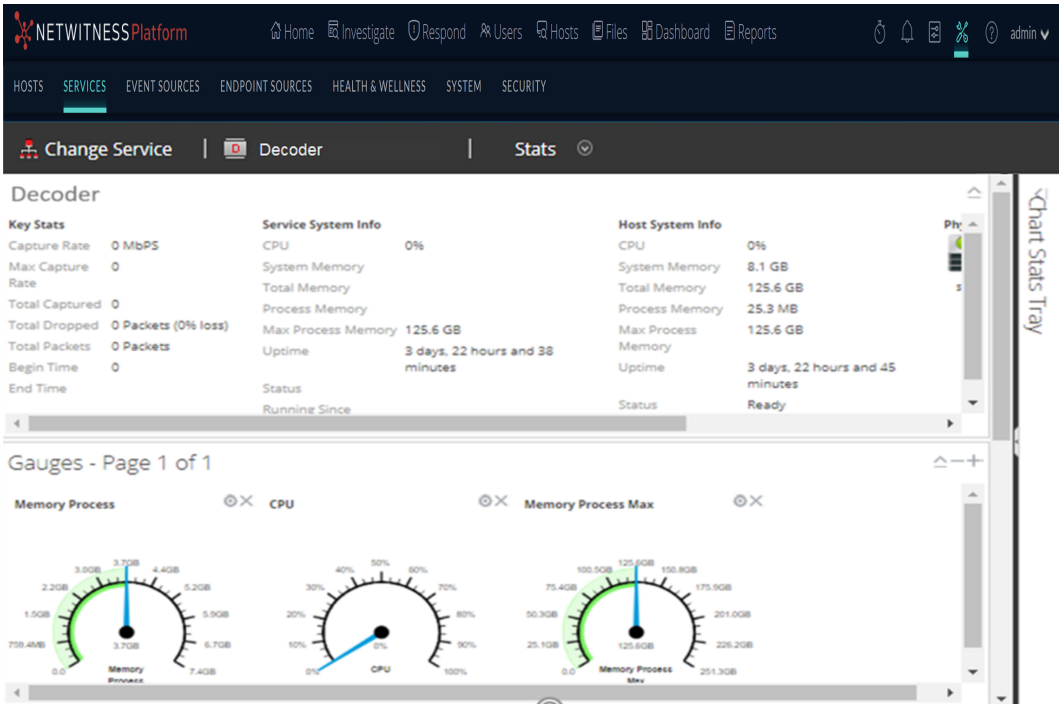
* You can perform these tasks in the current view.

Related Topics

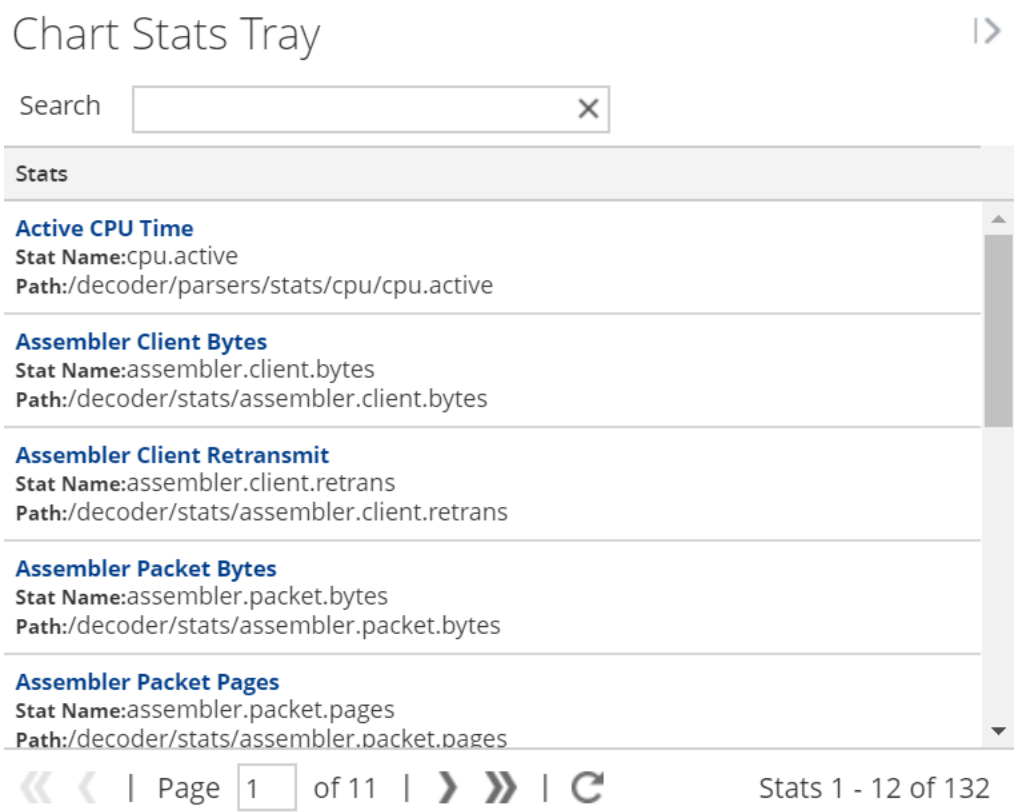
- Services Stats View - Gauges
- Services Stats View - Timeline Charts
- Services Config View

Quick Look

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



To view the Chart Stats Tray, click on the  to expand the Chart Stats Tray.



The Chart Stats Tray has different statistics for different types of services. In the example above, 132 statistics are available for the Network Decoder. The following table describes features of the Chart Stats Tray.

Feature	Description
	Click to expand the panel horizontally.
	Click to collapse the panel horizontally.
Search	Type a search term in the field and press **RETURN**. Statistics that match are displayed with the matching word highlighted.
	Click to go to the first page.
	Click to go to the previous page.
Page 1 of 11	Type a page number in the Page field.
	Click to go to the next page.
	Click to go to the last page.

Feature	Description
	Click to refresh the view.
Stats 1 - 12 of 132	Displays the range of statistics being displayed. The total number statistics varies by service type.

Services Stats View - Gauges

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.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	view statistics in the form of an analog gauge.*	See the *System Maintenance Guide*.

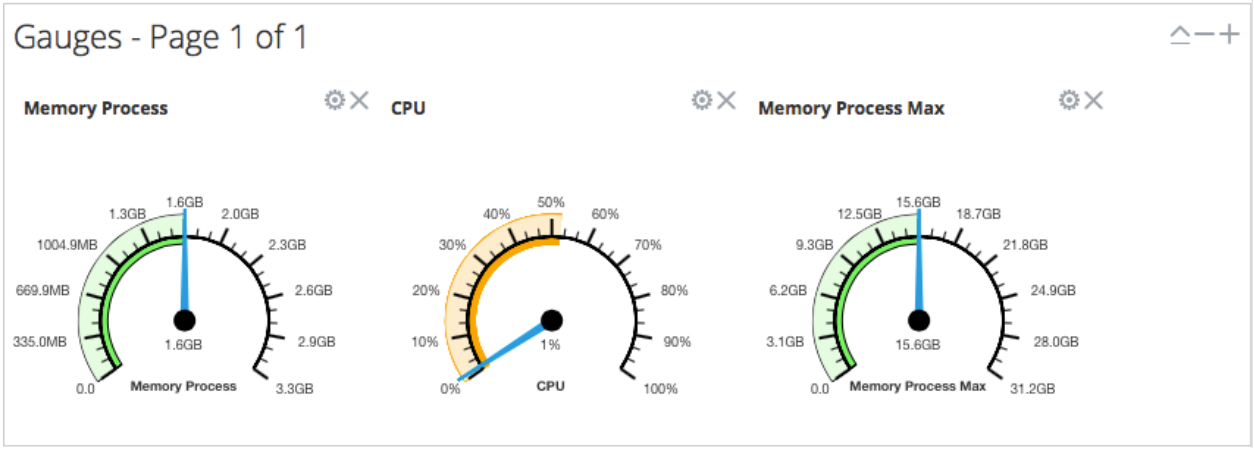
* You can perform these tasks in the current view.

Related Topics

- Services Stats View - Chart Stats Tray
- Services Stats View - Timeline Charts
- Services Config View

Quick Look

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



The default gauges show these statistics:

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

The controls in the Gauges title bar and in each gauge are the standard dashlet controls. Dashlets are the parts that make up a dashboard.



- In the Gauges title bar (from left to right), you can collapse/expand, delete a page, add a page, page backward, and page forward.
- In each gauge, you can edit properties ( ) and delete ( ) the gauge.

Services Stats View - Timeline Charts

The Services Stats view Timeline Charts sections 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 or Historical 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.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	view statistics in the form of a current or historical timeline.*	See the *System Maintenance Guide*.

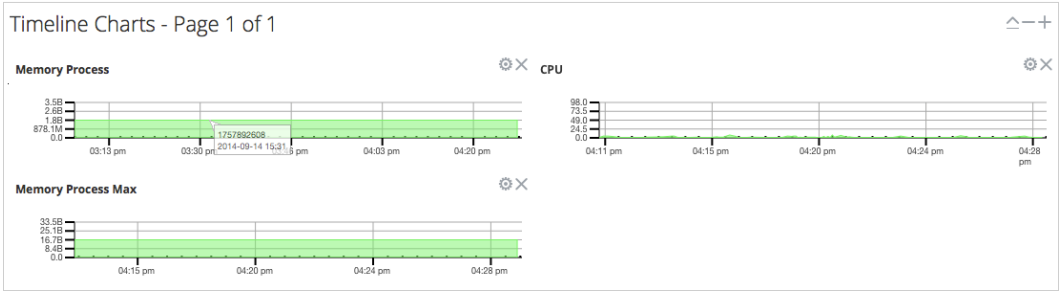
* You can perform these tasks in the current view.

Related Topics

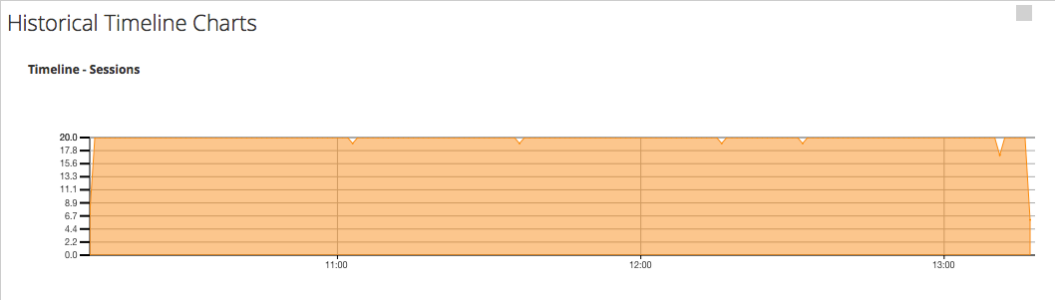
- Services Stats View - Chart Stats Tray
- Services Stats View - Gauges
- Services Config View

Quick Look

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. The Historical Timeline Charts title bar and timelines have the same controls.



- In the Timeline Charts title bar (from left to right), you can collapse/expand, delete a page, add a page, page backward, and page forward.
- 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.

Services System View

This topic introduces features in the Services System view using Decoders (Network Decoder and Log Decoder) as an example. See the appropriate configuration guides for other services (for example, the *NetWitness Broker and Concentrator Configuration Guide*) for details on their respective **(Admin) > Services > System** views.

A Log Decoder is a special type of Decoder, and is configured and managed in a similar way to a Network Decoder. Therefore, most of the information in this section refers to both types of Decoders. Differences for Log Decoders are noted. For more information on Decoders, see the *Decoder Configuration Guide*.

Workflow



What do you want to do?

User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	view system and session information about a service.*	See the *System Maintenance Guide*.

* You can perform these tasks in the current view.

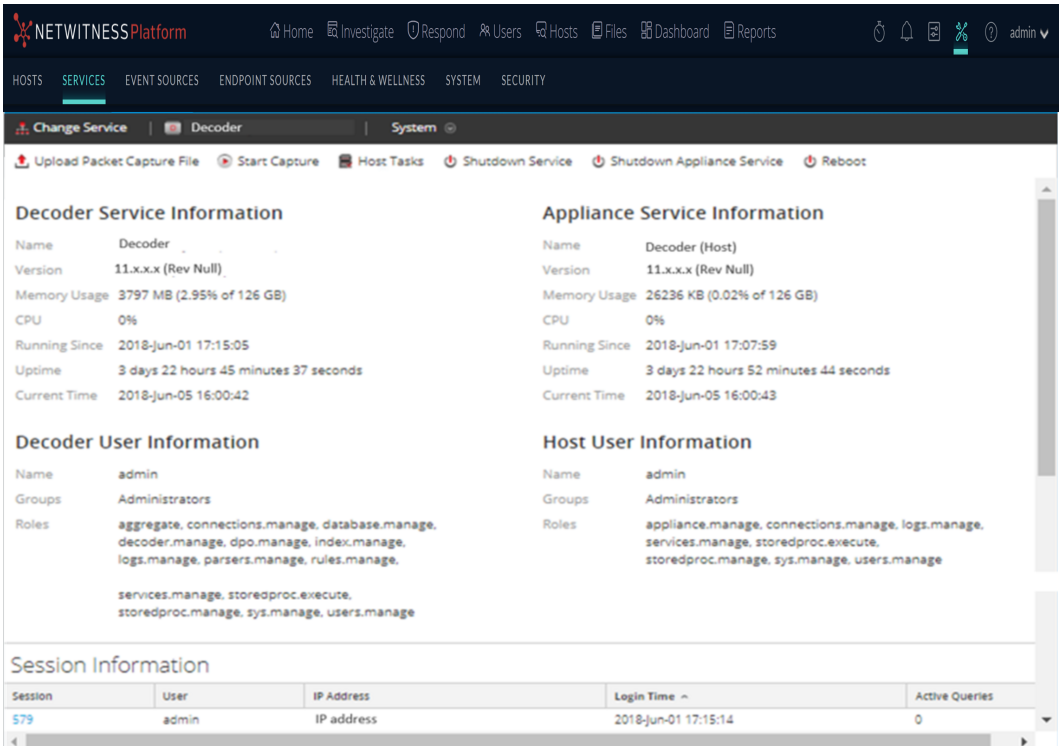
Related Topics

- Edit Service Dialog
- Services Config View
- Services Explore View
- Services Logs View
- Services Security View

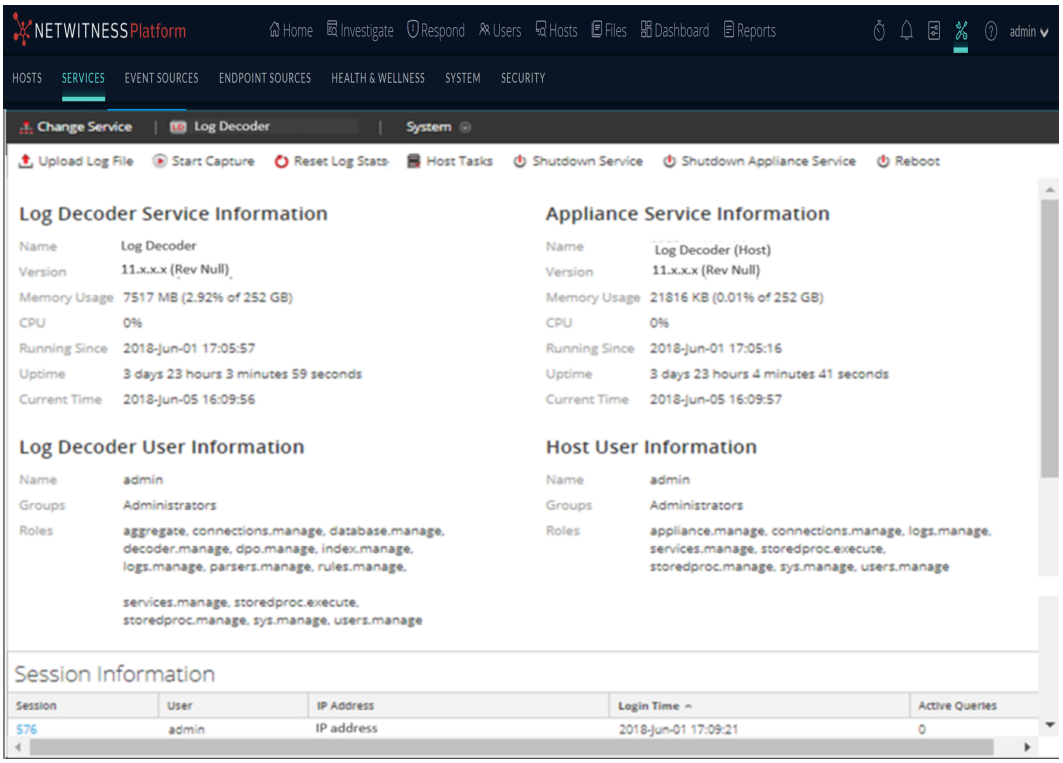
- Services Stats View
- Services View

Quick Look

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



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



Services Info Toolbar

The following toolbars show the options specific to Log Decoders (top) and Network Decoders (bottom).





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

Related Topics

- Services System View - Host Task List Dialog

Services Topology View

This topic introduces the services topology, a hierarchical view of the NetWitness Platform core services depicting the collection and aggregation in your deployment.

This visualization displays the topology for the Broker, Concentrator, Log Decoder, Packet Decoder, Hybrids, ESA and Log Collector. You can view the services that are online and details of each node.

Workflow

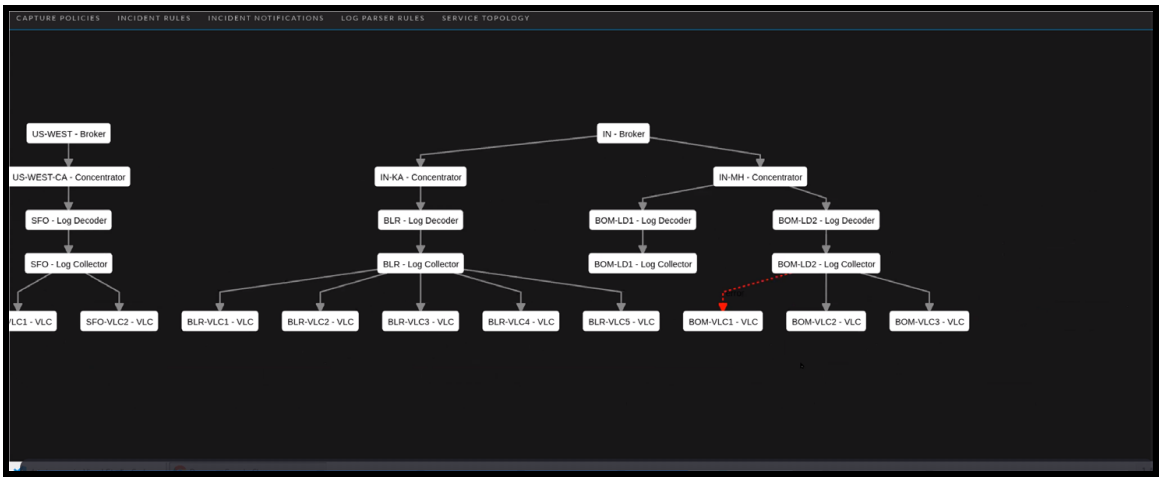


What do you want to do?

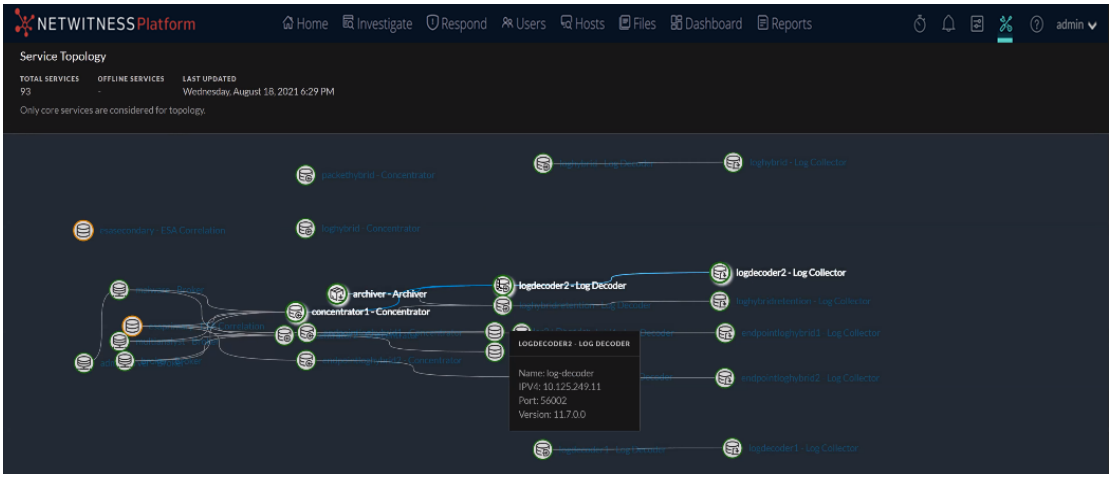
User Role	I want to...	Documentation
Administrator	maintain a service.	Maintaining Services

Quick Look

The following figure shows an example of how each service is aggregating data in a hierarchy along with which services are online or offline.



The following figure shows the details of a node. When you hover over any of the services, additional details such as name, IP version, Port number and Version number are displayed.



Action	Description
Node	Displays a dialog that provides name, IP version, Port number and Version number.
Search	Enter the service name to locate a specific service.

Services System View - Host Task List Dialog

In the NetWitness 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.

Workflow



What do you want to do?

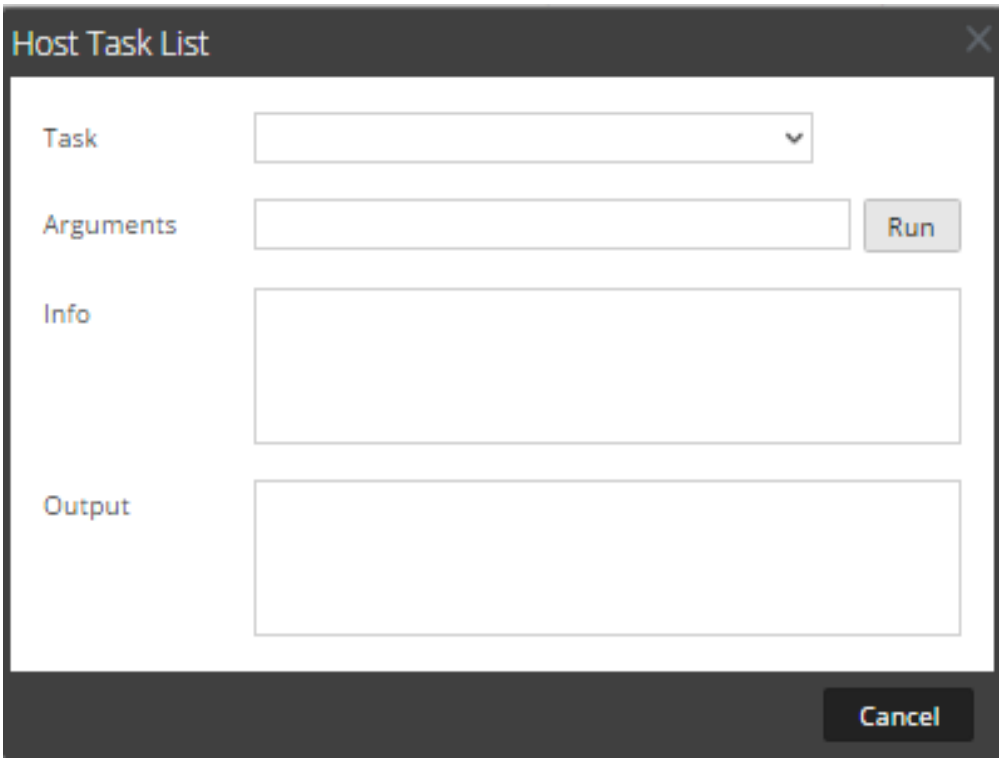
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	manage host-related tasks and host communications with the network.*	Hosts and Services Maintenance Procedures

* You can perform these tasks in the current view.

Related Topics

- Services System View

Quick Look



The table below describes the Host Task List 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.

Task	Description
Delete Filesystem Monitor	Stops monitoring the storage services attached to the specified filesystem. See Add and Delete a Filesystem Monitor.
Reboot Host	Shuts down and restarts the host. See Reboot a Host.
Set Host Built-in Clock	Sets the local host clock. See Set Host Built-In Clock.
Set Host Hostname	This method of changing the hostname is deprecated in NetWitness 10.6. To edit a hostname, see Edit or Delete a Service.
Set Network Time Source	Sets the clock source for this host. See Set Network Time Source.
Set Syslog Forwarding	Enables or disables syslog forwarding from a remote server to the selected service. See Set Syslog Forwarding.
Show Network Port Status	Shows the network interface information for a host. See Show Network Port Status.
Show Serial Number	Gets the host serial number. See Show Serial Number.
Shut Down Host	Shuts down the physical host and the host remains off. See Shut Down Host.
Start Service	Starts a service on this host. See Stop and Start a Service on a Host.
Stop Service	Stops a service on this host. See Stop and Start a Service on a 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 NetWitness Core services.

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

Aggregation Configuration Parameters

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

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

Configuration Path	/concentrator/config or /archiver/config
aggregate.time.window	Displays the maximum +/- time window, in seconds, that all services must be inside before another round of aggregation is requested. Zero turns off time window. Change takes effect immediately.
consume.mode	Determines if the concentrator can only aggregate locally or over a network, based on licensing restrictions. Change takes effect on service restart.
export.enabled	Allows export of session data, if enabled. Change takes effect on service restart.
export.expire.minutes	Lists the number of minutes before export cache files are expired and flushed. Change takes effect immediately.
export.format	Determines the file format used during data export. Change takes effect on service restart.
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-separated list of fields. * means all fields. * and field list means all fields except the listed fields. Just the field list means only those fields are included. Change takes effect immediately.
export.remote.path	Displays the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.rollup	Determines the rollup interval for export files. Change takes effect on service restart.
export.session.max	Displays the maximum sessions per exported file. For export file types that cache, this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.size.max	Displays the maximum bytes per exported file. For export file types that cache, this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.usage.max	Displays the maximum percentage of cache space used before stopping aggregation. Zero is no limit. Change takes effect immediately.
heartbeat.error	Lists the number of seconds to wait after a service error before attempting a service reconnect. Change takes effect immediately.
heartbeat.interval	Lists the number of milliseconds between heartbeat service checks. Change takes effect immediately.

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

Appliance Service Configuration Parameters

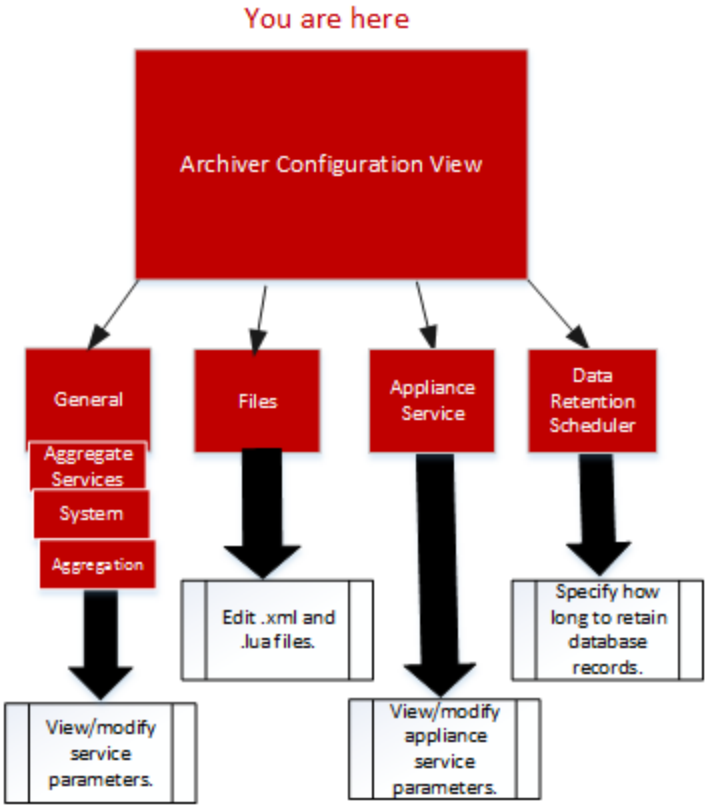
The NetWitness Core Appliance service provides hardware monitoring on legacy NetWitness hardware. The list describes the Appliance Configuration parameters.

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

Archiver Service Configuration View

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

Workflow



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

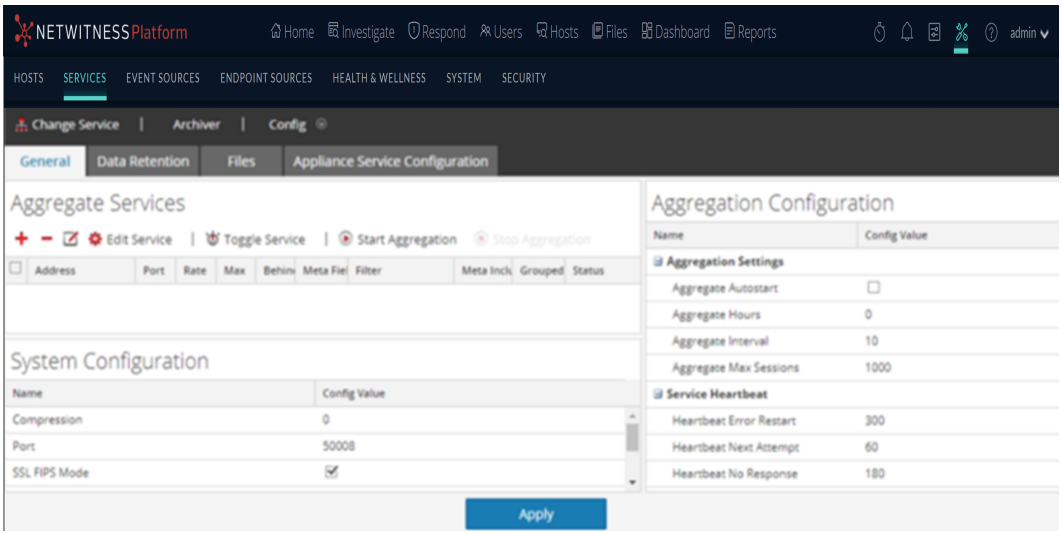
Quick Look

To access the Services Config view:

1. In **NetWitness**, 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

The following list 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 "Database Configuration Nodes" in the *NetWitness Core Services Database Tuning Guide*.
Index	`/index/config`
`index.dir`	The directory where the broker device mapping files are stored. Change takes effect on service restart.
`language.filename`	The index language specification (XML) that is loaded on startup. Change requires service restart.
Logs	`/logs/config` refer to Core Service Logging Configuration Parameters
REST	`/rest/config` refer to REST Interface Configuration Parameters
SDK	`/sdk/config` refer to "SDK Configuration Nodes" in the *NetWitness Core Services Database Tuning Guide* and NetWitness Platform Core Service system.roles Modes
Services	`/services/<service name>/config` refer to Core Service-to-Service Configuration Parameters

Broker Parameter Field	Description
System	`/sys/config` refer to Core Service System Configuration Parameters

Concentrator Service Configuration Parameters

The following list describes the Concentrator configuration parameters.

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

Core Service Logging Configuration Parameters

The following table describes the logging configuration parameters for all NetWitness Core services. Logging configuration is the same for all Core services.

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.

Logs Configuration Folder	/logs/config
log.snmp.agent	Sets a remote SNMP Trap Receiving agent.
snmp.trap.version	Sets the SNMP version (2c or 3) to be used for gets and traps.
snmpv3.engine.boots	Displays the SNMPv3 engine boots count. This field auto-increments on startup and should not normally need to be set by the user.
snmpv3.engine.id	Sets the SNMPv3 engine ID, which is 10-64 hexadecimal digit number optionally preceded by 0x. You can add suffix values at the end of the engine ID for each of the SA Core services running on the same host. For example, if the generated Engine ID for the SA Core host is 0x1234512345, you can set the Engine ID for the Decoder service as 0x123451234501 and set 0x123451234504 for the Appliance service.
snmpv3.trap.auth.local.key	Sets the SNMPv3 Trap Authentication Local Key, which is a 16 or 20 hexadecimal digit number (depending on which authentication protocol is used) preceded by 0x. For MD5, the key is 16 hexadecimal digits, while SHA uses 20 hexadecimal digits. You can use any desired algorithm to generate the local keys. It is recommended that a generation method involving randomness be used as opposed to selecting key values manually.
snmpv3.trap.auth.protocol	Displays the SNMPv3 Trap Authentication Protocol (none, MD5 or SHA).
snmpv3.trap.priv.local.key	Sets the SNMPv3 Trap Privacy Local Key, which is a 16 hexadecimal digit number preceded by 0x.
snmpv3.trap.priv.protocol	Displays the SNMPv3 Trap Privacy Protocol (none or AES).
snmpv3.trap.security.level	Displays the SNMPv3 Trap Security Level, which indicates whether authentication and privacy are used or not. Possible values are noAuthNoPriv, authNoPriv, or authPriv.
snmpv3.trap.security.name	Sets the SNMPv3 Trap Security Name used during SNMPv3 trap authentication.
syslog.size.max	Displays the maximum size of a log sent to syslog (some syslog daemons have issues with very large messages). Zero means no limit. Change takes effect immediately.

Core Service-to-Service Configuration Parameters

This topic lists and describes the configuration parameters that control how a Core service connects to another Core service. For example, when a Concentrator connects to a Network Decoder, the connection parameters 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 Network 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 list 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

The following list describes the System configuration parameters that are common to all NetWitness Core services.

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.

System Configuration Folder	/sys/config
service.name.override	Displays an optional service name used by upstream services for aggregation in lieu of hostname.
ssl	Encrypts all traffic using SSL, if enabled. Change takes effect on service restart.
stat.compression	Compresses stats as they are written to the database, if enabled. Change takes effect on service restart.
stat.dir	Displays the directory where the historical stats database is stored (separate multiple dirs with semicolon). Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
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 Configuration Parameters

The following list describes the configuration parameters that are identical on both Network Decoder and Log Decoder services.

Configuration Path	<service>/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 pre-cache 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.

Configuration Path	<service>/config
assembler.session.flush	Flushes sessions either when they are complete, or when they are parsed. 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.
capture.device.params	Displays capture service specific parameters. Change takes effect on service restart. The parameters understood by this field are specific to the currently selected capture device. If any of the parameters are not recognized by the current capture device, they are ignored. On Log Decoders, there is only the Log Events capture device. It accepts some optional parameters. • use-envision-time: If this is set to 1, the time metadata 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.

Configuration Path	<service>/config
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.
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-separated list of fields. * means all fields. * plus field list means all fields BUT listed fields. Just field list means only those fields are included. 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.
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.

Configuration Path	<service>/config
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.

Network Decoder Service Configuration Parameters

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

Decoder Parameter Field	Description
Decoder	/decoder/config refer to Decoder Configuration Parameters.
Database	/database/config refer to "Database Configuration Nodes" in the *NetWitness Core Database Tuning Guide*.
Index	/index/config refer to "Index Configuration Nodes" in the *NetWitness Core Database Tuning Guide*.
Logs	/logs/config refer to Core Service Logging Configuration Parameters.
REST	/rest/config refer to REST Interface Configuration Parameters.
SDK	/sdk/config refer to "SDK Configuration Nodes" in the *NetWitness Core Database Tuning Guide* and NetWitness Platform Core Service system.roles Modes.
System	/sys/config refer to Core Service System Configuration Parameters.

Log Decoder Service Configuration Parameters

This topic lists and describes the available configuration parameters for Log Decoder configuration settings.

Log Decoder Setting Field	Description
Database	/database/config refer to "Database Configuration Nodes" in the *NetWitness Core Database Tuning Guide*.

Log Decoder Setting Field	Description
Decoder	`/decoder/config` refer to Decoder Configuration Parameters.
Index	`/index/config` refer to "Index Configuration Nodes" in the *NetWitness Core Database Tuning Guide.*
Logs	`/logs/config` refer to Core Service Logging Configuration Parameters.
REST	`/rest/config` refer to REST Interface Configuration Parameters.
SDK	`/sdk/config` refer to "SDK Configuration Nodes" in the *NetWitness Core Database Tuning Guide*and NetWitness Platform Core Service system.roles Modes.
System	`/sys/config` refer to Core Service System Configuration Parameters.

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`
URLSCAN	Scans for text that appears to be a URL 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`

Parser Name	Description	Configuration Parameters
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`

Log Tokenizer Configuration Parameters.

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

Log Decoder Parser Setting Field	Description
token.unicode	This boolean setting controls whether unicode classification rules are applied when classifying characters according to the token.char.classes setting. When 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. When this is set to false, 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

The following list describes the available configuration parameters for the REST interface built in to all NetWitness Core Services.

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.
ssl	Encrypts all REST traffic using SSL, if enabled. The default system means use setting from /sys/config/ssl. Change takes effect on service restart.

NetWitness Platform Core Service system.roles Modes

All NetWitness Platform 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 metadata 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 Platform user interface (see "Data Privacy Tab" 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 metadata, 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

Centralized Service Configuration via Policy Settings

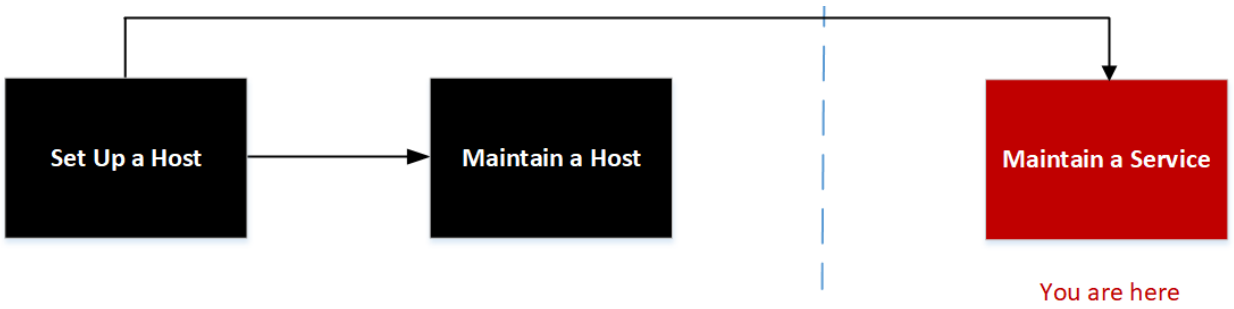
This topic introduces the available centralized service configuration settings for Concentrators, Decoders and Log Decoders services.

Centralized Service Configuration – Groups Tab

Note: The information in this topic applies to NetWitness Platform Version 11.7 and Later.

The  (**Configure**) > **Policies** view contains two tabs: **Groups** and **Policies**.

Workflow



What do you want to do?

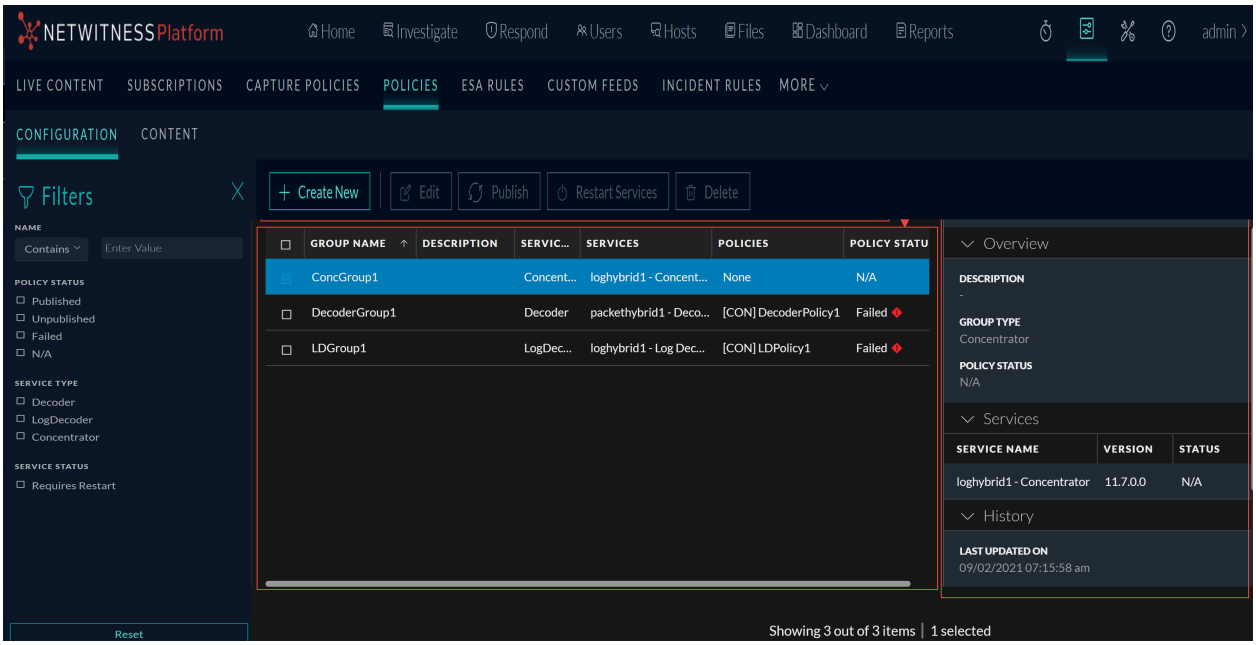
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services
Administrator	Centrally Create and Maintain Service Groups.*	Hosts and Services Maintenance Procedures

* You can perform these tasks in the current view.

Related Topics:

- Hosts and Services Set Up Procedures
- Hosts and Services Maintenance Procedures

Quick Look



Below is an example of the **Groups** tab:

The following table describes the Groups tab.

1	**Toolbar**
	• **Create New**- Lets you create a new group. For more information, see "Create a Group" in the Centralized Service Configuration via Policy.
	• **Edit** – Lets you edit the group. For more information, see "Managing Policies and Groups" in the Centralized Service Configuration via Policy.
	• **Publish** – Publishes selected groups.
	• **Restart Services** – Restarts the service associated with the selected group. This option is disable if:
	  ◦ There are no services in the group.
	  ◦ No service restart is required.
	• **Delete**- Deletes the selected groups.

2 **Filter Pane**

- **Filters**: You can filter groups based on Policy Type and Policy Status, Service Type and Service Status.

  To hide, click the  icon at the top-right of the panel. To display if hidden, click the  icon in the toolbar.

- **Reset**: Removes the currently applied filter criteria.

For more information, see "Filter Groups" in the Centralized Service Configuration via Policy.

3 **Group List Pane**

- **Group Name** – Name of the group.
- **Description** – Description of the group.
- **Service Type** – Displays the service type to which the group is applied.
- **Services** – Displays the service to the which the group is applied.
- **Policies** – Displays the policy to which the group is applied.
- **Policy Status** – Status of the policy. The values are: Published, Unpublished, Failed, N/A.

You can also sort on any column. If you mouse over a column header, a sort icon is displayed:  . Click the icon to sort by the selected column.

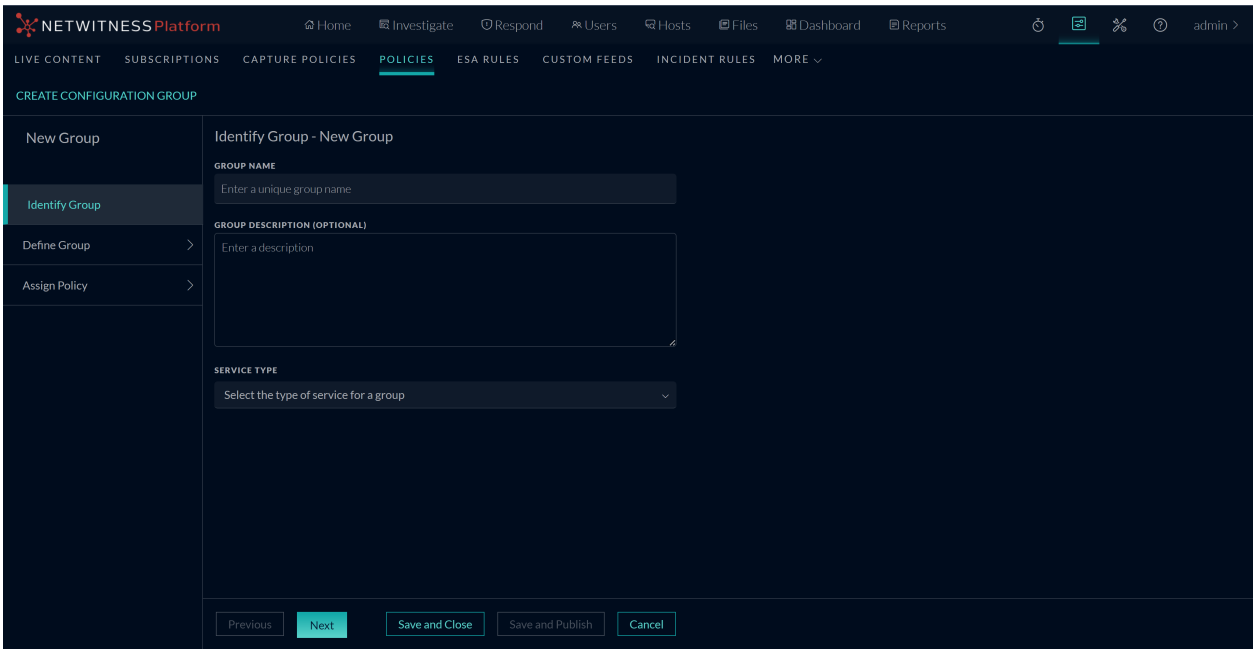
4 **Groups Details Panel**

Displays the properties of the selected group.

Note: Click the row to view the Properties panel for a group.

Create Group Dialog

Below is an example of the Create Group dialog.

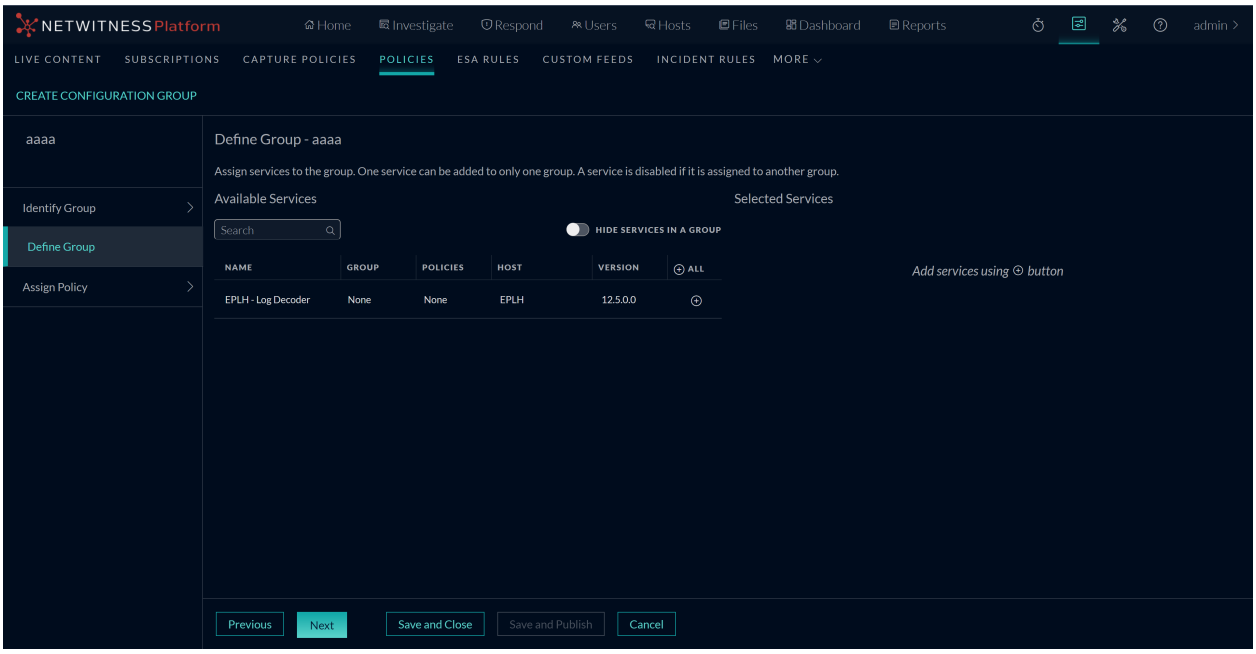


The table describes the information and options in the Create Group dialog.

Field	Description
Group Name	Name of the group. The name should be unique.
Group Description (Optional)	Description of the group. Description should not exceed 8000 characters.
Service Type	Select the type of service for a group. Available options are Log Decoder, Decoder, and Concentrator.
Save and Close	Saves the settings and closes the Create Group dialog.

Define Group Dialog

Below is an example of the define group dialog.



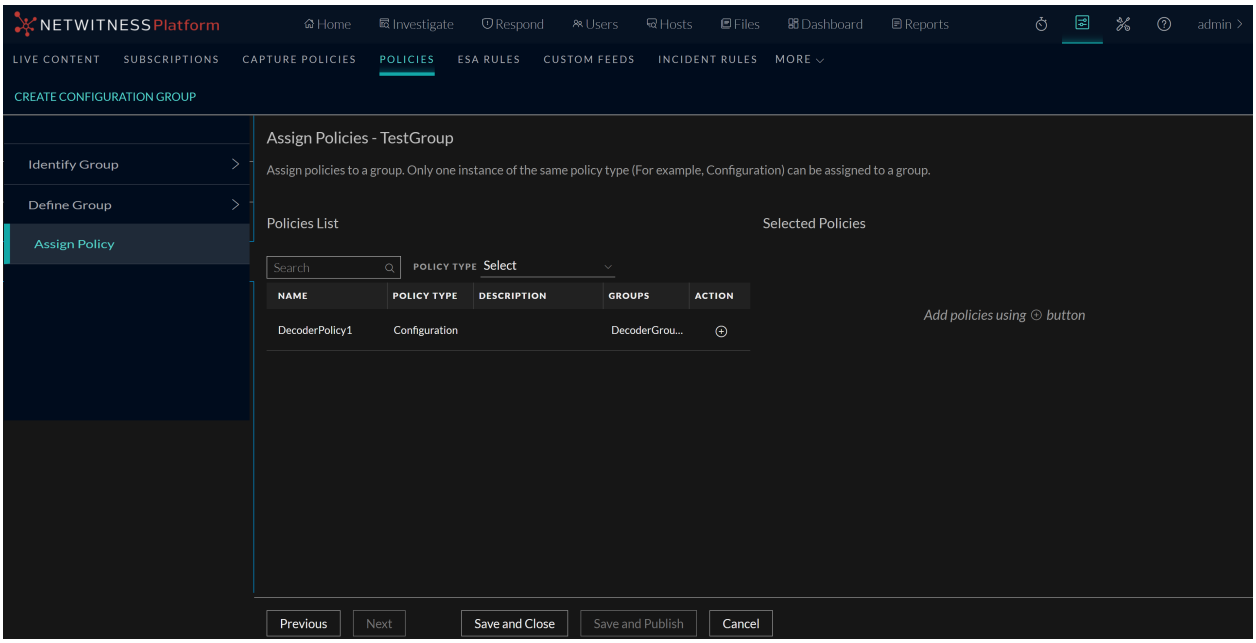
The table describes the information and options in the Define Group dialog.

Field	Description
Service List	Displays the list of services associated with the selected service type. The following describes services list: • **Service name** – Name of the service. • **Service type** – Displays the service type of the service. • **Group** – Name of the group. • **Policies** – Displays the policies associated with the service. • **Host** – Host name of the service. • **Version** – Service version. • **All** – Lets you to add services to the group. You can either click  to add all services or click  to add specific service.

Field	Description
Hide Services in a Group	Displays the services that is not assigned to any group. By default, this option is disabled.
Selected Services	Displays the list of selected services for the group.
Save and Close	Saves the setting and closes the Define Group dialog.
Save and Publish	Saves and publishes the created group. **Note:** This option is disabled if you have not: - Assigned services - Assigned policies

Assign Policy Dailog

Below is an example of Assign Policy dialog.



The following table describes assign policy dialog:

Field	Description
Policies List	Displays the list of policies associated with the group. The following describes policies list: • **Name** – Name of the policy. • **Policy Type** – Displays the policy type. • **Description** – Description of the policy. • **Groups** – Groups associated with the policy. • **Action** - Click  to add policies to the group.
Policy Type	Select the policy type from the drop-down list.
Selected Policies	Displays the list of selected policies for the group.
Save and Close	Saves the settings and closes the Create Group dialog.

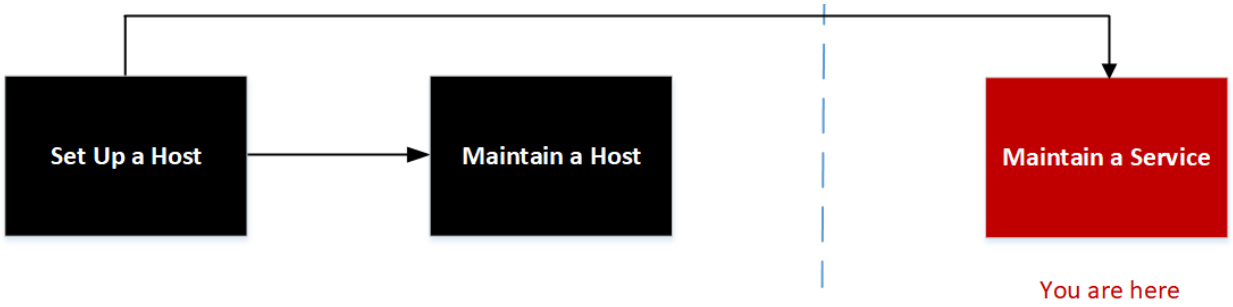
Field	Description
Save and Publish	Saves and publishes the created group. **Note:** This option is disabled if you have not: - Assigned services. - Assigned policies.

Centralized Service Configuration – Policies Tab

Note: The information in this topic applies to NetWitness Platform Version 11.7 and Later.

The  (**Configure**) > **Policies** view contains two tabs: **Groups** and **Policies**.

Workflow



Related Topics:

- Hosts and Services Set Up Procedures
- Hosts and Services Maintenance Procedures

What do you want to do?

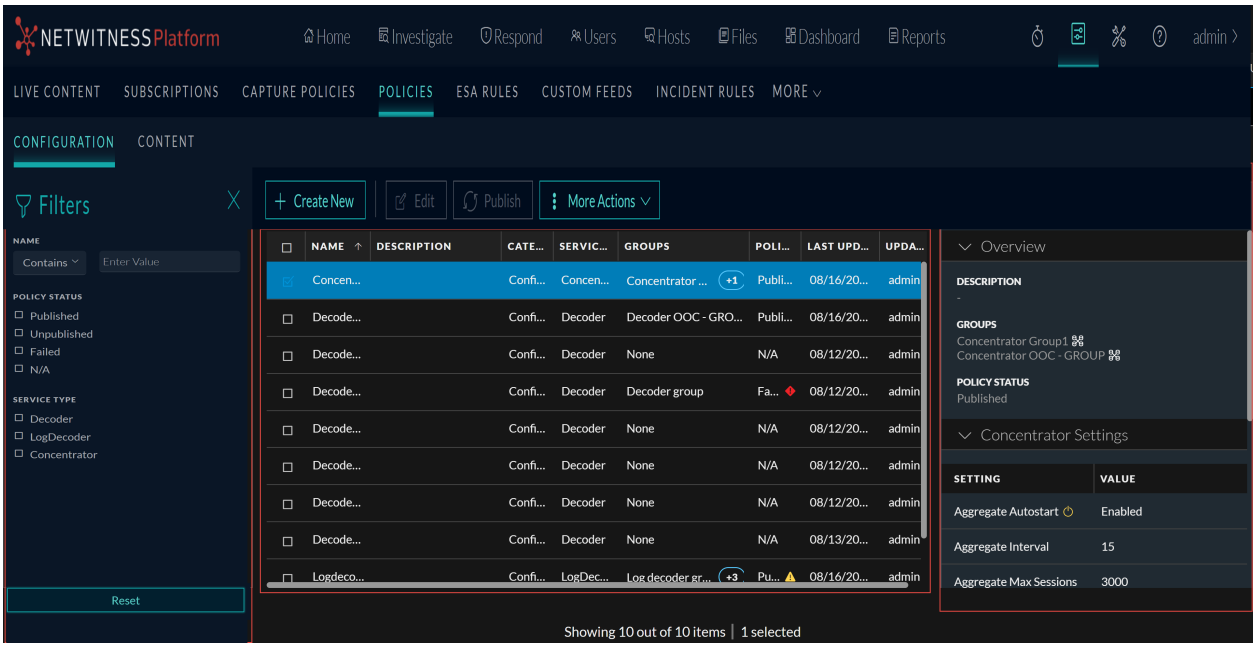
User Role	I want to...	Documentation
Administrator	set up a host.	Setting Up a Host
Administrator	maintain a host.	Maintaining Hosts
Administrator	maintain a service.	Maintaining Services

User Role	I want to...	Documentation
Administrator	Centrally Create and Maintain Service Policy.*	Hosts and Services Maintenance Procedures

* You can perform these tasks in the current view.

Quick Look

Below is an example of the **Policies** tab:



1 **Toolbar**

- **Create New**- Lets you create a new policy. For more information, see "Create a Policy" in the Centralized Service Configuration via Policy.
- **Edit** – Lets you edit the policy. For more information, see "Managing Policies and Groups" in the Centralized Service Configuration via Policy.
- **Publish** – Publishes the selected policy or policies.
- **More Actions**
  - **Assign to Group** -Lets you assign policy to a group.
  - **Clone** – Lets you clone a policy.
  - **Revert** – Lets you revert to previous policy settings. By default, the revert value is set to 5. You can customize the revert value in Explorer view.
  - **Delete** - Deletes the selected policy or policies permanently.

2 **Filter Pane**

- **Filters**: You can filter policies based on Policy Type and Policy Status and Service Type.

  To hide, click the  icon at the top-right of the panel. To display if hidden, click the  icon in the toolbar.

- **Reset**: Removes the currently applied filter criteria.

For more information, see "Filter Policies" in the Centralized Service Configuration via Policy.

3 **Policy List Pane**
Name – Name of the policy.

• **Description** – Description of the policy.

• **Category** – Type of policies applied.

• **Service Type** – Displays the service type to which the policy is applied.

• **Groups** - Lists the group to which this policy is applied.

• **Policy Status** – Status of the policy. The values are: Published, Unpublished, Failed, N/A.

• **Last Updated** – Displays the time when the policy is updated.

• **Updated By** – The user who updated the policy.

You can also sort on any column. If you mouse over a column header, a sort icon is displayed:  . Click the icon to sort by the selected column.

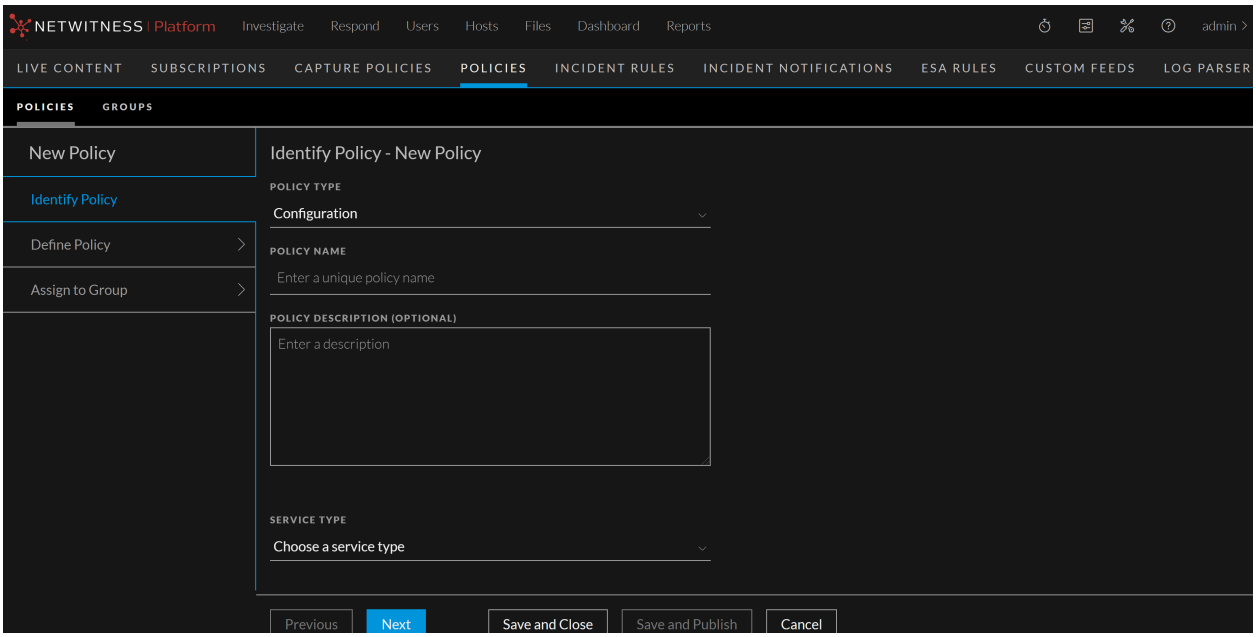
4 **Policy Details Pane**

Displays the properties of the selected policy.

Note: Click the row to view the Properties panel for a policy.

Create Policy

Below is an example of the Create Policy dialog.

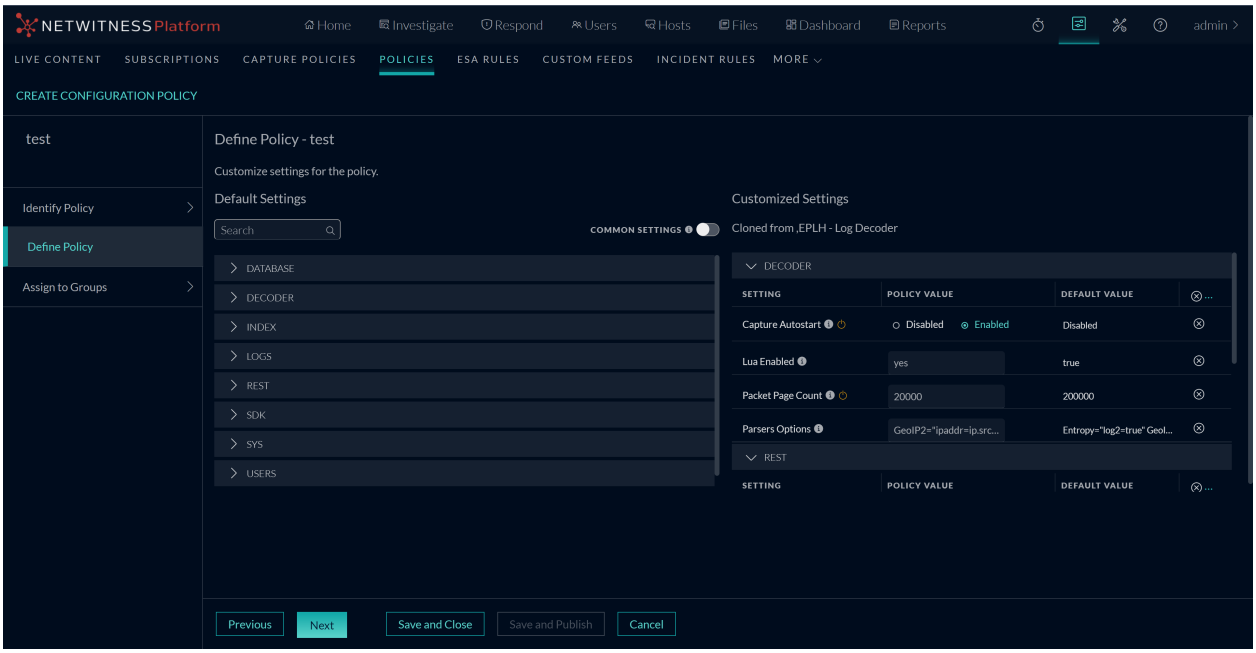


The table describes the information and options in the Create Policy dialog.

Field	Description
Policy Type	Displays the policy type.
Policy Name	Name of the policy. The name should be unique.
Policy Description (Optional)	Description of the policy. Description should not exceed 8000 characters.
Service Type	Displays the type of the service. Available options are Log Decoder, Decoder, and Concentrator.

Field	Description
(For version 11.7.1 and Later) Clone from Existing Service (Optional)	Displays the list of services based on the service type to clone those settings.
Save and Close	Saves the settings and closes the Create Policy dialog.

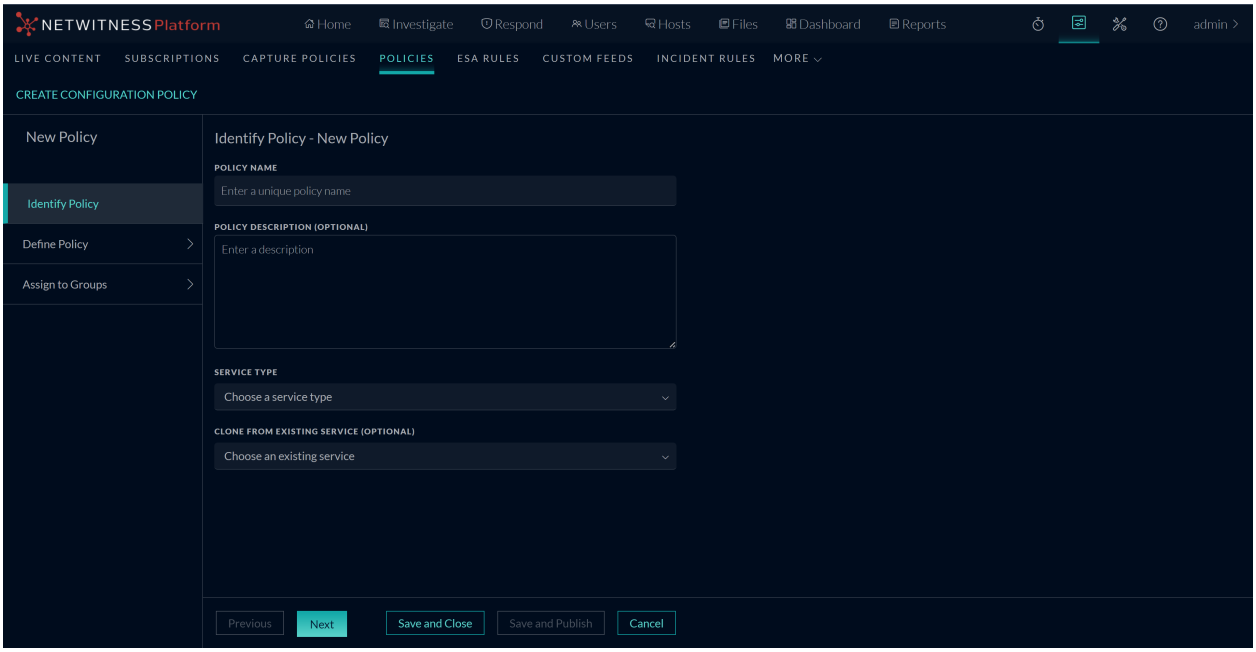
Define Policy Settings



Field	Description
Default Settings	Displays the settings of the service based on the category, for example, Database, Decoder and so on. Click  to expand the setting category.  The following describes Default settings: • **Setting**- Name of the setting. • **Value**- The settings value. • **Description**- Description of the setting. • **All** – Lets you to select the settings for customization. You can either click  to customize all the settings value or click  on a specific setting
Common Settings	Displays the common settings of the service. By default, it is disabled.
(For version 11.7.1 and Later) 10g Settings	Fetches the 10g settings.

Field	Description
Customized Settings	Lists the selected settings for customization. Click  to add the setting.  Update the value based on your requirement. 

Assign to Group



Field	Description
Group List	Displays the list of group associated with the policy. A group is disabled if it is already assigned to another policy. • Group Name • Policies • Services • Service Type • Action
Selected Group	Lists the selected groups. Click  to add groups.
Save and Close	Saves the settings and closes the Assign to Group dialog.
Save and Publish	Saves and publishes the created policy. **Note:** This option is disabled if: - Policy settings are not customized. - Policy is not assigned to groups.

Troubleshooting Version Installations and Updates

This section describes the error messages displayed in the Hosts view when it encounters problems updating host versions and installing services on hosts in the Hosts view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact Customer Support.

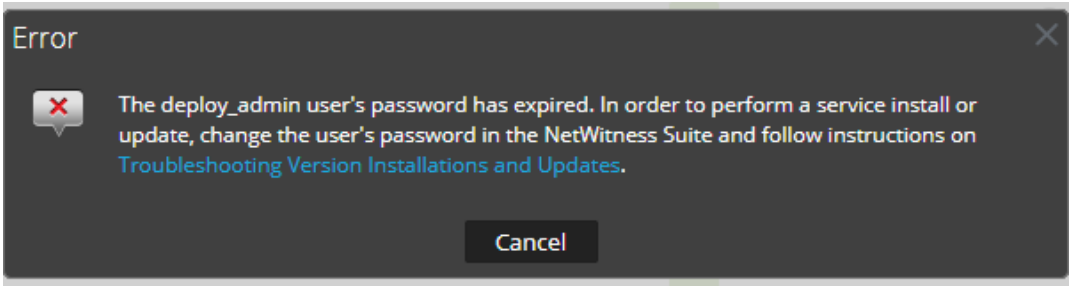
Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

- deploy_admin Password Expired Error
- Downloading Error
- Error Deploying Version <version-number> Missing Update Packages
- Upgrade Failed Error
- External Repo Update Error
- Host Installation Failed Error
- Host Update Failed Error
- Missing Update Packages Error
- OpenSSL 1.1.x Error
- Patch Update to Non-NW Server Error
- Reboot Host After Update from Command Line Error
- Reporting Engine Restarts After Upgrade

Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

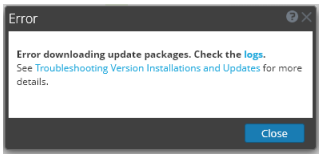
- Log Collector Service
- NW Server
- Orchestration
- Reporting Engine
- Event Stream Analysis

deploy_admin User Password Has Expired Error

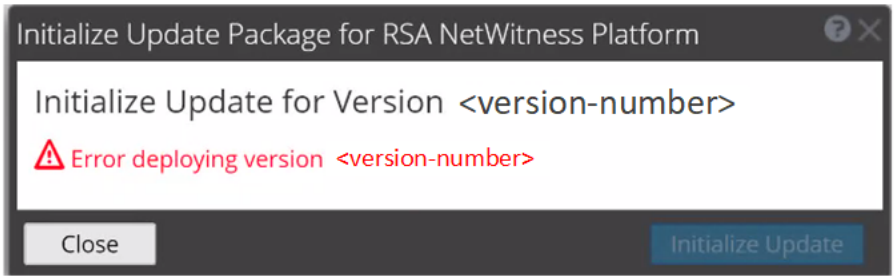
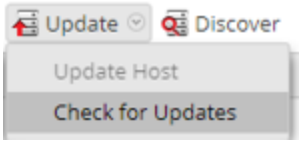
Error Message	
Cause	The `deploy_admin` user password has expired.

Solution	Reset your `deploy_admin` password password.
	1. On the NW Server host only, run the following command.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. Review the output of the `nw-manage --update-deploy-admin-pw` command to verify the `deploy_admin` password was successfully updated on all hosts. If an NW host is down or fails for any reason as displayed by the output of the `nw-manage --update-deploy-admin-pw` command, run `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` to synchronize the password between the NW Server and the host that failed once the communication failure is resolved.
	3. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

Downloading Error

Error Message	
Problem	When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete.
Cause	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
Solution	1. Try to update again. 2. If it fails again with the same error, try to update using the offline methods as described in "Offline Method from Hosts View" or "Offline Method Using Command Line Interface" in the *Upgrade Guide for NetWitness Platform 11.6*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues. 3. If you are still not able to update, contact Customer Support.

Error Deploying Version <version-number> Missing Update Packages

Error Message	
Problem	Error deploying version <version-number> is displayed in the **Initialize Update Package for RSA NetWitness Platform** dialog after you click on **Initialize Update** if the update package is corrupted.
Solution	1. Click **Close** to close the dialog. 2. Remove the version folder from staging folder. 3. Make sure that the salt-master service is running. 4. Recopy the update package zip file to the staging folder. 5. In the Hosts view toolbar, select Check for Updates again.  6. Click **Initialize Update**. 7. Click **Update** > **Update Hosts** from the toolbar. 8. Click **Begin Update** from the **Update Available** dialog. After the host is updated, it prompts you to reboot the host. 9. Click **Reboot** from the toolbar.

Upgrade Failed Error

Error Message	While updating/installing a device to version 11.2 or above, the following error can occur and be found in /var/log/netwitness/config-management/chef-solo.log: [2019-04-16T20:55:32+00:00] ERROR: Running exception handlers [2019-04-16T20:55:32+00:00] ERROR: Exception handlers complete [2019-04-16T20:55:32+00:00] FATAL: Stacktrace dumped to /var/lib/netwitness/config-management/cache/chef-stacktrace.out [2019-04-16T20:55:32+00:00] FATAL: Please provide the contents of the stacktrace.out file if you file a bug report [2019-04-16T20:55:32+00:00] ERROR: ruby_block[resolve ips] (nw-dns-client::config line 69) had an error: Resolv::ResolvError: no address for 889e5752-6ae3-4286-33f4ccbc [2019-04-16T20:55:32+00:00] FATAL: Chef::Exceptions::ChildConvergeError: Chef run process exited unsuccessfully (exit code 1)

Cause	The reason can be because the target host is unable to communicate to the Admin Server on port 53 as it is attempting to use the dnsmasq service on the Admin Server to resolve, in this case, 889e5752-6ae3-4286-a944-c182 33f4ccbc. This is the salt minion id of the admin server. You can see this by running "cat /etc/salt/minion" on the Admin Server to compare. Example output:
	`[root@S5-NWAdmin ~]# cat /etc/salt/minion`
	`master: localhost`
	`hash_type: sha256`
	`log_level: info`
	`id: 889e5752-6ae3-4286-a944-c18233f4ccbc`

Solution	If possible, configure any firewalls between the target host and the Admin Server host to be able to communicate on port 53. If this is not possible, the workaround is to include the minion id in the /etc/host file on the component hosts and starting in the 11.4 release, modify the chef recipe not to overwrite this workaround.
Workaround	Refer to Install/Upgrade fails in RSA NetWitness Platform because Resolv::ResolvError: no address for a particular host KB Article.

Error Message	Received an error in the error log similar to the following when trying to update to version 11.6 : `FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt`
Cause	Custom builds/rpms installed for certain components installed on hosts, such as in the case of installing Hotfixes.

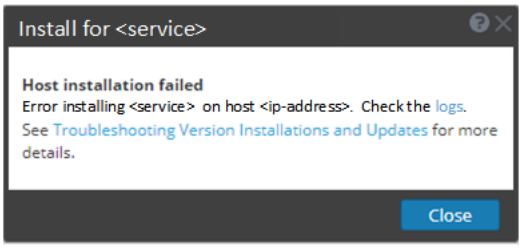
Solution	To resolve the issue, follow the below steps.
	1. SSH to Admin Server.
	2. Locate the component descriptor file by running the following command.
	`cd /etc/netwitness/component-descriptor/`
	3. Open the component descriptor file by running the following command.
	`vi nw-component-descriptor. json`
	4. Search for “packages” section for the component you have custom build/rpm. For example, below shown is the package details for “concentrator” host that has custom build/rpm.
	`“concentrator”: {`
	`“cookbook_name”: “rsa-concentrator”,`
	`“service_names”: [“rsa-nw-concentrator”],`
	`“family”: “launch”,`
	`“default_port”: xxxx, “description”: “Concentrator”,`
	`“packages”:[{ “name”: “rsa-nw-concentrator”,`
	`“version” : “11.6.0.0-2003001075220.5.cecf24b.e.17.centos”`
	`},`
	5. Delete the complete version details including (,) character in the packages section. For

	example, it should look like as shown below after you delete the version details.
	`"packages": [{`
	`"name": "rsa-nw-concentrator"`
	`},`
	Note: You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.
	6. Run the upgrade process again.

External Repo Update Error

Error Message	Received an error similar to the following error when trying to update to a new version from the : `.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
Cause	There is an error the path you specified.
Solution	Make sure that: • the URL does exist on the NW Server host. • you used the correct path and remove any spaces from it.

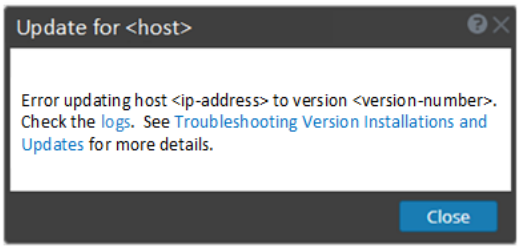
Host Installation Failed Error

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

Solution	1. Try to install the service again.
	Often this is all you need to do.
	2. If you still cannot install the service:
	a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`

	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error appears in one or more of these logs.
	b. Try to resolve the issue and reinstall the service.
	• Cause 1 - Entered the wrong `deploy_admin` password in the nwsetup-tui.
	Solution - Reset your `deploy_admin` password password.
	1. On the NW Server host and all other hosts on 12.x, run the following command.
	`/opt/rsa/saTools/bin/set-deploy-admin-password`
	2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.
	• Cause 2 -The `deploy_admin` password has expired.
	Solution - Reset your `deploy_admin` password password.
	1. On the NW Server host and all other hosts on 12.x, run the following command.
	`/opt/rsa/saTools/bin/set-deploy-admin-password`
	2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.
	3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support.

Host Update Failed Error

Error Message	
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.
Solution	1. Try to apply the version update to the host again. Often this is all you need to do. 2. If you still cannot apply the new version update:

a. Monitor the following logs on NW Server as it progresses (for example, run the `tail -f` command from the command line):
`/var/netwitness/uax/logs/sa.log`
`/var/log/netwitness/orchestration-server/orchestration-server.log`
`/var/log/netwitness/deployment-upgrade/chef-solo.log`
`/var/log/netwitness/config-management/chef-solo.log`
`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
The error appears in one or more of these logs.

b. Try to resolve the issue and reapply the version update.

- Cause 1 - `deploy_admin` password has expired.
  Solution - Reset your `deploy_admin` password .
  Complete the following steps to resolve Cause 1.

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

- Cause 2 -The `deploy_admin` password was changed on NW Server host but not changed on non-NW Server hosts.
  Complete the following step to resolve Cause 2.

  - On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.
  `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support.

Missing Update Packages Error

Error Message	**Initialize Update for Version xx.x.x.x** Missing the following update package(s) Download Packages from RSA Link

Problem	Missing the following update package(s) is displayed in the **Initialize Update Package for RSA NetWitness Platform** dialog when you are updating a host from the **Hosts** view offline and there are packages missing in the staging folder.
Solution	1. Click Download Packages from RSA Link in the **Initialize Update Package for RSA NetWitness Platform** dialog. The NetWitness Community page that contains the update files for the selected version is displayed. 2. Select the missing packages from the staging folder. The **Initialize Update Package for RSA NetWitness Platform** dialog is displayed telling you that it is ready to initialize the update packages.

OpenSSL 1.1.x

Error Message	The following example illustrates an ssh error that can occur when the ssh client is run from a host with OpenSSL 1.1.x installed: `$ ssh root@10.1.2.3` **`ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect`**

Problem	Advanced users who want to ssh to a NetWitness Platform host from a client that is using OpenSSL 1.1.x encounter this error because of incompatibility between CENTOS 7.x and OpenSSL 1.1.x. For example:
	`$ rpm -q openssl`
	`openssl-1.1.1-8.el8.x86_64`

Solution	Specify the compatible cipher list on the command line. For example:
	`$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3`
	`I've read & consent to terms in IS user agreement.`
	`root@10.1.2.3's password:`
	`Last login: Mon Oct 21 19:03:23 2019`

Patch Update to Non-NW Server Error

Error Message	The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error: **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
Problem	After you update the NW Server host to a version, you must update all non-NW Server hosts to the same version. For example, if you update the NW Server from 11.4.0.0 to 11.6.0.0 , the only update path for the non-NW Server hosts is the same version (that is, 11.6.0.0). If you try to update any non-NW Server host to a different version (for example, from 11.4.0.0 to an 11.4.x.x) you will get this error.
Solution	You have two options:

	• Update the non-NW Server host to 11.6.0.0, or • Do not update the non-NW Server host (keep it at its current version)

Reboot Host After Update from Command Line Error

Error Message	You receive a message in the User Interface to reboot the host after you update and reboot the host offline. 
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Reporting Engine Restarts After Upgrade

Problem	In some cases, after you upgrade to 11.6 from versions of 11.x, such as 11.4, the Reporting Engine service attempts to restart continuously without success.
Cause	The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.
Solution	To resolve the issue, do the following: 1. Check which database files are corrupted: Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks: • If the live charts db file is corrupted, the following logs are displayed: Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • If the alert status db file is corrupted, the following logs are displayed:

Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

at org.h2.message.DbException.get(DbException.java:168)

org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'

- If the report status db file is corrupted, the following logs are displayed:

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading
record: null. Possible solution: use the recovery tool
[90030-196]
```

2. To resolve the live charts database file corruption, perform the following steps:
   a. Stop the Reporting Engine service.
   b. Move the `livechart.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` folder to a temporary location.
   c. Restart the Reporting Engine service.

   Note: Some live charts data may be lost on performing the above steps.

   To resolve the alert status or report status database file corruption, perform the following steps:

   a. Stop the Reporting Engine service.
   b. Replace the corrupted db file with the latest `alertstatusmanager.mv.db` or `reportstatusmanager.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/archives` folder.
   c. Restart the Reporting Engine service.

   For more information, see the Knowledge Base article Reporting Engine restarts After upgrade to RSA NetWitness Platform 11.4.

Problem	After you upgrade to version 11.6, the Reporting Engine service does not restart.
Cause	The Reporting Engine service may not start due to any of the following reasons. - workspace.xml not updated. - Time is not converted properly in livechart h2 database. - JCR (Jackrabbit repository) is corrupted with primary key violation.
Solution	To resolve the issue, run the Reporting Engine Migration Recovery tool (`rsa-nw-re-migration-recovery.sh`) on the Admin Server where the Reporting Engine service is installed.

	Note: You can find the Reporting Engine Migration Recovery tool in the below location.
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1. SSH to Admin Server.
	2. Untar the RE (Reporting Engine) tool, run the following command.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	3. (Optional) If you want to untar the RE tool file in some other directory, you can create a directory and untar the RE tool. Run the following commands.
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4. Run the script, run the following command.
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`
	For more information, see the Knowledge Base article **Reporting Engine Migration Recovery Tool**.

Log Collector Service (`nwlogcollector`)

Log Collector installation logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

Error Message	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	If you use a Log Collector Lockbox, log in to NetWitness and configure the Lockbox as described in the "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

Error Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

Error Message	Decoder tries to start capture events but fails. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`

Solution	To resolve the issue, do the following steps,
	1. SSH to the Decoder host.
	2. Run the following commands.
	`yum reinstall pfring*`
	`systemctl restart nwdecoder`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 11.4.x.x or 11.5.x.x. to 11.6.0.0.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Orchestration

The orchestration server logs are posted to `/var/log/netwitness/orchestration-server/orchestration-server.log` on the NW Server Host.

Problem	1. Tried to upgrade a non-NW Server host and it failed. 2. Retried the upgrade for this host and it failed again. You will see the following message in the `orchestration-server.log`. `"'file' _virtual_ returned False: cannot import name HASHES""`
Cause	Salt minion may have been upgraded and never restarted on failed non-NW Server host

Solution	1. SSH to the non-NW Server host that failed to upgrade.
	2. Submit the following commands.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Retry the upgrade of the non-NW Server host.

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Error Message	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space.

Event Stream Analysis

Problem	After upgrading to version 11.6, the ESA correlation server does not aggregate events from the configured data sources.
Error Message	`Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)`
Solution	To resolve the issue, do the following steps. In the NetWitness user interface,

1. Go to  **(Configure) > ESA Rules**.
   ESA Rules panel is displayed with **Rules** tab open.
2. In the Rules tab options panel, under Deployments, select a deployment.
3. In the **Data Sources** section, select the data source and click  in the toolbar.
4. In the **Edit Service** dialog, type the password for that data source.
5. Click the **Test Connection** button to make sure that it can communicate with the ESA service and then click **OK**.

Note: Do the above procedure for all the configured data sources.

6. After you finish making changes to the deployment, click **Deploy Now** to redeploy the ESA rule deployment.