RSA NETWITNESS® SUITE

System Maintenance Guide

for Version 11.1

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

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

Distribution

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

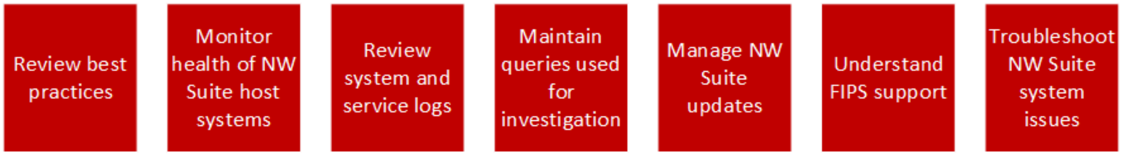
July 2018

Contents

NetWitness Suite System Maintenance

This guide encompasses the tasks that administrators perform after initial network setup to allow NetWitness Suite to manage hosts and services in the network, maintain and monitor the network, manage jobs, and tune performance.

The following diagram shows the different system maintenance tasks available to you.


Review best practices
Monitor health of NW Suite host systems
Review system and service logs
Maintain queries used for investigation
Manage NW Suite updates
Understand FIPS support
Troubleshoot NW Suite system issues

The following topics describe these tasks:

- Best Practices
- Monitoring Health and Wellness of NetWitness Suite
- Displaying System and Service Logs
- Maintaining Queries Using URL Integration
- Managing NetWitness Suite Updates
- FIPS Support
- Troubleshoot NetWitness Suite

Best Practices

Safeguarding Assets with RSA Supplied Policies

The purpose of the RSA Core Policies delivered with NetWitness Suite is to help you safeguarding your NetWitness Suite Domain assets immediately (before you configure rules specific to your environment and your Security Policy).

RSA recommends that you set up email notifications to the appropriate asset owners for these policies as soon as possible. This will notify them when performance and capacity thresholds are crossed so they can take action immediately.

RSA also recommends that you evaluate the Core policies and disable a policy or change its service/group assignments according to your specific monitoring requirements.

Safeguarding Assets with Policies Based on Your Environment

RSA Core Policies are generic and may not provide sufficient monitoring coverage for your environment. RSA recommends that you gather issues over a period of time, not identified by the RSA Core Policies, and configure rules to help you prevent these issues.

Creating Rules and Notifications Judiciously

RSA recommends that you make sure that each rule and policy is necessary before you implement it, if possible. RSA also recommends that you review implemented policies or a regular basis for their validity. Invalid alarms and email notifications can adversely affect the focus of the asset owners.

Troubleshooting Issues

RSA recommends that you review Troubleshooting Health & Wellness and Troubleshoot NetWitness Suite when you receive error messages in the user interface and log files from hosts and services.

Monitoring Health and Wellness of NetWitness Suite

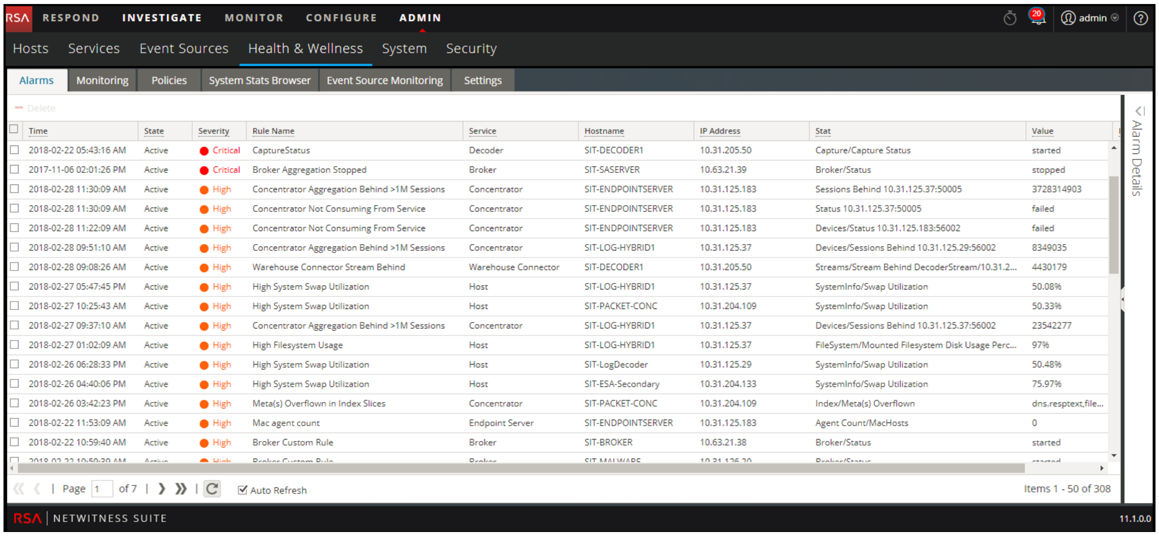
The Health & Wellness module of NetWitness Suite provides the ability to:

- View the current health of all the hosts, services running on the hosts, and various aspects of the hosts’ health.
- Monitor the hosts and services in your network environment.
- View details of various event sources configured with NetWitness Suite.
- View system stats for the selected hosts by filtering the views as required.

In addition, you can configure Archiver monitoring and Warehouse Connector monitoring, use the procedures on monitoring host statistics, and work with system logs to monitor NetWitness Suite.

> **Note:** All users have permission to view the entire Health and Wellness interface by default. The Administrator and the Operator roles are the only roles that can manage the Policies view by default. Please refer to the "Role Permissions" topic in the *Security User Management Guide* for a complete list of the default permissions for the NetWitness Suite Interface.

The figure displays the Health & Wellness module of the NetWitness Suite user interface and various sections in the Health & Wellness module.



□	Time	State	Severity	Rule Name	Service	Hostname	IP Address	Stat	Value
□	2018-02-22 05:43:16 AM	Active	● Critical	CaptureStatus	Decoder	SIT-DECODER1	10.31.205.50	Capture/Capture Status	started
□	2017-11-06 02:01:26 PM	Active	● Critical	Broker Aggregation Stopped	Broker	SIT-SASERVER	10.63.21.39	Broker/Status	stopped
□	2018-02-28 11:30:09 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Sessions Behind 10.31.125.37:50005	3728314903
□	2018-02-28 11:30:09 AM	Active	● High	Concentrator Not Consuming From Service	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Status 10.31.125.37:50005	failed
□	2018-02-28 11:22:09 AM	Active	● High	Concentrator Not Consuming From Service	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Devices/Status 10.31.125.183:56002	failed
□	2018-02-28 09:51:10 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-LOG-HYBRID1	10.31.125.37	Devices/Sessions Behind 10.31.125.29:56002	8349035
□	2018-02-28 09:08:26 AM	Active	● High	Warehouse Connector Stream Behind	Warehouse Connector	SIT-DECODER1	10.31.205.50	Streams/Stream Behind DecoderStream/10.31.2...	4430179
□	2018-02-27 05:47:45 PM	Active	● High	High System Swap Utilization	Host	SIT-LOG-HYBRID1	10.31.125.37	SystemInfo/Swap Utilization	50.08%
□	2018-02-27 10:25:43 AM	Active	● High	High System Swap Utilization	Host	SIT-PACKET-CONC	10.31.204.109	SystemInfo/Swap Utilization	50.33%
□	2018-02-27 09:37:10 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-LOG-HYBRID1	10.31.125.37	Devices/Sessions Behind 10.31.125.37:56002	23542277
□	2018-02-27 01:02:09 AM	Active	● High	High Filesystem Usage	Host	SIT-LOG-HYBRID1	10.31.125.37	FileSystem/Mounted Filesystem Disk Usage Perc...	97%
□	2018-02-26 06:28:33 PM	Active	● High	High System Swap Utilization	Host	SIT-LogDecoder	10.31.125.29	SystemInfo/Swap Utilization	50.48%
□	2018-02-26 04:40:06 PM	Active	● High	High System Swap Utilization	Host	SIT-ESA-Secondary	10.31.204.133	SystemInfo/Swap Utilization	75.97%
□	2018-02-26 03:42:23 PM	Active	● High	Meta(s) Overflown in Index Slices	Concentrator	SIT-PACKET-CONC	10.31.204.109	Index/Meta(s) Overflown	dns.resptext,file...
□	2018-02-22 11:53:09 AM	Active	● High	Mac agent count	Endpoint Server	SIT-ENDPOINTSERVER	10.31.125.183	Agent Count/MacHosts	0
□	2018-02-22 10:59:40 AM	Active	● High	Broker Custom Rule	Broker	SIT-BROKER	10.63.21.38	Broker/Status	started

Page 1 of 7 | ☑ Auto Refresh

Items 1 - 50 of 308

RSA | NETWITNESS SUITE

11.1.0.0

Manage Policies

Policies are either user-defined or supplied by RSA. A policy defines:

- Services and hosts to which the policy applies.
- Rules that specify statistical thresholds that govern alarms.
- When to suppress the policy.
- Who to notify when an alarm triggers and when to notify them.

For the related reference topics, see NetWitness Suite Out-of-the-Box Policies

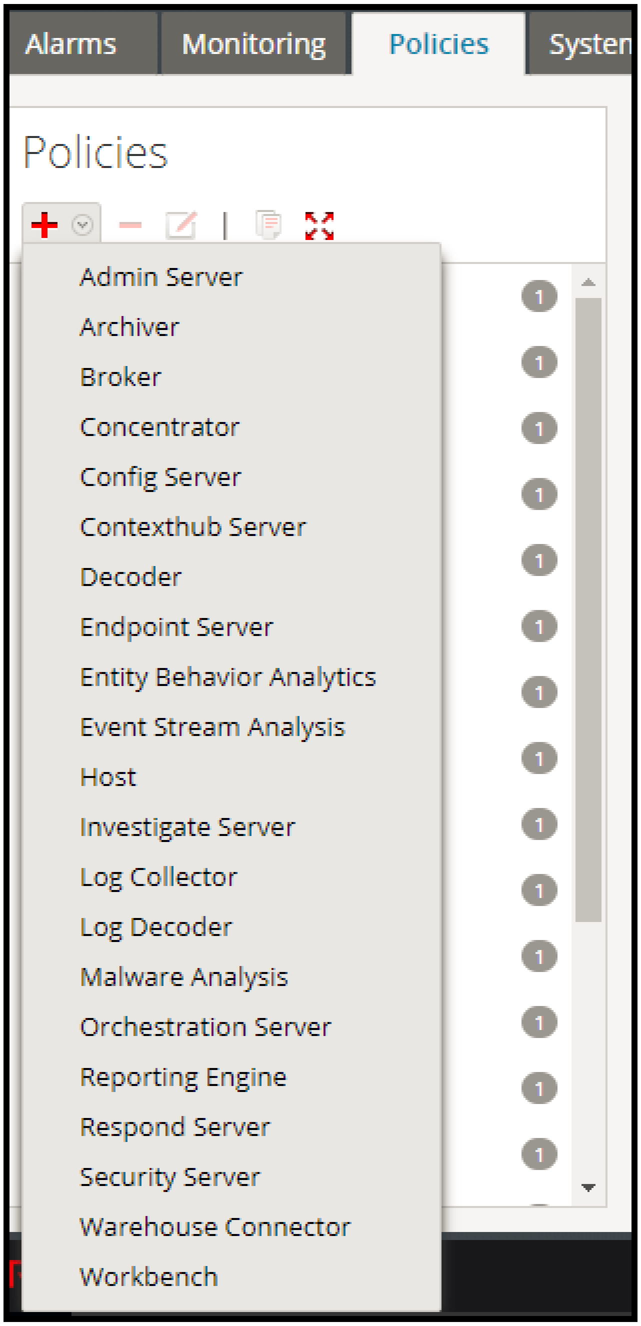
Note: You can now configure a policy to notify Public Key Infrastructure (PKI) certificate expiration status.

Add a Policy

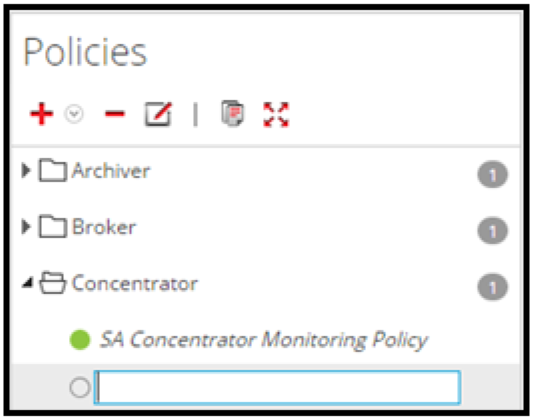
1. Go to **ADMIN > Health & Wellness.**
2. Click **Policies** tab.

   The Policies view is displayed.
3. Click + ⌄ in the **Policies** panel.

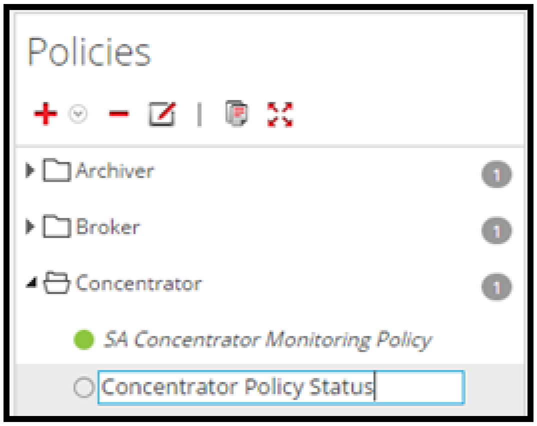
   A list of your hosts and services displays for which you can create health policies.



4. Select a host or service (for example, **Concentrator**).
   For PKI policy, you must select a host (for example, Host).
   The host or service is displayed in the Policies panel with a blank Policy Detail panel.



5. Enter a name for the Policy (for example, **Concentrator Policy Status**) in the **Policies** panel.



Concentrator Policy Status

The name (for example, **Concentrator Policy Status**) is now displayed as the policy name in Policy Detail panel.

6. Create a Policy in the Policy Detail panel:

   a. Select the **Enable** checkbox.

   b. Add relevant services (in this example, any relevant Concentrator services) that you want to monitor for health statistics.
   For PKI policy, you must select the LOCALHOST to monitor for health statistics.

   c. Add relevant rule conditions you want to configure for the policy.

   d. Suppress enforcement of the policy for the time periods you want.

   e. Add any email notifications you want for the policy.

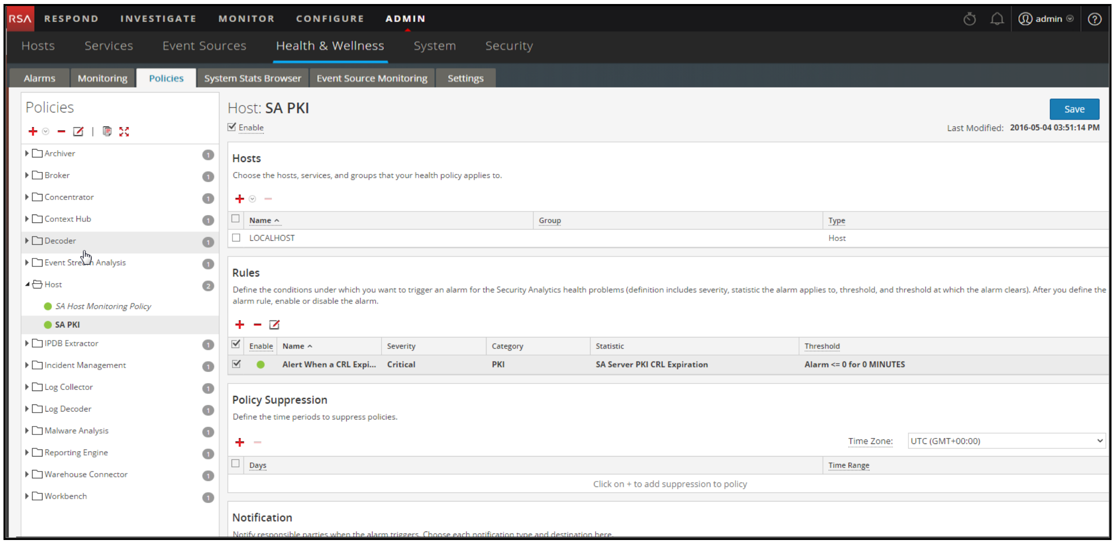
   f. Click **Save** in the Policy Detail panel.

   The Policy is added.

Add Policy Example

Below is the high-level example for configuring PKI policy:

1. Add a new PKI policy.



Policies

- Archiver 1
- Broker 1
- Concentrator 1
- Context Hub 1
- Decoder 1
- Event Stream Analysis 1
- Host 2
  - ● *SA Host Monitoring Policy*
  - ● **SA PKI**
- IPDB Extractor 1
- Incident Management 1
- Log Collector 1
- Log Decoder 1
- Malware Analysis 1
- Reporting Engine 1
- Warehouse Connector 1
- Workbench 1

Host: **SA PKI**

☑ Enable

Last Modified: **2016-05-04 03:51:14 PM**

Hosts

Choose the hosts, services, and groups that your health policy applies to.

□	Name ^	Group	Type
□	LOCALHOST		Host

Rules

Define the conditions under which you want to trigger an alarm for the Security Analytics health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

☑	Enable	Name ^	Severity	Category	Statistic	Threshold
☑	●	**Alert When a CRL Expi...**	**Critical**	**PKI**	**SA Server PKI CRL Expiration**	**Alarm <= 0 for 0 MINUTES**

Policy Suppression

Define the time periods to suppress policies.

Time Zone: UTC (GMT+00:00)

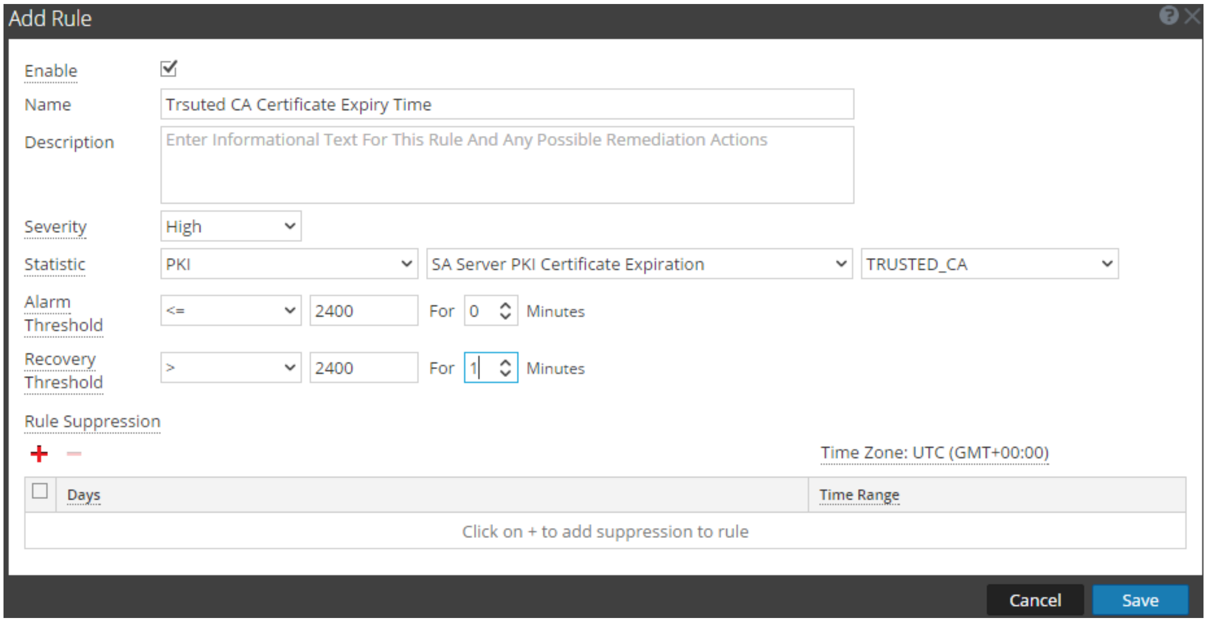
□	Days	Time Range
	Click on + to add suppression to policy	

Notification

Notify responsible parties when the alarm triggers. Choose each notification type and destination here.

2. Add a Rule with Statistics:

- For CA Expiration



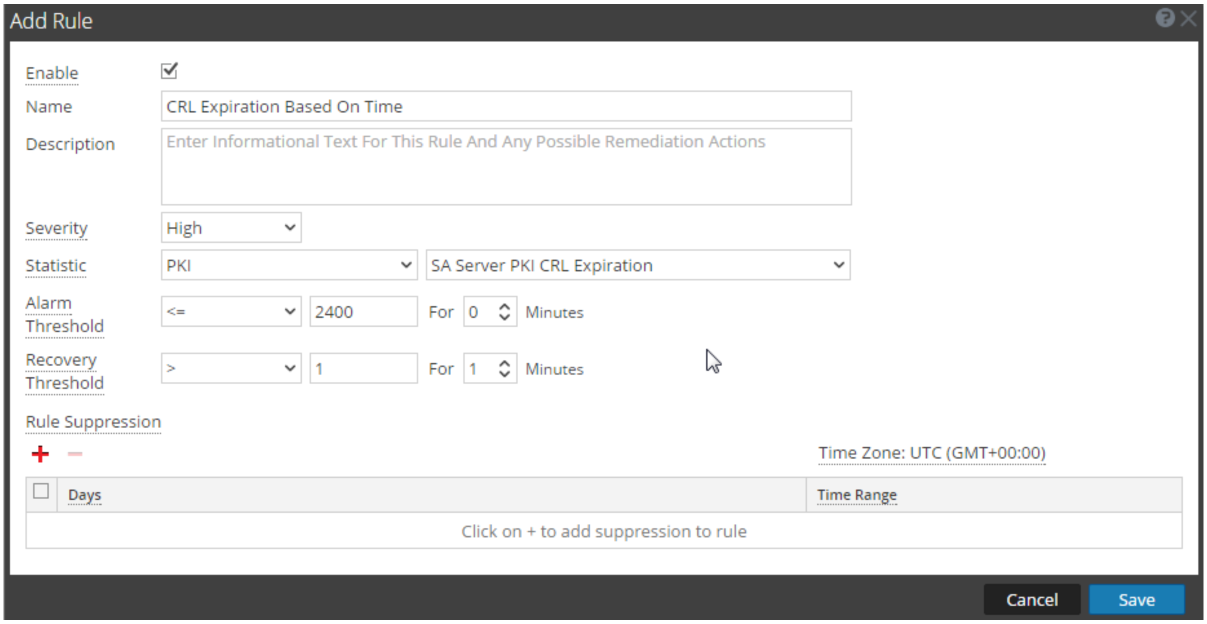
Enable	☑
Name	Trsuted CA Certificate Expiry Time
Description	Enter Informational Text For This Rule And Any Possible Remediation Actions
Severity	High
Statistic	PKI / SA Server PKI Certificate Expiration / TRUSTED_CA
Alarm Threshold	<= 2400 For 0 Minutes
Recovery Threshold	> 2400 For 1 Minutes

Rule Suppression

Time Zone: UTC (GMT+00:00)

□	Days	Time Range
	Click on + to add suppression to rule	

- For CRL Expiration



Enable ☑

Name: CRL Expiration Based On Time

Description: Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity: High

Statistic: PKI | SA Server PKI CRL Expiration

Alarm Threshold: <= 2400 For 0 Minutes

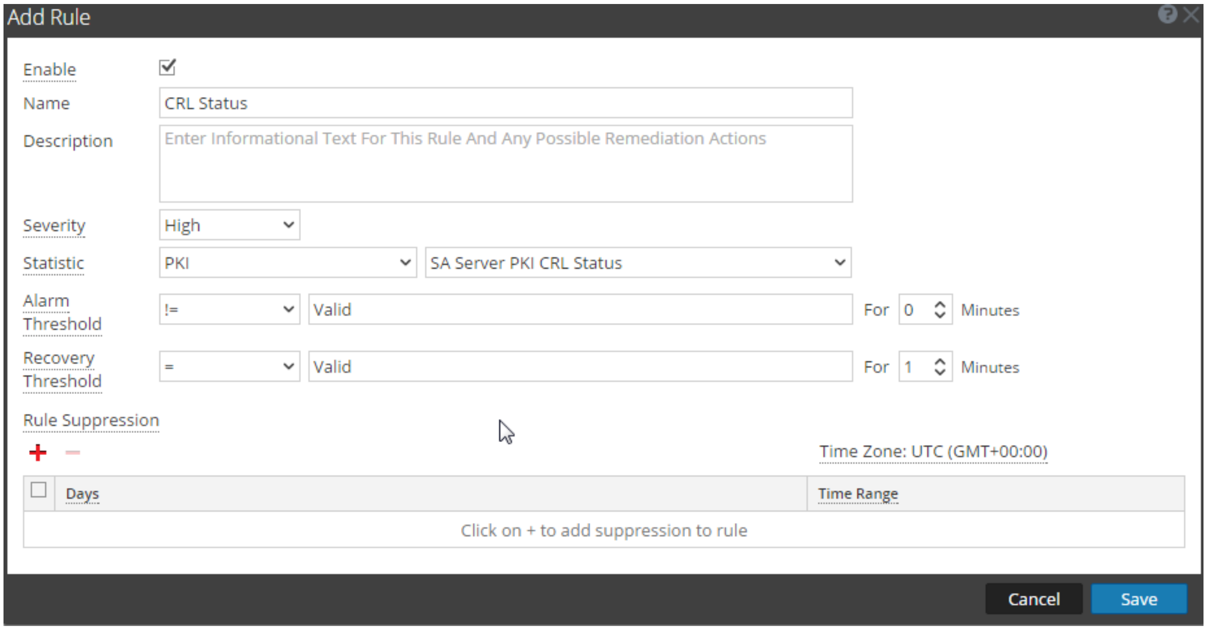
Recovery Threshold: > 1 For 1 Minutes

Rule Suppression

Time Zone: UTC (GMT+00:00)

□	Days	Time Range
	Click on + to add suppression to rule	

- For CRL Status



Enable ☑

Name: CRL Status

Description: Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity: High

Statistic: PKI | SA Server PKI CRL Status

Alarm Threshold: != Valid For 0 Minutes

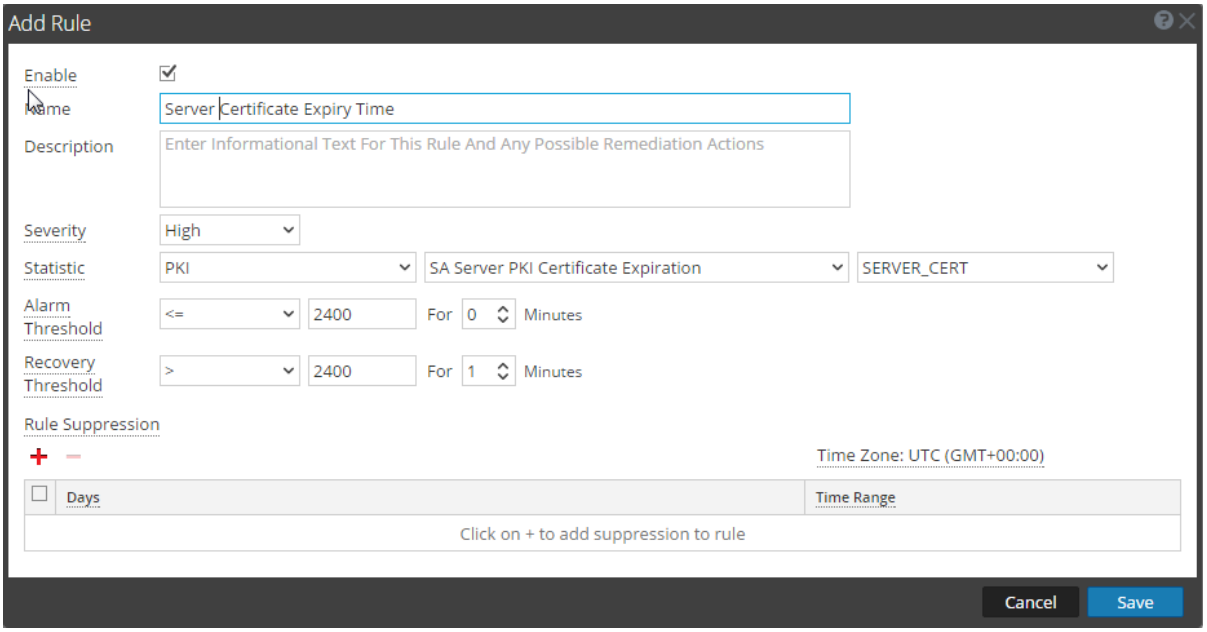
Recovery Threshold: = Valid For 1 Minutes

Rule Suppression

Time Zone: UTC (GMT+00:00)

□	Days	Time Range
	Click on + to add suppression to rule	

- For Server Certificate Expiration



Add Rule

Enable ☑

Name: Server Certificate Expiry Time

Description: Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity: High

Statistic: PKI | SA Server PKI Certificate Expiration | SERVER_CERT

Alarm Threshold: <= 2400 For 0 Minutes

Recovery Threshold: > 2400 For 1 Minutes

Rule Suppression

Time Zone: UTC (GMT+00:00)

□ Days	Time Range
Click on + to add suppression to rule	

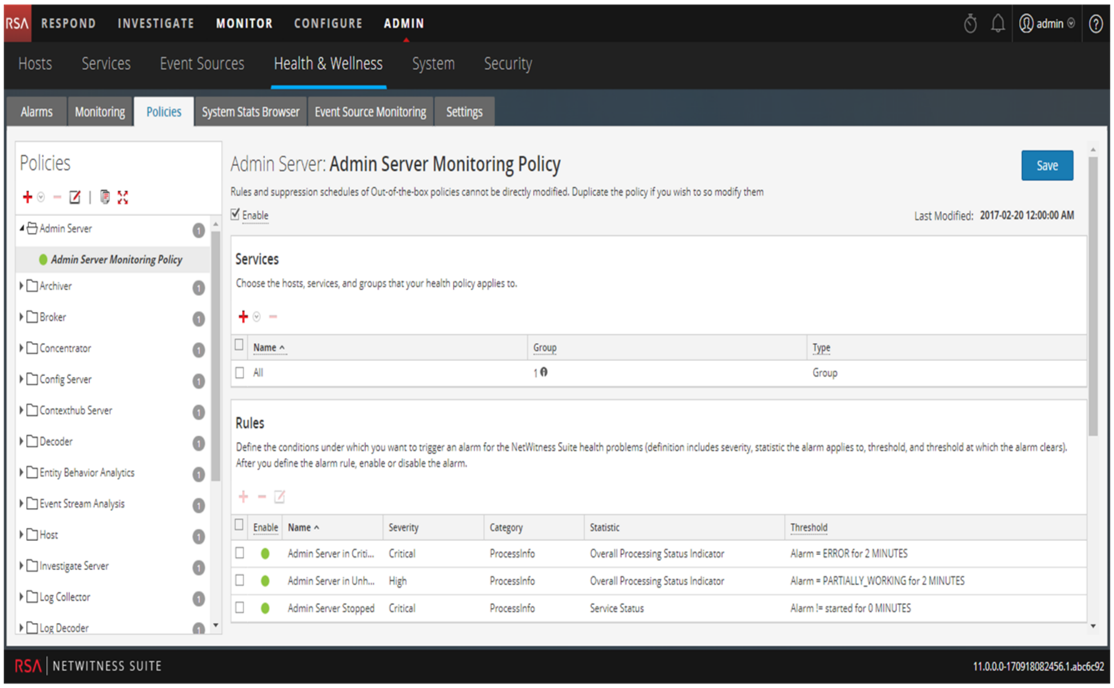
Edit a Policy

1. Go to **ADMIN** > **Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.
3. Select a policy (for example, **Concentrator Policy Status**) under a host or service.

   The Policy Detail is displayed.
4. Click ✎.

   The policy name (for example, **Admin Server Monitoring Policy**) and policy detail panel become editable.



Admin Server: **Admin Server Monitoring Policy**

Rules and suppression schedules of Out-of-the-box policies cannot be directly modified. Duplicate the policy if you wish to so modify them

☑ Enable

Last Modified: **2017-02-20 12:00:00 AM**

Services

Choose the hosts, services, and groups that your health policy applies to.

□	Name	Group	Type
□	All	1	Group

Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Suite health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

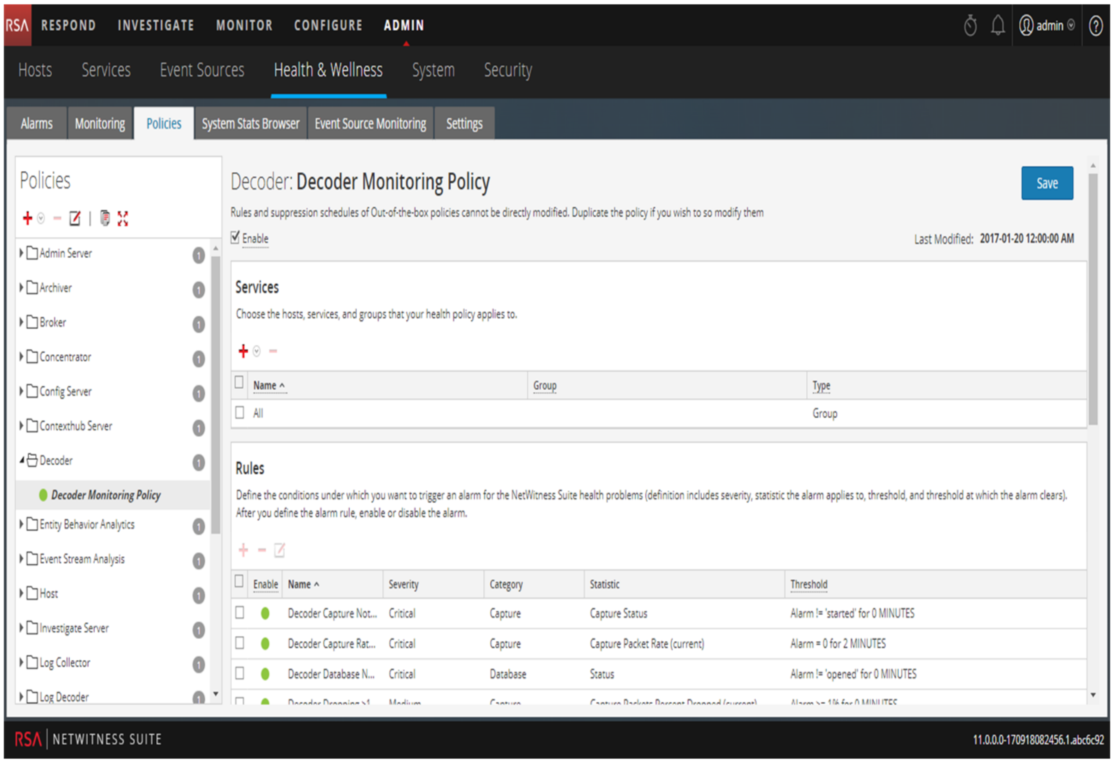
□	Enable	Name	Severity	Category	Statistic	Threshold
□	●	Admin Server in Criti...	Critical	ProcessInfo	Overall Processing Status Indicator	Alarm = ERROR for 2 MINUTES
□	●	Admin Server in Unh...	High	ProcessInfo	Overall Processing Status Indicator	Alarm = PARTIALLY_WORKING for 2 MINUTES
□	●	Admin Server Stopped	Critical	ProcessInfo	Service Status	Alarm != started for 0 MINUTES

5. Make the required changes and click **Save** in the Policy Detail panel. You can:
   - Edit the Policy name.
   - Enable or disable the policy.
   - Add or delete hosts and services in the policy.
   - Add, delete or modify rules in the policy.
   - Add/Edit/Delete suppressions in the policy.
   - Add/Edit/Delete notifications in the policy.

Note: Save applies the policy rules based on the selection of enable/disable. It also resets the rule condition timers for changed rules, and the entire Policy.

Duplicate a Policy

1. Go to **ADMIN** > **Health & Wellness**.
2. Click the **Policies** tab.
3. Select a policy (for example, **Concentrator Policy Status**) under a host or service.
4. Click .NetWitness Suite copies the policy and lists it with **(1)** appended to the original policy's name.



Policies

- Admin Server 1
- Archiver 1
- Broker 1
- Concentrator 1
- Config Server 1
- Contexthub Server 1
- Decoder 1
  - Decoder Monitoring Policy
- Entity Behavior Analytics 1
- Event Stream Analysis 1
- Host 1
- Investigate Server 1
- Log Collector 1
- Log Decoder 1

Decoder: **Decoder Monitoring Policy**

Rules and suppression schedules of Out-of-the-box policies cannot be directly modified. Duplicate the policy if you wish to so modify them

☑ Enable

Last Modified: **2017-01-20 12:00:00 AM**

Services

Choose the hosts, services, and groups that your health policy applies to.

□	Name ^	Group	Type
□	All		Group

Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Suite health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

□	Enable	Name ^	Severity	Category	Statistic	Threshold
□	●	Decoder Capture Not...	Critical	Capture	Capture Status	Alarm != 'started' for 0 MINUTES
□	●	Decoder Capture Rat...	Critical	Capture	Capture Packet Rate (current)	Alarm = 0 for 2 MINUTES
□	●	Decoder Database N...	Critical	Database	Status	Alarm != 'opened' for 0 MINUTES
□	●	Decoder Dropping >1	Medium	Capture	Capture Packets Percent Dropped (current)	Alarm >= 1% for 0 MINUTES

5. Click ✎ and rename the Policy [for example, rename **Decoder Monitoring Policy(1)** to **New Concentrator Policy Status**.

> **Note:** A duplicated policy is disabled by default and the host and service assignments are not duplicated. Assign any relevant hosts and services to the duplicated policy before you use it to monitor health and wellness of the NetWitness Suite infrastructure.

Assign Services or Groups

To assign hosts or services to a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

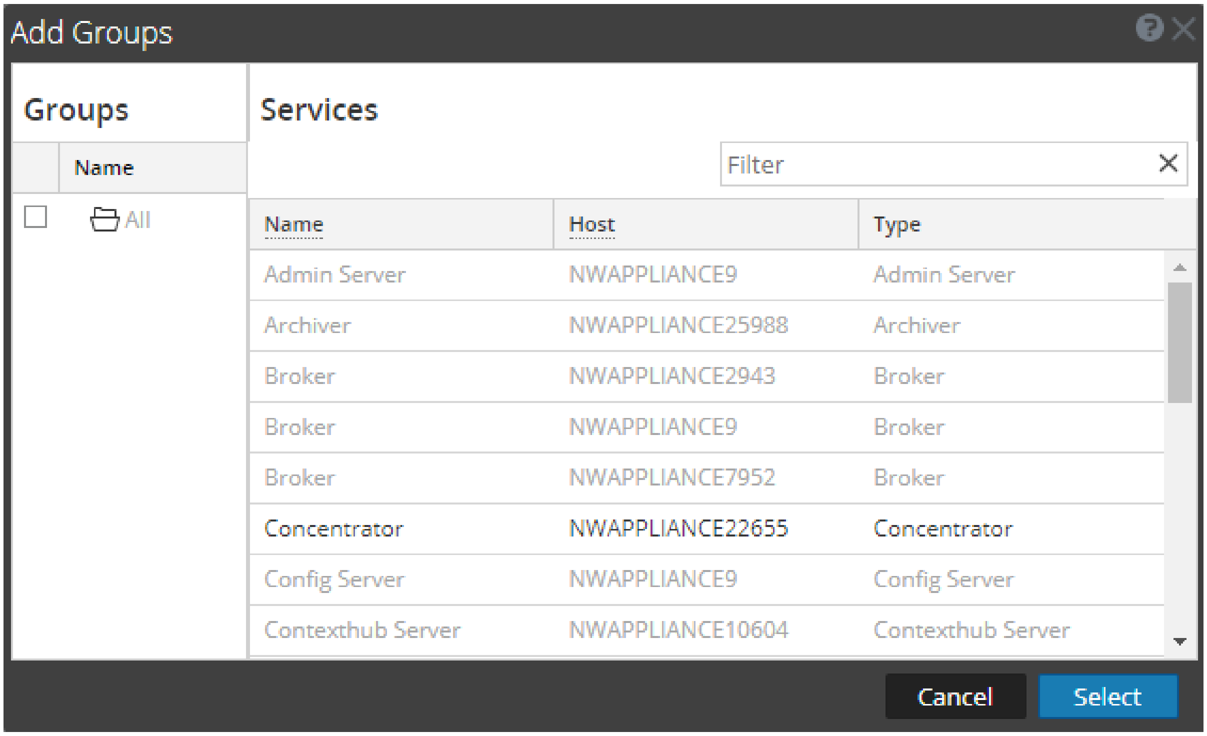
   The Policies view is displayed.
3. Select a policy (for example, **First Policy**) under a host or service.

   The Policy Detail is displayed.
4. Click + in the Services and Groups list toolbar.
5. Choose one of the following actions:

- For Hosts, select **Groups** or **Hosts** from the selection menu.
- For Services, select **Groups** or **Services** from the selection menu.

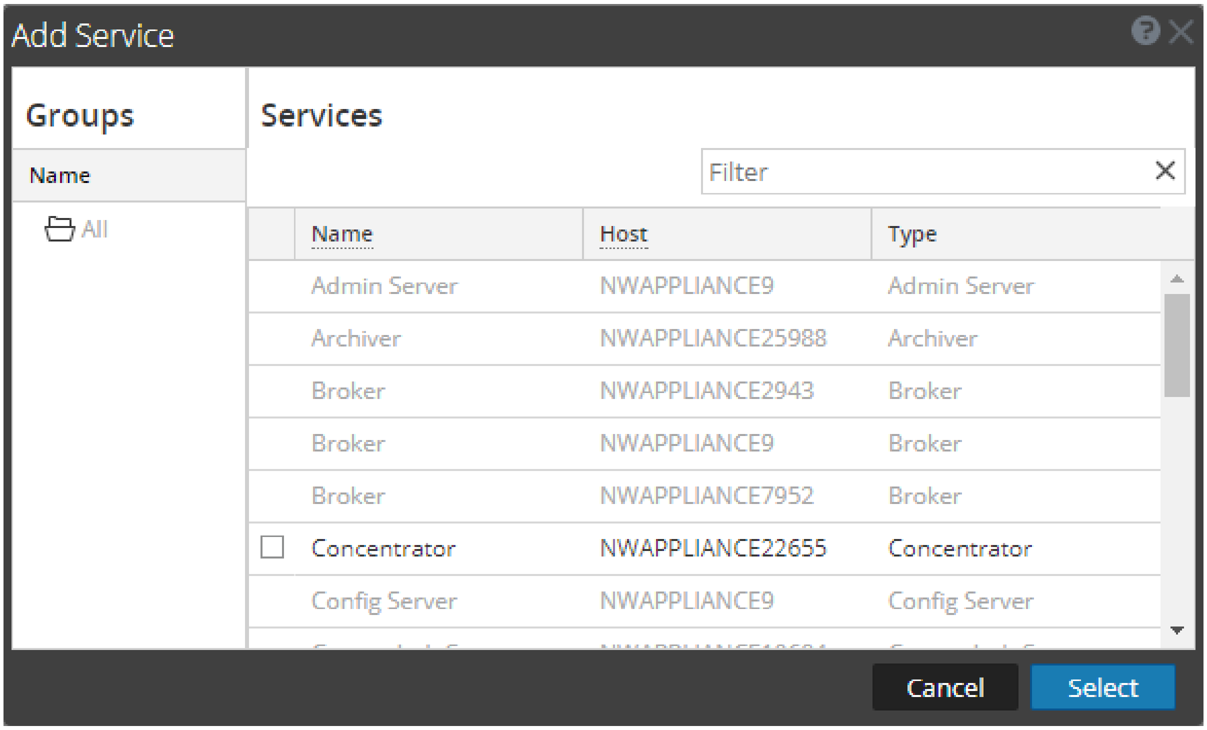
6. Depending on whether you are assigning services or groups, perform one of the following actions:

   - **Groups**, the **Groups** dialog is displayed from which you can select predefined groups of hosts or services.



Name	Host	Type
Admin Server	NWAPPLIANCE9	Admin Server
Archiver	NWAPPLIANCE25988	Archiver
Broker	NWAPPLIANCE2943	Broker
Broker	NWAPPLIANCE9	Broker
Broker	NWAPPLIANCE7952	Broker
Concentrator	NWAPPLIANCE22655	Concentrator
Config Server	NWAPPLIANCE9	Config Server
Contexthub Server	NWAPPLIANCE10604	Contexthub Server

- **Services**, the **Services** dialog is displayed from which you can select individual services.



	Name	Host	Type
	Admin Server	NWAPPLIANCE9	Admin Server
	Archiver	NWAPPLIANCE25988	Archiver
	Broker	NWAPPLIANCE2943	Broker
	Broker	NWAPPLIANCE9	Broker
	Broker	NWAPPLIANCE7952	Broker
□	Concentrator	NWAPPLIANCE22655	Concentrator
	Config Server	NWAPPLIANCE9	Config Server

7. Select the checkbox next to the groups or services you want to assign to the policy, click **Select** in the dialog, and click **Save** in the Policy Detail panel.

Note: Services are filtered for selection based on the type of policies. For example, you can only select concentrator services for a concentrator type policy.

Remove Services or Groups

To remove a host or service from a policy:

1. Go to **ADMIN** > **Health & Wellness**.
2. Click **Policies** tab.

   The Policies view is displayed.
3. Select a policy under a service.

   The Policy Detail is displayed.
4. Select a host or service.
5. Click − .

   The host or service is removed from the policy.

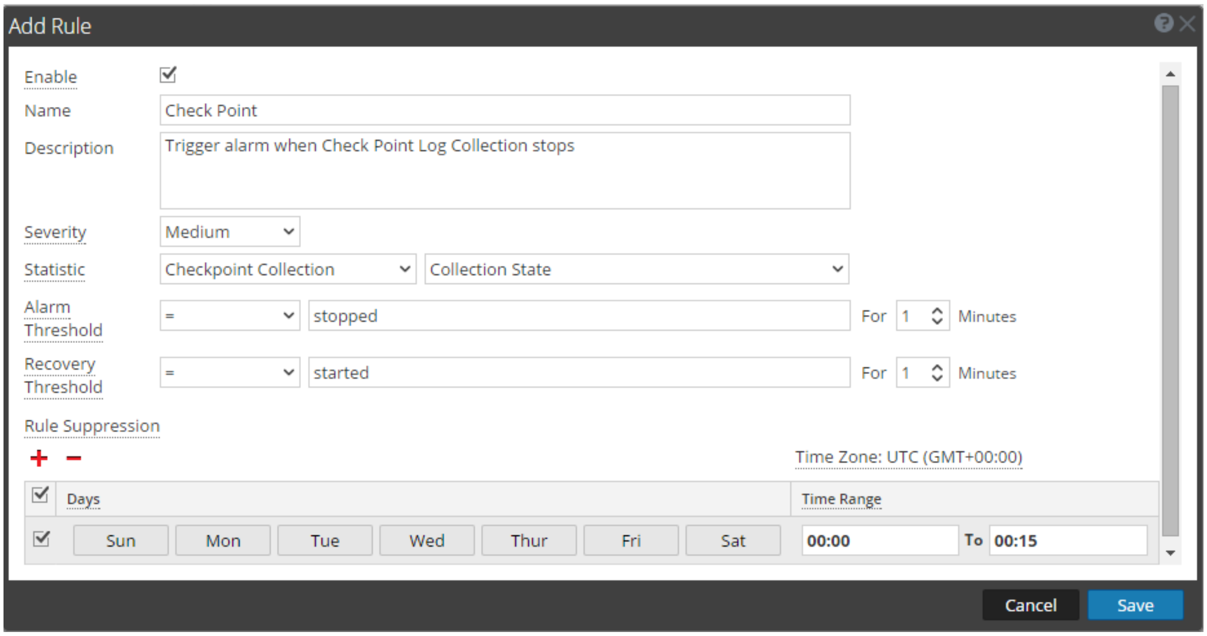
Add or Edit a Rule

To add a rule to a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.
3. Select a policy (for example, **Checkpoint**) under a host or service.

   The Policy Detail is displayed.
4. Depending on whether you are adding an existing rule or adding a rule, do the following:
   - To add: click + in the Rules list toolbar.
   - To edit: select a rule from the Rules list and click ✎.
5. Complete the dialog to define or update the rule.
6. Add the **Description** field as shown in the following example.



Add Rule

Enable ☑

Name: Check Point

Description: Trigger alarm when Check Point Log Collection stops

Severity: Medium

Statistic: Checkpoint Collection | Collection State

Alarm Threshold: = stopped For 1 Minutes

Recovery Threshold: = started For 1 Minutes

Rule Suppression

Time Zone: UTC (GMT+00:00)

☑	Days	Time Range
☑	Sun Mon Tue Wed Thur Fri Sat	00:00 To 00:15

7. Click **OK**.

   The rule is added (or updated) to the policy.

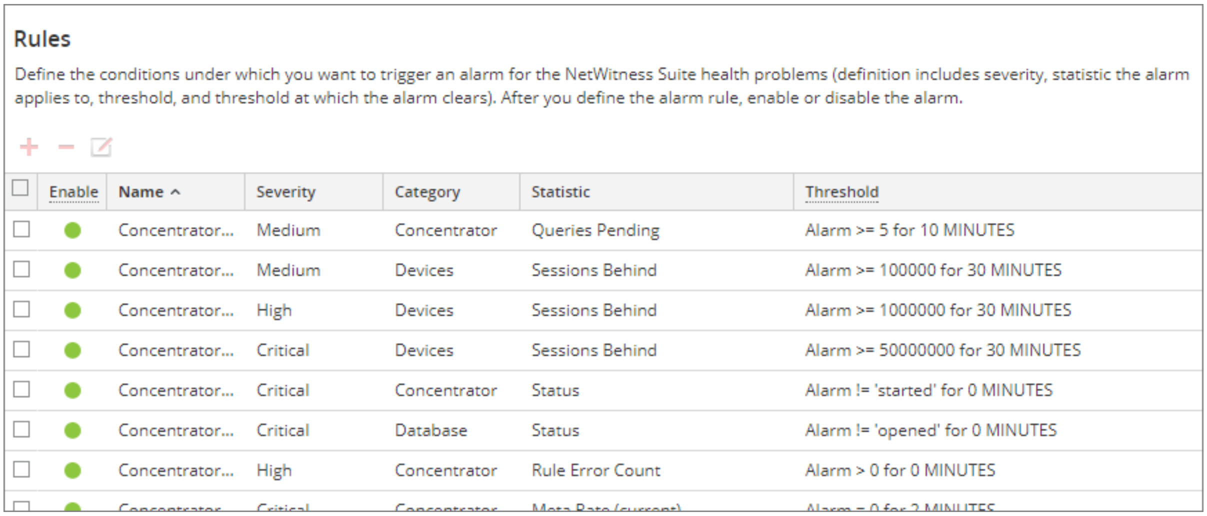
Hide or Show Rule Conditions Columns

To hide or show rule conditions columns in the Rules panel:

1. Go to **ADMIN > Health & Wellness.**
2. Click **Policies** tab.

   The Policies view is displayed.
3. Select a policy under a service.

   The Policy Detail is displayed.
4. Go to the **Rules** panel.



Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Suite health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

□	Enable	Name ^	Severity	Category	Statistic	Threshold
□	●	Concentrator...	Medium	Concentrator	Queries Pending	Alarm >= 5 for 10 MINUTES
□	●	Concentrator...	Medium	Devices	Sessions Behind	Alarm >= 100000 for 30 MINUTES
□	●	Concentrator...	High	Devices	Sessions Behind	Alarm >= 1000000 for 30 MINUTES
□	●	Concentrator...	Critical	Devices	Sessions Behind	Alarm >= 50000000 for 30 MINUTES
□	●	Concentrator...	Critical	Concentrator	Status	Alarm != 'started' for 0 MINUTES
□	●	Concentrator...	Critical	Database	Status	Alarm != 'opened' for 0 MINUTES
□	●	Concentrator...	High	Concentrator	Rule Error Count	Alarm > 0 for 0 MINUTES
□	●	Concentrator...	Critical	Concentrator	Meta Rate (current)	Alarm = 0 for 2 MINUTES

5. Click **v** to the right of **Category** , select **Columns**, and uncheck the **Static** and **Threshold** rule conditions.

   You can check or uncheck any Rules column to show or hide it.
   The **Rules** panel displays without the rule conditions.

Delete a Rule

To remove a host or service from a policy:

1. Go to **ADMIN > Health & Wellness.**
2. Click the **Policies** tab.
   The Policies view is displayed.
3. Select a policy under a service.
   The Policy Detail is displayed.
4. Select a rule from the **Rules** list (for example, **Checkpoint**).
5. Click − .

   The rule is removed from the policy.

Suppress a Rule

1. Click the **Policies** tab.

   The Policies view is displayed.

2. Select a policy under a service.

   The Policy Detail is displayed. You can specify rule suppressions time ranges when you initially add it or you can edit the rule and specify suppression time ranges.

3. Add or edit a rule.

4. In the **Rules Suppression** panel of the **Add** or **Edit Rule** dialog, specify the days and time ranges during which you want the rule suppressed.

Suppress a Policy

1. Add or edit a policy.

   The Policies view is displayed.

2. In the **Policy Suppression** panel:

   a. Select a time zone from the **Time Zone** drop-down list.

      This time zone applies to the entire policy (both policy suppression and rule suppression).

   b. Click + in the toolbar.

   c. Specify the days and time ranges during which you want the policy suppressed.

Add an Email Notification

To add an email notification to a policy:

1. Add or edit a policy.

   The Policies view is displayed.

2. In the **Notification** panel:

   a. Click + in the toolbar.

      A blank EMAIL notification row is displayed.

   b. Select the email:

      - Notification types in the Recipient column (see "Configure Notification Outputs" in the *NetWitness Suite System Configuration Guide* for the source of the values in this drop-down list).

- Notification server in the Notification Server column (see 'Configure Notification Servers" in the *NetWitness Suite System Configuration Guide* for the source of the values in this drop-down list).
- Template server in the Template column (see "Configure Notification Templates" in the *NetWitness Suite System Configuration Guide*for the source of the values in this drop-down list).

Note: Refer to **Include the Default Email Subject Line** if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Delete an Email Notification

To add an email notification to a policy:

1. Add or edit a policy.
   The Policies view is displayed.
2. In the **Notification** panel:
   a. Select an email notification.
   b. Click − .
      The notification is removed.

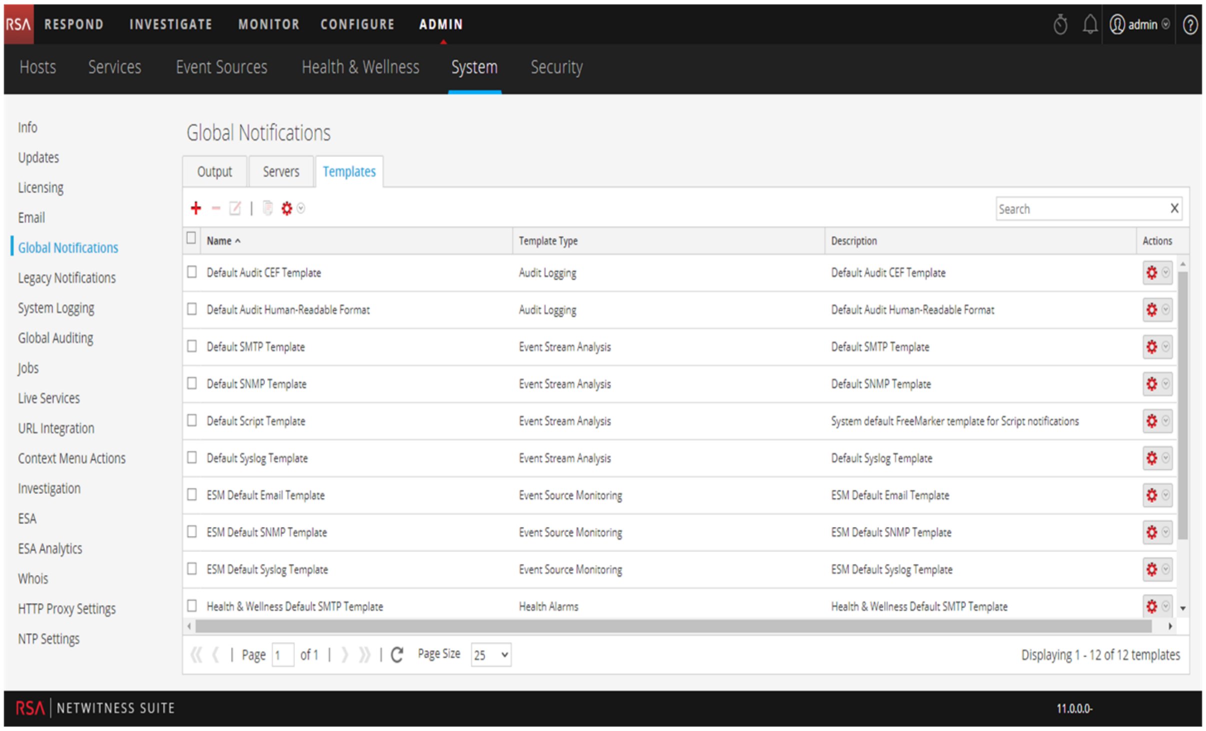
Include the Default Email Subject Line

The emails generated by the notifications you set up for policies do not include the subject line from the Health & Wellness Default Email Notification templates. You need to specify the subject line in the do not include subject lines. This procedure shows you how to insert a subject line into the templates.

For related reference topics, see Policies View and NetWitness Suite Out-of-the-Box Policies.

To include the subject line from a Health & Wellness email template in your email notification:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Select a Health & Wellness Email Template (for example, **Health & Wellness Default SMTP Template**).



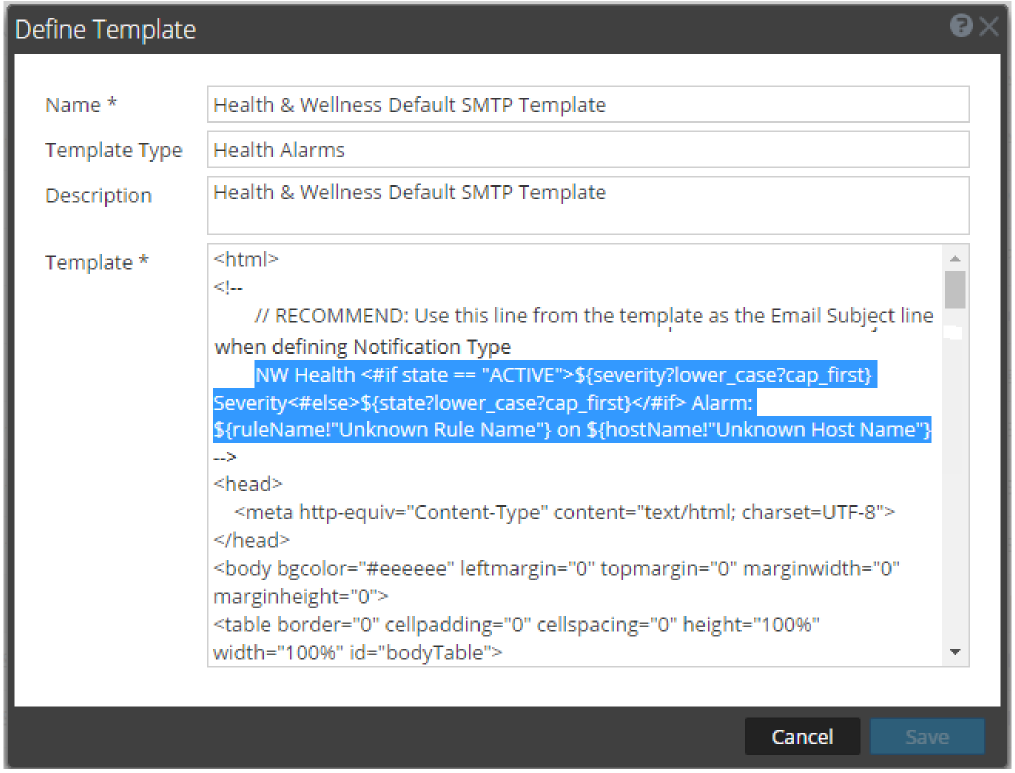
Global Notifications

Name ^	Template Type	Description	Actions
Default Audit CEF Template	Audit Logging	Default Audit CEF Template	
Default Audit Human-Readable Format	Audit Logging	Default Audit Human-Readable Format	
Default SMTP Template	Event Stream Analysis	Default SMTP Template	
Default SNMP Template	Event Stream Analysis	Default SNMP Template	
Default Script Template	Event Stream Analysis	System default FreeMarker template for Script notifications	
Default Syslog Template	Event Stream Analysis	Default Syslog Template	
ESM Default Email Template	Event Source Monitoring	ESM Default Email Template	
ESM Default SNMP Template	Event Source Monitoring	ESM Default SNMP Template	
ESM Default Syslog Template	Event Source Monitoring	ESM Default Syslog Template	
Health & Wellness Default SMTP Template	Health Alarms	Health & Wellness Default SMTP Template	

Displaying 1 - 12 of 12 templates

The Define Template dialog is displayed.

4. Click ✎, then in the **Template** field, copy the Subject Line (Highlight the subject line and press Ctrl-C) into the buffer.



Define Template

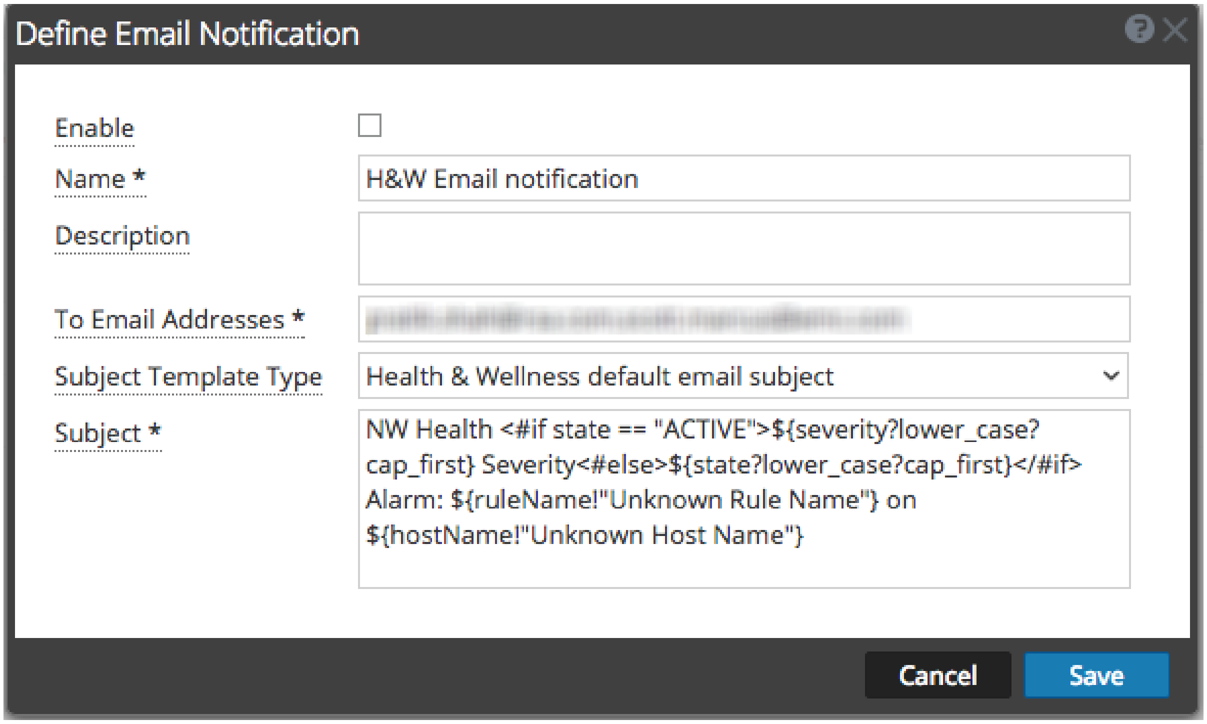
Name *	Health & Wellness Default SMTP Template
Template Type	Health Alarms
Description	Health & Wellness Default SMTP Template

Template *

```
<html>
<!--
      // RECOMMEND: Use this line from the template as the Email Subject line
when defining Notification Type
      NW Health <#if state == "ACTIVE">${severity?lower_case?cap_first}
Severity<#else>${state?lower_case?cap_first}</#if> Alarm:
${ruleName!"Unknown Rule Name"} on ${hostName!"Unknown Host Name"}
-->
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
</head>
<body bgcolor="#eeeeee" leftmargin="0" topmargin="0" marginwidth="0"
marginheight="0">
<table border="0" cellpadding="0" cellspacing="0" height="100%"
width="100%" id="bodyTable">
```

5. Click **Cancel** to close the Template.
6. Click the **Output** tab and select a notification (for example **Health & Wellness**).
7. Click ✎.

   The **Define Email Notification** dialog is displayed.
8. Replace the value in **Subject** field text box with the subject line that you have in the buffer (highlight the existing text and press Ctl-V).



Enable	□
Name *	H&W Email notification
Description	
To Email Addresses *	[redacted]
Subject Template Type	Health & Wellness default email subject
Subject *	NW Health <#if state == "ACTIVE">${severity?lower_case?cap_first} Severity<#else>${state?lower_case?cap_first}</#if> Alarm: ${ruleName!"Unknown Rule Name"} on ${hostName!"Unknown Host Name"}

9. Click **Save**.

Monitor System Statistics

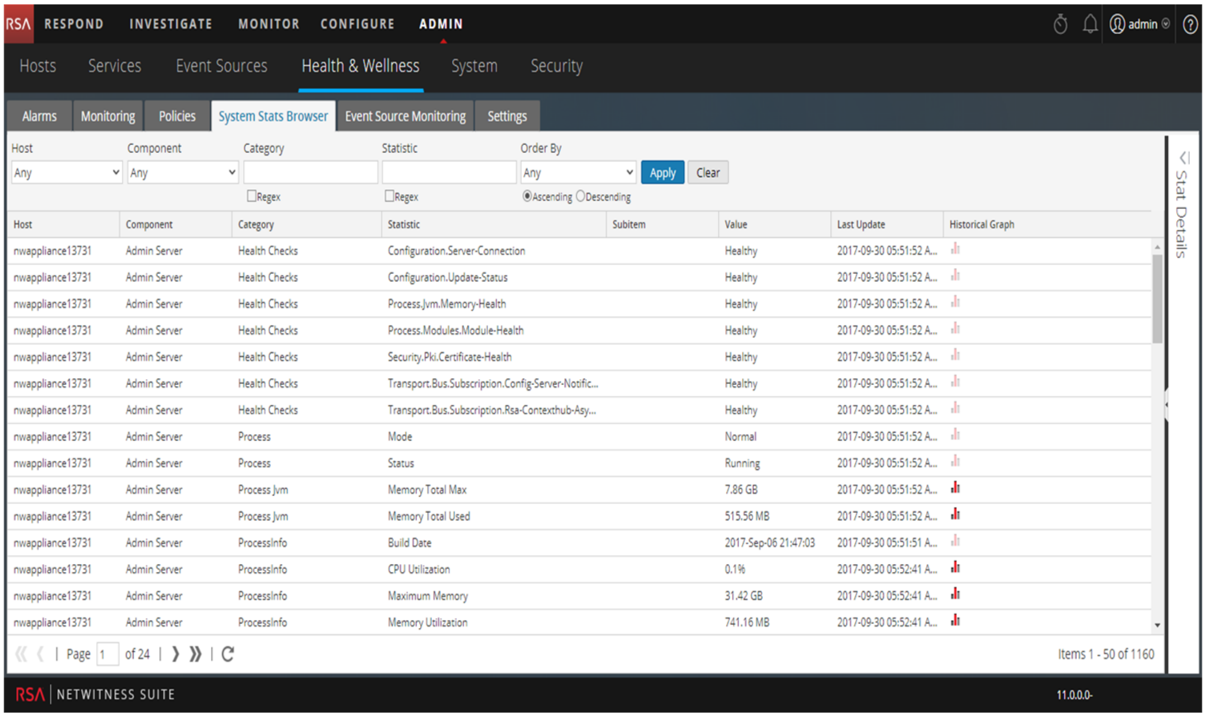
The System Stats Browser filters statistics by the selected host, component running on the host, statistical category, individual statistic, or any combination of host, component, category, and statistic. You can also choose the order in which to display this information.

To access the System Stats browser:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.
2. Click the **System Stats Browser** tab.

The System Stats Browser tab is displayed.



Host: Any
Component: Any
Category: ☐ Regex
Statistic: ☐ Regex
Order By: Any
● Ascending ○ Descending

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
nwappliance13731	Admin Server	Health Checks	Configuration.Server-Connection		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Configuration.Update-Status		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Jvm.Memory-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Modules.Module-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Security.Pki.Certificate-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Config-Server-Notific...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Rsa-Contexthub-Asy...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Mode		Normal	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Status		Running	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Max		7.86 GB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Used		515.56 MB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	ProcessInfo	Build Date		2017-Sep-06 21:47:03	2017-09-30 05:51:51 A...	
nwappliance13731	Admin Server	ProcessInfo	CPU Utilization		0.1%	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	ProcessInfo	Maximum Memory		31.42 GB	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	ProcessInfo	Memory Utilization		741.16 MB	2017-09-30 05:52:41 A...	

Page 1 of 24

Items 1 - 50 of 1160

Filter System Statistics

You can filter the System Statistics in one of the following ways to monitor:

- Statistics collected for a particular host
- Statistics collected for a particular component
- Statistics collected of a particular type or that belongs to a certain category
- Statistics listed in an ordered way as per the selection chosen

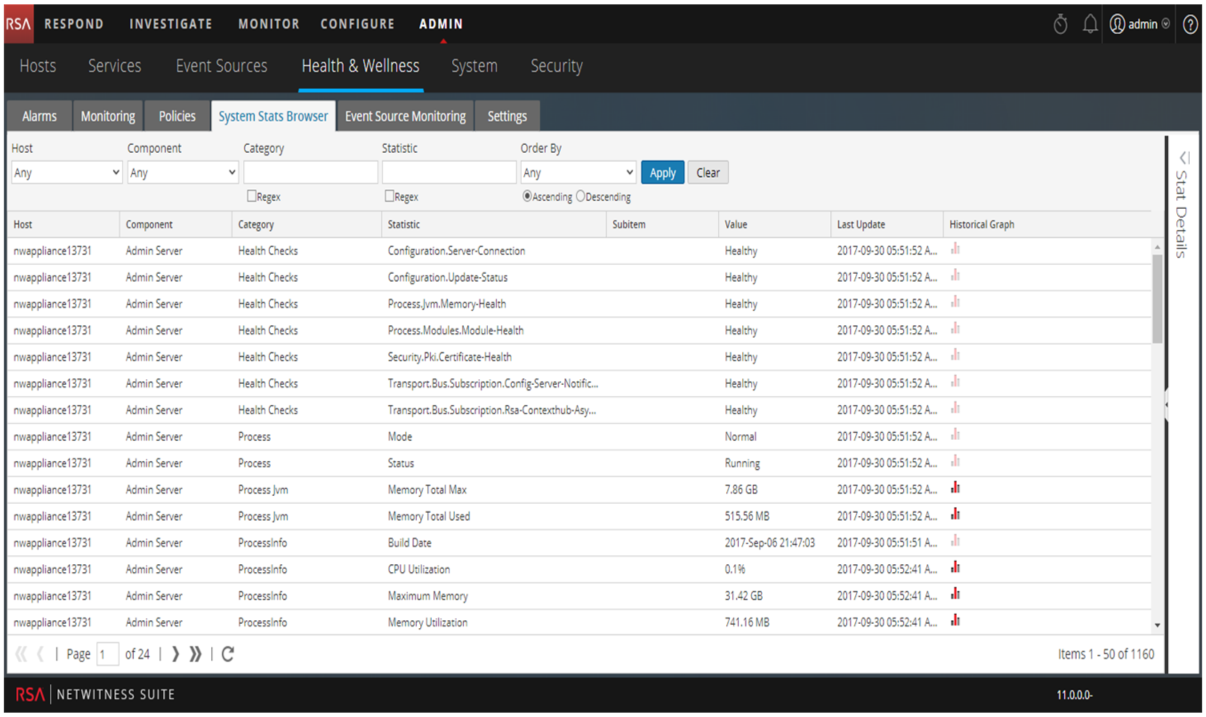
To filter the list of system statistics:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Click **System Stats Browser**.

   The System Stats Browser tab is displayed.



Host: Any
Component: Any
Category: □Regex
Statistic: □Regex
Order By: Any ● Ascending ○ Descending

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
nwappliance13731	Admin Server	Health Checks	Configuration.Server-Connection		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Configuration.Update-Status		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Jvm.Memory-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Modules.Module-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Security.Pki.Certificate-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Config-Server-Notific...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Rsa-Contexthub-Asy...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Mode		Normal	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Status		Running	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Max		7.86 GB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Used		515.56 MB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	ProcessInfo	Build Date		2017-Sep-06 21:47:03	2017-09-30 05:51:51 A...	
nwappliance13731	Admin Server	ProcessInfo	CPU Utilization		0.1%	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	ProcessInfo	Maximum Memory		31.42 GB	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	ProcessInfo	Memory Utilization		741.16 MB	2017-09-30 05:52:41 A...	

Page 1 of 24

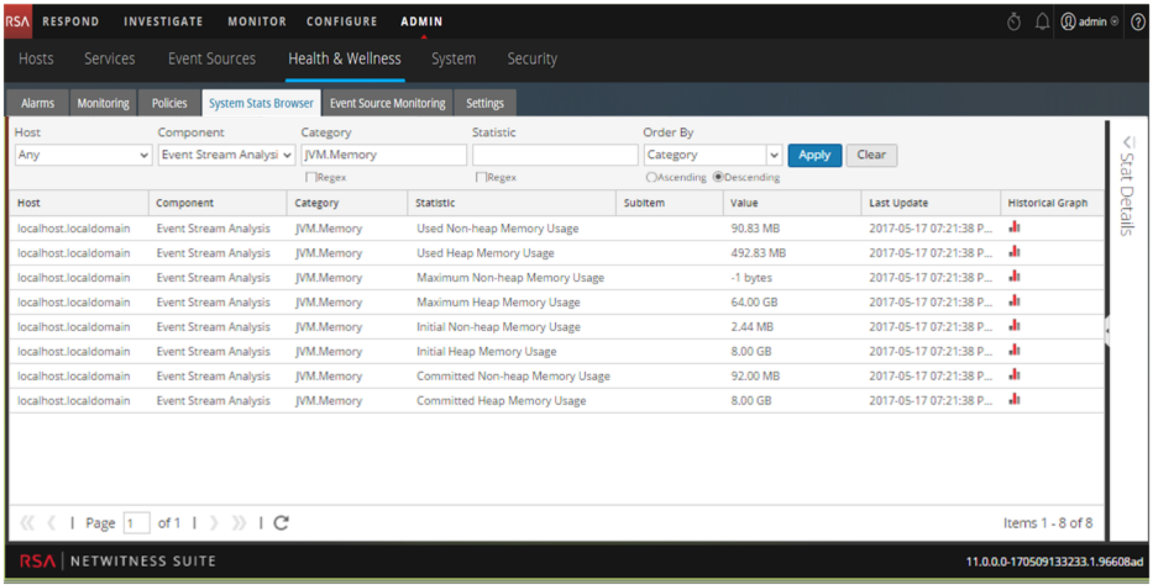
Items 1 - 50 of 1160

Filter the list of System Statistics in one of the following ways:

- To view System Stats of a particular host, select the host in the **Host** drop-down list.
  The System Stats for the selected host is displayed.
- To view System Stats of a particular component, select the component in the **Component** drop-down list.
  The System Stats for the selected component is displayed.
- To view System Stats of a particular category, type the category name in the **Category** field.
  Select **Regex** to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
  The System Stats for the selected category is displayed.
- To order the list of statistics in a preferred order you can set the order in the **OrderBy** column
- To view a particular statistic across hosts, type the statistic name in the **Statistic** field.
  Select **Regex** to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
  The System Stats for the selected statistics is displayed.

  The following figure shows the System Stats Browser filtered by the

NWAPPLIANCE10604 host listed in descending statistical category order.



Host: Any
Component: Event Stream Analysi
Category: JVM.Memory □ Regex
Statistic: □ Regex
Order By: Category ○ Ascending ● Descending

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
localhost.localdomain	Event Stream Analysis	JVM.Memory	Used Non-heap Memory Usage		90.83 MB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Used Heap Memory Usage		492.83 MB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Maximum Non-heap Memory Usage		-1 bytes	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Maximum Heap Memory Usage		64.00 GB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Initial Non-heap Memory Usage		2.44 MB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Initial Heap Memory Usage		8.00 GB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Committed Non-heap Memory Usage		92.00 MB	2017-05-17 07:21:38 P...	📊
localhost.localdomain	Event Stream Analysis	JVM.Memory	Committed Heap Memory Usage		8.00 GB	2017-05-17 07:21:38 P...	📊

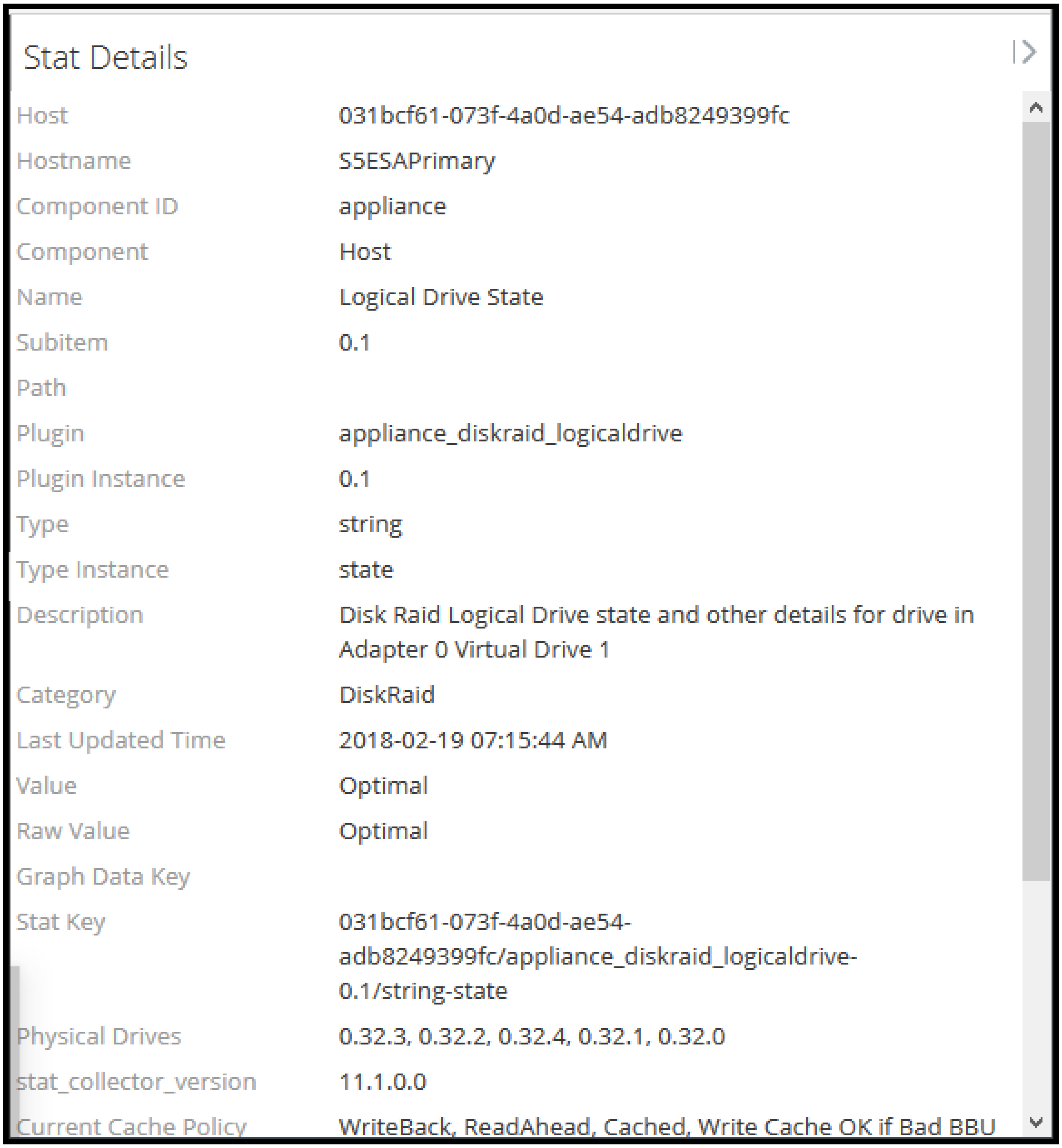
Page 1 of 1

Items 1 - 8 of 8

4. To view the details for an individual statistic:

   a. Select a row to select a statistic.

   b. Click <| .
   The Stat Details is displayed.



Stat Details

Host	031bcf61-073f-4a0d-ae54-adb8249399fc
Hostname	S5ESAPrimary
Component ID	appliance
Component	Host
Name	Logical Drive State
Subitem	0.1
Path	
Plugin	appliance_diskraid_logicaldrive
Plugin Instance	0.1
Type	string
Type Instance	state
Description	Disk Raid Logical Drive state and other details for drive in Adapter 0 Virtual Drive 1
Category	DiskRaid
Last Updated Time	2018-02-19 07:15:44 AM
Value	Optimal
Raw Value	Optimal
Graph Data Key	
Stat Key	031bcf61-073f-4a0d-ae54-adb8249399fc/appliance_diskraid_logicaldrive-0.1/string-state
Physical Drives	0.32.3, 0.32.2, 0.32.4, 0.32.1, 0.32.0
stat_collector_version	11.1.0.0
Current Cache Policy	WriteBack, ReadAhead, Cached, Write Cache OK if Bad BBU

For details on various parameters in the **ADMIN** > **Health & Wellness** > **System Stats Browser** view, see System Stats Browser View

View Historical Graph of System Statistics

The historical graph of the collected system stats gives you information about the variation of the stats over a time frame selected.

To view a historical graph:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

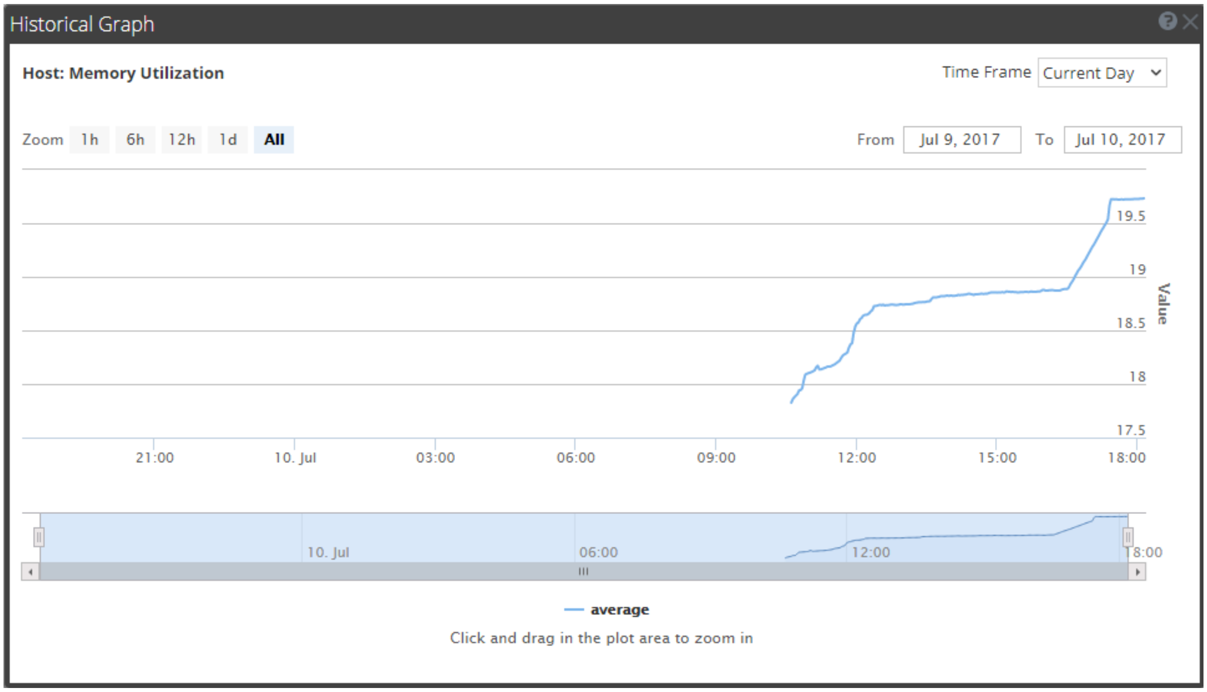
2. Click the **System Stats Browser** tab.

3. In the System Stats Browser tab, specify the filter criteria to display the statistics you want.

4. In the **Historical Graph** column, select 📊.

   The Historical graph for the selected statistic is displayed.

   The figure below gives an example of the historical graph for Memory Utilization statistic for a host.



Historical Graph

Host: Memory Utilization

Time Frame: Current Day

From: Jul 9, 2017 To: Jul 10, 2017

Click and drag in the plot area to zoom in

The graphical view is customized to display the statistics collected for the current day and the values are zoomed in for an interval of an hour (10.15 - 11.15 hrs). Hover over the graph to view the details at a particular instant. For example, in the figure it displays the memory utilization at 11.00 hrs.

Note: You can customize the graph view by selecting the Time Frame and Date range. You can zoom in using the zoom in value, time window, or by just a click and a drag in the plot area. For details on the parameters to customize and zoom in functions, see Historical Graph for System Stats. Any break or gap in chart line indicates that the service or host was down during that time.

Monitor Service Statistics

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

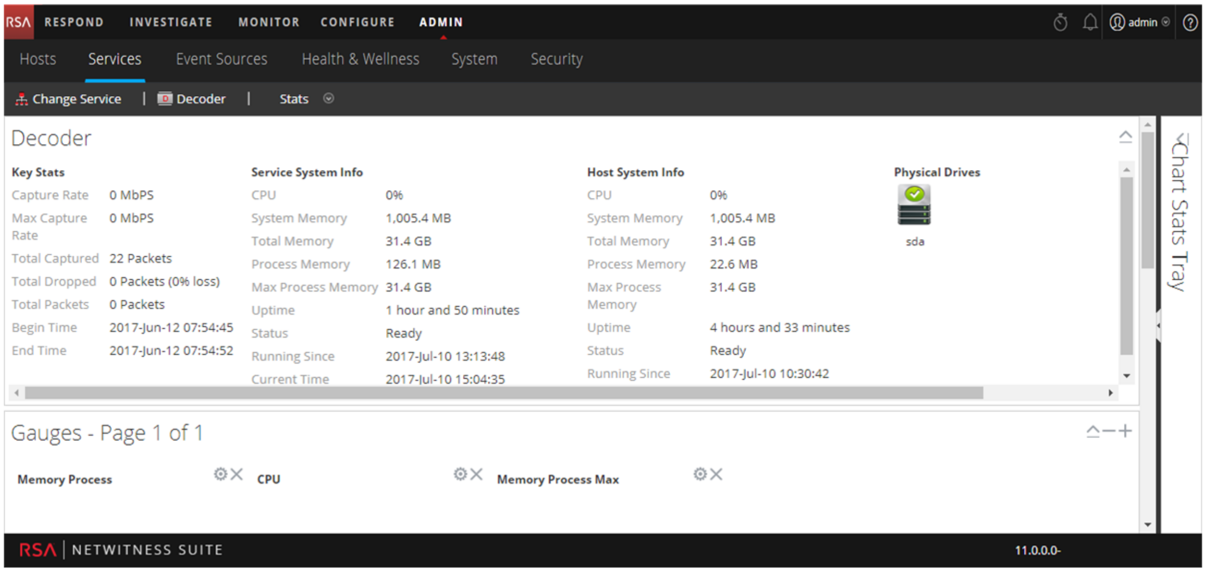
Although different statistics are available for different types of services, certain elements are common for any Core device.

To monitor service statistics in NetWitness Suite:

1. Go to **ADMIN** > **Services**.

   The Services view is displayed.

2. Select a service, and select **View** > **Stats** in the Actions column.



Decoder

Key Stats	
Capture Rate	0 MbPS
Max Capture Rate	0 MbPS
Total Captured	22 Packets
Total Dropped	0 Packets (0% loss)
Total Packets	0 Packets
Begin Time	2017-Jun-12 07:54:45
End Time	2017-Jun-12 07:54:52

Service System Info	
CPU	0%
System Memory	1,005.4 MB
Total Memory	31.4 GB
Process Memory	126.1 MB
Max Process Memory	31.4 GB
Uptime	1 hour and 50 minutes
Status	Ready
Running Since	2017-Jul-10 13:13:48
Current Time	2017-Jul-10 15:04:35

Host System Info	
CPU	0%
System Memory	1,005.4 MB
Total Memory	31.4 GB
Process Memory	22.6 MB
Max Process Memory	31.4 GB
Uptime	4 hours and 33 minutes
Status	Ready
Running Since	2017-Jul-10 10:30:42

Physical Drives

sda

Gauges - Page 1 of 1

Memory Process

CPU

Memory Process Max

3. To customize the view: Collapse or expand charts, for example expand the Chart Stats Tray to see available charts. Drag a section up or down to change the sequence. For example, drag the Gauges section to the top so that it is above the Summary Stats section.

Add Statistics to a Gauge or Chart

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

Create a Gauge for a Statistic

To create a gauge for a statistic in the Services Stats view:

1. Go to **ADMIN** > **Services**.

   The Admin Services View is displayed.

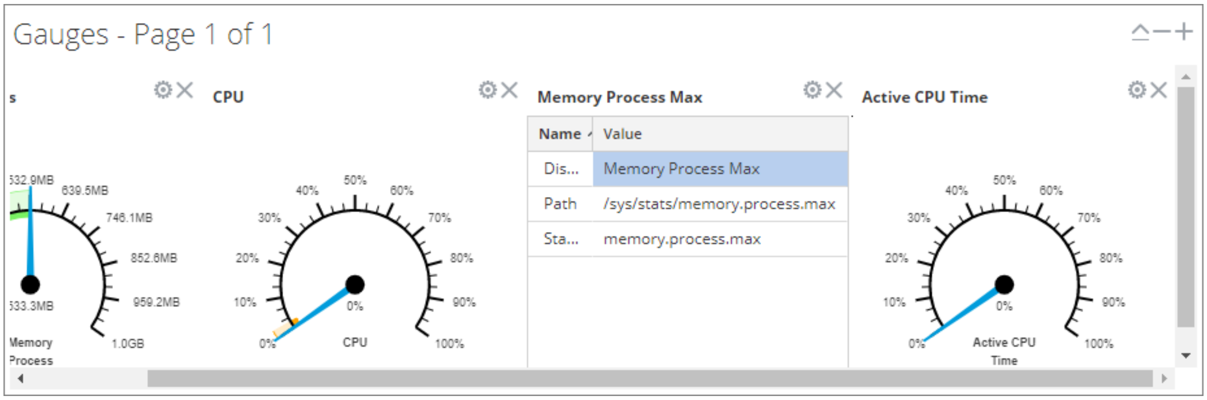
2. Select a service and select **View** > **Stats** in the Actions column.

   The Chart Stats Tray is displayed on the right side.

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

4. From the **Chart Stats Tray**, click on any statistic and drag it into the **Gauges** section.

   A gauge is created for the statistic. If there is no space for the gauge, a new page is created on the Gauges section and the gauge is added to the new page. In the example, the Active CPU Time chart was added to the Gauges section by dragging it from the Chart Stats Tray.



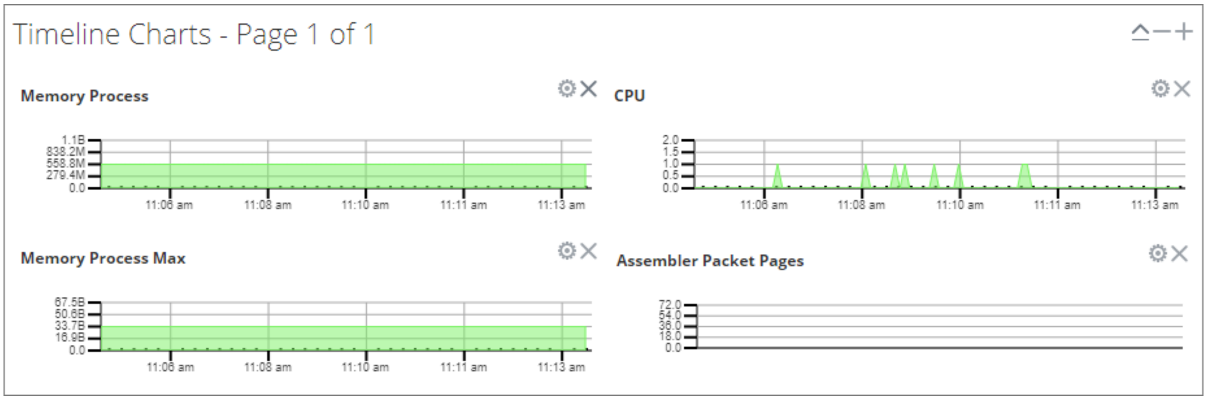
Name	Value
Dis...	Memory Process Max
Path	/sys/stats/memory.process.max
Sta...	memory.process.max

Create a Timeline Chart for a Statistic

To create a timeline for a statistic:

From the **Chart Stats Tray**, click on a statistic and drag it into the **Timeline Charts** or the **Historical Timeline Charts** section.

A timeline chart is created for the statistic. If there is no space for the chart, a new page is created on the Timeline Chart section and the chart is added to the new page. In the example, the Assembler Packet Pages chart was added to the Timeline Charts section by dragging it from the Chart Stats Tray.



Search for a Statistic in the Chart Stats Tray

To search for a statistic, type a search term; for example, **session**, in the Search field and press **RETURN**. Statistics that match are displayed with the matching word highlighted.

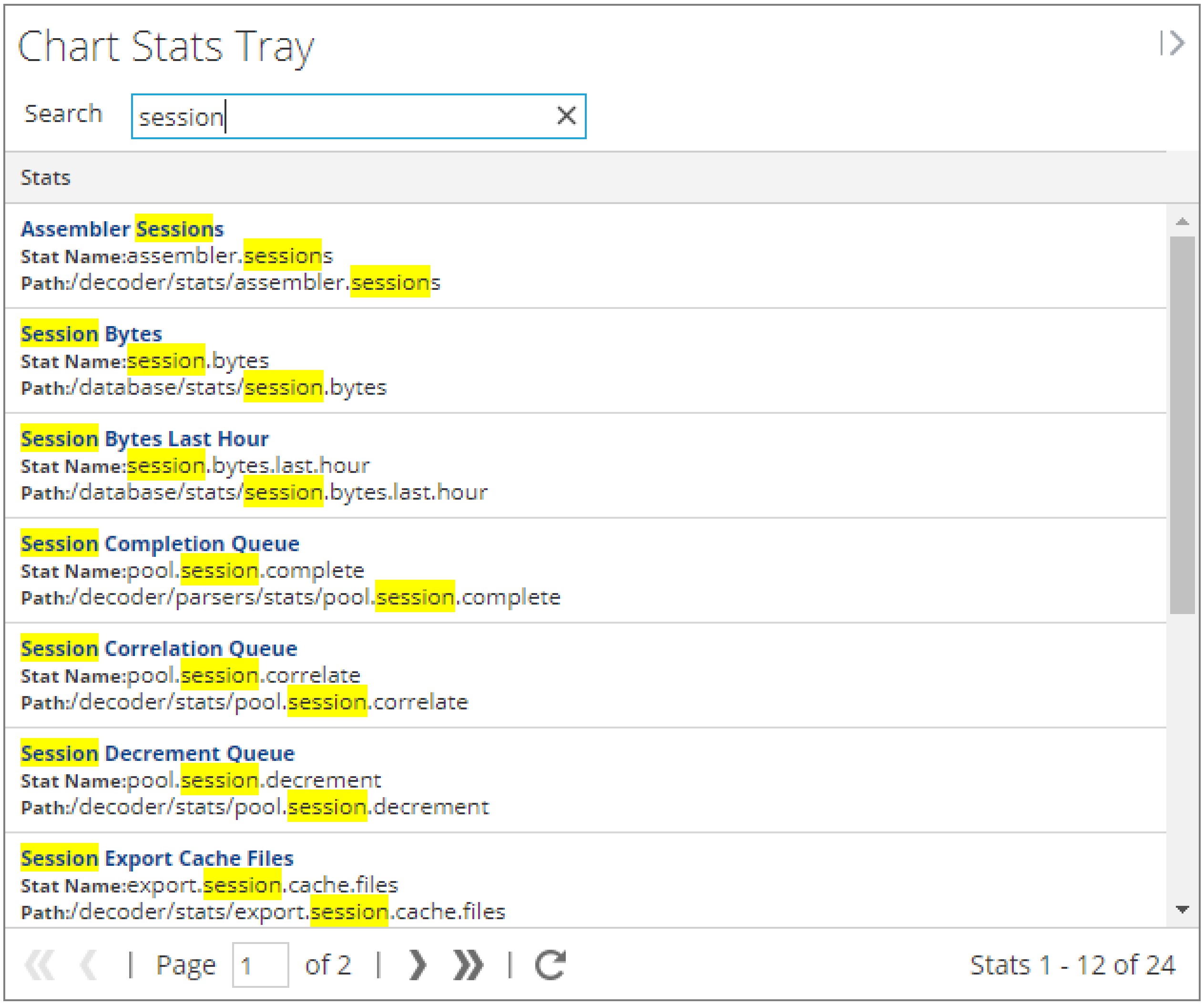


Chart Stats Tray

Search session

Stats

Assembler Sessions
Stat Name:assembler.sessions
Path:/decoder/stats/assembler.sessions

Session Bytes
Stat Name:session.bytes
Path:/database/stats/session.bytes

Session Bytes Last Hour
Stat Name:session.bytes.last.hour
Path:/database/stats/session.bytes.last.hour

Session Completion Queue
Stat Name:pool.session.complete
Path:/decoder/parsers/stats/pool.session.complete

Session Correlation Queue
Stat Name:pool.session.correlate
Path:/decoder/stats/pool.session.correlate

Session Decrement Queue
Stat Name:pool.session.decrement
Path:/decoder/stats/pool.session.decrement

Session Export Cache Files
Stat Name:export.session.cache.files
Path:/decoder/stats/export.session.cache.files

Page 1 of 2

Stats 1 - 12 of 24

Edit Properties of Statistics Gauges

The Gauges section of the Service Stats view presents statistics in the form of an analog gauge. The properties of each individual gauge are editable; all gauges have an editable title and some have additional editable properties.

Edit Properties of a Gauge

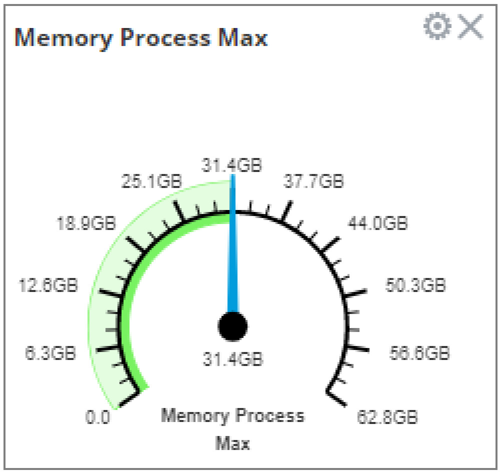
1. Go to **ADMIN** > **Services**

   The Admin Services view is displayed.

2. Select a service and select **View** > **Stats** in the Actions column.

   The Service Stats view includes the Gauges section.

3. Go to the gauge for which you want to edit properties (for example, **Memory Process**).



4. Click the Properties icon (⚙) to display the parameter names and values.

5. To highlight the value of the **Display Name** field, double-click on the value; for example, **Memory Process**.

   > **Note:** Clicking the other two values does nothing because the properties are not editable in the gauge.

5. Type a new value for the Display Name and click the **Properties** icon (⚙).

   The new title replaces **Memory Process**.

Add Stats to the Gauges Section

You can add more gauges by dragging a statistic from the **Chart Stats Tray** into the **Gauges** section.

1. To expand the Chart Stats Tray, click <|.

2. Scroll down and select a statistic, for example, **Session Rate (maximum)**.

3. Drag the statistic to the **Gauges** section.

   The new gauge is displayed in the Gauges section.

Edit Properties of Timeline Charts

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

To access the charts:

1. Go to **ADMIN > Services**.

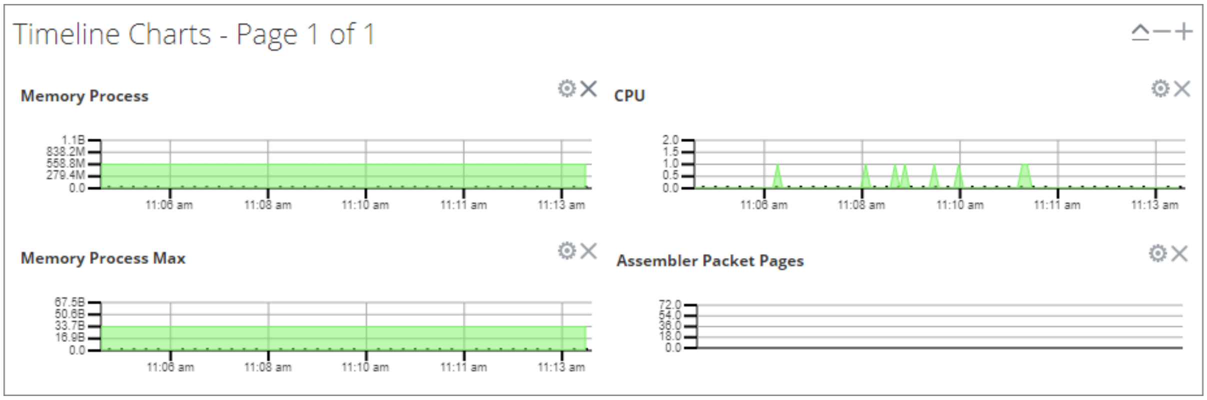
2. Select a service and click **Stats**.

   The Services Stats view is displayed. The charts are in this view.

Edit Properties of a Timeline

To edit properties of a timeline chart:

1. Go to the timeline chart for which you want to edit properties (for example, **Memory Process**).



2. Click the **Properties** icon (⚙) to display the parameter names and values.

3. Double-click on a value (for example, the **Display Name** field) to make the value editable.

> **Note:** Clicking the other two values does nothing because the properties are not editable in the chart.

4. Type a new value and click the **Properties** icon.

   The timeline chart is displayed with new values.

Edit Properties of a Historical Timeline

To edit properties of a historical timeline chart:

1. Go to Historical Timeline Charts.
2. Click the **Properties** icon (⚙) to display the parameter names and values.
3. Click on a value (for example, **01/27/2015** for the **Begin Date** field) to make the value editable.
4. Type a new value.
5. Edit the **End Date** and **Display Name** if required.
6. Click the **Properties** icon (⚙).

   The historical timeline is displayed with new values.

Note: To return the properties of the historical timeline chart back to the default so that the values dynamically update, remove the Begin Date and the End Date, place your cursor in the Begin Date field, and refresh your browser.

Add Stats to Timeline Charts

You can add timeline charts by dragging a statistic from the Chart Stats Tray into the Timelines section.

1. To expand the Chart Stats Tray, click <| .
2. Scroll down and select a statistic; for example, **Session Rate (maximum)**.
3. Drag the statistic to the **Timelines Section**.

   The new timeline is displayed in the Timelines section.

Monitor Hosts and Services

NetWitness Suite provides a way to monitor the status of hosts and services installed. You can view the current health of all the hosts, services running on the hosts, their CPU usage and memory consumption and the host details and service details.

To monitor hosts and services in NetWitness Suite:

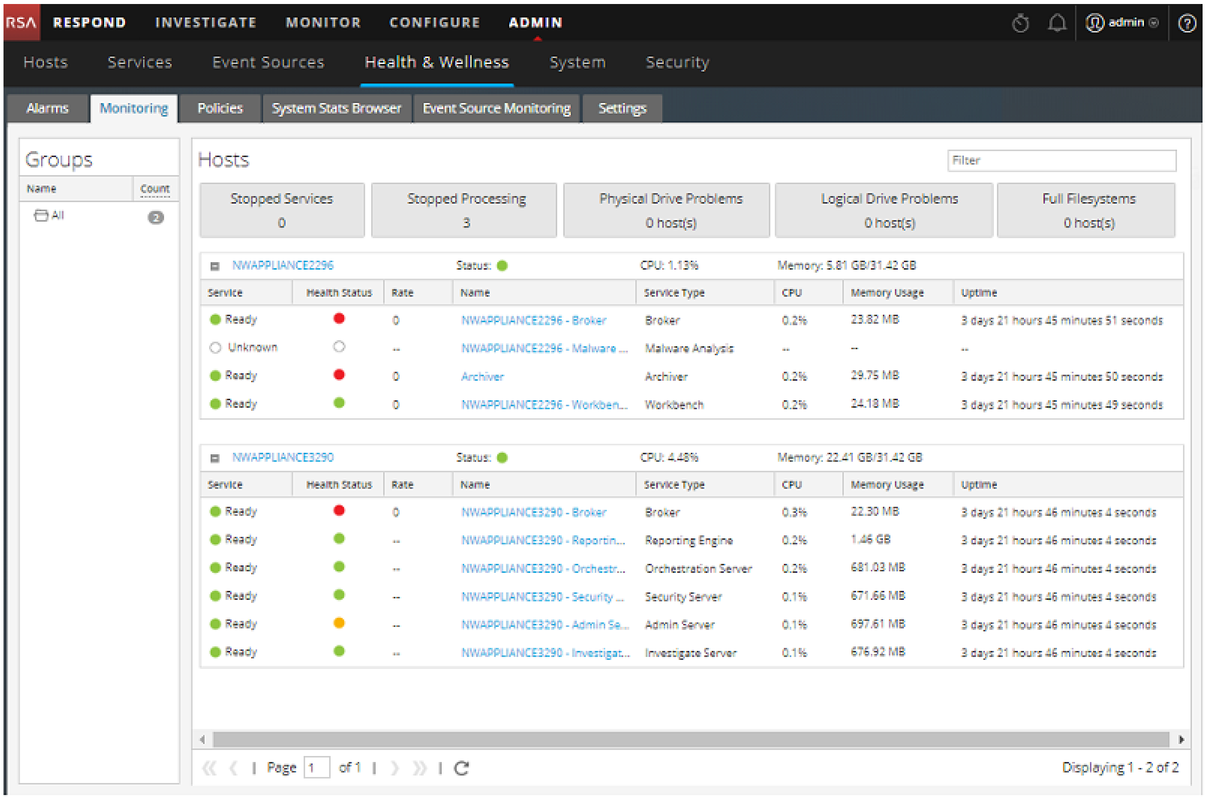
1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Select the **Monitoring** tab.

   A list of all hosts and their associated services that belong to the group **All** is displayed by default.

   The operational status, CPU usage, and memory usage for each host is displayed.



Stopped Services	Stopped Processing	Physical Drive Problems	Logical Drive Problems	Full Filesystems
0	3	0 host(s)	0 host(s)	0 host(s)

NWAPPLIANCE2296 Status: 🟢 CPU: 1.13% Memory: 5.81 GB/31.42 GB

Service	Health Status	Rate	Name	Service Type	CPU	Memory Usage	Uptime
🟢 Ready	🔴	0	NWAPPLIANCE2296 - Broker	Broker	0.2%	23.82 MB	3 days 21 hours 45 minutes 51 seconds
○ Unknown	○	--	NWAPPLIANCE2296 - Malware ...	Malware Analysis	--	--	--
🟢 Ready	🔴	0	Archiver	Archiver	0.2%	29.75 MB	3 days 21 hours 45 minutes 50 seconds
🟢 Ready	🟢	0	NWAPPLIANCE2296 - Workben...	Workbench	0.2%	24.18 MB	3 days 21 hours 45 minutes 49 seconds

NWAPPLIANCE3290 Status: 🟢 CPU: 4.48% Memory: 22.41 GB/31.42 GB

Service	Health Status	Rate	Name	Service Type	CPU	Memory Usage	Uptime
🟢 Ready	🔴	0	NWAPPLIANCE3290 - Broker	Broker	0.3%	22.30 MB	3 days 21 hours 46 minutes 4 seconds
🟢 Ready	🟢	--	NWAPPLIANCE3290 - Reportin...	Reporting Engine	0.2%	1.46 GB	3 days 21 hours 46 minutes 4 seconds
🟢 Ready	🟢	--	NWAPPLIANCE3290 - Orchestr...	Orchestration Server	0.2%	681.03 MB	3 days 21 hours 46 minutes 4 seconds
🟢 Ready	🟢	--	NWAPPLIANCE3290 - Security ...	Security Server	0.1%	671.66 MB	3 days 21 hours 46 minutes 4 seconds
🟢 Ready	🟠	--	NWAPPLIANCE3290 - Admin Se...	Admin Server	0.1%	697.61 MB	3 days 21 hours 46 minutes 4 seconds
🟢 Ready	🟢	--	NWAPPLIANCE3290 - Investigat...	Investigate Server	0.1%	676.92 MB	3 days 21 hours 46 minutes 4 seconds

   Click ⊞ to the left of a host (⊞ is visible if there are services installed on a host)

3. A list of services installed on the selected host is displayed.

   The name, operating status, CPU usage, memory usage, and the time operating for each service is displayed.

Filter Hosts and Services in the Monitoring View

You can filter hosts and services in the monitoring view in one of the following ways:

- Hosts belonging to a particular group
- Specific host and its associated services
- Hosts whose services are stopped
- Hosts whose services have stopped processing or processing has been turned off

- Hosts that have Physical drive problems
- Hosts that have Logical drive problems
- Hosts that have Full File systems

For the related reference topic, see Monitoring View.

To filter hosts and services:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open by default.

2. Select the **Monitoring** tab.

3. Filter the hosts and services in one of the following ways:

   - To view a list of hosts and their associated services belonging to a particular group, select the group in the Groups panel.

     All hosts and their associated services belonging to the specified group are displayed in the Hosts panel.

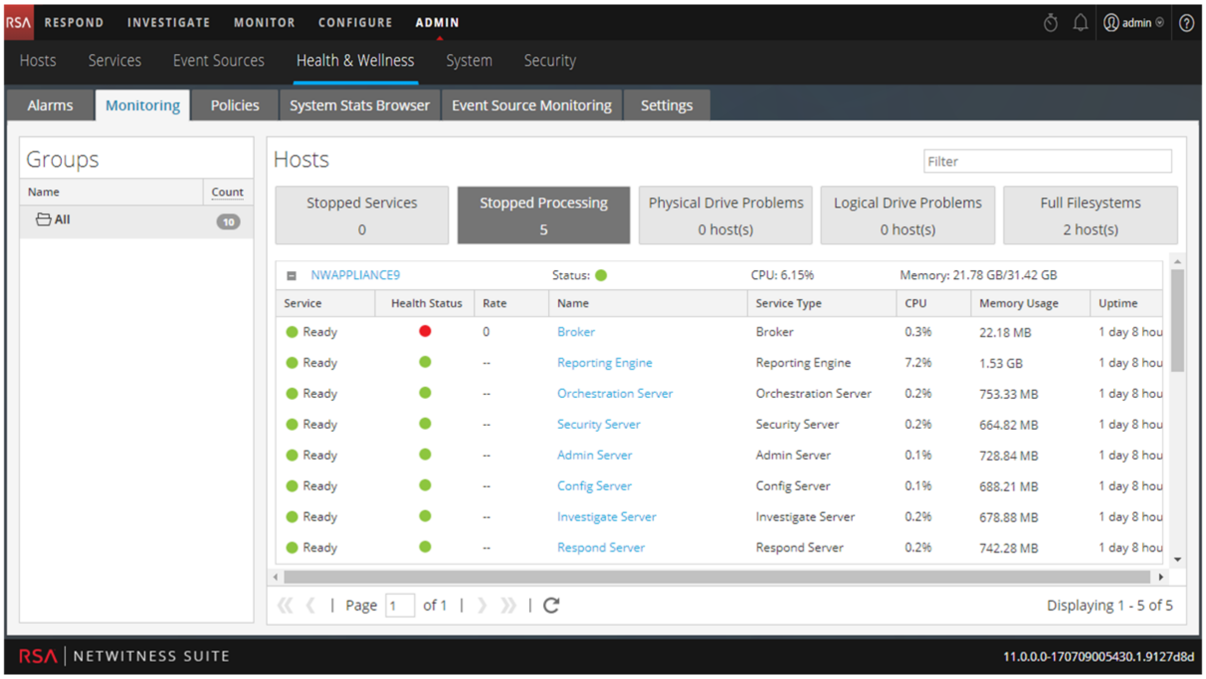
     Note: The grouping of hosts is derived from the groups created in the Administration page. All groups created in the Administration page are displayed here.

     For example, if you select the group **LC_Group** in the Groups panel, a list of all hosts that are part of the group are displayed.

   - To view a list of all services that have stopped processing, click **Stopped Processing** in the Hosts panel.

     A list of all the hosts that have at least one service with the status as stopped processing is displayed.

     Note: The buttons on the top display the System Statistics for all the hosts configured in NetWitness Suite and does not change with application of filters on groups.



NWAPPLIANCE9 Status: ● CPU: 6.15% Memory: 21.78 GB/31.42 GB

Service	Health Status	Rate	Name	Service Type	CPU	Memory Usage	Uptime
● Ready	●	0	Broker	Broker	0.3%	22.18 MB	1 day 8 hou
● Ready	●	--	Reporting Engine	Reporting Engine	7.2%	1.53 GB	1 day 8 hou
● Ready	●	--	Orchestration Server	Orchestration Server	0.2%	753.33 MB	1 day 8 hou
● Ready	●	--	Security Server	Security Server	0.2%	664.82 MB	1 day 8 hou
● Ready	●	--	Admin Server	Admin Server	0.1%	728.84 MB	1 day 8 hou
● Ready	●	--	Config Server	Config Server	0.1%	688.21 MB	1 day 8 hou
● Ready	●	--	Investigate Server	Investigate Server	0.2%	678.88 MB	1 day 8 hou
● Ready	●	--	Respond Server	Respond Server	0.2%	742.28 MB	1 day 8 hou

Page 1 of 1

Displaying 1 - 5 of 5

11.0.0.0-170709005430.1.9127d8d

Note: In a similar way you can filter the list of hosts and the associated services by choosing the right filter
- Click Stopped Services to display a list of all stopped services.
- Click Physical Drive Problems to display a list of host with Physical Drive Problems.
- Type the host name in the Filter box to display only the required host and the services running on the host.

Monitor Host Details

You can view the details of the host, its memory and CPU usage, system information, the physical drive, logical drive and file system details to further investigate if you encounter some problem with the host.

To view host details:

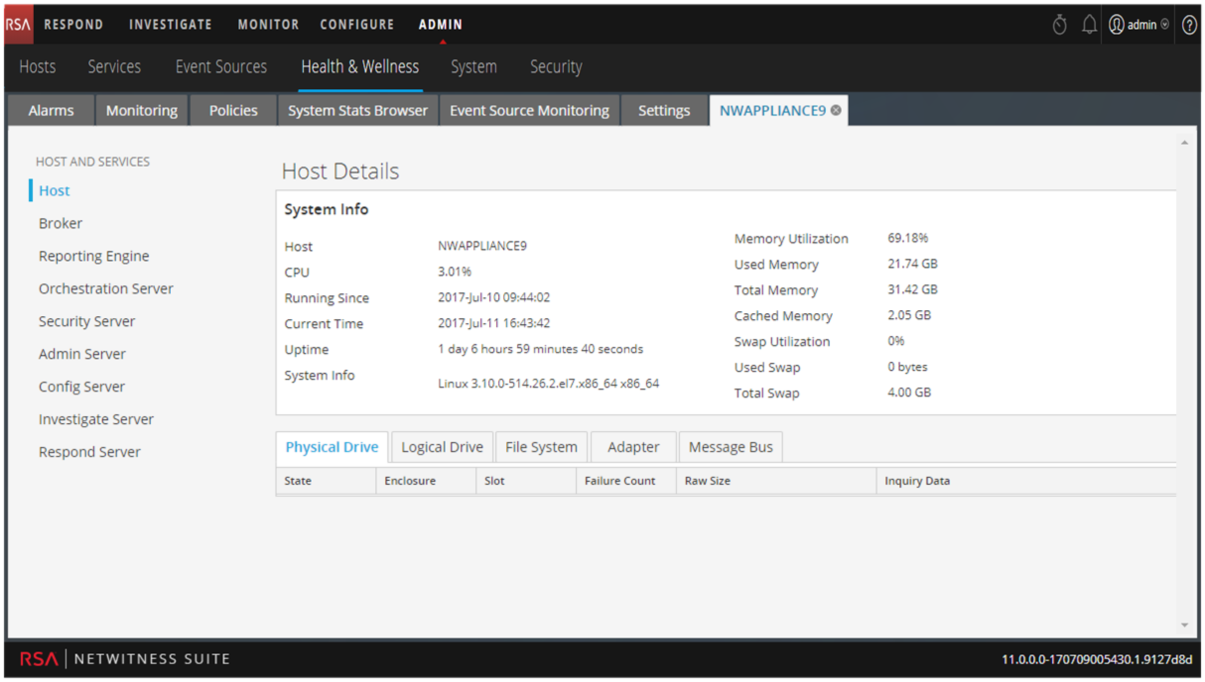
1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Select the **Monitoring** tab.

3. Click a host in the **Hosts** panel.

The Host Details view is displayed as a new page.



Host Details

System Info

Host	NWAPPLIANCE9	Memory Utilization	69.18%
CPU	3.01%	Used Memory	21.74 GB
Running Since	2017-Jul-10 09:44:02	Total Memory	31.42 GB
Current Time	2017-Jul-11 16:43:42	Cached Memory	2.05 GB
Uptime	1 day 6 hours 59 minutes 40 seconds	Swap Utilization	0%
System Info	Linux 3.10.0-514.26.2.el7.x86_64 x86_64	Used Swap	0 bytes
		Total Swap	4.00 GB

State	Enclosure	Slot	Failure Count	Raw Size	Inquiry Data

Monitor Service Details

You can view the details of a service, its memory and CPU usage, system information, and various details depending on the service selected.

To view service details:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

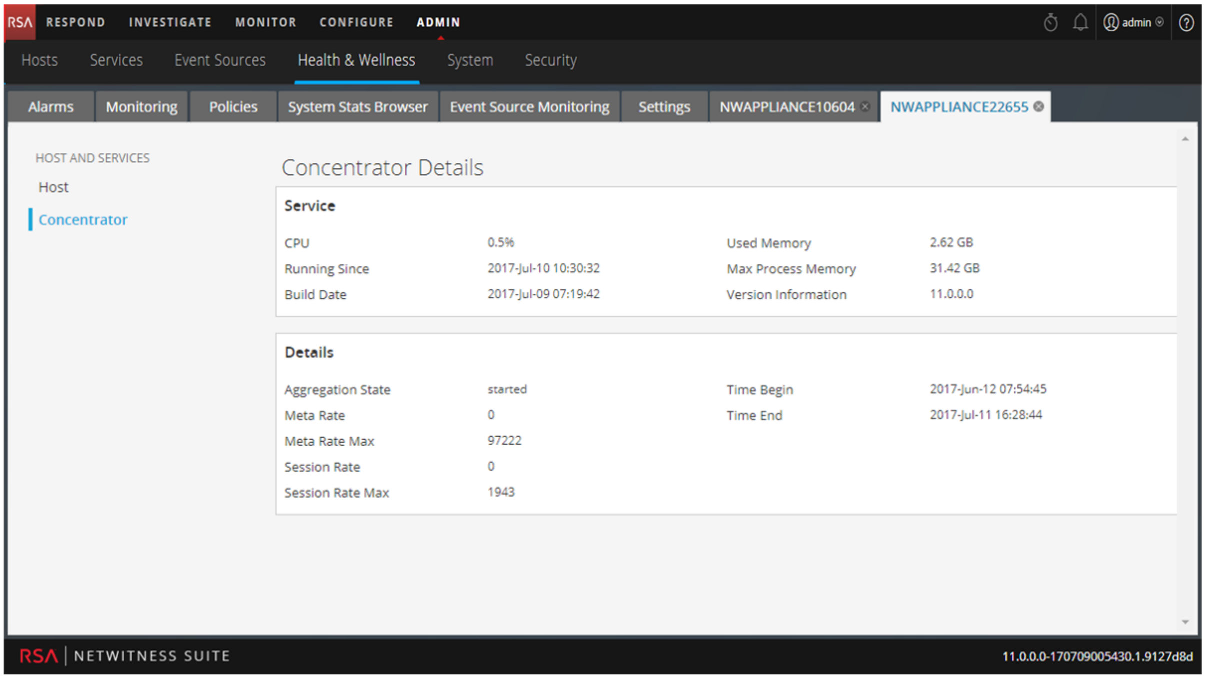
2. Select the **Monitoring** tab.

3. Click ⊞ for a host in the Hosts panel.

   A list of services running on the host is displayed.

4. Click on any service.

   The service details view is displayed as a new page. The Archiver, Broker, Concentrator, and Decoder service details views have the **Service** and **Details** panels.



Concentrator Details

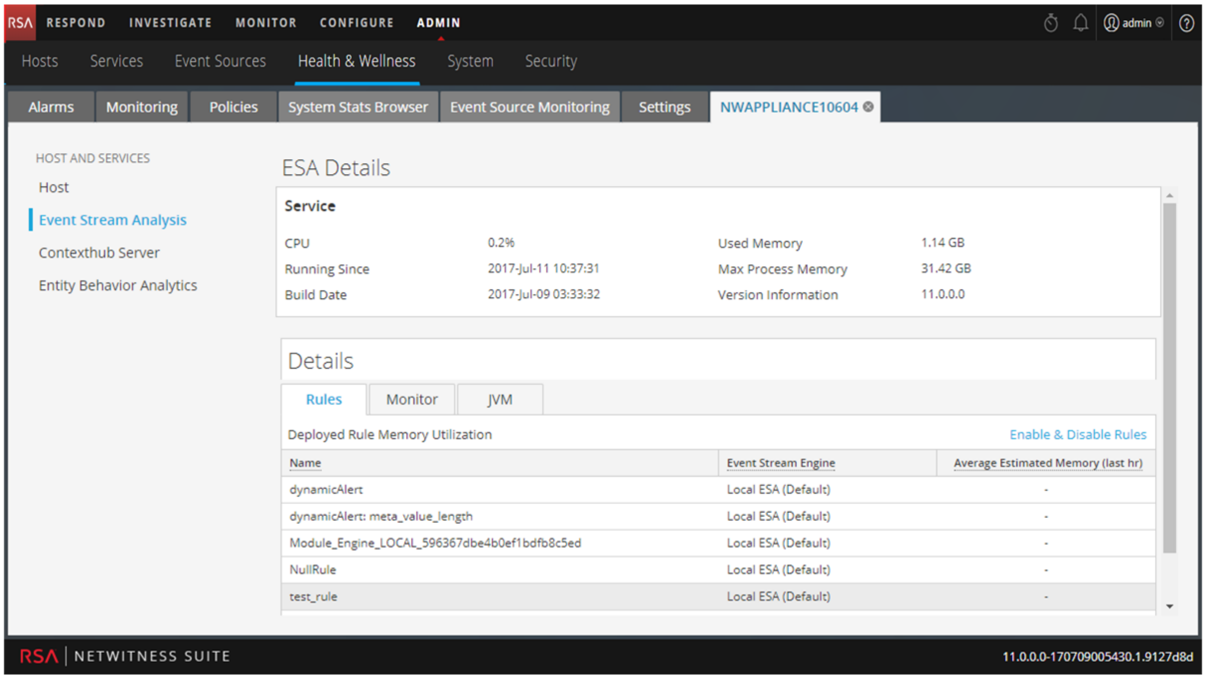
Service

CPU	0.5%	Used Memory	2.62 GB
Running Since	2017-Jul-10 10:30:32	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:19:42	Version Information	11.0.0.0

Details

Aggregation State	started	Time Begin	2017-Jun-12 07:54:45
Meta Rate	0	Time End	2017-Jul-11 16:28:44
Meta Rate Max	97222		
Session Rate	0		
Session Rate Max	1943		

The Event Stream Analysis (ESA) service details view has the **Service**and **Details** panels, plus the **Monitor** and **JVM** tabs that show additional statistics.



ESA Details

Service

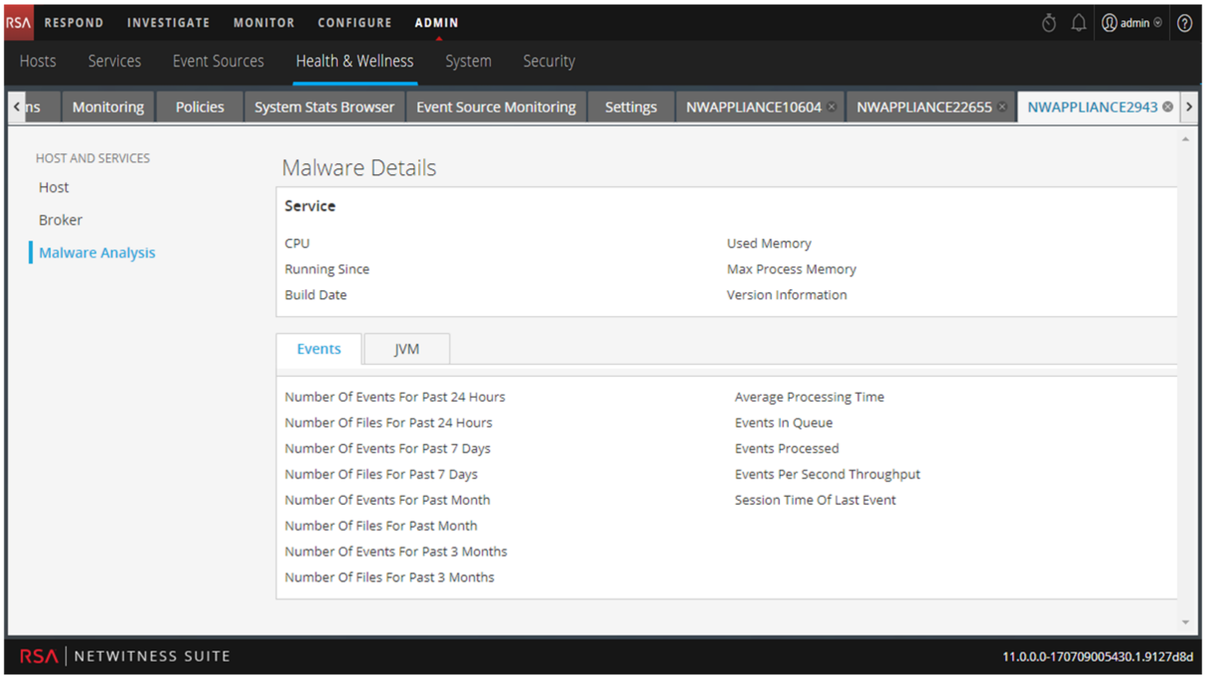
CPU	0.2%	Used Memory	1.14 GB
Running Since	2017-Jul-11 10:37:31	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 03:33:32	Version Information	11.0.0.0

Details

Deployed Rule Memory Utilization

Name	Event Stream Engine	Average Estimated Memory (last hr)
dynamicAlert	Local ESA (Default)	-
dynamicAlert: meta_value_length	Local ESA (Default)	-
Module_Engine_LOCAL_596367dbe4b0ef1bdfb8c5ed	Local ESA (Default)	-
NullRule	Local ESA (Default)	-
test_rule	Local ESA (Default)	-

The Malware Analysis service details view has the **Service** panel plus the **Rules, Events,** and **JVM** tabs that show additional statistics.



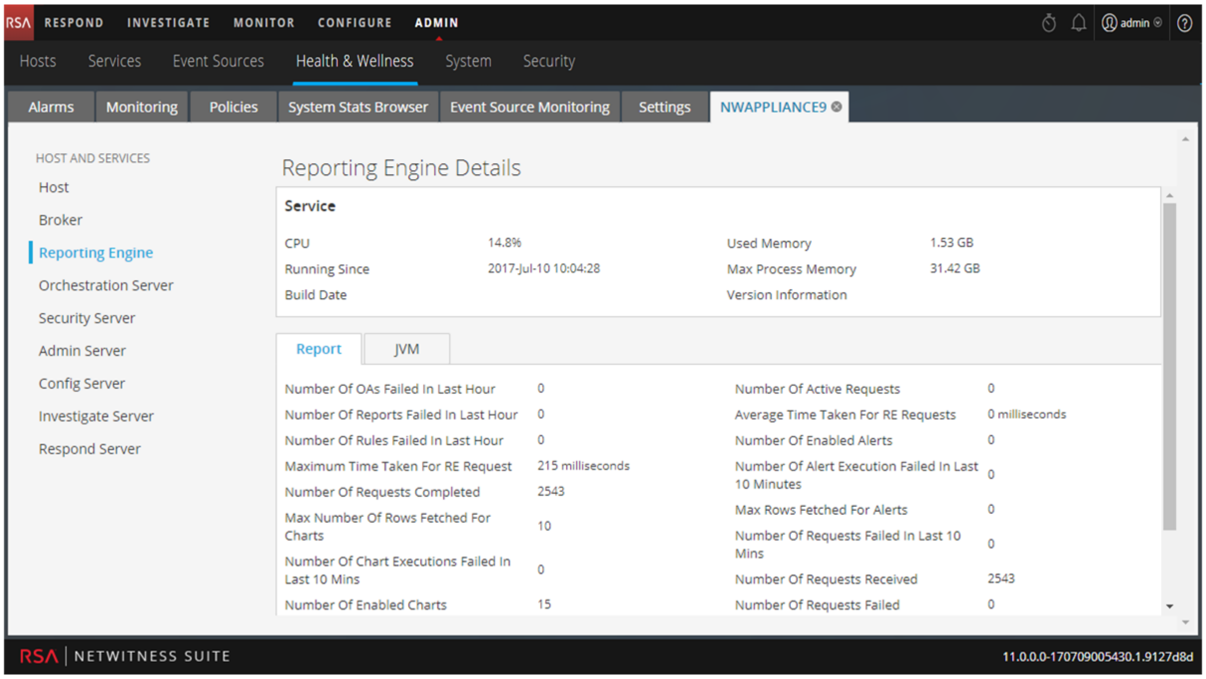
Malware Details

Service

CPU	Used Memory
Running Since	Max Process Memory
Build Date	Version Information

Number Of Events For Past 24 Hours	Average Processing Time
Number Of Files For Past 24 Hours	Events In Queue
Number Of Events For Past 7 Days	Events Processed
Number Of Files For Past 7 Days	Events Per Second Throughput
Number Of Events For Past Month	Session Time Of Last Event
Number Of Files For Past Month	
Number Of Events For Past 3 Months	
Number Of Files For Past 3 Months	

The Reporting Engine service details view has the **Service** panel plus the **Report** and **JVM** tabs that show additional statistics.



Reporting Engine Details

Service

CPU	14.8%	Used Memory	1.53 GB
Running Since	2017-Jul-10 10:04:28	Max Process Memory	31.42 GB
Build Date		Version Information	

Number Of OAs Failed In Last Hour	0	Number Of Active Requests	0
Number Of Reports Failed In Last Hour	0	Average Time Taken For RE Requests	0 milliseconds
Number Of Rules Failed In Last Hour	0	Number Of Enabled Alerts	0
Maximum Time Taken For RE Request	215 milliseconds	Number Of Alert Execution Failed In Last 10 Minutes	0
Number Of Requests Completed	2543	Max Rows Fetched For Alerts	0
Max Number Of Rows Fetched For Charts	10	Number Of Requests Failed In Last 10 Mins	0
Number Of Chart Executions Failed In Last 10 Mins	0	Number Of Requests Received	2543
Number Of Enabled Charts	15	Number Of Requests Failed	0

> **Note:** Alternatively, you can access the service details page by clicking the services listed in the options panel in the Host Details view.

Refer to Monitoring View for a detailed description of the Details view for each service.

Monitor Event Sources

The event source monitoring feature of NetWitness Suite provides the following functionalities:

- Support for failover
- Provides a consolidated list of event sources and their associated collector and log decoder devices
- Regex support for rules
- Decommission
- Filtering capabilities
- Historical graph

In addition, you can monitor event sources, check the number of events generated from a source type and view the historical graph of the events collected. To monitor event sources you have to configure the event sources so that they generate and send out notifications when required.

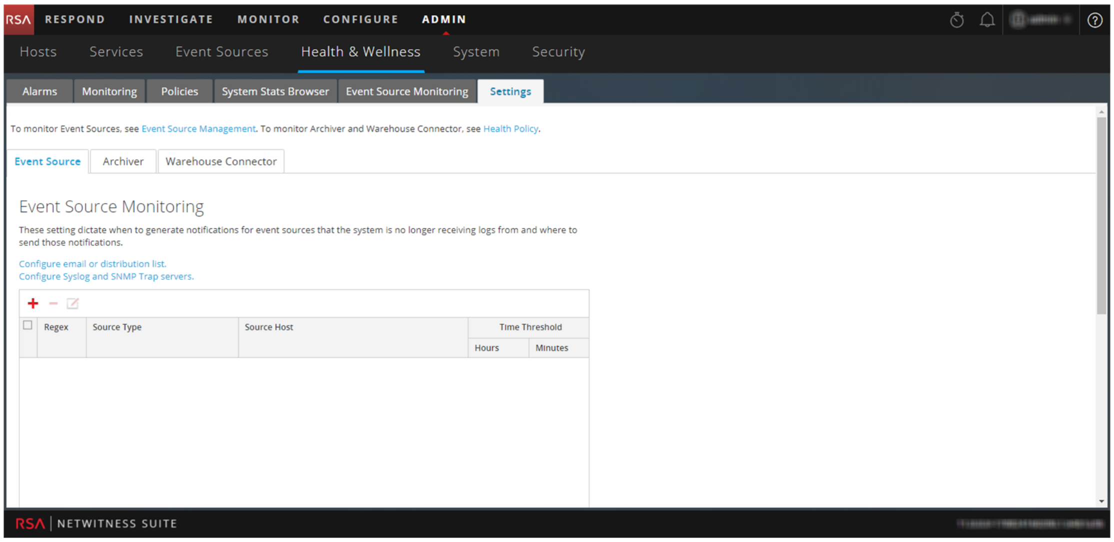
Configure Event Source Monitoring

To monitor event sources you have to configure the event sources so that they generate and send out notifications when required. For the related reference topic, see Health and Wellness Settings View - Event Sources.

To configure and enable event monitoring in NetWitness Suite:

1. Go to **ADMIN** > **Health & Wellness**.
2. Select **Settings** > **Event Source**.

   The Event Source tab is displayed.



To monitor Event Sources, see Event Source Management. To monitor Archiver and Warehouse Connector, see Health Policy.

Event Source Monitoring

These setting dictate when to generate notifications for event sources that the system is no longer receiving logs from and where to send those notifications.

Configure email or distribution list.
Configure Syslog and SNMP Trap servers.

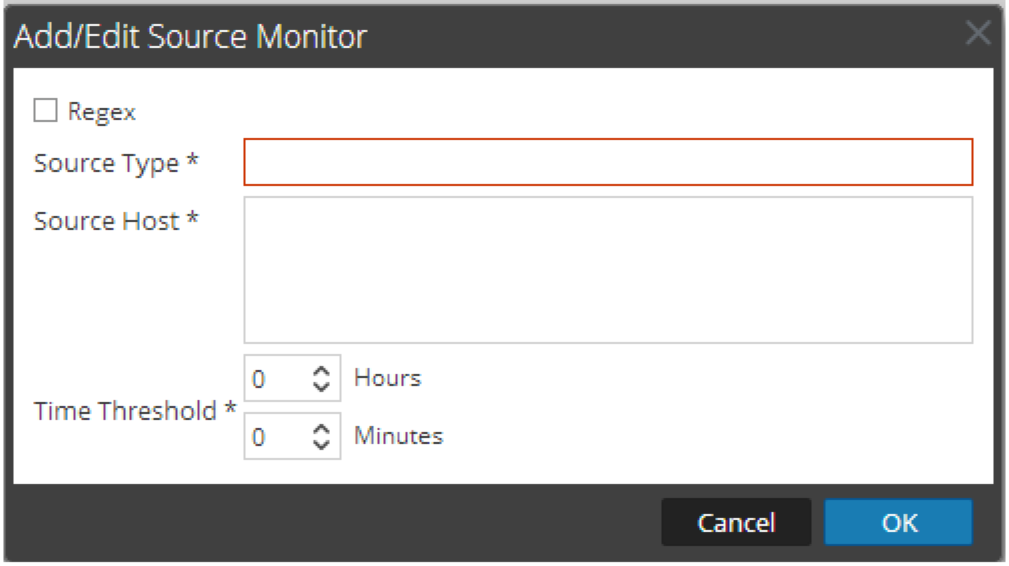
□	Regex	Source Type	Source Host	Time Threshold	
				Hours	Minutes

3. Under **Event Source Monitoring**, click +.

   The Add/Edit Source Monitor dialog is displayed.

4. Define the **Source Type**, **Source Host**, and **Time Threshold** for the source of the event source that you want to monitor to detect when NetWitness Suite stops receiving logs from it. If you do not specify a **Time Threshold**, NetWitness Suite monitors the event source until you set a threshold.

   Note: For **Source Type** and **Source Host**, you must specify the values that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view. You add or modify the the event sources that you want to monitor. The two parameters that identify an event source are **Source Type** and **Source Host**. You can use **globbing** (pattern matching and wildcard characters) to specify the **Source Type** and **Source Host** of event sources



Add/Edit Source Monitor

☐ Regex

Source Type *

Source Host *

Time Threshold * 0 Hours 0 Minutes

5. Click **OK**.

   The event source is displayed in the panel.

6. Configure the method of notification, by doing one of the following:

   - Select **Configure email or distribution list**.

     The AMIN > System > Email Configuration Panel is displayed so that you can specify to whom the notifications are sent.

   - Select **Configure Syslog and SNMP Trap servers**.

     The Administration > System Auditing Configuration panel is displayed so that you can configure the Syslog and SNMP Traps to which the notifications are sent.

7. Click **Apply**.

   NetWitness Suite begins sending notifications when it stops receiving events from this event source after the time threshold has elapsed.

For details on parameters in the Event Source Monitoring settings view, see Event Source Monitoring View.

Decommission Event Source Monitoring

If a Log Collector service (Local Collector or Remote Collector) for which you set up Event Source monitoring becomes inoperable, NetWitness Suite continues to notify that you it is not receiving events from it until you decommission the Collector.

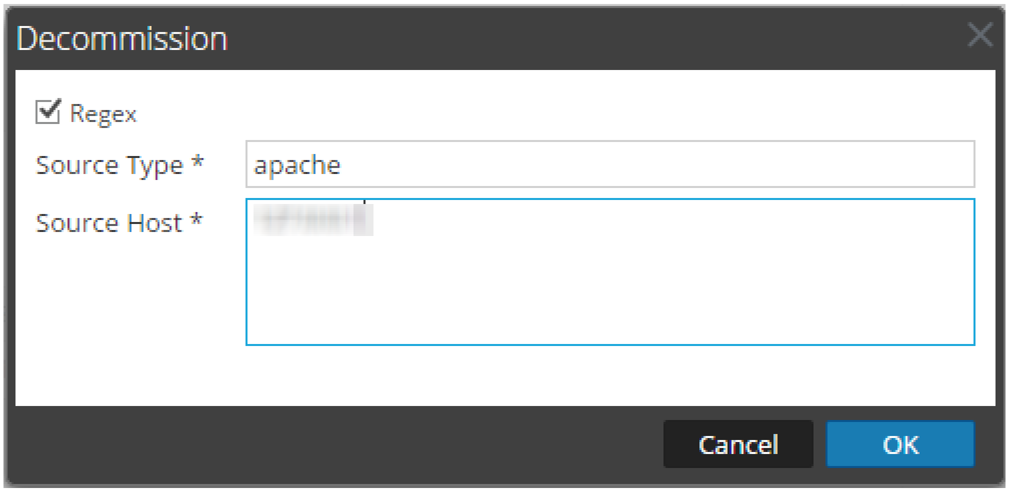
> **Caution:** If you configured a failover Local Collector for a Remote Collector and the Local Collector fails over to a standby Log Decoder, you must decommission the Local Collector to stop the notifications.

To decommission event source monitoring for an event source:

1. Go to **ADMIN**> **Health & Wellness**.
2. Select **Settings** > **Event Source**.

   The **Event Source** tab is displayed.
3. Under **Decommission**, click +.

   The **Decommission** dialog displays.
4. Define the **Source Type** and the **Source Host** for the source for which you want to decommission event monitoring notifications.



Decommission

☑ Regex

Source Type * apache

Source Host * [redacted]

Filter Event Sources

You can choose a filter to display:

- Events belonging to a particular event source
- Events belonging to particular event source types
- Events collected from a particular log Collector
- Events list arranged in a order based on the Event Source Type, Log Collector, Log Decoder or Last Event Time.

To filter the list of event sources:

1. Go to **ADMIN > Health & Wellness**.
2. Select **Event Source Monitoring**.
3. Filter the list in one of the following ways:

- To view the events generated by a particular event source, type the required event source in the **Event Source** field. Select **Regex** to enable Regex filter and click **Apply**. It performs a regular expression search against text and lists out the specified category. This field also supports globbing pattern matching.
  All events generated by the Event Source specified are displayed.
- To view events collected from a particular Log Collector, select a Log Collector from the drop-down list and click **Apply**.
  A list of all events being collected from the specified Log Collector from various event sources is displayed.

Note: Similarly, you can also choose the following filters:
- To view events belonging to an event source type, select the event source type and click **Apply**.
- To view events received in a specified time frame, select the required time frame and click **Apply**. You can further filter the query results to contain only event sources that logs have been received from within the selected time or the query results to contain only event sources that logs have not been received from within the selected time.

For details on various parameters and description, see Event Source Monitoring View.

View Historical Graph of Events Collected for an Event Source

The historical graph of the events collected from an event source gives you information about the variation of the collection over a time frame selected.

To view a historical graph:

1. Go to **ADMIN > Health & Wellness**.
   The Health & Wellness view is displayed with the Alarms tab open.

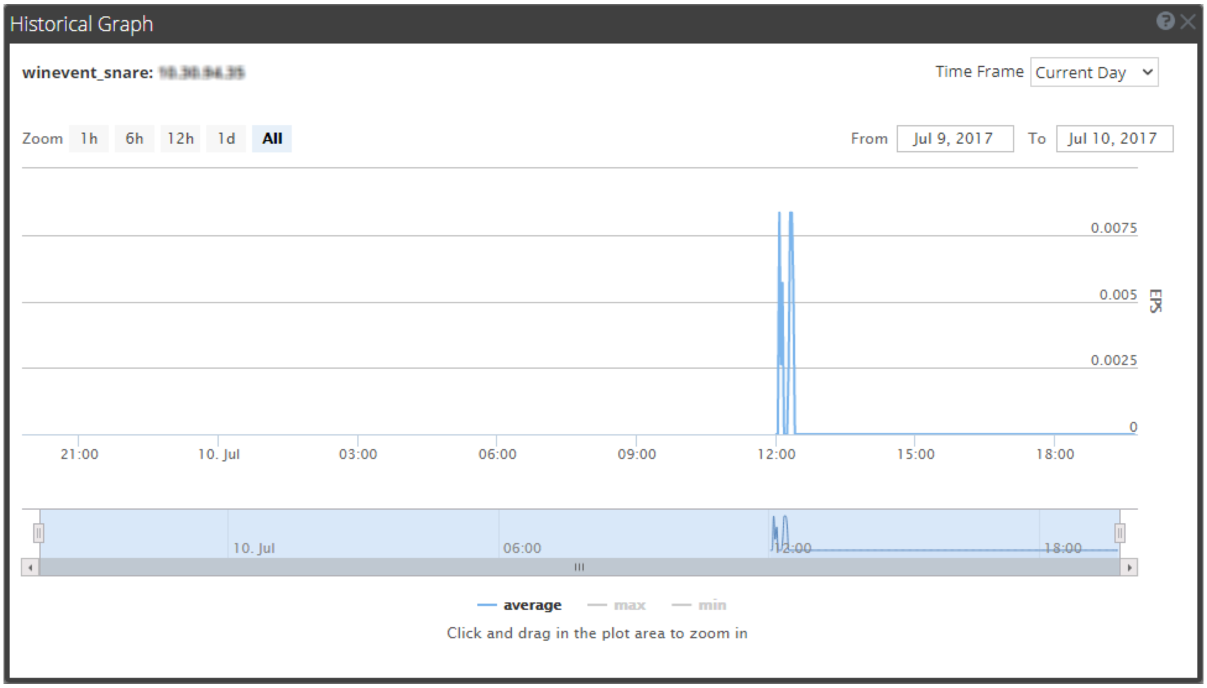
2. Click **Event Source Monitoring**.

   The Event Source Monitoring view is displayed.

3. In the **Historical Graph** column, select 📊.

   The Historical graph for the selected event source is displayed.

   The figure below gives an example of the historical graph for the event source type **winevent_snare**.



Historical Graph

winevent_snare: [redacted]

Time Frame: Current Day

From: Jul 9, 2017 To: Jul 10, 2017

The graphical view is customized to display the events collected for the current day and the values are zoomed in for an interval of an hour (09.05 - 105.05 hrs). Hover over the graph to view the details at a particular instant. For example, in the figure it displays the average rate of collection at 09.30 hrs.

Note: You can customize the graph view by selecting the Time Frame and Date range. You can zoom in using the zoom in value, time window, or by just a click and a drag in the plot area. For details on the parameters to customize and zoom in functions see Health and Wellness Historical Graphs collected from an event source.

If there is no data displayed on the chart it may be due to one of the following reasons:

- event source is down.
- event source is not processing anything right now.

Monitor Alarms

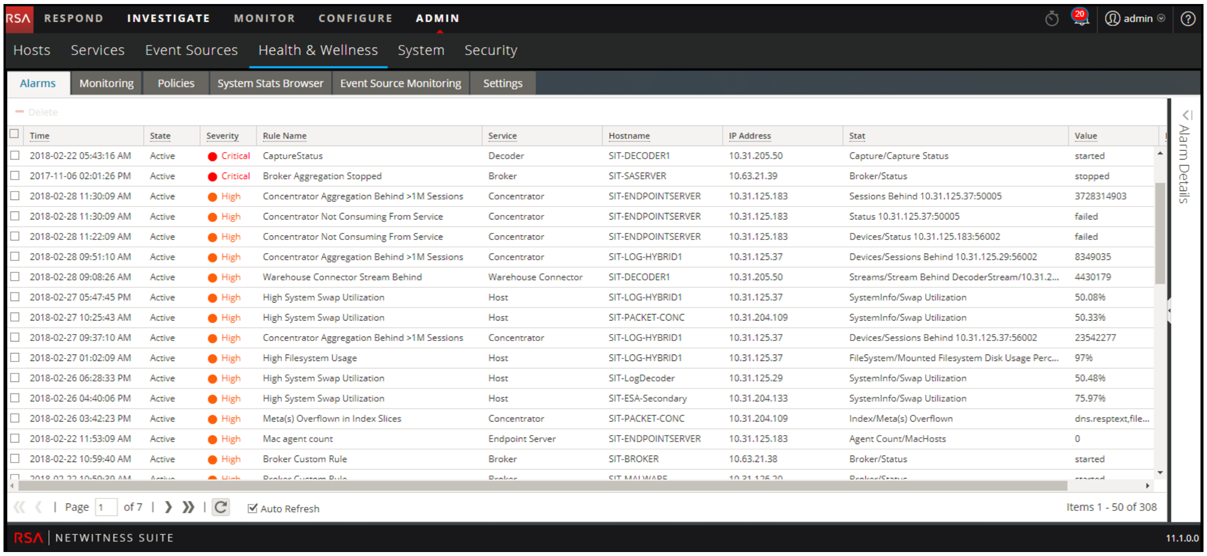
You can set up alarms and monitor them in the Health and Wellness interface for the hosts and services in your NetWitness Suite domain. Alarms display in the view as **Active** when the Policy-rule-defined statistical thresholds for hosts and services have been crossed. Alarms are grayed out and change to the **Cleared** status when the clearing threshold has been crossed.

You set up the parameters for alarms in Manage PoliciesManage Policies For the related reference topic, see Health and Wellness View - Alarms View.

To monitor the alarms set up in NetWitness Suite:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open by default.

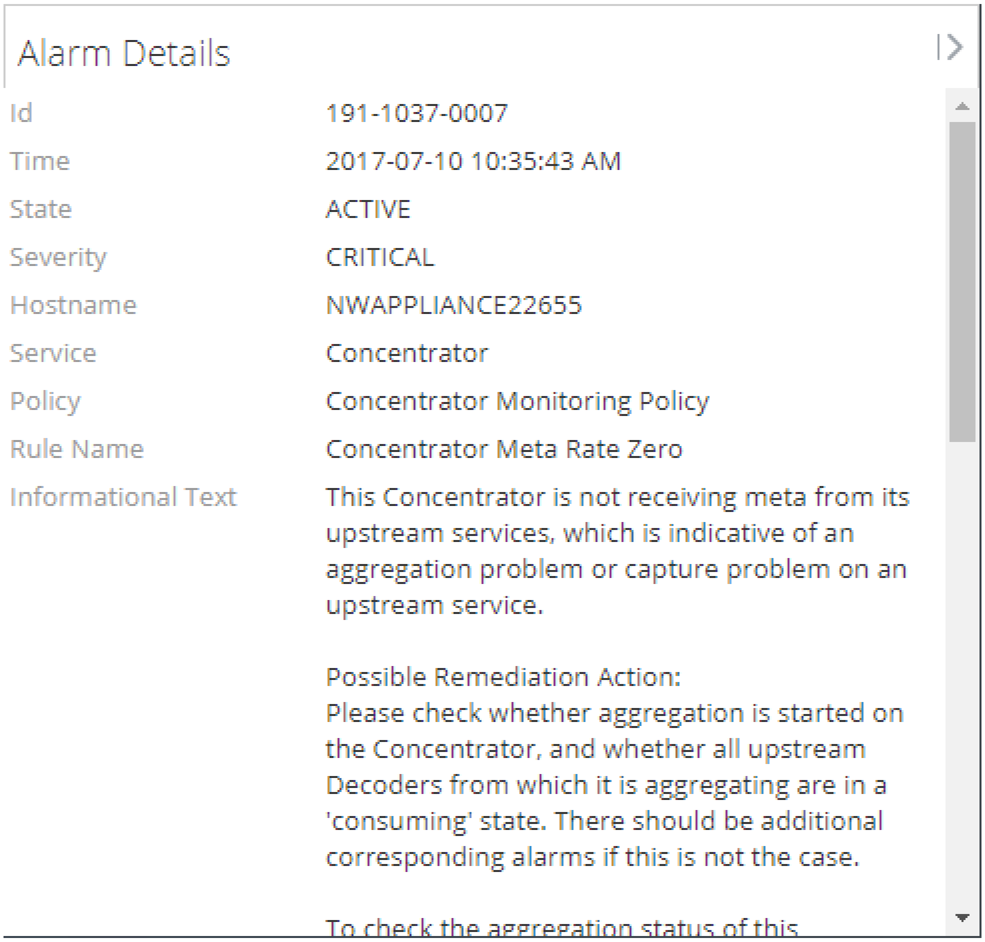


	Time	State	Severity	Rule Name	Service	Hostname	IP Address	Stat	Value
□	2018-02-22 05:43:16 AM	Active	● Critical	CaptureStatus	Decoder	SIT-DECODER1	10.31.205.50	Capture/Capture Status	started
□	2017-11-06 02:01:26 PM	Active	● Critical	Broker Aggregation Stopped	Broker	SIT-SASERVER	10.63.21.39	Broker/Status	stopped
□	2018-02-28 11:30:09 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Sessions Behind 10.31.125.37:50005	3728314903
□	2018-02-28 11:30:09 AM	Active	● High	Concentrator Not Consuming From Service	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Status 10.31.125.37:50005	failed
□	2018-02-28 11:22:09 AM	Active	● High	Concentrator Not Consuming From Service	Concentrator	SIT-ENDPOINTSERVER	10.31.125.183	Devices/Status 10.31.125.183:56002	failed
□	2018-02-28 09:51:10 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-LOG-HYBRID1	10.31.125.37	Devices/Sessions Behind 10.31.125.29:56002	8349035
□	2018-02-28 09:08:26 AM	Active	● High	Warehouse Connector Stream Behind	Warehouse Connector	SIT-DECODER1	10.31.205.50	Streams/Stream Behind DecoderStream/10.31.2...	4430179
□	2018-02-27 05:47:45 PM	Active	● High	High System Swap Utilization	Host	SIT-LOG-HYBRID1	10.31.125.37	SystemInfo/Swap Utilization	50.08%
□	2018-02-27 10:25:43 AM	Active	● High	High System Swap Utilization	Host	SIT-PACKET-CONC	10.31.204.109	SystemInfo/Swap Utilization	50.33%
□	2018-02-27 09:37:10 AM	Active	● High	Concentrator Aggregation Behind >1M Sessions	Concentrator	SIT-LOG-HYBRID1	10.31.125.37	Devices/Sessions Behind 10.31.125.37:56002	23542277
□	2018-02-27 01:02:09 AM	Active	● High	High Filesystem Usage	Host	SIT-LOG-HYBRID1	10.31.125.37	FileSystem/Mounted Filesystem Disk Usage Perc...	97%
□	2018-02-26 06:28:33 PM	Active	● High	High System Swap Utilization	Host	SIT-LogDecoder	10.31.125.29	SystemInfo/Swap Utilization	50.48%
□	2018-02-26 04:40:06 PM	Active	● High	High System Swap Utilization	Host	SIT-ESA-Secondary	10.31.204.133	SystemInfo/Swap Utilization	75.97%
□	2018-02-26 03:42:23 PM	Active	● High	Meta(s) Overflown in Index Slices	Concentrator	SIT-PACKET-CONC	10.31.204.109	Index/Meta(s) Overflown	dns.resptext,file...
□	2018-02-22 11:53:09 AM	Active	● High	Mac agent count	Endpoint Server	SIT-ENDPOINTSERVER	10.31.125.183	Agent Count/MacHosts	0
□	2018-02-22 10:59:40 AM	Active	● High	Broker Custom Rule	Broker	SIT-BROKER	10.63.21.38	Broker/Status	started

Items 1 - 50 of 308

2. Click on the alarm for which you want to display details in the Details Panel.

3. Click <| (expand) to view the details for the alarm you selected.



Alarm Details

Id	191-1037-0007
Time	2017-07-10 10:35:43 AM
State	ACTIVE
Severity	CRITICAL
Hostname	NWAPPLIANCE22655
Service	Concentrator
Policy	Concentrator Monitoring Policy
Rule Name	Concentrator Meta Rate Zero
Informational Text	This Concentrator is not receiving meta from its upstream services, which is indicative of an aggregation problem or capture problem on an upstream service. Possible Remediation Action: Please check whether aggregation is started on the Concentrator, and whether all upstream Decoders from which it is aggregating are in a 'consuming' state. There should be additional corresponding alarms if this is not the case. To check the aggregation status of this

Monitor Health and Wellness Using SNMP Alerts

You can monitor an NetWitness Server component to proactively alert using Simple Network Management Protocol (SNMP) based on the thresholds or system failures.

You can monitor the following for NetWitness Suite components:

- CPU utilization that reaches a defined threshold.
- Memory utilization that reaches a defined threshold.
- Disk utilization that reaches a defined threshold.

SNMP Configuration

The NetWitness Servers can be configured to send out SNMPv3 Threshold Traps and Monitor Traps. Threshold traps are sent in conjunction with configured node thresholds by the NetWitness Suite Core applications themselves. Monitor traps are sent by the SNMP daemon itself for the items indicated in its configuration file. The customer must set up the SNMP daemon on another service to receive SNMP traps from NetWitness Suite. You can set up SNMP on NetWitness Suite in the configuration setting for the NetWitness Server. For more information, see "Service Configuration Settings" in the *NetWitness Suite Host and Services Getting Started Guide* for the specific host.

Thresholds

Thresholds can be set on any service statistics that can accept the setLimit message. You can retrieve the current thresholds using the getLimit message. To set a limit, you can pass a low and high threshold value.

When the value of the stat crosses either the low or high threshold, a SNMP trap is triggered indicating the threshold is crossed. The trap will not be triggered if the value is below the low and above the high value, but another trap is triggered if it crosses back into the normal range (above the low and below the high).

You must set the threshold for the service using the Service Explorer view or the REST API.

Following is a sample threshold for monitoring CPU usage (below 10% or above 90%):

```
/sys/stats/cpu setLimit low=10 high=90
```

Following is an example of how the threshold is set using REST API:

```
http://<log decoder>:50102/sys/stats/cpu?msg=setLimit&low=10&high=90
```

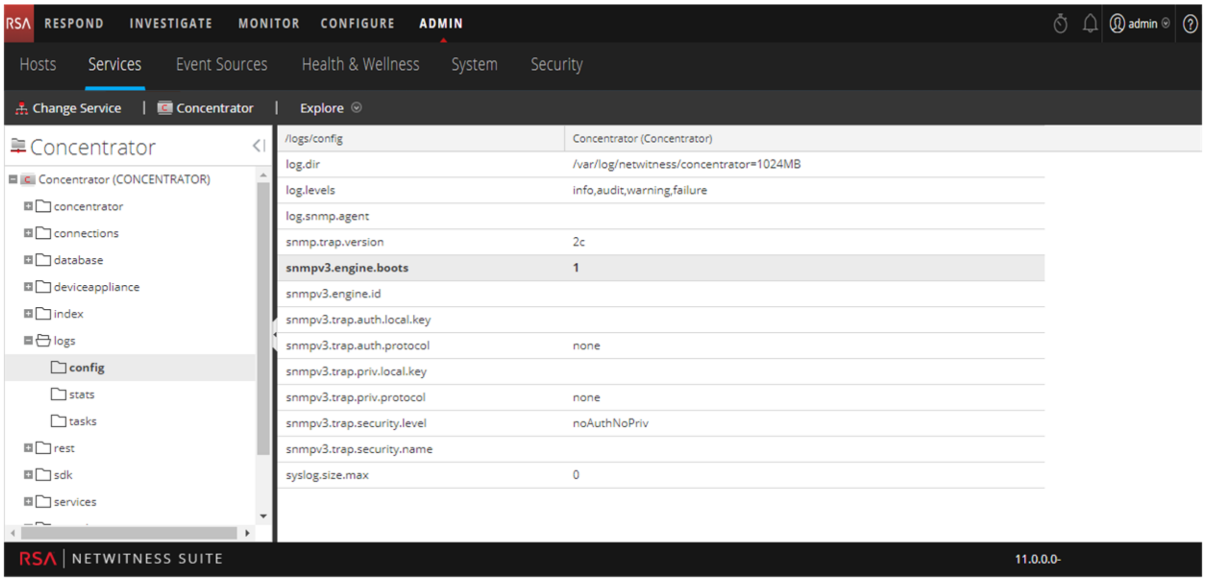
If the CPU usage spikes to 90% or higher, a SNMP trap will be generated:

```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu
old=77% new=91
```

Configure SNMPv3 for a Host

1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. Select the service.
3. In the Actions column, select **View > Explore**.
4. In the nodes list, expand the list and select a config folder. For example, logs > config

5. Set the SNMPv3 configuration.



/logs/config	Concentrator (Concentrator)
log.dir	/var/log/netwitness/concentrator=1024MB
log.levels	info,audit,warning,failure
log.snmp.agent	
snmp.trap.version	2c
snmpv3.engine.boots	**1**
snmpv3.engine.id	
snmpv3.trap.auth.local.key	
snmpv3.trap.auth.protocol	none
snmpv3.trap.priv.local.key	
snmpv3.trap.priv.protocol	none
snmpv3.trap.security.level	noAuthNoPriv
snmpv3.trap.security.name	
syslog.size.max	0

Set the Threshold for a Service

1. Go to **ADMIN** > **Services**.

   The Services view is displayed.

2. Select the service.

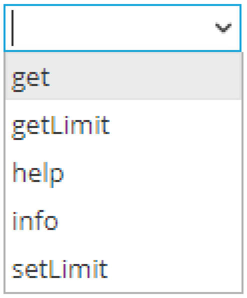
3. In the Actions column, select **View** > **Explore**.

4. In the nodes list, expand the list and select a stat folder.

5. Select a stat, for example, cpu, and right-click.

6. From the drop-down menu, select **Properties.**

   The Properties panel is displayed. The Properties panel has a drop-down list of available messages for the parameter.



7. Select setLimit.

8. Specify the low and high values.

SNMP Traps for System Status

The threshold mechanism can also be used to monitor string-valued stats generated by Core services. There are two ways to monitor string-valued stats:

1. Generate a trap whenever the status value is NOT an expected value. For example, if you want monitor the stat `/broker/stats/status` and generate a trap whenever the value is not `started`, set the `high` limit on the stat to the expected value. You would use the `setLimit` message on `/broker/stats/status` as follows:
   ```
   setLimit high=started
   ```
2. Generate a trap whenever the status value matches an expected value. This is accomplished by using the `low` limit on the stat. For example, if you wanted generate a trap when the stat `/sys/stats/service.status` has the value "`Initialization Failure`", you would use the `setLimit` message on `/sys/stats/service.status` as follows:
   ```
   setLimit low="Initialization Failure"
   ```

In both of these scenarios, it is possible to check for multiple values by using a comma-separated list of values to check for.

Troubleshooting Health & Wellness

Issues Common to All Hosts and Services

You may see the wrong statistics in the Health & Wellness interface if:

- Some or all the hosts and services are not provisioned and enabled correctly.
- You have a mixed-version deployment (that is, hosts updated to different NetWitness Suite versions).
- Supporting services are not running.

Issues Identified by Messages in the Interface or Log Files

This section provides troubleshooting information for issues identified by messages NetWitness Suite displays in the Health & Wellness Interface or includes in the Health & Wellness log files.

Message	User Interface: **Cannot connect to System Management Service**
	System Management Service (SMS) logs:
	
	`Caught an exception during connection recovery!`
	` java.io.IOException`
	` at com.rabbitmq.client.impl.AMQChannel.wrap`
	`(AMQChannel.java:106) at`
	`com.rabbitmq.client.impl.AMQChannel.wrap`

```
(AMQChannel.java:102) at
com.rabbitmq.client.impl.AMQConnection.start(

AMQConnection.java:346) at
com.rabbitmq.client.impl.recovery.

RecoveryAwareAMQConnectionFactory.
newConnection

(RecoveryAwareAMQConnectionFactory.java:36)
 at com.rabbitmq.client.impl.recovery.

AutorecoveringConnection.
recoverConnection(AutorecoveringConnection.java:388)
at com.rabbitmq.client.impl.recovery.

AutorecoveringConnection.beginAutomaticRecovery
(AutorecoveringConnection.java:360)
at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.

access$000(AutorecoveringConnection.java:48)
at com.rabbitmq.client.impl.recovery.

AutorecoveringConnection$1.shutdownCompleted
(AutorecoveringConnection.java:345)
at com.rabbitmq.client.impl.ShutdownNotifierComponent.

notifyListeners(ShutdownNotifierComponent.java:75)
at com.rabbitmq.client.impl.AMQConnection$MainLoop.run
(AMQConnection.java:572)
at java.lang.Thread.run(Thread.java:745)
Caused by: com.rabbitmq.client.ShutdownSignalException:
connection error at
com.rabbitmq.utility.ValueOrException.getValue
(ValueOrException.java:67)
at com.rabbitmq.utility.BlockingValueOrException.

uninterruptibleGetValueBlockingValueOrException.java:33)
at
com.rabbitmq.client.impl.AMQChannel$BlockingRpcContinuation.

getReply
(AMQChannel.java:343)
 at com.rabbitmq.client.impl.AMQConnection.start
(AMQConnection.java:292)
 ... 8 more
 Caused by: java.net.SocketException: Connection reset
 at java.net.SocketInputStream.read
(SocketInputStream.java:189)
 at java.net.SocketInputStream.read
(SocketInputStream.java:121)
```

	` at java.io.BufferedInputStream.fill`
	`(BufferedInputStream.java:246)`
	` at java.io.BufferedInputStream.read`
	`(BufferedInputStream.java:265)`
	` at java.io.DataInputStream.readUnsignedByte`
	`(DataInputStream.java:288)`
	` at com.rabbitmq.client.impl.Frame.readFrom(Frame.java:95)`
	` at com.rabbitmq.client.impl.SocketFrameHandler.readFrame`
	`(SocketFrameHandler.java:139)`
	` at com.rabbitmq.client.impl.AMQConnection$MainLoop.run`
	`(AMQConnection.java:532)`

Possible Cause	RabbitMQ service not running on the NetWitness Server.

Solution	Restart the RabbitMQ, SMS, and NetWitness Suite services using the following commands.
	`systemctl restart rabbitmq-server`
	`systemctl restart rsa-sms`
	`systemctl restart jetty`

Message/ Problem	User Interface: **Cannot connect to System Management Service**
Cause	The System Management Service, RabbitMQ, or Mongo service is not running.

Solution	Run the following commands on NetWitness Server to make sure all these services are running.
	`[root@nwserver ~]# systemctl status rsa-sms`
	` RSA NetWitness SMS :: Server is not running.`
	` [root@nwserver ~]# systemctl start rsa-sms`
	` Starting RSA NetWitness SMS :: Server...`
	` [root@nwserver ~]# systemctl status rsa-sms`
	` RSA NetWitness SMS :: Server is running (5687).`
	` [root@nwserver ~]# systemctl status mongod`
	` mongod (pid  2779) is running...`
	` systemctl status rabbitmq-server`

```
 Status of node nw@localhost ...
 [{pid,2501},
  {running_applications,
   [{rabbitmq_federation_management,"RabbitMQ Federation
Management",
  "3.3.4"},
```

Message/ Problem	User Interface: **Cannot connect to System Management Service**
Possible Cause	`/var/lib/rabbitmq` partition usage is 70% or greater.
Solution	Contact Customer Care.

Message/ Problem	User Interface: **Host migration failed.**
Possible Cause	One or more NetWitness Suite services may be in a **stopped** state.
Solution	Make sure that the following services are running then restart the NetWitness Server: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problem	User Interface: **Server Unavailable.**
Possible Cause	One or more NetWitness Suite services may be in a **stopped** state.

Solution	Make sure that the following services are running then restart the NetWitness Server: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problem	User Interface: **Server Unavailable**
Possible Cause	System Management Service (SMS), RabbitMQ, or Mongo service is not running.

Solution 1	Run the following commands on NetWitness Server to make sure all these services are running.
	`[root@nwserver ~]# systemctl status rsa-sms`
	` RSA NetWitness SMS :: Server is not running.`
	` [root@nwserver ~]# systemctl start rsa-sms`
	` Starting RSA NetWitness SMS :: Server...`
	` [root@nwserver ~]# systemctl status rsa-sms`
	` RSA NetWitness SMS :: Server is running (5687).`
	` [root@nwserver ~]# systemctl status mongod`
	` mongod (pid  2779) is running...`
	`  systemctl status rabbitmq-server`
	` Status of node nw@localhost ...`
	` [{pid,2501},`
	`  {running_applications,`
	`   [{rabbitmq_federation_management,"RabbitMQ Federation Management",`
	`  "3.3.4"},`

Solution 2	Make sure `/var/lib/rabbitmq` partition is less than 75% full
Solution 3	Check NetWitness Server log files (`var/lib/netwitness/uax/logs/nw.log`) for any errors.

Message/ Problem	ContextHub stops and does not allow you to add or edit data sources and lists.
Possible Cause	The storage is full by 95% or above.
Solution 1	Increase the storage by updating the YML file, located at /etc/netwitness/contexthub-server/ contexthub-server.yml. For example, to increase storage from 120 to 150 GB, enter a value (in bytes) by editing the relevant parameter: `rsa.contexthub.data.disk-size: 161061273600`
Solution 2	Delete unwanted or unused large list.
Solution 3	Configure the TTL index for the list to automatically delete STIX and TAXI data and to clean up storage space.

Message/ Problem	Context Hub runs on a fixed memory and 50% is reserved for cache. When cache is 100% full, the cache response stops. For all new lookups the response will be slow.
Possible Cause	The cache is full by 50% or above.
Solution 1	By default, Context Hub cleans the cache every 30 minutes. Reduce the cache expiration time of data sources.
Solution 2	Disable cache for data sources.
Solution 3	Increase the RAM of the CH Java process by editing the `-Xmx` option available in the /etc/netwitness/contexthub-server/contexthub-server.conf file. In `JAVA_OPTS`, search for the `-Xmx` option. For example, edit the entry as follows: `-Xmx8G` where `8G` represents 8GB space. Then restart the ContextHub service. **Note:** The memory is less than the available system memory. Be aware that there are many other services running on the host.

Message/ Problem	List Data Source displays an unhealthy stats or status.
Possible Cause 1	Unable to: • access the data source • parse or read a CSV file • schema mismatched CSV
Possible Cause 2	Unable to authenticate when accessing the data source.
Solution 1	Make sure to save the csv file at correct location i.e/var/lib/netwitness/contexthub-server/data/ and verify the required read permissions.
Solution 2	Make sure the csv file schema specified while configuring the data source matches. If not, then either create a new data source with the new schema or edit the csv file to match the schema. For example, if you configure a List Data Source with a schema with column1, column2, and column3. And next time you update the csv file where the number of column increase or decrease or the order of the columns are changed. In this case there is a schema mismatch and the configured list data source will show “Unhealthy” in Health and Wellness stats.
Solution 3	Make sure the password is correct. To confirm edit the data source, enter the password and click test connection. For more information related the above solutions, see "Configure Lists as a Data Source" topic in the *Context Hub Configuration Guide*.

Issues Not Identified by the User Interface or Logs

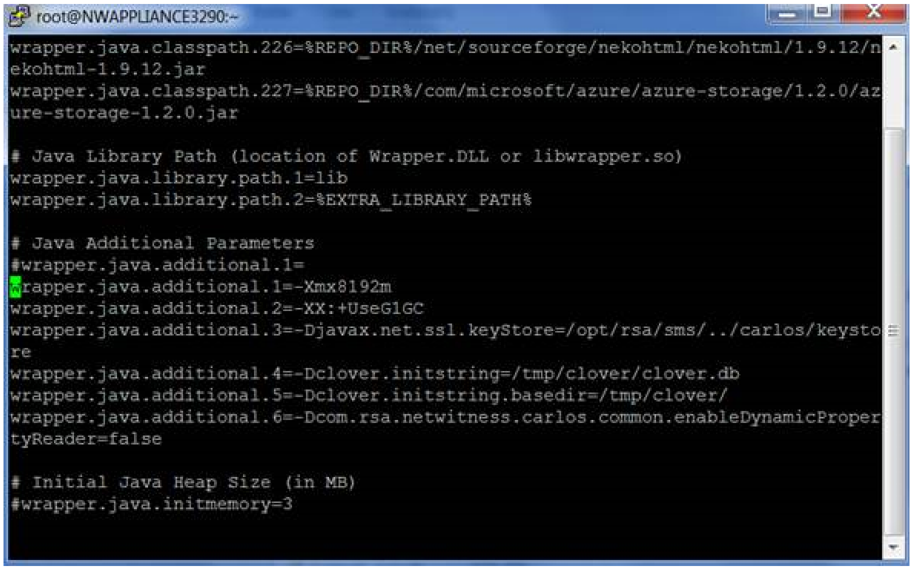
This section provides troubleshooting information for issues that are not identified by messages NetWitness Suite displays in the Health & Wellness Interface or includes in the Health & Wellness log files. For example, you may see incorrect statistical information in the Interface.

Problem	Incorrect statistics displayed in Health and Wellness interface.
Possible Cause	SMS service is not running. SMS service must be running on the NetWitness Server.
Solution	Restart SMS service.

Problem	NetWitness Suite does not show the version to which you upgraded until you restart jettysrv (jeTTy server).
Possible Cause	When NetWitness Suite checks a connection, it polls a service every 30 seconds to see if it is active. During that 30 seconds, if the service comes back up, it will not get the new version.
Solution	1. Manually stop the service. 2. Wait until you see that it is it offline. 3. Restart the service. NetWitness Suite displays the correct version.

Problem	NetWitness Server does not display the **Service Unavailable** page.
Possible Cause	After you upgrade to NetWitness Suite version 10.5, JDK 1.8 is not default version and this causes the jettysrv (jeTTy server) to fail to start. Without the jeTTy server, the NetWitness Suite server cannot display the **Service Unavailable** page.
Solution	Restart jettysrv.

Problem	The SMS service is stopped and the following error is displayed in the log file: `java.lang.OutOfMemoryError: Java heap space`
Solution	You can use the following solution to increase the memory according to your needs. 1. Open /opt/rsa/sms/conf/wrapper.conf



```
wrapper.java.classpath.226=%REPO_DIR%/net/sourceforge/nekohtml/nekohtml/1.9.12/n
ekohtml-1.9.12.jar
wrapper.java.classpath.227=%REPO_DIR%/com/microsoft/azure/azure-storage/1.2.0/az
ure-storage-1.2.0.jar

# Java Library Path (location of Wrapper.DLL or libwrapper.so)
wrapper.java.library.path.1=lib
wrapper.java.library.path.2=%EXTRA_LIBRARY_PATH%

# Java Additional Parameters
#wrapper.java.additional.1=
wrapper.java.additional.1=-Xmx8192m
wrapper.java.additional.2=-XX:+UseG1GC
wrapper.java.additional.3=-Djavax.net.ssl.keyStore=/opt/rsa/sms/../carlos/keysto
re
wrapper.java.additional.4=-Dclover.initstring=/tmp/clover/clover.db
wrapper.java.additional.5=-Dclover.initstring.basedir=/tmp/clover/
wrapper.java.additional.6=-Dcom.rsa.netwitness.carlos.common.enableDynamicProper
tyReader=false

# Initial Java Heap Size (in MB)
#wrapper.java.initmemory=3
```

2. Replace `wrapper.java.additional.1=-Xmx8192m` with:
   `wrapper.java.additional.1=-Xmx16g`

3. Restart the SMS service:

   ```
   systemctl start rsa-sms
   ```

Managing NetWitness Suite Updates

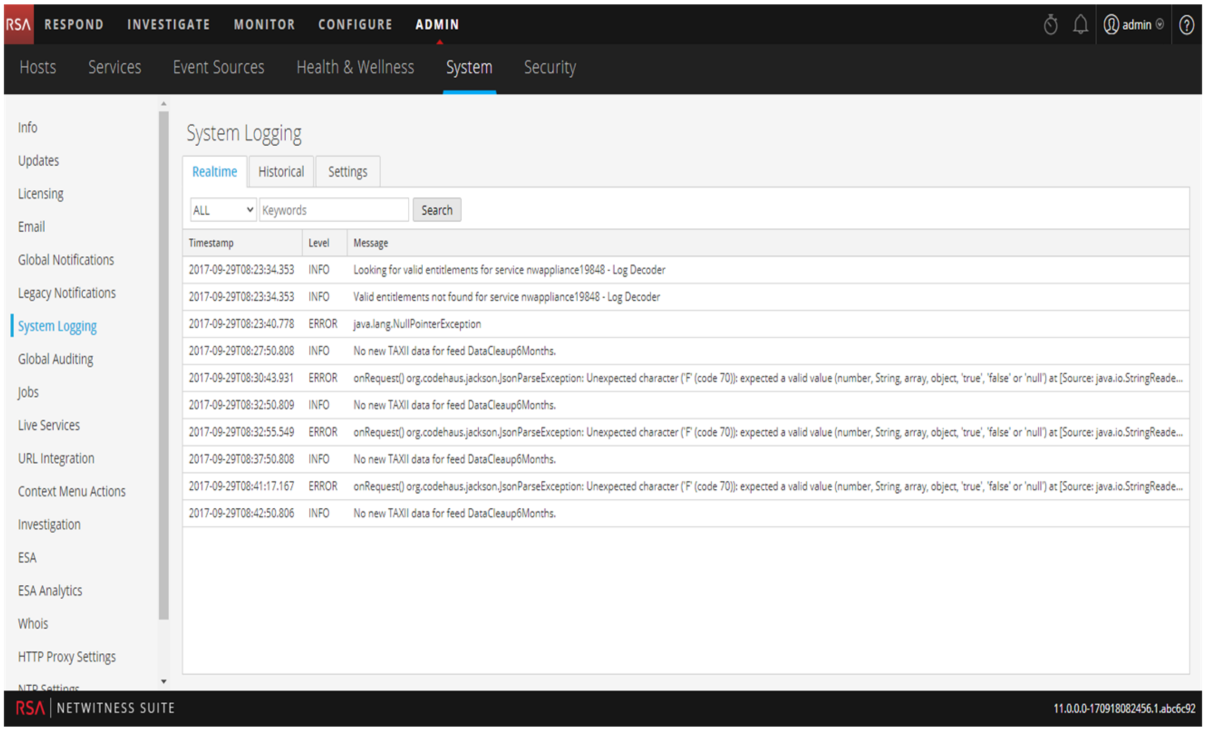
RSA issues NetWitness Suite software version updates on a regular basis as it strives to continually improve the product. A software version update consists of a release, service pack, or patch (including security patch) and ancillary software on which the release, service pack, or patch depends. User guides are provided for each software version update release, which include detailed steps for installing the update. It is important that you download the update guide for the release from RSA Link (https://community.rsa.com/community/products/netwitness) and follow the steps described there. Additional information is available in the "Update Existing Host to New Version" topic in the *Hosts and Services Getting Started Guide* and in System Updates Panel - Settings Tab.

Displaying System and Service Logs

NetWitness Suite provides views into system logs and service logs. When you view service logs, you can also select messages for the service or host.

View System Logs

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.



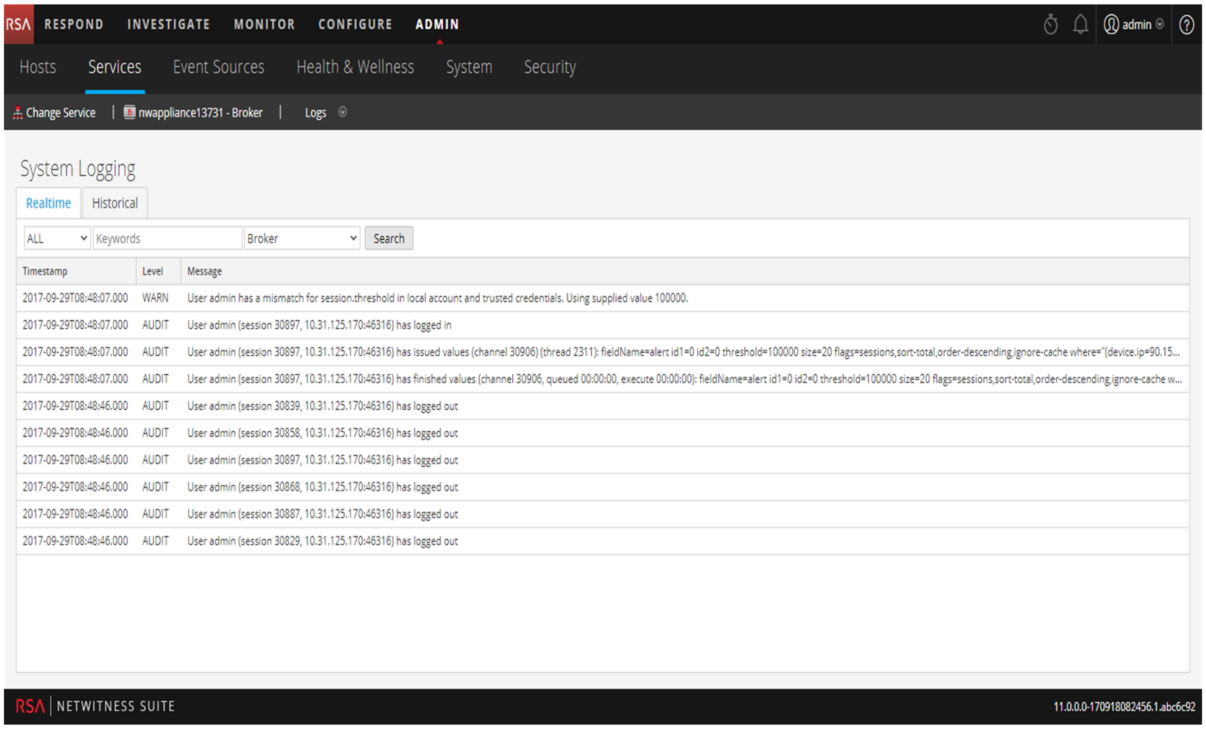
Timestamp	Level	Message
2017-09-29T08:23:34.353	INFO	Looking for valid entitlements for service nwappliance19848 - Log Decoder
2017-09-29T08:23:34.353	INFO	Valid entitlements not found for service nwappliance19848 - Log Decoder
2017-09-29T08:23:40.778	ERROR	java.lang.NullPointerException
2017-09-29T08:27:50.808	INFO	No new TAXII data for feed DataCleaup6Months.
2017-09-29T08:30:43.931	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:32:50.809	INFO	No new TAXII data for feed DataCleaup6Months.
2017-09-29T08:32:55.549	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:37:50.808	INFO	No new TAXII data for feed DataCleaup6Months.
2017-09-29T08:41:17.167	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:42:50.806	INFO	No new TAXII data for feed DataCleaup6Months.

Display Service Logs

To display NetWitness Suite service logs:

1. Go to **ADMIN > Services**.
2. In the **Services** grid, select a service.

3. In the **Actions** column, select **View > Logs**.



Timestamp	Level	Message
2017-09-29T08:48:07.000	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has logged in
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has issued values (channel 30906) (thread 2311): fieldName=alert id1=0 id2=0 threshold=100000 size=20 flags=sessions,sort-total,order-descending,ignore-cache where="(device.ip=90.15...
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has finished values (channel 30906, queued 00:00:00, execute 00:00:00): fieldName=alert id1=0 id2=0 threshold=100000 size=20 flags=sessions,sort-total,order-descending,ignore-cache w...
2017-09-29T08:48:46.000	AUDIT	User admin (session 30839, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30858, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30868, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30887, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30829, 10.31.125.170:46316) has logged out

Filter Log Entries

To filter the results shown in the Realtime tab:

1. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
2. (Optional) For service logs, select the Service: host or service.
3. Click **Filter**.

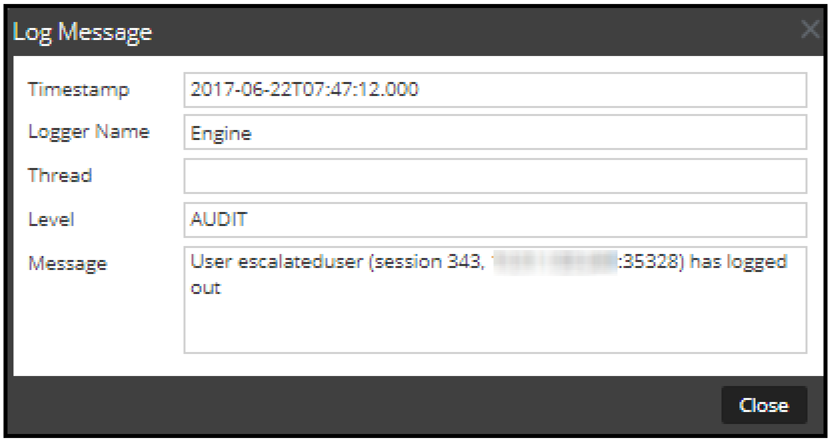
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the Realtime tab Log grid provides the summary information of a log entry. To view complete details:

1. Double-click a log entry.

   The **Log Message** dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.

   Timestamp: 2017-06-22T07:47:12.000
   Logger Name: Engine
   Thread:
   Level: AUDIT
   Message: User escalateduser (session 343, [redacted]:35328) has logged out

2. After viewing, click **Close**.

Access Reporting Engine Log File

All Log Files

The Reporting Engine stores the following logs in the **rsasoc/rsa/soc/reporting-engine/log** directory:

- Current logs in the **reporting-engine.log** file.
- Backup copies of previous logs in the **reporting-engine.log.*** file.
- All UNIX script logs in the files that have the following syntax: **reporting-engine.sh_*timestamp*.log** (for example, **reporting-engine.sh_20120921.log**).

The Reporting Engine rarely writes command line error messages to the **rsasoc/nohup.out** file.

Upstart Logs

The Reporting Engine appends the log messages and output written by upstart daemon and the commands used to start the reporting-engine to the **/var/log/secure** directory.

An upstart log file is a system log file so only the root user can read it. The Reporting Engine generates log files, retains backup copies of previous log files, stores UNIX script log files, and appends upstart log files to another directory.

Search and Export Historical Logs

NetWitness Suite provides a searchable view of the NetWitness Suite log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the service. You can export logs from the current view.

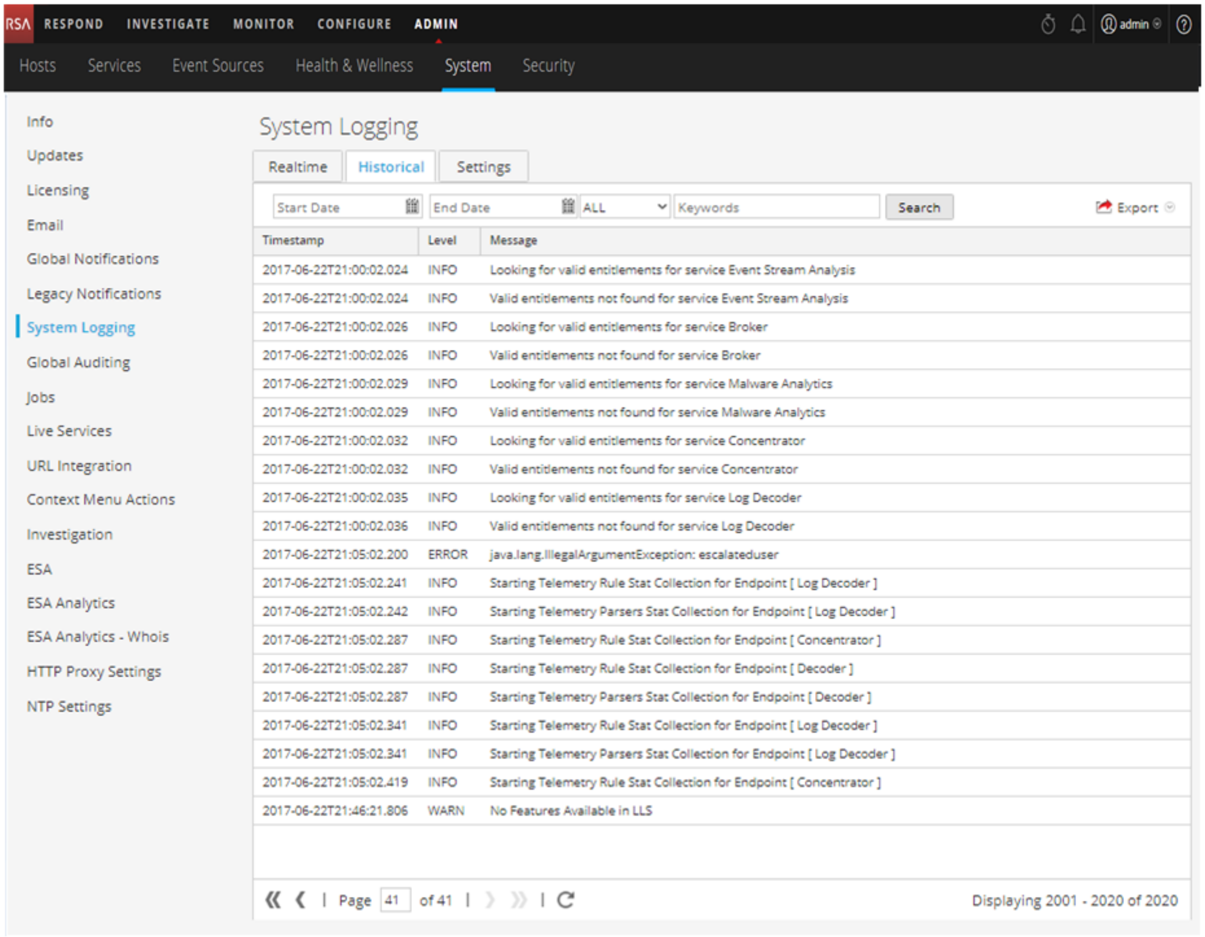
Display the Historical System Log

To display the historical log for the system:

1. Go to **ADMIN** > **System.**
2. In the options panel, select **System Logging**.

   The System Logging panel is opened to the Realtime tab by default.
3. Click the **Historical** tab.

   A list of historical logs for the system is displayed.



Timestamp	Level	Message
2017-06-22T21:00:02.024	INFO	Looking for valid entitlements for service Event Stream Analysis
2017-06-22T21:00:02.024	INFO	Valid entitlements not found for service Event Stream Analysis
2017-06-22T21:00:02.026	INFO	Looking for valid entitlements for service Broker
2017-06-22T21:00:02.026	INFO	Valid entitlements not found for service Broker
2017-06-22T21:00:02.029	INFO	Looking for valid entitlements for service Malware Analytics
2017-06-22T21:00:02.029	INFO	Valid entitlements not found for service Malware Analytics
2017-06-22T21:00:02.032	INFO	Looking for valid entitlements for service Concentrator
2017-06-22T21:00:02.032	INFO	Valid entitlements not found for service Concentrator
2017-06-22T21:00:02.035	INFO	Looking for valid entitlements for service Log Decoder
2017-06-22T21:00:02.036	INFO	Valid entitlements not found for service Log Decoder
2017-06-22T21:05:02.200	ERROR	java.lang.IllegalArgumentException: escalateduser
2017-06-22T21:05:02.241	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.242	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Concentrator]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Decoder]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Decoder]
2017-06-22T21:05:02.341	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.341	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.419	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Concentrator]
2017-06-22T21:46:21.806	WARN	No Features Available in LLS

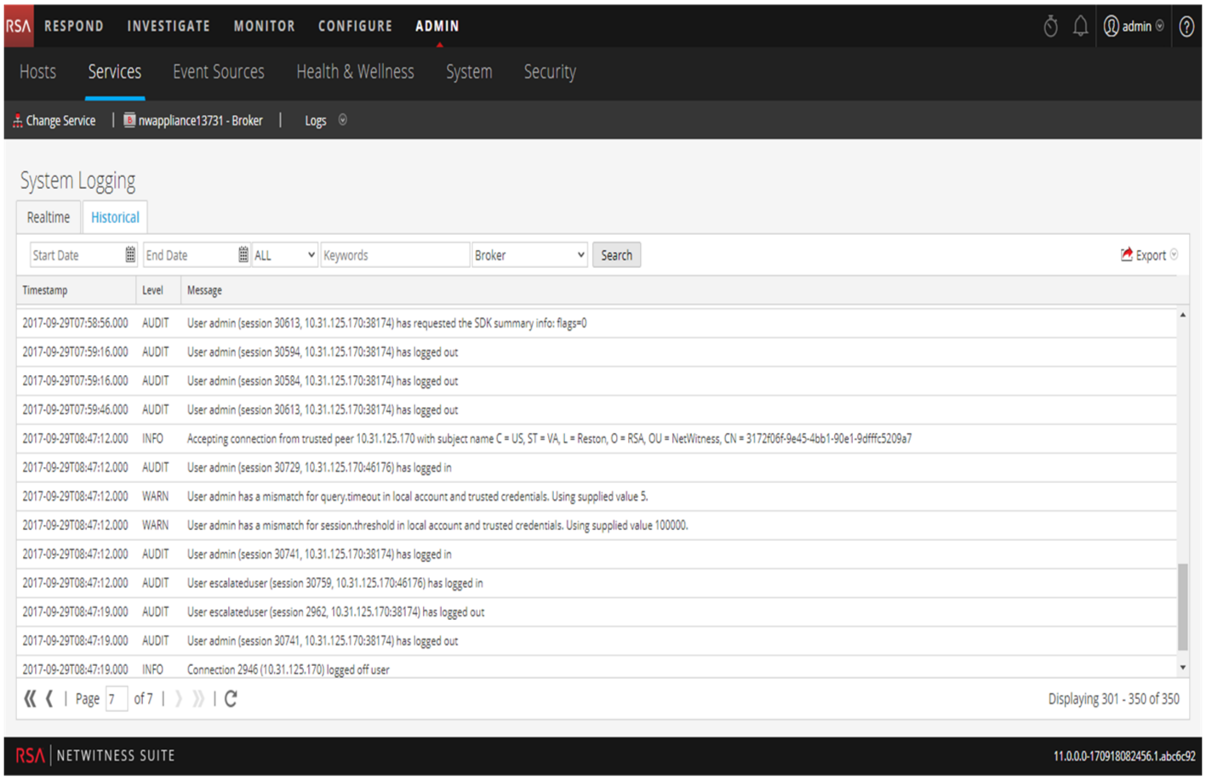
Display a Historical Service Log

To display the historical log for services:

1. Select **ADMIN** > **Services**.
2. Select a service.
3. In the **Actions** column, select **View** > **Logs**.

   The service logs view is displayed with the Realtime tab open.
4. Click the **Historical** tab.

   A list of historical logs for the selected service is displayed.



Timestamp	Level	Message
2017-09-29T07:58:56.000	AUDIT	User admin (session 30613, 10.31.125.170:38174) has requested the SDK summary info: flags=0
2017-09-29T07:59:16.000	AUDIT	User admin (session 30594, 10.31.125.170:38174) has logged out
2017-09-29T07:59:16.000	AUDIT	User admin (session 30584, 10.31.125.170:38174) has logged out
2017-09-29T07:59:46.000	AUDIT	User admin (session 30613, 10.31.125.170:38174) has logged out
2017-09-29T08:47:12.000	INFO	Accepting connection from trusted peer 10.31.125.170 with subject name C = US, ST = VA, L = Reston, O = RSA, OU = NetWitness, CN = 3172f06f-9e45-4bb1-90e1-9dfffc5209a7
2017-09-29T08:47:12.000	AUDIT	User admin (session 30729, 10.31.125.170:46176) has logged in
2017-09-29T08:47:12.000	WARN	User admin has a mismatch for query.timeout in local account and trusted credentials. Using supplied value 5.
2017-09-29T08:47:12.000	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2017-09-29T08:47:12.000	AUDIT	User admin (session 30741, 10.31.125.170:38174) has logged in
2017-09-29T08:47:12.000	AUDIT	User escalateduser (session 30759, 10.31.125.170:46176) has logged in
2017-09-29T08:47:19.000	AUDIT	User escalateduser (session 2962, 10.31.125.170:38174) has logged out
2017-09-29T08:47:19.000	AUDIT	User admin (session 30741, 10.31.125.170:38174) has logged out
2017-09-29T08:47:19.000	INFO	Connection 2946 (10.31.125.170) logged off user

Search Log Entries

To search the results shown in the **Historical** tab:

1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
3. (Optional) For service logs, select the Service: host or service.

4. Click **Search**.

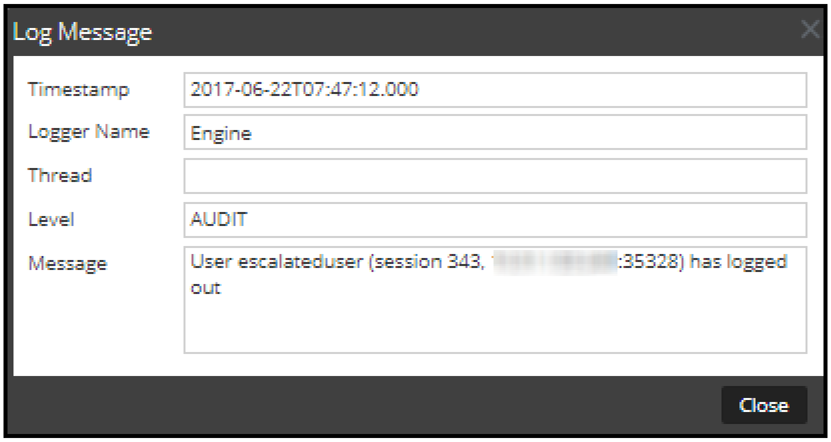
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the **Historical** tab Log grid provides the summary information of a log entry. To display all the details for a log message:

1. Double-click a log entry.

   The **Log Message** dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



Log Message

Timestamp: 2017-06-22T07:47:12.000

Logger Name: Engine

Thread:

Level: AUDIT

Message: User escalateduser (session 343, [redacted]:35328) has logged out

2. After viewing, click **Close**.

   The dialog closes.

Page Through Log Entries

To peruse the different pages of the grid, use the paging controls on the bottom of the grid as follows:

- Use the navigation buttons
- Manually type the page number you want to view, and press **ENTER**.

Export a Log File

To export the logs in the current view:

Click **Export**, and select one of the drop-down options: **CSV Format** or **Tab Delimited**.
 The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a NetWitness Suite system log exported with comma-separated values is named **UAP_log_export_CSV.txt**, and a host log exported with tab-separated values is named **APPLIANCE_log_export_TAB.txt**.

Maintaining Queries Using URL Integration

A URL integration provides a way to represent the bread crumbs, or query path, you take when actively investigating a service in the Navigate view. You do not need to display and edit these objects often.

A URL integration maps a unique ID that is automatically created each time you click on a navigation link in the Navigation view to drill into data. When the drill-down completes, the URL reflects the query IDs for the current drill point. The Display Name is displayed in the bread crumb in the Navigate view.

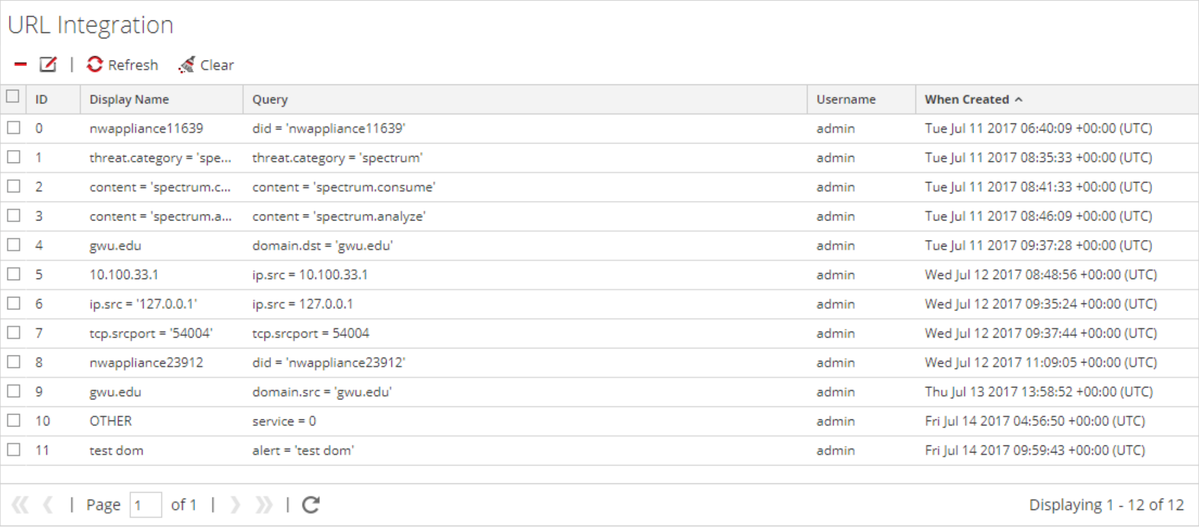
The **URL Integration** panel provides a list of queries and allows users who have the proper permissions to modify this underlying source of data and analyze the query patterns of other users of the NetWitness Suite system. Within the panel, you can:

- Refresh the list.
- Edit a query.
- Delete a query.
- Clear all queries in the list.

Caution: After a query has been removed from the system, any Investigation URLs that included the ID of that query will no longer function.

Edit a Query

1. Go to **ADMIN** > **System**.
2. In the options panel, select **URL Integration**.

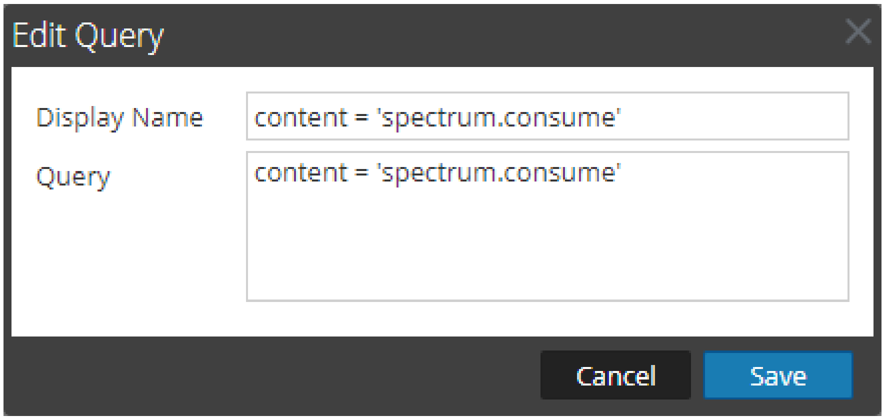


URL Integration

□	ID	Display Name	Query	Username	When Created ^
□	0	nwappliance11639	did = 'nwappliance11639'	admin	Tue Jul 11 2017 06:40:09 +00:00 (UTC)
□	1	threat.category = 'spe...	threat.category = 'spectrum'	admin	Tue Jul 11 2017 08:35:33 +00:00 (UTC)
□	2	content = 'spectrum.c...	content = 'spectrum.consume'	admin	Tue Jul 11 2017 08:41:33 +00:00 (UTC)
□	3	content = 'spectrum.a...	content = 'spectrum.analyze'	admin	Tue Jul 11 2017 08:46:09 +00:00 (UTC)
□	4	gwu.edu	domain.dst = 'gwu.edu'	admin	Tue Jul 11 2017 09:37:28 +00:00 (UTC)
□	5	10.100.33.1	ip.src = 10.100.33.1	admin	Wed Jul 12 2017 08:48:56 +00:00 (UTC)
□	6	ip.src = '127.0.0.1'	ip.src = 127.0.0.1	admin	Wed Jul 12 2017 09:35:24 +00:00 (UTC)
□	7	tcp.srcport = '54004'	tcp.srcport = 54004	admin	Wed Jul 12 2017 09:37:44 +00:00 (UTC)
□	8	nwappliance23912	did = 'nwappliance23912'	admin	Wed Jul 12 2017 11:09:05 +00:00 (UTC)
□	9	gwu.edu	domain.src = 'gwu.edu'	admin	Thu Jul 13 2017 13:58:52 +00:00 (UTC)
□	10	OTHER	service = 0	admin	Fri Jul 14 2017 04:56:50 +00:00 (UTC)
□	11	test dom	alert = 'test dom'	admin	Fri Jul 14 2017 09:59:43 +00:00 (UTC)

3. Select the row in the grid and either double-click the row or click ✎.

   The **Edit Query Dialog** is displayed.



Edit Query

Display Name: content = 'spectrum.consume'

Query: content = 'spectrum.consume'

4. Edit the **Display Name** and the **Query**, but do not leave either field blank.
5. To save the changes, click **Save**.

Delete a Query

Caution: After a query has been removed from the system, any Investigation URLs that included the ID of that query will no longer function.

To remove a query from NetWitness Suite entirely:

1. Select the query.
2. Click −

A dialog requests confirmation that you want to delete the query.

3. Click **Yes**.

Clear All Queries

To clear all queries from the list:

- Click Clear

  The entire list is cleared.

Use a Query in a URI

URL Integration facilitates integrations with third-party products by allowing a search against the NetWitness Suite architecture. By using a query in a URI, you can pivot directly from any product that allows custom links, into a specific drill point in the Investigation view in NetWitness Suite.

The format for entering a URI using a URL-encoded query is:

http://<nw host:port>/investigation/<serviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
where

- **<nw host: port>** is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is only needed if access is configured over a non-standard port through a proxy.
- **<serviceId>** is the internal Service ID in the NetWitness Suite instance for the service to query against. The service ID can be represented only as an integer. You can see the relevant service ID from the url when accessing the investigation view within NetWitness Suite. This value will change based on the service being connected to for analysis.
- **<encoded query>** is the URL-encoded NetWitness Suite query. The length of query is limited by the HTML URL limitations.
- **<start date>** and **<end date>** define the date range for the query. The format is <yyyy-mm-dd>T<hh:mm>. The start and end dates are required. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.

For example:
http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00/2012-10-31T00:00

Examples

These are query examples where the NetWitness Server is 192.168.1.10 and the serviceID is identified as 2.

All activity on 03/12/2013 between 5:00 and 6:00 AM with a hostname registered

- Custom Pivot: alias.host exists
- https://192.168.1.10/investigation/2...13-03-12T06:00

All activity on 3/12/2013 between 5:00 and 5:10 PM with http traffic to and from IP address 10.10.10.3

- Custom Pivot: service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- Encoded Pivot Dissected:
  - service=80 => service&3D80
  - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - https://192.168.1.10/investigation/2...13-03-12T17:10

Additional Notes

Some values may not need to be encoded as part of the query. For example, commonly the IP src and dst is used for this integration point. If leveraging a third-party application for integration of this feature, it is possible to reference those without encoding applied.

FIPS Support

NetWitness Suite 11.0 ships with FIPS-validated 140-2 Cryptographic Modules that support all cryptographic operations within NetWitness Suite. NetWitness Suite leverages two modules that support a level 3 design assurance:

- RSA BSAFE Crypto-J
- OpenSSL with BSAFE (OWB)

Both modules have been certified with an operational environment comparable to the standard NetWitness Suite configuration.

By default, the cryptographic modules enforce the usage of FIPS-certified cipher suites wherever possible. For exceptions, refer to the information below and to the release notes. For additional information about the FIPS modules, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

The RSA BSAFE Crtypo-J FIPS Certificate number is 2468 and the OWB FIPS Certificate is included in the RSA BSAFE Crypto-C Micro Edition with certificate number 2300.

In 11.0.0.0, FIPS is enabled on all services except Log Collector. This includes Log Decoder and Decoder if they were FIPS-enabled in 10.6.4.x. FIPS cannot be disabled on any services except for Log Collector, Log Decoder and Decoder.

Note: For a fresh installation of 11.0.0.0, by default, all core services will be FIPS enforced except Log Collector and Log Decoder. FIPS cannot be disabled on any services except for Log Collector, Log Decoder and Packet Decoder.

Note: For upgrades to 11.0.0.0 from 10.6.4.x, the following conditions apply for the Log Collector, Log Decoder and Decoder services:
- Log Collector is not FIPS enabled after upgrading to 11.0.0.0, even if FIPS was enabled in 10.6.4.x. You must enable FIPS support after upgrading to 11.0.0.0. See the instructions in FIPS support for Log Collectors.
- If FIPS was enabled for the Log Decoder and Packet Decoder services in 10.6.4.x, FIPS will also be enabled in 11.0.0.0. However, if Log Decoder and Packet Decoder were NOT FIPS enabled in 10.6.4.x, they will not be enabled in 11.0.0.0, and you can manually enable FIPS for these services if required. See the instructions in FIPS support for Log Decoders and Decoders.

FIPS support for Log Collectors

To enable FIPS for Log Collectors:

1. Stop the Log Collector service.
2. Open the `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` file.
3. Change the value of the following variable to **off** as described here:

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```

   to

   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```
4. Reload the system daemon by running the following command:

   ```
   systemctl daemon-reload
   ```
5. Restart the Log Collector service.
6. Set the FIPS mode for the Log Collector service in the UI :

   > **Note:** This step is not required if you are upgrading from 10.6.4 to 11.0.0.0 and FIPS was enabled in 10.6.4.

   a. Go to **ADMIN** > **Services**.

   b. Select the Log Collector service and go to **View** > **Config**.

   c. In SSL FIPS Mode, select the checkbox under Config Value and click **Apply**.

FIPS support for Log Decoders and Decoders

To enable FIPS for Log Decoders and Decoders that did not have FIPS enabled in 10.6.4.x:

1. Go to **ADMIN** > **Services** and select a Log Decoder or Packet Decoder service.
2. Select **View** > **Config**, and in **System Configuration**, enable **SSL FIPS Mode** by selecting the check box in the **Config Value** column.
3. Restart the service.
4. Click **Apply**.

Troubleshoot NetWitness Suite

For information about troubleshooting NetWitness Suite, see the following topics:

- Debugging Information
- Error Notification
- Miscellaneous Tips
- NwLogPlayer
- Troubleshoot Feeds

Debugging Information

NetWitness Suite Log Files

The following files contain NetWitness Suite log information.

Component	File
rabbitmq	/var/log/rabbitmq/nw@localhost.log /var/log/rabbitmq/nw@localhost-sasl.log
collectd	/var/log/messages
nwlogcollector	/var/log/messages
nwlogdecoder	/var/log/messages
sms	/opt/rsa/sms/wrapper.log
sms	/opt/rsa/sms/logs/sms.log
sms	/opt/rsa/sms/logs/audit/audit.log
NetWitness Suite	/var/lib/netwitness/uax/logs/nw.log
NetWitness Suite	/var/lib/netwitness/uax/logs/ audit/audit.log
NetWitness Suite	/opt/rsa/jetty9/logs

Files of Interest

The following files are used in key NetWitness Suite components, and can be useful when trying to track down miscellaneous issues.

Component	File	Description
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQ configuration file. This configuration file partially drives the behavior of RabbitMQ, particularly around network/SSL settings.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQ environment configuration file. This file specifies the RabbitMQ node name and location of the enabled plugins file.
rabbit	/etc/rabbitmq/rsa_enabled_plugins	This file specifies the list of enabled plugins in RabbitMQ. This file is managed by the RabbitMQ server, via the rabbitmq-plugins command. This file overrides the /etc/rabbitmq/enabled_plugins path, in order to work around issues with upgrading the Log Collector from early versions.

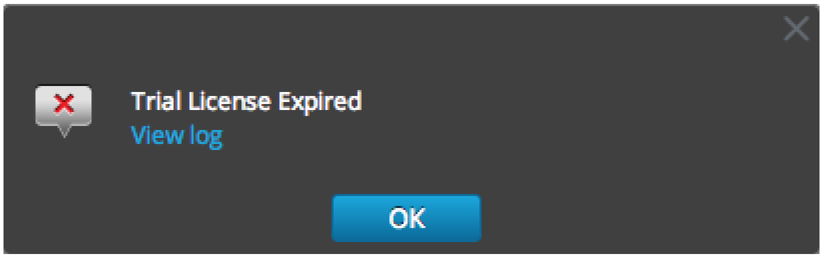
Component	File	Description
rabbit	/etc/rabbitmq/ssl/truststore.pem	The RabbitMQ trust store. This file contains a sequence of PEM-encoded X.509 certificates, represented trust CAs. Any clients that connect to RabbitMQ and present a certificate that is signed by a CA in this list is considered a trusted client.

Component	File	Description
rabbit	/var/log/rabbitmq/mnesia/nw@localhost	The RabbitMQ Mnesia directory. Mnesia is the Erlang/OTP database technology, for storing Erlang objects persistently. RabbitMQ uses this technology for storing information such as the current set of policies, persistent exchanges and queues, and so forth. Importantly, the msg_store_persistent and msg_store_transient directories are where RabbitMQ stores messages that have been spooled to disk, e.g., if messages are published as persistent messages, or which have paged off to disk due to memory limitations. Keep a close eye on this directory, if the disk or memory alarms have tripped in RabbitMQ. **Caution:** Do not delete these files manually. Use RabbitMQ tools to purge or delete queues. Modifying these files manually may render your RabbitMQ instance inoperable.

Error Notification

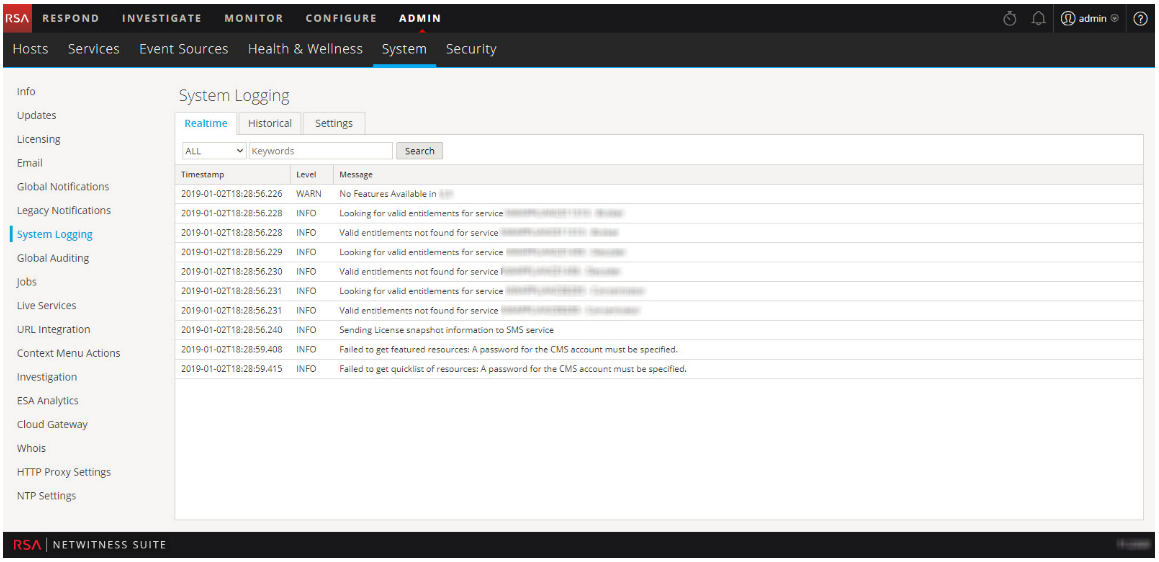
NetWitness Suite has a set of error message types associated with different components and operations. NetWitness Suite displays feedback in the form of a simple error notification and a log entry.

When an error notification dialog is displayed, you have two options: simply acknowledge the message or view the system log for more information.



Trial License Expired

If you want to view the system log for more information when an error notification is displayed, click **View log**. The log opens in the **Administration** > **System** view with a list of messages. Time stamp and message level are also listed.



System Logging

Timestamp	Level	Message
2019-01-02T18:28:56.226	WARN	No Features Available in [redacted]
2019-01-02T18:28:56.228	INFO	Looking for valid entitlements for service [redacted]
2019-01-02T18:28:56.228	INFO	Valid entitlements not found for service [redacted]
2019-01-02T18:28:56.229	INFO	Looking for valid entitlements for service [redacted]
2019-01-02T18:28:56.230	INFO	Valid entitlements not found for service [redacted]
2019-01-02T18:28:56.231	INFO	Looking for valid entitlements for service [redacted]
2019-01-02T18:28:56.231	INFO	Valid entitlements not found for service [redacted]
2019-01-02T18:28:56.240	INFO	Sending License snapshot information to SMS service
2019-01-02T18:28:59.408	INFO	Failed to get featured resources: A password for the CMS account must be specified.
2019-01-02T18:28:59.415	INFO	Failed to get quicklist of resources: A password for the CMS account must be specified.

Miscellaneous Tips

Audit Log Messages

It can be useful to see which user actions result in which log message types in the **/var/log/**messages file.

The event categories spreadsheet included in the log parser package in the NetWitness Suite Parser v2.0.zip archive lists the event categories and the event parser lines to help with building reports, alerts, and queries.

NwConsole for Health & Wellness

RSA has added a command option called **logParse** in **NwConsole**. This command option supports log parsing, a convenient way to check log parser without setting up the full system to do log parse. For more information about the **logParse** command, at the command line, type `help logParse`.

Thick Client Error: remote content device entry not found

Error: "*The remote content device entry was not found*," generated for a correlation rule applied to a concentrator.

Problem: in Investigation, if you click the `correlation-rule-name` meta value in the Alert meta key, you do not get session information.

Solution: Instead of using correlation rules on decoders and concentrators, use ESA rules. The ESA rules **do** record the correlation sessions that match the ESA rule.

View Example Parsers

Since flex and lua parsers are encrypted when they are delivered by Live, you cannot easily view their contents.

However, some plain text examples are available here: **https://community.emc.com/docs/DOC-41108**.

Configure WinRM Event Sources

The following Inside EMC article has a video that walks through the process of setting up Windows RM (Remote Management) collection: **https://inside.emc.com/docs/DOC-122732**.

Additionally, it contains two scripts that are shortcuts for procedures described in the "Windows Event Source Configuration Guide."

NwLogPlayer

NwLogPlayer is a utility that simulates syslog traffic. In the hosted environment, `NwLogPlayer.exe` is a command line utility located on the RSA NetWitness® Suite Client machine in the following directory:

```
C:\Program Files\NetWitness\NetWitness 9.8
```

NwLogPlayer is also located on the Log Decoder host in `/usr/bin`.

Usage

At the command line, type `nwlogplayer.exe -h` to list the available options, as reproduced here:

`--priority arg`	set log priority level
`-h [ --help ]`	show this message
`-f [ --file ] arg (=stdin)`	input message; defaults to **stdin**
`-d [dir ] arg`	input directory
`-s [ --server ] arg (=localhost)`	remote server; defaults to **localhost**
`-p [ --port ] arg (=514)`	remote port; defaults to **514**
`-r [ --raw ] arg (=0)`	Determines raw mode. • 0 = add priority mark (default) • 1= File contents will be copied line by line to the server. • 3 = auto detect • 4 = enVision stream • 5 = binary object
`-m [ --memory ] arg`	Speed test mode. Read up to 1 Megabyte of messages from the file content and replays.
`--rate arg`	Number of events per second. This argument has no effect if **rate** > eps that the program can achieve in continuous mode.
`--maxcnt arg`	maximum number of messages to be sent
`-c [ --multiconn ]`	multiple connection
`-t [ --time ] arg`	simulate time stamp time; format is `yyyy-m-d-hh:mm:ss`
`-v [ --verbose ]`	If **true**, output is verbose
`--ip arg`	simulate an IP tag
`--ssl`	use SSL to connect

`--certdir arg`	OpenSSL certificate authority directory
`--clientcert arg`	use this PEM-encoded SSL client certificate
`--udp`	send in UDP

Troubleshoot Feeds

Overview

The purpose of the feed generator is to generate a mapping of an event source to the list of groups to which it belongs.

If you have an event source from which you are collecting messages, and yet it is not displayed in the correct event source groups, then this topic provides background and information to help you track down the problem.

Details

The ESM Feed maps multiple keys to single value. It maps the DeviceAddress, Forwarder, and DeviceType attributes to groupName.

The purpose of the ESM feed is to enrich event source Meta with the groupName collected on the Log Decoder.

How it Works

The feed generator is scheduled to update every minute. However, it is triggered only if there are any changes (create, update, or delete) in event sources or groups.

It generates a single feed file with event source to group mapping, and pushes the same feed to all of the Log Decoders that are connected to NetWitness Suite.

Once the feed file is uploaded on the Log Decoders, for any new events, it enriches events Meta data with groupName, and appends this groupName to logstats.

Once the groupName is in logstats, the ESM Aggregator groups information and sends it to ESM. At this point, you should see the **Group Name** column under the **Event Source Monitoring** tab.

The entire process can take some time. Therefore, you may need to wait for several seconds after you add a new group or event source, before the Group name is displayed.

Note: If the event source type attribute changes when the feed is updated, NetWitness Suite adds a new logstats entry, rather than updating the existing one. Thus, there will be two different logstats entries in logdecoder. Previously existing messages would have been listed under the previous type, and all new messages are logged for the new event source type.

Feed File

The format of the feed file is as follows:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

The `DeviceAddress` is either `ipv4, ipv6`, or `hostname`, depending on which of these have been defined for the event source.

The following is a sample of the feed file:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apachegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","Apachegrp"
```

Troubleshooting

You can check the following items to narrow down where the problem is occurring.

Feed File Existence

Verify that the feeds ZIP archive exists in the following location:

```
/opt/rsa/sms/esmfeed.zip
```

Do not modify this file.

Group Meta Populated on LD

Verify that the group meta is populated on the Log Decoder. Navigate to the Log Decoder REST and check logstats:

```
http://LogDecoderIP:50102/decoder?msg=logStats&force-content-
type=text/plain
```

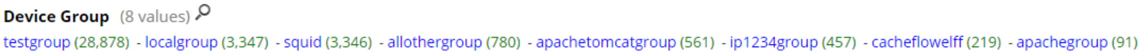
This is a sample logstats file with group information:

```
device=apache  forwarder=NWAPPLIANCE10304  source=1.2.3.4  count=338
lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat  forwarder=NWAPPLIANCE10304  source=5.6.7.8
count=1301  lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-
04 22:30:19  groups=AllOtherGroup,ApacheTomcatGroup
```

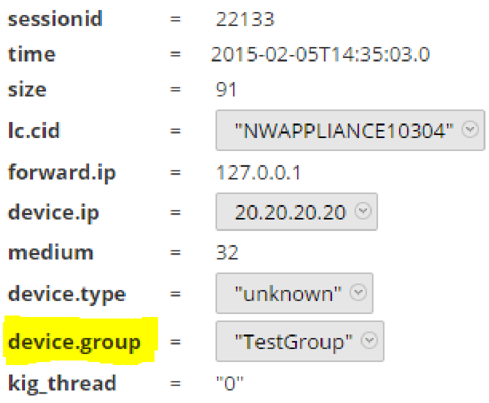
In the above text, the group information is **bold**.

Device Group Meta on Concentrator

Verify that the **Device Group** meta exists on the Concentrator, and that events have values for the `device.group` field.



Device Group (8 values)
testgroup (28,878) - localgroup (3,347) - squid (3,346) - allothergroup (780) - apachetomcatgroup (561) - ip1234group (457) - cacheflowelff (219) - apachegroup (91)



sessionid = 22133
time = 2015-02-05T14:35:03.0
size = 91
lc.cid = "NWAPPLIANCE10304"
forward.ip = 127.0.0.1
device.ip = 20.20.20.20
medium = 32
device.type = "unknown"
device.group = "TestGroup"
kig_thread = "0"

SMS Log File

Check the SMS log file in the following location to view informational and error messages: `/opt/rsa/sms/logs/sms.log`

The following are example informational messages:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

The following are example error messages:

```
Error creating CSV File : <reason>Unable to push the ESM Feed: Unable to
create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> : Error: <error>
Unable to push the ESM Feed: CSV file is empty, make sure you have al-
least on group with al-least one eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on LogDecoder-
<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error: The zip
archive "/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not be
opened
Unable to push the ESM Feed: <reason>
```

Verify Logstats data is getting Read & Published by ESMReader & ESMAggregator

These are the steps to verify that logstats are collected by **collectd** and published to Event Source Management.

ESMReader

1. On LogDecoders add **debug "true"** flag in **/etc/collectd.d/NwLogDecoder_ESM.conf**:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>        </stats>    </Module>    <Module
"NgEsmReader" "update">        port      "56002"
```

```
            ssl       "yes"
            keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
    4838-a2f7-    ba7e9a165aae.pem"
            certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
    a2f7-   ba7e9a165aae.pem"
            interval  "60"
            query     "update"
            <stats>        </stats>    </Module></Plugin>
```

2. Run the command:
   `collectd service restart`
3. Run the following command:
   `tail –f /var/log/messages | grep collectd`
   Verify that ESMReader is reading logstats and there are no errors. If there are any read issues, you will see errors similar to the following:

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. On NetWitness Suite, uncomment the verbose flag in **/etc/collectd.d/ESMAggregator.conf**:

```
# ESMAggregator module collectd.conf configuration file
#
# Copyright (c) 2014 RSA The Security Divsion of EMC
#

<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"

<Module "ESMAggregator">
        verbose 1
        interval "60"
        cache_save_interval "600"
```

```
                persistence_dir "/var/lib/netwitness/collectd"
        </Module>    </Plugin>
```

2. Run the following:
   `collectd service restart`.
3. Run the following command:
   `run “tail –f /var/log/messages | grep ESMA`
   Look for for ESMAggregator data and make sure your logstat entry is available in logs.

Sample output:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
```

```
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Configure JMX Feed Generator Job Interval

Although the feed generation job is scheduled to execute every minute by default, you can change this by using `jconsole`, if necessary.

To change the feed generator job interval:

1. Open **jconsole** for the SMS service.
2. On the MBeans tab, navigate to **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributes**.
3. Modify the value for the property **FeedGeneratorJobIntervalInMinutes**.
4. Go to **Operations** under the same navigation tree, an click **commit()**. This persists the new value in the corresponding json file under **/opt/rsa/sms/conf**, and uses the value if SMS is restarted.

Setting a new value reschedules the feed generator job for the new interval.

References

This section describes the NetWitness Suite user interface views in which you can perform system maintenance tasks. You use this interface to:

- Monitor and maintain services (settings, statistics, command and message syntax, REST API, RSA Console utility, and protocols supported in NetWitness Suite).
- Display the current NetWitness Suite version and license status.
- Manage your Local Update Repository from which you apply software version updates to hosts.

The following topics describe each interface in detail:

- Health and Wellness View
- System View - System Info Panel

Health and Wellness View

The Health and Wellness settings allow you to set and view alarms, monitor events, and view policies and system statistics. For more details on each of these, see the following topics:

- Health and Wellness View - Alarms View
- Event Source Monitoring View
- Health and Wellness Historical Graphs
- Health and Wellness Settings View - Archiver
- Health and Wellness Settings View - Event Sources
- Health and Wellness Settings View - Warehouse Connector
- Monitoring View
- Policies View
- System Stats Browser View

Health and Wellness View - Alarms View

You can monitor hosts and services to determine when user-defined limitations have been reached by viewing all the active alarms. Policy rules, that you define or assign to hosts and services, in the **Policies tab** trigger these alarms. You can:

- View all the alarms that are currently active for all your systems and services
- Select an alarm and view its details

What do you want to do?

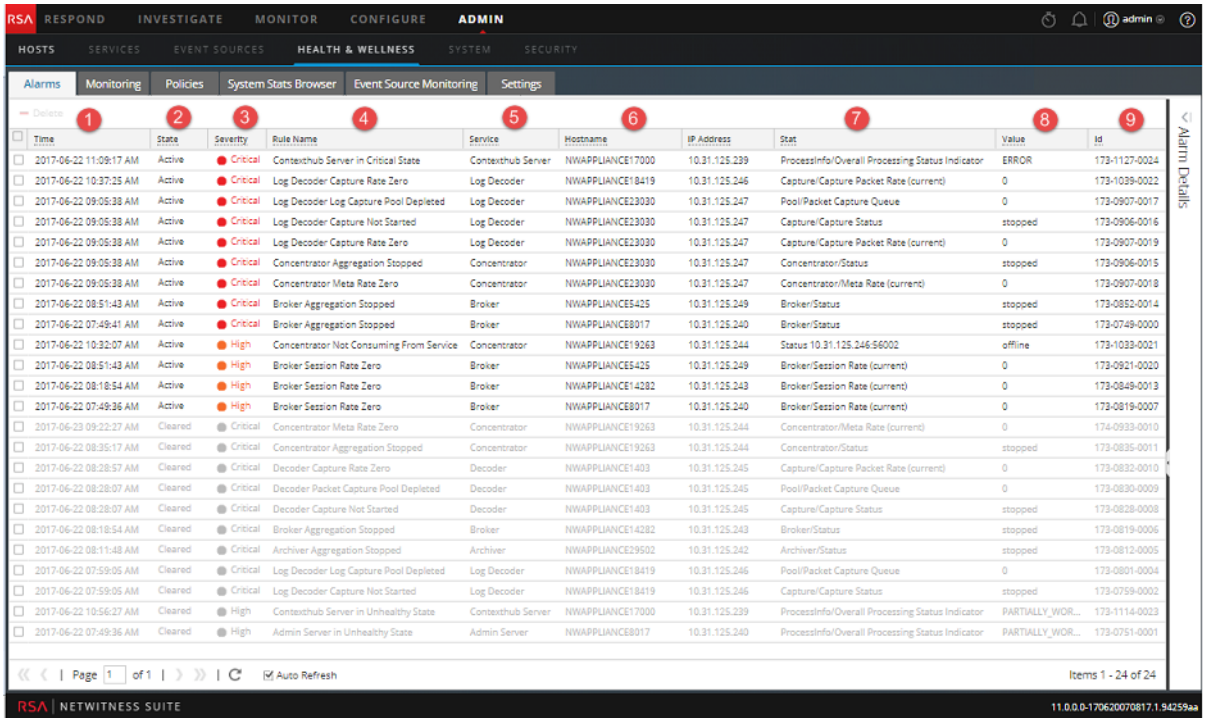
Role	I want to ...	Show me how
Administrator	View the alarm status of NetWitness Servers and services.	Monitor Alarms
Administrator	View detailed information about a specific alarm.	Monitor Alarms

Related Topics

Manage Policies

Quick Look

The required permission to access this view is **Manage services**. To access the Alarms view, go to **Admin** > **Health & Wellness**. The Health & Wellness view opens with the Alarms tab displayed. The Alarms tab contains an alarms list and an Alarm Details panel.



□	Time	State	Severity	Rule Name	Service	Hostname	IP Address	Stat	Value	Id
□	2017-06-22 11:09:17 AM	Active	● Critical	Contexthub Server in Critical State	Contexthub Server	NWAPPLIANCE17000	10.31.125.239	ProcessInfo/Overall Processing Status Indicator	ERROR	173-1127-0024
□	2017-06-22 10:37:25 AM	Active	● Critical	Log Decoder Capture Rate Zero	Log Decoder	NWAPPLIANCE18419	10.31.125.246	Capture/Capture Packet Rate (current)	0	173-1039-0022
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Log Capture Pool Depleted	Log Decoder	NWAPPLIANCE23030	10.31.125.247	Pool/Packet Capture Queue	0	173-0907-0017
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Capture Not Started	Log Decoder	NWAPPLIANCE23030	10.31.125.247	Capture/Capture Status	stopped	173-0906-0016
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Capture Rate Zero	Log Decoder	NWAPPLIANCE23030	10.31.125.247	Capture/Capture Packet Rate (current)	0	173-0907-0019
□	2017-06-22 09:05:38 AM	Active	● Critical	Concentrator Aggregation Stopped	Concentrator	NWAPPLIANCE23030	10.31.125.247	Concentrator/Status	stopped	173-0906-0015
□	2017-06-22 09:05:38 AM	Active	● Critical	Concentrator Meta Rate Zero	Concentrator	NWAPPLIANCE23030	10.31.125.247	Concentrator/Meta Rate (current)	0	173-0907-0018
□	2017-06-22 08:51:43 AM	Active	● Critical	Broker Aggregation Stopped	Broker	NWAPPLIANCE5425	10.31.125.249	Broker/Status	stopped	173-0852-0014
□	2017-06-22 07:49:41 AM	Active	● Critical	Broker Aggregation Stopped	Broker	NWAPPLIANCE8017	10.31.125.240	Broker/Status	stopped	173-0749-0000
□	2017-06-22 10:32:07 AM	Active	● High	Concentrator Not Consuming From Service	Concentrator	NWAPPLIANCE19263	10.31.125.244	Status 10.31.125.246:56002	offline	173-1033-0021
□	2017-06-22 08:51:43 AM	Active	● High	Broker Session Rate Zero	Broker	NWAPPLIANCE5425	10.31.125.249	Broker/Session Rate (current)	0	173-0921-0020
□	2017-06-22 08:18:54 AM	Active	● High	Broker Session Rate Zero	Broker	NWAPPLIANCE14282	10.31.125.243	Broker/Session Rate (current)	0	173-0849-0013
□	2017-06-22 07:49:36 AM	Active	● High	Broker Session Rate Zero	Broker	NWAPPLIANCE8017	10.31.125.240	Broker/Session Rate (current)	0	173-0819-0007
□	2017-06-23 09:22:27 AM	Cleared	● Critical	Concentrator Meta Rate Zero	Concentrator	NWAPPLIANCE19263	10.31.125.244	Concentrator/Meta Rate (current)	0	174-0933-0010
□	2017-06-22 08:35:17 AM	Cleared	● Critical	Concentrator Aggregation Stopped	Concentrator	NWAPPLIANCE19263	10.31.125.244	Concentrator/Status	stopped	173-0835-0011
□	2017-06-22 08:28:57 AM	Cleared	● Critical	Decoder Capture Rate Zero	Decoder	NWAPPLIANCE1403	10.31.125.245	Capture/Capture Packet Rate (current)	0	173-0832-0010
□	2017-06-22 08:28:07 AM	Cleared	● Critical	Decoder Packet Capture Pool Depleted	Decoder	NWAPPLIANCE1403	10.31.125.245	Pool/Packet Capture Queue	0	173-0830-0009
□	2017-06-22 08:28:07 AM	Cleared	● Critical	Decoder Capture Not Started	Decoder	NWAPPLIANCE1403	10.31.125.245	Capture/Capture Status	stopped	173-0828-0008
□	2017-06-22 08:18:54 AM	Cleared	● Critical	Broker Aggregation Stopped	Broker	NWAPPLIANCE14282	10.31.125.243	Broker/Status	stopped	173-0819-0006
□	2017-06-22 08:11:48 AM	Cleared	● Critical	Archiver Aggregation Stopped	Archiver	NWAPPLIANCE29502	10.31.125.242	Archiver/Status	stopped	173-0812-0005
□	2017-06-22 07:59:05 AM	Cleared	● Critical	Log Decoder Log Capture Pool Depleted	Log Decoder	NWAPPLIANCE18419	10.31.125.246	Pool/Packet Capture Queue	0	173-0801-0004
□	2017-06-22 07:59:05 AM	Cleared	● Critical	Log Decoder Capture Not Started	Log Decoder	NWAPPLIANCE18419	10.31.125.246	Capture/Capture Status	stopped	173-0759-0002
□	2017-06-22 10:56:27 AM	Cleared	● High	Contexthub Server in Unhealthy State	Contexthub Server	NWAPPLIANCE17000	10.31.125.239	ProcessInfo/Overall Processing Status Indicator	PARTIALLY_WOR...	173-1114-0023
□	2017-06-22 07:49:36 AM	Cleared	● High	Admin Server in Unhealthy State	Admin Server	NWAPPLIANCE8017	10.31.125.240	ProcessInfo/Overall Processing Status Indicator	PARTIALLY_WOR...	173-0751-0001

Items 1 - 24 of 24

1 Time when the alarm was triggered.

2 Status of the alarm:

- **Active -** the statistical threshold was crossed triggering the alarm.
- **Cleared -** the clearing threshold was crossed and the alarm is no longer active.

3 Severity assigned to this alarm:

- **Critical**
- **High**
- **Medium**
- **Low**

4 Name of the rule that triggers the alarm.

5 Service defined in the rule.

6 Host on which the alarm is triggered.

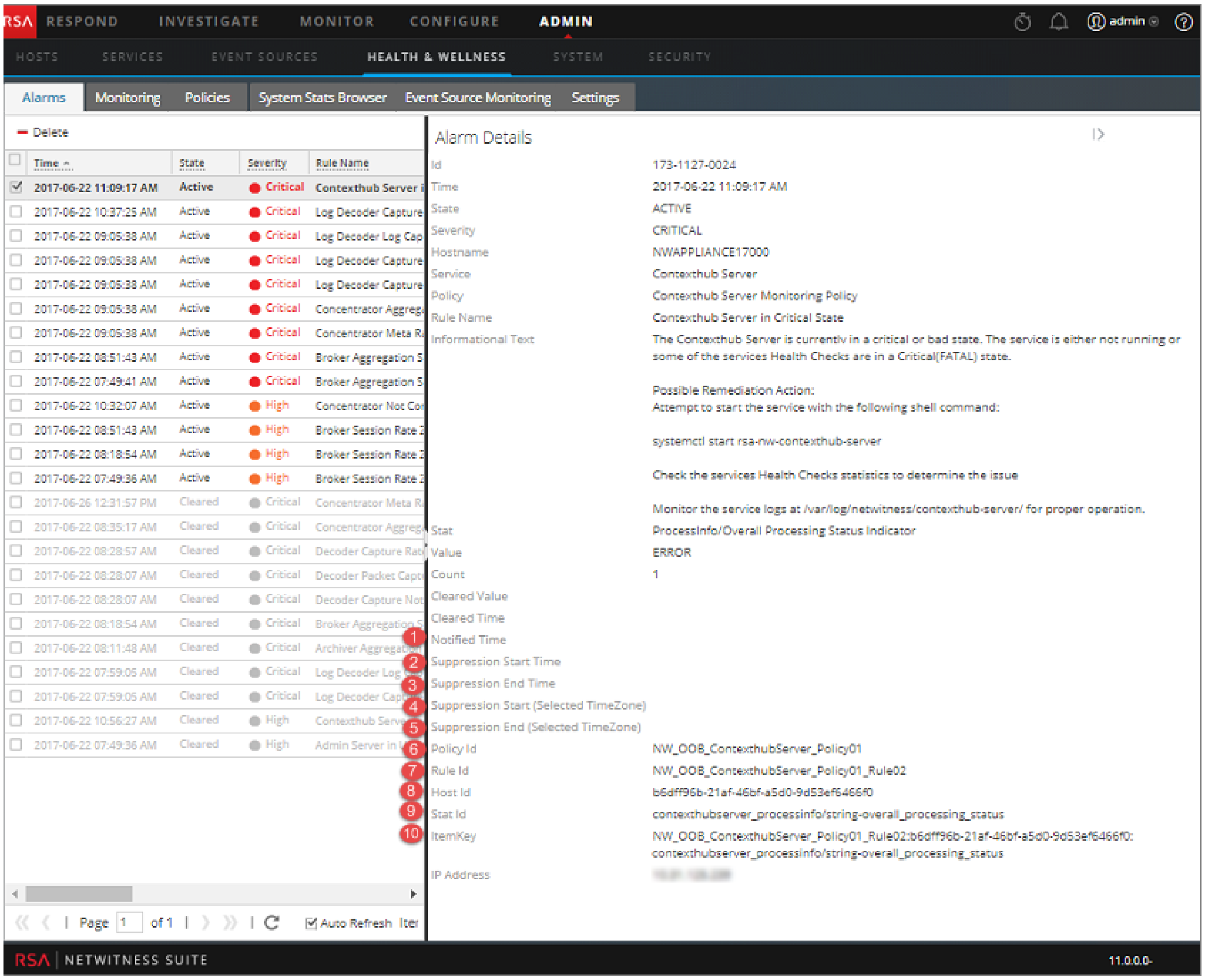
7 Statistic selected in the rule that triggers the alarm.

8 Value of the statistic that triggered the alarm.

9 Identification number of the alarm.

Note: NetWitness Suite sorts the alarms in time order. You can sort the relevant parameters in ascending or descending order.

This figure shows the Alarms tab with the Alarm Details panel expanded.



□	Time	State	Severity	Rule Name
☑	2017-06-22 11:09:17 AM	Active	● Critical	Contexthub Server i
□	2017-06-22 10:37:25 AM	Active	● Critical	Log Decoder Capture
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Log Cap
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Capture
□	2017-06-22 09:05:38 AM	Active	● Critical	Log Decoder Capture
□	2017-06-22 09:05:38 AM	Active	● Critical	Concentrator Aggreg
□	2017-06-22 09:05:38 AM	Active	● Critical	Concentrator Meta R
□	2017-06-22 08:51:43 AM	Active	● Critical	Broker Aggregation S
□	2017-06-22 07:49:41 AM	Active	● Critical	Broker Aggregation S
□	2017-06-22 10:32:07 AM	Active	● High	Concentrator Not Co
□	2017-06-22 08:51:43 AM	Active	● High	Broker Session Rate 2
□	2017-06-22 08:18:54 AM	Active	● High	Broker Session Rate 2
□	2017-06-22 07:49:36 AM	Active	● High	Broker Session Rate 2
□	2017-06-26 12:31:57 PM	Cleared	● Critical	Concentrator Meta R
□	2017-06-22 08:35:17 AM	Cleared	● Critical	Concentrator Aggreg
□	2017-06-22 08:28:57 AM	Cleared	● Critical	Decoder Capture Rat
□	2017-06-22 08:28:07 AM	Cleared	● Critical	Decoder Packet Capt
□	2017-06-22 08:28:07 AM	Cleared	● Critical	Decoder Capture Not
□	2017-06-22 08:18:54 AM	Cleared	● Critical	Broker Aggregation S
□	2017-06-22 08:11:48 AM	Cleared	● Critical	Archiver Aggregation
□	2017-06-22 07:59:05 AM	Cleared	● Critical	Log Decoder Log
□	2017-06-22 07:59:05 AM	Cleared	● Critical	Log Decoder Cap
□	2017-06-22 10:56:27 AM	Cleared	● High	Contexthub Serve
□	2017-06-22 07:49:36 AM	Cleared	● High	Admin Server in

Alarm Details

Id 173-1127-0024
Time 2017-06-22 11:09:17 AM
State ACTIVE
Severity CRITICAL
Hostname NWAPPLIANCE17000
Service Contexthub Server
Policy Contexthub Server Monitoring Policy
Rule Name Contexthub Server in Critical State
Informational Text The Contexthub Server is currentlv in a critical or bad state. The service is either not running or some of the services Health Checks are in a Critical(FATAL) state.

Possible Remediation Action:
Attempt to start the service with the following shell command:

```
systemctl start rsa-nw-contexthub-server
```

Check the services Health Checks statistics to determine the issue

Monitor the service logs at /var/log/netwitness/contexthub-server/ for proper operation.

Stat ProcessInfo/Overall Processing Status Indicator
Value ERROR
Count 1
Cleared Value
Cleared Time
Notified Time
Suppression Start Time
Suppression End Time
Suppression Start (Selected TimeZone)
Suppression End (Selected TimeZone)
Policy Id NW_OOB_ContexthubServer_Policy01
Rule Id NW_OOB_ContexthubServer_Policy01_Rule02
Host Id b6dff96b-21af-46bf-a5d0-9d53ef6466f0
Stat Id contexthubserver_processinfo/string-overall_processing_status
ItemKey NW_OOB_ContexthubServer_Policy01_Rule02:b6dff96b-21af-46bf-a5d0-9d53ef6466f0:contexthubserver_processinfo/string-overall_processing_status
IP Address [redacted]

Alarm Details Panel

The Alarm Details panel displays information for the alarm selected in the Alarms list. It contains all the information in the Alarms list plus the following fields.

1	Alarm Notified time
2	Suppression start time
3	Suppression end time
4	Suppression start (selected time zone)
5	Suppression end (selected time zone)
6	The Policy ID

7	The Rule ID
8	The Host ID
9	The Stat ID
10	Item key

Event Source Monitoring View

Note: To manage Event Sources, see "About Event Source Management" in the *NetWitness Suite Event Source Management Guide*.

NetWitness Suite provides a way to monitor the statistics for various event sources in the User Interface. The information displayed is historical and comes from the Log decoder. You can customize the view depending on the parameter you select to filter the data.

To access the Event Source Monitoring view:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Click **Event Source Monitoring**.

What do you want to do?

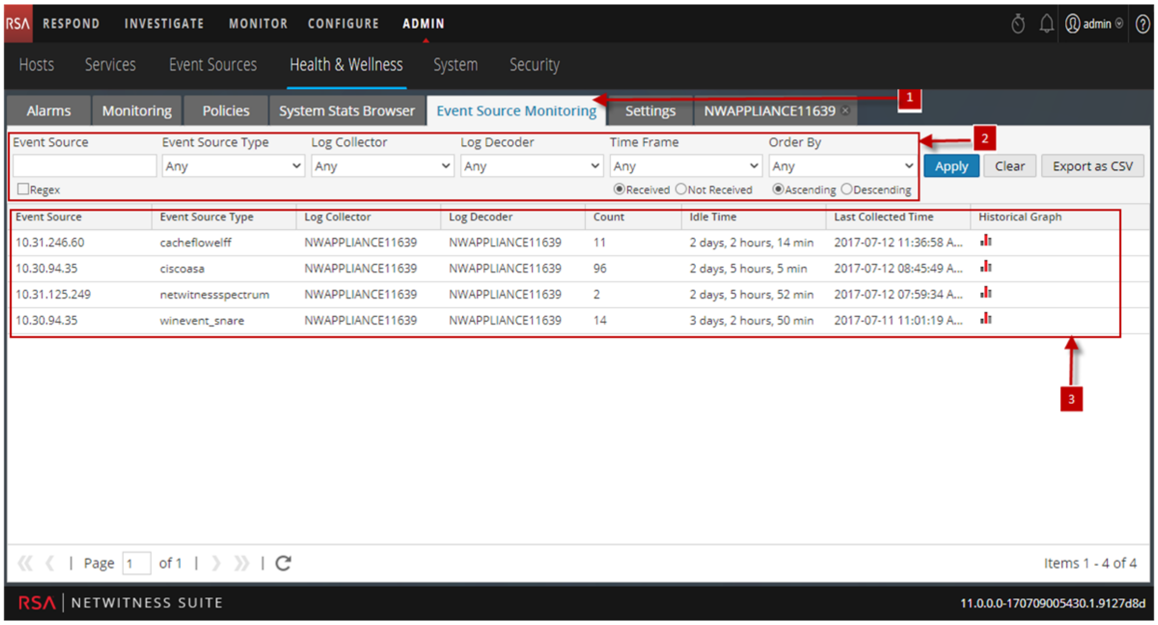
Role	I want to ...	Show me how
Administrator	View the Events Collected from an Event Source	Historical Graph View for Events Collected from an Event Source

Related Topics

- Monitor Event Sources
- Filter Event Sources
- View Historical Graph of Events Collected for an Event Source

Quick Look

The Event Source Monitoring view is displayed.



Event Source: | Event Source Type: Any | Log Collector: Any | Log Decoder: Any | Time Frame: Any | Order By: Any

□ Regex ● Received ○ Not Received ● Ascending ○ Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historical Graph
10.31.246.60	cacheflowelff	NWAPPLIANCE11639	NWAPPLIANCE11639	11	2 days, 2 hours, 14 min	2017-07-12 11:36:58 A...	
10.30.94.35	ciscoasa	NWAPPLIANCE11639	NWAPPLIANCE11639	96	2 days, 5 hours, 5 min	2017-07-12 08:45:49 A...	
10.31.125.249	netwitnessspectrum	NWAPPLIANCE11639	NWAPPLIANCE11639	2	2 days, 5 hours, 52 min	2017-07-12 07:59:34 A...	
10.30.94.35	winevent_snare	NWAPPLIANCE11639	NWAPPLIANCE11639	14	3 days, 2 hours, 50 min	2017-07-11 11:01:19 A...	

1	Displays Event Source Monitoring tab.
2	Toolbar used to filter and customize the Event Source Monitoring tab.
3	Displays Event Source Stats panel.

Filters

This table lists the various parameters you can use to filter and customize the event source monitoring view.

Parameter	Description
Event Source	Type the name of an event source you want to monitor. Select Regex to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Event Source Type	Select an event source type for the event source selected.
Log Collector	Select the Log Collector to display the data collected by the specified Log Collector.

Parameter	Description
Log Decoder	Select a Log Decoder to display the data collected by the specified Log Decoder.
Time Frame	Select the time frame for which you want the stats. Select **Received** if you need the query results to contain only event sources that logs have been received from within the selected time. or Select **Not Received** if you need the query results to contain only event sources that logs have not been received from within the selected time
Order By	Select the order in which the list needs to be filtered. Select Ascending to filter it in an ascending order.
Apply	Click to apply the filters chosen and display the list accordingly.
Clear	Click to clear the chosen filters.
Export as CSV	Click to export the information as a csv file.

Event Source Stats View Display

Parameter	Description
Event Source	Displays the name of the event source.
Event Source Type	Displays the event source type.
Log Collector	Displays the Log Collector from where the events were initially captured.
Log Decoder	Displays the Log Decoder where the events are being processed.
Count	Displays the number of events received by Log Decoder since last reset of count value.
Idle Time	Displays the time lapsed after the last stat collection.

Parameter	Description
Last Collected Time	Displays the time at which the Log Decoder last processed an event for the event source
Historical Graph	Click 📊 to view the historical graph of the stats collected for the event source.

Health and Wellness Historical Graphs

Configuring the Archiver monitoring enables you to automatically generate notification when critical thresholds concerning Archiver aggregation and storage have been met. The Historical Graph view provides a visualization of historical data.

Note: Historical graphs are not available for non-numeric statistics, and is indicated by a greyed out icon.

See the following topics for more details:

- Historical Graph View for Events Collected from an Event Source
- Historical Graph for System Stats

Historical Graph View for Events Collected from an Event Source

The Historical Graph view for events collected from an event source provides a visualization of historical data. To access this view:

1. Go to **ADMIN > Health & Wellness**.

   The Health & Wellness view is displayed with the Monitoring tab open.

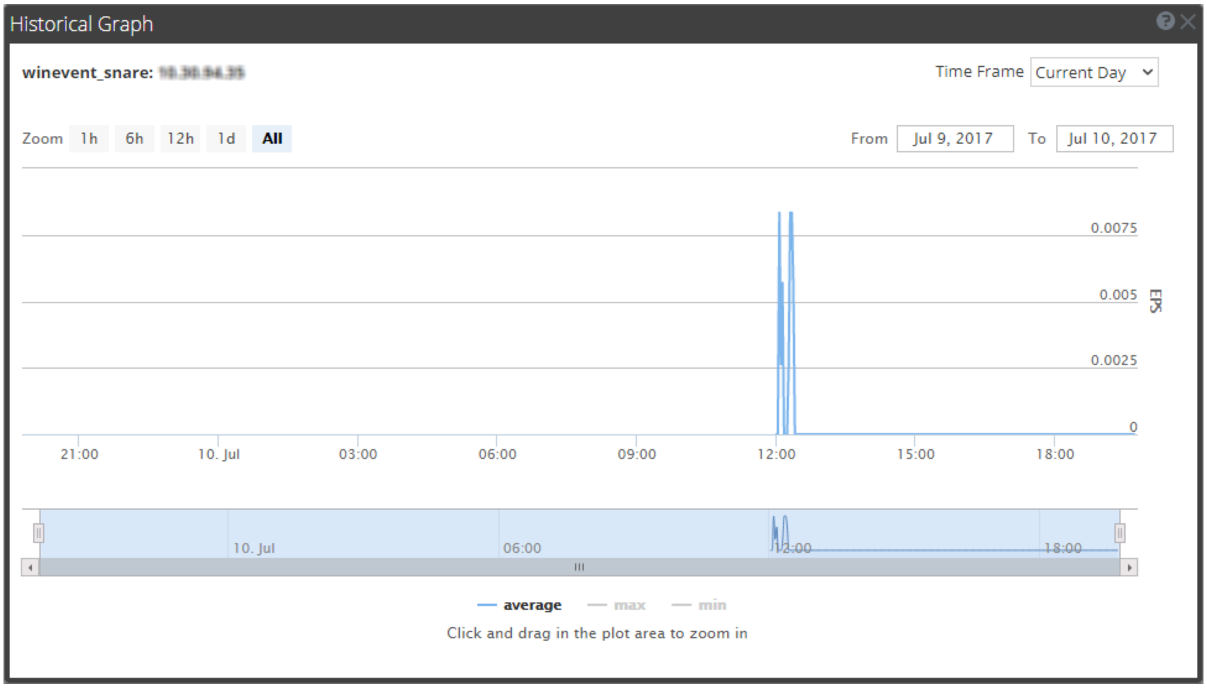
2. Click **Event Source Monitoring**.

   The Event Source Monitoring view is displayed.

3. In the **Historical Graph** column, select 📊.

   The Historical graph for the selected event source type is displayed in a popup window.

The figure displays the events collected from the event source type **winevent_snare**.



Historical Graph

winevent_snare: [redacted]

Time Frame: Current Day

From Jul 9, 2017 To Jul 10, 2017

You can customize the graph as required. The table lists the various parameters used to customize the historical graph.

Parameter	Description
Time Frame	Select the Time Frame for which you want to view the historical data. The available options are: Current Day, Current, Week, Current Month.
From <date> To <date>	Select the date range for which you want to view the historical data.

You can zoom in for a detailed view of the data in the Historical graph.

Zoom In Function 1 and 2

You can select one of the values to view the historical data for the selected value. The figure below displays an example for the 6h frame selected for zoom in. The slider bar at the right bottom corner is also changed to a 6h window.

Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.

Zoom In Function 3

You can click and drag in the plot area to zoom in for a required frame of time.

Historical Graph for System Stats

To access the Historical Graph for the System Stats:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

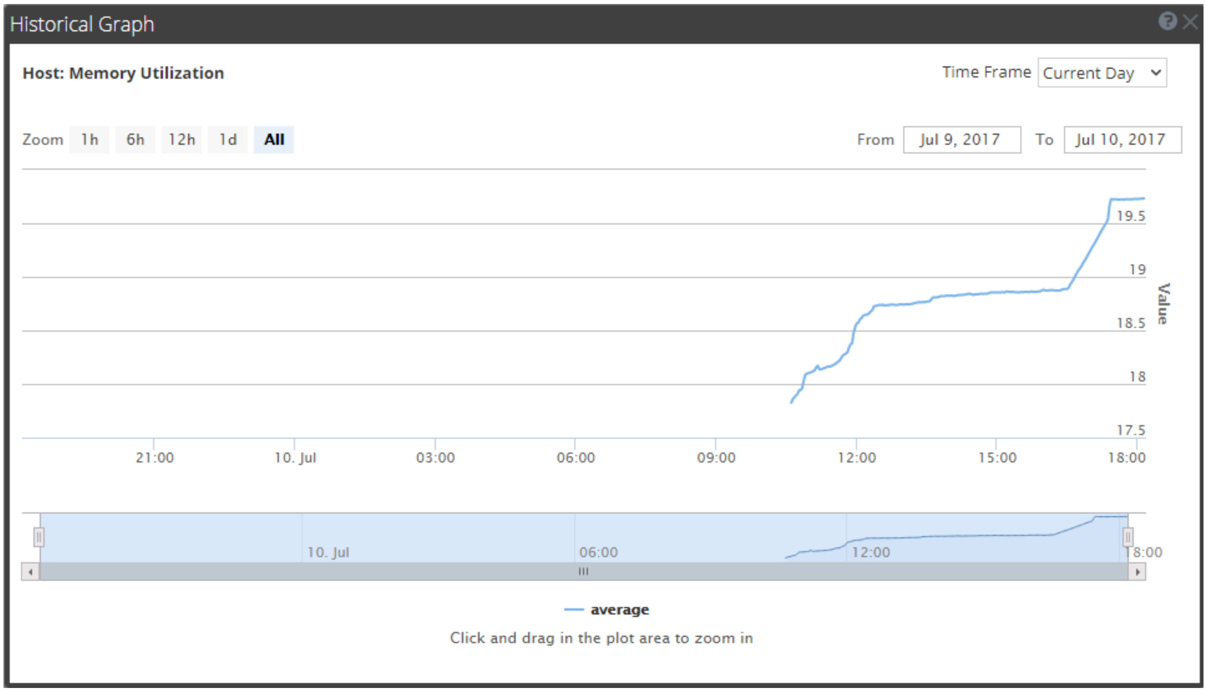
2. Click the **System Stats Browser** tab.

   The System Stats Browser tab is displayed.

3. In the **Historical Graph** column, select 📊.

   The Historical graph for the selected statistic for a host is displayed.

   The figure displays the system stats view for the Memory Utilization statistics.



Historical Graph

Host: Memory Utilization

Time Frame: Current Day

From: Jul 9, 2017 To: Jul 10, 2017

Parameters

You can customize the graph view as required. The table lists the various parameters used to customize the historical graph view.

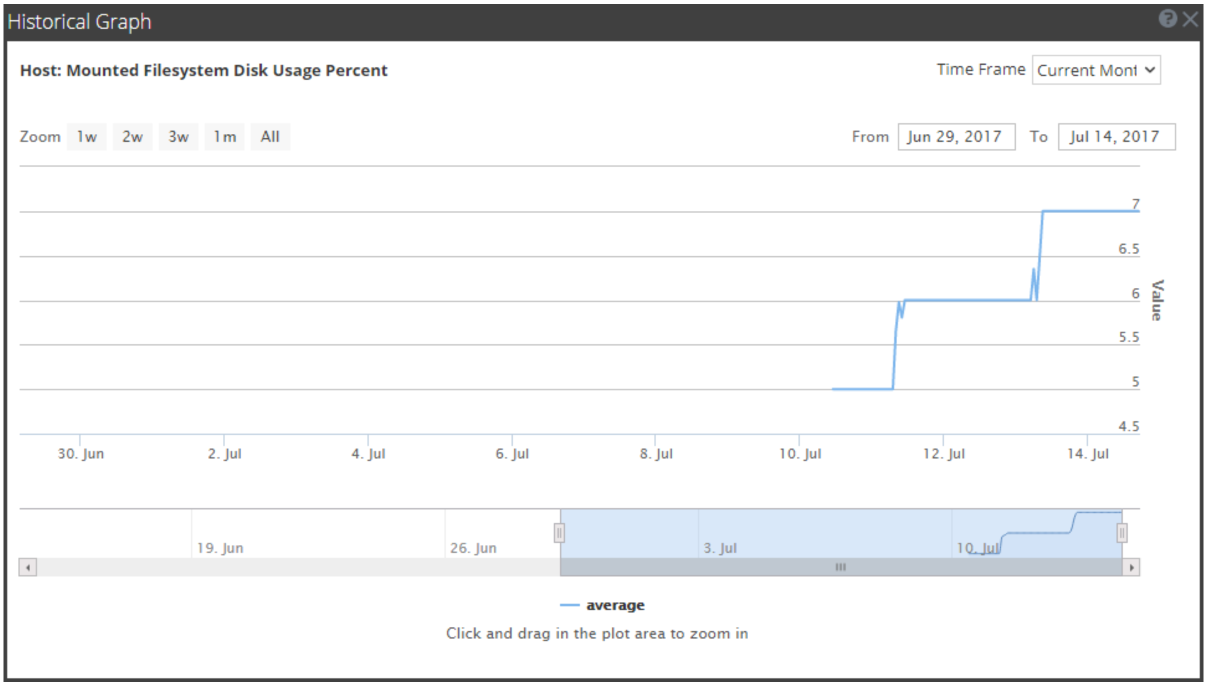
Parameter	Description
Time Frame	Select the time frame for which you want to view the historical data. The available options are: **Current Day**, **Current Week**, **Current Month**, and **Current Year**.
From <date> To <date>	Select the date range for which you want to view the historical data,

You can zoom in for a detailed view of the data in the Historical graph.

Zoom in function 1 and 2:

You can select one of the values to view the historical data for the selected value. The figure below displays an example for the 6h frame selected for zoom in. The slider bar at the right bottom corner is also changed to a 6h window.

Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.



Historical Graph

Host: Mounted Filesystem Disk Usage Percent

Time Frame: Current Mont

Zoom 1w 2w 3w 1m All

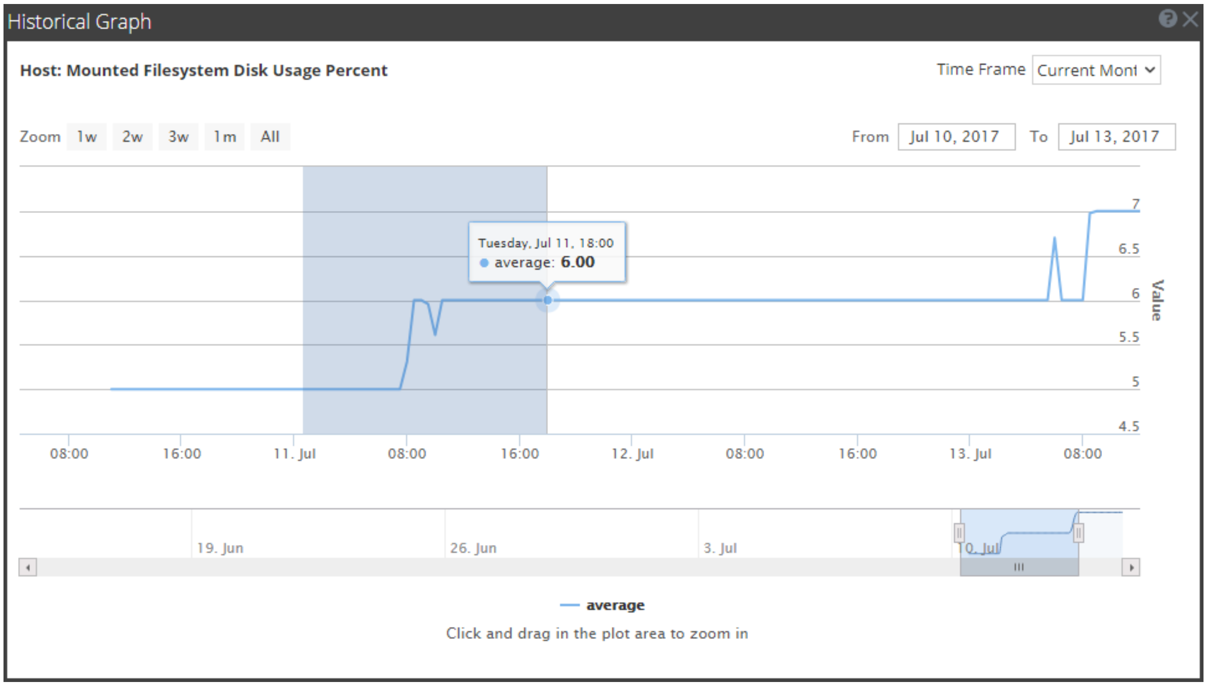
From: Jun 29, 2017 To: Jul 14, 2017

Click and drag in the plot area to zoom in

Zoom in function 3:

You can click and drag in the plot area to zoom in for a required frame of time.

The figure below displays an example of how the graph appears while you click and drag.



Historical Graph

Host: Mounted Filesystem Disk Usage Percent

Time Frame: Current Mont

From: Jul 10, 2017 To: Jul 13, 2017

Health and Wellness Settings View - Archiver

Note: To monitor Archiver and Warehouse Connector, see Health Policy.

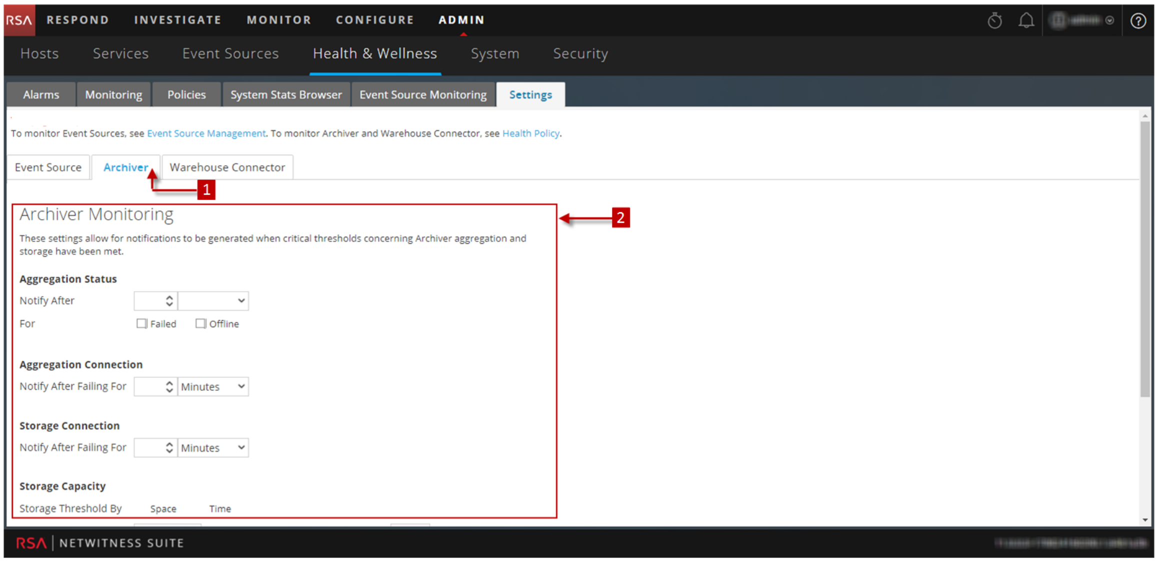
To access the Archiver Monitoring view:

1. Go to **Administration** > **Health & Wellness**.
2. Select **Settings** > **Archiver**.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Monitor service details of Archiver	Monitor Service Details

Quick Look



To monitor Event Sources, see Event Source Management. To monitor Archiver and Warehouse Connector, see Health Policy.

Archiver Monitoring

These settings allow for notifications to be generated when critical thresholds concerning Archiver aggregation and storage have been met.

Aggregation Status

Notify After

For ☐ Failed ☐ Offline

Aggregation Connection

Notify After Failing For Minutes

Storage Connection

Notify After Failing For Minutes

Storage Capacity

Storage Threshold By Space Time

1	Displays Archiver Monitoring Panel
2	Configure Archiver Monitoring Panel to automatically receive notification

Features

The following table lists the parameters required to configure the Archiver to automatically generate notification when critical thresholds are reached.

Parameter	Value	Description
Aggregation Status	Notify After	Number of minutes or hours after which the you will get notified of the Aggregation status
	For	Failed - If enabled, you get notification when the Archiver aggregation status is failed for the defined number of minutes or hours. Offline - If enabled, you get a notification when the Archiver aggregation status is offline for the defined number of minutes or hours
Aggregation Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver aggregation connection fails.
Storage Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver storage connection fails.
Storage Capacity	Storage Threshold By	Select **Space**, if you want to receive a notification when the Archiver storage capacity exceeds the percentage defined in the **When Storage Size Is** field. Select **Time**, if you want to receive a notification when the files stored in the Archiver exceeds the defined number of days in the **When Oldest Storage File Is** field
	When Storage Size Is	Enter what percent full the storage size should be if you want to receive a notification.
	When Warm Storage Size Is	Enter what percent full the warm storage size should be if want to receive a notification.

Parameter	Value	Description
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness Suite.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.
	NW Console, Email, Syslog Notification, SNMP Trap Notification	Enable NW Console to get notifications on the NetWitness Suite UI notification toolbar. Enable Email to get email notifications. Enable Syslog Notification to generate syslog events. Enable SNMP Trap Notification to get audit events as SNMP traps.

Health and Wellness Settings View - Event Sources

Note: To manage Event Sources, see "About Event Source Management" in the *RSA NetWitness Suite Event Source Management Guide*.

The Event Source Monitoring view consists of the Event Source panel, Add/Edit Source Monitor dialog, Decommission panel, and the Decommission dialog. You use the view to configure:

- When to generate notifications for event sources from which the Log Collector is no longer receiving logs.
- Where to send those notifications.
- When to decommission a Log Collector when a Remote Collector and the Local Collector fails over to a standby Log Decoder.

The required role to access this view is **Manage NW Auditing**. To access this view:

1. Go to **Admin** > **Health & Wellness**.
2. Select **Settings** > **Event Source**.

What do you want to do?

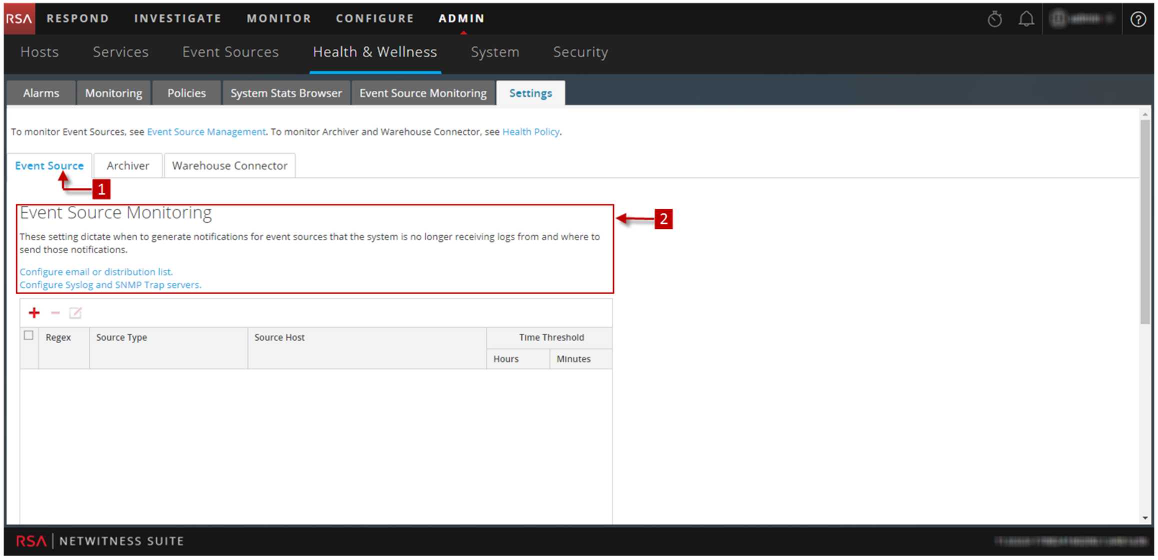
Role	I want to ...	Show me how
Administrator	View the functionality of Event Source Monitoring	Monitor Event Sources

Related Topics

Configure Event Source Monitoring

Quick Look

The Event Source tab is displayed.



To monitor Event Sources, see Event Source Management. To monitor Archiver and Warehouse Connector, see Health Policy.

Event Source Monitoring

These setting dictate when to generate notifications for event sources that the system is no longer receiving logs from and where to send those notifications.

Configure email or distribution list.
Configure Syslog and SNMP Trap servers.

□	Regex	Source Type	Source Host	Time Threshold	
				Hours	Minutes

1	Displays Event Source Monitoring Panel
2	Configure Event Source Monitoring Panel to receive notification

Event Source Monitoring Panel

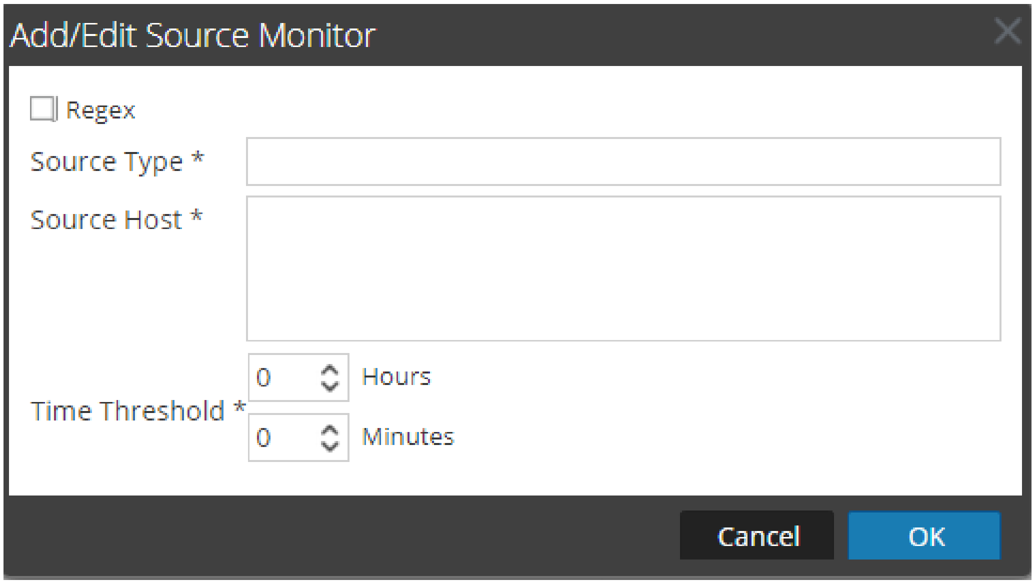
Feature	Description
Configure email or distribution list.	Opens the **Administration** > **System** > **Email view** so you can adjust the email distribution for the Event Source Monitoring output, if necessary.
Configure Syslog and SNMP Trap servers.	Opens the **Administration** > **System** > **Auditing view** so you can adjust the Syslog and SNMP trap distribution for the Event Source Monitoring output, if necessary.
+	Displays the Add/Edit Source Monitor dialog in which you add or modify event sources to monitor.
−	Deletes the selected event sources from monitoring.
□	Selects an event source.

Feature	Description
Source Type	Displays the source type of the event source.
Source Host	Displays the source host of the event source.
Time Threshold	Displays the time period after which NetWitness Suite stops sending notifications (Time Threshold).
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancels any additions, deletion, or changes.

Decommission Panel

Feature	Description
+	Displays the Decommission dialog in which you add or modify event sources to decommission.
−	Deletes the selected event sources from decommissioning.
□	Selects an event source.
Regex	Displays if you choose to use regular expressions
Source Type	Displays the source type of the decommissioned event source.
Source Host	Displays the source host of the decommissioned event source.
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancels any additions, deletions, or changes.

Add/Edit Source Monitor Dialog


Add/Edit Source Monitor

☐ Regex

Source Type *

Source Host *

Time Threshold * 0 Hours 0 Minutes

In **Add/Edit Source Monitor** dialog, you add or modify the the event sources that you want to monitor. The two parameters that identify an event source are **Source Type** and **Source Host**. You can use **globbing** (pattern matching and wildcard characters) to specify the Source Type and Source Host of event sources as shown in the following example:

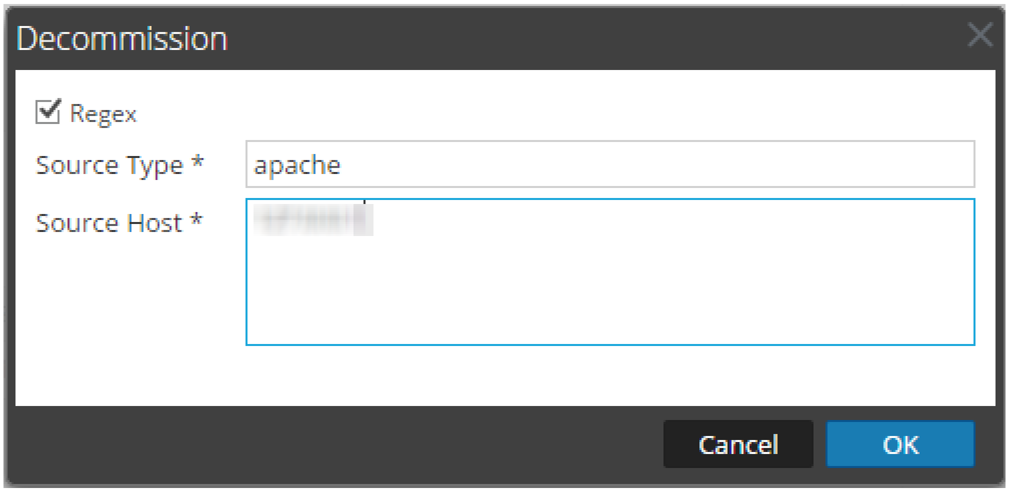
<table>
<tr><th>Source Type</th><th>Source Host</th></tr>
<tr><td>ciscopix</td><td>1.1.1.1</td></tr>
<tr><td>*</td><td>1.1.1.1</td></tr>
<tr><td>*</td><td>*</td></tr>
<tr><td>*</td><td>1.1.1.1|1.1.1.2</td></tr>
<tr><td>*</td><td>1.1.1.[1|2]</td></tr>
<tr><td>*</td><td>1.1.1.[123]</td></tr>
<tr><td>*</td><td>1.1.1.[0-9]</td></tr>
<tr><td>*</td><td>1.1.1.11[0-5]</td></tr>
<tr><td>*</td><td>1.1.1.1,1.1.1.2</td></tr>
<tr><td>*</td><td>1.1.1.[0-9]|1.1.1.11[0-5]</td></tr>
</table>

Source Type	Source Host
*	**1.1.1.[0-9]|1.1.1.11[0-5],10.31.204.20**
*	**1.1.1.***
*	**1.1.1.[0-9]{1,3}**

Features

Feature	Description
Regex	Select the checkbox if you want to use regular expressions
Source Type	The source type of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view.
Source Host	Hostname or IP address of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector device > **View** > **Config** view.
Time Threshold	The time period after which NetWitness Suite starts sending notifications.
Cancel	Closes the dialog without adding the event source, or changes to the event source, to the Event Source Monitoring panel.
OK	Adds the event source to the Event Source Monitoring panel.

Decommission Dialog



Decommission

☑ Regex

Source Type * apache

Source Host * [redacted]

Feature	Description
Source Type	The source type of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector device > **View** > **Config** view.
Source Host	Hostname or IP address of the event source. You must use the value that you configured for the event source in the **Event Sources** tab of the **Administration** > **Services** > Log Collector service > **View** > **Config** view.
Cancel	Closes the dialog without applying any event source additions, deletions, or changes to the Decommissioning panel.
OK	Applies any event source additions, deletions, or changes to the Decommissioning panel.

Health and Wellness Settings View - Warehouse Connector

Note: To monitor Archiver and Warehouse Connector, see "Health Policy".

Configuring the Warehouse Connector monitoring enables you to automatically generate notification when critical thresholds concerning Warehouse Connector and storage have been met.

Access the Warehouse Connector Monitoring view

1. Go to **Admin** > **Health & Wellness**.
2. Select **Settings** > **Warehouse Connector**.

What do you want to do?

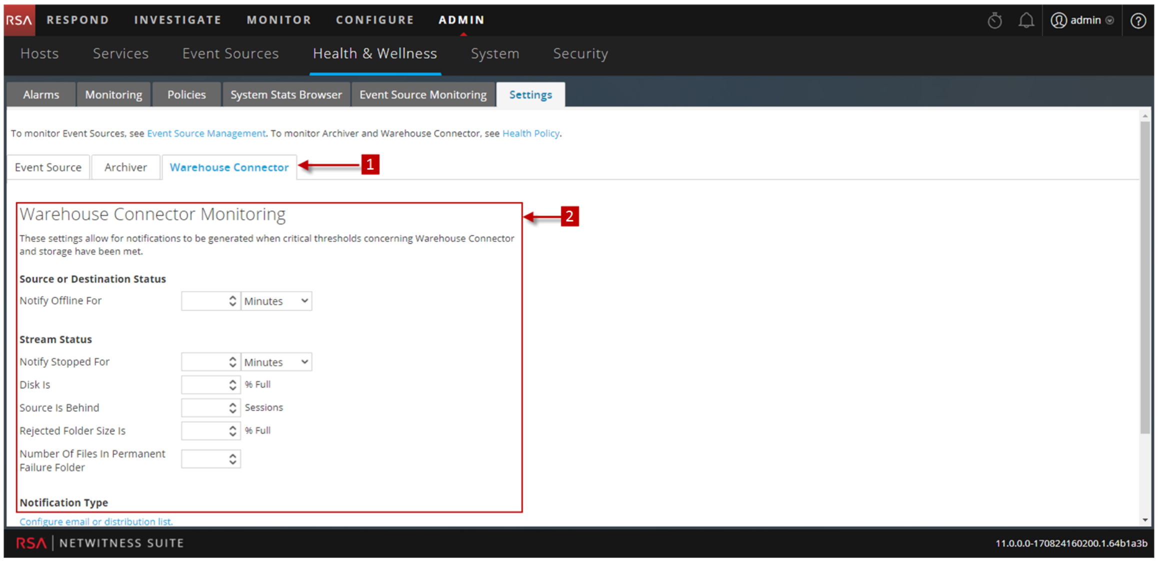
Role	I want to ...	Show me how
Administrator	View the details of Warehouse connector	Warehouse Connector Details View

Related topics

Monitor Service Details

Quick Look

The Warehouse Connector Monitoring view is displayed.



To monitor Event Sources, see Event Source Management. To monitor Archiver and Warehouse Connector, see Health Policy.

Warehouse Connector Monitoring

These settings allow for notifications to be generated when critical thresholds concerning Warehouse Connector and storage have been met.

Source or Destination Status

Notify Offline For — Minutes

Stream Status

Notify Stopped For — Minutes

Disk Is — % Full

Source Is Behind — Sessions

Rejected Folder Size Is — % Full

Number Of Files In Permanent Failure Folder

Notification Type

Configure email or distribution list.

1	Displays Warehouse Connector Monitoring view Panel
2	Allows to configure Warehouse Connector Monitoring parameters

Warehouse Connector Monitoring parameters

The following table lists the parameters required to configure the Warehouse Connector to automatically generate notification when critical thresholds are reached.

Parameter	Value	Description
Source or Destination Status	Notify Offline For	Number of minutes or hours after which the you will receive a notification if the source or destination connection fails.
Stream Status	Notify Stopped For	Number of minutes or hours after which you would like to receive a notification when the Stream goes offline.
	Disk Is	The limit on the percentage of disk usage after which you would like to receive a notification.
	Source Is Behind	Number of sessions after which a notification is raised if the source goes behind the defined number of sessions.
	Rejected Folder Size Is	Limit on the percentage of folder usage after which you would like to receive a notification.
	Number Of Files in Permanent Failure Folder	Limit on the number of files in the permanent failure folder after which you would like to receive a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness Suite.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.

Parameter	Value	Description
	NW Console, Email, Syslog Notification, SNMP Trap Notification	Enable NW Console to get notifications on the NetWitness Suite UI notification toolbar. Enable Email to get email notifications. Enable Syslog Notification to generate syslog events. Enable SNMP Trap Notification to get audit events as SNMP traps.

Monitoring View

NetWitness Suite provides detailed statistics and other information about the host and the individual NetWitness Suite services on Details views. You can view the current health of all the hosts, services running on the hosts, various aspects of the hosts' health, host details and service details in the Monitoring view.

To access this view:

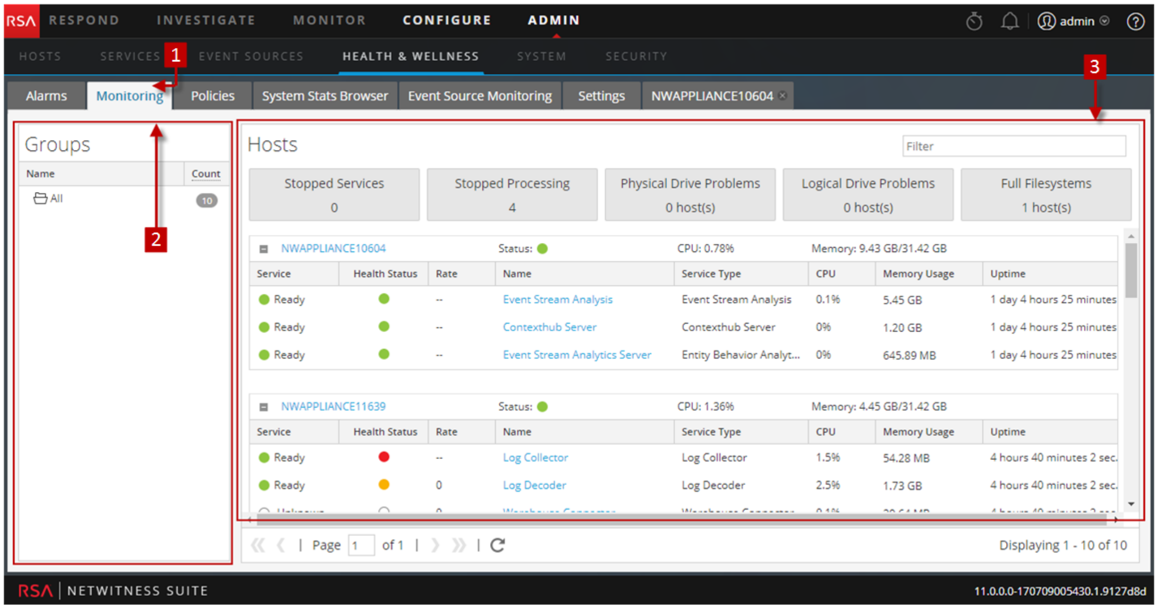
1. Go to **ADMIN > Health & Wellness**.
2. Click the **Monitoring** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View and Perform Procedures	Monitor Hosts and Services

Quick Look

The Monitoring view is displayed.



Stopped Services	Stopped Processing	Physical Drive Problems	Logical Drive Problems	Full Filesystems
0	4	0 host(s)	0 host(s)	1 host(s)

NWAPPLIANCE10604 Status: ● CPU: 0.78% Memory: 9.43 GB/31.42 GB

Service	Health Status	Rate	Name	Service Type	CPU	Memory Usage	Uptime
● Ready	●	--	Event Stream Analysis	Event Stream Analysis	0.1%	5.45 GB	1 day 4 hours 25 minutes
● Ready	●	--	Contexthub Server	Contexthub Server	0%	1.20 GB	1 day 4 hours 25 minutes
● Ready	●	--	Event Stream Analytics Server	Entity Behavior Analyt...	0%	645.89 MB	1 day 4 hours 25 minutes

NWAPPLIANCE11639 Status: ● CPU: 1.36% Memory: 4.45 GB/31.42 GB

Service	Health Status	Rate	Name	Service Type	CPU	Memory Usage	Uptime
● Ready	●	--	Log Collector	Log Collector	1.5%	54.28 MB	4 hours 40 minutes 2 sec.
● Ready	●	0	Log Decoder	Log Decoder	2.5%	1.73 GB	4 hours 40 minutes 2 sec.

1	Displays Monitoring tab.
2	Group Panel to select a Group.
3	Hosts panel displays operational statistics.

Groups Panel

The Groups panel lists all the groups of hosts available. When you select a group, the associated content is displayed in the Hosts panel.

Note: If the total host **Count** in the **Groups** panel is lower than the actual number of hosts displayed in the **Hosts** panel, please refer to the Troubleshooting Health & Wellness topic for possible causes of this issue and recommended solutions.

Hosts Panel

The Hosts panel displays operational statistics for hosts and the services running on each host.

Parameter	Description
Filter	Type a host name or a service name in the Filter field to display the corresponding hosts and services in the Host panel.
Stopped Services	Click **Stopped Services** to display a list of all stopped services. It also displays the host on which the service is installed.
Stopped Processing	Click **Stopped Processing** to display a list of all the hosts that have services installed on them that are in the stopped processing status.
Physical drive Problems <#> host(s)	Click to view the hosts that have physical drive problems.
Logical Drive Problems <#> host(s)	Click to view the hosts that have logical drive problems.
Full Filesystems <#> host(s)	Click to view the hosts that have full file systems.

Note: The summary information in the boxes at the top displays the System Statistics for all the hosts configured in NetWitness Suite and does not change with host of filters on groups.

The top panel is followed by a list of hosts, the services installed on them and information regarding the hosts and services.

Parameter	Description
Host Name	Displays the host name. If a host has services installed you will see a ⊞ prefixed to the host name. Click ⊞ to view all the services installed on the host.
Status	Displays the status of the Host. 🟢 - denotes that the host is active and running. 🔴 - denotes that the host is stopped or yet to start processing.
CPU	Displays the current CPU usage of the host.
Memory	Displays the Memory used by the host.

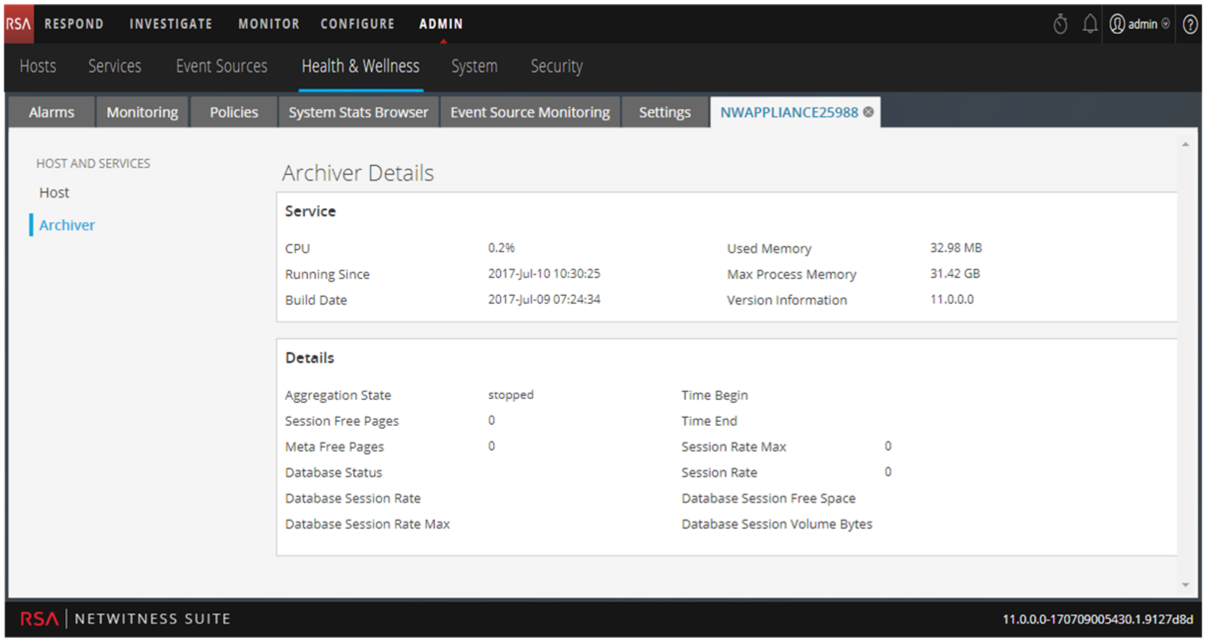
When you click ⊞ prefixed to the host name, a list of all the services installed on the host is displayed. The table below describes various parameters displayed for a service and their description.

Parameter	Description
Service	Displays the status of the service. 🟢 Ready - denotes that the service is active and running. 🔴 Stopped - denotes that the service is stopped or yet to start processing.
Health Status	Displays the processing status of the Service. 🟢 - denotes that the process is running and the data is being processed at a rate greater than zero. 🔴 - denotes that the processing is stopped. 🟠 - denotes that the processing is turned on but the data is not being processed.
Rate	Denotes the rate at which the data is being processed.
Name	Name of the service.

Parameter	Description
Service Type	Name of the type of service.
CPU	Displays the current CPU usage of the service.
Memory Usage	Displays the Memory used by the service.
Uptime	Displays the time for which the service has been running.

Archiver Details View

The Archiver Details view provides information about the Archiver. The following figure depicts the Archiver Details.



Archiver Details

Service

CPU	0.2%	Used Memory	32.98 MB
Running Since	2017-Jul-10 10:30:25	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:24:34	Version Information	11.0.0.0

Details

Aggregation State	stopped	Time Begin	
Session Free Pages	0	Time End	
Meta Free Pages	0	Session Rate Max	0
Database Status		Session Rate	0
Database Session Rate		Database Session Free Space	
Database Session Rate Max		Database Session Volume Bytes	

For the related procedure, see Monitor Service Details

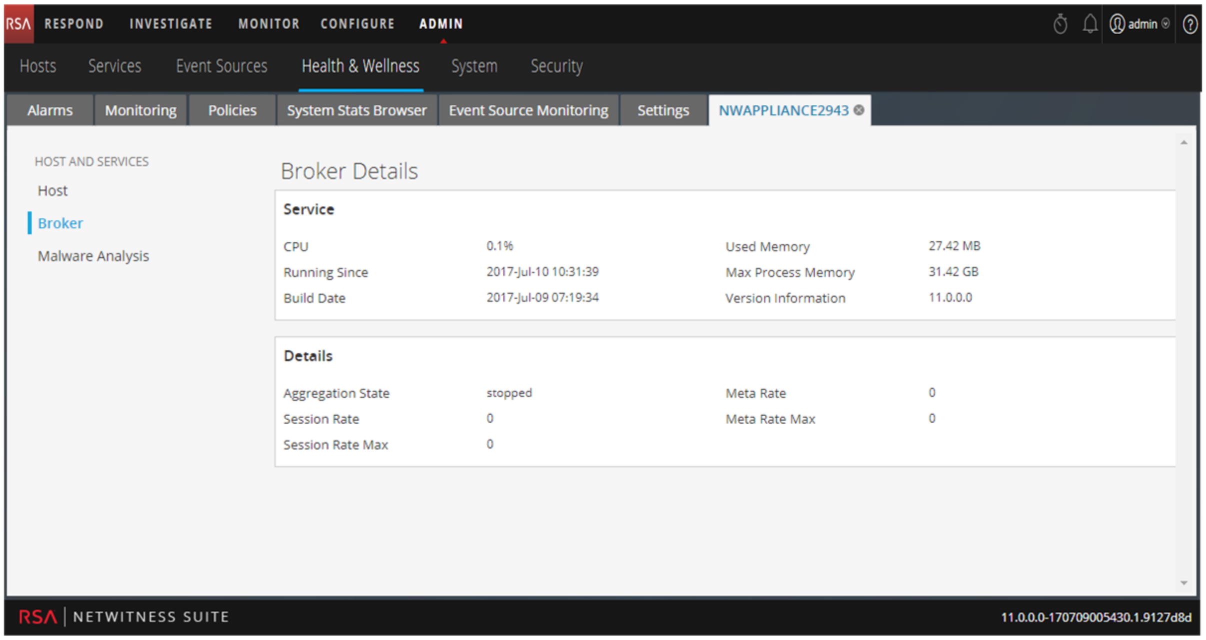
This section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Time Begin	Time (UTC) when the first session was tracked by the index.
Session Free Pages	Session pages available for aggregation.
Time End	Time (UTC) when the last session was tracked by the index.
Meta Free Pages	Pages available for aggregation.
Session Rate Max	Maximum sessions per second rate.

Statistic	Description
Database Status	Status of databases. Valid values are: • **closed** - not available for QUERY and UPDATE (databases are being initialized). This value is seldom seen. • **opened** - available for QUERY and UPDATE. • **failure** - failed to open. This can happen for any number of reasons. You can check this if CAPTURE fails to start or if queries fail to return data. This is normally caused by database corruption.
Session Rate	Sessions per second rate.
Database Session Rate	Per second rate at which the service is writing sessions to the database.
Database Session Free Space	Amount of session free space available for aggregation.
Database Session Rate Max	Maximum per second rate at which the service is writing sessions to the database.
Database Session Volume Bytes	Number of session bytes in the database.

Broker Details View

The Broker Details view provides information for the Broker. The following figure depicts the Broker Details.



Broker Details

Service

CPU	0.1%	Used Memory	27.42 MB
Running Since	2017-Jul-10 10:31:39	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:19:34	Version Information	11.0.0.0

Details

Aggregation State	stopped	Meta Rate	0
Session Rate	0	Meta Rate Max	0
Session Rate Max	0		

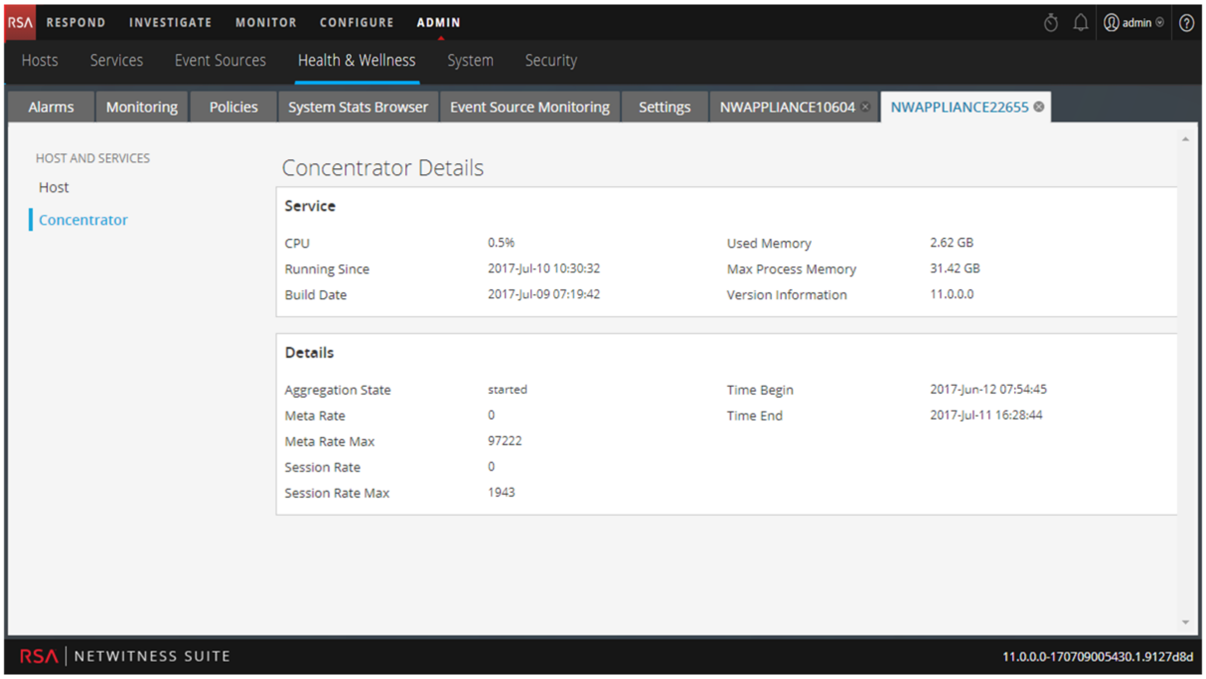
For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Meta Rate	Metadata objects per second rate.
Session Rate	Sessions per second rate.
Meta Rate Max	Maximum metadata objects per second rate.
Session Rate Max	Maximum sessions per second rate.

Concentrator Details View

The Concentrator Details view provides information for the Concentrator. The following figure depicts the Concentrator Details.



Concentrator Details

Service

CPU	0.5%	Used Memory	2.62 GB
Running Since	2017-Jul-10 10:30:32	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:19:42	Version Information	11.0.0.0

Details

Aggregation State	started	Time Begin	2017-Jun-12 07:54:45
Meta Rate	0	Time End	2017-Jul-11 16:28:44
Meta Rate Max	97222		
Session Rate	0		
Session Rate Max	1943		

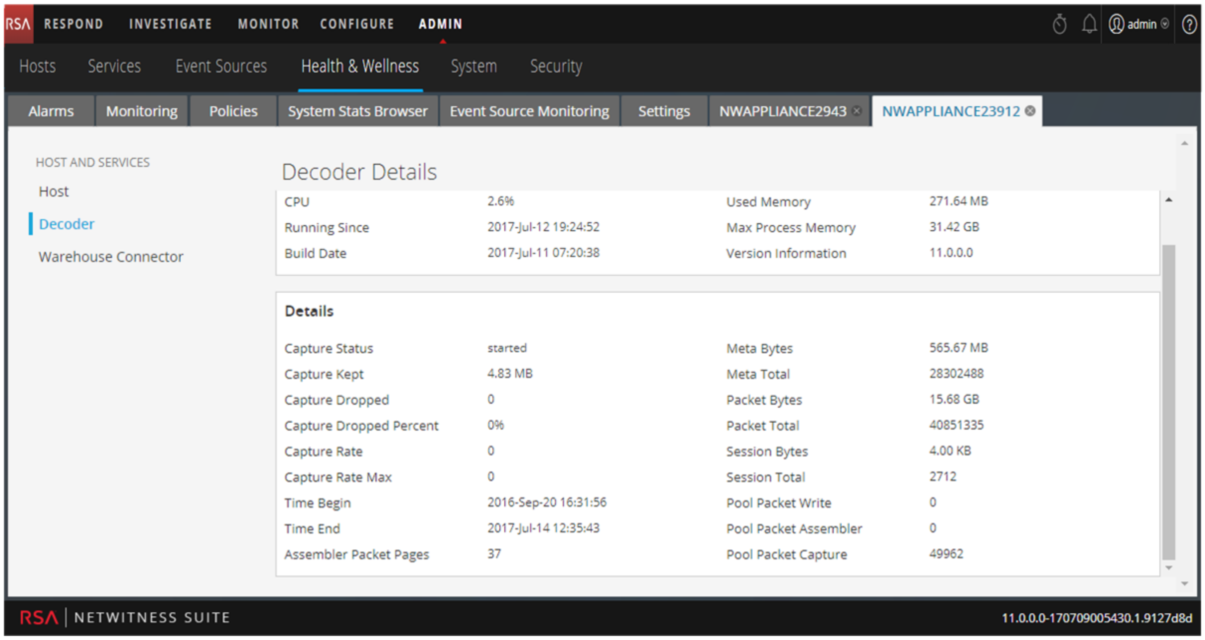
For the related procedure, see Monitor Service Details

The section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.
Time Begin	Time (UTC) when the first session was tracked by the index.
Meta Rate	Metadata objects per second rate.
Time End	Time (UTC) when the last session was tracked by the index.
Meta Rate Max	Maximum metadata objects per second rate.
Session Rate	Sessions per second rate.
Session Rate Max	Maximum sessions per second rate.

Decoder Details View

The Decoder Details view provides information for the Decoder. The following figure depicts the Decoder Details.



Decoder Details

CPU	2.6%	Used Memory	271.64 MB
Running Since	2017-Jul-12 19:24:52	Max Process Memory	31.42 GB
Build Date	2017-Jul-11 07:20:38	Version Information	11.0.0.0

Details

Capture Status	started	Meta Bytes	565.67 MB
Capture Kept	4.83 MB	Meta Total	28302488
Capture Dropped	0	Packet Bytes	15.68 GB
Capture Dropped Percent	0%	Packet Total	40851335
Capture Rate	0	Session Bytes	4.00 KB
Capture Rate Max	0	Session Total	2712
Time Begin	2016-Sep-20 16:31:56	Pool Packet Write	0
Time End	2017-Jul-14 12:35:43	Pool Packet Assembler	0
Assembler Packet Pages	37	Pool Packet Capture	49962

For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

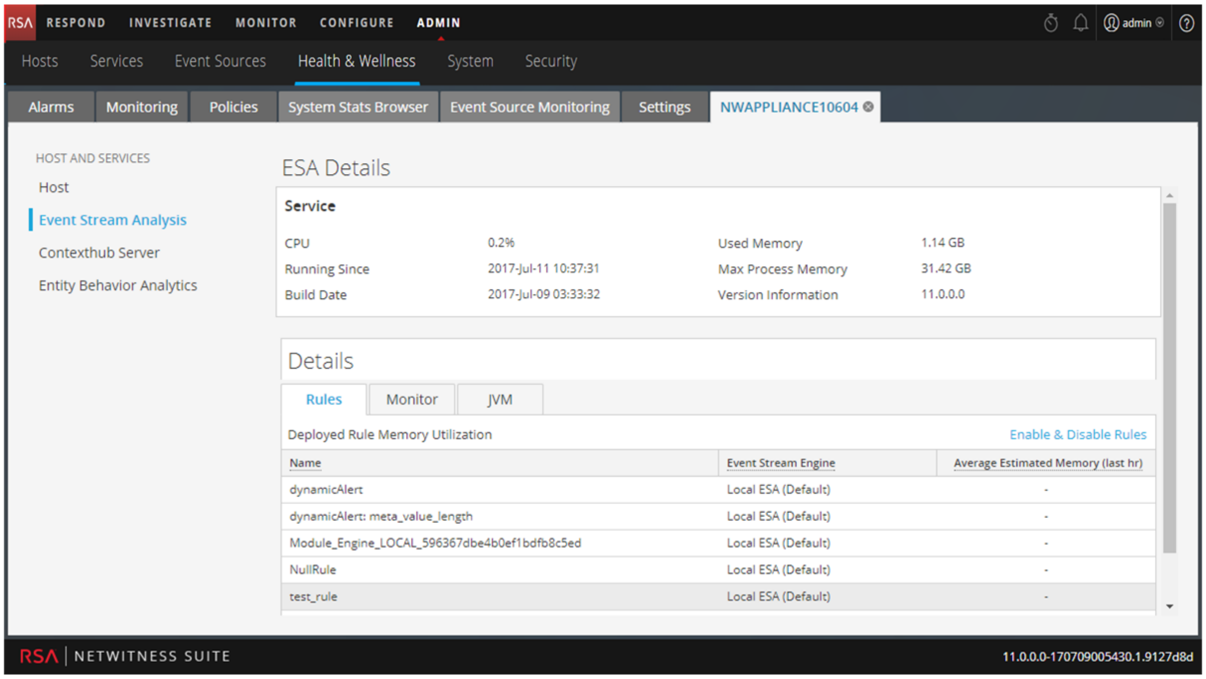
Statistic	Description
Capture Status	Status of data capture. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started**- Capturing data. • **stopping**- Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Decoder service.
Meta Bytes	Number of meta bytes in the database.
Capture Kept	Number of packets kept during capture.

Statistic	Description
Meta Total	Number of metadata in the database.
Capture Dropped	Number of packets reported by the network card as dropped. After the service stops capturing data, rate is reset to zero.
Packet Bytes	Number of packet bytes in the database.
Capture Dropped Percent	Packets reported by the network card as dropped as a percentage.
Packet Total	Number of packet objects held in the packet database. The total decreases when the database rolls files off due to size constraints. After the service stops capturing data, the number is not reset.
Capture Rate	Megabits per second rate at which the service is capturing data. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, rate is reset to zero.
Session Bytes	Number of session bytes in the database.
Capture Rate Max	Maximum megabits per second rate at which the service is capturing data. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate during data capture.
Session Total	Number of sessions held in the session database. This value shrinks when the database rolls files off due to size constraints. After the service stops capturing data, the number is not reset.
Time Begin	Time when first packet was captured (time when the first packet was stored in the packet database). This time increases as packets are rolled out of the packet database.

Statistic	Description
Pool Packet Write	Number of packet pages currently in the PCS pipeline that need to be written to the database.
Time End	Time when the last packet was captured (time when packet was written to the database). The time increases as new packets are captured.
Pool Packet Assembler	Number of packet pages waiting to be assembled.
Assembler Packet Pages	Number of packet pages waiting to be assembled.
Pool Packet Capture	Number of packet pages available for capture.

Event Steam Analysis (ESA) Details View

The Event Stream Analysis Details view provides information for ESA. The following figure depicts the Event Stream Analysis Details.



ESA Details

Service

CPU	0.2%	Used Memory	1.14 GB
Running Since	2017-Jul-11 10:37:31	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 03:33:32	Version Information	11.0.0.0

Details

Deployed Rule Memory Utilization

Name	Event Stream Engine	Average Estimated Memory (last hr)
dynamicAlert	Local ESA (Default)	-
dynamicAlert: meta_value_length	Local ESA (Default)	-
Module_Engine_LOCAL_596367dbe4b0ef1bdfb8c5ed	Local ESA (Default)	-
NullRule	Local ESA (Default)	-
test_rule	Local ESA (Default)	-

11.0.0.0-170709005430.1.9127d8d

For the related procedure, see Monitor Service Details.

This section displays the current generic statistics and Rule information for the service. It consists of **Rules**, **Monitor**, and Java Virtual Machine (**JVM**) tabs that show Event Stream Analysis rules and additional statistics.

Monitor tab

Displays the following generic statistical information for the Event Stream Analysis service:

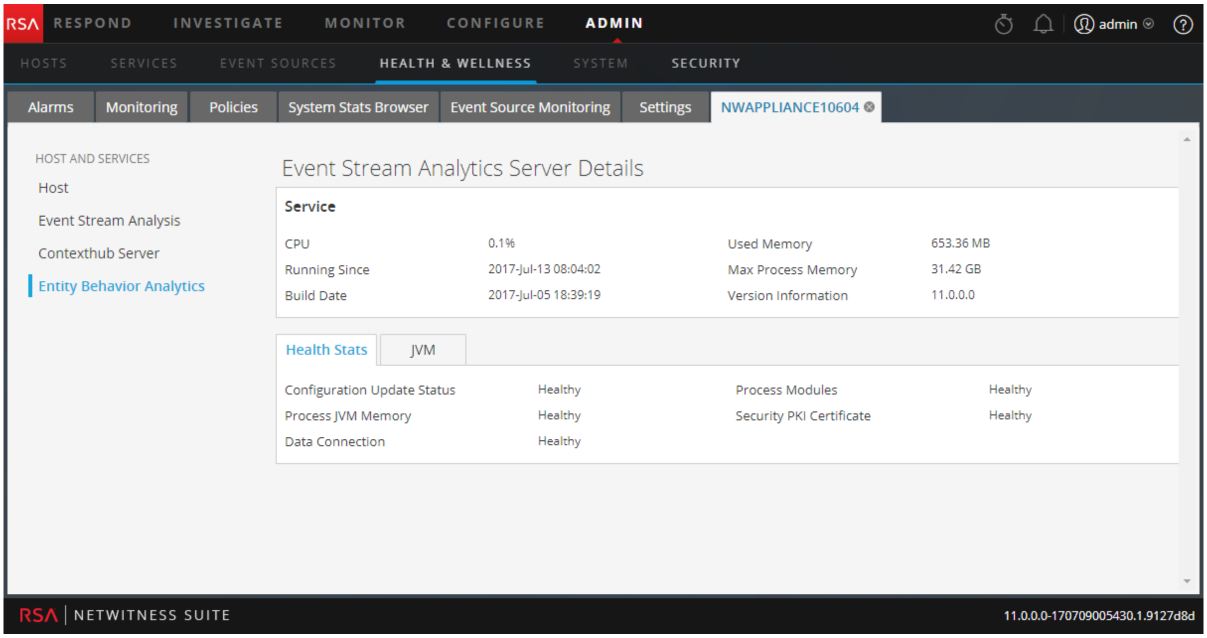
- Average number of bytes received per event message field.
- Average number of bytes received per event message.
- Total number of bytes of bytes received.
- Total number of fields received.
- Number of rules deployed on the ESA Service. The Sum of Enabled rules and Disabled rules should equal to Deployed
- Total number of events matched to all rules on the ESA service.
- Total number of events analyzed by the ESA Service since the last service start.
- Total number of alerts fired based on all the rules on the ESA service.
- Total dropped as late.
- Total fed on time.

- Total exit early.
- Seconds between feeds.
- Time span in window.
- Total events in window.
- Percent window consumed.
- Total source work units.
- Total bus dropped by payload.
- Total bus dropped events.
- Total bus dropped by fields.
- Total number of alerts sent to the message bus.
- Total number of bus events.
- Total number of Bus work units.
- Total endpoints detected.
- Total lost endpoints.
- Total failed client count.
- Total successful client count.
- Total successful server count.
- Minutes since last success.
- Number of times proxy was requested and granted.
- Total successful requests.
- Number of times proxy was requested and not granted.
- Total unsuccessful requests.

ESA Analytics Details View

The ESA Analytics Details view provides health status information about the selected ESA Analytics service. ESA Analytics services process the data for automated threat detection. It is important that you address any checked item that shows a status other than green (healthy), so that data processing is not interrupted and critical events are not missed.

The following figure shows the ESA Analytics Details view.



Event Stream Analytics Server Details

Service

CPU	0.1%	Used Memory	653.36 MB
Running Since	2017-Jul-13 08:04:02	Max Process Memory	31.42 GB
Build Date	2017-Jul-05 18:39:19	Version Information	11.0.0.0

Configuration Update Status	Healthy	Process Modules	Healthy
Process JVM Memory	Healthy	Security PKI Certificate	Healthy
Data Connection	Healthy		

For the related procedure, see Monitor Service Details.

ESA Analytics Details

This section displays the current generic statistics for the selected ESA Analytics service.

Health Status

The Health Status section shows the health of the following items for the selected ESA Analytics service:

- Mongo
- JVM (Java Virtual Machine)
- Disk Space
- Suspicious Domains Module
- User Behavior Analytics Module

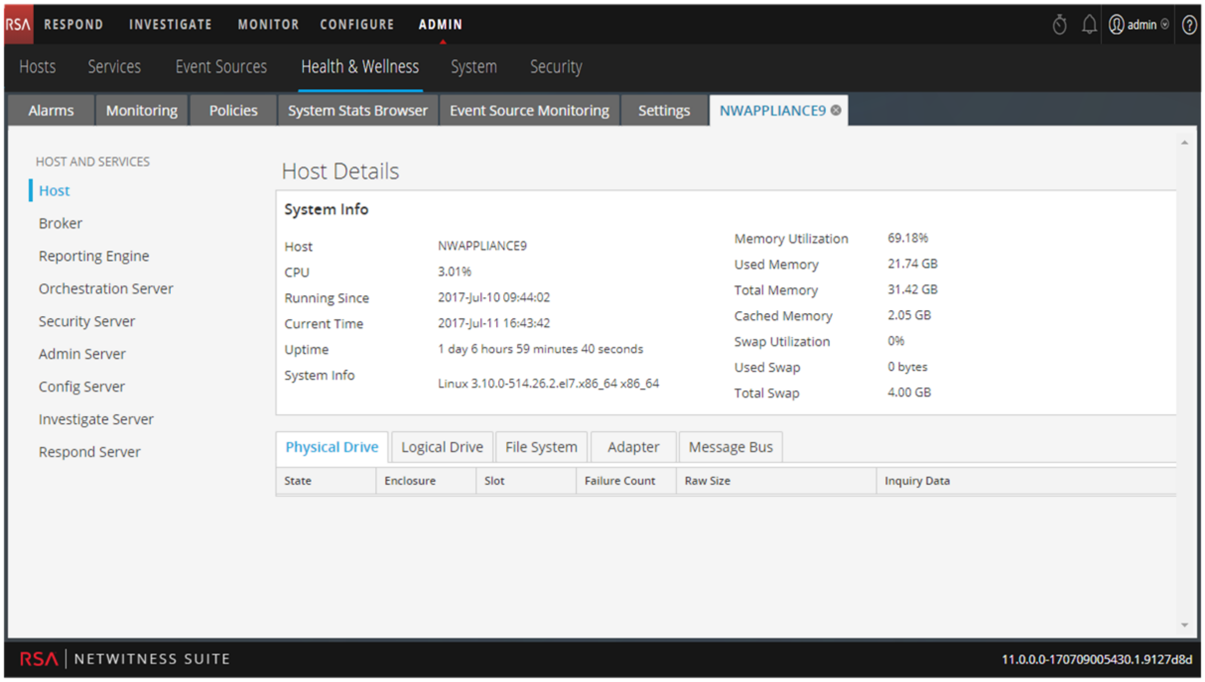
The following table describes the meaning of each health status.

Health Status	Description
Green	Healthy
Yellow	Unhealthy
Red	Critical and it needs immediate attention.

Health Status	Description
- -	Inapplicable

Host Details View

The Host Details view provides information about a host. The following figure depicts the Host Details.



Host Details

System Info

Host	NWAPPLIANCE9	Memory Utilization	69.18%
CPU	3.01%	Used Memory	21.74 GB
Running Since	2017-Jul-10 09:44:02	Total Memory	31.42 GB
Current Time	2017-Jul-11 16:43:42	Cached Memory	2.05 GB
Uptime	1 day 6 hours 59 minutes 40 seconds	Swap Utilization	0%
System Info	Linux 3.10.0-514.26.2.el7.x86_64 x86_64	Used Swap	0 bytes
		Total Swap	4.00 GB

State	Enclosure	Slot	Failure Count	Raw Size	Inquiry Data

The options panel on the left displays the host and the services installed on the host. You can click on Host any service to view the statistics and other pertinent information for that host or service.

The Details panel displays information that is specific to the host and provides additional information regarding the hardware of the host.

For the related procedure, see .Monitor Service Details

This section displays the current performance, capacity, and historical statistics for the host.

Parameter	Description
Host	Hostname.
CPU	Current CPU usage of the host.
Running Since	Time when the host was started.

Parameter	Description
Current Time	Current time on the host
Uptime	Time for which the host has been active.
System Info	OS version installed on the host.
Memory Utilization	Percentage of memory utilized by the host.
Used Memory	Memory used in GB.
Total Memory	Capacity of the memory installed on the system.
Cached Memory	Memory that is cached to disk in GB.
Swap Utilization	Percentage of system swap in use.
Used Swap	Swap used in GB.
Total Swap	Capacity of the swap installed on the system.

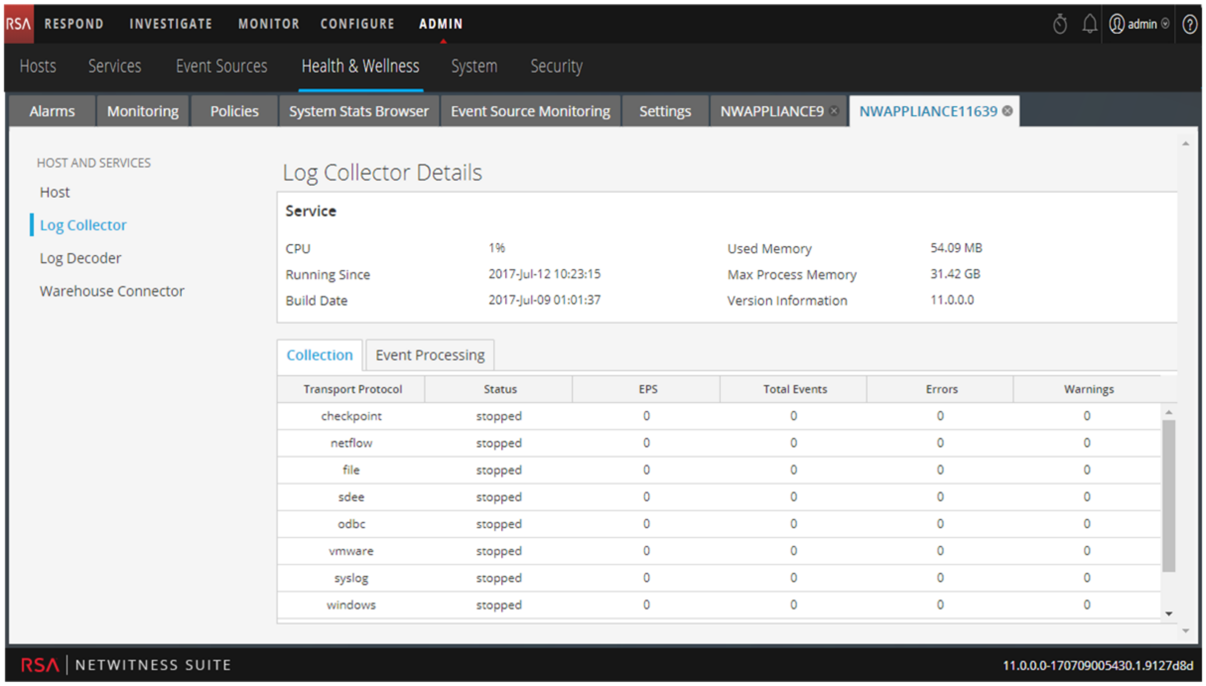
The lower section displays the current generic statistics for the host in the tabs described in the following table.

Tab	Description
Physical Drive	Type of physical drive, its usage and additional information of the physical drive on the host.
Logical Drive	Logical drive on the host.
File System	File system information, the size, current usage and available capacity on the host.
Adapter	Adapter used on the host.

Tab	Description
Message Bus	**Publish In Rate** - rate at which incoming messages are published to the message bus queue. **Total Messages Queued** - number of messages in the message queue. **Memory Used** - amount of memory used by the message bus (in bytes). **Disk Free** - free disk space available for the message bus (in bytes). **Memory Limit** - system memory limit. If the memory usage exceeds this value, this trips the **Memory Alarm** and Security Analytics stops accepting messages. **Disk Free Limit** - limit of free disk space available for the message bus. If the available disk space falls below this value, this trips the **Disk Free Alarm** and Security Analytics stops accepting messages. **Memory Limit Available** - Amount of memory available to this message broker (in bytes) before the **Memory Used Alarm** is tripped. **Disk Limit Available** - Amount of free disk space available to this message broker (in bytes) before the **Disk Free Limit** alarm is tripped. **Disk Free Alarm** - **True** or **False**. **True** indicates that the available disk space is below the value set in **Disk Free Limit** and Security Analytics has stopped accepting messages. **Memory Alarm** - **True** or **False**. **True** indicates that the available memory is below the value set in **Memory Limit** and Security Analytics has stopped accepting messages.

Log Collector Details View

The Log Collector Details view provides information for the Log Collector. The following figure depicts the Log Collector Details.



Log Collector Details

Service

CPU	1%	Used Memory	54.09 MB
Running Since	2017-Jul-12 10:23:15	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 01:01:37	Version Information	11.0.0.0

Transport Protocol	Status	EPS	Total Events	Errors	Warnings
checkpoint	stopped	0	0	0	0
netflow	stopped	0	0	0	0
file	stopped	0	0	0	0
sdee	stopped	0	0	0	0
odbc	stopped	0	0	0	0
vmware	stopped	0	0	0	0
syslog	stopped	0	0	0	0
windows	stopped	0	0	0	0

For the related procedure, see Monitor Service Details.

The lower section consists of the **Collection** and **Event Processing** tabs that display generic statistics for the service.

Collection Tab

Displays the event collection statistics for each Log Collection protocol you have implemented in NetWitness Suite (see "Log Collection Getting Started Guide" in the ***Log Collection Guides***).

Event Processing Tab

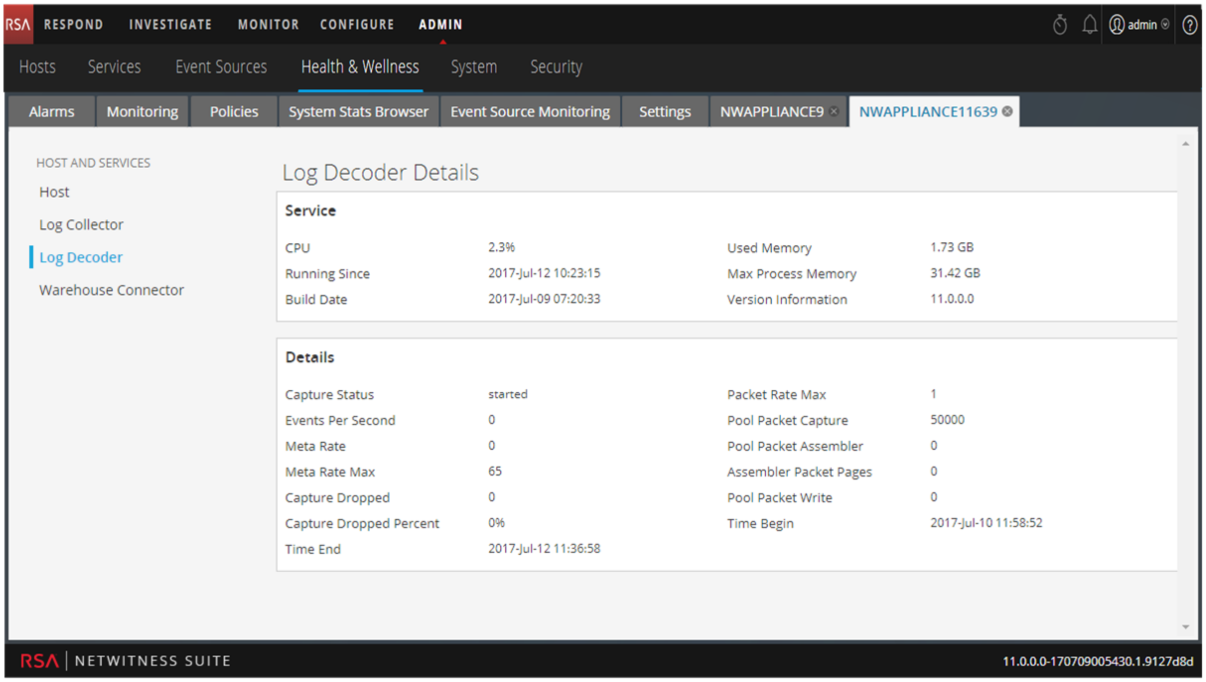
Displays statistics for the NetWitness Suite internal event processing protocol (that is, the Log Decoder) for Log Collection.

Parameter	Description
Transport Protocol	NetWitness Suite protocol use for Log Collections (that is, the Log Decoder).

Parameter	Description
Status	Status of the Log Decoder. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started** - Capturing data. • **stopping**- Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Decoder service.
EPS	Rate (events per second) at which this the Log Decoder is processing events from the Log Collector.
Total Events	Total events processed by the Log Decoder.
Errors	Number of errors encountered.
Warnings	Number of warnings encountered.
Byte Rate	Current throughput in bytes per second.

Log Decoder Details View

The Log Decoder Details view provides information for the Log Decoder. The following figure depicts the Log Decoder Details.



Log Decoder Details

Service

CPU	2.3%	Used Memory	1.73 GB
Running Since	2017-Jul-12 10:23:15	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:20:33	Version Information	11.0.0.0

Details

Capture Status	started	Packet Rate Max	1
Events Per Second	0	Pool Packet Capture	50000
Meta Rate	0	Pool Packet Assembler	0
Meta Rate Max	65	Assembler Packet Pages	0
Capture Dropped	0	Pool Packet Write	0
Capture Dropped Percent	0%	Time Begin	2017-Jul-10 11:58:52
Time End	2017-Jul-12 11:36:58		

For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

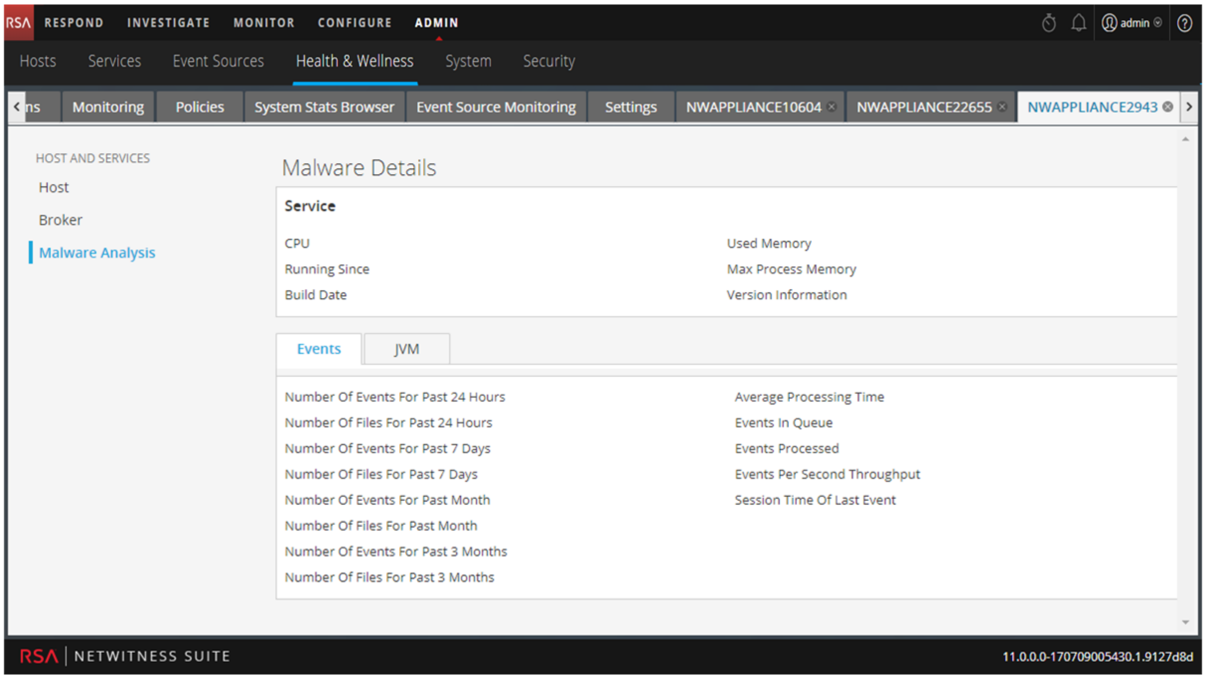
Statistic	Description
Capture Status	Status of data capture. Valid values are: • **starting** - Starting data capture (not capturing data yet). • **started** - Capturing data. • **stopping** - Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • **stopped** - Not capturing data. • **disabled** - Not configured as a Log Decoder service.
Packet Rate Max	Maximum per second rate at which the service is writing packets to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate during data capture.
Events Per Second	Rate (events per second) at which the Log Decoder is processing events from the Log Collector.

Statistic	Description
Pool Packet Capture	Number of packet pages available for capture.
Meta Rate	Per second rate at which the service is writing metadata objects to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, rate is reset to zero.
Pool Packet Assembler	Number of packet pages waiting to be assembled.
Meta Rate Max	Maximum per second rate at which the service is writing metadata objects to the database. Rate is a rolling average sample over a short time period (10 seconds). After the service stops capturing data, displays the maximum rate reached during data capture.
Assembler Packet Pages	Number of packet pages waiting to be assembled.
Capture Dropped	Number of packets reported by the network card as dropped. After the service stops capturing data, rate is reset to zero.
Pool Packet Write	Number of packet pages in the PCS pipeline that need to be written to the database.
Capture Dropped Percent	Packets reported by the network card as dropped as a percentage.
Time Begin	Time when first packet was captured (time when the first packet was stored in the packet database). This time increases as packets are rolled out of the packet database.

Statistic	Description
Time End	Time when the last packet was captured (time when packet was written to the database). The time increases as new packets are captured.

Malware Details View

The Malware Details view provides information for Malware Analysis. The following figure depicts the Malware Details.



Malware Details

Service

CPU
Running Since
Build Date
Used Memory
Max Process Memory
Version Information

Events | JVM

Number Of Events For Past 24 Hours
Number Of Files For Past 24 Hours
Number Of Events For Past 7 Days
Number Of Files For Past 7 Days
Number Of Events For Past Month
Number Of Files For Past Month
Number Of Events For Past 3 Months
Number Of Files For Past 3 Months
Average Processing Time
Events In Queue
Events Processed
Events Per Second Throughput
Session Time Of Last Event

For the related procedure, see Monitor Service Details.

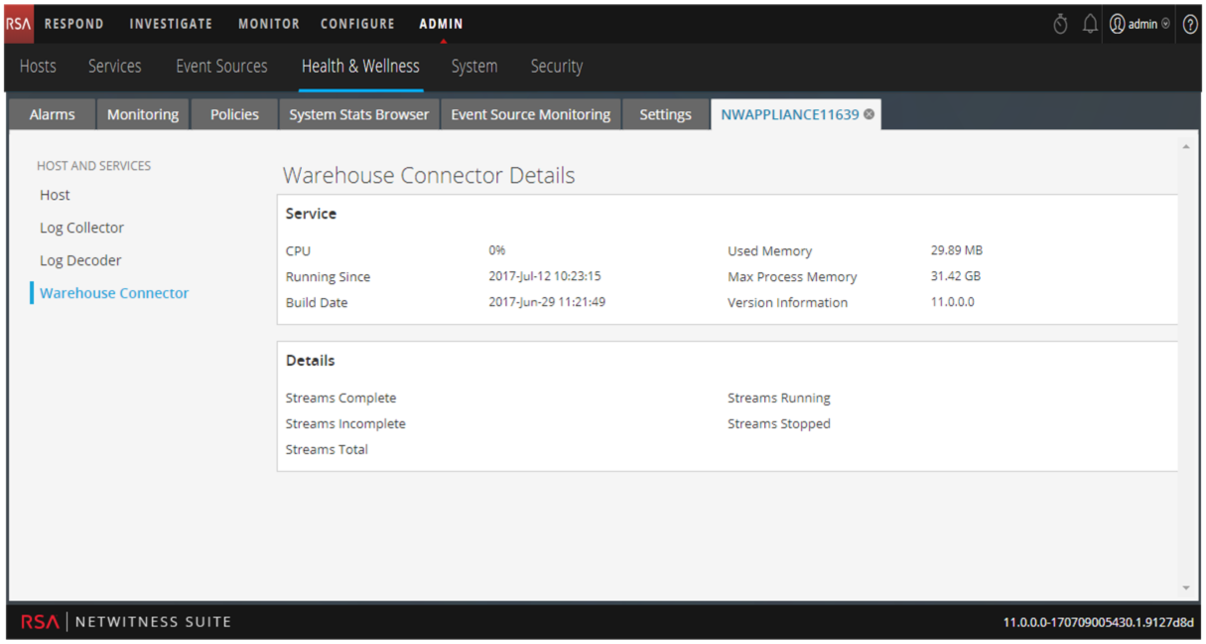
Displays the following event-related statistical information for the Malware Analysis service.

- Number of events for the past 24 hours
- Average processing time
- Number of files for the past 24 hours
- Events in queue
- Number of events for the past 7 days
- Events processed
- Number of events for the past 7 days
- Events per second throughput

- Number of events for the past month
- Session time of the last event
- Number of files for the past month
- Number of events for the past 3 months
- Number of files for the past 3 months

Warehouse Connector Details View

The Warehouse Connector Details tab provides information for the Warehouse Connector, such as the date it was built, CPU, and version information. The following figure depicts the Warehouse Connector Details.



Warehouse Connector Details

Service

CPU	0%	Used Memory	29.89 MB
Running Since	2017-Jul-12 10:23:15	Max Process Memory	31.42 GB
Build Date	2017-Jun-29 11:21:49	Version Information	11.0.0.0

Details

Streams Complete	Streams Running
Streams Incomplete	Streams Stopped
Streams Total	

For the related procedure, see Monitor Service Details.

Policies View

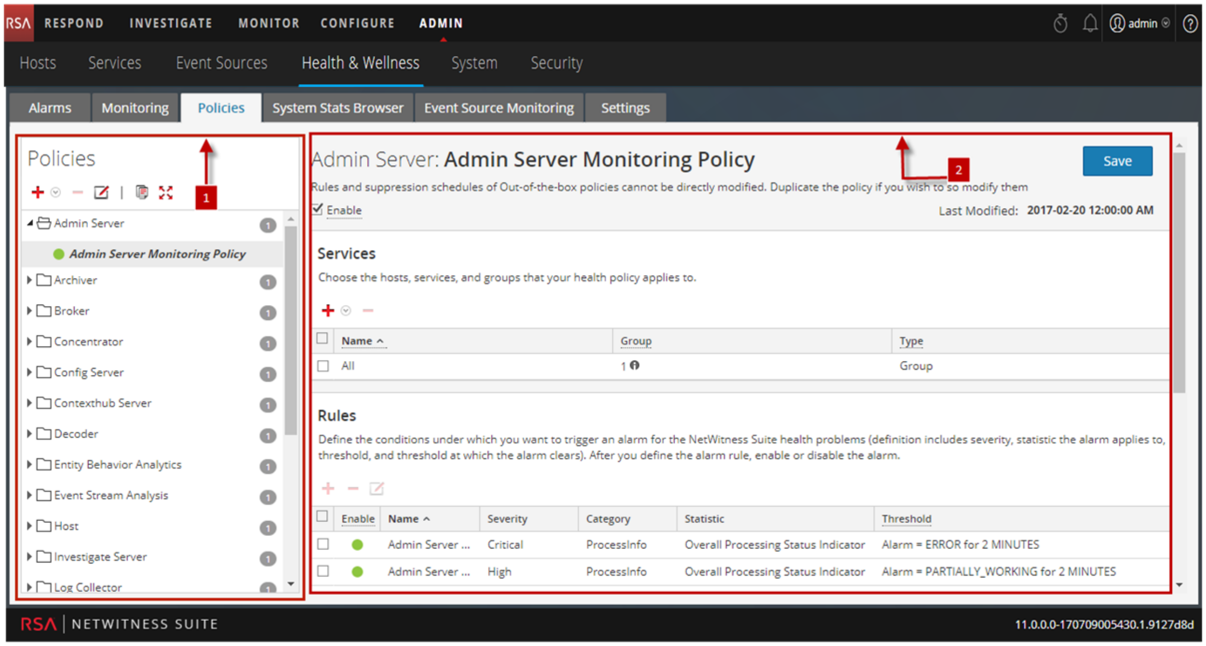
The required permission to access this view is **Manage services**.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the policies NetWitness Server and Services	Manage Policies
Administrator	Add, Edit, Duplicate, and Delete Policies	Manage Policies

Quick Look

The figure depicts the Policies view.



Admin Server: **Admin Server Monitoring Policy**

Rules and suppression schedules of Out-of-the-box policies cannot be directly modified. Duplicate the policy if you wish to so modify them

☑ Enable

Last Modified: **2017-02-20 12:00:00 AM**

Services

Choose the hosts, services, and groups that your health policy applies to.

□	Name ^	Group	Type
□	All	1	Group

Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Suite health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

□	Enable	Name ^	Severity	Category	Statistic	Threshold
□	●	Admin Server ...	Critical	ProcessInfo	Overall Processing Status Indicator	Alarm = ERROR for 2 MINUTES
□	●	Admin Server ...	High	ProcessInfo	Overall Processing Status Indicator	Alarm = PARTIALLY_WORKING for 2 MINUTES

1	Policies Panel
2	Policy Detail Panel

1. Go to **ADMIN** > **Health & Wellness**.
2. Click the **Policies** tab.

Policies Panel

In the Policies panel, you can add or delete policies for hosts and services in this panel.

Feature	Description
+ ⌄	Displays available service types to create a new policy . Select one so that you can define a policy or policies for it.
−	Deletes the selected policy from the Policies panel. You can only delete one policy at a time.
✎	Allows you to change the name of the policy.
⧉	Creates a copy of the selected policy. For example, if you select **First Policy** and click ⧉, NetWitness Suite creates a copy of this policy and names it First Policy (1).
⤢	Expands the list of policies under the services and hosts in the **Policies** panel.
⤡	Contracts the list of policies under the services and hosts in the **Policies** panel.
	List of: • Services and hosts for which you have defined policies. • RSA standard policies that you can apply to hosts and services.

Policy Detail Panel

The **Policy Detail** panel displays the policy selected from the Policies panel.

Feature	Description
Save	Saves any changes you made in this panel.
Policy Type	Displays the type of policy you selected.
Modified Date	Displays the last date this policy was modified.
□ Enable	Select and deselect this checkbox to enable and disable the policy.
Services	

Feature	Description
+ ⌄	Displays menu in which you select: • **Groups** to display the **Groups** dialog from which you select service groups to this policy. • **Service/Host** to display the **Services/Hosts** dialog from which you select services to add to this policy. If policy type is **Host**, the menu will have **Host** not **Service**. You can select services based on policy type.
−	Deletes the selected service or group from this policy.
Rules	
+	Displays the Add Rule dialog in which you define a rule for this policy.
−	Deletes the selected rule from this policy.
✎	Displays the Edit Rule dialog for the selected rule.
Policy Suppression	
+	Adds a policy suppression timeframe row.
−	Deletes the selected policy suppression timeframe row.
Time Zone	Selects the time zone for the Policy from the drop-down list. This time zone applies to both Policy Suppression and Rule Suppression.
☐	Selects the checkbox to select a policy suppression timeframe row.
Days	Days of the week that you want to suppress the policy according to the time range specified. Click on the day of the week that you want to suppress the policy. You can select any combination of days including all days.
Time Range	Time range during which the policy is suppressed for the days selected.
Notifications	

Feature	Description
+	Adds an EMAIL notification row.
−	Deletes the selected policy suppression timeframe row.
Notification Settings	Opens the Notification Servers view in which you can define the Email notification settings.
□	Selecting the checkbox selects a policy suppression time frame row.
Output	The type of notification defined on the Global Notifications page. Can be email, SNMP, Syslog, or Script.
Recipient	The name of the person receiving the notification.
Notification Server	Select the EMAIL notification server. See "Configure Notification Servers" in the *System Configuration Guide* for the source of the values in this drop-down list.
Template	Select the Template for this EMAIL notification. RSA provides the Health & Wellness Default SMTP Template and the alarms template. See" Configure Notification Templates"in the *System Configuration Guide* for the source of the other values in this drop-down list. **Note:** Refer to Include the Default Email Subject Line if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Groups dialog

Feature	Description
Groups panel	
Name	Displays the service groups you have defined. You can select: • **All** to display all your services in the **Services** panel. • A group to display the services in comprise that group in the **Services** panel.
Services panel	

Feature	Description
Name	Displays the name of the service.
Host	Displays the host on which the service is running.
Type	Displays the type of service.

Rules Dialog

Feature	Description
□ Enable	Select and deselect this checkbox to enable and disable the rule for this policy.
Name	Enter the name of the rule.
Description	Enter the description of the rule. RSA suggests that you include the following information in this field. • Informational description - purpose of the rule and what problem it monitors. • Remediation - steps to take to resolve the condition that triggers the alarm for this rule.
Severity	Select the severity of the rule. Valid values are: • Critical • High • Medium • Low

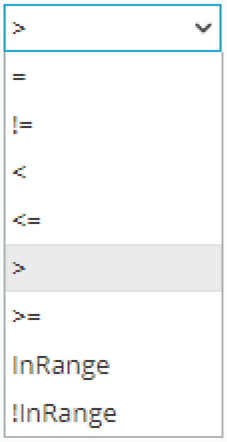
Feature	Description
Statistic	Select the statistics you want to check with this rule. You can select: - Statistical category from the left drop-down list. - Statistic from the right drop-down list. **Note:** For Public Key Infrastructure (PKI) policy, select PKI in the category and statistics as any one of the following: - NetWitness Server PKI Certificate Expiration - Displays the time left before the certificate expires. - NetWitness Server PKI CRL Expiration - Displays the time left before the Certificate Revocation List (CRL) expires. - NetWitness Server PKI CRL Status - Displays the current status of the CRL. Please refer to the System Stats Browser View for examples of the statistics you may want to check with a rule.
Alarm Threshold	Define the threshold of the rule that will trigger the policy alarm: - Amount **Note:** For CRL expiry the supported format is ddddhhmm, for example: - 10000 represent 1 day - 2359 represent 23 hours and 59 minutes - 10023 represent 1 day and 23 minutes - 3650100 represent 365 days and 1 hour - Time in minutes
Recovery	Defines when to clear the threshold of the rule: - Operator: - For NetWitness Suite 10.5 (=, !=, <, <=, >, or >=) - For NetWitness Suite 10.5.0.1 and later (See Threshold Operators below) - Amount - Time in minutes
Rule Suppression	
+	Selecting this option allows you to add a rule suppression timeframe row.

Feature	Description
−	Selecting this option allows you to delete the selected rule suppression time frame row.
□	Selecting the checkbox allows you to select a rule suppression time frame row.
Time Zone: *time-zone*	Displays the Policy time zone. You select the time zone for a policy in the Policy Suppression panel.
Days	Days of the week that you want to suppress the rule according to the time range specified. Click on the day of the week that you want to suppress the rule. You can select any combination of days including all days.
Time Range	Time range during which the rule is suppressed for the days selected.

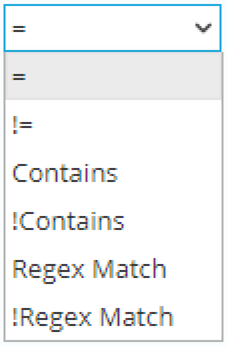
Threshold Operators

The **Alarm Threshold** and **Recovery Threshold** fields in the **Rules** dialog prompt you for either numeric or string operators based on the statistic criteria you specify.

Numeric operators drop-down menu:



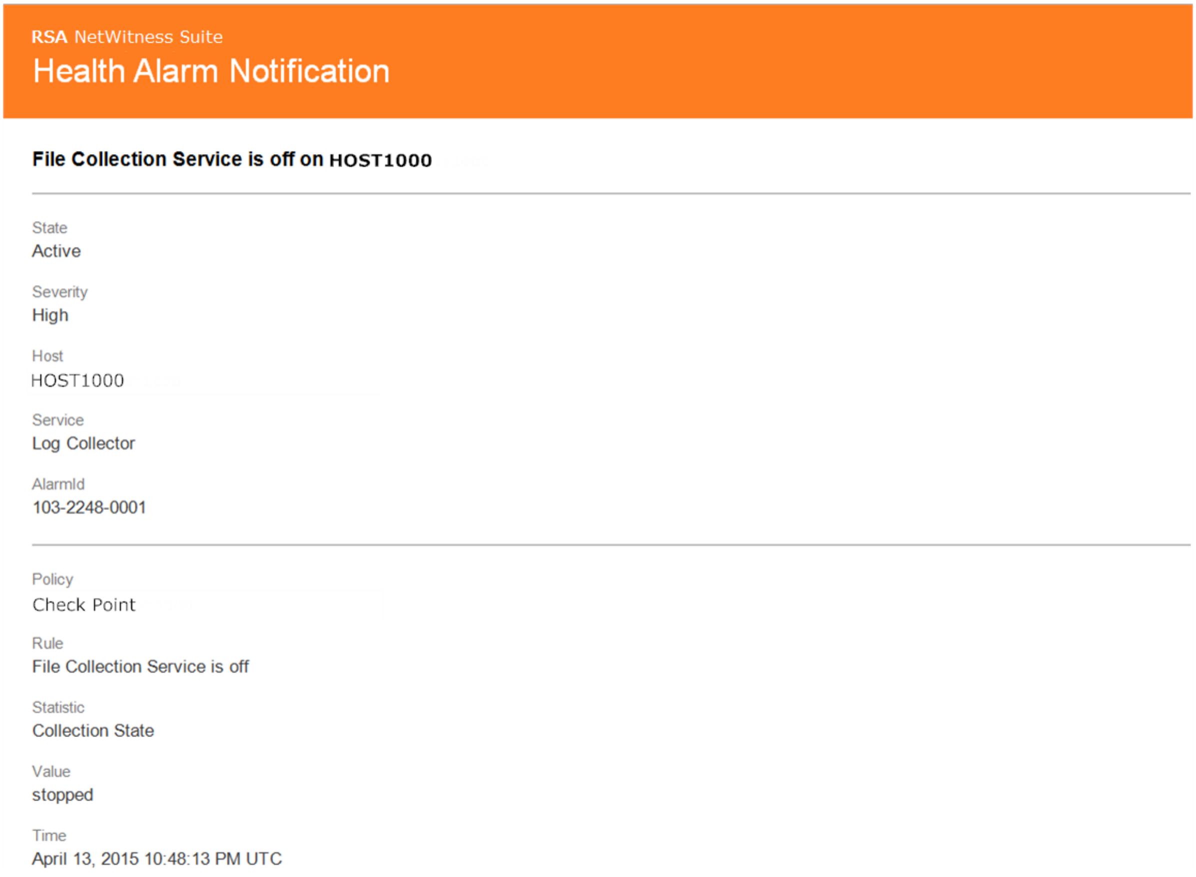
String operators drop-down menu:



RSA Health & Wellness Email Templates

> **Note:** Please refer to Include the Default Email Subject Line if you want to include the default Email subject line from the Health & Wellness template in your Health & Wellness Email notifications for specified recipients.

Health & Wellness Default SMTP Template



RSA NetWitness Suite

Health Alarm Notification

File Collection Service is off on HOST1000

State
Active

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
Check Point

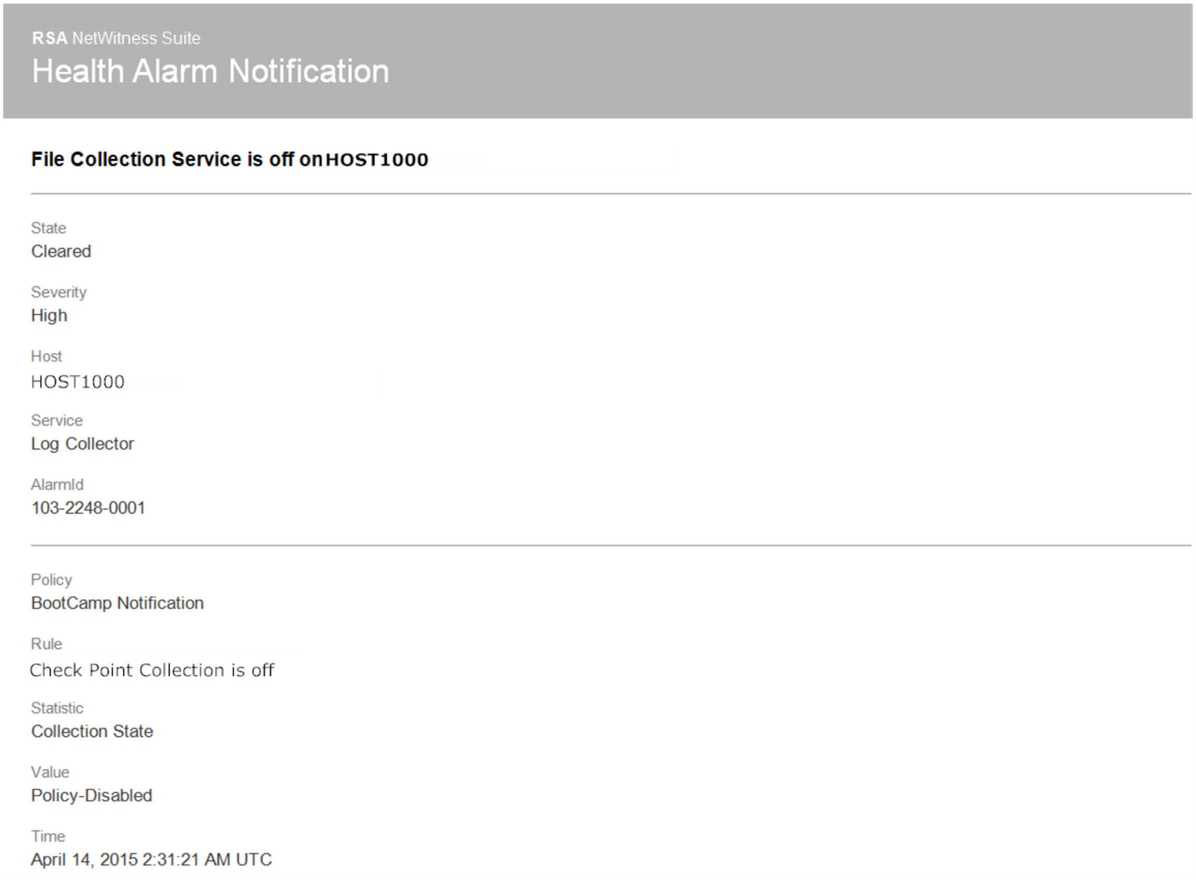
Rule
File Collection Service is off

Statistic
Collection State

Value
stopped

Time
April 13, 2015 10:48:13 PM UTC

Alarms Template



RSA NetWitness Suite

Health Alarm Notification

File Collection Service is off on HOST1000

State
Cleared

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
BootCamp Notification

Rule
Check Point Collection is off

Statistic
Collection State

Value
Policy-Disabled

Time
April 14, 2015 2:31:21 AM UTC

NetWitness Suite Out-of-the-Box Policies

The following table lists the NetWitness Suite Out-of-the-Box Policies with the rules defined for each policy.

You can perform the following tasks on any of these policies:

- Change service/group assignments.
- Disable/enable them.

You cannot perform the following tasks on any of these policies:

- Delete them.
- Edit Policy names.

Note: Additional information about the Out-of-the-Box Policies can be found in the User Interface under
Health & Wellness – Policies.

Policy Name	Rule Name	Alarm Triggered
	Communication Failure Between Master Security Analytics Host and a Remote Host	Host is down, Network is down, Message Broker is Down, or Invalid or missing security certificates for 10 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Server Monitoring Policy	Critical Usage on Rabbitmq Message Broker Filesystem	For `var/lib/rabbitmq`, Mounted Filesystem Disk Usage goes over 75%.
	Filesystem is Full	Overall Mounted Filesystem Disk Usage reaches 100%.
	High Filesystem Usage	Overall Mounted Filesystem Disk Usage goes over 95%.
	High System Swap Utilization	Swap Utilization goes under 5 % for 5 minutes or more.
	High Usage on Rabbitmq Message Broker Filesystem	Mounted Filesystem Disk Usage for `var/lib/rabbitmq` goes over 60%.
	Host Unreachable	Host down.
	LogCollector Event Processor Exchange Bindings Status	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Bindings	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Consumers	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	Power Supply Failure	Host not receiving power.
	RAID Logical Drive Degraded	For Raid Logical Drive, Drive State equals Degraded or Partially Degraded.

Policy Name	Rule Name	Alarm Triggered
	RAID Logical Drive Failed	For Raid Logical Drive, Logical Drive State equals Offline, Failed, or Unknown.
	RAID Logical Drive Rebuilding	For Raid Logical Drive, Logical Drive State equals Rebuild.
	RAID Physical Drive Failed	For Raid Physical Drive, Physical Drive State does not equal Online, Online Spun Up, or Hotspare.
	RAID Physical Drive Failure Predicted	For Raid Physical Drive, Physical Drive Predictive Failure Count is greater than 1.
	RAID Physical Drive Rebuilding	For Raid Physical Drive, Physical Drive State equals Rebuild.
	RAID Physical Drive Unconfigured	For Raid Physical Drive, Physical Drive State contains Unconfigured(good).
	SD Card Failure	SD Card Status does not equal ok.
NetWitness Suite Archiver Monitoring Policy	Archiver Aggregation Stopped	Archiver Status does not equal started.
	Archiver Database(s) Not Open	Database Status does not equal opened.
	Archiver Not Consuming From Service	Devices Status does not equal consuming.
	Archiver Service in Bad State	Service State does not equal started or ready.
	Archiver Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Broker Monitoring Policy	Broker >5 Pending Queries	Queries Pending greater than or equal to 5 for 10 minutes or more.
	Broker Aggregation Stopped	Broker Status does not equal started.
	Broker Not Consuming From Service	Devices Status does not equal consuming.
	Broker Service in Bad State	Service State does not equal started or ready.
	Broker Service Stopped	Server Status does not equal started.
	Broker Session Rate Zero	Session Rate (current) equals 0 for 2 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Concentrator Monitoring Policy	Concentrator >5 Pending Queries	Queries Pending greater than or equal to 5 for 10 minutes or more.
	Concentrator Aggregation Behind >100K Sessions	Devices Sessions Behind is greater than or equal to 100000 for 1 minute or more.
	Concentrator Aggregation Behind >1M Sessions	Devices Sessions Behind is greater than or equal to 1000000 for 1 minute or more.
	Concentrator Aggregation Behind >50M Sessions	Devices Sessions Behind is greater than or equal to 50000000 for 1 minute or more.
	Concentrator Aggregation Stopped	Broker Status does not equal started.
	Concentrator Database(s) Not Open	Database Status does not equal opened.
	Concentrator Meta Rate Zero	Concentrator Meta Rate (current) equals 0 for 2 minutes or more.
	Concentrator Not Consuming From Service	Devices Status does not equal consuming.
	Concentrator Service in Bad State	Service State does not equal started or ready.
	Concentrator Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Decoder Monitoring Policy	Decoder Capture Not Started	Capture Status does not equal started.
	Decoder Capture Rate Zero	Capture Rate (current) equals 0 for 2 minutes or more.
	Decoder Database Not Open	Database Status does not equal opened.
	Decoder Dropping >1% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 1%.
	Decoder Dropping >10% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 10%.
	Decoder Dropping >5% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 5%.
	Decoder Packet Capture Pool Depleted	Packet Capture Queue equals 0 for 2 minutes or more.
	Decoder Service in Bad State	Service State does not equal started or ready.
	Decoder Service Stopped	Server Status does not equal started.
NetWitness Suite Event Steam Analysis Monitoring Policy	ESA Overall Memory Utilization > 85%	Total ESA Memory Usage % is greater than or equal to 85 %.
	ESA Overall Memory Utilization > 95%	Total ESA Memory Usage % is greater than or equal to 95 %.
	ESA Service Stopped	Server Status does not equal started.
	ESA Trial Rules Disabled	Trial Rules Status does not equal enabled.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite IPDB Extractor Monitoring Policy	IPDB Extractor Service in Bad State	Service State does not equal started or ready.
	IPDB Extractor Service Stopped	Server Status does not equal started.
NetWitness Suite Incident Management Monitoring Policy	Incident Management Service Stopped	Server Status does not equal started.
NetWitness Suite Log Collector Monitoring Policy	Log Collector Service Stopped	Server Status does not equal started.
	Log Decoder Event Queue > 50% Full	Number of events currently in the queue is using 50% or more of the queue.
	Log Decoder Event Queue > 80% Full	Number of events currently in the queue is using 80% or more of the queue.
	Log Collector Service in Bad State	Service State does not equal started or ready.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Log Decoder Monitoring Policy	Decoder Dropping>10% of Packets	Capture Packets Percent Dropped (current) is greater than or equal to 10%
	Log Capture Not Started	Capture Status does not equal started.
	Log Decoder Capture Rate Zero	Capture Rate (current) equals 0 for 2 minutes or more.
	Log Decoder Database Not Open	Database Status does not equal opened.
	Log Decoder Dropping >1% of Logs	Capture Packets Percent Dropped (current) is greater than or equal to 1%.
	Log Decoder Dropping >5% of Logs	Capture Packets Percent Dropped (current) is greater than or equal to 5%.
	Log Decoder Packet Capture Pool Depleted	Packet Capture Queue equals 0 for 2 minutes or more.
	Log Decoder Service Stopped	Server Status does not equal started.
	Log Decoder Service in Bad State	Service State does not equal started or ready.
NetWitness Suite Malware Analysis Monitoring Policy	Malware Analysis Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Reporting Engine Monitoring Policy	Reporting Engine Alerts Critical Utilization	Alerts Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Available Disk <10%	Available disk space is less than 10%.
	Reporting Engine Available Disk <5%	Available disk space is less than or equal to 5%.
	Reporting Engine Charts Critical Utilization	Charts Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Rules Critical Utilization	Rules Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Schedule Task Pool Critical Utilization	Schedule Task Pool Utilization is greater than or equal to 10 for 15 minutes or more.
	Reporting Engine Service Stopped	Server Status does not equal started.
	Reporting Engine Shared Task Critical Utilization	Shared Task Pool Utilization is greater than or equal to 10 for 5 minutes or more.

Policy Name	Rule Name	Alarm Triggered
NetWitness Suite Warehouse Connector Monitoring Policy	Warehouse Connector Service in Bad State	Service State does not equal started or ready.
	Warehouse Connector Service Stopped	Server Status does not equal started.
	Warehouse Connector Stream Behind	Stream Behind is greater than or equal to 2000000.
	Warehouse Connector Stream Disk Utilization > 75%	Stream Disk Usage (Pending Destination Load) is greater than or equal to 75.
	Warehouse Connector Stream in Bad State	Stream Status does not equal consuming or online for 10 minutes r more.
	Warehouse Connector Stream Permanently Rejected Files > 300	Number of files in the permanently rejected files is greater than or equal to 300.
	Warehouse Connector Stream Permanently Rejected Folder > 75% Full	Rejected folder usage is greater than or equal to 75%.
NetWitness Suite Workbench Monitoring Policy	Workbench Service in Bad State	Service State does not equal started or ready.
	Workbench Service Stopped	Server Status does not equal started.

System Stats Browser View

NetWitness Suite provides a way to monitor the status and operations of hosts and services. The System Stats Browser tab displays key statistics, service system information, and host system information for a host or service.

You can customize the stats view depending on the parameter you select to filter the data.

To access the System Stats Browser view:

1. Go to **ADMIN** > **Health & Wellness**.

   The Health & Wellness view is displayed with the Alarms tab open.

2. Click the **System Stats Browser** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the System Stat Historical Graph	Historical Graph for System Stats

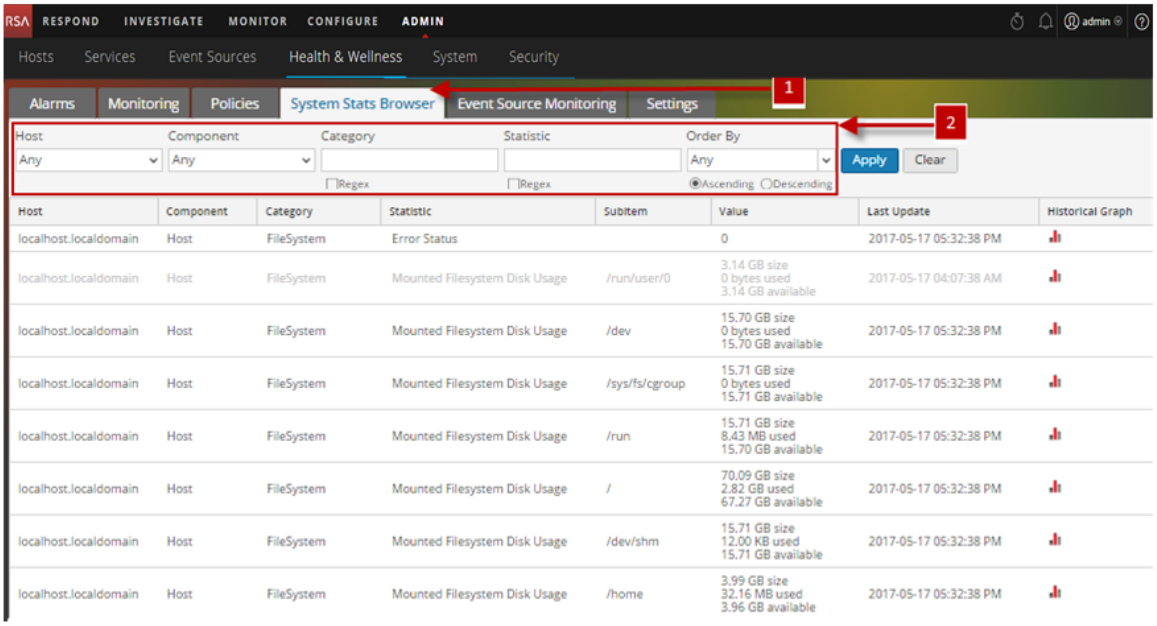
Related Topics

Monitor Service Statistics

Filter System Statistics

Quick Look

The System Stats Browser view is displayed.



Host: Any
Component: Any
Category: □Regex
Statistic: □Regex
Order By: Any ●Ascending ○Descending

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
localhost.localdomain	Host	FileSystem	Error Status		0	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/run/user/0	3.14 GB size 0 bytes used 3.14 GB available	2017-05-17 04:07:38 AM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/dev	15.70 GB size 0 bytes used 15.70 GB available	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/sys/fs/cgroup	15.71 GB size 0 bytes used 15.71 GB available	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/run	15.71 GB size 8.43 MB used 15.70 GB available	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/	70.09 GB size 2.82 GB used 67.27 GB available	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/dev/shm	15.71 GB size 12.00 KB used 15.71 GB available	2017-05-17 05:32:38 PM	
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/home	3.99 GB size 32.16 MB used 3.96 GB available	2017-05-17 05:32:38 PM	

1	Displays System Stats Browser View
2	Toolbar used to filter and customize the System Stats Browser View

Note: Historical graphs are enabled, and can be displayed, for statistics with numeric values. However, historical graphs are disabled for statistics with string values, for example, Health checks (Healthy), and are displayed as gray in the UI.

Filters

This table lists the various parameters you can use to filter and customize the System Stats view.

Parameter	Description
Host	Select a host from the drop-down menu to display the stats of the selected host. Select **Any** to list all the available hosts.
Component	Select a component from the drop-down menu to display the stats for the selected component. Select **Any** to list out all the components on a selected host.
Category	Type the category to display the stats for the required category. Select Regex to enable Regex filter. It performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Statistic	Type the statistic to display the required statistic on all the hosts or components. Select Regex to enable Regex filter. This performs a regular expression search against text and lists out the specified category. If Regex is not selected it supports globbing pattern matching.
Order By	Select the order in which the list needs to be filtered. Select Ascending to filter the list it in an ascending order.

Commands

Command	Action
Apply	Click to apply the filters chosen and display the list accordingly.

Command	Action
Clear	Click to clear the chosen filters.

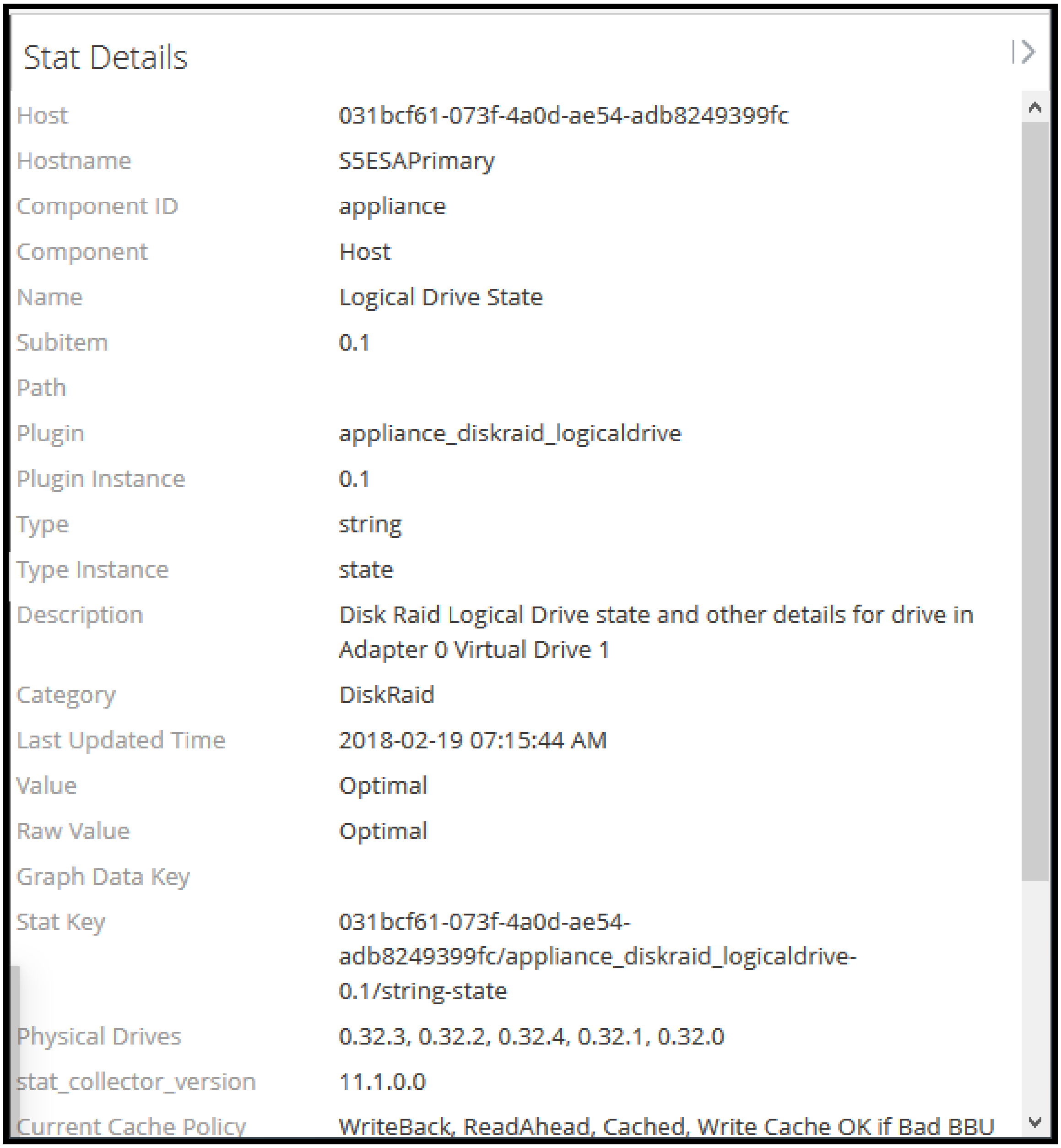
System Stats View Display

Displays statistics, service system information, and host system information for a host or service.

Access Stats Details

Select one of the stats and click **Stats Details** on the right hand side of the panel.

The Stats details panel opens with details of the selected stats.



Stat Details

Host	031bcf61-073f-4a0d-ae54-adb8249399fc
Hostname	S5ESAPrimary
Component ID	appliance
Component	Host
Name	Logical Drive State
Subitem	0.1
Path	
Plugin	appliance_diskraid_logicaldrive
Plugin Instance	0.1
Type	string
Type Instance	state
Description	Disk Raid Logical Drive state and other details for drive in Adapter 0 Virtual Drive 1
Category	DiskRaid
Last Updated Time	2018-02-19 07:15:44 AM
Value	Optimal
Raw Value	Optimal
Graph Data Key	
Stat Key	031bcf61-073f-4a0d-ae54-adb8249399fc/appliance_diskraid_logicaldrive-0.1/string-state
Physical Drives	0.32.3, 0.32.2, 0.32.4, 0.32.1, 0.32.0
stat_collector_version	11.1.0.0
Current Cache Policy	WriteBack, ReadAhead, Cached, Write Cache OK if Bad BBU

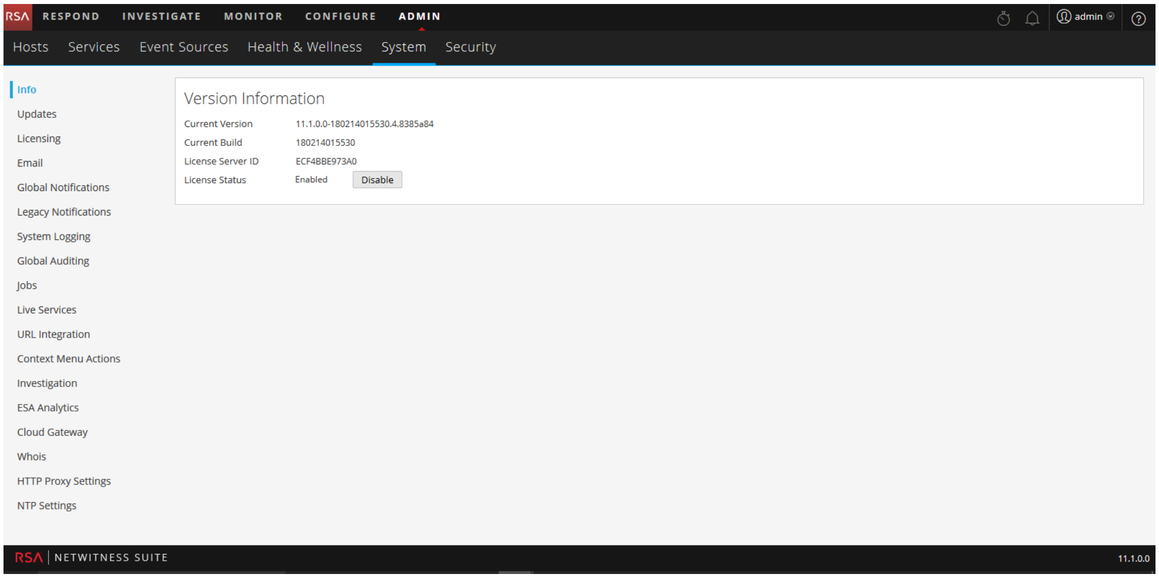
System View - System Info Panel

This topic describes the System Information panel, which displays information about the system version and license status.

The required role to access this view is **Manage System Settings**.

To access this view, do one of the following:

- Go to **ADMIN** > **System**.
  The System Information panel is displayed by default.
- When you receive a notification that a new version of NetWitness Suite is available in the Notifications tray, click **View**.



Version Information

Current Version	11.1.0.0-180214015530.4.8385a84
Current Build	180214015530
License Server ID	ECF4BBE973A0
License Status	Enabled

The Version Information section displays version information about the version of NetWitness Suite that is currently installed. The following table describes the features of the Version Information section.

Name	Description
Current Version	Displays the version of Security Analytics that is currently running. The format of the version is *major-relase.minor-release.stability-id.build-number*. Possible values for the *stability-id* are: • 1 - Development • 2 - Alpha • 3 - Beta • 4 - RC • 5 - Gold
Current Build	Identifies the current build revision for use in troubleshooting situations.
License Server ID	Each client host is shipped with the Local Licensing Server (LLS) installed to manage host licenses. This field indicates whether the LLS is installed for this instance of Security Analytics. • When the LLS is installed, the Licensing Server ID is displayed. • **Unknown** indicates that the LLS is not installed.
License Status	Indicates whether or not the license is enabled. If the license is: • Enabled, **Enabled** is displayed in this field and there is a **Disable** button to the right so you can disable it. • Disabled, **Disabled** is displayed in this field and there is an **Enable** button to the right so you can enable it.

System Updates Panel - Settings Tab

System Updates Settings tab describes the interface you use to set up a connection to Live Update Repository. These settings ensure that the NetWitness Suite can reach the Live Update Repository and synchronize it with your Local Update Repository.

The required permission to access this view is **Apply System Updates**.

To access this view:

1. Go to **ADMIN** > **System**.
2. Select **Updates**.

What do you want to do?

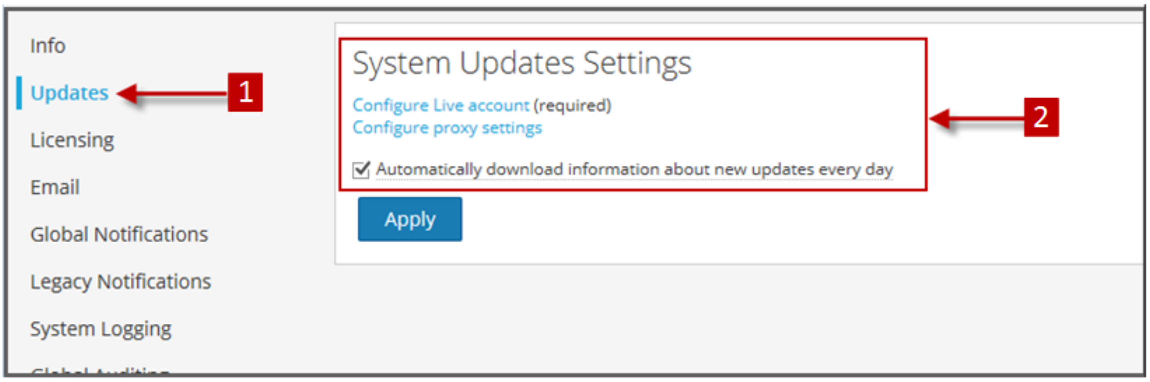
Role	I want to ...	Show me how
Administrator	Automatically download updates	Enable automatic synchronization with the RSA update repository.

Related Topics

Managing NetWitness Suite Updates

Quick Look

The System Updates Settings panel is displayed.



System Updates Settings

Configure Live account (required)
Configure proxy settings

☑ Automatically download information about new updates every day

1	Displays System Update Setting Tab
2	Configure Account and Setting for Automatic Updates

Features

This table describes the features in the System Updates Settings panel.

Feature	Description
Configure Live account	Displays the **ADMIN** > **System** > **Live Services** panel in which you can configure your Live Account credentials if they are not configured.
Configure proxy settings	Displays the **ADMIN** > **System** > **HTTP Proxy Settings** panel in which you can configure an HTTP proxy if it is not configured.
Automatically download information about new updates every day	Select to enable automatic synchronization with the RSA update repository. If there are new updates available, information will automatically be displayed in the **ADMIN** > **HOSTS** panel.
Apply	Applies the settings in this tab.

System Logging - Settings View

The RSA NetWitness SuiteSettings view in the System Logging panel configures the size of the log files, the number of backup log files maintained, as well as the default logging levels for the packages within NetWitness Suite. The **Configure Log File Settings** topic in the *System Configuration Guide* provides detailed procedures.

To access the Settings tab:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.
   The System Logging panel opens to the Realtime tab by default.
3. Click the **Settings** tab.

What do you want to do?

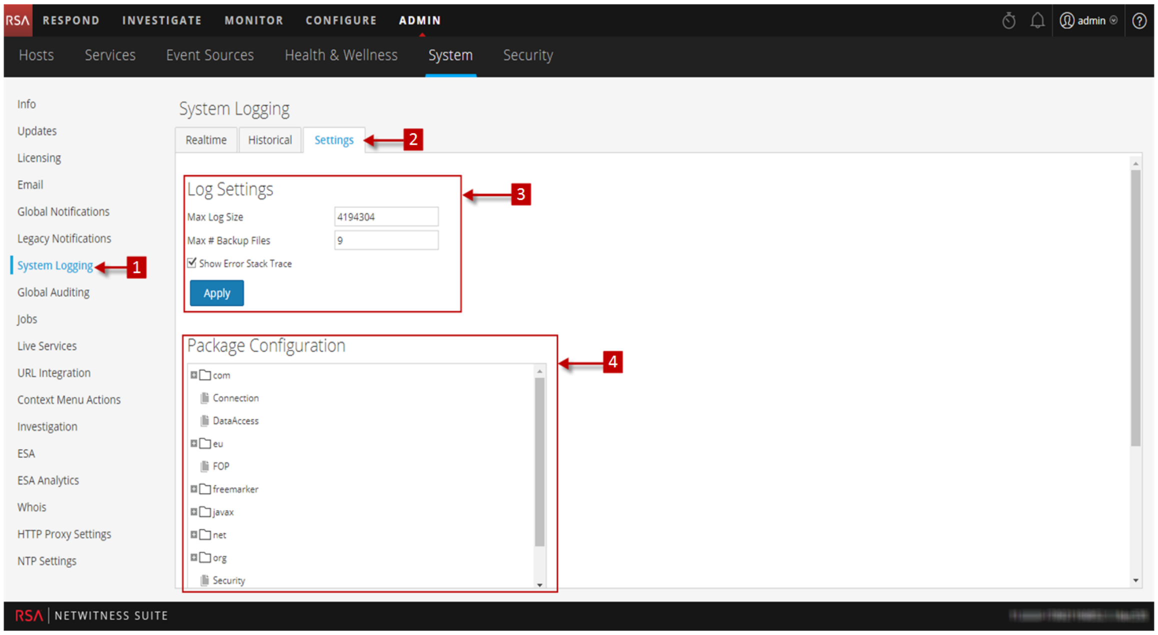
Role	I want to ...	Show me how
Administrator	Configure the size of the Log files	Setup the Log Settings Toolbar

Related Topics

System Logging - Historical Tab

System Logging - Realtime Tab

Quick Look



Max Log Size 4194304

Max # Backup Files 9

☑ Show Error Stack Trace

1 Displays System Logging Panel

2 Displays Settings Tab

3 The section allows the user to configure Log Settings

4 The section allows the user to configure Package

Features

The **Settings** tab has two sections: Log Settings and Package Configuration.

Log Settings

The Log Settings section configures the size of the NetWitness Suite log files and the number of backup logs that NetWitness Suite maintains.

Feature	Description
Max Log Size	Configures the maximum size in bytes of each log file. The minimum value for this setting is **4096**.

Feature	Description
Max # Backup Files	Specifies how many backup log files are maintained. The minimum value for this setting is **0**. When the maximum number of log files is attained, and a new backup file is made, the oldest backup is discarded.
□ Show Error Stack Trace	Select checkbox to display ERROR, STACK, and TRACE log messages.
Apply	Puts the settings into effect immediately for all future logs.

Package Configuration

The Package Configuration section shows the NetWitness Suite packages in a tree structure.

Feature	Description
Package tree	The tree contains all the packages used within NetWitness Suite. You can drill down into the tree to view the log levels of each package. The **root** logging level represents the default log level for all packages that are not explicitly set. The root level is set to **INFO**
Package field	This field is populated with the name of the selected package when you select a package in the **Package** tree.
Log Level	If the selected package has a log level explicitly set, the value is displayed in the **Log Level** field.
□ Reset recursively	Select checkbox to reset the log recursively.
Apply	This button puts the settings into effect immediately for all future logs.
Reset	This button resets the selected package to the log level of **root**.

System Logging - Realtime Tab

This topic describes the features of the System Logging > Realtime tab and the Services Logs view > Realtime tab.

The **Realtime** tab is a view of the NetWitness Suitelog or a service log. When it is initially loaded, the view contains the last 10 log entries. As new entries become available, the view is updated with those entries.

To access the Realtime tab:

1. Go to **ADMIN > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the **Realtime** tab by default.

What do you want to do?

Role	I want to ...	Show me how
Administrator	See details of Log entry	Displaying System and Service Logs

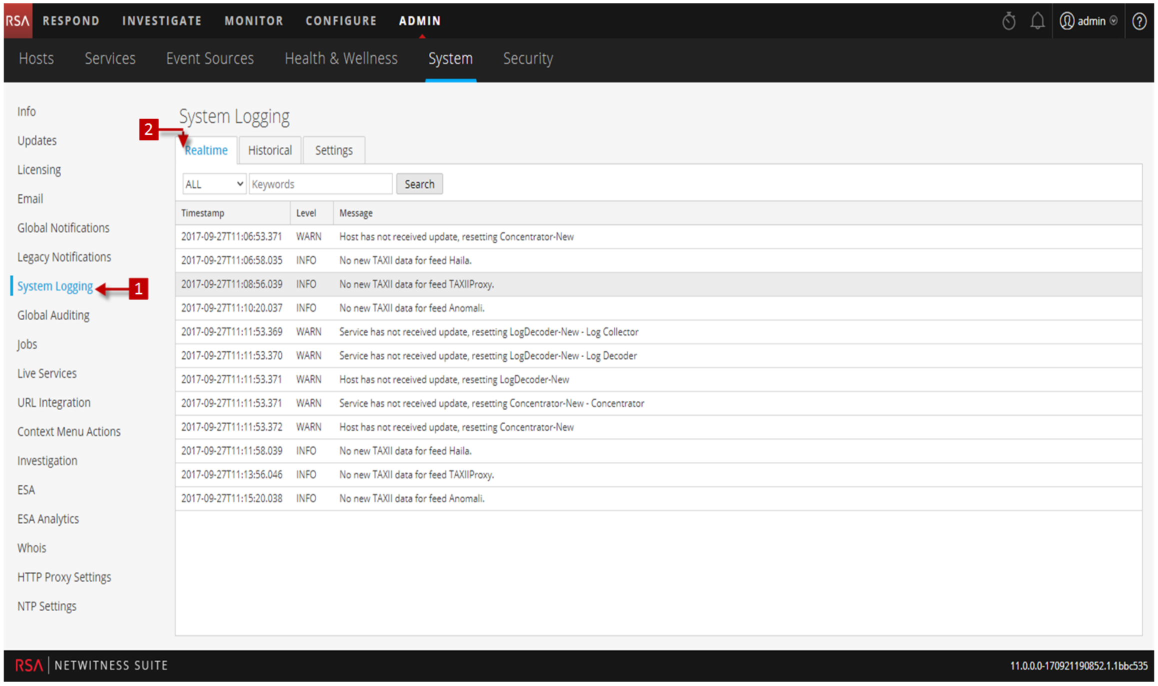
Related Topics

System Logging - Settings View

System Logging - Historical Tab

Quick Look

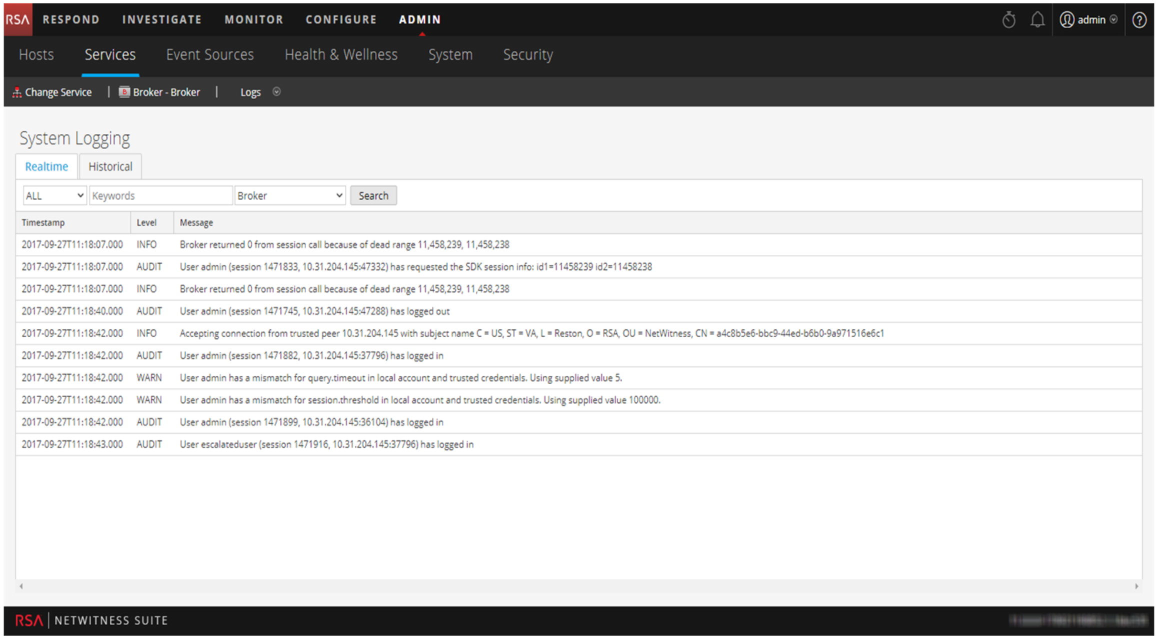
The following is an example of the **Realtime** tab in the System Logging panel.



Timestamp	Level	Message
2017-09-27T11:06:53.371	WARN	Host has not received update, resetting Concentrator-New
2017-09-27T11:06:58.035	INFO	No new TAXII data for feed Haila.
2017-09-27T11:08:56.039	INFO	No new TAXII data for feed TAXIIProxy.
2017-09-27T11:10:20.037	INFO	No new TAXII data for feed Anomali.
2017-09-27T11:11:53.369	WARN	Service has not received update, resetting LogDecoder-New - Log Collector
2017-09-27T11:11:53.370	WARN	Service has not received update, resetting LogDecoder-New - Log Decoder
2017-09-27T11:11:53.371	WARN	Host has not received update, resetting LogDecoder-New
2017-09-27T11:11:53.371	WARN	Service has not received update, resetting Concentrator-New - Concentrator
2017-09-27T11:11:53.372	WARN	Host has not received update, resetting Concentrator-New
2017-09-27T11:11:58.039	INFO	No new TAXII data for feed Haila.
2017-09-27T11:13:56.046	INFO	No new TAXII data for feed TAXIIProxy.
2017-09-27T11:15:20.038	INFO	No new TAXII data for feed Anomali.

1	Displays System Logging Panel
2	Displays Realtime Tab

The following is an example of the **Realtime** tab in the Services Logs view, which is similar.

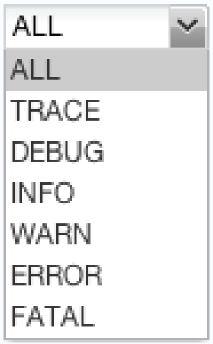


Timestamp	Level	Message
2017-09-27T11:18:07.000	INFO	Broker returned 0 from session call because of dead range 11,458,239, 11,458,238
2017-09-27T11:18:07.000	AUDIT	User admin (session 1471833, 10.31.204.145:47332) has requested the SDK session info: id1=11458239 id2=11458238
2017-09-27T11:18:07.000	INFO	Broker returned 0 from session call because of dead range 11,458,239, 11,458,238
2017-09-27T11:18:40.000	AUDIT	User admin (session 1471745, 10.31.204.145:47288) has logged out
2017-09-27T11:18:42.000	INFO	Accepting connection from trusted peer 10.31.204.145 with subject name C = US, ST = VA, L = Reston, O = RSA, OU = NetWitness, CN = a4c8b5e6-bbc9-44ed-b6b0-9a971516e6c1
2017-09-27T11:18:42.000	AUDIT	User admin (session 1471882, 10.31.204.145:37796) has logged in
2017-09-27T11:18:42.000	WARN	User admin has a mismatch for query.timeout in local account and trusted credentials. Using supplied value 5.
2017-09-27T11:18:42.000	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2017-09-27T11:18:42.000	AUDIT	User admin (session 1471899, 10.31.204.145:36104) has logged in
2017-09-27T11:18:43.000	AUDIT	User escalateduser (session 1471916, 10.31.204.145:37796) has logged in

Features

The **Realtime** tab has a toolbar with input fields to allow filtering of the entries, and below the toolbar is a grid containing the log entries.

Toolbar

Feature	Description
Log Level drop-down  ALL ALL TRACE DEBUG INFO WARN ERROR FATAL	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.
Keywords field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Filter button	Click to activate filtering based on the log level, keyword, and service selections.

Log Grid Columns

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

System Logging - Historical Tab

The Historical tab provides a searchable view of the NetWitness Suite log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the system.

To access the Historical tab:

1. Go to **ADMIN** > **System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the **Realtime** tab by default.
3. Click the **Historical** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	View the Historical Graph	Historical Graph for System Stats

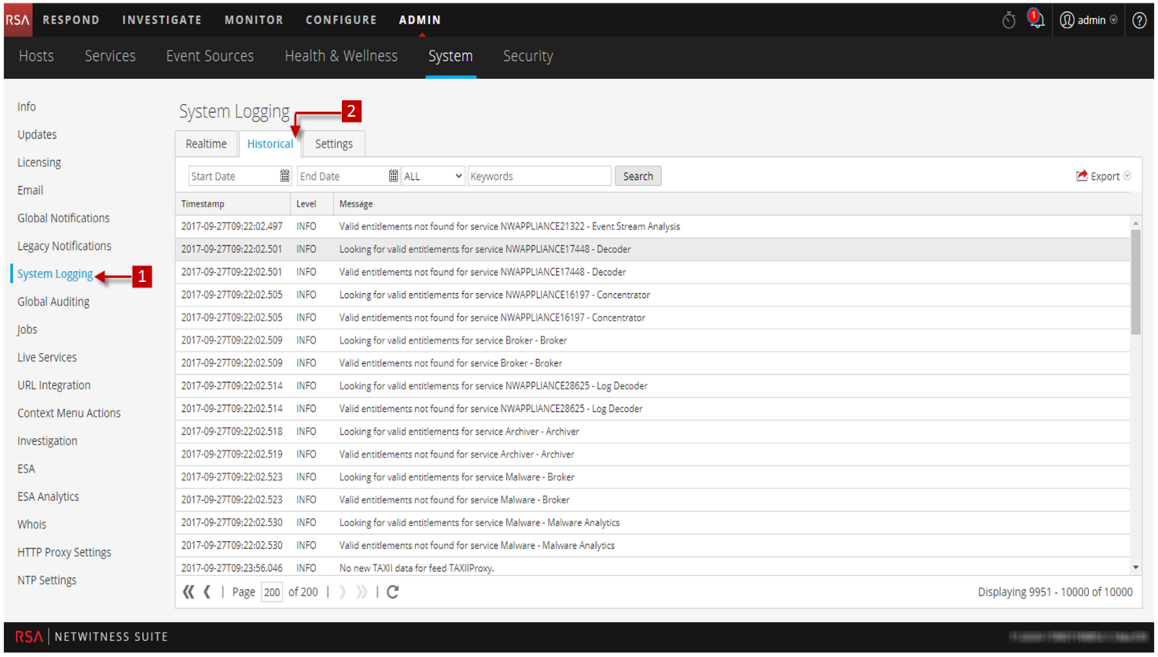
Related Topics

System Logging - Realtime Tab

System Logging - Settings View

Quick Look

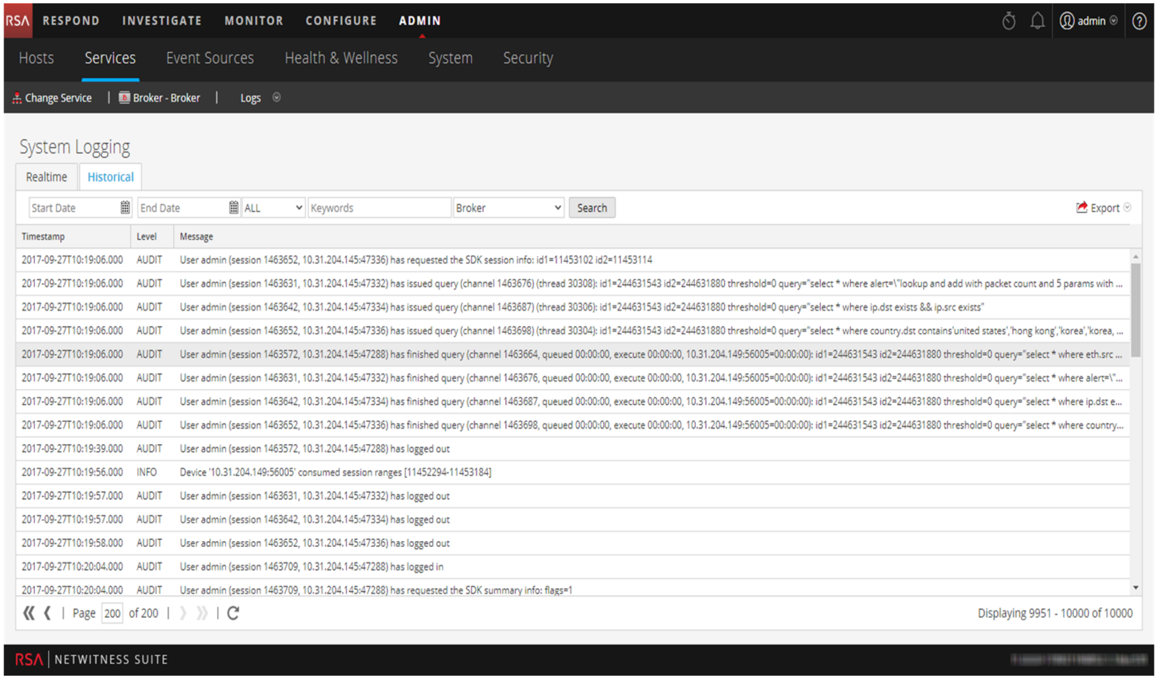
The following is an example of the **Historical** tab in the System Logging panel. It shows the NetWitness Suite logs.



Timestamp	Level	Message
2017-09-27T09:22:02.497	INFO	Valid entitlements not found for service NWAPPLIANCE21322 - Event Stream Analysis
2017-09-27T09:22:02.501	INFO	Looking for valid entitlements for service NWAPPLIANCE17448 - Decoder
2017-09-27T09:22:02.501	INFO	Valid entitlements not found for service NWAPPLIANCE17448 - Decoder
2017-09-27T09:22:02.505	INFO	Looking for valid entitlements for service NWAPPLIANCE16197 - Concentrator
2017-09-27T09:22:02.505	INFO	Valid entitlements not found for service NWAPPLIANCE16197 - Concentrator
2017-09-27T09:22:02.509	INFO	Looking for valid entitlements for service Broker - Broker
2017-09-27T09:22:02.509	INFO	Valid entitlements not found for service Broker - Broker
2017-09-27T09:22:02.514	INFO	Looking for valid entitlements for service NWAPPLIANCE28625 - Log Decoder
2017-09-27T09:22:02.514	INFO	Valid entitlements not found for service NWAPPLIANCE28625 - Log Decoder
2017-09-27T09:22:02.518	INFO	Looking for valid entitlements for service Archiver - Archiver
2017-09-27T09:22:02.519	INFO	Valid entitlements not found for service Archiver - Archiver
2017-09-27T09:22:02.523	INFO	Looking for valid entitlements for service Malware - Broker
2017-09-27T09:22:02.523	INFO	Valid entitlements not found for service Malware - Broker
2017-09-27T09:22:02.530	INFO	Looking for valid entitlements for service Malware - Malware Analytics
2017-09-27T09:22:02.530	INFO	Valid entitlements not found for service Malware - Malware Analytics
2017-09-27T09:23:56.046	INFO	No new TAXII data for feed TAXIIProxy.

1	Displays System Logging Tab
2	Displays Historical Tab

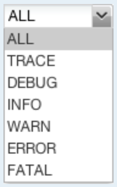
The following is an example of the **Historical** tab in the Services Logs view. It shows the services logs.



Timestamp	Level	Message
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463652, 10.31.204.145:47336) has requested the SDK session info: id1=11453102 id2=11453114
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463631, 10.31.204.145:47332) has issued query (channel 1463676) (thread 30308): id1=244631543 id2=244631880 threshold=0 query="select * where alert=\"lookup and add with packet count and 5 params with ...
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463642, 10.31.204.145:47334) has issued query (channel 1463687) (thread 30306): id1=244631543 id2=244631880 threshold=0 query="select * where ip.dst exists && ip.src exists"
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463652, 10.31.204.145:47336) has issued query (channel 1463698) (thread 30304): id1=244631543 id2=244631880 threshold=0 query="select * where country.dst contains'united states','hong kong','korea','korea, ...
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463572, 10.31.204.145:47288) has finished query (channel 1463664, queued 00:00:00, execute 00:00:00, 10.31.204.149:56005=00:00:00): id1=244631543 id2=244631880 threshold=0 query="select * where eth.src ...
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463631, 10.31.204.145:47332) has finished query (channel 1463676, queued 00:00:00, execute 00:00:00, 10.31.204.149:56005=00:00:00): id1=244631543 id2=244631880 threshold=0 query="select * where alert=\"...
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463642, 10.31.204.145:47334) has finished query (channel 1463687, queued 00:00:00, execute 00:00:00, 10.31.204.149:56005=00:00:00): id1=244631543 id2=244631880 threshold=0 query="select * where ip.dst e...
2017-09-27T10:19:06.000	AUDIT	User admin (session 1463652, 10.31.204.145:47336) has finished query (channel 1463698, queued 00:00:00, execute 00:00:00, 10.31.204.149:56005=00:00:00): id1=244631543 id2=244631880 threshold=0 query="select * where country...
2017-09-27T10:19:39.000	AUDIT	User admin (session 1463572, 10.31.204.145:47288) has logged out
2017-09-27T10:19:56.000	INFO	Device '10.31.204.149:56005' consumed session ranges [11452294-11453184]
2017-09-27T10:19:57.000	AUDIT	User admin (session 1463631, 10.31.204.145:47332) has logged out
2017-09-27T10:19:57.000	AUDIT	User admin (session 1463642, 10.31.204.145:47334) has logged out
2017-09-27T10:19:58.000	AUDIT	User admin (session 1463652, 10.31.204.145:47336) has logged out
2017-09-27T10:20:04.000	AUDIT	User admin (session 1463709, 10.31.204.145:47288) has logged in
2017-09-27T10:20:04.000	AUDIT	User admin (session 1463709, 10.31.204.145:47288) has requested the SDK summary info: flags=1

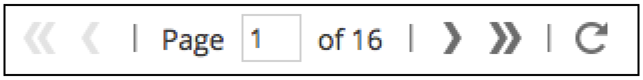
Features

The **Historical** tab has a toolbar with input fields to allow filtering of the entries, a grid containing the log entries, and paging tools.

Feature	Description
Start Date and **End Date**	The **Start Date** and **End Date** range search options limit the log entries to a point in time. When used, you must provide both a start and end date. The times are optional. The date range is validated to assure that the end date is not before the start date.
Log Level drop-down  ALL ALL TRACE DEBUG INFO WARN ERROR FATAL	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.
Keyword field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Search button	Click to activate a search based on the start and end date, log level, keyword, and service selections.
Export	Click to export the currently viewed grid entries to a text file. You can select either comma-separated or tab-separated format for the entries in the file.

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

The paging tools below the grid provide a way to navigate through the pages of log entries.



Search Log Entries

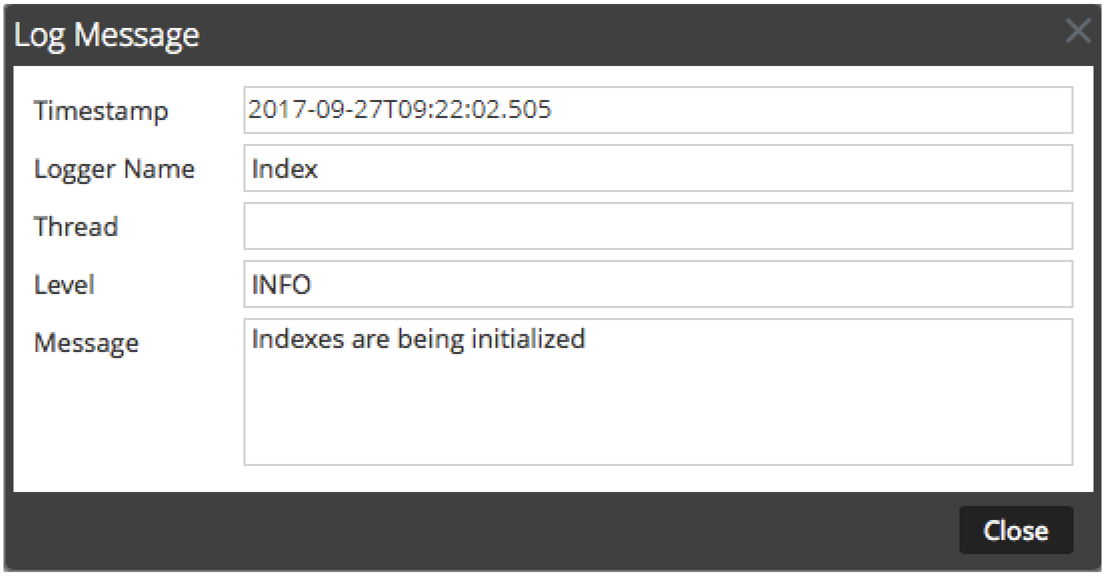
To search the results shown in the **Historical** tab:

1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both.
3. (Optional) For service logs, select the **Service**: host or service.
4. Click **Search**.
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the **Historical** tab Log grid provides the summary information of a log entry. To view complete details:

1. Double-click a log entry.
   The Log Message dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



Timestamp: 2017-09-27T09:22:02.505

Logger Name: Index

Thread:

Level: INFO

Message: Indexes are being initialized

2. When finished viewing, click **Close**.

Page Through the Entries

To view the different pages of the grid, use the paging controls on the bottom of the grid as follows:

- Use the navigation buttons
- Manually enter the page you want to view, and press **ENTER**.

Export

To export the logs in the current view:

Click **Export**, and select one of the drop-down options, **CSV Format** or **Tab Delimited**.
The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a NetWitness Suite system log exported with comma-separated values is named **UAP_log_export_CSV.txt**, and an appliance log exported with tab-separated values is named **APPLIANCE_log_export_TAB.txt**.