NetWitness® Platform XDR

Version 12.3.0.0

System Maintenance Guide

NETWITNESS

Platform XDR

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

Miscellaneous

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

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2023

Contents

System Maintenance **13**

Review Best Practices **14**

Safeguarding Assets with NetWitness Supplied Policies 14

Safeguarding Assets with Policies Based on Your Environment 14

Creating Rules and Notifications Judiciously 14

Troubleshooting Issues 14

Monitor NetWitness Platform Health **15**

Monitor Health and Wellness using NetWitness Platform UI 16

Manage Policies 17

Add a Policy 17

Add Policy Example 20

Edit a Policy 22

Duplicate a Policy 23

Assign Services or Groups 24

Remove Services or Groups 26

Add or Edit a Rule 26

Hide or Show Rule Conditions Columns 27

Delete a Rule 28

Suppress a Rule 28

Suppress a Policy 29

Add an Email Notification 29

Delete an Email Notification 29

Include the Default Email Subject Line 30

Monitor System Statistics 33

Filter System Statistics 34

View Historical Graphs of System Statistics 37

Monitor Service Statistics 38

Add Statistics to a Gauge or Chart 39

Create a Gauge for a Statistic 39

Create a Timeline Chart for a Statistic 39

Search for a Statistic in the Chart Stats Tray 40

Edit Properties of Statistics Gauges 41

Edit Properties of a Gauge 41

Add Stats to the Gauges Section 41

Edit Properties of Timeline Charts 43

Edit Properties of a Timeline 43

Edit Properties of a Historical Timeline 43
Add Stats to Timeline Charts 44
Monitor Hosts and Services 45
Filter Hosts and Services in the Monitoring View 46
Monitor Host Details 48
Monitor Service Details 49
Monitor Event Sources 52
Monitor Alarms 53
Monitor Health and Wellness Using SNMP Alerts 55
SNMP Configuration 55
Thresholds 55
Configure SNMPv3 for a Host 55
Set the Threshold for a Service 56
SNMP Traps for System Status 57
Troubleshooting Health & Wellness 58
Issues Common to All Hosts and Services 58
Issues Identified by Messages in the Interface or Log Files 58
Issues Not Identified by the User Interface or Logs 63
Monitor New Health and Wellness 65
Dashboard 65
Visualization 65
Monitors 66
Notifications 66
Installing New Health and Wellness 66
Accessing New Health and Wellness Dashboards 66
Configuring Notifications 67
Adding Alert Notifications 68
Suppressing Notifications 69
Monitoring through Dashboards 70
Creating a Custom Dashboard 71
Monitoring through Alerts 72
Creating Custom Monitors 74
Adding Custom Trigger to an Existing Monitor 75
Managing Dashboards and Alerts 77
Modify a Dashboard 77
Delete a Dashboard 77
Delete a Visualization 78
Modify an Existing Trigger 78
Managing Notifications 79
Modify a Notification 79
Modify a Notification Suppression Policy 79

Advanced Configurations 80
Restore Default Content 80
Enable Services 80
Disable Services 81
Update an Interval 82
Update the Default Configuration 83
Configure the Data Retention Policy 85
Backup and Restore New Health and Wellness 89
Troubleshooting New Health and Wellness 90
Appendices 92
New Health and Wellness Dashboards 93
Deployment Health Overview Dashboard 93
Hosts Dashboard 95
Logs Dashboard 97
Packet Overview Dashboard 99
Analysis Dashboard 101
Endpoint Dashboard 103
ESA Correlation Overview Dashboard 105
Logstash Input Plugin Dashboard 106
License Usage Dashboard 108
New Health and Wellness Monitors 113
Uninstall New Health and Wellness 116
Manage NetWitness Platform Updates 120
Reissue Certificates 121
Introduction 121
CA Certificate Reissue 121
Service Certificate Reissue 121
Reissuing Service Certificate 122
When to Use the --host-all Argument 123
cert-reissue Arguments and Options for All Hosts 123
When to Use the Individual Host Argument (--host-key <ID, IP, hostname or display name of host>) 124
Reissuing Certificates for All Hosts Except Windows Legacy Collection (WLC) host 125
Running the Cert-Reissue Command for All Hosts 125
Running the Cert-Reissue Command for an Individual Host 125
Reissuing Certificates for a WLC Host 125
Successful Reissue Summary Report 126
Unsuccessful Reissue Summary Reports 126
Reissue Failed for Host and Aborted Command 126
Reissue Certificate Partially Executed 127

Display System and Service Logs **128**
View System Logs 128
Display Service Logs 128
Filter Log Entries 129
Show Details of a Log Entry 129
Access Reporting Engine Log File 131
All Log Files 131
Upstart Logs 131
Search and Export Historical Logs 132
Display the Historical System Log 132
Display a Historical Service Log 132
Search Log Entries 133
Show Details of a Log Entry 133
Page Through Log Entries 134
Export a Log File 134
Maintain Queries Using URL Integration **135**
Edit a Query 135
Delete a Query 136
Clear All Queries 136
Use a Query in a URI 136
Manage the deploy_admin Account **138**
Change the deploy_admin Account Password 138
Change the deploy_admin Account Password in a Mixed Version Environment 138
Change the deploy_admin Account Password for a Component Host that is Unavailable 139
NW Server Host Secondary IP Configuration Management **140**
Change Host Network Configuration **141**
Change Host Network Configuration 141
SSO 144
Reporting Engine 145
UCF 146
PAM 146
ECAT 146
RSA NetWitness Orchestrator (By Demisto) 149
Audit Logging 150
Health and Wellness 150
Malware Analysis 150
Windows Legacy Collection 151
Change Network Configuration for Warm Standby (Secondary) Server 152
Reconnecting Component Hosts with NW Server Hosts 152

Manage Custom Host Entries **154**
Manage Custom Host Entries in /etc/hosts 154
Manage Public or NAT IPv4 Addresses for Hosts 154
Manage Custom Jetty Configuration 154
Configure FIPS Support **156**
FIPS support for Log Collectors 157
FIPS support for Log Decoders and Decoders 157
DISA STIG **159**
How STIG Limits Account Access 159
NetWitness Passwords 159
Generate the OpenSCAP Report 159
Disable Rules in OpenSCAP Report that Hang the Report 160
Install OpenSCAP 160
Sample Report 160
Report Fields 161
Create the OpenSCAP Report 162
Create Report in HTML Only 162
Create Report in XML Only 162
Create Report in Both XML and HTML 163
Manage STIG Controls Script (manage-stig-controls) 163
Commands 163
Control Groups 164
Other Arguments 165
Rules List 166
Exceptions to STIG Compliance 181
Key to Elements in Exception Descriptions 181
CCE Number 181
Control Group ID 181
Check 181
Comments 182
Customer Responsibility Exceptions 182
CCE-26952-2 Configure Periodic Execution of AIDE (Control Group = audit) 182
CCE-27096-7 Install AIDE (Control Group = n/a) 182
CCE-27218-7 Remove the X Windows Package Group 182
CCE-27295-5 Use Only FIPS 140-2 Validated Ciphers (Control Group = n/a) 183
CCE-27334-2 Ensure SELinux State is Enforcing 183
CCE-27445-6 Disable SSH Root Login (Control Group = ssh-prevent-root) 183
CCE-80127-4 Install McAfee Virus Scanning Software (Control Group = n/a) 183
CCE-80129-0 Virus Scanning Software Definitions Are Updated (Control Group = n/a) 183
CCE-80207-4 Enable Smart Card Login (Control Group = n/a) 184

CCE-80359-3 Enable FIPS Mode in GRUB2 (Control Group = fips-kernel) 184
CCE-80374-2 Configure Notification of Post-AIDE Scan Details (Control Group = n/a) 184
CCE-80375-9 Configure AIDE to Verify Access Control Lists (Control Group = n/a) 185
CCE-80376-7 Configure AIDE to Verify Extended Attributes (Control Group = n/a) 185
CCE-80377-5 Configure AIDE to Use FIPS 140-2 for Validating Hashes (Control Group = n/a) 185
CCE-80519-2 Install Smart Card Packages For Multi-Factor Authentication (Control Group = n/a) 185
Exceptions That Are Not a Finding 186
CCE-26404-4 Ensure /var Located On Separate Partition (Control Group = n/a) 186
CCE-26828-4 Set GNOME Login Inactivity timeout (Control Group = n/a) 186
CCE-26884-7 Set Lockout Time For Failed Password Attempts (Control Group = auth) 186
CCE-26971-2 Ensure /var/log/audit Located On Separate Partition (Control Group = audit) 187
CCE-27127-0 Enable Randomized Layout of Virtual Address Space (Control Group = n/a) 187
CCE-27157-7 Verify File Hashes with RPM (Control Group = n/a) 187
CCE-27339-1 Record Events that Modify the System's Discretionary Access Controls - chmod 188
CCE-27209-6 Verify and Correct File Permissions with RPM (Control Group = n/a) 188
CCE-27303-7 (Control ID = 2) Modify the System Login Banner (Control Group = ssh) 189
CCE-27311-0 Very Permissions on SHH Server *.pub Key Files (Control Group = na) 189
CCE-27314-4 Enable SSH Warning Banner (Control Group = na) 189
CCE-27349-0 Set Default firewalld Zone for Incoming Packets (Control Group = n/a) 190
CCE-27386-2 Ensure Default SNMP Password Is Not Used (Control Group = n/a) 190
CCE-27455-5 Use Only FIPS 140-2 Validated MACs (Control Group = na) 190
CCE-27471-2 Disable SSH Access via Empty Passwords (Control Group = n/a) 190
CCE-27485-2 Very Permissions on SHH Server Private *.key Key Files (Control Group = na) 190
CCE-80156-3 Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces (Control Group = n/a) 191
CCE-80157-1 Disable Kernel Parameter for IP Forwarding (Control Group = n/a) 191
CCE-80158-9 Configure Kernel Parameter for Accepting ICMP Redirects for All Interfaces (Control Group = n/a) 191
CCE-80163-9 Configure Kernel Parameter for Accepting ICMP Redirects By Default (Control Group = n/a) 191
CCE-80165-4 Configure Kernel Parameter to Ignore ICMP Broadcast Echo Requests (Control Group = n/a) 192
CCE-80225-6 Print Last Log (Control Group = n/a) 192
CCE-80226-4 Enable Encrypted X11 Forwarding (Control Group = n/a) 192
CCE-80348-6 Ensure gpgcheck Enabled for Repository Metadata (Control Group = n/a) 192
CCE-80383-3 Record Attempts to ALter Logon Events - failock (Control Group = na) 193
CCE-80399-9 Ensure auditd Collects Information on the Use of Privileged Commands - userhelper (Control Group = na) 193
CCE-80437-7 Configure PAM in SSSD Services (Control Group = n/a) 193
CCE-80438-5 Configure Multiple DNS Servers in /etc/resolv.conf (Control Group = n/a) 193

CCE-80439-3 Configure Time Service Maxpoll Interval (Control Group = na) 193
CCE-80447-6 Configure the Firewalld Ports (Control Group = n/a) 194
CCE-80515-0 Configure SSSD LDAP Backend Client CA Certificate Location (Control Group = n/a) 194
CCE-80545-7 Verify and Correct Ownership with RPM (Control Group = n/a) 194
CCE-80546-5 Configure SSSD LDAP Backend to Use TLS For All Transactions (Control Group = n/a) 195
CCE-80998-8 Verify firewall Enabled 195
CCE-82035-7 Ensure /var/log/audit Located On Separate Partition 196
CCE-82053-0 Ensure /tmp Located On Separate Partition 196
CCE-82353-4 Ensure /var Located On Separate Partition 196
Rules Supported in a Future Release 196
CCE-27277-3 Disable Modprobe Loading of USB Storage Driver (Control Group = services) 197
CCE-27309-4 Set Boot Loader Password in grub2 (Control Group = fips-kernel) 197
CCE-80179-5 Configure Kernel Parameter for Accepting IPv6 Source-Routed Packets for All Interfaces 197
CCE-80660-4 Record Any Attempts to Run setfiles (Control Group = audit) 198
CCE-80661-2 Ensure auditd Collects Information on Kernel Module Loading - create_module (Control Group = audit) 198

Troubleshoot NetWitness Platform 199

Debugging Information 200
NetWitness Log Files 200
Files of Interest 200
Error Notification 202
Miscellaneous Tips 203
Audit Log Messages 203
NwConsole for Health & Wellness 203
Thick Client Error: remote content device entry not found 203
View Example Parsers 203
Configure WinRM Event Sources 203
Troubleshoot Feeds 204
Overview 204
Details 204
How it Works 204
Feed File 204
Troubleshooting 205
Feed File Existence 205
Group Meta Populated on LD 205
Device Group Meta on Concentrator 206
SMS Log File 206
Verify Logstats Data is Getting Read and Published by ESMReader and ESMAggregator 207

Configure JMX Feed Generator Job Interval ... 209
Troubleshooting Cert-Reissue Command ... 211
Argument Options Used for Troubleshooting ... 211
Problems and How to Troubleshoot Them ... 212
References ... 216
Health and Wellness View ... 217
Health and Wellness View - Alarms View ... 218
What do you want to do? ... 218
Related Topics ... 218
Quick Look ... 218
Alarm Details Panel ... 220
Event Source Monitoring View ... 221
Health and Wellness Historical Graphs ... 222
Historical Graph View for Events Collected from an Event Source ... 223
Historical Graph for System Stats ... 224
Health and Wellness Settings View - Archiver ... 226
What do you want to do? ... 226
Quick Look ... 226
Features ... 226
Health and Wellness Settings View - Event Sources ... 228
Health and Wellness Settings View - Warehouse Connector ... 229
Access the Warehouse Connector Monitoring view ... 229
What do you want to do? ... 229
Related topics ... 229
Quick Look ... 229
Warehouse Connector Monitoring parameters ... 230
Monitoring View ... 231
What do you want to do? ... 231
Quick Look ... 231
Groups Panel ... 231
Hosts Panel ... 232
Archiver Details View ... 234
Broker Details View ... 236
Concentrator Details View ... 237
Decoder Details View ... 238
ESA Correlation Details View ... 240
Health Stats Tab ... 240
JVM Tab ... 241
ESA Analytics Details View ... 242
Host Details View ... 243

Log Collector Details View 245
Collection Tab 245
Event Processing Tab 245
Log Decoder Details View 247
Malware Details View 249
Warehouse Connector Details View 250
Policies View 251
What do you want to do? 251
Quick Look 251
Policies Panel 251
Policy Detail Panel 252
Groups dialog 254
Rules Dialog 254
Threshold Operators 256
Health & Wellness Email Templates 257
Health & Wellness Default SMTP Template 257
Alarms Template 258
NetWitness Platform Out-of-the-Box Policies 259
System Stats Browser View 265
What do you want to do? 265
Related Topics 265
Quick Look 265
Filters 266
Commands 266
System Stats View Display 266
New Health & Wellness Tab 268
What do you want to do? 268
Related Topics 268
Quick Look 268
System View - System Info Panel 270
System Updates Panel - Settings Tab 272
What do you want to do? 272
Related Topics 272
Quick Look 272
Features 272
System Logging - Settings View 274
What do you want to do? 274
Related Topics 274
Quick Look 274
Features 275

Log Settings 275
Package Configuration 275
System Logging - Realtime Tab 277
What do you want to do? 277
Related Topics 277
Quick Look 277
Features 278
Toolbar 278
Log Grid Columns 279
System Logging - Historical Tab 280
What do you want to do? 280
Related Topics 280
Quick Look 280
Features 281
Search Log Entries 282
Show Details of a Log Entry 282
Page Through the Entries 283
Export 283

System Maintenance

This guide tells administrators how to manage hosts and services in the network, maintain and monitor the network, run jobs, and tune performance after initial network setup.

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

The following topics describe these tasks:

- Review Best Practices
- Monitor Health and Wellness using NetWitness Platform UI
- Manage NetWitness Platform Updates
- Display System and Service Logs
- Maintain Queries Using URL Integration
- Configure FIPS Support
- Change Host Network Configuration
- DISA STIG
- Troubleshoot NetWitness Platform

Review Best Practices

Review the following best practices to maintain your NetWitness Platform deployment.

Safeguarding Assets with NetWitness Supplied Policies

The purpose of the NetWitness core policies delivered with NetWitness are for safeguarding your NetWitness domain assets immediately (before you configure rules specific to your environment and your security policy).

NetWitness 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.

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

Safeguarding Assets with Policies Based on Your Environment

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

Creating Rules and Notifications Judiciously

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

Troubleshooting Issues

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

Monitor NetWitness Platform Health

Monitor the Health & Wellness of the NetWitness using any of the following:

- Monitor Health and Wellness using NetWitness Platform UI
- Monitor New Health and Wellness

Monitor Health and Wellness using NetWitness Platform UI

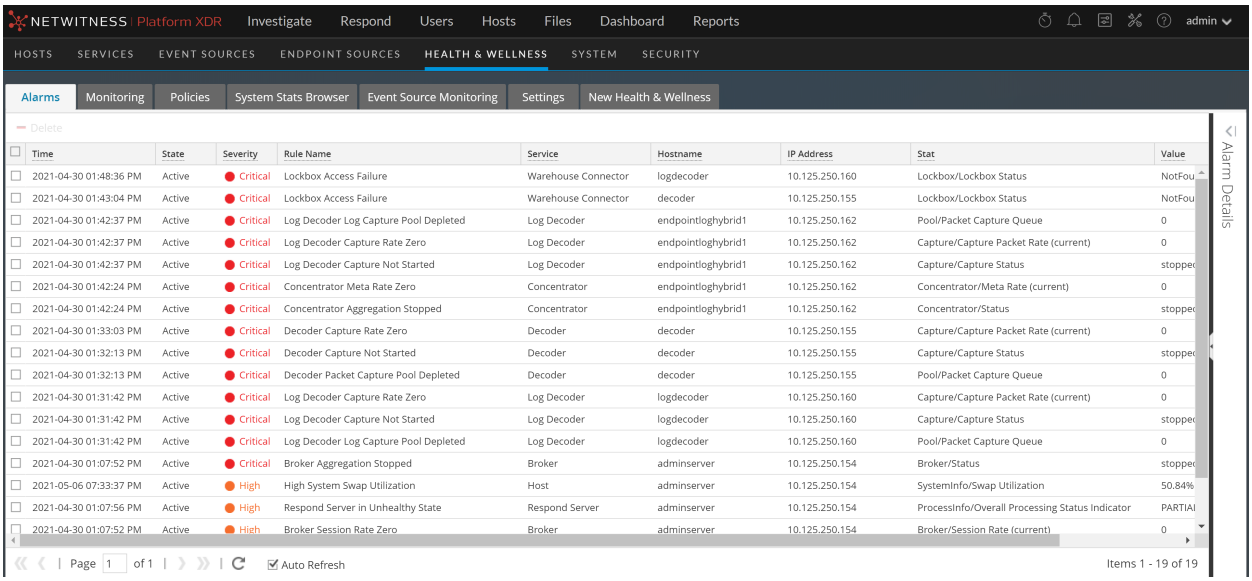
The Health & Wellness module of NetWitness enables you to:

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

You can also configure Archiver and Warehouse Connector monitoring, monitor host statistics, and work with system logs to monitor NetWitness.

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. Refer to the "Role Permissions" topic in the *Security User Management Guide* for a complete list of the default permissions for the NetWitness Interface.

The following figure displays the Health & Wellness module of the NetWitness user interface.



Manage Policies

Policies are either user-defined or supplied by NetWitness. 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.

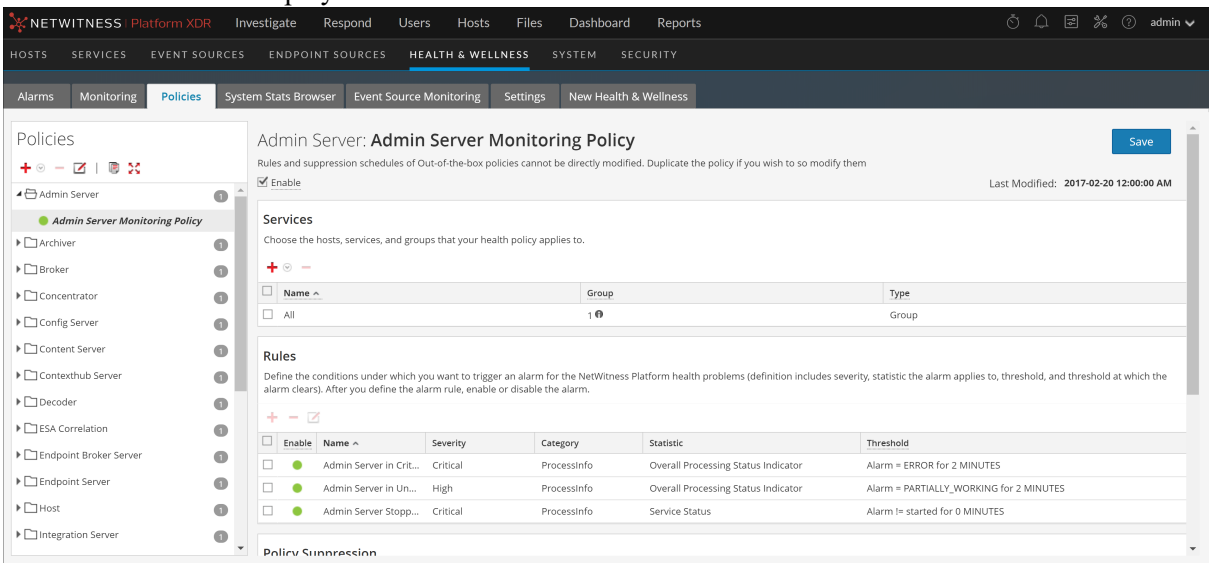
For related reference topics, see NetWitness Platform Out-of-the-Box Policies

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

Add a Policy

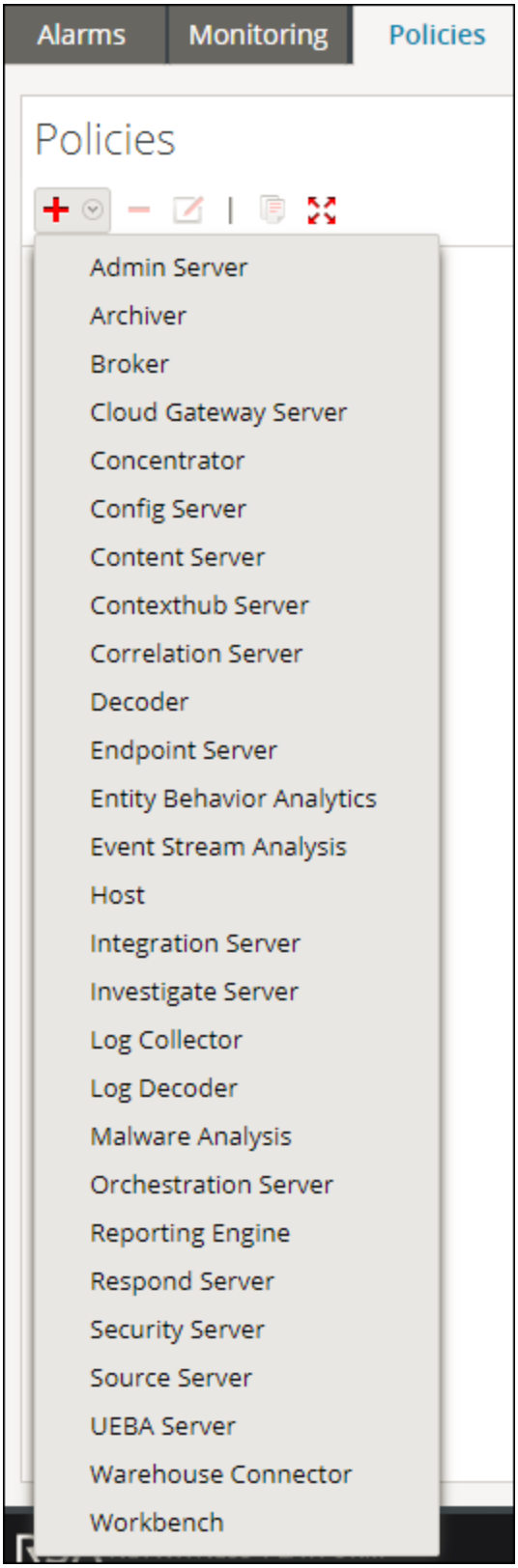
1. Go to **(Admin) > Health & Wellness.**
2. Click the **Policies** tab.

   The Policies view is displayed.

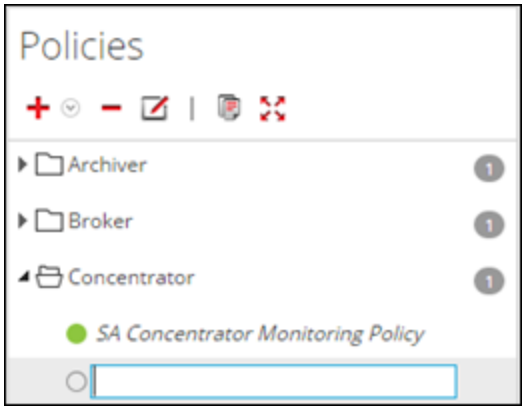


3. Click in the **Policies** panel.

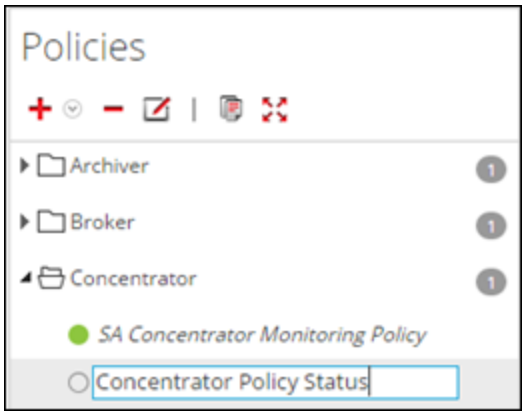
A list of your hosts and services displays for which you can create health policies.



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



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



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

6. Create a Policy in the Policy Detail panel:

   a. Select the **Enable** checkbox.

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

   c. Add rule conditions to configure the policy.

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

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

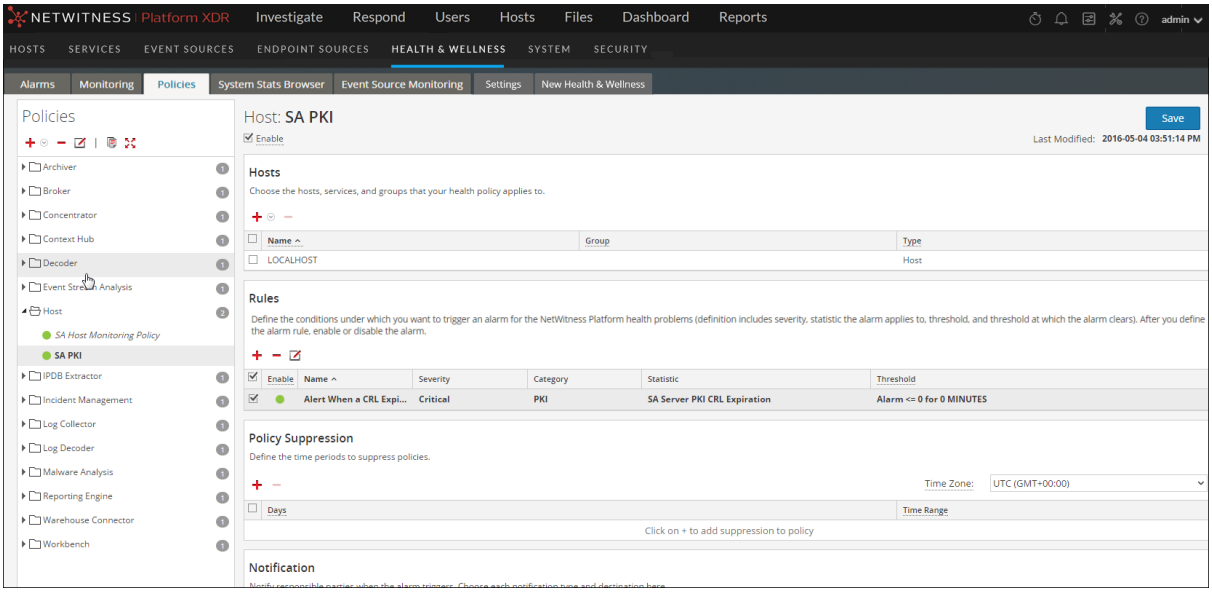
   f. Click **Save** in the Policy Detail panel.

      The Policy is added.

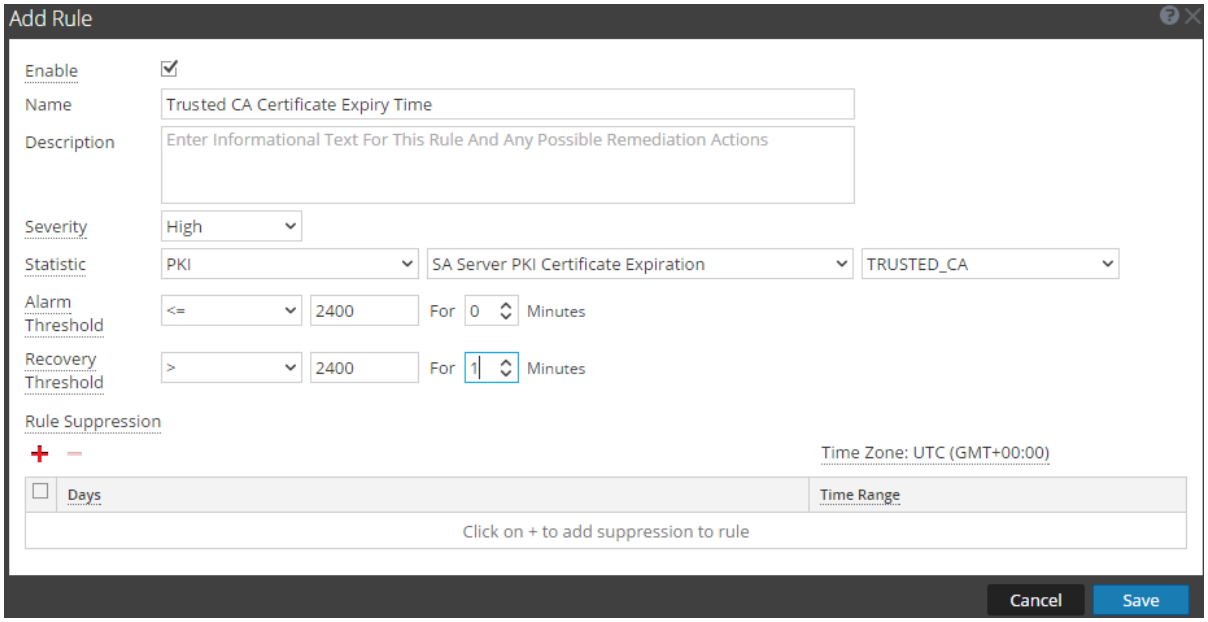
Add Policy Example

Below is a high-level example of configuring a PKI policy:

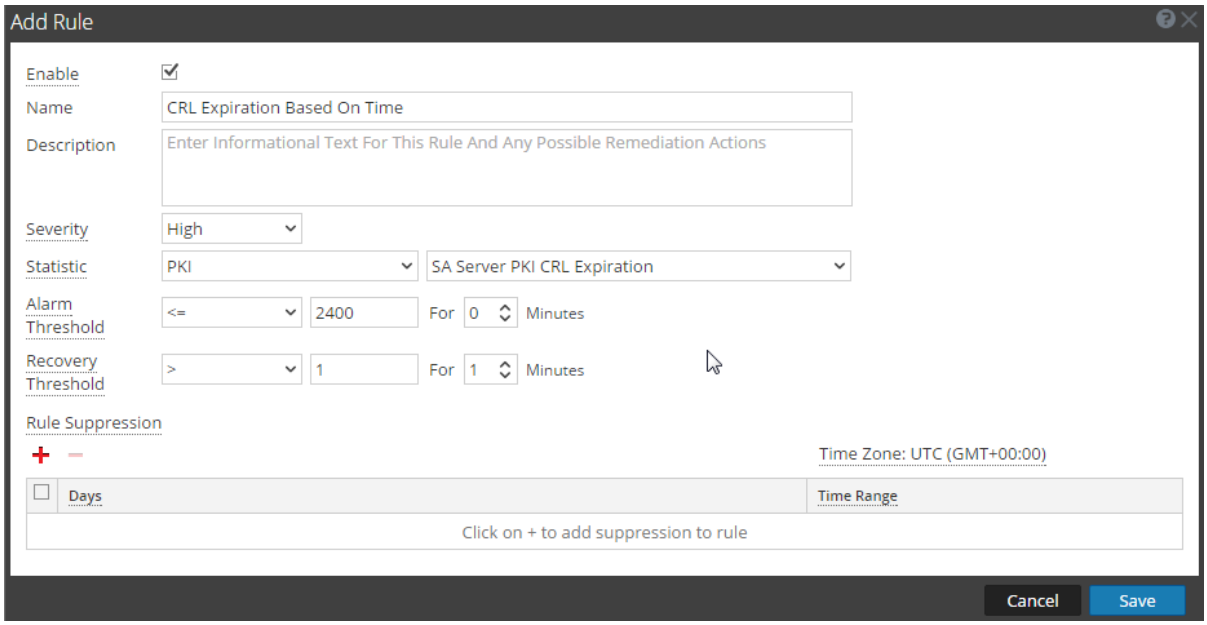
1. Add a new PKI policy.



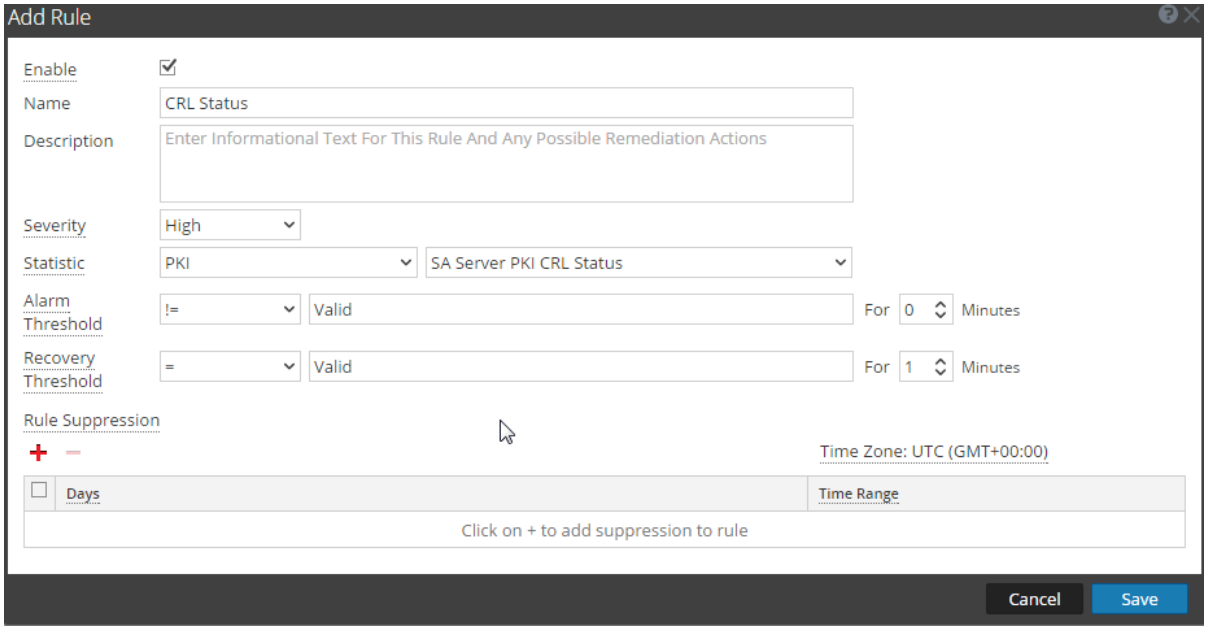
2. Add a Rule with Statistics:
   - For CA Expiration



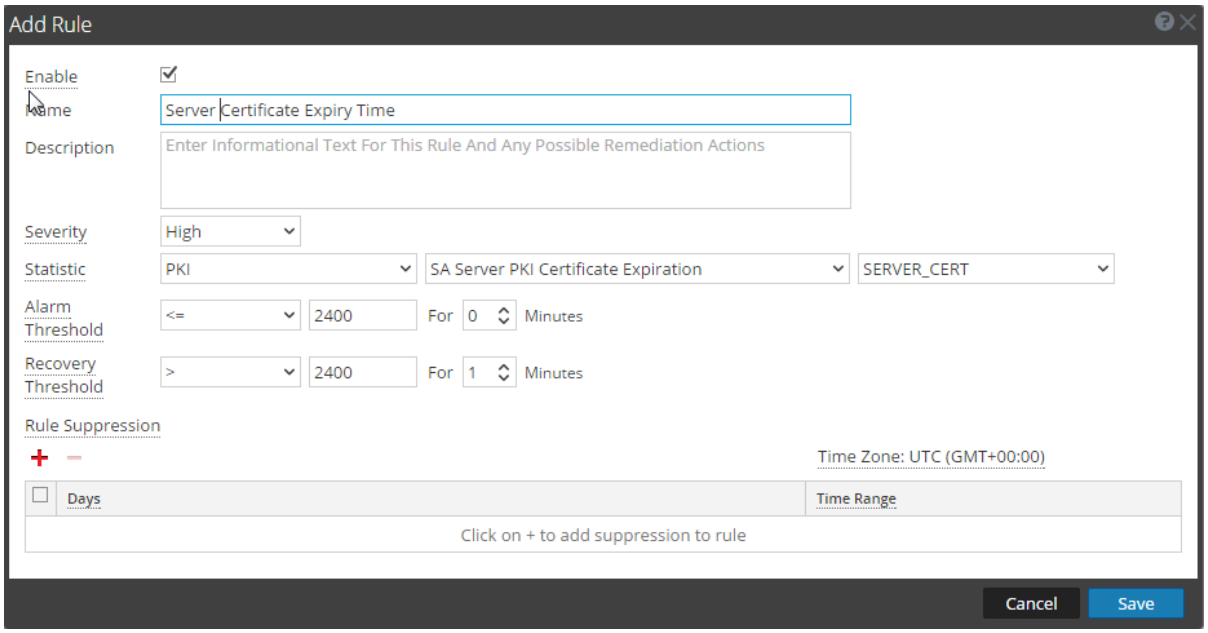
   - For CRL Expiration



- For CRL Status



- For Server Certificate Expiration



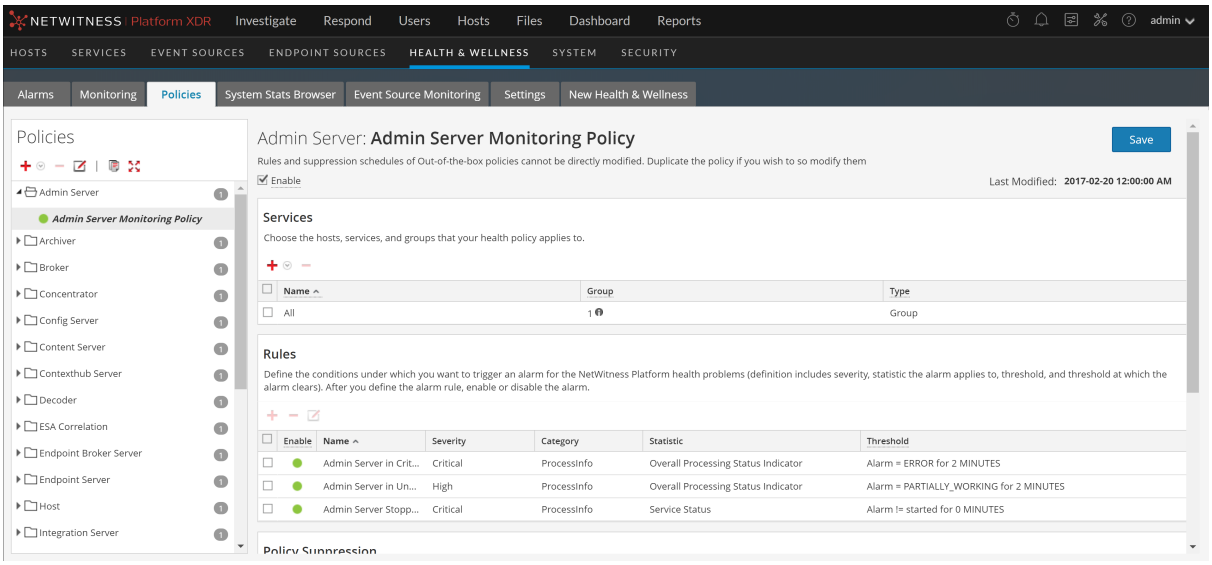
Edit a Policy

1. Go to **(Admin) > Health & Wellness.**
2. Click the **Policies** tab.

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

   The Policy Detail is displayed.
4. Click .

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

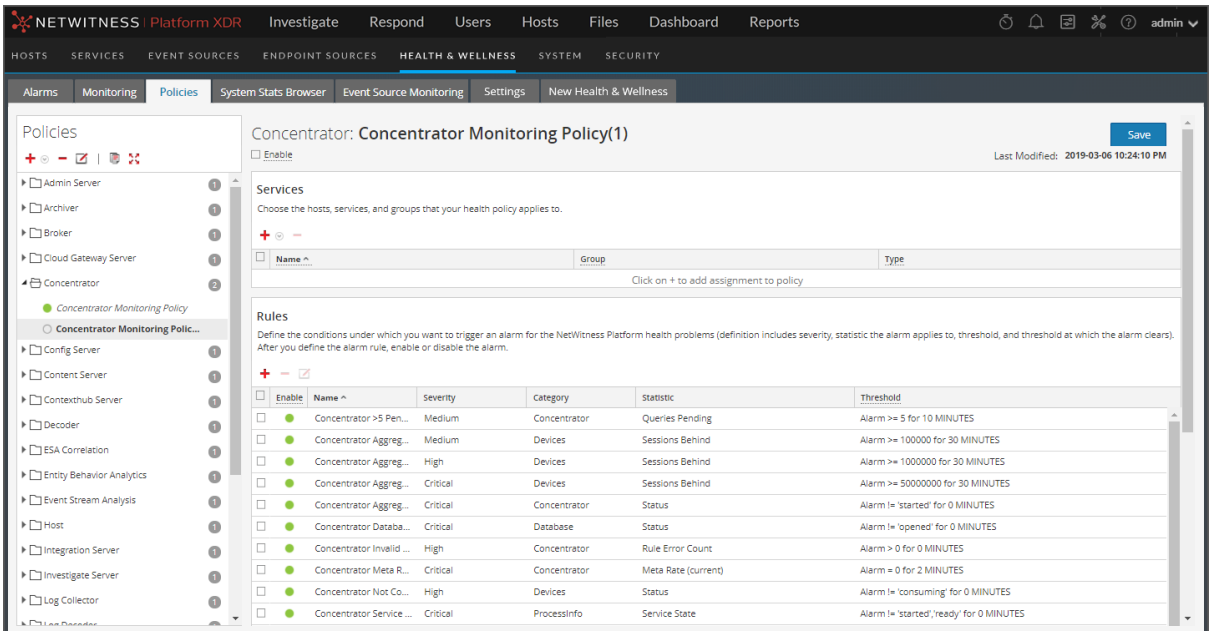


5. Make the required changes and click **Save** in the Policy Detail panel. You can:
   - Edit the policy name.
   - Enable or disable the policy.
   - Add or delete hosts and services in the policy.
   - Add, delete or modify rules in the policy.
   - Add, edit, or delete suppressions in the policy.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

Note: Save applies the policy rules based on the selection of enable or 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 Monitoring Policy**) under a host or service.
4. Click .NetWitness copies the policy and lists it with **(1)** appended to the original policy name.



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

> **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 infrastructure.

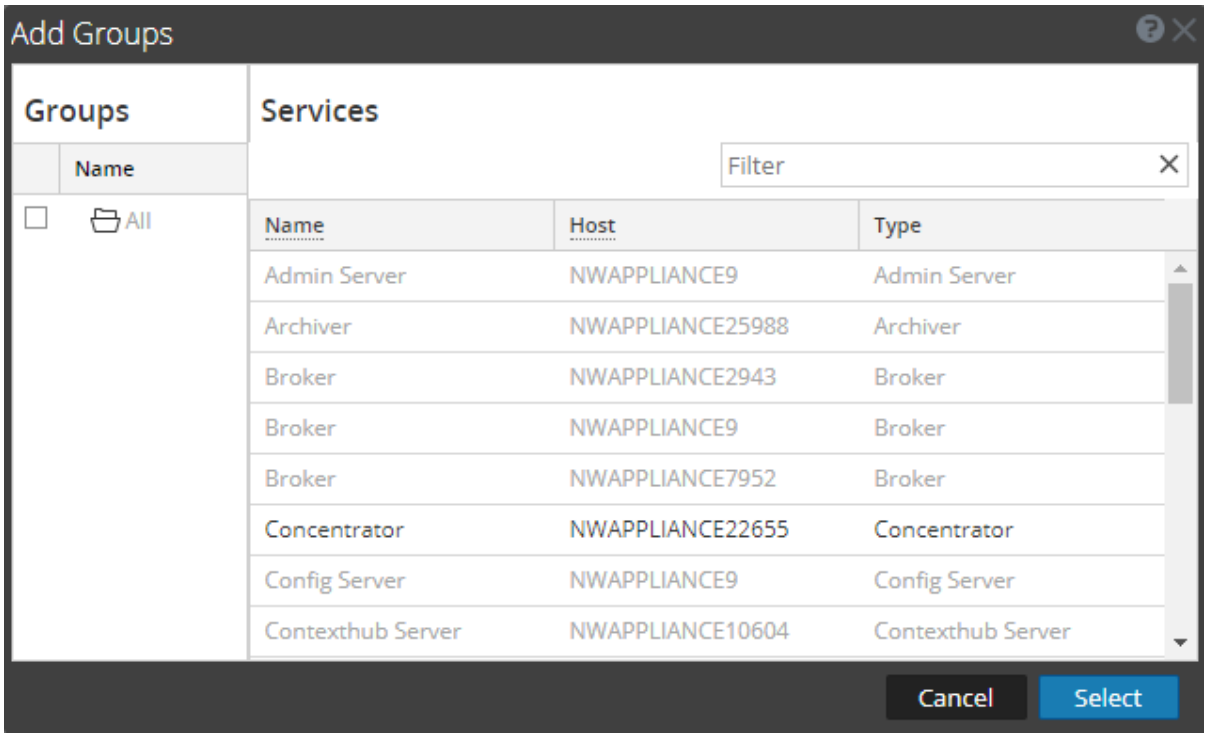
Assign Services or Groups

To assign hosts or services to a policy:

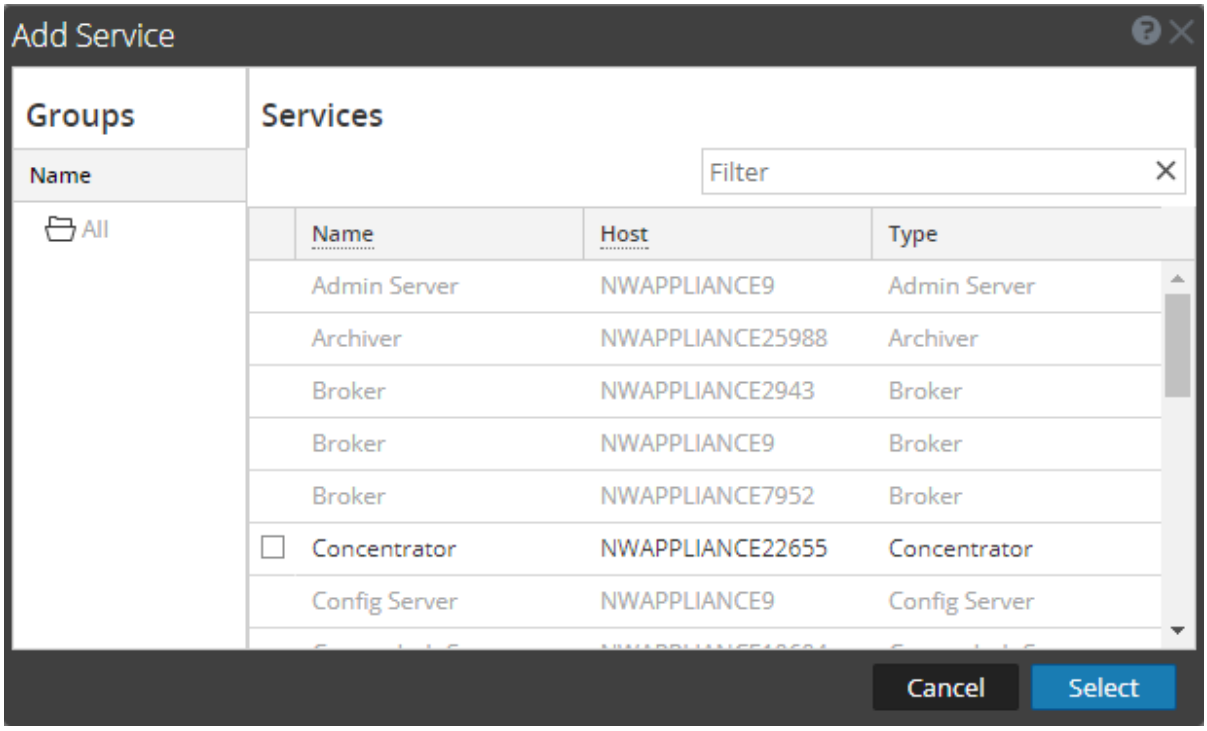
1. Go to **(Admin) > Health & Wellness.**
2. Click the **Policies** tab.

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

   The Policy Detail view is displayed.
4. Click in the Services and Groups list toolbar.
5. Choose one of the following actions:
   - For hosts, select **Groups** or **Hosts** from the selection menu.
   - For services, select **Groups** or **Services** from the selection menu.
6. Depending on whether you are assigning services or groups, perform one of the following actions:
   - **Groups**, the **Groups** dialog is displayed from which you can select predefined groups of hosts or services.



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



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

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

Remove Services or Groups

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 view is displayed.
4. Select a host or service.
5. Click .

   The host or service is removed from the policy.

Add or Edit a Rule

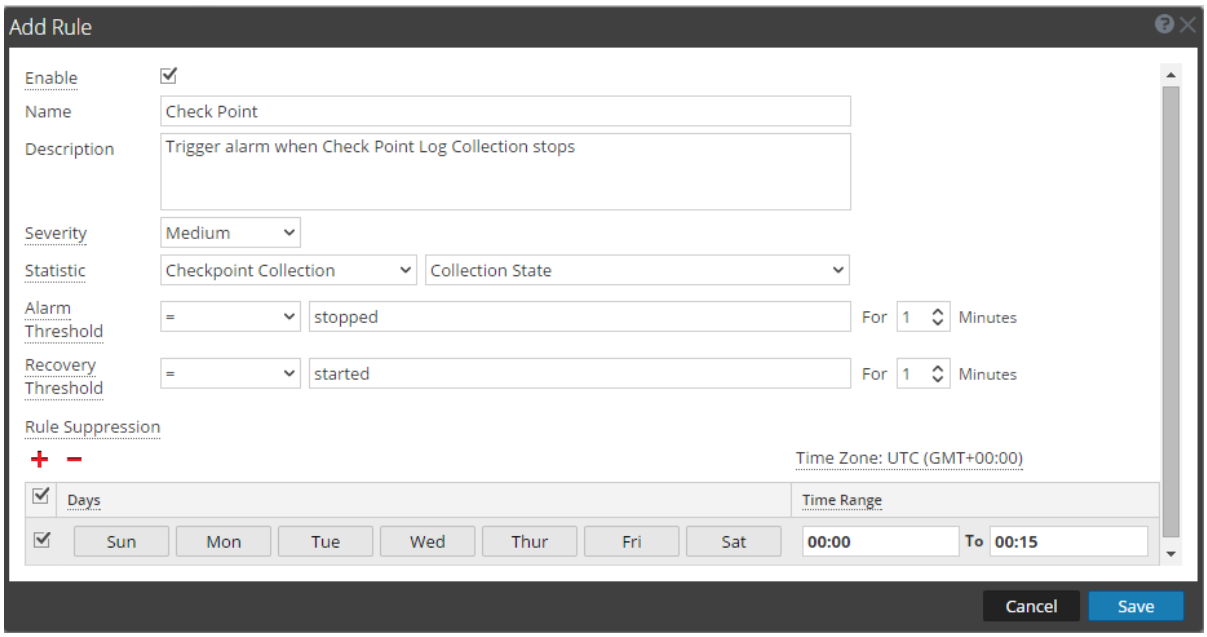
To add a rule to a policy:

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 view is displayed.
4. Depending on whether you are adding or editing rule, do the following:

   - To add a rule, click in the Rules list toolbar.
   - To edit a rule, select a rule from the Rules list and click .
5. Complete the dialog to define or update the rule.
6. Add a description as shown in the following example.



7. Click **OK**.

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

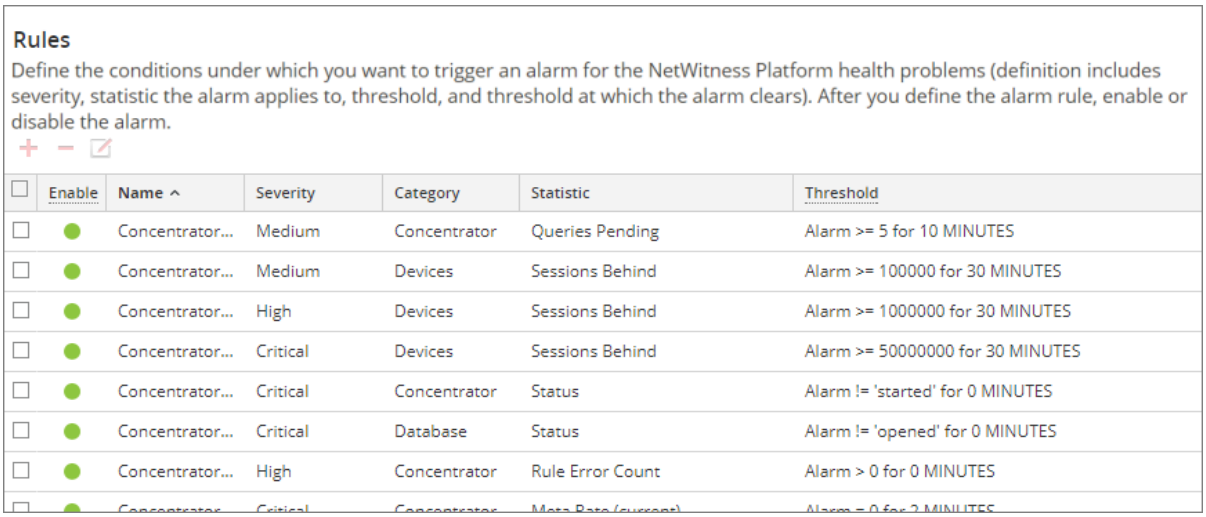
Hide or Show Rule Conditions Columns

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

1. Go to **(Admin) > Health & Wellness.**
2. Click **Policies** tab.

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

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



Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Platform 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

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

   You can set or clear 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 view 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 view 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 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 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 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.

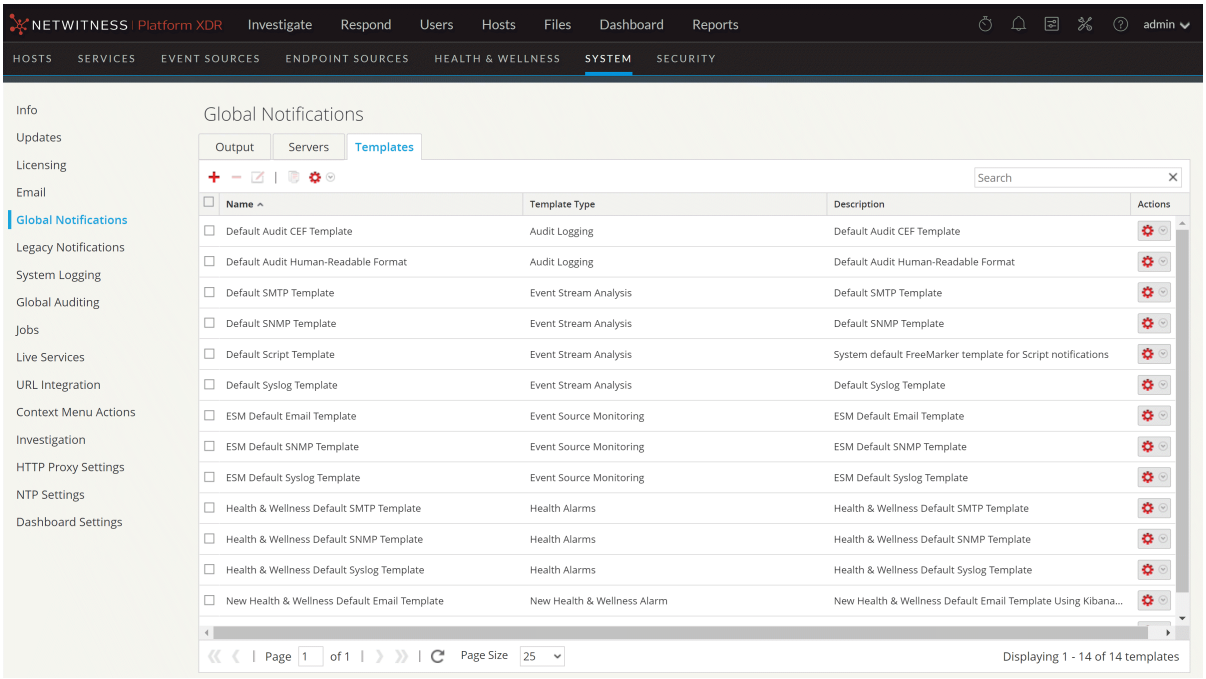
Include the Default Email Subject Line

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 Platform Out-of-the-Box Policies.

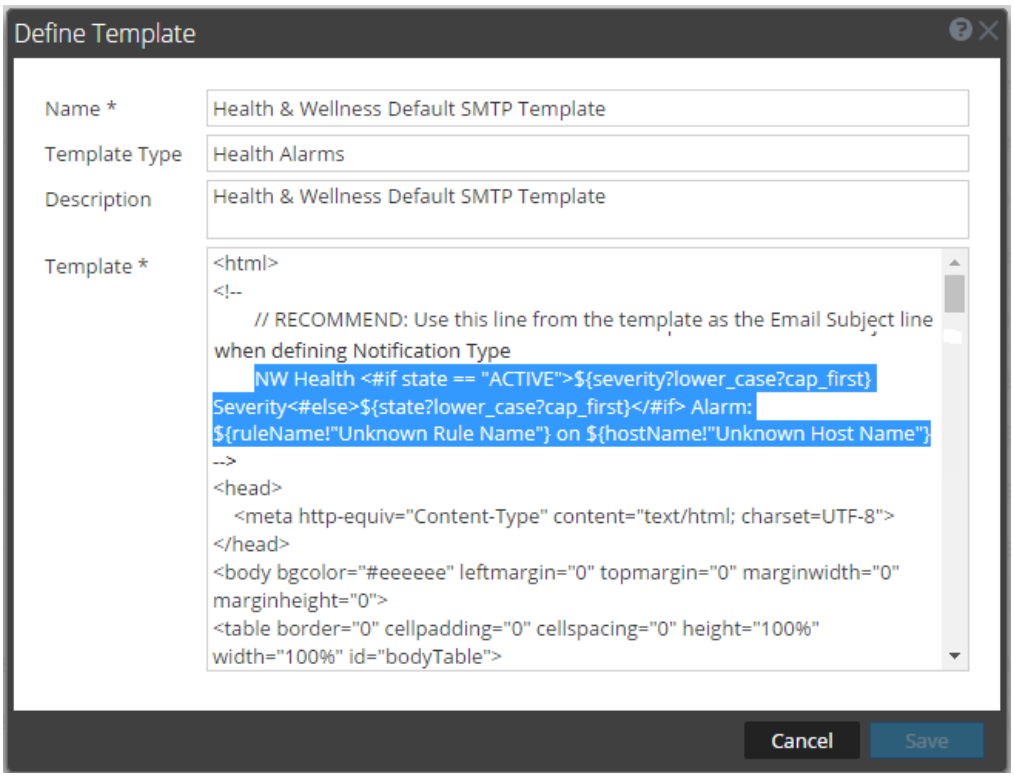
To include the subject line from a Health & Wellness email template in your email notification:

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



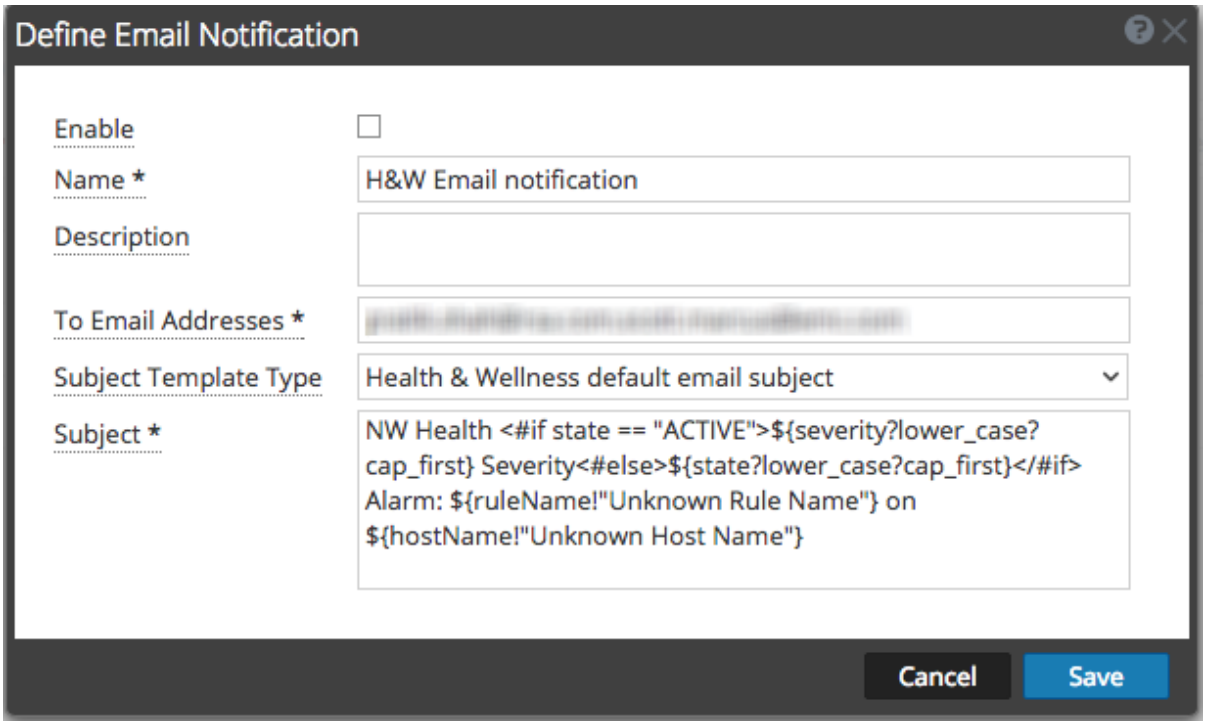
The Define Template dialog is displayed.

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



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

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


Define Email Notification
Enable
Name *
H&W Email notification
Description
To Email Addresses *
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"}
Cancel
Save

9. Click **Save**.

Monitor System Statistics

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

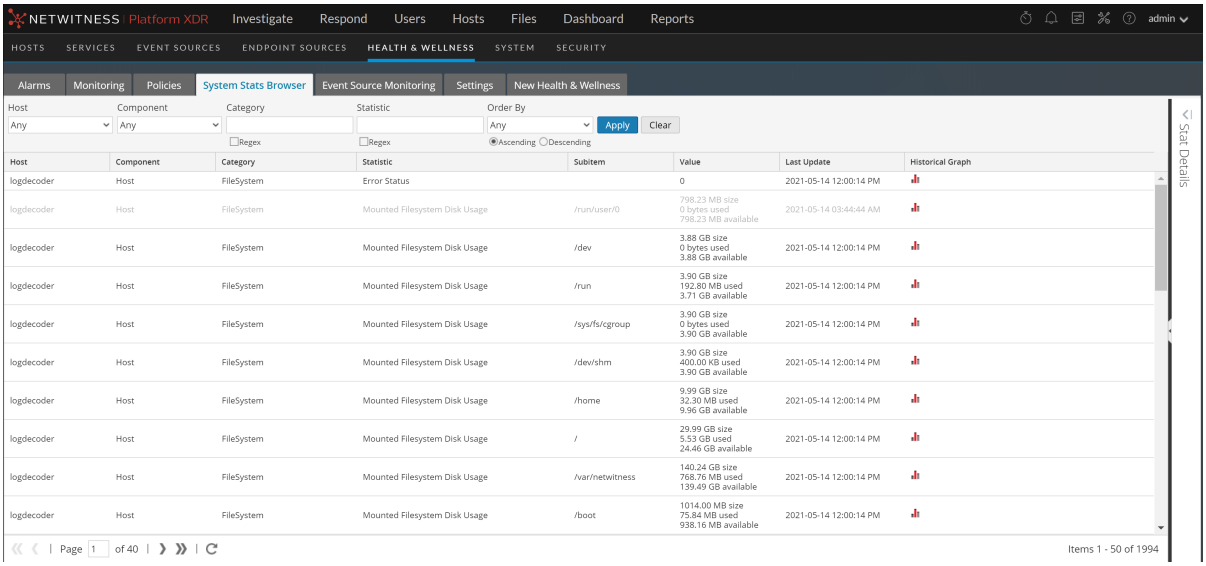
To access the System Stats browser:

1. Go to **(Admin)** > **Health & Wellness**.

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

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

   The System Stats Browser tab is displayed.



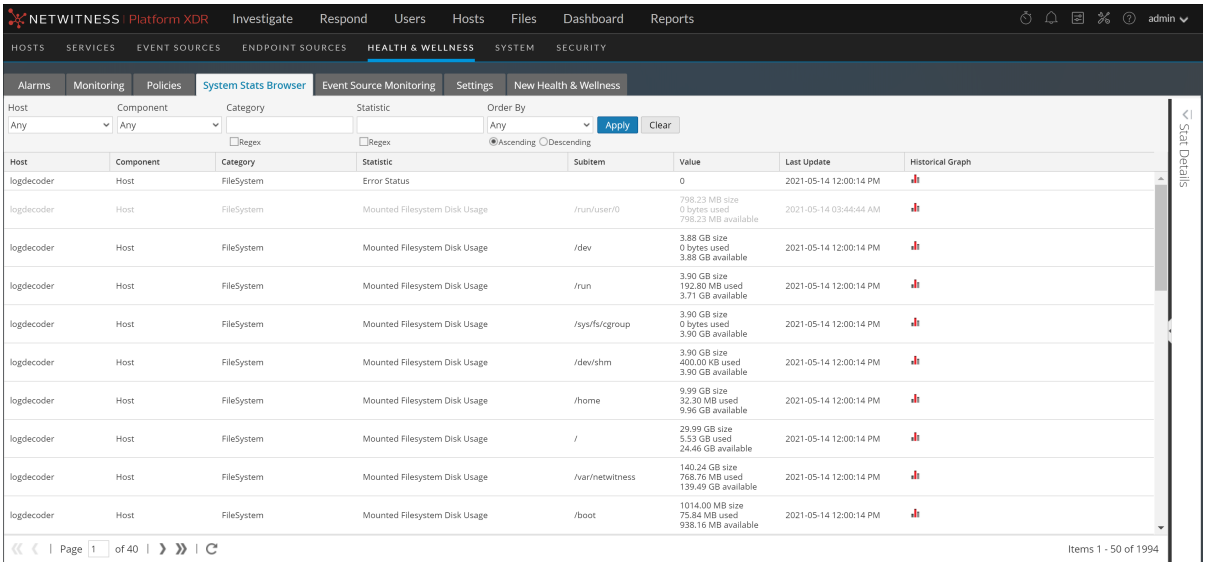
Filter System Statistics

You can filter system statistics to monitor:

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

To filter the list of system statistics:

1. Go to **(Admin) > Health & Wellness**.
   The Health & Wellness view is displayed with the Alarms tab open.
2. Click **System Stats Browser**.
   The System Stats Browser tab is displayed.

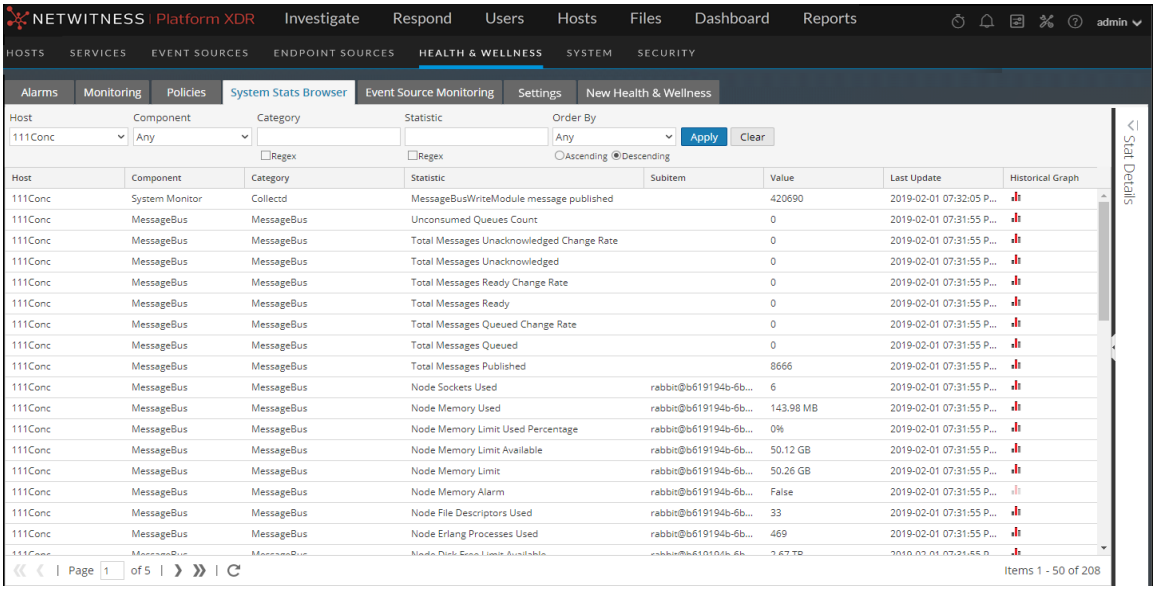


Filter the list of system statistics in one of the following ways:

- To view system statistics for a particular host, select the host in the **Host** drop-down list.
  The system statistics for the selected host is displayed.
- To view system statistics for a particular component, select the component in the **Component** drop-down list.
  The system statistics for the selected component are displayed.
- To view system statistics for a particular category, type the category name in the **Category** field. Select **Regex** to enable the Regex filter. It performs a regular expression search against text and lists the specified category. If Regex is not selected, it supports globbing pattern matching.
  The System Stats for the selected category is displayed.
- To list 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 the Regex filter. It performs a regular expression search against text and lists the specified category. If Regex is not selected it supports globbing pattern matching. The information for the selected statistics is displayed.

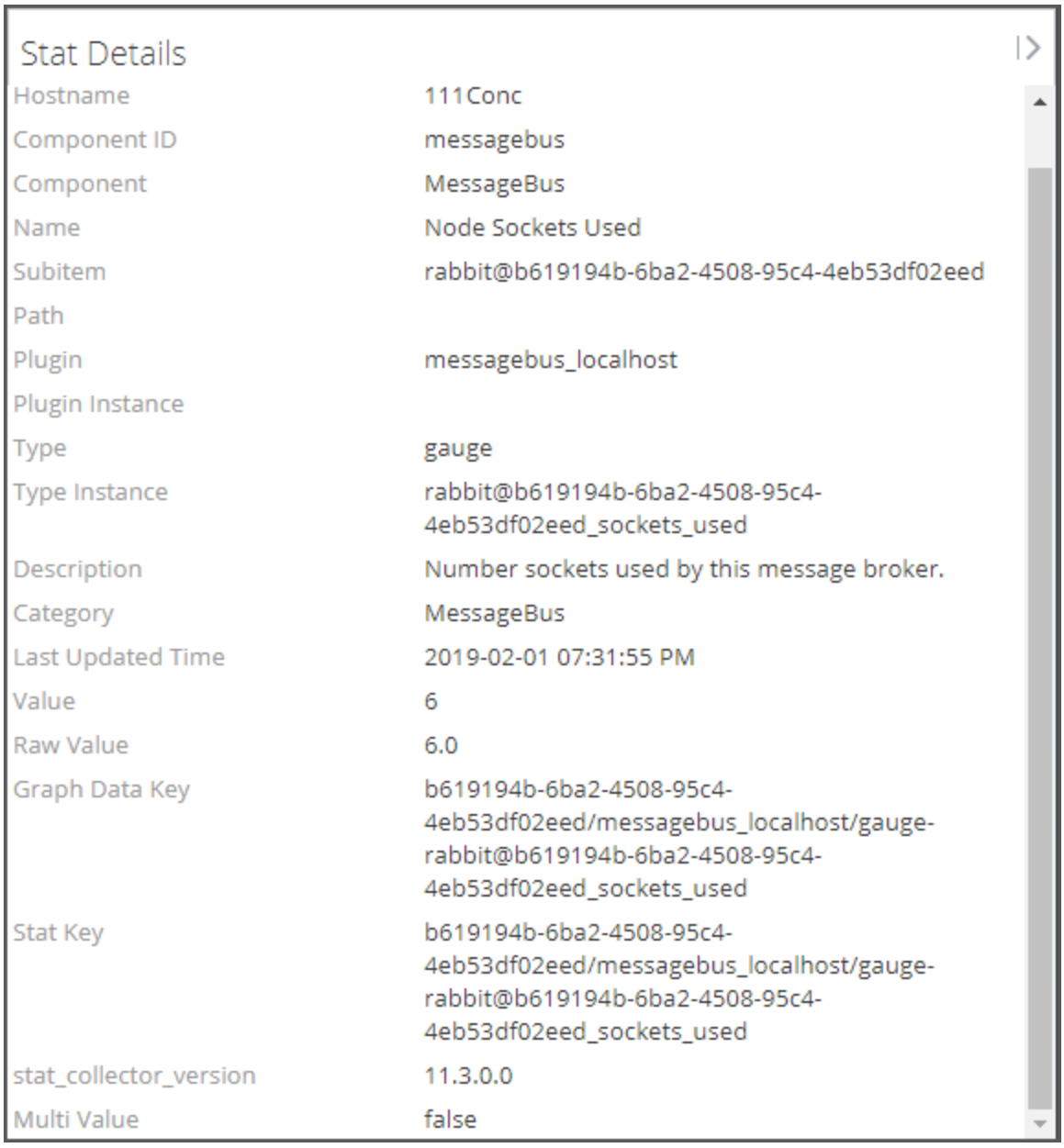
  The following figure shows the System Stats Browser filtered by the 111Conc host listed in descending statistical category order.



3. To view the details for an individual statistic:

   a. Select a row to select a statistic.

   b. Click .
   The Stat Details pane is displayed.



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

View Historical Graphs of System Statistics

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

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 the Memory Utilization statistic for a host.

   The graphical view is customized to display the statistics collected for the current day and the values are zoomed in for an interval of an hour (10.15 - 11.15 hrs). Hover over the graph to view the details at a particular instant. For example, in the figure it displays the memory utilization at 12.00 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 clicking and dragging 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 the chart line indicates that the service or host was down during that time.

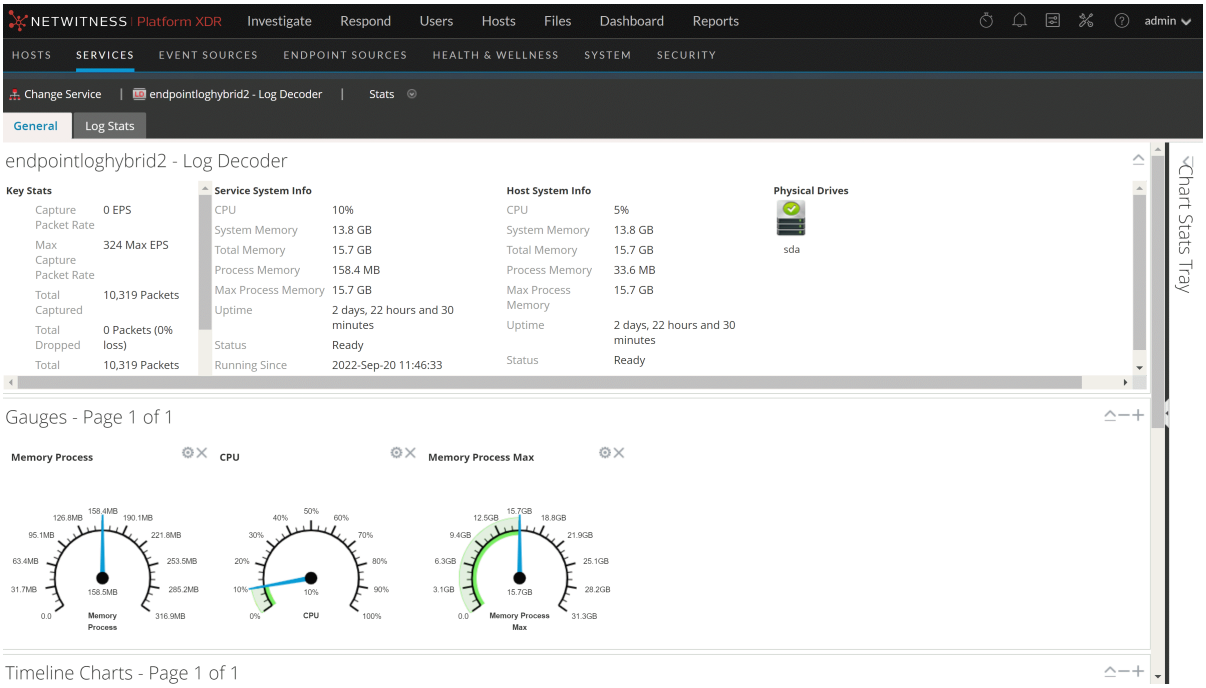
Monitor Service Statistics

NetWitness 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. 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:

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. Select a service, and select **View > Stats** in the Actions column.



3. To customize the view, collapse or expand charts. For example, expand the Chart Stats Tray to see available charts, and then drag a section up or down to change the sequence. Or, 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.

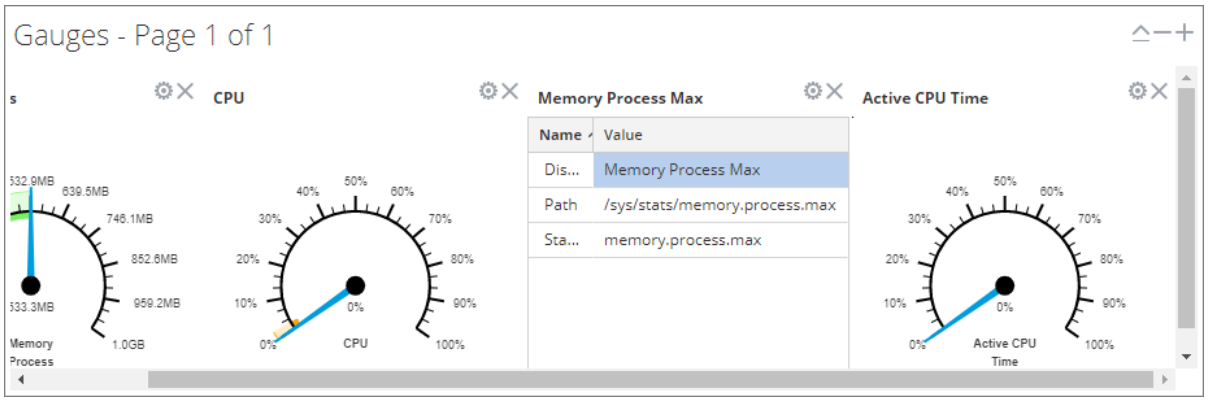
2. Select a service and select **View > Stats** in the Actions column.

   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 in the Gauges section and the gauge is added to the new page. In the example, the Active CPU Time chart was added to the Gauges section by dragging it from the Chart Stats Tray.

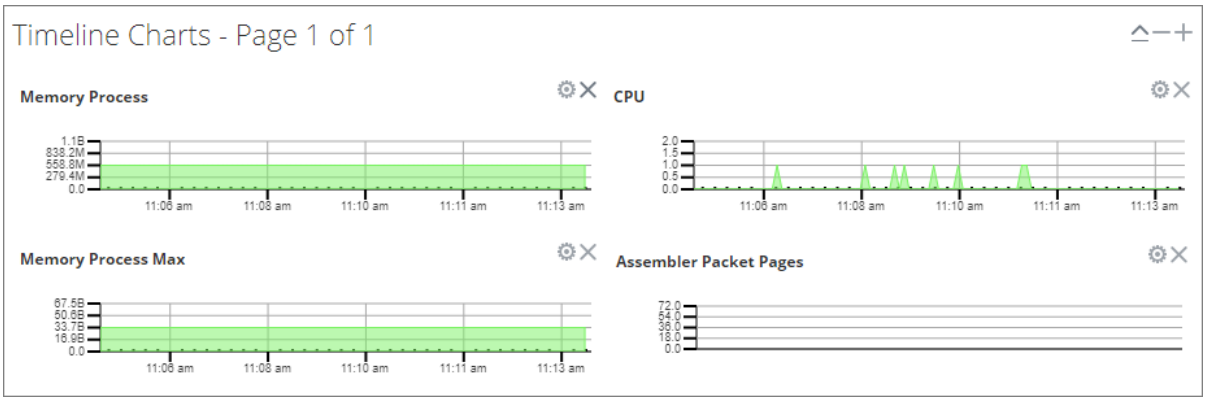


Create a Timeline Chart for a Statistic

To create a timeline for a statistic:

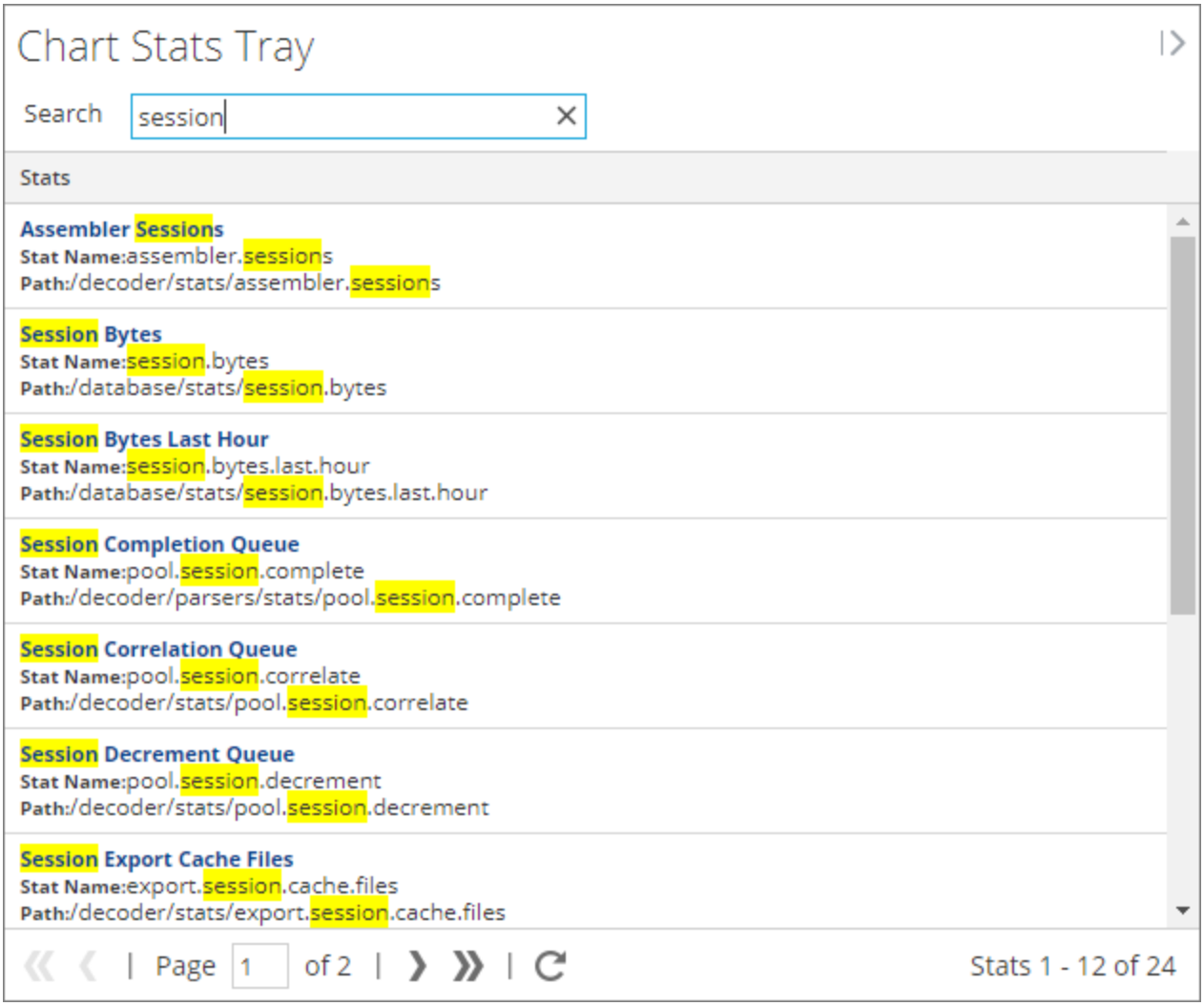
From the **Chart Stats Tray**, click on a statistic and drag it into the **Timeline Charts** or the **Historical Timeline Charts** section.

A timeline chart is created for the statistic. If there is no space for the chart, a new page is created in 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 **Enter**. Statistics that match are displayed with the matching word highlighted.

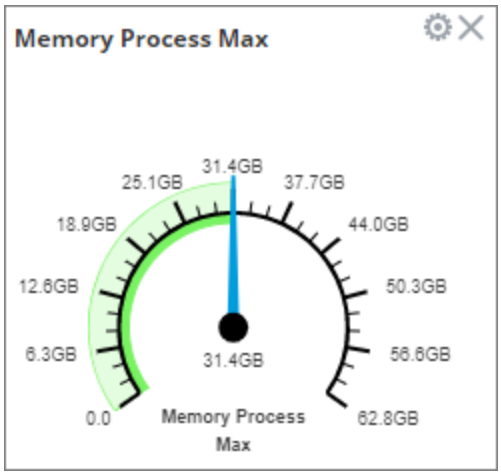


Edit Properties of Statistics Gauges

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

Edit Properties of a Gauge

1. Go to **(Admin) > Services**
   The Admin Services view is displayed.
2. Select a service and select **View > Stats** in the Actions column.
   The Service Stats view includes the Gauges section.
3. Go to the gauge for which you want to edit properties (for example, **Memory Process**).



4. Click the Properties icon ( ) to display the parameter names and values.
5. To highlight the value of the **Display Name** field, double-click on the value; for example, **Memory Process**.

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

6. 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:

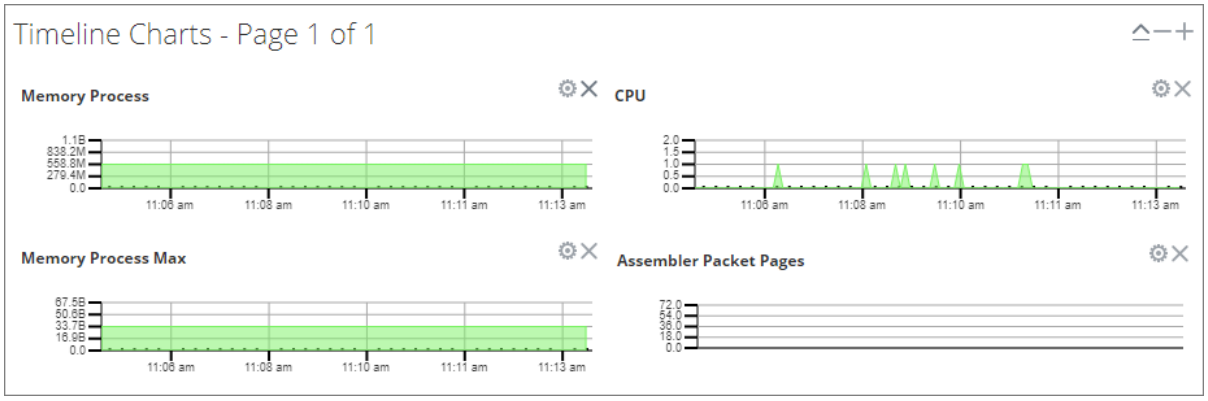
1. Go to **(Admin) > Services**.
2. Select a service and click **Stats**.

   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, **01/27/2019** 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.

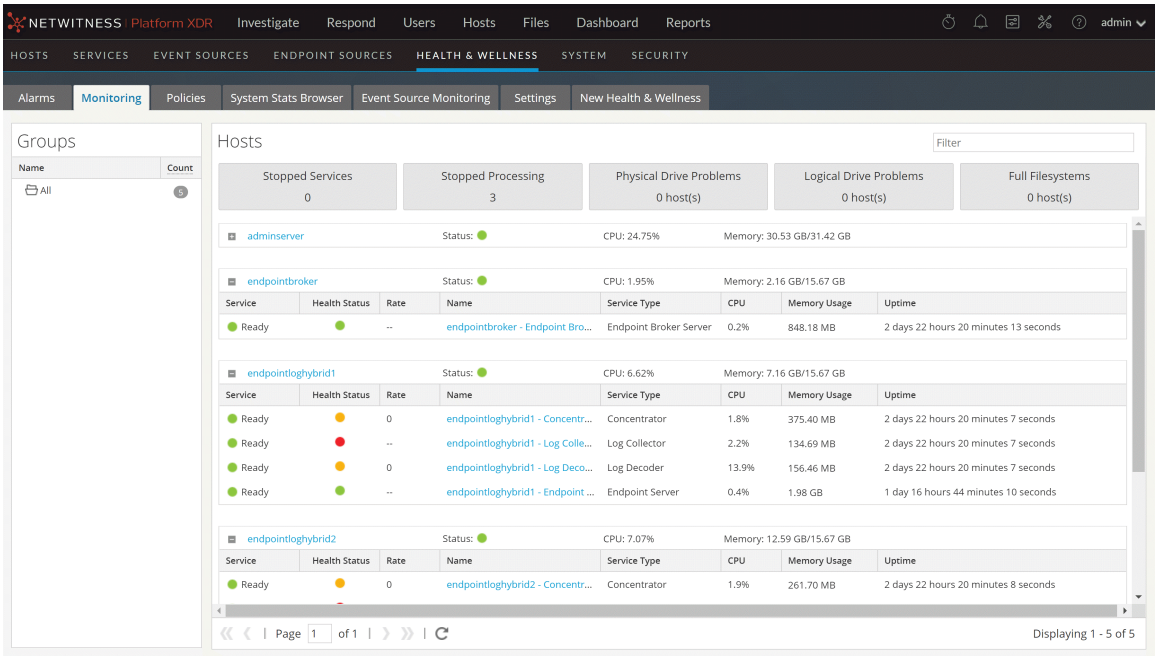
1. To expand the Chart Stats Tray, click .
2. Scroll down and select a statistic; for example, **Session Rate (maximum)**.
3. Drag the statistic to the **Timelines Section**.
   The new timeline is displayed in the Timelines section.

Monitor Hosts and Services

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

To monitor hosts and services in NetWitness:

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.



A list of services installed on the host is shown below the host. If you cannot see the services, click ⊞ to the left of a host to display the services.
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
- A 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.

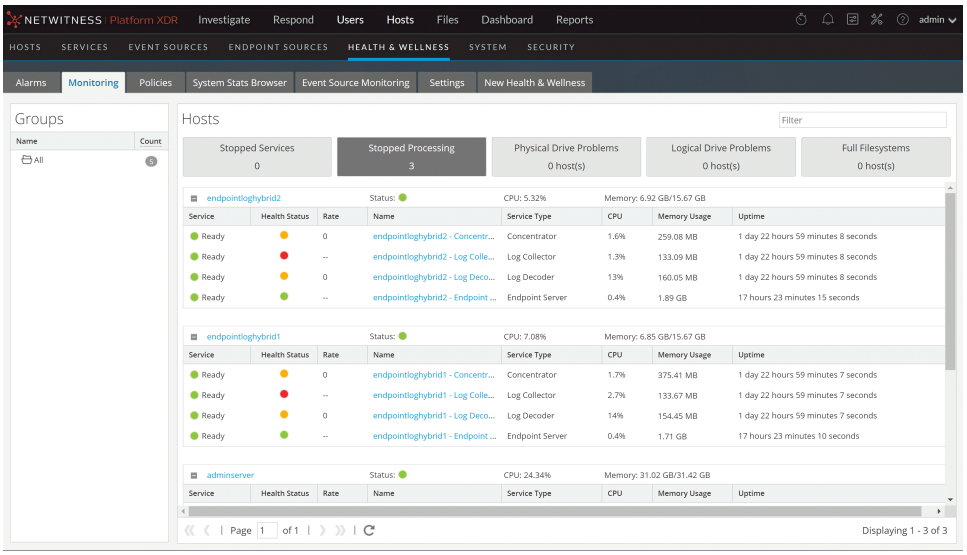
     All hosts and their associated services belonging to the specified group are displayed in the Hosts panel.

     Note: The grouping of hosts is derived from the groups created in the Admin Hosts view. All groups created in the Admin Hosts view 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 of the hosts configured in NetWitness and does not change with the application of filters on the groups.



- In a similar way, you can filter the list of hosts and the associated services by choosing the appropriate 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.

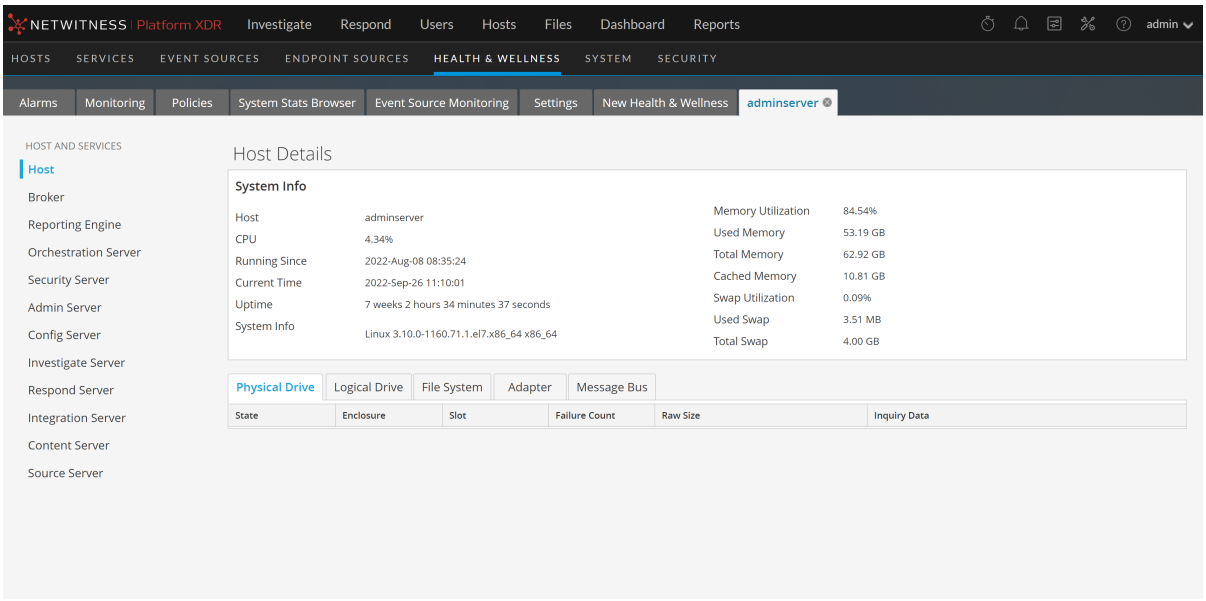
Monitor Host Details

You can view the details of a host, its memory and CPU usage, system information, physical drive, logical drive, and file system details to investigate potential problems with the host.

To view host details:

1. Go to **(Admin) > Health & Wellness > Monitoring** tab.
2. Click a host in the **Hosts** panel.

   The Host Details view shows important system information about the selected host, such as memory utilization and file system usage.



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.

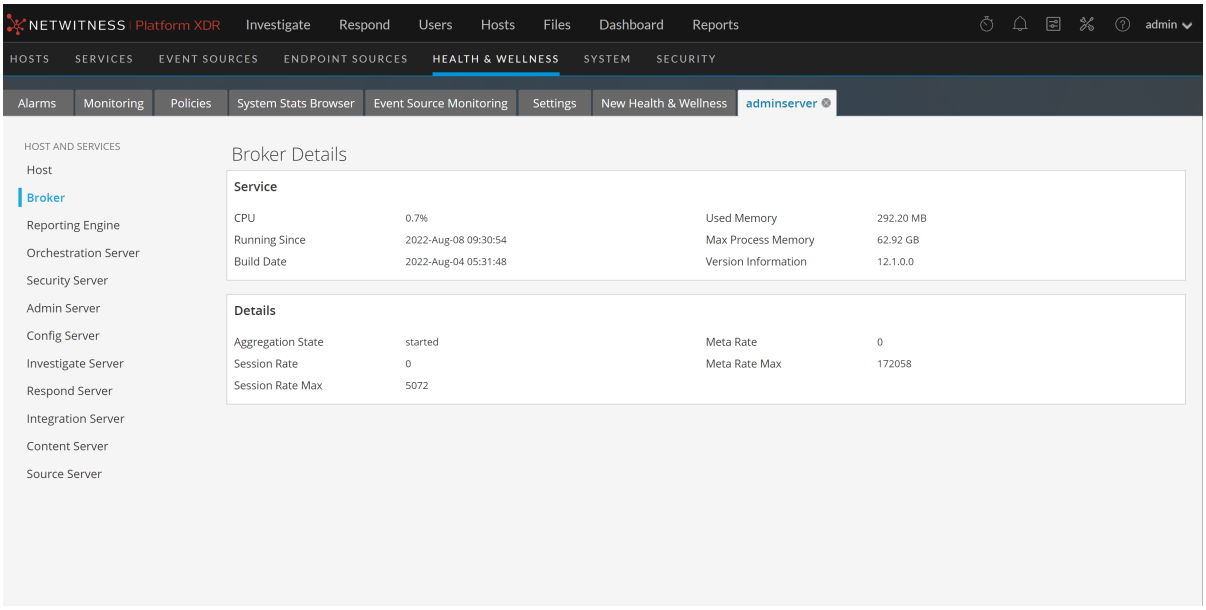
To view service details:

1. Go to **(Admin) > Health & Wellness > Monitoring** tab.

   The Hosts panel shows the services running on each host.

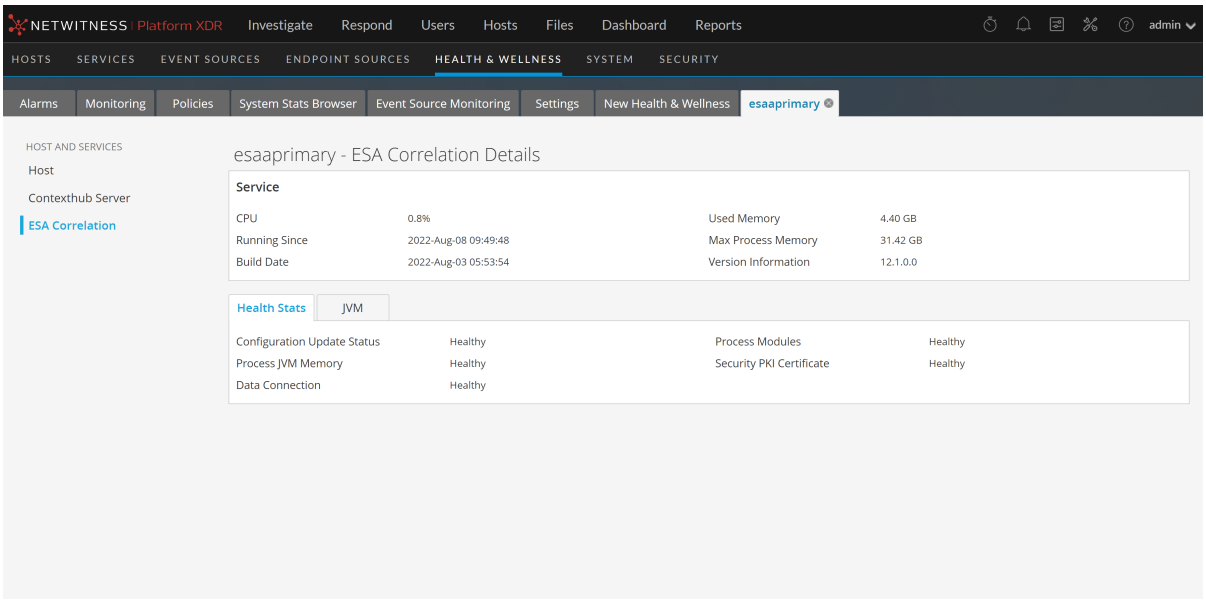
2. In the Hosts panel, click a service name link to get more information.

   The service details view shows the health status of the selected service. The Decoder service details include capture statistics and the Concentrator and Broker details include aggregation statistics.

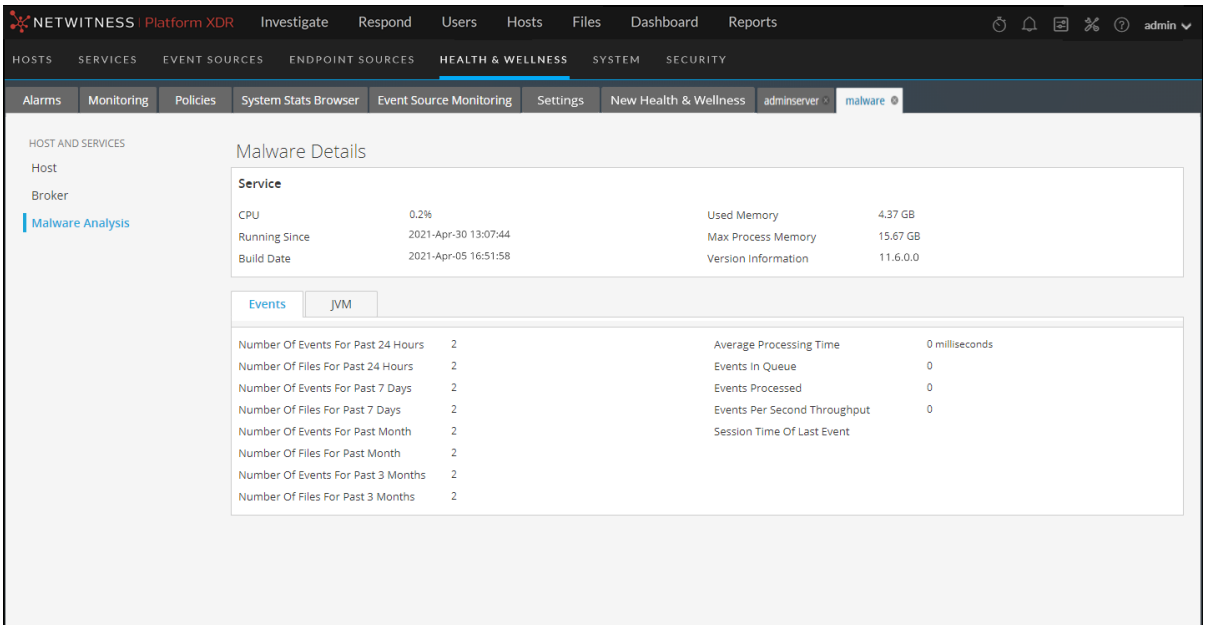


   Many services, including the ESA Correlation service, have a **Health Stats** tab that provides information about the health status of the service. The **JVM tab** shows the total memory used by the selected service and the total memory capacity of the host. For more information, see Health Stats Tab and JVM Tab.

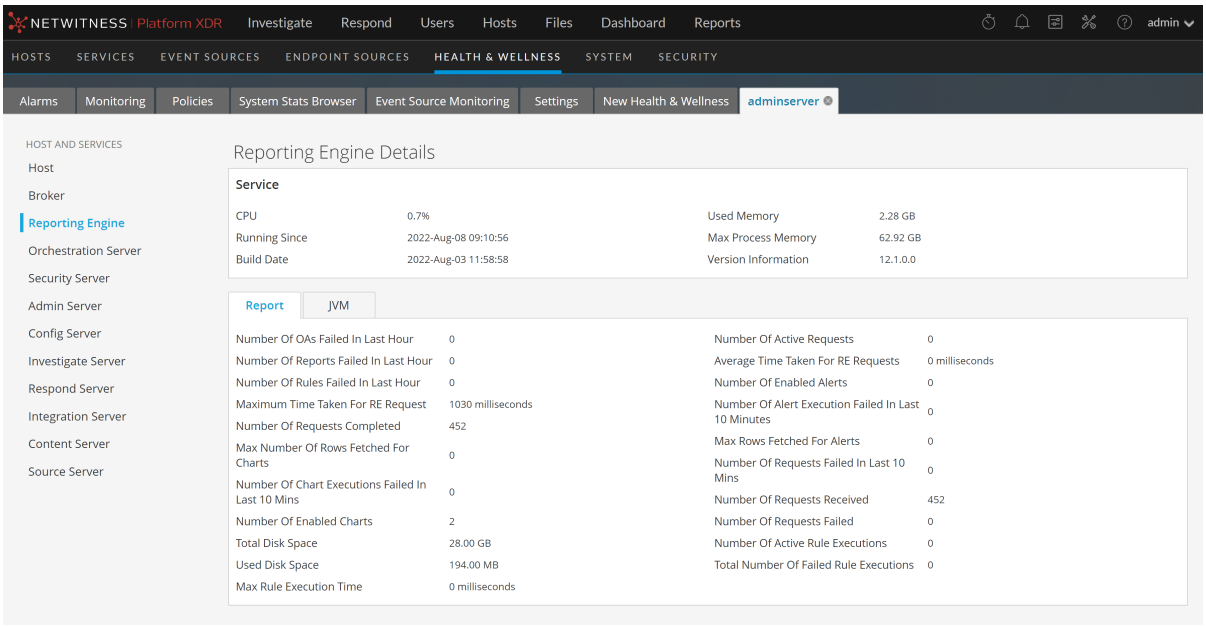
   For more information on the ESA Correlation service and ESA Rule memory usage, see the *Alerting with ESA Correlation Rules User Guide*.



The Malware Analysis service details view has **Service** information plus the **Event,** and **JVM** tabs that show additional statistics. The **Events** tab shows event processing statistics.



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



You can also view the details of other services by clicking the services listed in the options panel on the left.

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

Monitor Event Sources

Note: For NetWitness 11.4.1, this view has been deprecated. To manage Event Sources, use the (Admin) > Event Sources view. For details, see "About Event Source Management" in the*NetWitness Event Source Management Guide*.

Monitor Alarms

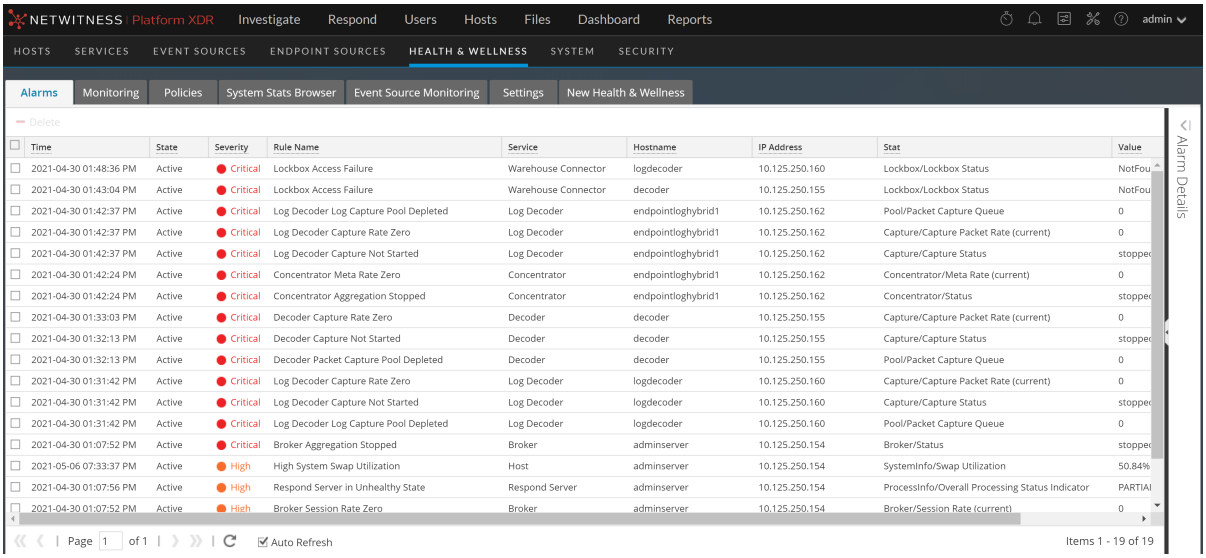
You can set up alarms and monitor them in the Health and Wellness interface for the hosts and services in your NetWitness domain. Alarms display in the view as **Active** when the statistical thresholds for hosts and services have been crossed. Alarms are grayed out and change to the **Cleared** status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

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

To monitor alarms:

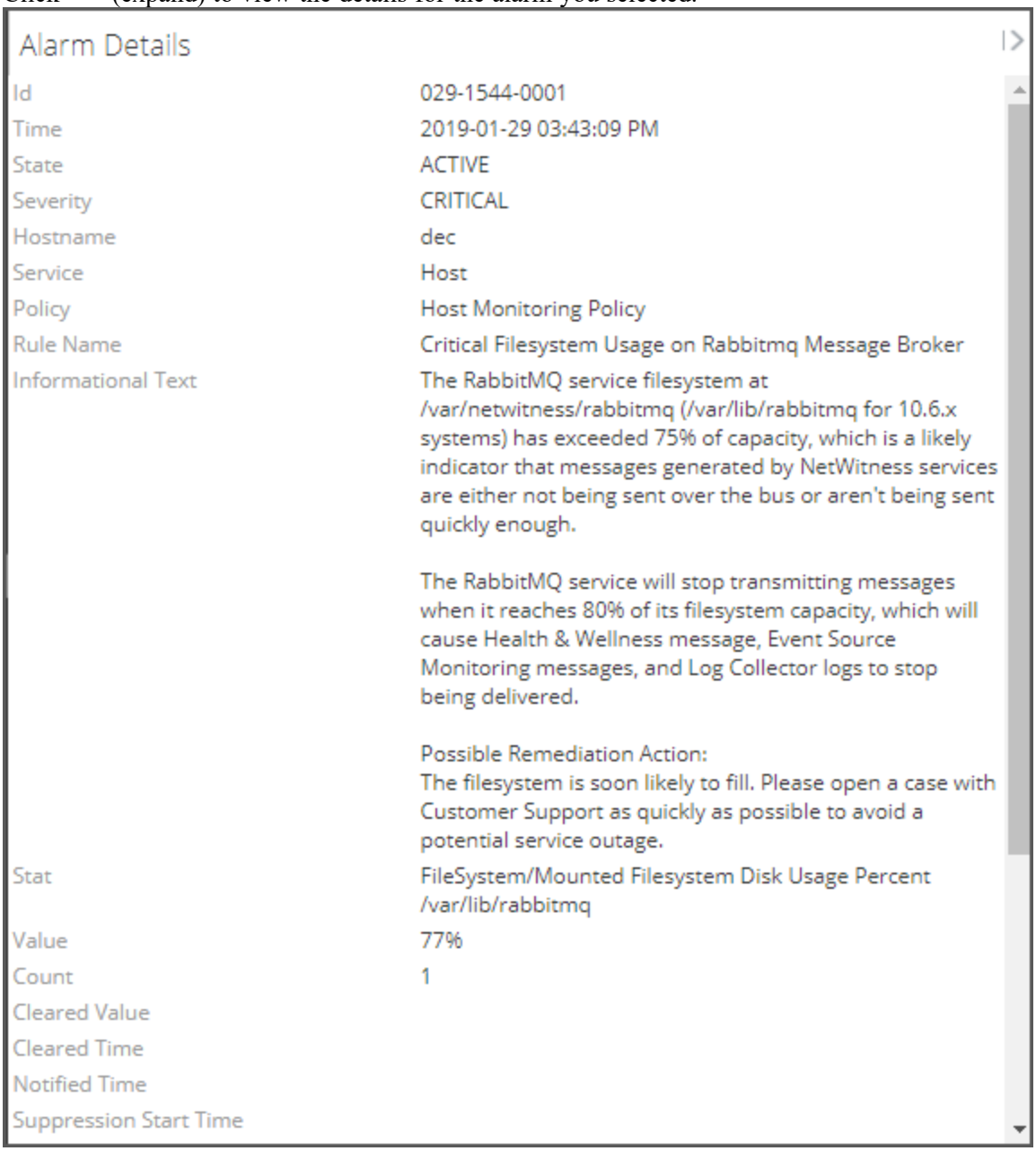
1. Go to **(Admin) > Health & Wellness**.

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



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

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



Monitor Health and Wellness Using SNMP Alerts

You can monitor a NetWitness component to proactively send alerts, using Simple Network Management Protocol (SNMP) that is based on thresholds or system failures.

You can monitor the following for NetWitness components:

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

SNMP Configuration

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

Thresholds

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

When the value of a statistic crosses either the low or high threshold, an SNMP trap is triggered, indicating that the threshold has been crossed. The trap is not 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.

This example shows a sample threshold for monitoring CPU usage (below 10% or above 90%):

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

This example shows how the threshold is set using REST API:

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

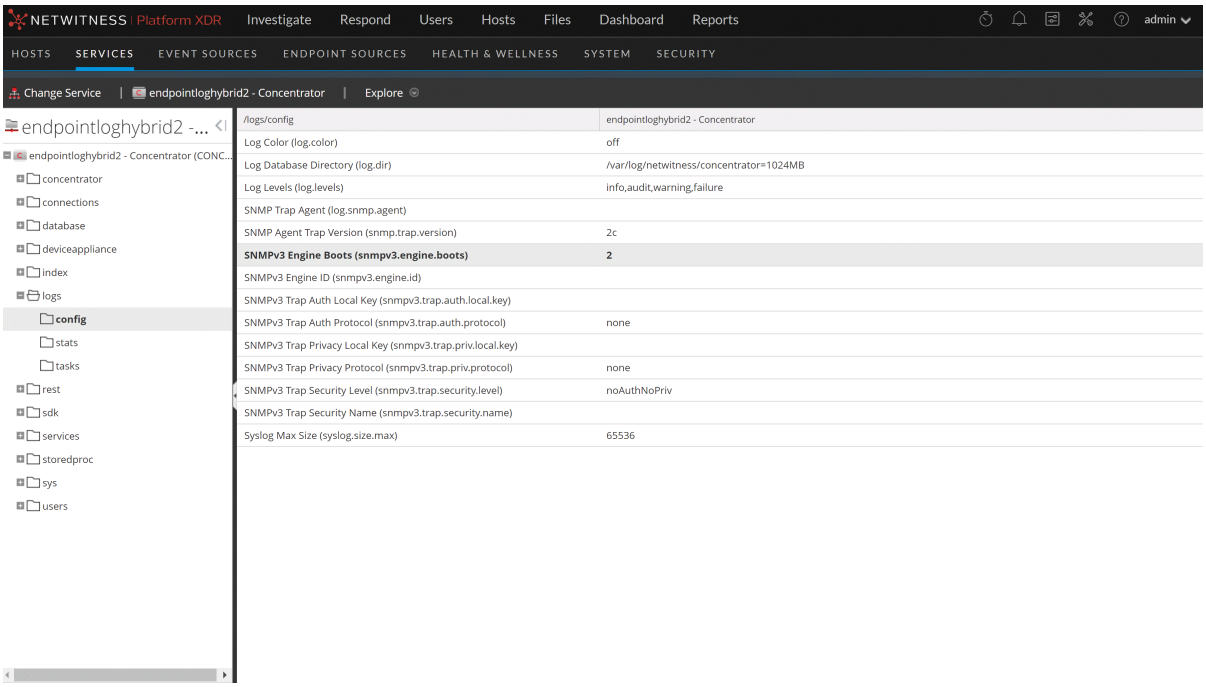
If the CPU usage spikes to 90% or higher, an SNMP trap is generated:

```
23435333 2018-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**.

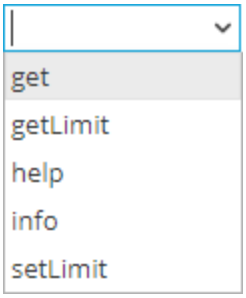
4. In the nodes list, expand the list and select a configuration folder. For example, **logs** > **config**
5. Set the SNMPv3 configuration.



Set the Threshold for a Service

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. Select the service.
3. In the Actions column, select **View > Explore**.
4. In the nodes list, expand the list and select a stat folder.
5. Select a stat, for example, CPU, and right-click.
6. From the drop-down menu, select **Properties.**

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



7. Select **setLimit**.
8. Specify the low and high values.

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 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 displayed in the Health & Wellness Interface or included 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 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 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 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

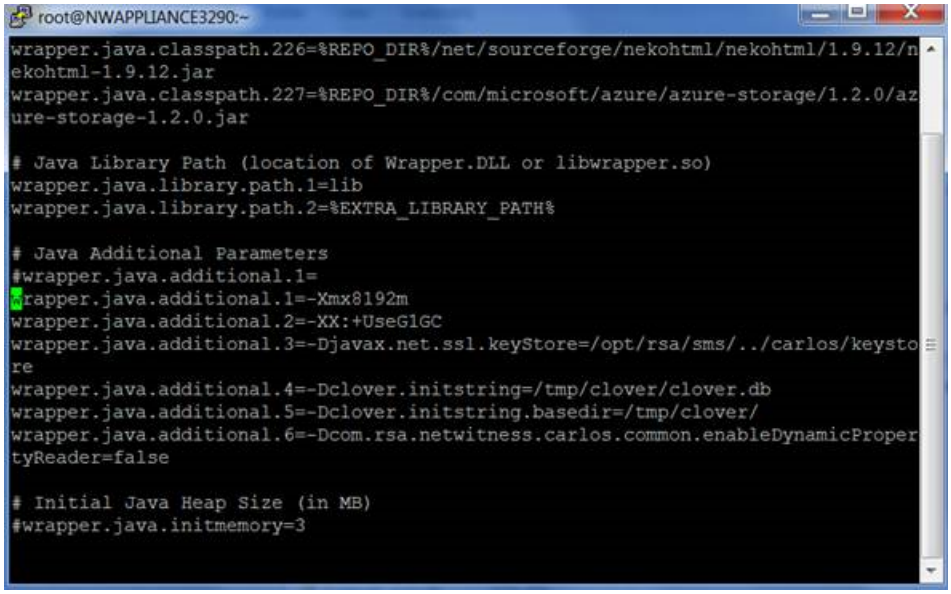
This section provides troubleshooting information for issues that are not identified by messages NetWitness displays in the Health & Wellness Interface or includes in the Health & Wellness log files. For example, you may see incorrect statistical information in the Interface.

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 does not show the version to which you upgraded until you restart jettysrv (jeTTy server).
Possible Cause	When NetWitness 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 displays the correct version.

Problem	NetWitness Server does not display the **Service Unavailable** page.
Possible Cause	After you upgrade to NetWitness 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 server cannot display the **Service Unavailable** page.
Solution	Restart jettysrv.

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



2. Replace `wrapper.java.additional.1=-Xmx16g` with:
   `wrapper.java.additional.1=-Xmx20g`
3. Restart the SMS service:
   `systemctl start rsa-sms`

Monitor New Health and Wellness

NetWitness New Health and Wellness is an advanced monitoring and alerting system that provides insights on the operational state of the host and services in your deployment, and helps identify potential issues. NetWitness Platform is prepackaged with a third-party tool that renders interactive dashboards and visualizations.

New Health and Wellness provides:

- Dashboards with interactive visualization.
- Easy-to-create customized content.
- Alerts on your data and customize alert conditions.
- Ability to add alert notifications (for example, Email and Syslog notifications).
- Ability to suppress alert notifications for a time period as required.

New Health and Wellness provides default content, such as dashboards, visualizations, and monitors, to set up monitoring and alerting.

Please direct any New Health and Wellness feedback to nw.health.wellness.feedback@rsa.com.

Dashboard

The dashboard is a collection of intuitive visualizations for the administrator to monitor the health of the host and services, identify trends, track performance, and drill down to specific details.

After installation of the New Health and Wellness service, the following default dashboards are available to begin monitoring.

- Deployment Health Overview dashboard
- Hosts dashboard
- Logs dashboard
- Packets Overview dashboard
- Analysis dashboard
- Endpoint dashboard
- ESA Correlation Overview dashboard

For more information on the dashboards, see New Health and Wellness Dashboards .

Visualization

A visualization is a graphical representation of data in your deployment. You can create new visualizations or use the existing visualizations to build dashboards. Depending on the visualization you select the data is displayed in the dashboard.

Monitors

A monitor is a job that runs on a defined schedule, which queries Elasticsearch to evaluate the system health. You can define one or more triggers for a monitor and assign a severity level based on the threshold. When one or more trigger conditions are met, New Health and Wellness generates an alerts. You can create new monitors or customize the existing monitors based on your requirement.

Notifications

Notifications can be sent when health alerts are generated, for example, email and syslog notifications.

If you do not want to receive notifications, you can suppress them for a time period. For example, if you want to suppress low-severity alerts during weekends, you can do so by specifying a suppression policy.

After the suppression time period, the notifications will be sent for the alerts triggered during the suppression time.

Installing New Health and Wellness

You can deploy the New Health and Wellness feature on any one of the following, listed in the order of preferred deployment method with most preferred first:

- Standalone virtual host (Most preferred recommendation to ensure no performance impact on any other functionality of deployed nodes)
- Physical machine:
  - Broker
  - Admin Server
  - ESA

Installing New Health and Wellness enables all hosts and services in your deployment to start sending metrics for monitoring. For more information on installing New Health and Wellness, see the "Deployment Optional Setup Procedures" topic in the *Deployment Guide*.

Accessing New Health and Wellness Dashboards

After you deploy New Health and Wellness, you can access New Health and Wellness dashboards. By default, only Administrator can access New Health and Wellness dashboards. Other roles do not have permission to view New Health and Wellness dashboards.

To access New Health and Wellness dashboards:

1. Log in to NetWitness Platform.
2. Go to **(Admin) > Health & Wellness.**
3. Click **New Health & Wellness**.
4. Click **Pivot to Dashboard**.

Note: To view dashboards, your browser must be configured to allow popups and redirects.

Configuring Notifications

You can choose to receive notifications of alert, when an alert (monitor) is triggered. You can configure the following types of notifications for the alerts.

- Email
- Syslog

To set up notifications, you must configure the following :

- **Notification Server**: This is the source of the notifications and must be configured to specify the Email or Syslog server settings.
- **Notifications Output**: This is the notification type, namely Email or Syslog. When you set up a notification, you must specify the notification output for an alert.
- **Templates**: The message format of an alert notification is defined using template. Default template is available for New Health and Wellness notifications or you can create new templates.

Adding Alert Notifications

To add notifications such as email or syslog, you must specify the notification details as follows:

- Output Type
- Recipient
- Notification Server
- Template

Note: You must ensure that the notification server and template is configured before you set up the notifications. You can use an existing server if required. For detailed procedures, see the *System Configuration Guide*.

To add a notification:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Click **View Notifications Settings**.
4. Specify the following:
   - **Output Type -** Notification type such as Email or Syslog.
   - **Recipient** - Select the recipient based on the output type selected.
   - **Notification Server** - Select the server that will send the notification. If you want to add a new notification server, see "Configure Notification Servers" in the *System Configuration Guide*.
   - **Template** - Notification template such as Email or Syslog.
5. If you want to add another notification, click **Add Condition** and repeat step 4.

Note: You can specify a maximum of four conditions in the notification settings.

6. Click **Save**.

Suppressing Notifications

You can suppress notifications for a time period by specifying a suppression policy. For example, you do not want to receive notifications of low-severity alerts during peak hours or weekends. This ensures that notifications are not sent during the selected time period. The notifications triggered during this time period will be sent after the suppression period.

A suppression policy consists of condition that defines the day and time range for suppressing a notification.

Note: You can specify a maximum of seven conditions in the policy.

To suppress alert notification:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. In the **New Health & Wellness** tab, do anyone of the following:
   - Select the alert or alerts for which you want to apply a suppression policy.
   - Select all to apply a suppression policy to all alerts.
   - Filter alerts on **suppression applied**, **monitor name**, **trigger name**, and **severity** and apply the suppression policy.
4. Click **View Suppression Policy**.
   The policy suppression dialog is displayed.
5. Specify the days and time range during which you want to suppress the notification.

Note: Time range is based on the Time Zone configured in the User Preferences panel as described in "Setting User Preferences" in the *Getting Started Guide*.

6. To add an additional suppression policy, click **Add condition** and repeat step 5.

Note: The maximum number of suppression policy supported for an alert is seven, after which the **Add Condition** option is disabled.

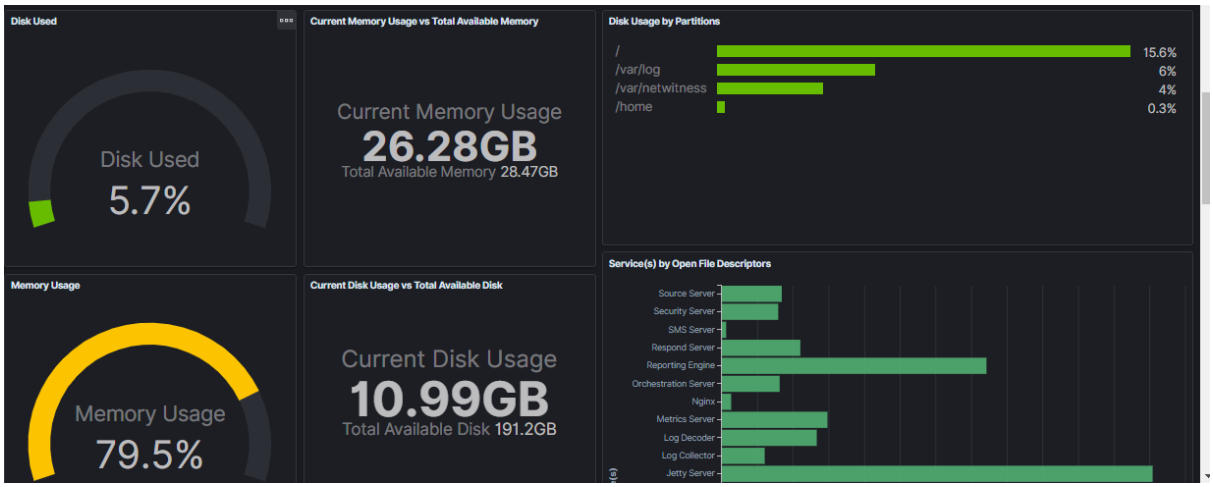
7. Click **Save**.

Monitoring through Dashboards

For a thorough analysis of the health of NetWitness Platform hosts and services using the different dashboards, you can pivot to dashboard without any additional authentication. By default, the last 6 hours of data is displayed in the dashboard. For more information on the default dashboards, see New Health and Wellness Dashboards.

To monitor through the dashboard:

1. Go to **(Admin) > Health & Wellness**.
2. Click **New Health & Wellness**.
3. Click **Pivot to Dashboard**.
   The Deployment Health Overview dashboard is displayed.
4. Go to > **Dashboard** to view all the available dashboards.
5. Select the dashboard you want to view.
6. Click the dashboard link. For example, Hosts.
   Once the dashboard view is displayed you can look at the visualizations (charts, tables, and so on) to view current disk usage of hosts, incoming and outgoing traffic of the host, active queries on a service, and so on.



7. You can adjust the time range on the top right corner and apply filters to view the statistics.

Creating a Custom Dashboard

You can create a new dashboard by adding one or more existing visualizations or a new visualization.

To create a new dashboard:

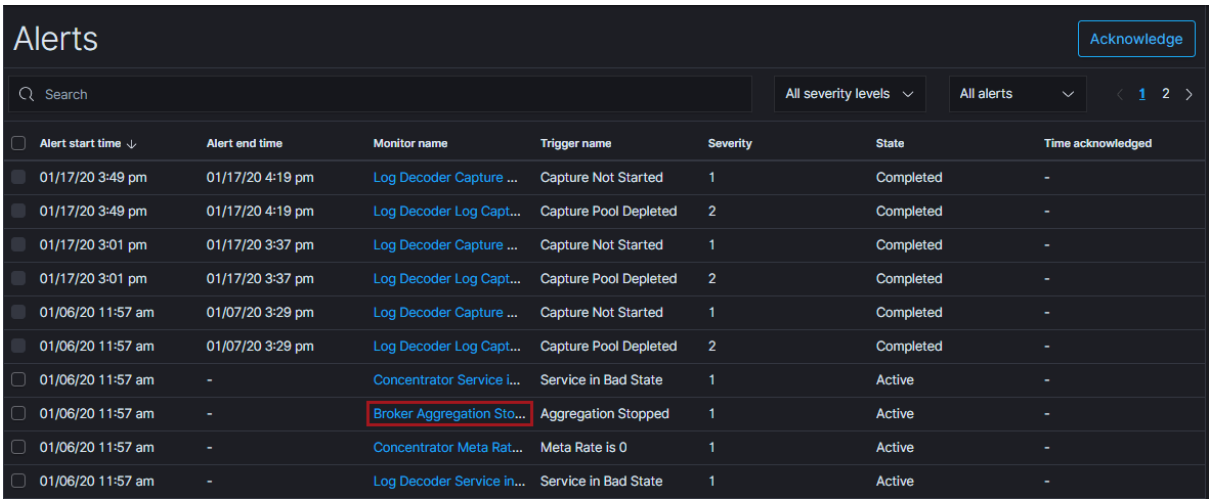
1. Log in to NetWitness Platform.
2. Go to **(Admin) > Health & Wellness.**
3. Click **New Health & Wellness**.
4. Click **Pivot to Dashboard**.
5. Go to > **Kibana** > **Dashboard**.
6. In the **Dashboards** panel, click **Create dashboard**.
7. Click **Create new**.
8. Select a visualization that you want to add to the dashboard. For more information on Visualization, see "Visualize" topic in the Kibana 7.10.0 guide.
9. Click **Save**.

Monitoring through Alerts

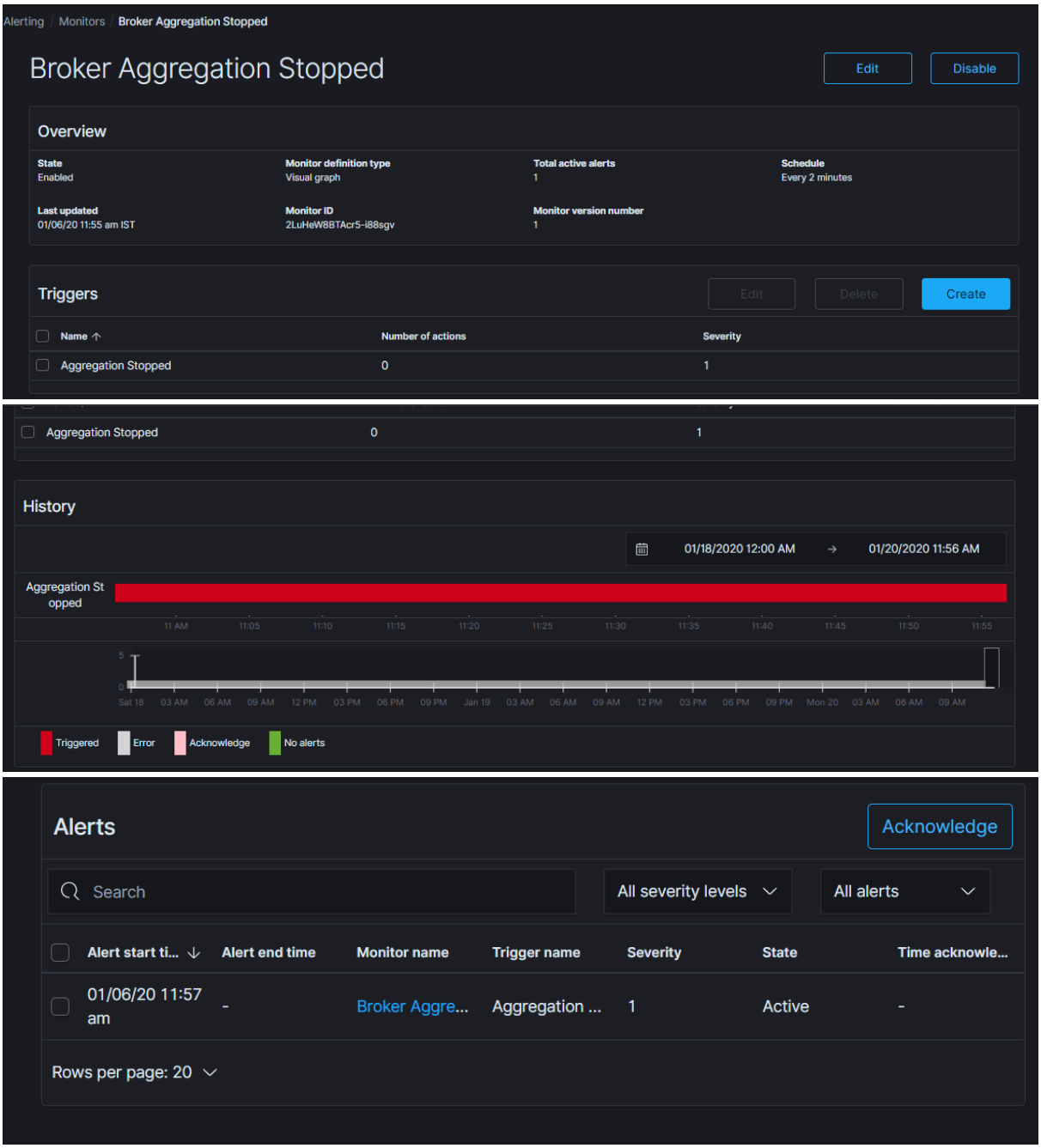
You can monitor the health of NetWitness Platform hosts and services using the alerts.

To monitor using alerts:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Go to >**Open Distro for Elasticsearch** > **Alerting**.
   The alerts view summarizes the alerts generated over the period of time along with the trigger, severity (Critical, High, Medium or Low) and state of the alert.
4. To view the monitors and triggers associated with the alert, click the **Monitor name** link.



For example, if an alert is generated by the monitor name Broker Aggregation Stopped, you can view more details by clicking on the Broker Aggregation Stopped monitor link.


Alerting / Monitors / Broker Aggregation Stopped
Broker Aggregation Stopped
Edit
Disable
Overview
State
Enabled
Monitor definition type
Visual graph
Total active alerts
1
Schedule
Every 2 minutes
Last updated
01/06/20 11:55 am IST
Monitor ID
2LuHeW8BTAcr5-i88sgv
Monitor version number
1
Triggers
Edit
Delete
Create
Name
Number of actions
Severity
Aggregation Stopped
0
1
Aggregation Stopped
0
1
History
01/18/2020 12:00 AM
01/20/2020 11:56 AM
Aggregation Stopped
11 AM
11:05
11:10
11:15
11:20
11:25
11:30
11:35
11:40
11:45
11:50
11:55
5
0
Sat 18
03 AM
06 AM
09 AM
12 PM
03 PM
06 PM
09 PM
Jan 19
03 AM
06 AM
09 AM
12 PM
03 PM
06 PM
09 PM
Mon 20
03 AM
06 AM
09 AM
Triggered
Error
Acknowledge
No alerts
Alerts
Acknowledge
Search
All severity levels
All alerts
Alert start ti...
Alert end time
Monitor name
Trigger name
Severity
State
Time acknowle...
01/06/20 11:57 am
-
Broker Aggre...
Aggregation ...
1
Active
-
Rows per page: 20

Creating Custom Monitors

You can create a new monitor for the host and services and define a trigger.

To create monitors:

1. Log in to NetWitness Platform.
2. Go to **(Admin) > Health & Wellness.**
3. Click **New Health & Wellness**.
4. Click **Pivot to Dashboard**.
5. Go to > **Open Distro for Elasticsearch** > **Alerting**.
6. In the **Monitors** tab, click **Create monitors**.
7. In the **Create Monitors** section, specify the required details.
8. Click **Create**.

   After a monitor is created, you can add a trigger to this monitor.
9. In the **Create Trigger** view, provide the required details:
   a. **Trigger name** - Specify the name of the trigger.
   b. **Severity level** - Set the severity level from range 1–5. 1 is the highest severity and 5 is the lowest severity.
   c. **Trigger condition** - Set the trigger condition with the value. The options are IS ABOVE, IS BELOW, IS EQUAL. For example, IS ABOVE 200.
10. Click **Create** to save the trigger.

Note: After the specified duration, defined as **FOR THE LAST** in the **Define monitor** view, the alert state will change if the trigger condition is met. For more information, refer https://nw-corp.atlassian.net/browse/ASOCKB-65.

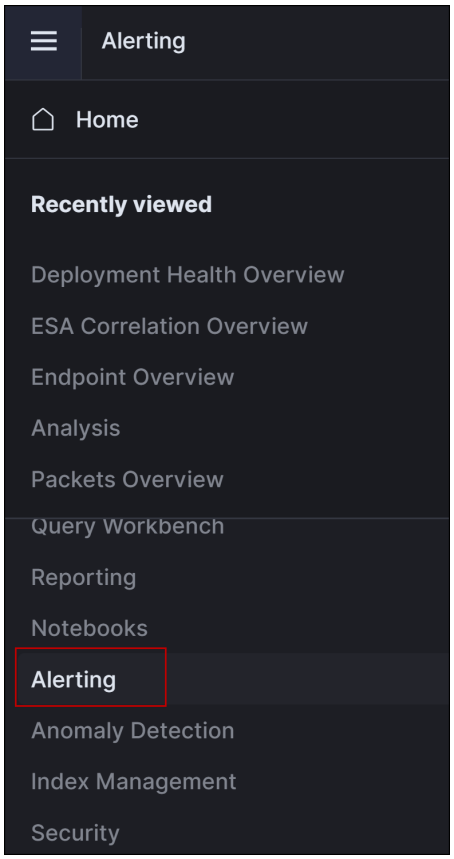
For more information on creating monitors, see "Alerting" in the Open Distro for Elasticsearch 1.12.0 guide.

Adding Custom Trigger to an Existing Monitor

You can add one or more triggers to an existing monitor and assign severity level.

To add trigger to an existing monitor:

1. Log in to NetWitness Platform.
2. Go to **(Admin) > Health & Wellness.**
3. Click **New Health & Wellness**.
4. Click **Pivot to Dashboard**.
5. Go to > **Open Distro for Elasticsearch** > **Alerting**.



6. In the **Monitor** section, click the **monitor** for which new trigger need be added.
7. In the **Triggers** section, select **Create**.
8. In the **Create Trigger** view, provide the required details:
   a. **Trigger name** – specify the name of the trigger.
   b. **Severity level** - Set the severity level from range 1-5. 1 is the highest severity and 5 is the lowest severity.

c. **Trigger condition** – Set the trigger condition with the value. The options are IS ABOVE, IS BELOW, IS EQUAL. For example, IS ABOVE 200.

9. Click **Create** to save the trigger.

Note: After the specified duration, defined as **FOR THE LAST** in the **Define monitor** view, the alert state will change if the trigger condition is met. For more information, refer https://nw-corp.atlassian.net/browse/ASOCKB-65.

Managing Dashboards and Alerts

You can modify the dashboards and alerts to monitor details of interest.

Modify a Dashboard

You can modify the dashboard to edit the visualization, delete visualization, customize the panel title, or change the positions of visualization. You can organize the visualization in the dashboard to display data of greatest interest on the top.

Note: Any changes to the visualization in a dashboard modifies the visualization content.

To modify a dashboard:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Click **Pivot to Dashboard**.
4. Go to > **Kibana** > **Dashboard**.
5. Click the dashboard link you want to modify. For example, Hosts overview.
6. Click **Edit** and make the necessary changes to the dashboard. For example, you can edit or delete visualization, customize panel.
7. Click **Save and return**.

Delete a Dashboard

Once the dashboard is deleted, you cannot monitor the details specific to the dashboard.

To delete a dashboard:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Click **Pivot to Dashboard**.
4. Go to > **Kibana** > **Dashboard**.
5. Select the check box of the dashboard you want to delete and click **Delete**.

You can delete one or more dashboards at a time.

Delete a Visualization

To delete a visualization:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Click **Pivot to Dashboard**.
4. Go to > **Kibana** > **Visualize**.
5. In the **Visualizations** view, select the visualizations you want to delete.
6. Click **Delete visualization**.

   You can delete one or more visualization at a time.

Modify an Existing Trigger

To modify an existing trigger:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness** tab.
3. Click **Pivot to Dashboard**.
4. Go to > **Open Distro for Elasticsearch** > **Alerting**.
5. In the **Dashboard** tab, select the monitor whose trigger is to be modified.
6. In the **Triggers** section, select the trigger you want to modify from list of Triggers and select **Edit**.
7. In the **Edit Trigger** view, make the necessary changes. You can change the Trigger name, severity level, Trigger condition.
8. Click **Update** to save the changes.

Managing Notifications

You can manage alert (monitor) notifications based on your requirement.

Modify a Notification

To modify a notification:

1. Log in to NetWitness Platform.
2. Go to **(Admin) > Health & Wellness.**
3. Click **New Health & Wellness**.
4. Click **View Notifications Settings**.
5. Make the necessary changes.
6. Click **Save**.

Modify a Notification Suppression Policy

When you modify a suppression policy, you can change the day or time ranges. If you select multiple alerts to modify the policy, any changes would overwrite all the existing policies.

To modify suppression policy:

1. Go to **(Admin) > Health & Wellness.**
2. Click **New Health & Wellness**.
3. Select one or multiple rows for which you to modify suppression policy.
4. Click **View Suppression Policy**.

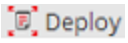
Note: If you have selected multiple alerts to modify the suppression policy,
- Only policies that are common are displayed. Policy suppression settings would be empty if there is no common polices.
- If you edit the common policies, the changes would overwrite all the selected alert policies.

5. Make the necessary changes.
6. Click **Save**.

Advanced Configurations

Restore Default Content

This allows you to bring back all the default content such as dashboards, visualizations, monitors to its original or default state. This overwrites any changes made to the default content. For example, if you have deleted any dashboard or visualization and want to bring back the default content.

1. Log in to NetWitness Platform UI.
2. Click (Configure) > **LIVE CONTENT**.
3. In the **Search Criteria** panel, select the **Resource Types** as:
   - Health and Wellness Dashboards
   - Health and Wellness Monitors
4. Click **Search**.
5. In the **Matching Resources** view, select the checkbox to the left of the resources that you want to deploy.
6. In the **Matching Resources** toolbar, click 

.
7. In the **Deployment Wizard** > **Resources** tab, click **Next**.
8. In the **Services** tab, select the Metrics Server service.
9. Click **Next**.
10. Click **Deploy**.
    The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.
11. Click **Close**.

Enable Services

This is used to enable all the services to start sending metrics for monitoring. For example, if you have disabled few services from sending metrics for monitoring and want to enable all those disabled services to start sending again.

1. SSH to the Admin Server.
2. Enter the following command:
   `nw-shell`
   The console window is displayed.

3. Connect to metrics-server using the following command:

   ```
   connect --service metrics-server
   ```

4. Enter the login command:
   ```
   login
   ```

5. Enter the admin username and password.
6. Navigate to the enable option using the following command:

   ```
   cd /rsa/metrics/elastic/enable-all
   ```

7. Execute the following command to enable all services:

   ```
   invoke
   ```

Disable Services

This is used to disable all the services to send metrics for monitoring. Once disabled, none of the services sends alerts to the Elasticsearch and the dashboards are not updated, and alerts will not be triggered.

1. SSH to the Admin Server.
2. Enter the following command:
   ```
   nw-shell
   ```
   The console window is displayed.

3. Connect to metrics-server using the following command:

   ```
   connect --service metrics-server
   ```

4. Enter the login command:
   ```
   login
   ```

5. Enter the admin username and password.

6. Navigate to Elasticsearch using the following command:

   ```
   cd /rsa/metrics/elastic/disable-all
   ```

7. Execute the following command to disable all services to stop writing to Elasticsearch:

   ```
   invoke
   ```

Note: This disables all services to send metrics to Elasticsearch but does not stop metric beat to send system level metrics to Elasticsearch. You need to manually stop metric beat on all hosts if you wish to stop using Health and Wellness.

Update an Interval

You can update a common interval for all the services to send data for monitoring. For example, if all the services are set to different intervals and you want to configure all the services to send data to elastic search on the same interval.

The interval can be set in seconds, minutes and hours.

1. SSH to the Admin Server.

2. Enter the following command:
   ```
   nw-shell
   ```
   The console window is displayed.

3. Connect to metrics-server using the following command:

   `connect --service metrics-server`

4. Enter the login command:
   `login`
5. Enter the admin username and password.
6. Navigate to the `update-interval` directory using the following command:

   `cd /rsa/metrics/elastic/update-interval`

7. Execute the following command to set a common interval for all the services:

   `invoke <interval>`

   For example, `invoke 30seconds`

Update the Default Configuration

By default, New Health and Wellness configurations are applied after the New Health and Wellness is enabled successfully. To change the configuration of a service, you need to update the existing configuration. After the configuration is updated, the service is notified of the changes.

To update the configuration, perform the following:

1. SSH to the Admin Server.
2. Enter the following command:
   `nw-shell`
   The console window is displayed.

3. Connect to the metrics-server using the following command:

   `connect --service metrics-server`

4. Enter the login command:

   `login`

5. Enter the admin username and password.
6. To get configuration of a service, execute following commands:
   a. `cd /rsa/metrics/elastic/get-config`
   b. `invoke <service-id>`

Note:
To get the service id for core services:
1) Go to **(Admin)** > Core service.
2) Click > **View** > **Explore**.
3) Expand the **sys/stats** node list.
4) In the **UUID** filed, copy the value.
To get the service id for launch services:
1) Go to **(Admin)** > Launch service.
2) Click > **View** > **Explore**.
3) Click the process node.
4) In the **service-id** field, copy the value.
To get the service id for Carlos services:
1) SSH to host in which the Carlos service is deployed.
2) Execute the following command:
For Reporting Engine:
`cat /var/netwitness/re-server/rsa/soc/reporting-engine/service-id`
For Legacy Web Server:
`cat /var/netwitness/uax/service-id`

Note: The core services are Archiver, Broker, Concentrator, Decoder, Log Decoder and; Carlos services are Reporting Engine, Legacy Web Server. All the other services that are not included in Core and Carlos services are part of launch services.

7. Copy the configuration and save it in a file.
   a. Copy the configuration from step 6 and exit from `nw-shell` using command:
      `exit`
   b. Create a file under `/root` in admin server, copy the configurations to the file and save it.

   For example, For the Reporting Engine service, create a file `reporting-engine.json` under `/root/` and copy the configurations obtained from step 6 and save.
8. To set configurations for a service:
   a. `cd /rsa/metrics/elastic/set-config`
   b. `invoke --file <absolute path of the path>`
      For example, `invoke --file /root/reporting-engine.json`

Configure the Data Retention Policy

You can configure the retention policy for monitors (alerts triggered) and metrics based on age and size.

By default, 90 days of data with 100 GB of size for monitors (alerts triggered) and 30 days of data with 100 GB of size for metrics are retained.

To change the configure for monitor (alerts triggered) retention:

1. SSH to the Admin Server.
2. Enter the following command:
   `nw-shell`
   The console window is displayed.

3. Connect to metrics-server using the following command:
   `connect --service metrics-server`

4. Enter the login command:
   `login`
5. Enter the admin username and password.
6. Go to alert-retention-threshold using command:
   `cd /rsa/metrics/elastic/data/retention/alert-retention-threshold`
7. Set the value between 1day to 90days using command:
   `set <number of days>`
   For example, `set 50days`
8. Exit from nw-shell using the command:
   `exit`
9. SSH to the host on which New Health and Wellness is installed.
10. Restart the metrics server on which New Health and Wellness is installed using the command:
    `service rsa-nw-metrics-server restart`

To change the configuration for metrics time threshold:

1. SSH to the Admin Server.
2. Enter the following command:
   `nw-shell`
   The console window is displayed.

3. Connect to metrics-server using the following command:
   `connect --service metrics-server`
4. Enter the login command:
   `login`
5. Enter the admin username and password.

6. Go to time-threshold using command:
   `cd /rsa/metrics/elastic/data/retention/time-threshold`
7. Set the value from **1day** to **90days** using command:
   `set <number of days>`
   For example, `set 40days`
8. Exit from `nw-shell` using the command:
   `exit`
9. SSH to the host on which New Health and Wellness is installed.
10. Restart the metrics server on which the New Health and Wellness is installed using the command:
    `service rsa-nw-metrics-server restart`

To change the size configuration:

1. SSH to the Admin Server.
2. Enter the following command:
   `nw-shell`
   The console window is displayed.

3. Connect to metrics-server using the following command:
   `connect --service metrics-server`
4. Enter the login command:
   `login`
5. Enter the admin username and password.
6. Go to allocated-size using command:
   `cd /rsa/metrics/elastic/data/retention/allocated-size`
7. Set the value using command:
   `set <size to be allocated>`

For example, `set 200GB`

8. Exit from nw-shell using the command:

   `exit`

9. SSH to the host on which New Health and Wellness is installed.
10. Restart the metrics server on which the New Health and Wellness is installed using the command:

    `service rsa-nw-metrics-server restart`

Note: Make sure the `/var/netwitness` partition on standalone New Health and Wellness has enough disk space. After you review your datastore configuration, you may determine that you need to add a new volume. For more information on adding a new volume, see "Add New Volume and Extend Existing File Systems" topic in the *Virtual Host Installation Guide*.

Backup and Restore New Health and Wellness

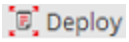
Perform the following steps in the order given:

1. Back up the Admin Server. For more information on the instructions, see "Disaster Recovery (Back Up and Restore)" topic in *Recovery Tool User Guide*.
2. At the root level, type the following command on the host on which New Health and Wellness is installed :

   ```
   nw-recovery-tool --export --dump-dir /var/netwitness/backup --category Search
   ```

   Note: Make sure that the Admin Server is restored, up and running successfully.
3. Restore the New Health and Wellness using the following command:

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category Search
   ```

   Note: Restore the search category (New Health and Wellness) on the same host on which New Health and Wellness is installed.
4. Reboot the Host on which search category (New Health and Wellness) is restored.
5. Restore the default content using RSA Live:
   a. Log in to NetWitness Platform UI.
   b. Click (Configure) > **LIVE CONTENT**.
   c. In the **Search Criteria** panel, select the **Resource Types** as:
      - Health and Wellness Dashboards
      - Health and Wellness Monitors
   d. Click **Search**.
   e. In the **Matching Resources** view, select the checkbox to the left of the resources that you want to deploy.
   f. In the **Matching Resources** toolbar, click 

   .
   g. In the **Deployment Wizard** > **Resources** tab, click **Next**.
   h. In the **Services** tab, select the Metrics Server service.
   i. Click **Next**.
   j. Click **Deploy**.
   The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.
   k. Click **Close**.

Troubleshooting New Health and Wellness

This topic describes how to troubleshoot New Health and Wellness issues.

Issue	An error ‘n of m shards failed’ or ‘unknown field in the index’ in the New Health and Wellness dashboards.
Resolution	Refresh the index patterns, perform the following: 1. Log in to NetWitness Platform. 2. Go to **(Admin) > Health & Wellness.** 3. Click **New Health & Wellness**. 4. Click **Pivot to Dashboard**. 5. Go to > **Stack Management** > **Index Patterns**. 6. Click **nw* index pattern**. 7. Click **Refresh** to refresh the index pattern on top right corner. **Note:** If the issue still persists, refresh other index patterns such as **nw-metricbeat*** or **nw-concentrator*** and so on.

Issue	Unable to send data to elastic search once disk usage reaches 85%.
Explanation	If the Elasticsearch disk usage reaches 85%, the saved objects (index patterns, dashboards, visualizations etc) becomes read-only mode. And, services does not write new metrics to Elasticsearch or allow to edit any saved objects.
Resolution	To change the indexes to write mode, execute the following command on the host in which Elasticsearch is installed: `curl -k --cert /etc/pki/nw/elastic/elasticsearch-cert.pem --key /etc/pki/nw/elastic/elasticsearch-key.pem -X PUT -H "Content-Type: application/json" -d '{"index.blocks.read_only_allow_delete": null }' https://localhost:9200/_all/_settings` **Note:** This command is supported only with certificates.

Issue	**New Health and Wellness** > **Pivot to Dashboard** fails due to time synchronization issue.
Explanation	Pivot to dashboard fails if there is no time synchronization between the NetWitness Server and the host on which New Health and Wellness is

Resolution	installed. You must synchronize the time and pivot to dashboard. To synchronize the time do one of the following: • Configure the NTP Server. For more information, see "Configure NTP Servers" in the *System Configuration Guide*. • Run the following commands on the host on which New Health and Wellness is installed 1. SSH to NetWitness host. 2. Run the following commands. ◦ `systemctl stop ntpd` ◦ `ntpdate nw-node-zero` ◦ `systemctl start ntpd`

Issue	NW Host High Swap Utilization monitor generates many false alerts.
Explanation	By default the set threshold is > 50 %, which might generate many false alerts on NW Host High Swap Utilization monitor for Linux hosts, which is considered normal. **Note:** On upgrade to 11.5.3.0 version or later, the monitor will be automatically deleted on the New Health & Wellness monitors view.
Resolution	On version 11.5.2.0 or lower, you can perform the following steps to delete the monitor: 1. Log in to the NetWitness Platform. 2. Go to **(missing or bad snippet)> Health & Wellness**. 3. Click **New Health & Wellness**. 4. Click **Pivot to Dashboard**. The **Deployment Health Overview** dashboard is displayed. 5. Go to > **Open Distro for Elasticsearch** > **Alerting**. The Dashboards tab is displayed by default. 6. Click **Monitors** tab. 7. Select the NW Host High Swap Utilization monitor and click > **Delete**. The monitor is deleted.

Appendices

This section is a collection of appendices for new health and wellness:

- New Health and Wellness Dashboards
- New Health and Wellness Monitors

New Health and Wellness Dashboards

This topic provides the list of default New Health and Wellness dashboards and associated visualizations and metrics.

Deployment Health Overview Dashboard

This dashboard provides the overall health of the NetWitness Platform hosts and services. The following table provides the information on default visualizations available on this dashboard.

Note: The parameters and metrics listed below are the default values. You can customize the parameters and metrics of any visualization based on your requirement. For example, you can customize a visualization to view the CPU utilization for all the core services or any particular service.

Visualization	Parameters and Metrics	Objective	Description
Alarms Summary	• Count of active alert • Alert severity	Provides the summary of active health alarms based on the severity.	Displays the active alarms grouped by severity (Critical, High, Medium, Low).
Offline Services	• Service name • Status Time • Refresh time 15 minutes	Identifies the list of unavailable services.	Displays the list of offline services.
Stopped Archiver Aggregation	• Count of archivers where aggregation is stopped • Refresh time 15 minutes	Identifies the number of Archivers where aggregation is stopped.	Displays the number of Archivers where aggregation is stopped. For more information, see Notifications.
Stopped Broker Aggregation	• Count of Brokers where aggregation is stopped • Refresh time 15 minutes	Identifies the number of Brokers where aggregation is stopped.	Displays the number of Brokers where aggregation is stopped. For more information, see Notifications.
Stopped Concentrator Aggregation	• Count of Concentrators where aggregation is stopped • Refresh time 15 minutes	Identifies the number of Concentrators where aggregation is stopped.	Displays the number of Concentrators where aggregation is stopped. For more information, see Notifications.

Visualization	Parameters and Metrics	Objective	Description
Stopped Decoder/Log Decoder Capture	• Count of Decoders or Log Decoders where capture is stopped • Refresh time 15 minutes	Identifies the number of Decoders or Log Decoders where capture is stopped.	Displays the number of Decoder or Log Decoder where capture is stopped. For more information, see Notifications.
Total vs Offline Services	• Total number of services • Count of offline services • Refresh time 15 minutes	Identifies the number of offline services versus total number of services.	Displays the total number of services and the number of services that are offline.
Stopped State Aggregation & Capture	• Services name • Host name • Service version	Provides the list of services where aggregation and capture are stopped.	Displays the list of services where aggregation and capture are stopped.
NetWitness Services Version Status	• Service version	Provides the status of NetWitness Platform service versions.	Displays the status of NetWitness Platform service versions.
NetWitness Services – Uptime Summary	• Service name • Host name • Running since	Provides an overview on the uptime of the services in the deployment.	Displays the list of services and their uptime.
Memory Utilization Trend	• Service name • Memory usage	Provides the memory utilization trend to detect any high utilizations and take necessary action.	Displays the memory utilization trend of the hosts.
Current CPU Usage	• Services name • CPU usage	Provides the CPU usage trend of the hosts to identify any high utilizations and take necessary action.	Displays the current CPU usage of the services.
Current Disk Usage	• Services name • Disk usage	Provides the disk utilization in the real time to identify any high utilizations and take necessary action.	Displays the current disk usage of the hosts.
Capture Rate for Log Decoders	• Service name • Capture rate	Provides the capture rate trend to identify any high values and take necessary action.	Displays the trend of Log Decoders capture rate.

Visualization	Parameters and Metrics	Objective	Description
Capture Rate for Network Decoders	• Service name • Capture rate	Provides the capture rate trend to identify any high values and take necessary action.	Displays the trend of Network Decoders capture rate.
Session Aggregation Rate and Trend for Concentrators	• Service name • Session aggregation rate	Provides an overview on the session rate of the Concentrators to identify any high values and take necessary action.	Displays the session aggregation rate and trend of Concentrator.
Retention Summary	• Service id • Service name • Running on host • Oldest meta file time • Oldest packet file time • Oldest session file time	Provides a quick view on the current retention of the Decoders, Concentrators and Archivers to check if the retention is lower than the configured retention.	Displays the oldest date for meta, session, packet present in decoders, logdecoders and concentrators
Total CPU Usage Trend for Services	• CPU usage • Service name	Provides the CPU usage trend of the services to detect the high utilization and take necessary action.	Displays the top 20 services where CPU usage is high.
Total Memory Usage Summary for Services	• Service name • Memory usage	Provides the memory usage summary of NetWitness Platform services to detect any high usage and take necessary actions.	Displays the top services that are utilizing the resident memories.

Hosts Dashboard

This dashboard provides the resource utilization and health of NetWitness hosts in your deployment. The following table provides information on default **Visualizations** available on this dashboard.

Visualization	Metrics	Objective	Description
Disk Used	• Disk usage	Provides the current disk usage of the hosts to detect the high utilization and take immediate action.	Displays the current disk usage of the host.

Visualization	Metrics	Objective	Description
Current Memory Usage vs Total Available	• Current memory usage • Total available memory	Provides the current memory usage versus total available memory to identify high usage and take necessary action.	Displays the current memory usage and total available memory of the host.
Current Disk Usage vs Total Available Disk	• Current disk usage • Total available disk	Provides the current disk usage versus total available disk to identify high usage and take necessary action.	Displays the current disk usage versus total available disk.
Disk Usage by Partitions	• Disk partition • Disk usage	Provides the disk usage by different partitions to identify high usage and take necessary action.	List of partitions and associated disk percentage.
Resident Memory Usage by Services	• Service name • Resident memory usage	Provides the resident memory usage per service to identify high usage and take necessary action.	Displays the resident memory usage of the service.
Memory Usage	Memory usage	Provides the current memory usage percentage of the hosts to identify high memory usage and take necessary action.	Displays the memory usage of the host.
CPU Usage	CPU usage	Provides the CPU usage percentage to identify high usage and take necessary action.	Displays the CPU usage of the host.
CPU Usage by Services	• Service name • CPU usage	Provides the CPU Percentage per service to detect high usage and take necessary action.	Displays the CPU usage of the service.
Interfaces by Incoming Traffic	Incoming traffic on interfaces	Provides the trend on interfaces incoming traffic to detect any deviation on time.	Display the incoming traffic interfaces.
Interfaces by Outgoing Traffic	Outgoing traffic on interfaces	Provides the trend on interfaces outgoing traffic to detect any deviation on time.	Display the interfaces outgoing traffic.
Services by Open File Descriptors	• Services • Open file descriptor	Provides the list of open file descriptor associate with a service.	Displays the list of open file descriptor associated with a service.

Visualization	Metrics	Objective	Description
TOP APPLIANCES BY DISK IO READ (Line) Vs WRITE (Bar)	• Service name • Disk IO Read • Disk IO Write	Provides the list of top appliances by disk IO read and write to detect any high usage and take necessary action.	Displays top appliances based on disk IO read and write usage.
Total Inbound Traffic for All Interfaces	• Count of inbound traffic on Interfaces • Total transferred traffic	Provides the total inbound traffic to detect any deviation on time.	Displays the current inbound traffic and total transferred traffic.
Total Outbound Traffic for All Interfaces	• Count of outbound traffic on Interfaces • Total transferred traffic	Provides the total outbound traffic to detect any deviation on time.	Display the current outbound traffic and total transferred traffic.

Logs Dashboard

This dashboard provides information on various NetWitness Platform logs. The following table provides information on default **Visualizations** available on this dashboard.

Visualization	Metrics	Objective	Description
Log Decoders by Capture Rate	• Service name • Capture Rate	Provides the capture rate of Log Decoders to detect high capture rate on time and take necessary action.	Displays the Log Decoders by capture rate.

Visualization	Metrics	Objective	Description
Log Decoders by Capture Packet Rate	• Service name • Capture Packet Rate	Provides the capture packet rate of Log Decoder to detect high capture packet rate on time and take necessary action.	Displays the Log Decoders by capture packet rate.
Log Decoders by CPU Percentage	• Service name • CPU usage	Identifies the Log Decoders by CPU usage to detect high usage and take necessary action.	Display the Log Decoders by CPU usage..
Log Decoders by Resident Memory Usage	• Service name • Resident Memory Usage	Identifies the Log Decoders by resident memory usage to detect high usage and take necessary action.	Display Log decoder by resident memory usage.
SDK Active Queries on Concentrators	• Service name • Count of active queries	Identifies the concentrators by SDK active queries.	Display concentrators by SDK active queries.
Concentrators Status	• Service running on host • Service type • Service version • Aggregation status • Average session rate • Max session rate • Active queries	Provides the concentrator status.	Display the list of concentrators and its status.

Visualization	Metrics	Objective	Description
Concentrator Session Aggregation Rate [Trend]	• Service name • Session rate	Provides the trend of Concentrator session aggregation rates to detect high session rates and take necessary action.	Displays Concentrator session aggregation rate.
SDK Active Queries on Brokers	• Service name • Count of Active Queries	Identifies the Brokers by SDK active queries.	Lists Brokers by SDK active queries.
Brokers Status	• Service running on host • Service type • Service version • Aggregation status • Average session rate • Max session rate • Active queries	Provides the Broker status.	Displays the list of Brokers and their status.

Packet Overview Dashboard

This dashboard provides information on NetWitness Platform network data. The following table provides information on default **Visualizations** available on this dashboard.

Visualization	Metrics	Objective	Description
Network Decoders by Capture Rate	• Service name • Capture rate	Identifies the capture rate of Network Decoder to detect high value and take necessary action.	Displays Network Decoders by capture rate.

Visualization	Metrics	Objective	Description
Network Decoders by Capture Drop	• Service name • Capture drop percentage	Identifies the capture drop rate of Network Decoders to detect drop rate and take necessary action.	Displays Network Decoders by capture drop.
Network Decoders by CPU Percentage	• Service name • CPU usage	Identifies the Network Decoders by CPU usage to detect high usage and take necessary action.	Displays Network Decoder by CPU used.
Network Decoders by Resident Memory Usage	• Service name • Resident memory usage	Identifies the Network Decoders by resident memory usage to detect high usage and take necessary action.	Displays Network Decoder by resident memory usage.
SDK Active Queries on Concentrators	• Service name • Count of active queries	Identifies the concentrators by SDK active queries.	Displays Concentrators by SDK active queries.
Concentrators Status	• Service running on host • Service type • Service version • Aggregation status • Average session rate • Max session rate • Active queries	Provides the Concentrator status.	Displays the list of Concentrators and their status.

Visualization	Metrics	Objective	Description
Concentrator Session Aggregation Rate [Trend]	• Service name • Session rate	Provides the trend of Concentrator session aggregation rate to detect high value and take necessary action.	Displays the trend of concentrator session aggregation rate.
SDK Active Queries on Brokers	• Service name • Count of active queries	Identifies the Brokers by SDK active queries.	Display the Broker by SDK active queries.
Brokers Status	• Service running on host • Service type • Service version • Aggregation status • Average session rate • Max session rate • Active queries	Provides the Broker status.	Displays the list of brokers and its status.

Analysis Dashboard

This dashboard provides details about Reporting Engines on Primary UI or Analyst UI. The following table provides the information on default **Visualizations** available on this dashboard.

Visualization	Metrics	Objective	Description
Reporting Engine Rule Query Executions	• Hostname • Failed rule executions • Cancelled rule execution • Active rule execution • Total rule execution	Provides the status of the queries executed by Reporting Engine to detect any deviations on time.	Displays the queries executed by Reporting Engine.

Visualization	Metrics	Objective	Description
Reporting Engine Reports Executions	• Hostname • Failed in last hour • Running more than one hour • Cancelled in last hour • Output actions failed in last hour	Provides the status of the reports executed by Reporting Engine to detect any deviations on time.	Displays the Reporting Engine reports.
Reporting Engine Alerts Execution	• Enabled alerts • Execution failed • Execution skipped in las 10 minutes • Running alerts • Output actions failed in last 10 minutes	Provides the status of the alerts generated by Reporting Engine to detect any deviations on time.	Displays the Reporting Engine alerts.
Reporting Engine Charts Executions	• Hostname • Enabled charts • Execution failed • Execution cancelled in last 10 minutes	Provides the status of the charts executed by Reporting Engine to detect deviations on time.	Displays Reporting Engine charts.
Reporting Engine Disk Usage	• Disk Used • Total disk space	Provides the disk usage by Reporting Engine to detect any deviations high usage and take necessary action.	Displays the disk used by Reporting Engine.
Unassigned Open Incidents	Count of unassigned open incidents	Identifies unassigned incidents to assist Administrator to take necessary action.	Displays the unassigned incidents.

Visualization	Metrics	Objective	Description
Incidents Sent to Archer	Count of incidents sent to archer	Provides statistics on the incidents sent to Archer to assist Administrator to take necessary action.	Displays the incidents sent Archers.

Endpoint Dashboard

This dashboard provides information on NetWitness Endpoints and agents installed on Endpoints. The following table provides information on default Visualizations available on this dashboard.

Visualization	Metrics	Objective	Description
Endpoint Server to Agent Communication Queued	• Service name • Count of queued request to Agent	Provides an overview of the queued agent communication to the Endpoint Server to identify any issues around the queued communication.	Displays the queued request to agent.
Endpoint Server to Agent Communication Rejected Count	• Service name • Count of rejected request to agent	Provides an overview of rejected agent communication to the Endpoint Server to identify any issues related to the rejected count.	Displays the rejected request to agent.
Endpoint Agent Overview	• Hostname • Total active agents • Active advanced • Active insights agents • Active advanced windows agents • Active advanced linux agents • Active advanced mac agents	Provides an overview of Endpoint Agents.	Displays list of agents and its details.

Visualization	Metrics	Objective	Description
Relay Servers Overview	• Hosts • Total relay servers • Agents communicated via relay server • Agents communicated in last two days via relay server	Provides an overview of the Relay Servers.	Displays the Relay server details.
Files Count by File Status	• Count of blacklisted files • Count of graylisted files • Count of netural file • Count of whitelisted files	Provides an overview of file status by count to assist an Administrator on the overall statistics of Endpoint actions on files.	Displays the file count of file statuses.
Files Count by Certificate Status	• Count of blacklisted certificates • Count of gray listed certificates • Count of neutral certificates • Count of whitelisted certificates	Provides an overview on certificate status to assist an Administrator to take necessary action.	Displays the count of certificate statuses.

Visualization	Metrics	Objective	Description
File Count by Reputation Status	• Count of unknown status • Count of suspicious status • Count of malicious status • Count of known good status • Count of known status • Count of invalid status	Provides an overview on the reputation status to assist an Administrator to take necessary action.	Displays the count of files reputation status.
Endpoint Hosts with Risk Score Greater than 90	Count of hosts with risk score greater than 90	Identifies the number of hosts with risk score higher than 90 for immediate attention.	Displays the count of hosts with risk score greater than 90.
Endpoint Files with Risk Score Greater than 90	Count of files with risk score greater than 90	Identifies the number of files with risk score higher than 90 for immediate attention.	Displays the count of files with risk score greater than 90.

ESA Correlation Overview Dashboard

This dashboard provides health statistics and trends on the ESA deployment. The following table provides the information on default **Visualizations** available on this dashboard.

You can choose the ESA host and Deployment name for the Dashboard view source using the filter.

Visualization	Metrics	Objective	Description
Sessions Behind by Sources	Count of sessions behind by sources.	Provides the session behind trend for the sources to take necessary actions when the session behind goes higher.	Displays the count of sessions behind by sources.
Sessions Rate by Sources	Count of sessions rate by sources.	Provides the session rate trend for the sources to take necessary actions when the session rate goes higher.	Displays the count of sessions rate by sources.
Top Rules by Memory	Memory used by rules.	Provides the memory usage per rule to identify the rule with high memory usage and take necessary action.	Displays the top rules based on memory usage.
Top Rules by CPU	CPU used by rules.	Provides the CPU usage per rule to identify the rule with high CPU usage and take necessary action.	Displays the top rules based on CPU usage.

Visualization	Metrics	Objective	Description
ESA Correlation Resident Memory Usage	Resident memory usage.	Provides resident memory usage trend to be able to detect high usage and take necessary action.	Displays the trend of ESA correlation resident memory usage.
ESA Correlation CPU Usage	CPU usage.	Provides CPU usage trend to detect high usage and take necessary action.	Displays the trend of ESA correlation CPU usage.
ESA CR - Event Rate by Deployments	Event rate of each ESA correlation deployment.	Identify the event rate by each deployment under ESA Correlation to detect high usage and take necessary action.	Displays the trend of ESA correlation event rate of each deployment.

Logstash Input Plugin Dashboard

The Logstash Input Plugin dashboard provides insight on Logstash event source and the NetWitness Input Plugin.

Prerequisites

- You must install the New Health and Wellness. For more information, see New Health and Wellness
- You must ensure to download the Logstash Input Plugin Dashboard from RSA Live. For more information, see Advanced Configurations

The following table provides the information on default **Visualizations** available on this dashboard.

Visualization	Metrics	Objective	Description
Logstash Inactive Pipelines	• Inactive pipeline • Total number of Pipeline	Provides the summary of inactive pipeline.	Displays the total number of inactive pipeline.
Logstash Inactive Sources	• Inactive sources • Total number of sources	Provides the summary of inactive sources.	Displays the total number of inactive sources.
Logstash Incoming Rate	• Incoming rate of Logstash event sources.	Provides the trend of incoming rate for Logstash event source.	Displays the trend of Logstash incoming rate.
Logstash Outgoing Rate	Outgoing rate of Logstash event sources.	Provides the trend of outgoing rate for Logstash event sources.	Displays the trend of Logstash outgoing rate.

Visualization	Metrics	Objective	Description
Logstash Data Persistence	Count of persisted Logstash event source.	Provides the trend of persisted Logstash event source to take necessary actions when the persisted data count goes higher.	Displays the trend of Logstash persisted data.
Logstash Pipelines status	• Inactive pipelines • Active pieplines • Total number of pipelines	Provides the status of Logstash pipeline.	Displays the status of Logstash pipeline.
Sources by Input event rate	• Input rate of sources	Provides the trend of source input rate to identify any high values and take necessary action.	Displays the trend of source input event rate.
Sources by Sessions behind	Logstash session behind	Provides the trend of Logstash session behind to identify any high values and take necessary action..	Displays the trend of Logstash session behind.
Events to consumer (Output Plugin)	Output event rate	Provides the trend of output event rate to identify any high values and take necessary action.	Displays the trend of Logstash output event rate.

Visualization	Metrics	Objective	Description
Logstash Service Uptime	• Service start time • Host name • Service name	Provides the time when the service is active.	Displays the time when the service is running.
Source Status	• Stream status • Source host • Service type • Service version • Logstash host • Average input event rate • Average source session rate • Average session behind	Provides overall status of the services. For example, stream status of the Decoder connected with the Logstash.	Displays the list of all services and its status.
Logstash Services by CPU Usage	• CPU usage • Service name	Provides the CPU usage trend of the Logstash services to identify any high utilizations and take necessary action.	Displays the CPU utilization trend of the Logstash services.
Logstash Service by Resident Memory Usage	• Resident memory usage • Service name	Provides the resident memory usage trend of the Logstash services to identify any high utilizations and take necessary action.	Displays the resident memory utilization trend of the Logstash services.

License Usage Dashboard

The License Usage Dashboard provides License usage statistics and trends on the Log Decoder, Packet Decoder, Endpoint, UEBA, and Malware services and at aggregated levels under throughput license. It provides an overview of the usage of all types of Throughput licenses in your deployment.

It helps you:

- Track daily license usage for individual hosts
- Track daily usage of Throughput licenses for all the hosts in your deployment
- Download license usage reports

Prerequisites

- You must install the New Health and Wellness. For more information, see New Health and Wellness
- You must ensure to download the License Usage Dashboard from RSA Live. For more information, see Advanced Configurations

IMPORTANT: The date shown in the user interface is set by the browser's time zone. The user's browser may be different from the time zone of the Admin server host. To make a date shown in the user interface to match the Admin server, change the time zone setting under Stack Management > Advanced Settings. If you update the time zone under Advanced settings, it affects other DateTime displays throughout the user interface.

The following table provides the information on default **Visualizations** available on this dashboard. You can choose any host and Deployment name for the Dashboard view source using the filter.

Visualization	Metrics	Objective	Description
Packets Analyzed	• Usage in bytes • Per day	Provides the packet data analyzed in bytes for Packet Decoder. Helps to track daily usage.	Displays the packet data analyzed daily in bytes.
Packets on Disk	• Usage in bytes • Per day	Provides the amount of data stored on the disk daily in bytes for the Packet Decoder. Helps to track daily usage.	Displays the amount of packet data usage on the disk daily in bytes.
Logs Processed	• Usage in bytes • Per day	Provides the Log data processed in bytes for Log Decoders. Helps to track daily usage.	Displays the Log data processed daily in bytes.
Users Analyzed	• Users Analyzed • Per day	Provides the number of users analyzed. Helps to track daily usage.	Displays the number of users analyzed daily.

Visualization	Metrics	Objective	Description
Files Analyzed	• Usage in bytes • Per day	Provides the files analyzed in bytes. Helps to track daily usage.	Displays the files analyzed daily in bytes.
Hosts Analyzed	• Hosts Analyzed • Per day	Provides the number of hosts analyzed. Helps to track daily usage.	Displays the number of hosts analyzed daily.
Aggregate Usage - Logs Processed	• Usage in bytes • Per day	Provides an aggregated log of data from all the log services under the throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated log of data from all the log services daily.
Aggregate Usage - Packet Analyzed	• Usage in bytes • Per day	Provides an aggregated packet of data from all the packet services under the throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated packet of data from all the packet services daily.

Visualization	Metrics	Objective	Description
Aggregate Usage - Packets on Disk	• Usage in bytes • Per day	Provides an aggregated packet data stored on the disk from all the packet services under the throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated packet data stored on the disk from all the packet services daily.
Aggregate Usage - File Analyzed	• Usage in bytes • Per day	Provides an aggregated file usage in bytes from all the Malware services under throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated file usage in bytes from all the Malware services daily.
Aggregate Usage - Host Analyzed	• Hosts analyzed • Per day	Provides an aggregated list of hosts from all the endpoint servers under the throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated list of hosts from all the hosts daily.

Visualization	Metrics	Objective	Description
Aggregate Usage - User Analyzed	• Users analyzed • Per day	Provides an aggregated users from all the UEBA servers under the throughput license. Helps to track daily usage, detect high value, and take necessary action.	Displays an aggregated users from all the UEBA servers daily.

New Health and Wellness Monitors

This topic lists the default New Health and Wellness monitors.

Number	Monitor
1.	Respond Server Risk Scoring Unprocessed Alerts High Count
2.	Respond Server Risk Scoring Unprocessed Alert Older Than 24 Hours
3.	Respond Server Risk Scoring Transient Alerts Ignored High Count
4.	Reporting Engine Shared Task Critical Utilization
5.	Reporting Engine Schedule Task Pool Critical Utilization
6.	Reporting Engine Rule(s) Execution Failed
7.	Reporting Engine Report(s) Running > 1 hour
8.	Reporting Engine Report(s) Executions Failed
9.	Reporting Engine Chart(s) Execution Failed
10.	Reporting Engine Available Disk < 5%
11.	Reporting Engine Available Disk < 20%
12.	Reporting Engine Available Disk < 2%
13.	Reporting Engine Available Disk < 10%
14.	NW Offline Service
15.	NW Host High Swap Utilization
16.	NW Host Filesystem Disk Full
17.	NW Host Critical Memory Usage
18.	NW Host Critical Disk Usage
19.	NW Host Critical CPU Usage
20.	Log Decoder Service in Bad State
21.	Log Decoder Log Capture Pool Depleted
22.	Log Decoder Invalid Rules Detected
23.	Log Decoder Dropping > 5% of Logs
24.	Log Decoder Dropping > 10% of Logs
25.	Log Decoder Dropping > 1% of Logs
26.	Log Decoder Database(s) Not Open

Number	Monitor
27.	Log Decoder Capture Rate Zero
28.	Log Decoder Capture Not Started
29.	Endpoint Server to Agent - Incoming UDP Packets Requested
30.	Endpoint Server to Agent - Incoming UDP Packets Rejected
31.	Endpoint Server to Agent - Incoming UDP Packets Queued
32.	Endpoint Server to Agent - Incoming UDP Packets Dropped
33.	Endpoint Server to Agent - Incoming UDP Packets Delayed
34.	Endpoint Server - Machine Persistence Failed
35.	Endpoint Server - Inactive Machine Retention Failed
36.	ESA Correlation - Sessions Behind on Datasources
37.	ESA Correlation - ESA Rule High Memory Usage
38.	ESA Correlation - ESA Rule High CPU Usage
39.	ESA Correlation - ESA Rule Critical Memory Usage
40.	ESA Correlation - ESA Rule Critical CPU Usage
41.	Decoder Service in Bad State
42.	Decoder Packet Capture Pool Depleted
43.	Decoder Invalid Rules Detected
44.	Decoder Dropping > 5% of Packets
45.	Decoder Dropping > 10% of Packets
46.	Decoder Dropping > 1% of Packets
47.	Decoder Database(s) Not Open
48.	Decoder Capture Rate Zero
49.	Decoder Capture Not Started
50.	Contexthub Server Query Response Cache Usage > 80%
51.	Contexthub Server High Query Response Cache Usage
52.	Contexthub Server Database High Disk Usage
53.	Contexthub Server Database Critical Disk Usage
54.	Contexthub Server Critical Query Response Cache Usage
55.	Concentrator Service in Bad State

Number	Monitor
56.	Concentrator Meta Rate Zero
57.	Concentrator Individual Rule(s) Detected
58.	Concentrator Database(s) Not Open
59.	Concentrator Aggregation Stopped
60.	Concentrator > 5 Pending Queries
61.	Broker Session Rate Zero
62.	Broker Service in Bad State
63.	Broker Aggregation Stopped
64.	Broker > 5 Pending Queries
65.	Archiver Service in Bad State
66.	Archiver Aggregation Stopped
67.	Logstash offline
68.	Logstash Persisting data

Uninstall New Health and Wellness

To uninstall New Health and Wellness, perform the following:

1. Take a backup of NetWitness Server host. For more information, see “Disaster Recovery (Back Up and Restore)” topic in the *NetWitness Recovery Tool User Guide*.

   ```
   nw-recovery-tool --export --dump-dir /some/folder --category AdminServer --
   category Search
   ```

   Note: If New Health and Wellness is not installed on NetWitness Server, you must take a backup of the host on which New Health and Wellness is installed.

2. Make sure that the installation or upgrades are not in progress and stop the orchestration server on NetWitness Server host:

   ```
   systemctl stop rsa-nw-orchestration-server
   ```

3. Remove the New Health and Wellness service category (“Search") from the host:

   a. SSH to Admin server

   b. Fetch host details where New Health and Wellness is installed using the following command:
   ```
   mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
   password> --authenticationDatabase admin --eval 'db.host.find({
   "installedServices": /.*Search.*/i })'
   ```

   Sample output

   ```
   { "_id" : "56f2a90b-1f03-d09a-fb71-42c2a93958a8", "hostname" :
   "10.10.10.11", "ipv4" : "10.10.10.11", "ipv4Public" : "", "displayName"
   : "adminserver", "version" : { "major" : 11, "minor" : 5, "servicePack"
   : 0, "patch" : 0, "snapshot" : false, "rawVersion" : "11.5.2.0" },
   "lastFailedRefreshAttempt" : NumberLong(0), "refreshAttemptDelayFactor"
   : 0, "thirdParty" : false, "installedServices" : [ "Search",
   "AdminServer" ], "meta" : { "node-zero" : true }, "_class" :
   "com.rsa.asoc.orchestration.host.HostEntity" }
   ```

   c. Remove the "Search" from the `installedServices`.

   IMPORTANT: Do not remove any other category names.

   d. Replace <LIST-OF-CATEGORIES-EXCEPT-SEARCH> with a comma-delimited AND double-quoted list of all the existing installed services found earlier EXCEPT "Search":
   ```
   mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
   password> --authenticationDatabase admin --eval 'db.host.update({ "_id"
   : "<hw-node-uuid>" },{$set: {"installedServices" : [ <LIST-OF-
   CATEGORIES-EXCEPT-SEARCH> ]}})'
   ```

   Example
   ```
   mongo localhost/orchestration-server -u deploy_admin -p netwitness --
   authenticationDatabase admin --eval 'db.host.update({ "_id" : "56f2a90b-
   1f03-d09a-fb71-42c2a93958a8" },{$set: {"installedServices" : [
   "AdminServer" ]}})'
   ```

   Sample output

   ```
   MongoDB shell version v4.0.19
   ```

```
connecting to: mongodb://localhost:27017/orchestration-
server?authSource=admin&gssapiServiceName=mongodb

Implicit session: session { "id" : UUID("04e32380-347e-4b7d-a63e-
a094536d7242") }

MongoDB server version: 4.0.19

WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
```

e. Make sure that the "Search" category is removed in the updated host record in the `installedServices` :

```
mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
password> --authenticationDatabase admin --eval 'db.host.find({ "_id" :
"<hw-node-uuid>" })'
```

Example

```
mongo localhost/orchestration-server -u deploy_admin -p netwitness --
authenticationDatabase admin --eval 'db.host.find({ "_id" : "56f2a90b-
1f03-d09a-fb71-42c2a93958a8" })'
```

Note: Any inconsistencies can result in unrecoverable errors.

Sample output

```
{ "_id" : "56f2a90b-1f03-d09a-fb71-42c2a93958a8", "hostname" :
"10.10.10.11", "ipv4" : "10.10.10.11", "ipv4Public" : "", "displayName" :
"adminserver", "version" : { "major" : 11, "minor" : 5, "servicePack" : 0,
"patch" : 0, "snapshot" : false, "rawVersion" : "11.5.2.0" },
"lastFailedRefreshAttempt" : NumberLong(0), "refreshAttemptDelayFactor" :
0, "thirdParty" : false, "installedServices" : [ "AdminServer" ], "meta" :
{ "node-zero" : true }, "_class" :
"com.rsa.asoc.orchestration.host.HostEntity" }
```

4. Stop the New Health and Wellness services:

```
systemctl stop rsa-nw-metrics-server elasticsearch opendistro-performance-
analyzer kibana
```

5. Disable the New Health and Wellness services:

```
systemctl disable rsa-nw-metrics-server elasticsearch opendistro-performance-
analyzer kibana
```

6. Uninstall the New Health and Wellness packages using the command:

```
yum erase -y rsa-nw-metrics-server opendistroforelasticsearch
opendistroforelasticsearch-kibana
```

Note: `rsa-nw-shell` (installed with metrics server) is a shared package and should not be removed.

7. Remove the configuration folders or files:

- `/etc/netwitness/metrics-server`
- `/etc/netwitness/platform/elasticsearch`
- `/etc/netwitness/platform/nodeinfo/metrics-server`
- `/etc/netwitness/platform/nodeinfo/elasticsearch-open-distro`

- /etc/netwitness/platform/nodeinfo/kibana-open-distro
- /etc/systemd/system/rsa-nw-metrics-server.service.d
- /etc/systemd/system/elasticsearch.service.d
- /etc/pki/nw/service/bootstrap/metrics-server.completed
- /etc/pki/nw/service/rsa-nw-metrics-server-cert.pem
- /etc/pki/nw/service/rsa-nw-metrics-server.chain
- /etc/pki/nw/elastic
- /etc/pki/nw/kibana
- /var/log/netwitness/metrics-server
- /var/log/kibana
- /etc/collectd.d/rsa-metrics-server.conf
- /etc/logrotate.d/kibana
- /etc/elasticsearch
- /etc/kibana
- /var/lib/elasticsearch
- /var/lib/kibana
- /var/netwitness/elasticsearch

8. Start the orchestration Server on NetWitness Server:
   `systemctl start rsa-nw-orchestration-server`
9. Unregister the New Health and Wellness from the `installedService`:
   a. Find the service IDs for metrics-server, elasticsearch-open-distro, and kibana-open-distro

      Note: Make sure you look for service IDs for the correct host; do not unregister elastic or kibana on an UEBA host.

      ```
      orchestration-cli-client --list-services | grep <hw-node-IP-address>
      ```

      Sample output

      ```
      ID=50082d04-320c-4ce2-8379-00f38ae2d1df, NAME=metrics-server,
      HOST=192.168.1.2:7018, TLS=true

      ID=530ff46a-8793-4e8e-be9c-742193d1705a, NAME=elasticsearch-open-distro,
      HOST=192.168.1.2:9200, TLS=true

      ID=4bad6ea8-e3a4-46ab-a342-34356bea65bb, NAME=kibana-open-distro,
      HOST=192.168.1.2:5601, TLS=true

      ... (other services) ...
      ```

   b. Remove the service IDs returned above for metrics-server, elasticsearch-open-distro, and kibana-open-distro (associated with New Health new Wellness host):

      ```
      orchestration-cli-client --remove-service --id <metrics-server-service-id>
      ```

```
orchestration-cli-client --remove-service --id <elasticsearch-open-distro-service-id>

orchestration-cli-client --remove-service --id <kibana-open-distro-service-id>
```

c. Verify if the services are removed:

```
orchestration-cli-client --list-services | grep <hw-node-IP-address>
```

10. On all hosts, except for UEBA, stop and disable metricbeat:

```
systemctl stop metricbeat

systemctl disable metricbeat
```

Note: For NetWitness Platform without UEBA, you can stop and disable metricbeat on all hosts through salt:
`salt '*' cmd.run 'systemctl stop metricbeat && systemctl disable metricbeat'`

11. (Optional) - If you are not reinstalling New Health and Wellness (on same or other hosts), you can also remove metricbeat package and configuration:

a. Package to uninstall:
`metricbeat`

b. Service configurations to uninstall:

- `/etc/metricbeat`
- `/var/log/metricbeat`
- `mongo account`
- `systemd configuration`

12. Refresh the New Health and Wellness host:
`nw-manage --refresh-host --host-key <node-ip>`
Make sure that the New Health and Wellness service is not installed or running and metricbeat service is not active on the New Health and Wellness host.

13. If you are not reinstalling New Health and Wellness on another host, you must refresh UI hosts (NetWitness Server host and Analyst UI) to update NGNIX:

```
nw-manage --refresh-host --host-key <node-ip>
```

Note: After uninstalling New Health and Wellness, if you want to install New Health and Wellness again, see "New Health and Wellness" in the *Deployment Guide*.

Manage NetWitness Platform Updates

NetWitness issues NetWitness 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 NetWitness Community (https://community.netwitness.com/) and follow the steps described there. Additional information is available in the "Apply Version Updates to a Host" topic in the *Hosts and Services Getting Started Guide* and in System Updates Panel - Settings Tab.

Reissue Certificates

Introduction

For a secure deployment, NetWitness has installed internal NetWitness-issued certificates such as CA Certificate and Service certificates .

The validity for NetWitness certificates are as follows:

- CA root certificate for 11.x deployment is valid for 10 years
- CA root certificate for 10.6.x deployment is valid for 5 years
- Service certificates are valid for 1000 days

> **Note:** The certificate expiration warning is triggered 30 days prior to expiration.

When these certificates are about to expire or have expired, you must renew and reissue the certificates as soon as possible to avoid any issues with your NetWitness deployment.

> **Note:** You can view the expiration details, by executing the `ca-expire-test-sh` script on the NetWitness Server. For more information, see Reissue root CA security certificates on NetWitness Platform 11.x and download the script.

CA Certificate Reissue

To renew the CA certificates, do the following:

- Before you upgrade from 10.6.x to 11.x, check the expiry and reissue those certificates. For more information, see the Reissue root CA security certificates on NetWitness Platform 11.x.
- If you are on 10.6.x , check the expiry and reissue all the certificates. For more information, see the Reissuing security certificates on NetWitness Platform 10.6.x.

> **Note:** If you have Windows Legacy Collectors (WLC) in your deployment, renew the CA certificate of the WLC after renewing the CA certificate of the NetWitness Admin Server.

Service Certificate Reissue

To renew the Service certificates, do the following:

- If your hosts are on NetWitness Platform 11.3 or later, you must use the `cert-reissue` script. For more information, see the Reissuing Service Certificate .
- If your hosts are on 11.1.x or 11.2.x, you must upgrade the NetWitness Platform to 11.3 or later and run the `cert-reissue` script.

Note: If you have a host that is decommissioned or plan to remove, do not renew the certificate for that host.

Reissuing Service Certificate

You can reissue service certificates in the following two ways.

- All at once
  Reboot NW Server host after the `cert-reissue --host-all` command completes.
- One at a time
  Reissue the NW Server host certificates first, restart the host, then reissue each component host.

IMPORTANT: If you are reissuing certificates for each host individually (one at a time), you must reissue the certificate for the NW Server host before you can reissue certificates for any other host.

When to Use the `--host-all` Argument

Use the `cert-reissue --host-all` command string if you have a large number of hosts. Make sure that:

- All your hosts are running 11.3.0.0 or later.
- All your hosts are online.
- The NW Server host run time services are running.

`cert-reissue` Arguments and Options for All Hosts

The following tables lists the argument you can use to reissue certificates for all hosts at one time. See Troubleshooting Cert-Reissue Command for additional options you can use with Customer Support to troubleshoot errors.

Arguments	Description
`--host-all`	Reissues certificates for all hosts at one time applying system health checks and restarts services. **Note:** If even one host is not online, this command fails. If you have numerous hosts in your deployment, make sure that all hosts are up and running.

Caution: Make sure you do not run this argument on a node or host that you plan to remove or decommission.

When to Use the Individual Host Argument (`--host-key <ID, IP, hostname or display name of host>`)

The `cert-reissue --host-key <ID, IP, hostname or display name of host>` command reissues a certificate for an individual host. You may want to reissue certificates for an individual host if you have a small number of hosts.

Make sure that:

- Each host is running 11.3.0.0 or later.
- Each host is online.
- The NW Server host run time services are running
- You reissue certificates for the NW Server host first.

Note: You must run the command for the NW Server host first and reboot that host before you run the command for each component host.

Reissuing Certificates for All Hosts Except Windows Legacy Collection (WLC) host

Use the `cert-reissue` command to reissue certificates for all hosts except the WLC host with the following procedures.

Running the Cert-Reissue Command for All Hosts

1. SSH to the NW Server host.
2. Submit the appropriate command string.
   `cert-reissue --host-all`

Running the Cert-Reissue Command for an Individual Host

1. SSH to the NW Server host.
2. Submit the appropriate command string:
   `cert-reissue --host-key <ID, IP, hostname or display name of host>`

Reissuing Certificates for a WLC Host

You must use the `wlc-cli-client` utility to reissue certificates for a WLC host (you cannot use the `cert-reissue` command). You also need to specify a number of WLC identification parameters with this utility.

Note: The certificates for a Windows Legacy Server host are stored in the following directories on the host.
`C:\ProgramData\netwitness\ng\logcollector_cert.pem`
`C:\ProgramData\netwitness\ng\logcollector_dh2048.pem`
Th validity period of WLC certificates can range from 2 to 20 years. If you rename or remove the files and restart **NwLogCollector** Service, NetWitness regenerates them.
`/ssl/truststore.pem` - is no longer used in 11.x
Every reissue of a certificate on the Windows Legacy server creates a new private key.

To reissue certificates on a WLC host.

1. SSH to the NW Server host.
2. Submit the following command string.
   ```
   wlc-cli-client --cert-renew --host 10.129.43.13 --port 50101 --use-ssl
   false --username <nwadmin service account> --password <'nwadmin service
   account password'> --ss-username <deploy_admin> --ss-password <'deploy_
   admin password'>
   ```

   Note: nwadmin service account is the WLC rest UI User and **'nwadmin service account password'** is the WLC rest UI password.

Successful Reissue Summary Report

When you run `cert-reissue --host-all` , the following summary report will be displayed if all hosts are online, all run time services are running, and all hosts on version 11.4.0.0 or higher.

```
+---------+--------------------+--------+-----------------------------------------------------+
|         | Host               | Status | Message                                             |
+---------+--------------------+--------+-----------------------------------------------------|
|<host-id>| <IP-address>       |Success |Cert reissue successful                              |
|<host-id>| <IP-address>       |Success |Cert reissue successful                              |
|<host-id>| <IP-address>       |Success |Cert reissue successful                              |
|<host-id>| <IP-address>       |Success |Cert reissue successful                              |
|<host-id>| <IP-address>       |Success |Cert reissue successful                              |
+---------+--------------------+--------+-----------------------------------------------------+
```

Unsuccessful Reissue Summary Reports

You must contact Customer Support (https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897) to troubleshoot problems. You know there is a problem if any `<host-id>` does not return a `Success`**Status**. `Success` indicates that certificates were reissued for a host. The following examples illustrate unsuccessful reissues.

Reissue Failed for Host and Aborted Command

The following three examples illustrate the failure of certificate reissuing for any hosts.

```
+---------+--------------------+--------+-----------------------------------------------------+
|         | Host               | Status | Message                                             |
+---------+--------------------+--------+-----------------------------------------------------|
|<host-id>| <IP-address>       |Failed! |failed to connect, is host online?                   |
|<host-id>| <IP-address>       |Failed! |service(s) down                                      |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
+---------+--------------------+--------+-----------------------------------------------------+
```

```
+---------+--------------------+--------+-----------------------------------------------------+
|         | Host               | Status | Message                                             |
+---------+--------------------+--------+-----------------------------------------------------|
|<host-id>| <IP-address>       |Failed! |version <version-earlier-than-11.3.0.0> not supported|
|<host-id>| <IP-address>       |Failed! |version <version-earlier-than-11.3.0.0> not supported|
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
+---------+--------------------+--------+-----------------------------------------------------+
```

Reissue Certificate Partially Executed

The NW Server Host certificates were reissued but failed to properly distribute the reissued certificates to one or more component hosts.

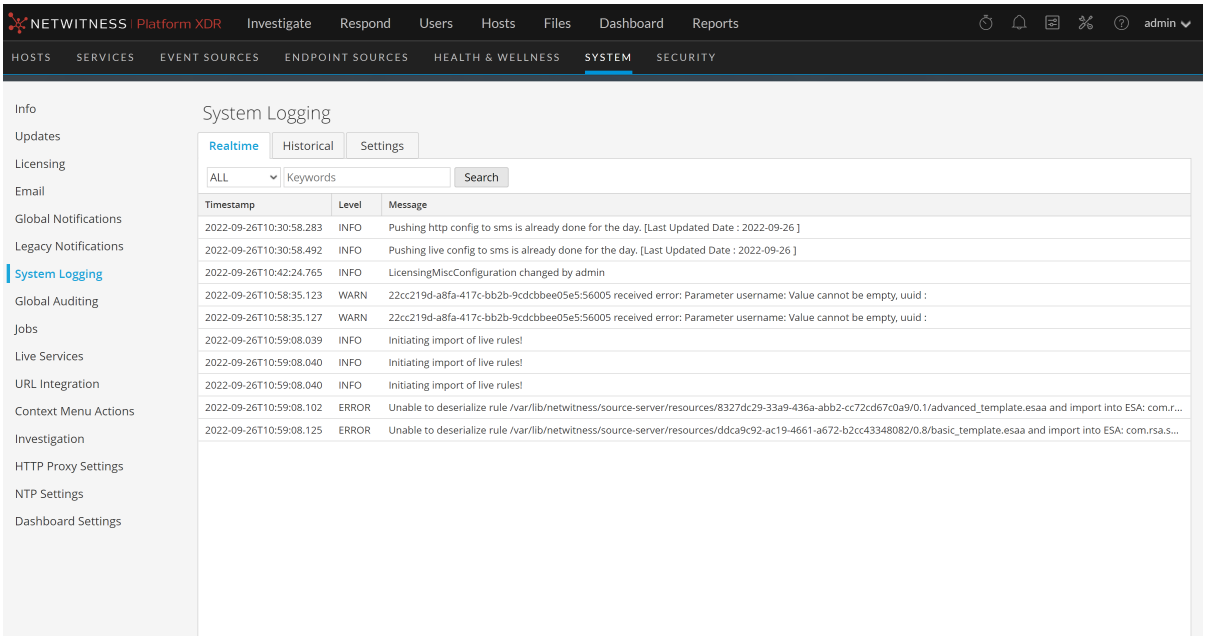
```
+---------+--------------------+
|         | Host               |
+---------+--------------------+
|<host-id>| <IP-address>       |
|<host-id>| <IP-address>       |
+---------+--------------------+
...
+---------+--------------------+--------+-----------------------------------------------------+
|         | Host               | Status | Message                                             |
+---------+--------------------+--------+-----------------------------------------------------|
|<host-id>| <IP-address>       |Partial |Reissue completed, triggers failed                   |
|<host-id>| <IP-address>       |N/A     |[ Skipped… ]                                         |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
|<host-id>| <IP-address>       |N/A     |[ Skipped... ]                                       |
+---------+--------------------+--------+-----------------------------------------------------+
```

Display System and Service Logs

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

View System Logs

1. Go to **(Admin) > System.**
2. In the options panel, select **System Logging**.

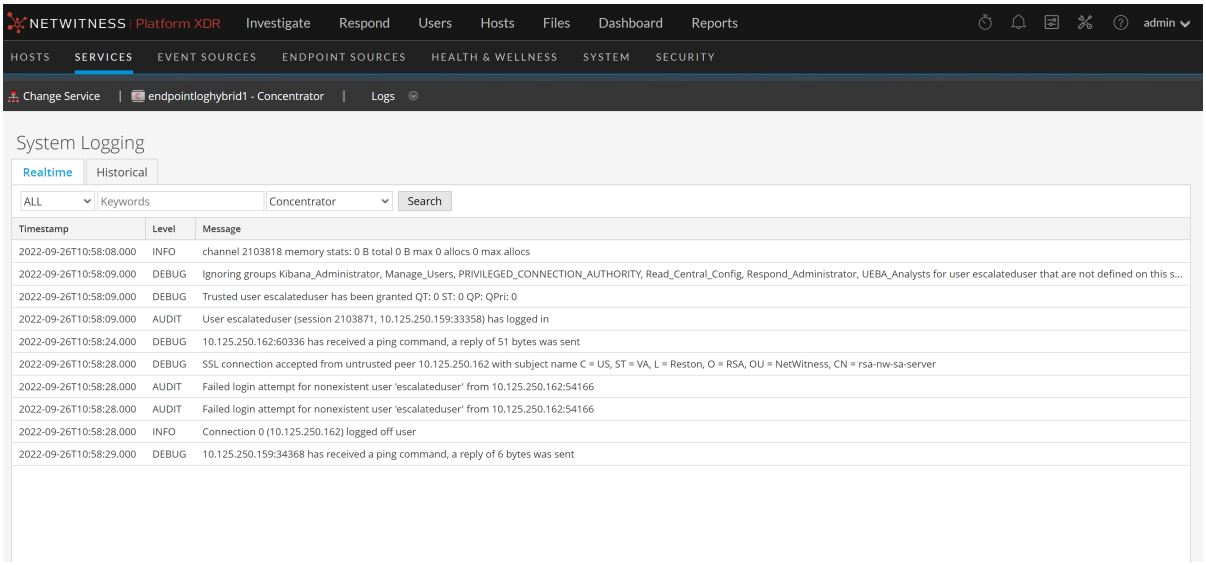


Display Service Logs

To display NetWitness service logs:

1. Go to **(Admin) > Services**.
2. In the **Services** list, select a service.

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



Filter Log Entries

To filter the results shown in the Realtime tab:

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

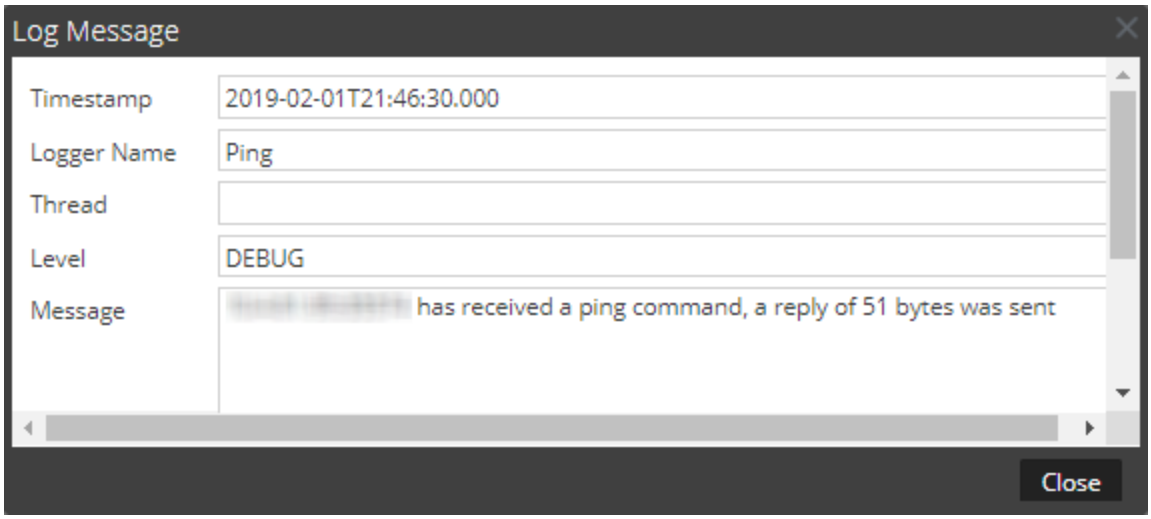
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

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

1. Double-click a log entry.

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



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

Access Reporting Engine Log File

All Log Files

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

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

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

Upstart Logs

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

An upstart log file is a system log file, which means that 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 provides a searchable view of the NetWitness log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the service. You can export logs from the current view.

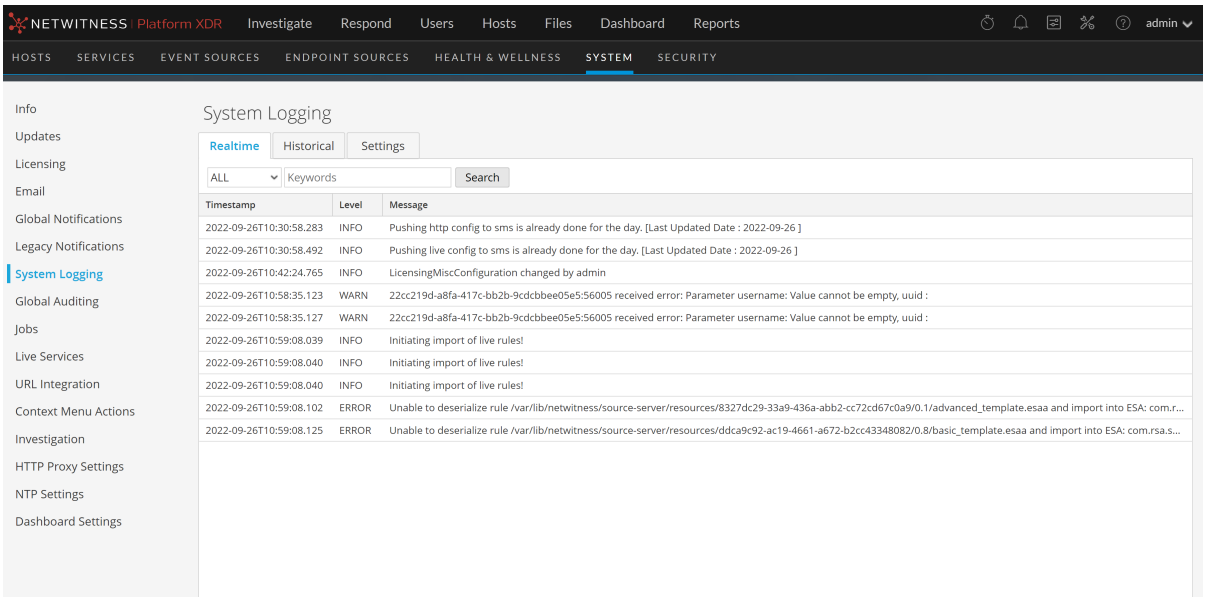
Display the Historical System Log

To display the historical log for the system:

1. Go to **(Admin) > System.**
2. In the options panel, select **System Logging**.

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

   A list of historical logs for the system is displayed.



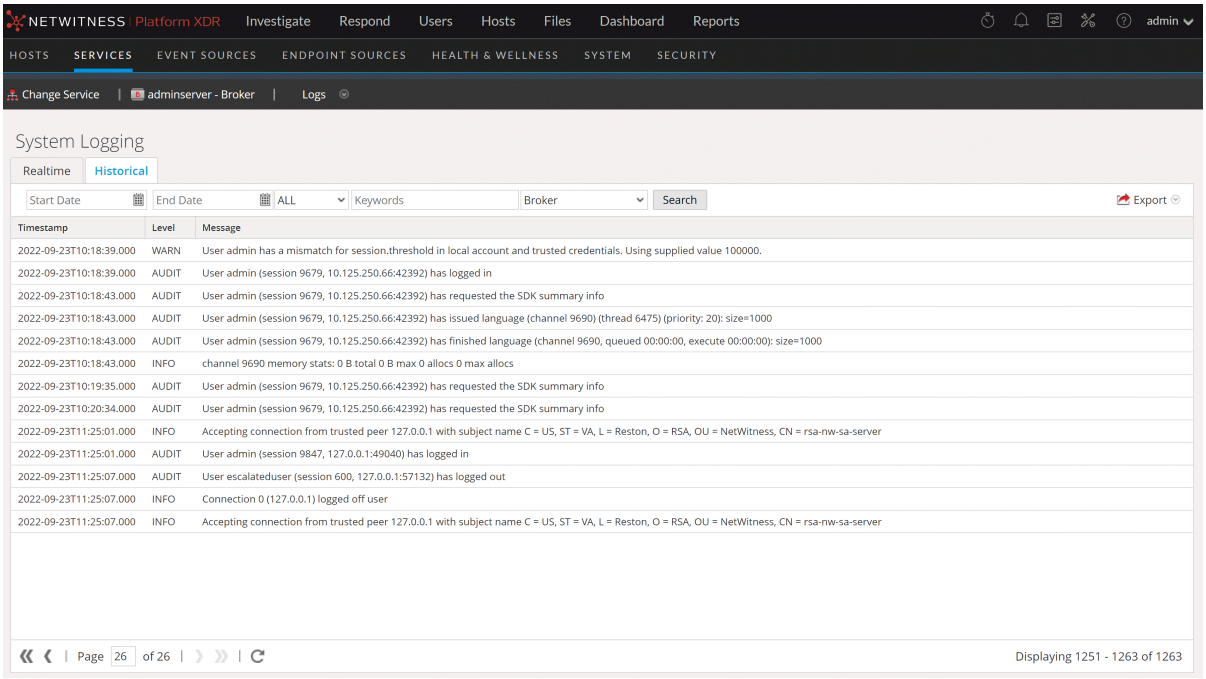
Display a Historical Service Log

To display the historical log for services:

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

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

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



Search Log Entries

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

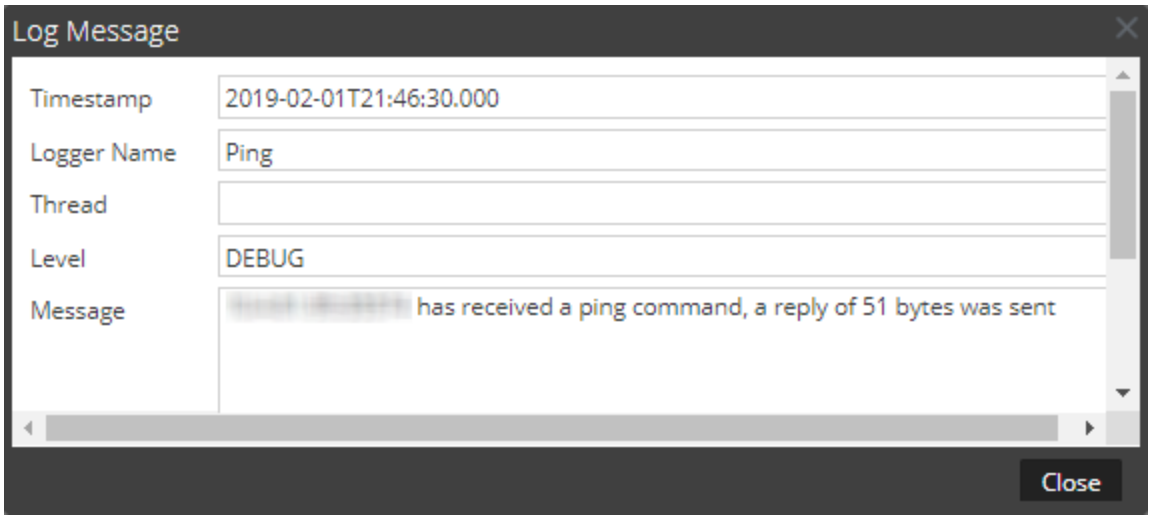
1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
3. (Optional) For service logs, select the Service: host or service.
4. Click **Search**.
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

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

1. Double-click a log entry.

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



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

Page Through Log Entries

To peruse the different pages of the list, 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 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`.

Maintain 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.

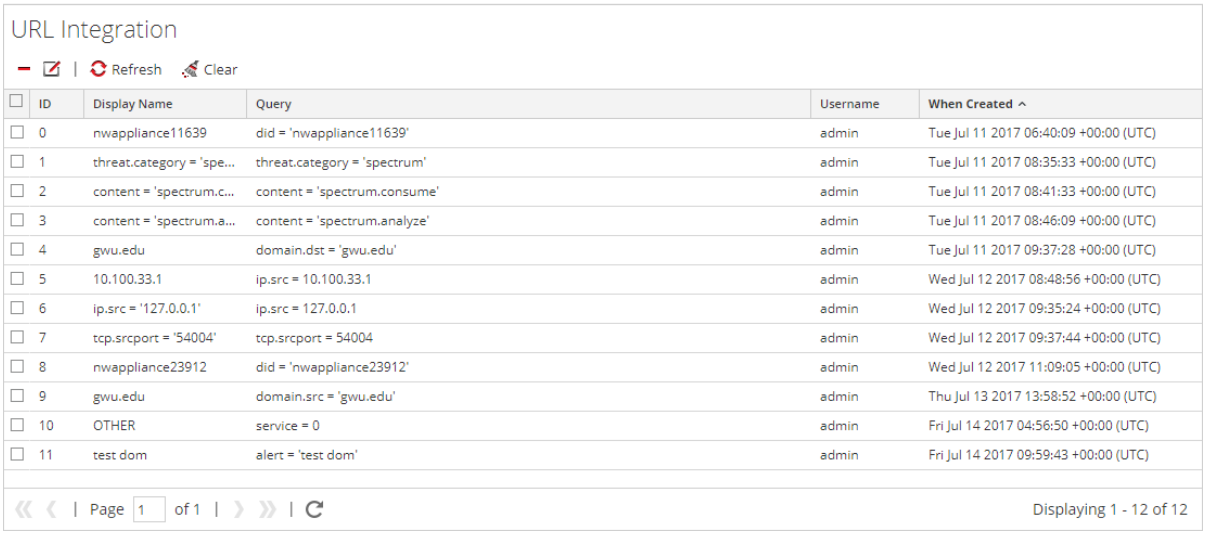
The URL Integration panel provides a list of queries and allows users who have the proper permissions to modify this underlying source of data and analyze the query patterns of other users of the NetWitness system. Within the panel, you can:

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

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

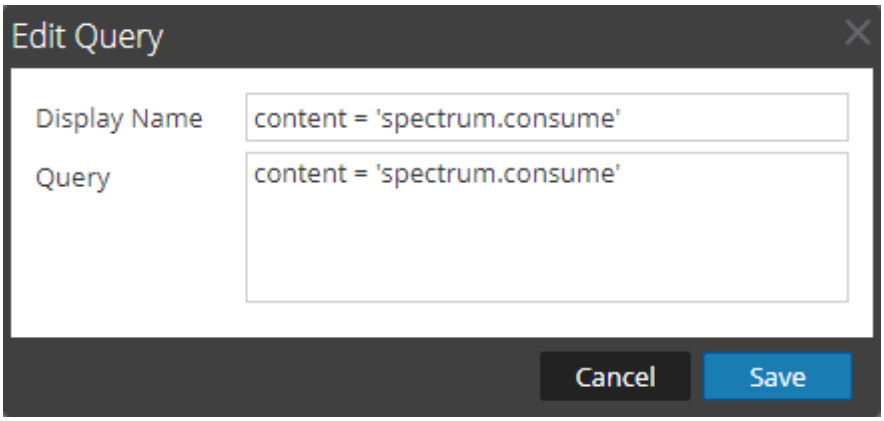
Edit a Query

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



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

   The **Edit Query Dialog** is displayed.



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

Delete a Query

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

To remove a query from NetWitness 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 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.

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 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. This value will change based on the service being connected to for analysis.
- <encoded query> is the URL-encoded NetWitness 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/2018-09-01T00:00/2018-10-31T00:00

Examples

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

All activity on 03/12/2018 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 3/12/2018 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 source (src) and destination (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.

Manage the deploy_admin Account

The depploy_admin account is used on every NetWitness host, and must be kept in sync between all hosts. Prior to 11.4.1, the process to change the deploy_admin account required administrators to log into every NetWitness host and run the /opt/rsa/saTools/bin/set-deploy-admin-password script on each system. Starting with 11.4.1, the deploy_admin password is centrally managed with the nw-manage script on the NW Server. nw-manage script execution updates the password on all NetWitness component hosts that use the deploy_admin account. The nw-manage script output displays the password update results for each host. If a NetWitness component host is down or unreachable for any reason, the nw-manage script provides an additional option to synchronize the deploy_admin password on the previously unresponsive host with the NW Server when that host becomes available again.

The following procedures describe how to change the deploy_admin password for all hosts in your environment, for hosts in a mixed version environment, and for hosts that are unavailable during the first attempt to change the deploy_admin password.

Change the deploy_admin Account Password

1. Log in to the NW Server host using SSH or the NwConsole.
2. Run the following command:
   nw-manage --update-deploy-admin-pw
   A prompt for the new password is displayed.
3. Enter the new password.

Change the deploy_admin Account Password in a Mixed Version Environment

If you are operating in a mixed version environment (for example, NW Server is on a newer version (greater than or equal to 11.4.1) and the NW component hosts are still on an older version of NetWitness (less than 11.4.1), the nw-manage script prompts you to run the /opt/rsa/saTools/bin/set-deploy-admin-password script on those older component hosts **first**. After the hosts on the older versions are updated, you rerun the nw-manage script on the NW Server with the --skip-version-checks argument.

1. On each component host that is on an older version, reset the deploy_admin password by running the following command:
   /opt/rsa/saTools/bin/set-deploy-admin-password
   This resets the deploy_admin password on all the component hosts with the older versions.
2. Log in to the NW Server host using SSH or the NwConsole and run the following command:
   nw-manage --update-deploy-admin-pw --skip-version-checks
   A prompt for the new password is displayed.
3. Enter the new password.

Change the deploy_admin Account Password for a Component Host that is Unavailable

If a component host is down or otherwise unreachable the first time you run the `nw-manage` script, it is identified as skipped in the `nw-manage --update-deploy-admin-pw` output. When the host is back online, its `deploy_admin` password must be synchronized with the NW Server.

To synchronize the previously unreachable host with the NW Server:

1. Log in to the NW Server host using SSH or the NwConsole.
2. Run the following command:
   ```
   nw-manage --sync-deploy-admin-pw --host-key <ID, IP, hostname or display name of host>
   ```

NW Server Host Secondary IP Configuration Management

Starting with 11.5, the NW Server has a new attribute, `secondary IP` that facilitates automated failover and IP address change management.

Note: For clarification, this attribute is simply another metadata host attribute that is specific to the NW Server; it does NOT describe, nor is it related to, a secondary network interface on the NW Server.

In the failover use case, the active NW Server has a `secondary IP` value that matches the standby server IP address. This `secondary IP` value is known to the other NetWitness hosts, and when the primary NW Server fails to respond in a timely fashion due to an IP address change of the active NW Server, or when there is a scheduled failover to the NW standby server, the other NetWitness hosts and services are configured to automatically attempt to connect to the secondary IP address, which in this case is the NW standby server.

The `secondary IP` attribute is also used for NW Server IP address change and for the NW standby server. The NW Server IP address change procedures automatically populate the secondary IP address of the NW Server to the new IP address and propagate that information to the other NetWitness hosts and services. Then, similar to the failover use case when NW Server's original IP address is no longer valid and the new IP address is active, the NetWitness hosts and services automatically switch to the new secondary IP address, which becomes the new NW Server IP address. If the NW standby server's IP address is changed, the `secondary IP` attribute on the NW Server needs to be updated with the new NW standby server IP address.

The `secondary IP` attribute is managed primarily with automated processes, but there are use cases that require manual management of the NW Server host `secondary IP` attribute, such as an IP address change of the NW standby server or a one-time registration during an NW standby server upgrade.

The `secondary IP` is managed using the `nw-manage` script on the NW Server:

- To add a secondary IP address to the NW Server host, run the following command:
  `nw-manage --add-nws-secondary-ip --ipv4 <secondary ip address>`
- To remove a secondary IP address from the NW Server host, run the following command:
  `nw-manage --remove-nws-secondary-ip --ipv4 <secondary ip address>`
- To view secondary IP addresses assigned to the NW Server host, run the following command:
  `nw-manage --get-nws-secondary-ip`

For information about changing IP addresses, see Change Host Network Configuration.

For information about failover procedures, see "Warm Standby NW Server Host" in the *Deployment Guide for NetWitness Platform*.

Change Host Network Configuration

This topic describes how to change the network configuration for NW Server and component hosts in your environment. **The instructions in this section assume that all the hosts in your environment are on version 11.7 or later**

Note: If your NW Server is referenced by other NW hosts that use a Network Address Translation (NAT) IP address, and you want to change the NAT IP address, you must remove the old NAT IP address and add the new NAT IP address using the instructions provided in NW Server Host Secondary IP Configuration Management.

This section contains the following procedures:

- Change Host Network Configuration
- Change Network Configuration for Warm Standby (Secondary) Server
- Reconnecting Component Hosts with NW Server Hosts

Note: Changing IPv6 addresses is not supported in version 11.7 and later.

Change Host Network Configuration

Use this procedure to update the network configuration for any host type in your environment for version 11.7 or later.

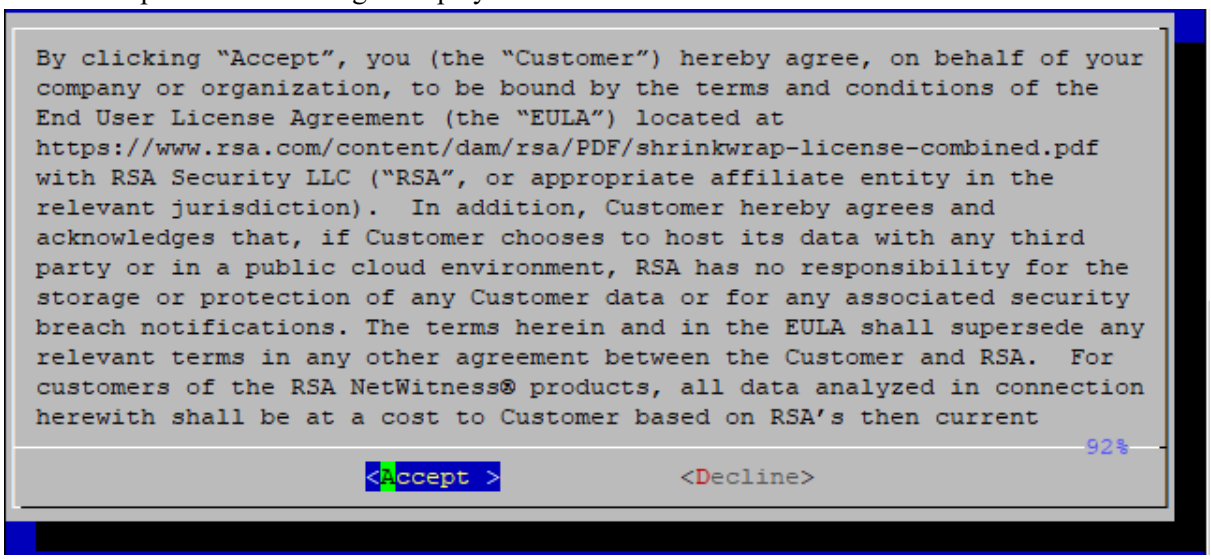
To change the network configuration of a host:

1. From the console, log in to the host for which you wish to change the network configuration.

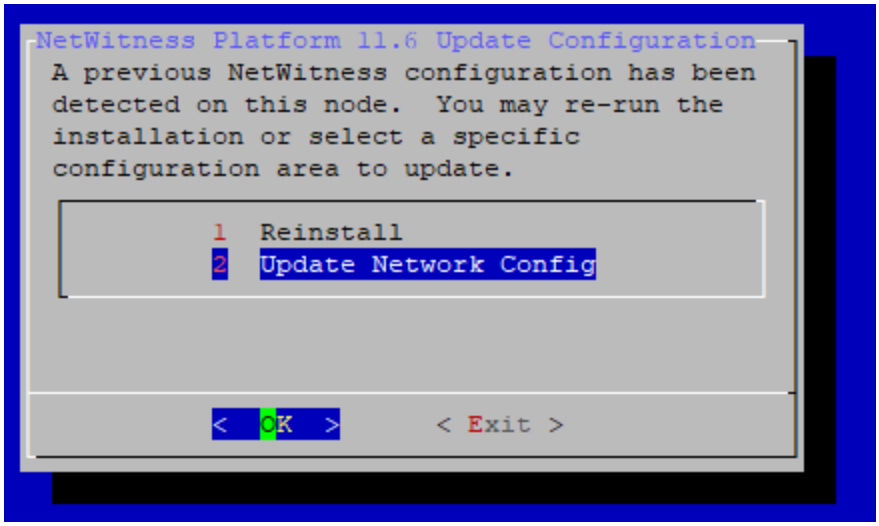
   Note: If you are updating the IP address of your NW Server and you are using DHCP, run the following command before you go to step 2:
   ```
   nw-manage --add-nws-secondary-ip --ipv4 <new DHCP allocated ip address of NW Server>
   ```

2. Run the following command:
   ```
   nwsetup-tui
   ```

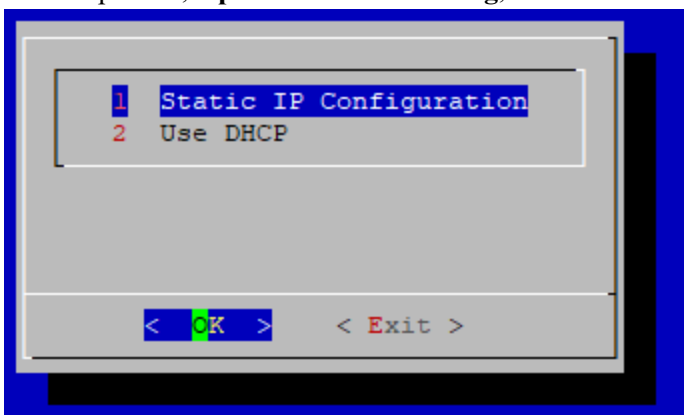
The nwsetup-tui license dialog is displayed.



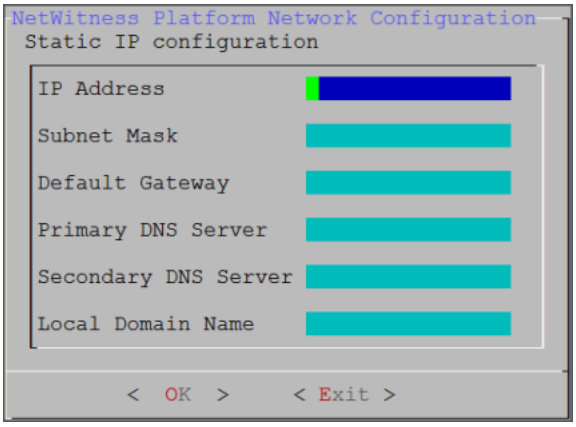
3. Click Accept. The NetWitness Platform Update Configuration dialog is displayed:



4. Select option 2, **Update Network Config**, and click **OK**.



5. Select option 1, **Static IP Configuration**, and click **OK**.
   The NetWitness Platform Network Configuration Static IP configuration dialog is displayed.



6. Enter the new network and DNS configuration and click **OK**.
   The new network and DNS configuration is applied to the host.

   Note: While changing the IP address, the user interface may become temporarily unavailable while the update is in process. The user interface will come back up shortly.

Note: After upgrading the NW Server host or a component host to 11.7 or later version, review the contents of the `/etc/hosts.user` file for any obsolete host entries. The `/etc/hosts.user` file contains system and user-generated entries that are not managed by NetWitness Platform. However, entries from `/etc/hosts.user` are merged with NetWitness Platform-generated host mappings to create and update `/etc/hosts`. To avoid conflicts with NetWitness Platform-generated mappings, and to avoid generating connectivity errors resulting from an IP address change, NetWitness recommends that you remove any entries in `/etc/hosts.user` that include a non-loopback IP address of a NetWitness Platform host. After updating `/etc/hosts.user`, you must refresh the system by running the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

Note: While changing a host's IP address or during failover, component hosts can become disconnected from NW Server hosts. Follow these steps to reconnect a host system to its NW Server system.
1. Log in to the component host using SSH or the console.
2. Run the command `nw-manage --override-nws-ip --ipv4 <current IP address of the NW Server.`
When this command completes, the component host is reconnected to the NW Server at the specified IP address.

Note:

- Before performing failover, make sure that the `deploy_admin` password of the Standby NW server is not expired. You can verify this by logging in to the Standby NW server nw-shell.

```
nw-shell
offline » login
user: deploy_admin
password: <deploy_admin_password>
WARNING: Login failure: User credentials have expired (The following warning message confirms that your deploy_admin credentials have expired)
```

Next step, update the `deploy_admin` password using `nw-manage --update-deploy-admin-pw`
After the command is successfully executed, verify the `deploy_admin` password using `security-cli-client --quiet --get-config-prop --prop-hierarchy nw.security-client --prop-name platform.deployment.password`

- Before performing failover, make sure that your Standby NW server certificates are up to date.

Follow the steps in the sections that apply to your environment.

- SSO
- Reporting Engine
- UCF
- PAM
- ECAT
- RSA NetWitness Orchestrator (By Demisto)
- Audit Logging
- Health and Wellness
- Malware Analysis
- Windows Legacy Collection

SSO

Update Configuration for Single Sign-On

Note: You must disable SSO configurations ONLY when NW Server IP is changed.

When the host network is configured with a new IP address, the SSO configurations also must be updated.

To do this:

1. Disable the SSO configuration using `nw-shell` after failover from new IP.
   To resolve this issue you must disable SSO manually, using the following commands:
   a. SSH to `admin server node`.
   b. Connect to `nw-shell`.
   c. Connect to admin server service using the `connect --service admin-server` command.

d. Log in to admin server using the `login` command.

e. Enter the admin username and password.

f. Execute the following commands:

- `cd /rsa/security/authentication/web/saml/sso-enabled`
- `set false`
- `logout`
- `exit`
- `systemctl restart rsa-nw-admin-server`

2. Change the host IP address to the new IP.

3. Generate the new metadata and reupload it in ADFS. For more information, see the "Configure SAML 2.0 provider settings for portals" topic in the Microsoft documentation.

For more information, see the "Troubleshooting" topic in the *System Security and User Management Guide.*

Reporting Engine

Update Configuration for Reporting Engine

Note: You must update the Reporting Engine configurations ONLY when NW Server IP is changed.

When the host network is configured with a new IP address, you must update and verify the Reporting Engin configurations. The hostname for NetWitness configurations under the Output Actions must be updated with the new IP.

To manually configure the new IP, perform the following steps:

1. Log in to NetWitness Platform.
2. Navigate to (Admin) > **Services > Reporting Engine > View > Config**.
3. Click the **Output Actions** tab.
4. Add the new IP address in the **Hostname** field.
5. Click **Apply**.

UCF

To enable UCF to communicate with NetWitness Platform:

1. On the UCF server, execute the `runConnectionManager.bat` file (the same file that is used for adding connection details).
2. Select **Option #2, Edit endpoints**.
3. Select the NW Server connection from the options that are displayed.
4. When you are prompted for Host Address (the old IP address is shown in parentheses) enter the new IP address.

   Note: Do not change any other setting.

PAM

If you have PAM configured, after the failover, you must configure the system again using the instructions in the "Configure PAM Login Capability" topic in the *System Security and User Management Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

ECAT

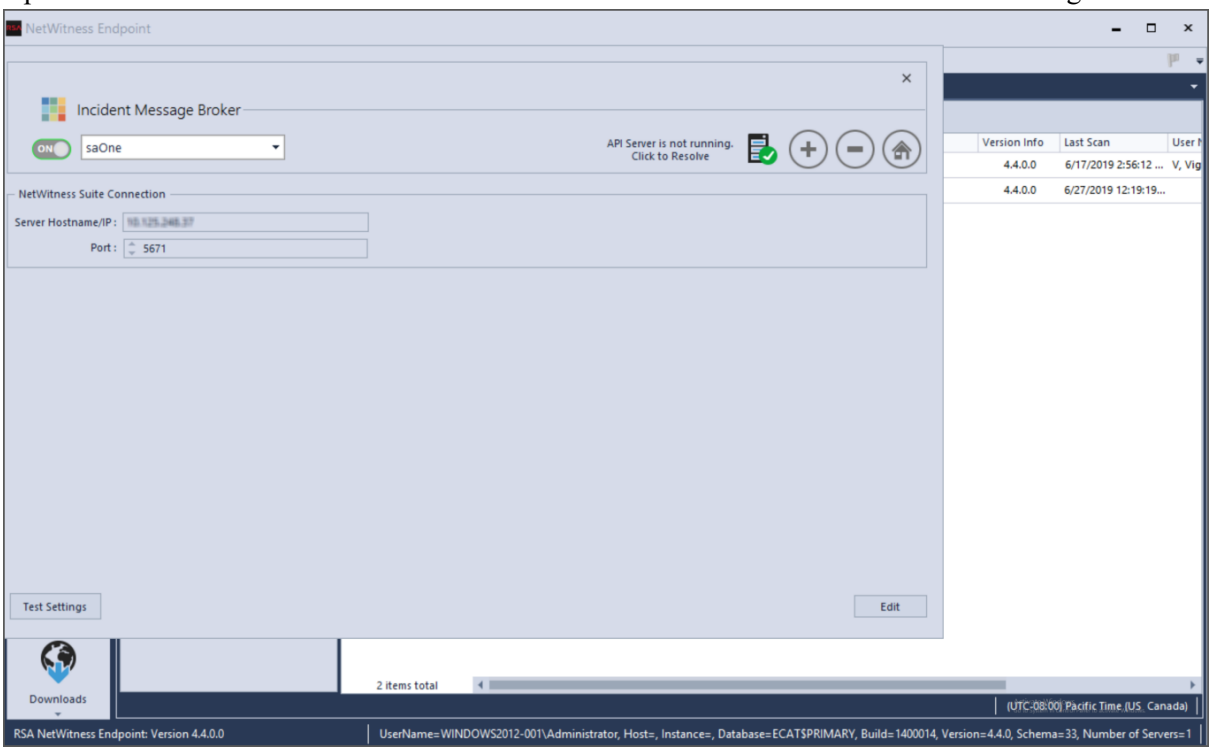
Update the following services:

- Incident Message Broker
- NetWitness Suite
- Syslog Server Settings

Incident Message Broker

1. Log in to the NetWitness Endpoint user interface and go to **Configure** > **Monitoring and External Components Configuration** > **Incident Message Broker**.

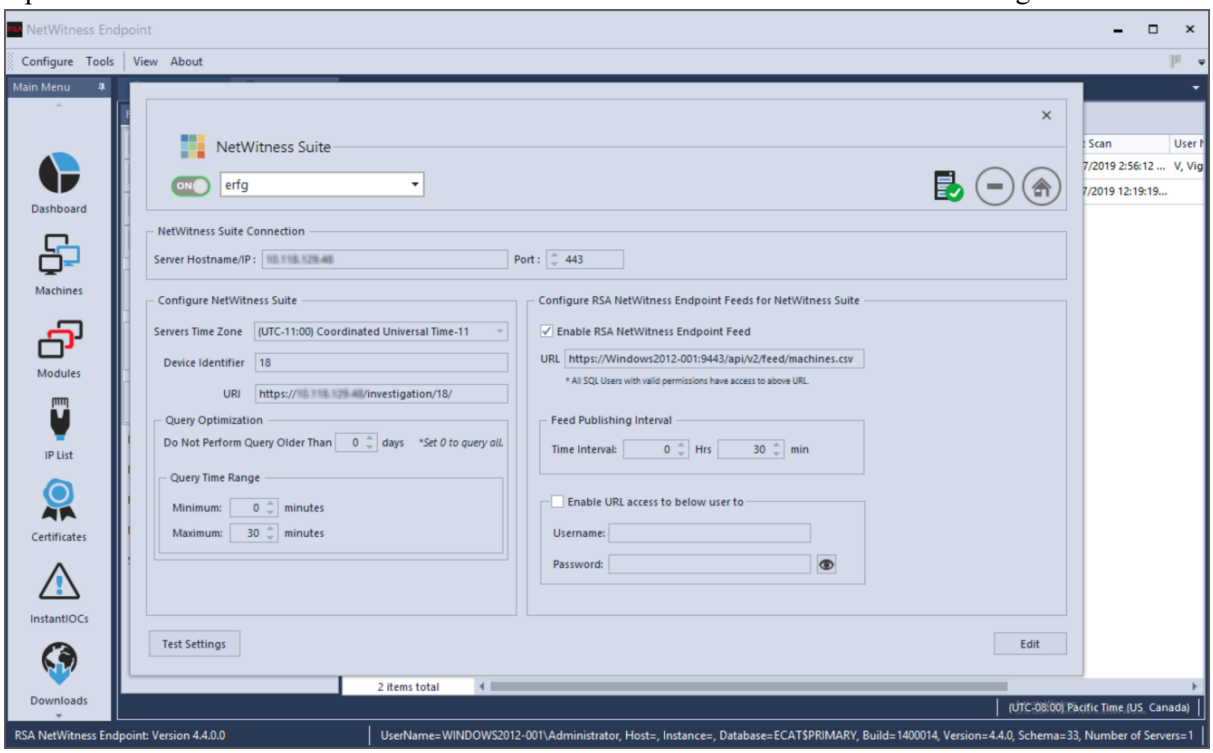
2. Update the server Hostname and IP Address to the current active server and test the settings.



NetWitness Suite

1. Log in to the NetWitness Endpoint user interface and go to **Configure** > **Monitoring and External Components Configuration** > **Netwitness Suite**.

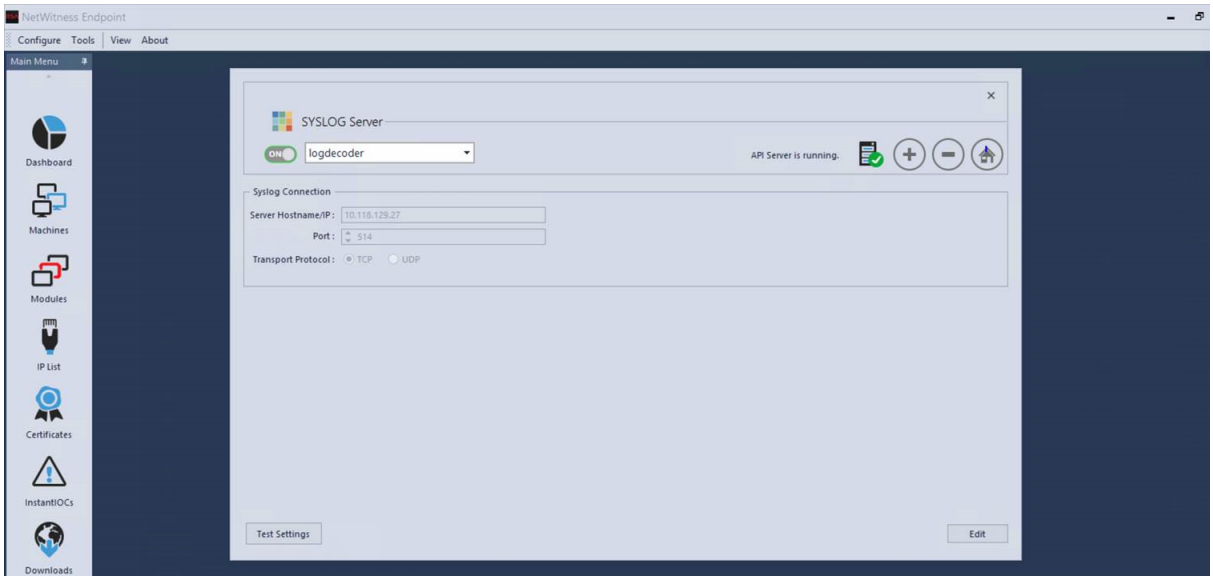
2. Update the server Hostname and IP address to the current active server and test settings.



Syslog Server Settings

If you are forwarding syslog messages to a NetWitness Platform Log Decoder, update the syslog server settings to point to the new IP address of the Log Decoder host.

1. Log in to the NetWitness Endpoint user interface and go to **Configure** > **Syslog Server**.

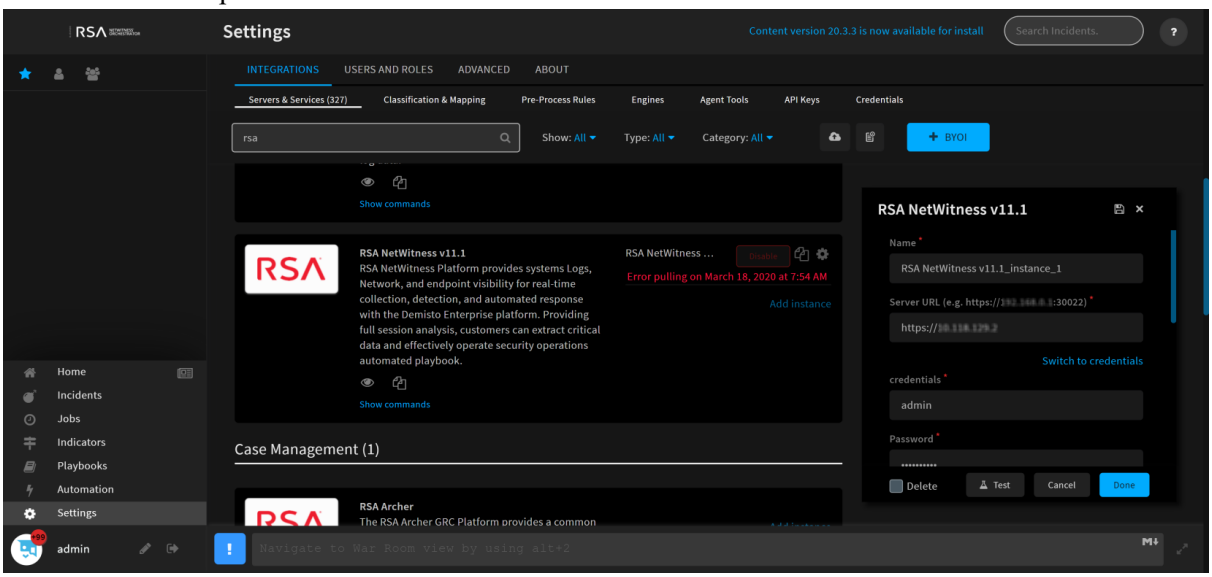


2. Select **logdecoder**, and in **Server Hostname/IP**, enter the new IP address of the Log Decoder host.

RSA NetWitness Orchestrator (By Demisto)

Update the Current Active NW Server to Fetch Respond Incidents and Alerts

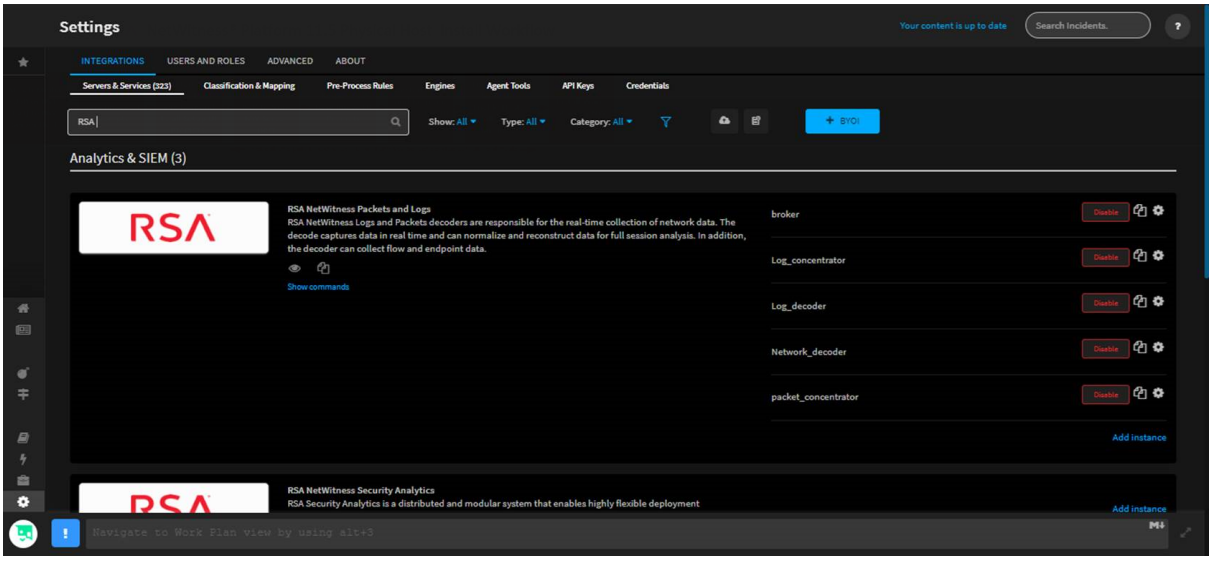
1. Log in to Orchestrator and go to **Settings** > **server&services**.
2. Edit the RSA NetWitness V11.1 instance by updating the server URL to the current active NW Server to fetch respond incidents and alerts.



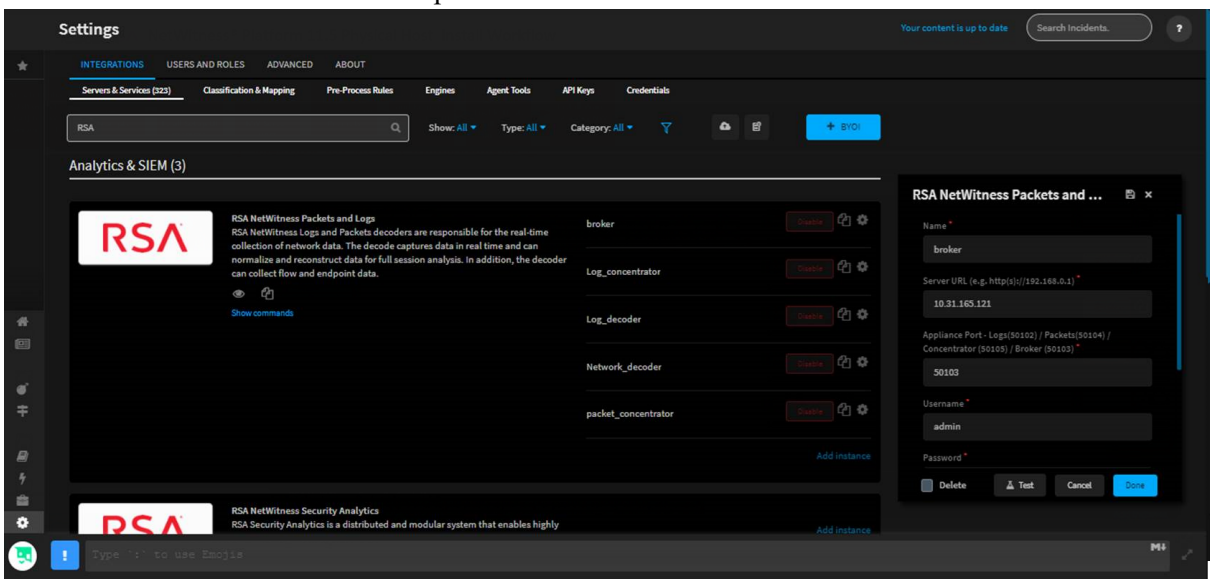
Update Component Hosts Acting as Data Sources

If you change the IP address of a component host, for example, a Concentrator, Network or Log Decoder, or Broker, that is acting as data source to the Orchestrator, update the following settings to point to the new IP address of the host.

1. Log in to Orchestrator and go to **Settings** > **server&services** and select the component host.



2. Enter the new IP address of the component host in **Server URL** and click **Done**.



Audit Logging

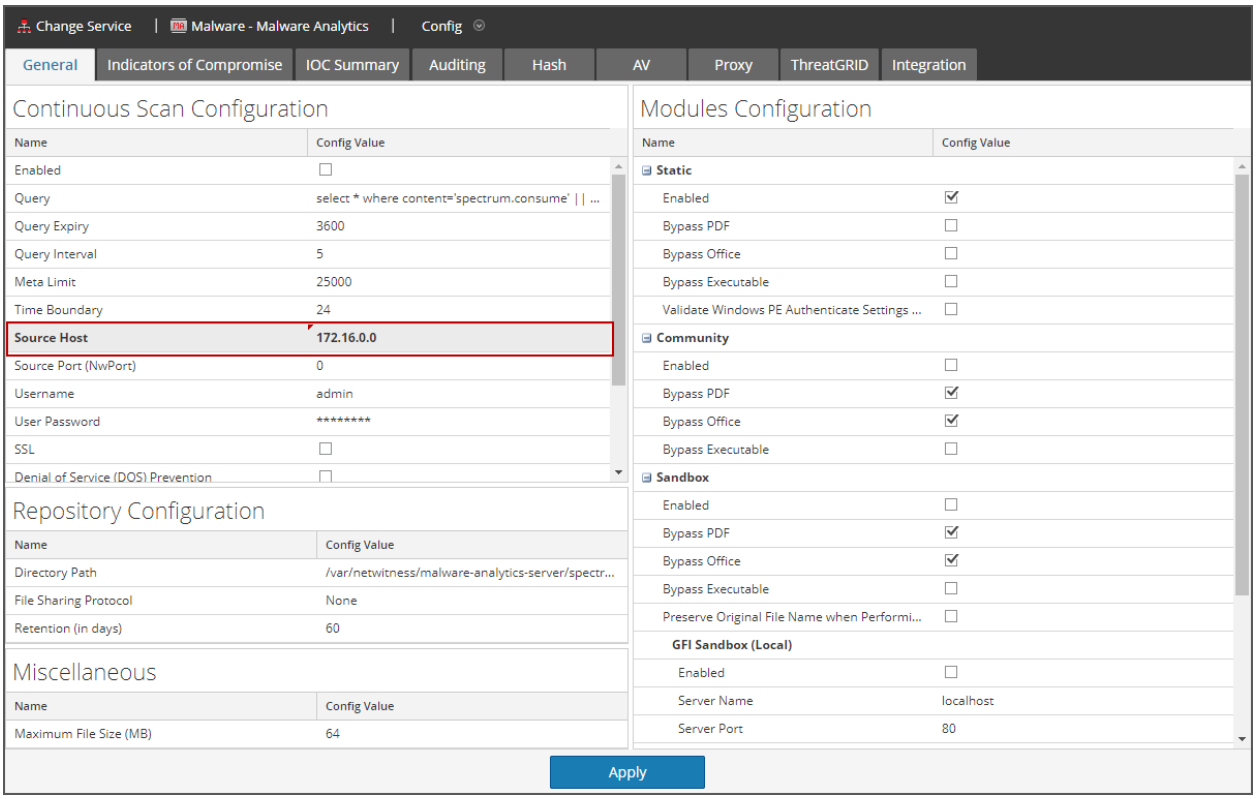
If you have changed the IP address of the NW Server, you must reconfigure audit logging. For instructions, see "Configure Global Audit Logging" in the *System Configuration Guide*.

Health and Wellness

If you have any Health and Wellness rules that contain IP addresses that have been changed, you must update those rules with the new IP addresses. For information about managing Health and Wellness rules, see "Monitor Health and Wellness using NetWitness Platform UI" in the *System Maintenance Guide*.

Malware Analysis

Source host IP address changes are not updated in the NetWitness user interface for Malware Analysis continuous scan configurations. You must manually update this configuration in the Malware Analysis Config view > **General** > **Continuous Scan Configuration** and update the source host IP address to the new host IP address.



Windows Legacy Collection

On occasion, you may need to change the IP address of your Windows Legacy Collector. You may also need to edit any Destination Groups that you have configured.

Change WLC IP Address

The following procedure describes how to change the IP address for your system.

1. Log onto the Windows Legacy Collector system and manually change the IP address on the system.
2. In the UI, confirm that the Log Collector service corresponding to the WLC system shows up in error (Red). It might take some time for it to reflect the changed status.
3. On the NetWitness Server, use the **nw-manage** utility to view the host information for the WLC using the following command:

   ```
   nw-manage --list-hosts
   ```

   Sample output from running the command is shown here:

   ```
   {
   "id" : "fdb8150c-e040-459e-8cc5-3c60ec2c65ae",
   "displayName" : "WLC-HOST-104",
   "hostname" : "10.101.216.102",
   "ipv4" : "10.101.216.102",
   "ipv4Public" : null
   } ]
   ```

   You use the value of **"id"** from your output in the following step.

4. Use the **nw-manage** utility to change the IP address of the WLC. For the **host-id** argument, use the value for the **"id"** that you noted from step 3. For the **ipv4** value, use the new IP Address to which you are changing.

   ```
   nw-manage --update-host --host-id "fdb8150c-e040-459e-8cc5-3c60ec2c65ae" --ipv4 10.101.216.105
   ```

5. After you see the message that the previous command ran successfully, go to the NetWitness Server UI and verify that the WLC service is running without any errors.

Edit Destination Groups For Log Collectors and VLCs

The Windows Legacy Collector is often configured with Destination Groups to forward events to Log Collectors or Virtual Log Collectors. If the IP address of any such Destination LC or VLC is changed, the Windows Legacy Collector can no longer forward events. To remediate this, you must edit the Destination groups for the WLC, making sure to select the new LC or VLC IP Address.

Change Network Configuration for Warm Standby (Secondary) Server

You can change the network configuration of a warm standby (secondary server) by following these steps:

1. Follow the steps described in Change Host Network Configuration to change the IP address on the secondary server.
2. Log in to the active NW Server and remove the previous secondary server IP address by running the following command:

   ```
   nw-manage --remove-nws-secondary-ip --ipv4 <previous standby server ip address>
   ```

3. On the active NW Server, add the new standby server secondary IP address value by running the following command:

   ```
   nw-manage --add-nws-secondary-ip --ipv4 <new standby server ip address>
   ```

4. Schedule the backup of the primary NW Server and the copying of backed-up data to the secondary NW Server. See step 18 in "Setup Secondary NW Server in Standby Role" in the *Deployment Guide for NetWitness Platform*.

For information about configuring warm standby servers, see "Warm Standby NW Server Host" in the *Deployment Guide for NetWitness Platform* and NW Server Host Secondary IP Configuration Management.

Reconnecting Component Hosts with NW Server Hosts

While changing a host's IP address or during failover, component hosts can become disconnected from NW Server hosts. Follow these steps to reconnect a host system to its NW Server system.

1. Log in to the component host using SSH or the console.
2. Run the following command:

   ```
   nw-manage --override-nws-ip --ipv4 <current IP address of the NW Server>
   ```

When this command completes, the component host is reconnected to the NW Server at the specified IP address.

Manage Custom Host Entries

If you have hosts in your environment that use custom entries, or if you want to use NAT IPv4 addresses for your hosts, this topic provides instructions for configuring these settings.

Manage Custom Host Entries in /etc/hosts

If you identify hosts in your environment that need custom entries, you can add custom entries for your hosts in the `/etc/hosts.user` file.

To add custom host entries:

1. From the console, log in to the host on which to define custom entries.
2. Add the custom entry to the `/etc/hosts.user` file.

To update or refresh a custom entry in `/etc/hosts`:

Run the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

Manage Public or NAT IPv4 Addresses for Hosts

To add or update public or Network Address Translation (NAT) IPv4 addresses for NW Hosts, run the following command:

```
nw-manage --update-host --host-id <NW Server Host UUID> --ipv4-public <IP address>
```

Manage Custom Jetty Configuration

If you want to have custom jetty configurations or additional JAVA_OPTIONS that persist during the upgrade, this topic provides the instructions for configuring custom jetty settings.

To add custom jetty configuration

1. From SSH prompt, create a copy of jetty configuration as `jetty.user` using the below command.
   `$ cp /etc/default/jetty /etc/default/jetty.user`
2. Edit the `/etc/default/jetty.user` and remove all lines EXCEPT one of the `JAVA_OPTIONS` additional settings lines.
   For example, `JAVA_OPTIONS="${JAVA_OPTIONS} -Drsa.primary.host=true "`
3. Edit the line with the option (in this example increasing the max memory option from 8G to 24G):
   `JAVA_OPTIONS="${JAVA_OPTIONS} -Xmx24G "`
4. Make sure to use the `JAVA_OPTIONS="${JAVA_OPTIONS} "` format to EXTEND the `JAVA OPTIONS`.

5. REMOVE the `[ -f /etc/default/jetty.user ] && source /etc/default/jetty.user` file.
6. Save the file.
7. Restart the jetty service.
   `systemctl restart jetty`

Note: When you overwrite the jetty.user custom config file, ensure that all the jetty configurations (JAVA_OPTIONS) present in /etc/default/jetty are available in this file. If any jetty configuration (JAVA_OPTIONS) is not available in the jetty.user file, you must copy it to the file and then restart the jetty service.

Configure FIPS Support

NetWitness 11.x ships with FIPS-validated 140-2 Cryptographic Modules that support all cryptographic operations within NetWitness. NetWitness leverages two modules that support a level three design assurance:

- RSA BSAFE Crypto-J
- RSA OwB

Both modules have been certified with an operational environment comparable to the standard NetWitness 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 https://csrc.nist.gov/publications/detail/fips/140/2/final.

The RSA BSAFE Crypto-J FIPS Certificate number is 3172, and OwB uses the CCME FIPS Module in FIPS-approved mode.

In 11.x, FIPS is enabled on all services except Log Collector. This includes Log Decoder and Decoder if they were FIPS-enabled in 10.6.x or any previous version. FIPS cannot be disabled on any services except for Log Collector, Log Decoder and Decoder.

Note: For a fresh installation of 11.x, 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 Network Decoder.

Note: For upgrades to 11.x from previous versions, the following conditions apply for the Log Collector, Log Decoder and Decoder services:
- Log Collector is not FIPS enabled after upgrading to 11.x, even if FIPS was enabled in a previous version. You must enable FIPS support after upgrading to 11.x. See the instructions in FIPS support for Log Collectors.
- If FIPS was enabled for the Log Decoder and Network Decoder services in a prevous version, FIPS will also be enabled in 11.x. However, if Log Decoder and Network Decoder were NOT FIPS enabled in a previous version, they will not be enabled in 11.x, 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.x to 11.x and FIPS was enabled in 10.6.x.

   a. Go to (Admin) > **Services**.

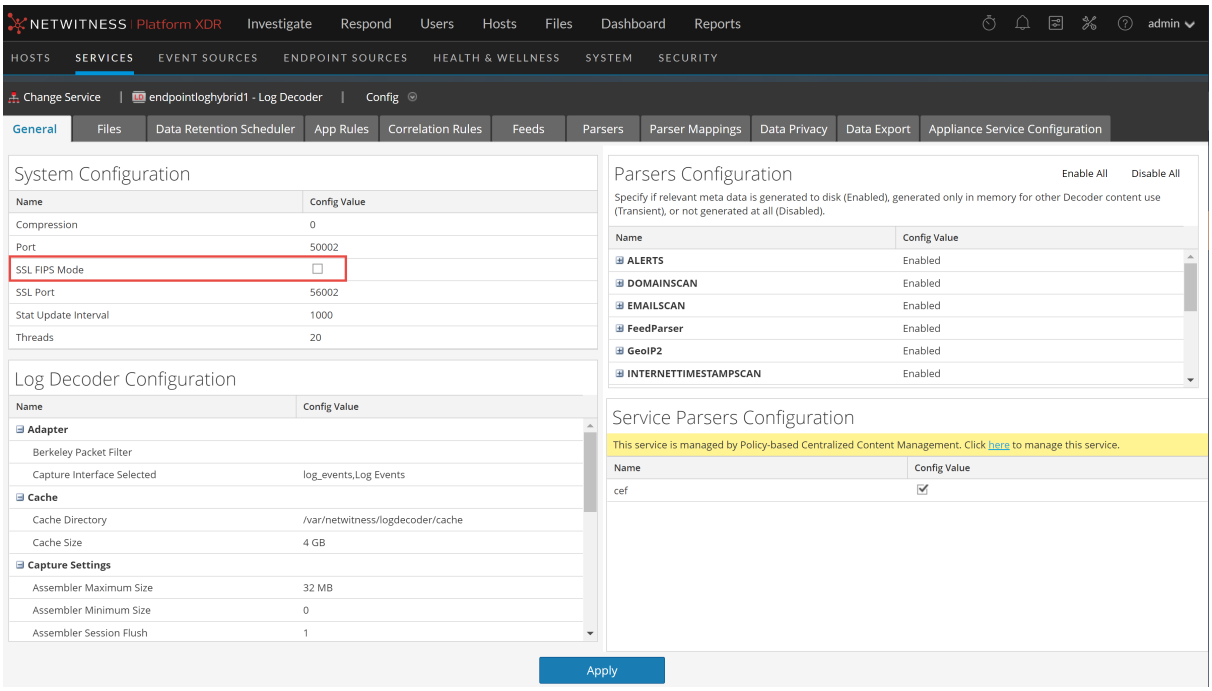
   b. Select the Log Collector service and go to **View** > **Config**.

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

FIPS support for Log Decoders and Decoders

To enable FIPS for Log Decoders and Decoders that did not have FIPS enabled in 10.6.x:

1. Go to (Admin) > **Services** and select a Log Decoder or Network 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**.

DISA STIG

Note: 11.3.1 feature - DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide) support was introduced in NetWitness Platform 11.3.1. Versions 11.0.0.0 to 11.3.0.0 do not support DISA STIG.

NetWitness Platform version 11.3.1 supports all Audit Rules in the DISA STIG Control Group. The supported version for DISA STIG is Red Hat Enterprise Linux V3R2. NetWitness will expand its support of STIG rules in future NetWitness Platform versions.

This section includes the following topics.

How STIG Limits Account Access

NetWitness Passwords

Generate the OpenSCAP Report

Manage STIG Controls Script (`manage-stig-controls`)

Rules List

Exceptions to STIG Compliance

IMPORTANT: All rules are enabled by default except for **control goup 1-ssh-prevent-root** an **control group 3-fips-kernel**. You can enable or disable rules by control group using the `manage-stig-controls` script.

How STIG Limits Account Access

The STIG hardening RPM helps to lock down information, systems, and software, which might otherwise be vulnerable to a malicious computer attack by limiting account access to a system. For example, the STIG script:

- Ensures that the account password has a length, complexity, expiration period, and lockout period that are in accordance with DISA best practices.
- Applies auditing and logging of user actions on the host.

NetWitness Passwords

NetWitness Platform requires passwords that are STIG compliant.

Generate the OpenSCAP Report

Security Content Automation Protocol (SCAP) is a line of standards or rules managed by the National Institute of Standards and Technology (NIST). It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying the presence of patches, checking system security configuration settings, and examining systems for signs of compromise.

The OpenSCAP report evaluates your environment against the SCAP rules. The results are sent to the `HOSTNAME-ssg-results.(XML|HTML)` depending on the output format you select.

Disable Rules in OpenSCAP Report that Hang the Report

There may be STIG rules that you do not want to include in the OpenSCAP report because they make the report hang. Use the following command to disable items on the SCAP report:

```
sed -i 's/select idref="rule-id" selected="true"/select idref="rule-id"
selected="false"/g' /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

where `rule-id` is the Rule ID that you can replace with the Rule ID that may hang during a test.

For example, the report has a rule ID called `partition_for_audit` (shown as `Rule ID: partition_for_audit`). If you disable a rule, OpenSCAP does not check against that rule. This means that you need to check for compliance to the `partition_for_audit` rule manually.

Install OpenSCAP

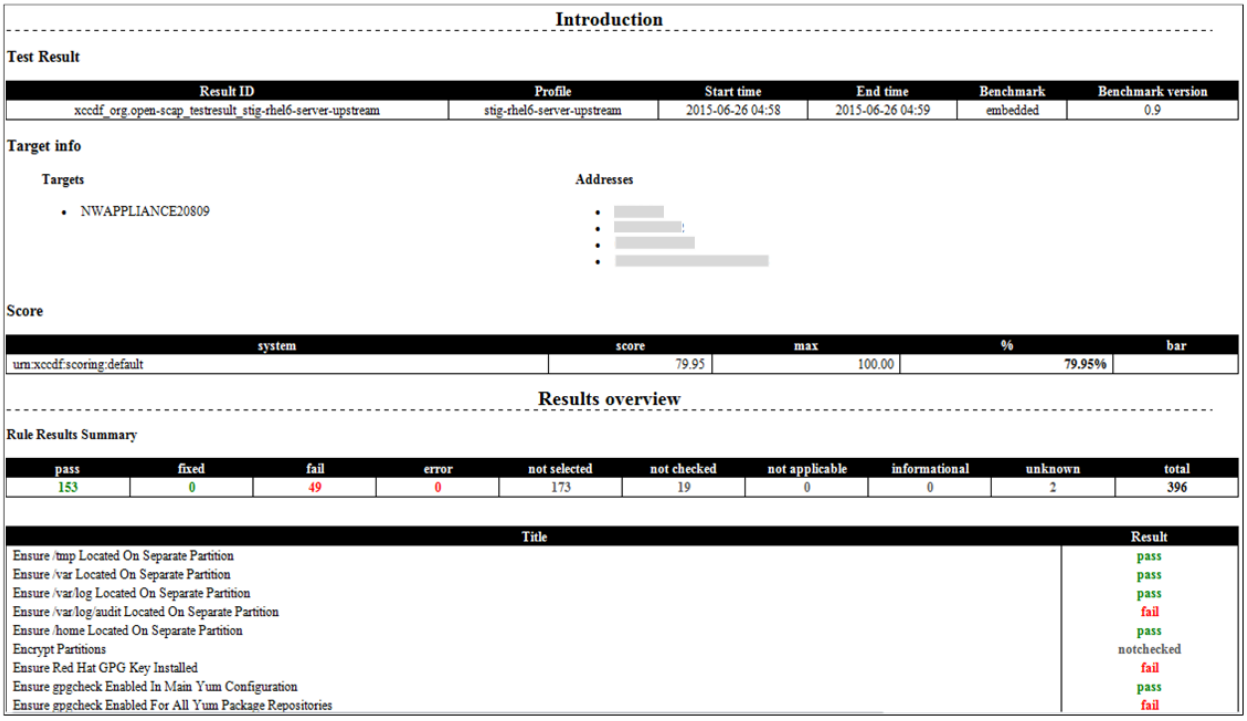
You must

1. SSH to the host
2. Execute the following commands.

```
yum install scap-security-guide
```

Sample Report

The following report is a sample section from an OpenSCAP report.



Introduction

Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_stig-rhel6-server-upstream	stig-rhel6-server-upstream	2015-06-26 04:58	2015-06-26 04:59	embedded	0.9

Target info

Targets

- NWAPPLIANCE20809

Addresses

- [redacted]

Score

system	score	max	%	bar
urn:xccdf:scoring:default	79.95	100.00	79.95%	

Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
153	0	49	0	173	19	0	0	2	396

Title	Result
Ensure /tmp Located On Separate Partition	pass
Ensure /var Located On Separate Partition	pass
Ensure /var/log Located On Separate Partition	pass
Ensure /var/log/audit Located On Separate Partition	fail
Ensure /home Located On Separate Partition	pass
Encrypt Partitions	notchecked
Ensure Red Hat GPG Key Installed	fail
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	fail

Report Fields

Section	Field	Description
Introduction - Test Result	Result ID	The Extensible Configuration Checklist Description Format (XCCDF) identifier of the report results.
	Profile	XCCDF profile under which the report results are categorized.
	Start time	When the report started.
	End time	When the report ended.
	Benchmark	XCCDF benchmark
	Benchmark version	Version number of the benchmark.
Introduction - Score	system	XCCDF scoring method.
	score	Score attained after running the report.
	max	Highest score attainable.
	%	Score attained after running the report as a percentage.
	bar	Not Applicable.
Results overview - Rule Results Summary	pass	Passed rule check.
	fixed	Rule check that failed previously is now fixed.
	fail	Failed rule check.
	error	Could not perform rule check.
	not selected	This check was not applicable to your NetWitness Platform deployment.
	not checked	Rule could not be checked. There are several reasons why a rule cannot be checked. For example, the rule check requires a check engine not supported by the OpenSCAP report.
	not applicable	Rule check does not apply to your NetWitness Platform deployment.
	informational	Rule checks for informational purposes only (no action required for **fail**).
	unknown	Report was able to check the rule. Run steps manually as described in the report to check the rule.
	total	Total number of rules checked.

Section	Field	Description
Exceptions	Title	Name of rule being checked.
	Result	Valid values are **pass**, **fixed**, **fail**, **error**, **not selected**, **not checked**, **not applicable**, **informational**, or unknown. **Note:** Results values are defined the **Results overview - Rule Results Summary**.

Create the OpenSCAP Report

The following tasks show you how to create the OpenSCAP Report in HTML, XML, or both HTML and XML.

Create Report in HTML Only

To create an OpenSCAP report in HTML only:

1. SSH to the host.
2. Submit the following command:

   ```
   mkdir -p /opt/rsa/openscap
   ```

3. Submit the following command for report upgrades only:

   ```
   sed -i -r -e "s/<platform.*//g" /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
   ```

4. Submit the following command:

   ```
   oscap xccdf eval --profile "stig" --report /opt/rsa/openscap/`hostname`.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
   ```

5. Report will be available under following location:

   ```
   /opt/rsa/openscap/
   ```

Create Report in XML Only

To create an OpenSCAP report in xml only:

1. SSH to the host.
2. Submit the following command:

   ```
   mkdir -p /opt/rsa/openscap
   ```

3. Submit the following command for report upgrades only:

   ```
   sed -i -r -e "s/<platform.*//g" /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
   ```

4. Submit the following command:

```
oscap xccdf eval --profile "stig" --results
/opt/rsa/openscap/`hostname`.xml --cpe /usr/share/xml/scap/ssg/content/ssg-
rhel7-cpe-dictionary.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-
xccdf.xml
```

5. Report will be available under following location:
   `/opt/rsa/openscap/`

Create Report in Both XML and HTML

To create an OpenSCAP report in both xml and html:

1. SSH to the host.
2. Submit the following command:
   ```
   mkdir -p /opt/rsa/openscap
   ```
3. Submit the following command for report upgrades only:
   ```
   sed -i -r -e "s/<platform.*//g" /usr/share/xml/scap/ssg/content/ssg-rhel7-
   xccdf.xml
   ```
4. Submit the following command:
   ```
   oscap xccdf eval --profile "stig" --results
   /opt/rsa/openscap/`hostname`.xml --report /opt/rsa/openscap/`hostname`.html
   --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml
   /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
   ```
5. Report will be available under following location:
   `/opt/rsa/openscap/`

Manage STIG Controls Script (`manage-stig-controls`)

You can use the `manage-stig-controls` script and its arguments to enable or disable STIG Control groups for which you want to apply STIG configuration. You can specify all hosts or individual hosts as arguments and you can enable or disable all control groups or individual control groups. This script is available in /usr/bin/ directory.

To manage STIG controls for a host:

1. SSH to the NW Server host or use the Console from the NetWitness Platform User Interface.
2. Submit the `manage-stig-controls` script with the commands, control groups, and other arguments you want to apply.
3. Reboot the host.

Commands

Command	Description
`--enable-all-controls`	Enables all STIG controls. For example: `manage-stig-controls --enable-all-controls`

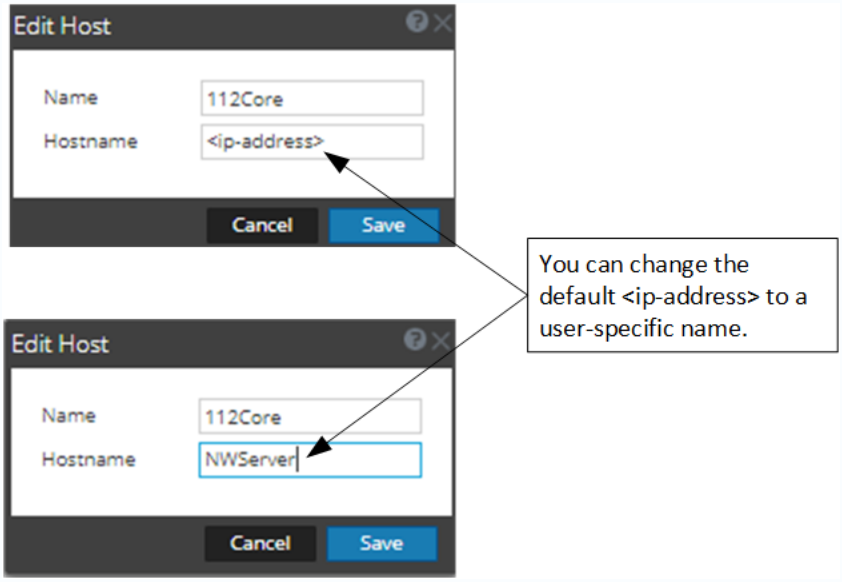
Command	Description
`--disable-all-controls`	Disables all STIG controls. For example: `manage-stig-controls --disable-all-controls`
`--enable-default-controls`	Enables all STIG Controls except ssh-prevent-root and fips-kernel. For example: `manage-stig-controls --enable-default-controls`
`--enable-control-groups <IDs>`	Enables (comma delimited) list of STIG Control GroupIDs. For example: `manage-stig-controls --enable-control-groups '1, 2, 3'`
`--disable-control-groups <IDs>`	Disables (comma delimited) list of STIG Control Group IDs For example: `manage-stig-controls --disable-control-groups '1, 2, 3'`

Control Groups

You use the ID as an argument for the control group or groups.

ID	Group	Description	Specified by Default
1	`ssh-prevent-root`	Prevent root login through SSH.	no
2	`ssh`	SSH STIG configuration.	yes
3	`fips-kernel`	FIPS Kernel configuration	no
4	`auth`	Authentication STIG configuration	yes
5	`audit`	Audit STIG configuration	yes
6	`packages`	RPM Package STIG configuration	yes
7	`services`	Services STIG configuration	yes

Other Arguments

Argument	Description
`--host-all`	Apply STIG configuration to all hosts. For example: `manage-stig-controls --host-all`
`--skip-health-checks`	Disable health checks for all hosts (not recommended). For example: `manage-stig-controls --skip-health-checks`
`--host-id <id>`	Apply STIG configuration for the host identified by `<id>` (host identification code). For example: `manage-stig-controls --host-id <id>`
`--host-name <display-name>`	Apply STIG configuration for host identified by `<display-name>`. `display-name` is the value shown under **Name** in the **(Admin)** > **Hosts** View in the NetWitness Platform Interface. For example: `manage-stig-controls --host-name <display-name>`
`--host-addr <Hostname-in UI>` or `--host-addr <hostname>`	Apply STIG configuration for the host identified by the value shown under **Hostname** in the **(Admin)** > **Hosts** > **Edit** dialog in the NetWitness Platform Interface. This value can be an ip-addres (default) or a user-specified name. For example: `manage-stig-controls --host-addr <hostname>` 
`-v, --verbose`	Enable verbose output. For example: `manage-stig-controls -v`

Rules List

The following table lists all the STIG rules with their:

- Control Group - you can use the Control Group ID as an argument in the manage-stig-controls script to expand on reduce the scope of rules checked. (1= ssh-prevent-root, 2 = ssh, 3 = fips-kernel, 4 = auth, 5 = audit, 6 = packages, 7 = services)
- Default Status - tells you if the rule is enabled or disabled by default.
- Passed or Exception status - tells you if the rule passed (that is, complies with STIG) or is an exception.

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-26404-4	Ensure /var Located On Separate Partition	n/a	n/a	Exception
CCE-26631-2	Set Password Strength Minimum Different Characters	auth	enabled	Passed
CCE-26828-4	Disable DCCP Support	n/a	n/a	Passed
CCE-26884-7	Set Lockout Time For Failed Password Attempts	auth	enabled	Exception
CCE-26892-0	Set the GNOME3 Login Warning Banner Text	n/a	enabled	Passed
CCE-26923-3	Limit Password Reuse	n/a	enabled	Passed
CCE-26952-2	Configure Periodic Execution of AIDE	audit	enabled	Exception
CCE-26970-4	Enable GNOME3 Login Warning Banner	audit	enabled	Passed
CCE-26971-2	Ensure /var/log/audit Located On Separate Partition	audit	enabled	Exception
CCE-26989-4	Ensure gpgcheck Enabled In Main Yum Configuration	n/a	enabled	Passed
CCE-27002-5	Set Password Minimum Age	n/a	enabled	Passed
CCE-27051-2	Set Password Maximum Age	auth	enabled	Passed
CCE-27053-8	Set Password Hashing Algorithm in /etc/libuser.conf	n/a	enabled	Passed
CCE-27082-7	Set SSH Client Alive Count	ssh	disabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-27096-7	Install AIDE	n/a	n/a	Exception
CCE-27127-0	Enable Randomized Layout of Virtual Address Space	n/a	enabled	Exception
CCE-27157-7	Verify File Hashes with RPM	n/a	n/a	Exception
CCE-27160-1	Set Password Retry Prompts Permitted Per-Session	n/a	enabled	Passed
CCE-27200-5	Set Password Strength Minimum Uppercase Characters	auth	enabled	Passed
CCE-27209-6	Verify and Correct File Permissions with RPM	n/a	n/a	Exception
CCE-27213-8	Record Events that Modify the System's Discretionary Access Controls - setxattr	audit	enabled	Passed
CCE-27214-6	Set Password Strength Minimum Digit Characters	auth	enabled	Passed
CCE-27218-7	Remove the X Windows Package Group	n/a	enabled	Passed
CCE-27275-7	Set Last Logon/Access Notification	n/a	enabled	Passed
CCE-27277-3	Disable Modprobe Loading of USB Storage Driver	services	enabled	Exception
CCE-27279-9	Configure SELinux Policy	n/a	enabled	Passed
CCE-27280-7	Record Events that Modify the System's Discretionary Access Controls - lsetxattr	audit	enabled	Passed
CCE-27286-4	Prevent Log In to Accounts With Empty Password	n/a	enabled	Passed
CCE-27287-2	Require Authentication for Single User Mode	n/a	enabled	Passed
CCE-27293-0	Set Password Minimum Length	auth	enabled	Passed
CCE-27295-5	Use Only FIPS 140-2 Validated Ciphers	n/a	enabled	Exception

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-27297-1	Set Interval For Counting Failed Password Attempts	auth	enabled	Passed
CCE-27303-7	Modify the System Login Banner	ssh	enabled	Exception
CCE-27309-4	Set Boot Loader Password in grub2	n/a	enabled	Exception
CCE-27311-0	Verify Permissions on SSH Server Public *.pub Key Files	n/a	enabled	Passed
CCE-27314-4	Enable SSH Warning Banner	ssh	enabled	Passed
CCE-27320-1	Allow Only SSH Protocol 2	n/a	enabled	Passed
CCE-27326-8	Ensure No Device Files are Unlabeled by SELinux	n/a	enabled	Passed
CCE-27334-2	Ensure SELinux State is Enforcing	n/a	enabled	Exception
CCE-27339-1	Record Events that Modify the System's Discretionary Access Controls - chmod	audit	enabled	Passed
CCE-27342-5	Uninstall rsh-server Package	n/a	enabled	Passed
CCE-27343-3	Ensure Logs Sent To Remote Host	n/a	n/a	Passed
CCE-27345-8	Set Password Strength Minimum Lowercase Characters	auth	enabled	Passed
CCE-27349-0	Set Default firewalld Zone for Incoming Packets	n/a	n/a	Exception
CCE-27350-8	Set Deny For Failed Password Attempts	auth	enabled	Passed
CCE-27351-6	Install the screen Package	n/a	enabled	Passed
CCE-27353-2	Record Events that Modify the System's Discretionary Access Controls - fremovexattr	audit	enabled	Passed
CCE-27355-7	Set Account Expiration Following Inactivity	n/a	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-27356-5	Record Events that Modify the System's Discretionary Access Controls - fchown	audit	enabled	Passed
CCE-27358-1	Deactivate Wireless Network Interfaces	n/a	enabled	Passed
CCE-27360-7	Set Password Strength Minimum Special Characters	auth	enabled	Passed
CCE-27363-1	Do Not Allow SSH Environment Options	ssh	enabled	Passed
CCE-27364-9	Record Events that Modify the System's Discretionary Access Controls - chown	audit	enabled	Passed
CCE-27367-2	Record Events that Modify the System's Discretionary Access Controls - removexattr	audit	enabled	Passed
CCE-27375-5	Configure auditd space_left Action on Low Disk Space	audit	enabled	Passed
CCE-27377-1	Disable SSH Support for .rhosts Files	n/a	enabled	Passed
CCE-27386-2	Ensure Default SNMP Password Is Not Used	n/a	n/a	Exception
CCE-27387-0	Record Events that Modify the System's Discretionary Access Controls - fchownat	audit	enabled	Passed
CCE-27388-8	Record Events that Modify the System's Discretionary Access Controls - fchmodat	audit	enabled	Passed
CCE-27389-6	Record Events that Modify the System's Discretionary Access Controls - fsetxattr	audit	enabled	Passed
CCE-27393-8	Record Events that Modify the System's Discretionary Access Controls - fchmod	audit	enabled	Passed
CCE-27394-6	Configure auditd mail_acct Action on Low Disk Space	audit	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-27401-9	Uninstall telnet-server Package	n/a	enabled	Passed
CCE-27399-5	Uninstall ypserv Package	n/a	enabled	Passed
CCE-27407-6	Enable auditd Service	audit	enabled	Passed
CCE-27410-0	Record Events that Modify the System's Discretionary Access Controls - lremovexattr	audit	enabled	Passed
CCE-27413-4	Disable Host-Based Authentication	n/a	enabled	Passed
CCE-27433-2	Set SSH Idle Timeout Interval	ssh	enabled	Passed
CCE-27434-0	Configure Kernel Parameter for Accepting IPv4 Source-Routed Packets for All Interfaces	n/a	enabled	Passed
CCE-27437-3	Ensure auditd Collects Information on the Use of Privileged Commands	audit	enabled	Passed
CCE-27445-6	Disable SSH Root Login	n/a	n/a	Exception
CCE-27447-2	Ensure auditd Collects Information on Exporting to Media (successful)	audit	enabled	Passed
CCE-27455-5	Use Only FIPS 140-2 Validated MACs	n/a	enabled	Passed
CCE-27458-9	Mount Remote Filesystems with Kerberos Security	n/a	enabled	Passed
CCE-27461-3	Ensure auditd Collects System Administrator Actions	audit	enabled	Passed
CCE-27471-2	Disable SSH Access via Empty Passwords	n/a	enabled	Exception
CCE-27485-2	Verify Permissions on SSH Server Private *_key Key Files	n/a	n/a	Passed
CCE-27498-5	Disable the Automounter	n/a	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-27503-2	All GIDs referenced in /etc/passwd must be defined in /etc/group	n/a	enabled	Passed
CCE-27511-5	Disable Ctrl-Alt-Del Reboot Activation	services	enabled	Passed
CCE-27512-3	Set Password Maximum Consecutive Repeating Characters	n/a	enabled	Passed
CCE-27557-8	Set Interactive Session Timeout	auth	disabled	Passed
CCE-80104-3	Disable GDM Automatic Login	n/a	enabled	Passed
CCE-80105-0	Disable GDM Guest Login	n/a	enabled	Passed
CCE-80108-4	Enable the GNOME3 Login Smartcard Authentication	n/a	enabled	Passed
CCE-80110-0	Set GNOME3 Screensaver Inactivity Timeout	n/a	enabled	Passed
CCE-80111-8	Enable GNOME3 Screensaver Idle Activation	n/a	enabled	Passed
CCE-80112-6	Enable GNOME3 Screensaver Lock After Idle Period	n/a	enabled	Passed
CCE-80127-4	Install McAfee Virus Scanning Software	n/a	n/a	Exception
CCE-80129-0	Virus Scanning Software Definitions Are Updated	n/a	n/a	Exception
CCE-80134-0	Ensure All Files Are Owned by a User	n/a	enabled	Passed
CCE-80135-7	Ensure All Files Are Owned by a Group	n/a	enabled	Passed
CCE-80136-5	Ensure All World-Writable Directories Are Owned by a System Account	n/a	enabled	Passed
CCE-80144-9	Ensure /home Located On Separate Partition	n/a	enabled	Passed
CCE-80148-0	Add nosuid Option to Removable Media Partitions	n/a	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80156-3	Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces	n/a	n/a	Exception
CCE-80157-1	Disable Kernel Parameter for IP Forwarding	n/a	n/a	Exception
CCE-80158-9	Configure Kernel Parameter for Accepting ICMP Redirects for All Interfaces	n/a	n/a	Exception
CCE-80162-1	Configure Kernel Parameter for Accepting Source-Routed Packets By Default	n/a	enabled	Passed
CCE-80163-9	Configure Kernel Parameter for Accepting ICMP Redirects By Default	n/a	n/a	Exception
CCE-80165-4	Configure Kernel Parameter to Ignore ICMP Broadcast Echo Requests	n/a	n/a	Exception
CCE-80174-6	Ensure System is Not Acting as a Network Sniffer	n/a	enabled	Passed
CCE-80179-5	Configure Kernel Parameter for Accepting IPv6 Source-Routed Packets for All Interfaces	n/a	n/a	Exception
CCE-80192-8	Ensure rsyslog Does Not Accept Remote Messages Unless Acting As Log Server	n/a	enabled	Passed
CCE-80205-8	Ensure the Default Umask is Set Correctly in login.defs	n/a	enabled	Passed
CCE-80207-4	Enable Smart Card Login	n/a	n/a	Exception
CCE-80213-2	Uninstall tftp-server Package	n/a	enabled	Passed
CCE-80214-0	Ensure tftp Daemon Uses Secure Mode	n/a	enabled	Passed
CCE-80215-7	Install the OpenSSH Server Package	n/a	enabled	Passed
CCE-80216-5	Enable the OpenSSH Service	n/a	enabled	Passed
CCE-80220-7	Disable GSSAPI Authentication	ssh	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80221-5	Disable Kerberos Authentication	n/a	enabled	Passed
CCE-80222-3	Enable Use of Strict Mode Checking	n/a	enabled	Passed
CCE-80223-1	Enable Use of Privilege Separation	n/a	enabled	Passed
CCE-80224-9	Disable Compression Or Set Compression to delayed	n/a	enabled	Passed
CCE-80225-6	Print Last Log	n/a	enabled	Exception
CCE-80226-4	Enable Encrypted X11 Forwarding	n/a	n/a	Exception
CCE-80240-5	Mount Remote Filesystems with nosuid	n/a	enabled	Passed
CCE-80245-4	Uninstall vsftpd Package	n/a	enabled	Passed
CCE-80258-7	Disable KDump Kernel Crash Analyzer (kdump)	services	enabled	Passed
CCE-80346-0	Ensure YUM Removes Previous Package Versions	packages	enabled	Passed
CCE-80347-8	Ensure gpgcheck Enabled for Local Packages	packages	enabled	Passed
CCE-80348-6	Ensure gpgcheck Enabled for Repository Metadata	n/a	n/a	Exception
CCE-80350-2	Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	n/a	enabled	Passed
CCE-80351-0	Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD	n/a	enabled	Passed
CCE-80352-8	Ensure the Logon Failure Delay is Set Correctly in login.defs	auth	enabled	Passed
CCE-80353-6	Configure the root Account for Failed Password Attempts	auth	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80354-4	Set the UEFI Boot Loader Password	fips-kernel	disabled	Passed
CCE-80359-3	Enable FIPS Mode in GRUB2	fips-kernel	disabled	Exception
CCE-80370-0	Set GNOME3 Screensaver Lock Delay After Activation Period	n/a	enabled	Passed
CCE-80371-8	Ensure Users Cannot Change GNOME3 Screensaver Settings	n/a	enabled	Passed
CCE-80372-6	Disable SSH Support for User Known Hosts	ssh	enabled	Passed
CCE-80373-4	Disable SSH Support for Rhosts RSA Authentication	audit	enabled	Passed
CCE-80374-2	Configure Notification of Post-AIDE Scan Details	n/a	n/a	Exception
CCE-80375-9	Configure AIDE to Verify Access Control Lists (ACLs)	n/a	n/a	Exception
CCE-80376-7	Configure AIDE to Verify Extended Attributes	n/a	n/a	Exception
CCE-80377-5	Configure AIDE to Use FIPS 140-2 for Validating Hashes	n/a	n/a	Exception
CCE-80378-3	Verify User Who Owns /etc/cron.allow file	n/a	enabled	Passed
CCE-80379-1	Verify Group Who Owns /etc/cron.allow file	n/a	enabled	Passed
CCE-80380-9	Ensure cron Is Logging To Rsyslog	n/a	enabled	Passed
CCE-80381-7	Shutdown System When Auditing Failures Occur	audit	enabled	Passed
CCE-80382-5	Record Attempts to Alter Logon and Logout Events - tallylog	audit	enabled	Passed
CCE-80383-3	Record Attempts to Alter Logon and Logout Events - faillock	n/a	n/a	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80384-1	Record Attempts to Alter Logon and Logout Events - lastlog	audit	enabled	Passed
CCE-80385-8	Record Unauthorized Access Attempts to Files (unsuccessful) - creat	audit	enabled	Passed
CCE-80386-6	Record Unauthorized Access Attempts to Files (unsuccessful) - open	audit	enabled	Passed
CCE-80387-4	Record Unauthorized Access Attempts to Files (unsuccessful) - openat	audit	enabled	Passed
CCE-80388-2	Record Unauthorized Access Attempts to Files (unsuccessful) - open_by_ handle_at	audit	enabled	Passed
CCE-80389-0	Record Unauthorized Access Attempts to Files (unsuccessful) - truncate	audit	enabled	Passed
CCE-80390-8	Record Unauthorized Access Attempts to Files (unsuccessful) - ftruncate	audit	enabled	Passed
CCE-80391-6	Record Any Attempts to Run semanage	audit	enabled	Passed
CCE-80392-4	Record Any Attempts to Run setsebool	audit	enabled	Passed
CCE-80393-2	Record Any Attempts to Run chcon	audit	enabled	Passed
CCE-80395-7	Ensure auditd Collects Information on the Use of Privileged Commands - passwd	audit	enabled	Passed
CCE-80396-5	Ensure auditd Collects Information on the Use of Privileged Commands - unix_chkpwd	audit	enabled	Passed
CCE-80397-3	Ensure auditd Collects Information on the Use of Privileged Commands - gpasswd	audit	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80398-1	Ensure auditd Collects Information on the Use of Privileged Commands - chage	audit	enabled	Passed
CCE-80399-9	Ensure auditd Collects Information on the Use of Privileged Commands - userhelper	audit	enabled	Passed
CCE-80400-5	Ensure auditd Collects Information on the Use of Privileged Commands - su	audit	enabled	Passed
CCE-80401-3	Ensure auditd Collects Information on the Use of Privileged Commands - sudo	audit	enabled	Passed
CCE-80402-1	Ensure auditd Collects Information on the Use of Privileged Commands - sudoedit	audit	enabled	Passed
CCE-80403-9	Ensure auditd Collects Information on the Use of Privileged Commands - newgrp	audit	enabled	Passed
CCE-80404-7	Ensure auditd Collects Information on the Use of Privileged Commands - chsh	audit	enabled	Passed
CCE-80405-4	Ensure auditd Collects Information on the Use of Privileged Commands - umount	audit	enabled	Passed
CCE-80406-2	Ensure auditd Collects Information on the Use of Privileged Commands - postdrop	audit	enabled	Passed
CCE-80407-0	Ensure auditd Collects Information on the Use of Privileged Commands - postqueue	audit	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80408-8	Ensure auditd Collects Information on the Use of Privileged Commands - ssh-keysign	audit	enabled	Passed
CCE-80410-4	Ensure auditd Collects Information on the Use of Privileged Commands - crontab	audit	enabled	Passed
CCE-80411-2	Ensure auditd Collects Information on the Use of Privileged Commands - pam_timestamp_check	audit	enabled	Passed
CCE-80412-0	Ensure auditd Collects File Deletion Events by User - rmdir	audit	enabled	Passed
CCE-80413-8	Ensure auditd Collects File Deletion Events by User - renameat	audit	enabled	Passed
CCE-80414-6	Ensure auditd Collects Information on Kernel Module Loading - init_ module	audit	enabled	Passed
CCE-80415-3	Ensure auditd Collects Information on Kernel Module Unloading - delete_ module	audit	enabled	Passed
CCE-80430-2	Record Events that Modify User/Group Information - /etc/security/opasswd	audit	enabled	Passed
CCE-80431-0	Record Events that Modify User/Group Information - /etc/shadow	audit	enabled	Passed
CCE-80432-8	Record Events that Modify User/Group Information - /etc/gshadow	audit	enabled	Passed
CCE-80433-6	Record Events that Modify User/Group Information - /etc/group	audit	enabled	Passed
CCE-80434-4	Ensure Home Directories are Created for New Users	n/a	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80435-1	Record Events that Modify User/Group Information - /etc/passwd	audit	enabled	Passed
CCE-80436-9	Mount Remote Filesystems with noexec	n/a	enabled	Passed
CCE-80437-7	Configure PAM in SSSD Services	n/a	n/a	Exception
CCE-80438-5	Configure Multiple DNS Servers in /etc/resolv.conf	n/a	n/a	Exception
CCE-80439-3	Configure Time Service Maxpoll Interval	services	enabled	Passed
CCE-80447-6	Configure the Firewalld Ports	n/a	n/a	Exception
CCE-80513-5	Remove Host-Based Authentication Files	n/a	enabled	Passed
CCE-80514-3	Remove User Host-Based Authentication Files	n/a	enabled	Passed
CCE-80515-0	Configure SSSD LDAP Backend Client CA Certificate Location	n/a	n/a	Exception
CCE-80519-2	Install Smart Card Packages For Multifactor Authentication	n/a	n/a	Exception
CCE-80537-4	Configure auditd space_left on Low Disk Space	audit	enabled	Passed
CCE-80544-0	Ensure Users Cannot Change GNOME3 Session Idle Settings	n/a	enabled	Passed
CCE-80545-7	Verify and Correct Ownership with RPM	n/a	n/a	Exception
CCE-80546-5	Configure SSSD LDAP Backend to Use TLS For All Transactions	n/a	n/a	Exception
CCE-80547-3	Ensure auditd Collects Information on Kernel Module Loading and Unloading - finit_module	audit	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-80563-0	Ensure Users Cannot Change GNOME3 Screensaver Lock After Idle Period	n/a	enabled	Passed
CCE-80564-8	Ensure Users Cannot Change GNOME3 Screensaver Idle Activation	n/a	enabled	Passed
CCE-80660-4	Record Any Attempts to Run setfiles	audit	enabled	Exception
CCE-80661-2	Ensure auditd Collects Information on Kernel Module Loading - create_ module	audit	enabled	Exception
CCE-80995-4	Ensure auditd Collects File Deletion Events by User - rename	audit	enabled	Exception
CCE-80996-2	Ensure auditd Collects File Deletion Events by User - unlinkat	audit	enabled	Exception
CCE-80998-8	Verify firewalld Enabled	n/a	n/a	Exception
CCE-81106-7	Ensure auditd Collects File Deletion Events by User - unlink	audit	enabled	Passed
CCE-81153-9	Add nosuid Option to /home	n/a	enabled	Passed
CCE-82020-9	Set Password Strength Minimum Different Characters	auth	enabled	Passed
CCE-82030-8	Limit Password Reuse	n/a	enabled	Passed
CCE-82035-7	Ensure /var/log/audit Located On Separate Partition	audit	enabled	Exception
CCE-82036-5	Set Password Minimum Age	n/a	enabled	Passed
CCE-82038-1	Set Password Hashing Algorithm in /etc/libuser.conf	n/a	enabled	Passed
CCE-82041-5	Limit the Number of Concurrent Login Sessions Allowed Per User	auth	enabled	Passed
CCE-82043-1	Set PAM's Password Hashing Algorithm	n/a	enabled	Passed

CCE Number	Rule Name	Control Group	Default Status	Passed/ Exception
CCE-82045-6	Set Password Strength Minimum Different Categories	audit	enabled	Passed
CCE-82050-6	Set Password Hashing Algorithm in /etc/login.defs	n/a	enabled	Passed
CCE-82053-0	Ensure /tmp Located On Separate Partition	n/a	n/a	Exception
CCE-82054-8	Verify Only Root Has UID 0	n/a	enabled	Passed
CCE-82353-4	Ensure /var Located On Separate Partition	n/a	n/a	Exception

Exceptions to STIG Compliance

This topic contains:

- Rule exceptions that are the responsibility of the customer to resolve.
- Rule exceptions that are "Not a Finding" which means that they do not apply to NetWitness Platform. NetWitness has verified that the system meets these requirements.
- Rules to be supported in future release.

Key to Elements in Exception Descriptions

CCE Number

The Common Configuration Enumeration (CCE), assigns unique entries (also called CCE numbers) to configuration guidance statements and configuration controls to improve workflow by facilitating fast and accurate correlation of configuration issues present in disparate domains. In this way, it is similar to other comparable data standards such as the **Common Vulnerability and Exposure (CVE®) List** (http://cve.mitre.org/cve), which assigns identifiers to publicly known system vulnerabilities. The OpenSCAP report lists exceptions by CCE number.

This sections lists the exceptions you can receive when you run the OpenSCAP report. The ID or Common Configuration Enumeration (CCE) number in the table is the identification number for the exception from the OpenSCAP report.

Control Group ID

Number that identifies the control group you specify in the manage-stig-controls script to enable or disable the rule.

ID	Group	Description	Specified by Default
1	`ssh-prevent-root`	Prevent root login through SSH.	no
2	`ssh`	SSH STIG configuration.	yes
3	`fips-kernel`	FIPS Kernel configuration	no
4	`auth`	Authentication STIG configuration	yes
5	`audit`	Audit STIG configuration	yes
6	`packages`	RPM Package STIG configuration	yes
7	`services`	Services STIG configuration	yes

Check

Describes what the rule checks to identify exceptions to DISA STIG compliance.

Comments

Provides insight on why you would receive this exception. This section includes one of the following comments that describes the exception:

- **Customer Responsibility** - You are responsible to make sure the system meets this requirement.
- **Not a Finding** - Exception does not apply to NetWitness Platform. NetWitness has verified that the system meets this requirement.
- **Future Feature** - NetWitness Platform does not meet this requirement. NetWitness plans to fix this in a future release of NetWitness Platform.

Customer Responsibility Exceptions

CCE-26952-2 Configure Periodic Execution of AIDE (Control Group = audit)

Check	At a minimum, configure AIDE to run a weekly scan and at most, daily. To implement a daily execution of AIDE at 4:05am using cron, add the following line to the `/etc/crontab` file:
	`05 4 * * * root /usr/sbin/aide --check`
	To implement a weekly execution of AIDE at 4:05am using cron, add the following line to the `/etc/crontab` file:
	`05 4 * * 0 root /usr/sbin/aide --check`
	AIDE can be executed periodically through other means; this is merely one example. The usage of cron's special time codes, such as `@daily` and `@weekly` is acceptable.

Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently as possible to adhere to your security policy.

CCE-27096-7 Install AIDE (Control Group = n/a)

Check	Install the AIDE package with the following command: `$ sudo yum install aid`
Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently possible to adhere to your security policy.

CCE-27218-7 Remove the X Windows Package Group

Check	The Rule CCE-27218-7 "Remove the X Windows Package Group" is an exception for Log Collector and Log Decoder services.
Comments	**Customer Responsibility.**Log Collector plugin collection framework uses SELinux sandbox technology that has a direct dependency on the given rpm. Removing of the rpm will lead to loss of plugin collection functionality in Log Collector service.

CCE-27295-5 Use Only FIPS 140-2 Validated Ciphers (Control Group = n/a)

Check	Limit the ciphers to those algorithms which are FIPS-approved. Counter (CTR) mode is also preferred over cipher-block chaining (CBC) mode. The following line in `/etc/ssh/sshd_config` demonstrates use of FIPS 140-2 validated ciphers:
	`Ciphers aes128-ctr,aes192-ctr,aes256-ctr`
	The following ciphers are FIPS 140-2 certified on RHEL 7:
	`- aes128-ctr - aes192-ctr - aes256-ctr - aes128-cbc - aes192-cbc - aes256-cbc - 3des-cbc - rijndael-cbc@lysator.liu.se`
	Any combination of the above ciphers will pass this check. Official FIPS 140-2 paperwork for RHEL7 can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2630.pdf.

Comments	Testing approach results in failed test, but the ciphers defined meet the STIG Rule definition. You can check cipher under this file: `/etc/ssh/sshd_config`

CCE-27334-2 Ensure SELinux State is Enforcing

Check	Ensure SELinux State is Enforcing.
Comments	SELinux state is default it is set to 'permissive' by default for all the NetWitness Platform hosts instead of 'Enforcing' due to performance impact.

CCE-27445-6 Disable SSH Root Login (Control Group = ssh-prevent-root)

Check	The root user should never be allowed to login to a system directly over a network.
Comments	**Customer Responsibility.** Disable root login through SSH by adding or editing the following line in the `/etc/ssh/sshd_config` file: `PermitRootLoginNetWitness`.

CCE-80127-4 Install McAfee Virus Scanning Software (Control Group = n/a)

Check	Install McAfee VirusScan Enterprise for Linux antivirus software which is provided for DoD systems and uses signatures to search for the presence of viruses on the filesystem.
Comments	**Customer Responsibility.** Install virus scanning software. NetWitness does not provide this software.

CCE-80129-0 Virus Scanning Software Definitions Are Updated (Control Group = n/a)

Check	Make sure that virus definition files are no older than 7 days or their last release.
Comments	**Customer Responsibility.** NetWitness does not provide this software.

CCE-80207-4 Enable Smart Card Login (Control Group = n/a)

Check	For guidance on enabling SSH to authenticate against a Common Access Card (CAC), consult documentation at: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System-Level_Authentication_Guide/smartcards.html#authconfig-smartcards https://access.redhat.com/solutions/82273
Comments	**Customer Responsibility.** The NetWitness Platform supports username/certificate for authentication to shell. If you want to configure a smart card log in, you must do this outside of NetWitness NetWitness.

CCE-80359-3 Enable FIPS Mode in GRUB2 (Control Group = fips-kernel)

Check	To ensure FIPS mode is enabled, install the `dracut-fips` package and rebuild `initramfs` by running the following commands:
	`$ sudo yum install dracut-fips dracut -f`
	After the `dracut` command has been run, add the `fips=1` argument to the default GRUB 2 command line for the Linux operating system in the `/etc/default/grub` file as shown in the following example:
	`GRUB_CMDLINE_LINUX='crashkernel=auto rd.lvm.lv=VolGroup/LogVol06 rd.lvm.lv=VolGroup/lv_swap rhgb quiet rd.shell=0 fips=1'`
	Finally, rebuild the `grub.cfg` file by using the `grub2-mkconfig -o` command as follows (On BIOS-based machines, issue the following command as root):
	`~]# grub2-mkconfig -o /boot/grub2/grub.cfg`
	On UEFI-based machines, issue the following command as root:
	`~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg`

Comments	**Customer Responsibility.** NetWitness Platform does not enabled by default. You can enable FIPS by following the procedures in the Configure FIPS Support.

CCE-80374-2 Configure Notification of Post-AIDE Scan Details (Control Group = n/a)

Check	AIDE should notify appropriate personnel of the details of a scan after the scan has been run. If AIDE has already been configured for periodic execution in the `/etc/crontab` file, append the following line to the existing AIDE line:
	`| /bin/mail -s '$(hostname) - AIDE Integrity Check' root@localhost`
	Otherwise, add the following line to the `/etc/crontab` file:
	`05 4 * * * root /usr/sbin/aide --check | /bin/mail -s '$(hostname) - AIDE Integrity Check' root@localhost`
	AIDE can be executed periodically through other means. This is just one example.

Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently possible to adhere to your security policy.

CCE-80375-9 Configure AIDE to Verify Access Control Lists (Control Group = n/a)

Check	By default, the `acl` option is added to the FIPSR ruleset in AIDE. If using a custom ruleset or the `acl` option is missing, add `acl` to the appropriate ruleset. For example, add `acl` to the following line in the `/etc/aide.conf` file: `FIPSR = p+i+n+u+g+s+m+c+acl+selinux+xattrs+sha256` AIDE rules can be configured in multiple ways; this is merely one example that is already configured by default.
Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently possible to adhere to your security policy.

CCE-80376-7 Configure AIDE to Verify Extended Attributes (Control Group = n/a)

Check	By default, the `xattrs` option is added to the FIPSR ruleset in AIDE. If using a custom ruleset or the `xattrs` option is missing, add `xattrs` to the appropriate ruleset. For example, add xattrs to the following line in the `/etc/aide.conf` file: `FIPSR = p+i+n+u+g+s+m+c+acl+selinux+xattrs+sha256` AIDE rules can be configured in multiple ways. This is just one example that is already configured by default.
Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently possible to adhere to your security policy.

CCE-80377-5 Configure AIDE to Use FIPS 140-2 for Validating Hashes (Control Group = n/a)

Check	By default, the `sha512` option is added to the `ORMAL` ruleset in AIDE. If using a custom `ruleset` or the `sha512` option is missing, add `sha512` to the appropriate ruleset. For example, add `sha512` to the following line in the `/etc/aide.conf` file:`ORMAL = FIPSR+sha512` AIDE rules can be configured in multiple ways; this is merely one example that is already configured by default.
Comments	**Customer Responsibility.** NetWitness Platform does not provide AIDE because it has a negative impact on performance. If you must install it, run as infrequently possible to adhere to your security policy.

CCE-80519-2 Install Smart Card Packages For Multi-Factor Authentication (Control Group = n/a)

Check	Configure the operating system to implement multifactor authentication by installing the required packages with the following command: `$ sudo yum install esc pam_pkcs11 authconfig-gtk`

Comments	**Customer Responsibility.** The NetWitness Platform supports username/certificate for authentication to shell. If you want to configure a smart card log in, you must do this outside of NetWitness NetWitness.

Exceptions That Are Not a Finding

The following exceptions do not apply to NetWitness Platform. NetWitness has verified that the system meets these requirements.

CCE-26404-4 Ensure /var Located On Separate Partition (Control Group = n/a)

Check	The `/var` directory is used by daemons and other system services to store frequently-changing data. Ensure that `/var` has its own partition or logical volume at installation time, or migrate it using LVM.
Comments	**Not a Finding.**NetWitness software is installed in `/var/netwitness` by default and has a separate partition on `/var/netwitness`.

CCE-26828-4 Set GNOME Login Inactivity timeout (Control Group = n/a)

Check	Verify that the GNOME Login Inactivity Timeout is set on the host (The graphical desktop environment must set the idle timeout to no more than 15 minutes.).
Comments	**Not a Finding.** NetWitness Platform does not use Gnome Graphical User Interface (GUI) Desktop.

CCE-26884-7 Set Lockout Time For Failed Password Attempts (Control Group = auth)

Check	To configure the system to lock out accounts after a number of incorrect login attempts and require an administrator to unlock the account using `pam_faillock.so`, modify the content of both `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` by adding the following line immediately before the `pam_unix.so` statement in the `AUTH` section:
	`auth required pam_faillock.so preauth silent deny= unlock_time= fail_interval=`
	Add the following line immediately after the `pam_unix.so` statement in the `AUTH` section:
	`auth [default=die] pam_faillock.so authfail deny= unlock_time= fail_interval=`
	Add the following line immediately before the `pam_unix.so` statement in the `ACCOUNT` section:
	`account required pam_faillock.s`

Comments	**Not a Finding.** `root_unlock_time` is set to `600` seconds.

CCE-26971-2 Ensure `/var/log/audit` Located On Separate Partition (Control Group = audit)

Check	Audit logs are stored in the `/var/log/audit` directory. Ensure that it has its own partition or logical volume at installation time, or migrate it later using LVM. Make absolutely certain that it is large enough to store all audit logs that will be created by the auditing daemon.
Comments	**Not a Finding.**NetWitness Platform has the `/var/log` directory as a separate partition.

CCE-27127-0 Enable Randomized Layout of Virtual Address Space (Control Group = n/a)

Check	To set the runtime status of the `kernel.randomize_va_space` kernel parameter, run the following command:
	`$ sudo sysctl -w kernel.randomize_va_space=2`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`kernel.randomize_va_space = 2`

Comments	**Not a Finding.** Value of `/proc/sys/kernel/randomize_va_space` is already `2`.

CCE-27157-7 Verify File Hashes with RPM (Control Group = n/a)

Check	Without cryptographic integrity protections, system executables and files can be altered by unauthorized users without detection. The RPM package management system can check the hashes of installed software packages, including many that are important to system security. To verify that the cryptographic hash of system files and commands match vendor values, run the following command to list which files on the system with hashes that differ from what is expected by the RPM database:
	`$ rpm -Va | grep '^..5' A 'c'`
	in the second column indicates that a file is a configuration file, which may appropriately be expected to change. If the file was not expected to change, investigate the cause of the change using audit logs or other means. The package can then be reinstalled to restore the file. Run the following command to determine which package owns the file:
	`$ rpm -qf`
	The package can be reinstalled from a yum repository using the command:
	`FILENAME $ sudo yum reinstall`
	Alternatively, the package can be reinstalled from trusted media using the command:
	`PACKAGENAME $ sudo rpm -Uvh PACKAGENAME`

Comments	**Not a Finding.** Only mismatched files not marked as config files in rpms are Commercial Off the Shelf (COTS) product based that cannot be updated. Most File Hash/RPM combinations are in sync. Any discrepancies are COTS products that cannot be updated.

CCE-27339-1 Record Events that Modify the System's Discretionary Access Controls - chmod

Check	Verify that the host records events that modify the system's discretionary access controls - `chown`.

Comments	**Not a Finding.** Make sure that you have the correct `chown` configuration on the host. The following settings are the correct configuration.
	`[root@localhost nwadmin]# grep chown /etc/audit/*`
	`/etc/audit/audit.rules:-a exit,always -F arch=b64 -S chown -S chmod -S fchmod -S fchmodat -S fchown -S fchownat -S fremovexattr -S fsetxattr -S lchown -S lremovexattr -S lremovexattr -S lsetxattr -S removexattr -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod`
	`/etc/audit/audit.rules:-a exit,always -F arch=b32 -S chown -S fchmod -S fchmodat -S fchown -S fchownat -S fremovexattr -S fsetxattr -S lchown -S lremovexattr -S lremovexattr -S lsetxattr -S removexattr -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod`

CCE-27209-6 Verify and Correct File Permissions with RPM (Control Group = n/a)

Rule Name	

Check	The RPM package management system can check file access permissions of installed software packages, including many that are important to system security. Verify that the file permissions of system files and commands match vendor values. Check the file permissions with the following command:
	`$ sudo rpm -Va | grep '^.M'`
	Output indicates files that do not match vendor defaults. After locating a file with incorrect permissions, run the following command to determine which package owns it:
	`$ rpm -qf FILENAME`
	Next, run the following command to reset its permissions to the correct values:
	`$ sudo rpm --quiet --setperms PACKAGENAME`

Comments	**Not a Finding.** The file permissions do not match the rpm, they are configured to be stricter during configuration management.

CCE-27303-7 (Control ID = 2) Modify the System Login Banner (Control Group = ssh)

Check	To configure the system login banner edit the `/etc/issue` file. Replace the default text with a message compliant with the local site policy or a legal disclaimer. The DoD required text is either: " You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: • The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. • At any time, the USG may inspect and seize data stored on this IS. • Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. • This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details." or " I've read & consent to terms in IS user agreem't."
Comments	**Not a Finding.** The login banner is displayed but does not hyphenate "agreem't"

CCE-27311-0 Very Permissions on SHH Server *.pub Key Files (Control Group = na)

Check	
Comments	**Not a Finding.** All public keys are set to with permissions 640 in the `/etc/ssh/` directory.

CCE-27314-4 Enable SSH Warning Banner (Control Group = na)

Check	
Comments	**Not a Finding.** The required configuration exists in the `etc/ssh/sshd_conf` file.

CCE-27349-0 Set Default `firewalld` Zone for Incoming Packets (Control Group = n/a)

Check	To set the default zone to drop for the built-in default zone which processes incoming IPv4 and IPv6 packets, modify the following line in the `/etc/firewalld/firewalld.conf` file to be: `DefaultZone=drop`
Comments	**Not a Finding.** NetWitness Platform `firewalld`service is disabled because it uses IP Tables, not FirewallD.

CCE-27386-2 Ensure Default SNMP Password Is Not Used (Control Group = n/a)

Check	Edit `/etc/snmp/snmpd.conf` file by removing or changing the default community strings of public and private. After the default community strings have been changed, restart the SNMP service: `$ sudo service snmpd restart`
Comments	**Not a Finding.** NetWitness Platform does not use `snmp`, and the `snmpd` service not enabled.

CCE-27455-5 Use Only FIPS 140-2 Validated MACs (Control Group = na)

Check	
Comments	**Not a Finding.** The following configuration exists in `/etc/ssh/sshd_config` file: `MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512`

CCE-27471-2 Disable SSH Access via Empty Passwords (Control Group = n/a)

Check	Explicitly disallow SSH login from accounts with empty passwords, add or correct the following line in the `/etc/ssh/sshd_config` file.
Comments	**Not a Finding.** NetWitness Platform sets the **permitemptypasswords** parameter to **no** by default. This should pass the DISA STIG rule check.

CCE-27485-2 Very Permissions on SHH Server Private *.key Key Files (Control Group = na)

Check	
Comments	**Not a Finding.** All private keys are set to with permissions 640 in the `/etc/ssh/` directory.

CCE-80156-3 Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces (Control Group = n/a)

Check	To set the runtime status of the `t.ipv4.conf.all.send_redirects` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv4.conf.all.send_redirects=0`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv4.conf.all.send_redirects = 0`

Comments	**Not a Finding.** NetWitness Platform does not accept incoming Internet Control Message Protocol (ICMP) traffic.

CCE-80157-1 Disable Kernel Parameter for IP Forwarding (Control Group = n/a)

Check	To set the runtime status of the `t.ipv4.ip_forward` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv4.ip_forward=0`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv4.ip_forward = 0`

Comments	**Not a Finding.** NetWitness Platform only uses FIPS certified MACs (for example, `MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512`).

CCE-80158-9 Configure Kernel Parameter for Accepting ICMP Redirects for All Interfaces (Control Group = n/a)

Check	To set the runtime status of the `t.ipv4.conf.all.accept_redirects` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv4.conf.all.accept_redirects=0`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv4.conf.all.accept_redirects = 0`

Comments	**Not a Finding** NetWitness Platform does not accept incoming Internet Control Message Protocol (ICMP) traffic.

CCE-80163-9 Configure Kernel Parameter for Accepting ICMP Redirects By Default (Control Group = n/a)

Check	To set the runtime status of the `t.ipv4.conf.default.accept_redirects` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv4.conf.default.accept_redirects=0`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv4.conf.default.accept_redirects = 0`

Comments	**Not a Finding** NetWitness Platform does not accept incoming Internet Control Message Protocol (ICMP) traffic.

CCE-80165-4 Configure Kernel Parameter to Ignore ICMP Broadcast Echo Requests (Control Group = n/a)

Rule Name	

Check	To set the runtime status of the `t.ipv4.icmp_echo_ignore_broadcasts` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv4.icmp_echo_ignore_broadcasts = 1`

Comments	**Not a Finding**NetWitness Platform does not accept incoming Internet Control Message Protocol (ICMP) traffic.

CCE-80225-6 Print Last Log (Control Group = n/a)

Check	When enabled, SSH will display the date and time of the last successful account log in. To enable `LastLog` in SSH, add or correct the following line in the `/etc/ssh/sshd_config` file: `PrintLastLog yes`
Comments	**Not a Finding.** NetWitness Platform sets `printlastlog` to `yes` by default.

CCE-80226-4 Enable Encrypted X11 Forwarding (Control Group = n/a)

Check	Enable Encrypted X11 Forwarding - By default, remote X11 connections are not encrypted when initiated by users. SSH has the capability to encrypt remote X11 connections when SSH's `X11Forwarding` option is enabled. To enable X11 Forwarding, add or correct the following line in the `/etc/ssh/sshd_config` file: `X11Forwarding yes`
Comments	**Not a Finding.**NetWitness Platform does not have X11 installed or running.

CCE-80348-6 Ensure gpgcheck Enabled for Repository Metadata (Control Group = n/a)

Check	Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components of local packages without verification of the repository metadata. Check that yum verifies the repository metadata prior to install with the following command. This should be configured by `setting repo_ gpgcheck` to `1` in `/etc/yum.conf`.
Comments	**Not a Finding.** .NetWitness Platform rpm signing procedures do not support signing the repo metadata

CCE-80383-3 Record Attempts to ALter Logon Events - failock (Control Group = na)

Check	
Comments	**Not a Finding.** The required rules are configured in the `/etc/audit/rules.d/nw-stig.rules` file.

CCE-80399-9 Ensure auditd Collects Information on the Use of Privileged Commands - userhelper (Control Group = na)

Check	
Comments	**Not a Finding.** The required rules are configured in the `/etc/audit/rules.d/nw-stig.rules` file.

CCE-80437-7 Configure PAM in SSSD Services (Control Group = n/a)

Check	SSSD should be configured to run SSSD pam services. To configure SSSD to known SSH hosts, add pam to services under the `[sssd]` section in `/etc/sssd/sssd.conf` file. For example: `[sssd] services = sudo, autofs, pam`
Comments	**Not a Finding.** NetWitness Platform does not currently support Multi-Factor authentication. As a result, SSSD service is not installed on a NetWitness Host.

CCE-80438-5 Configure Multiple DNS Servers in `/etc/resolv.conf` (Control Group = n/a)

Check	Multiple Domain Name System (DNS) Servers should be configured in the `/etc/resolv.conf` file. This provides redundant name resolution services in the event that a domain server crashes. To configure the system to contain as least 2 DNS servers, add a corresponding `nameserver` entry in `ip_address /etc/resolv.conf` file for each DNS server where `ip_address` is the IP address of a valid DNS server. For example: `search example.com nameserver 192.168.0.1 nameserver 192.168.0.2`
Comments	**Not a Finding.** NetWitness Platform orchestrates and configures an internal DNS server that all NetWitness hosts use for name resolution. You can configure external DNS servers, but it is dependent on your environment.

CCE-80439-3 Configure Time Service Maxpoll Interval (Control Group = na)

Check	
Comments	**Not a Finding.** The required `maxpoll 10` value is set in the `/etc/ntp.conf` file.

CCE-80447-6 Configure the Firewalld Ports (Control Group = n/a)

Check	Configure the `firewalld` ports to allow approved services to have access to the system. To configure `firewalld` to open ports, run the following command:
	`$ sudo firewall-cmd --permanent --add-port= or port_number/tcp $ sudo firewall-cmd --permanent --add-port=`
	Run the command list above for each of the ports listed below: <ports>
	To configure `service_nam firewalld` to allow access, run the following command(s):
	`firewall-cmd --permanent --add-service=ssh`

Comments	**Not a Finding.** NetWitness Platform `firewalld` service is disabled because it uses IP Tables, not FirewallD.

CCE-80515-0 Configure SSSD LDAP Backend Client CA Certificate Location (Control Group = n/a)

Check	Configure SSSD to implement cryptography to protect the integrity of LDAP remote access sessions. By setting the `ldap_tls_cacertdir` option in `/etc/sssd/sssd.conf` to point to the path for the X.509 certificates used for peer authentication. `ldap_tls_cacertdir /path/to/tls/cacert`
Comments	**Not a Finding.** NetWitness Platform does not currently support Multi-Factor authentication. As a result, SSSD service is not installed on a NetWitness Host.

CCE-80545-7 Verify and Correct Ownership with RPM (Control Group = n/a)

Check	The RPM package management system can check file ownership permissions of installed software packages, including many that are important to system security. After locating a file with incorrect permissions, which can be found with `rpm -Va | grep '^.....\(U|.G\)'`
	Run the following command to determine which package owns it:
	`$ rpm -qf`
	Next, run the following command to reset its permissions to the correct values:
	`FILENAME $ sudo rpm --setugids PACKAGENAME`

Comments	**Not a Finding.**Files/Directories with ownership differing from the rpm are generally COTS based and have been changed from root ownership to a specified COTS related account.

CCE-80546-5 Configure SSSD LDAP Backend to Use TLS For All Transactions (Control Group = n/a)

Check	This check verifies that RHEL7 implements cryptography to protect the integrity of remote LDAP authentication sessions. To determine if LDAP is being used for authentication, use the following command:
	`$ sudo grep -i useldapauth /etc/sysconfig/authconfig If USELDAPAUTH=yes`
	To check if LDAP is configured to use TLS, use the following command:
	`$ sudo grep -i ldap_id_use_start_tls /etc/sssd/sssd.conf`

Comments	**Not a Finding.**NetWitness Platform does not currently support Multi-Factor authentication. As a result, the SSSD service is not installed on a NetWitness Host.

CCE-80998-8 Verify firewall Enabled

Check	Verify the operating system enabled an application firewall. Check to see if "firewalld" is installed with the following command:
	`yum list installed firewalld`
	`firewalld-0.3.9-11.el7.noarch.rpm`
	If the "firewalld" package is not installed, ask the System Administrator if another firewall application (such as iptables) is installed.
	If an application firewall is not installed, this is a finding.
	Check to see if the firewall is loaded and active with the following command:
	`systemctl status firewalld`
	`firewalld.service - firewalld - dynamic firewall daemon`
	Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
	Active: active (running) since Tue 2014-06-17 11:14:49 CEST; 5 days ago
	If "firewalld" does not show a status of "loaded" and "active", this is a finding.
	Check the state of the firewall:
	`firewall-cmd --state`
	`running`
	If "firewalld" does not show a state of "running", this is a finding.

Comments	**Not a Finding.** NetWitness Platform firewalldservice is disabled because it uses IP Tables, not FirewallD.

CCE-82035-7 Ensure /var/log/audit Located On Separate Partition

Check	Determine if the operating system is configured to have the "/var/log/audit" path is on a separate file system.
	`grep /var/log/audit /etc/fstab`
	If no result is returned, or the operating system is not configured to have "/var/log/audit" on a separate file system, this is a finding.
	Verify that "/var/log/audit" is mounted on a separate file system:
	`mount | grep "/var/log/audit"`
	If no result is returned, or "/var/log/audit" is not on a separate file system, this is a finding.

Comments	**Not a Finding**. NetWitness Platform has the /var/log directory as a separate partition.

CCE-82053-0 Ensure /tmp Located On Separate Partition

Check	Verify that a separate file system/partition has been created for "/tmp". Check that a file system/partition has been created for "/tmp" with the following command:
	`systemctl is-enabled tmp.mount`
	`enabled`
	If the "tmp.mount" service is not enabled, check to see if "/tmp" is defined in the fstab with a device and mount point:
	`grep -i /tmp /etc/fstab`
	UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /tmp ext4 rw,relatime,discard,data=ordered,nosuid,noexec, 0 0
	If "tmp.mount" service is not enabled or the "/tmp" directory is not defined in the fstab with a device and mount point, this is a finding.

Comments	**Future Feature** - NetWitness Platform does not meet this requirement. NetWitness plans to fix this in a future release of NetWitness Platform.

CCE-82353-4 Ensure /var Located On Separate Partition

Check	Verify that a separate file system/partition has been created for "/var". Check that a file system/partition has been created for "/var" with the following command: `grep /var /etc/fstab` UUID=c274f65f /var ext4 noatime,nobarrier 1 2 If a separate entry for "/var" is not in use, this is a finding.
Comments	**Not a Finding.** Hardware is dedicated for NetWitness, and NetWitness software is installed in /var/netwitness by default and a separate partition is on /var/netwitness.

Rules Supported in a Future Release

The following checks for non-compliance to STIG rules are not supported in NetWitness Platform and will be added in a future release.

CCE-27277-3 Disable Modprobe Loading of USB Storage Driver (Control Group = services)

Check	To prevent USB storage devices from being used, configure the kernel module loading system to prevent automatic loading of the USB storage driver. To configure the system to prevent the usb-storage kernel module from being loaded, add the following line to a file in the `/etc/modprobe.d` directory : `install usb-storage /bin/true` This will prevent the `modprobe` program from loading the usb-storage module, but will not prevent an administrator (or another program) from using the `insmod` program to load the module manually.
Comments	**Future Feature.**

CCE-27309-4 Set Boot Loader Password in `grub2` (Control Group = fips-kernel)

Check	The `grub2` boot loader should have a superuser account and password protection enabled to protect boot-time settings. To do so, select a superuser account name and password and and modify the `/etc/grub.d/01_users` configuration file with the new account name. Because plain text passwords are a security risk, generate a hash for the password by running the following command:
	`$ grub2-setpassword`
	When prompted, enter the password that was selected.
	NOTE: It is recommended not to use common administrator account names like root, admin, or administrator for the `grub2` superuser account. Change the superuser to a different username (The default is 'root').
	`$ sed -i s/root/bootuser/g /etc/grub.d/01_users`
	To meet FISMA Moderate, the bootloader superuser account and password MUST differ from the root account and password. Once the superuser account and password have been added, update the `grub.cfg` file by running:
	`grub2-mkconfig -o /boot/grub2/grub.cfg`
	NOTE: Do NOT manually add the superuser account and password to the `grub.cfg` file as the `grub2-mkconfig` command overwrites this file.

Comments	**Future Feature.**

CCE-80179-5 Configure Kernel Parameter for Accepting IPv6 Source-Routed Packets for All Interfaces

Check	To set the runtime status of the `t.ipv6.conf.all.accept_source_route` kernel parameter, run the following command:
	`$ sudo sysctl -w net.ipv6.conf.all.accept_source_route=0`
	If this is not the system default value, add the following line to the `/etc/sysctl.conf` file:
	`t.ipv6.conf.all.accept_source_route = 0`

Comments	**Future Feature.**

CCE-80660-4 Record Any Attempts to Run setfiles (Control Group = audit)

Check	At a minimum, the audit system should collect any execution attempt of the setfiles command for all users and root. If the auditd daemon is configured to use the augenrules program to read audit rules during daemon startup (the default), add the following lines to a file with `.rules` in `/etc/audit/rules.d: -a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F auid!=429496729as a suffix 5 -F key=privileged-priv_change`. If the `auditd` daemon is configured to use the `auditctl` utility to read audit rules during daemon startup, add the following lines to `/etc/audit/audit.rules` file: `-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F auid!=4294967295 -F key=privileged-priv_chang`
Comments	**Future Feature.**

CCE-80661-2 Ensure `auditd` Collects Information on Kernel Module Loading - `create_module` (Control Group = audit)

Check	To capture kernel module loading events, use following line, setting ARCH to either b32 for 32-bit system, or having two lines for both b32 and b64 in case your system is 64-bit: `-a always,exit -F arch=` The place where you add the line depends on the way `ARCH -S create_module -F key=modules auditd` daemon is configured. If it is configured to use the augenrules program (the default), add the line to a file with the `.rules` suffix in the `/etc/audit/rules.d` directory. If the `auditd` daemon is configured to use the `auditctl` utility, add the line to the `/etc/audit/audit.rules`file .
Comments	**Future Feature.**

Troubleshoot NetWitness Platform

For information about troubleshooting NetWitness, see the following topics:

- Debugging Information
- Error Notification
- Miscellaneous Tips
- NwLogPlayer: see the *Log Parser Customization Guide* for details.
- Troubleshoot Feeds

Debugging Information

NetWitness Log Files

The following files contain NetWitness 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	/var/lib/netwitness/uax/logs/nw.log
NetWitness	/var/lib/netwitness/uax/logs/audit/audit.log
NetWitness	/opt/rsa/jetty9/logs

Files of Interest

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

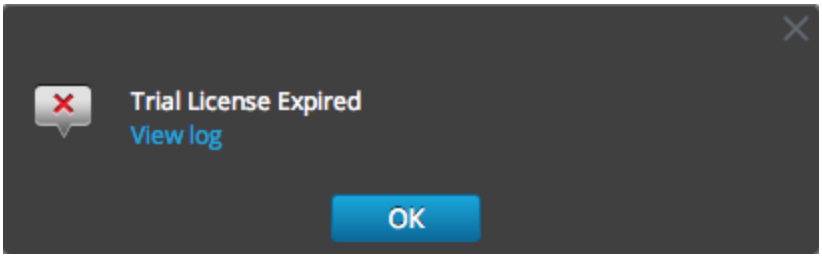
Component	File	Description
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQ configuration file. This configuration file partially drives the behavior of RabbitMQ, particularly around network/SSL settings.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQ environment configuration file. This file specifies the RabbitMQ node name and location of the enabled plugins file.

Component	File	Description
rabbit	/etc/rabbitmq/rsa_enabled_plugins	This file specifies the list of enabled plugins in RabbitMQ. This file is managed by the RabbitMQ server, with the `rabbitmq-plugins` command. This file overrides the `/etc/rabbitmq/enabled_plugins` path to work around issues with upgrading the Log Collector from early versions.
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.
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, for example, if messages are published as persistent messages, or have paged off to disk due to memory limitations. Keep a close eye on this directory if 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.

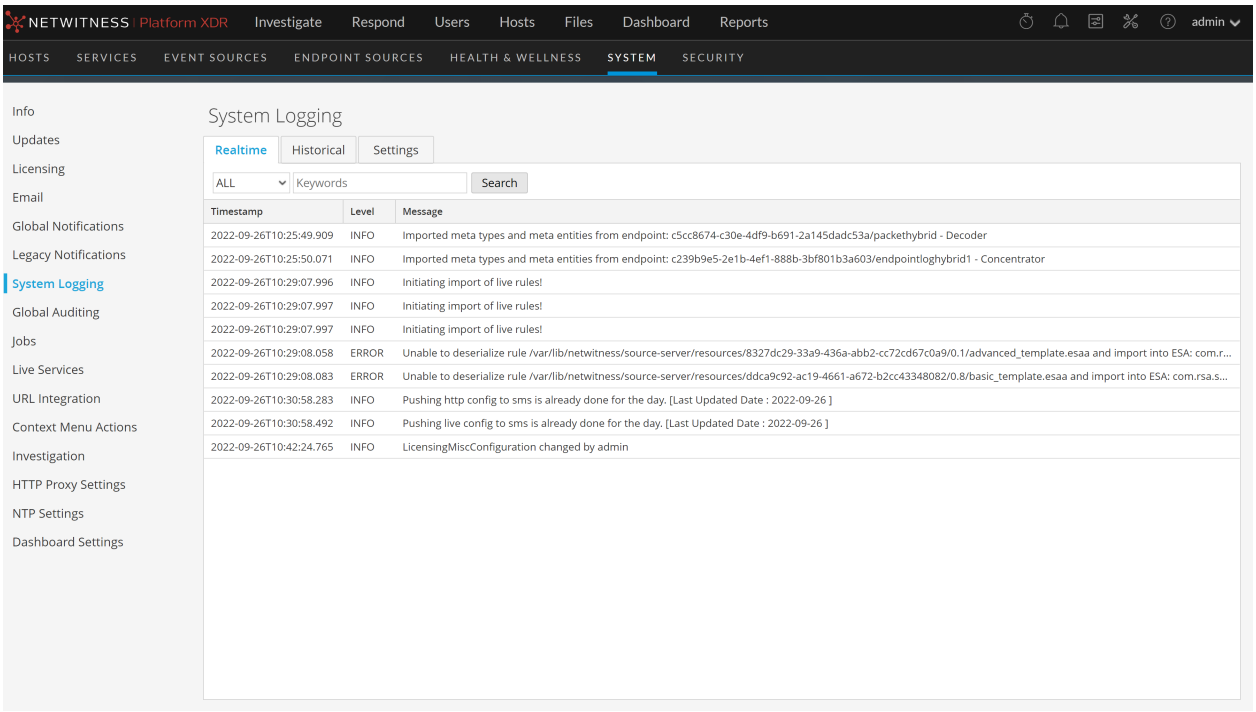
Error Notification

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

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



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



Miscellaneous Tips

Audit Log Messages

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

The event categories spreadsheet included in the log parser package in the NetWitness 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 the command option `logParse` in NwConsole. This command option supports log parsing, a convenient way to check a log parser without setting up the full system to perform log parsing. For more information about the `logParse` command, at the command line, type `help logParse`.

Thick Client Error: remote content device entry not found

The remote content device entry was not found error can be generated for a correlation rule applied to a Concentrator. In NetWitness Investigate, if you click the `correlation-rule-name` meta value in the Alert meta key, you do not get session information.

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://www.dell.com/support/home/en-us.

Configure WinRM Event Sources

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

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

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 it is not displayed in the correct event source groups, 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.

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 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 data exists on the Concentrator, and that events have values for the `device.group` field.

SMS Log File

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

The following are examples informational messages:

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

The following are examples of 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 and Published by ESMReader and ESMAggregator

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

ESMReader

1. On LogDecoders add the **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, 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 command:
   `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`.

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.

Troubleshooting Cert-Reissue Command

You must contact Customer Support (https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897) to troubleshoot problems. You know there is a problem if any `<host-id>` does not return a `Success`**Status**. `Success` indicates that certificates were reissued for a host.

Argument Options Used for Troubleshooting

You use the following argument options with `cert-reissue --host-all` to troubleshoot problems.

You can run `cert-reissue --host-all<arguments>` multiple times without an adverse effect.

Note: Use the following Argument Options with caution. They force the `cert-reissue` command to execute for all the hosts.

Argument Option	Description
`--skip-health-checks`	Reissues certificates for all hosts at one time without applying system health checks (force Reissue). This means that the command does not: • verify that all hosts are online line. • verify that all services are running. **Use case:** You have numerous hosts and you know that a small minority of them will fail. This updates all the hosts that conform to the checking rules and you can reissue certificates for the others subsequently with the help of Customer Support.
`--skip-version-checks`	Do not verify that hosts are running version 11.4.0.0 or later. **Use Case:** You have numerous hosts and your know that some of them are not updated to 11.4 or later. This reissues certificates for all the hosts that are at 11.4 or later and you can reissue certificates for the others subsequently with the help of Customer Support.
`--ignore-trigger-errors`	Ignore any errors that trigger failures. This option forces the cert reissue process to continue disregarding the errors instead of aborting or failing the cert reissue command quickly. When a cert reissue for a host succeeds, the reissued certificates on that host are not provisioned to other dependent hosts (referred to as trusts). In this case, the: • host with reissued certificates is reported as “Partial.” • the hosts with trusts that failed to update are listed separately in the summary table to tell you that these hosts may require a refresh using the new `--refresh-trusts-only` option.

Argument Option	Description
`--refresh-trusts-only`	Refreshes trusts exclusively for host identified by `<id>` (does not reissue certificates for that host).

Problems and How to Troubleshoot Them

This section describes solutions to problems that you may encounter when running the cert-reissue command to reissue certificates with suggested causes and solutions.

Status	Failed!
Error Message	... 2019-02-06 13:34:39.646 INFO 8540 --- [main] c.r.n.i.o.client.OrchestrationClient : Checking host connections... ... 2019-02-06 13:34:57.861 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator : Host '192.168.200.99' (nw-platform-esa-primary) verification failed! ... 2019-02-06 13:34:57.862 INFO 8540 --- [main] c.r.n.i.o.client.OrchestrationClient : Checking status of services... 2019-02-06 13:35:57.931 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator : Service 'nw-platform-node-zero - Investigate Server' not available! ... +---------+--------------------+--------+--+ | | Host | Status | Message | +---------+--------------------+--------+--+ |<host-id>| <IP-address> |Failed! |failed to connect, is host online? | |<host-id>| <IP-address> |Failed! |service(s) down | |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | +---------+--------------------+--------+--+
Cause	`cert-reissue --host-all` failed because one or more hosts are offline or one or more run time services are unreachable. You can force this command to run in spite of this error by specifying the `--skip-health-checks` option, that is: `cert-reissue --host-all--skip-health-checks`
Solution	1. Bring appropriate hosts back online or make sure the NW Server hosts run time services are running. 2. Run `cert-reissue` for the hosts affected.

Status	Failed!
Error Message	... 2019-02-06 13:34:39.643 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator : Host '192.168.200.102' (nw-platform-decoder) version '11.2.0.0' not supported, minimum required version: 11.3.0.0 2019-02-06 13:34:39.644 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator : Host '192.168.200.101' (nw-platform-concentrator) version '11.2.0.0' not supported, minimum required version: 11.3.0.0 ... +---------+--------------------+--------+---+ | | Host | Status | Message | +---------+--------------------+--------+---+ |<host-id>| <IP-address> |Failed! |version <version-earlier-than-11.3.0.0> not supported| |<host-id>| <IP-address> |Failed! |version <version-earlier-than-11.3.0.0> not supported| |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | +---------+--------------------+--------+---+
Cause	`cert-reissue -host-all` command string failed because one or more hosts are running a version earlier than 11.4.0.0 **Note:** You can force the reissue of certificates for the remaining hosts using the `-skip-version-checks` argument.
Solution	Update the host to 11.4 or later and run `cert-reissue` for that host again.

Status	Partial
Error Message	... 2019-02-06 02:27:09.078 ERROR 20647 --- [main] c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '<IP-address>' (nw-platform-decoder) 2019-02-06 02:27:09.079 ERROR 20647 --- [main] c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '<IP-address>' (nw-platform-concentrator) ... 2019-02-06 02:27:09.118 WARN 20647 --- [main] c.r.n.i.o.client.OrchestrationClient : One or more host(s) may require manual refresh due to failed triggers: +---------+--------------------+ | | Host | +---------+--------------------+ |<host-id>| <IP-address> | |<host-id>| <IP-address> | +---------+--------------------+ ... +---------+--------------------+--------+---+ | | Host | Status | Message | +---------+--------------------+--------+---+ |<host-id>| <IP-address> |Partial |Reissue completed, triggers failed | |<host-id>| <IP-address> |N/A |[Skipped…] | |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | |<host-id>| <IP-address> |N/A |[Skipped...] | +---------+--------------------+--------+---+
Cause	`cert-reissue` command completed on NW Server host however one or more triggers failed. This aborted the `cert-reissue` command for other hosts.
Solution	Address all the errors and run the `cert-reissue --host-all<arguments>` command string again.

Status	Partial
Error Message	... 2019-02-06 14:18:03.208 ERROR 17800 --- [main] c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '192.168.200.82' (nw-platform-node-x) ... ... 2019-02-06 14:29:05.200 WARN 17800 --- [main] c.r.n.i.o.client.OrchestrationClient : One or more host(s) may require manual refresh due to failed triggers: +---------+--------------------+ | | Host | +---------+--------------------+ |<host-id>| <IP-address> | +---------+--------------------+ ... +---------+--------------------+--------+---+ | | Host | Status | Message | +---------+--------------------+--------+---+ |<host-id>| <IP-address> |Failed! |Cert reissue failed! | |<host-id>| <IP-address> |Partial |Reissue completed, triggers failed | |<host-id>| <IP-address> |Success | Cert reissue successful | |<host-id>| <IP-address> |Success | Cert reissue successful | |<host-id>| <IP-address> |Success | Cert reissue successful | +---------+--------------------+--------+---+
Cause	One or more hosts did not pass system health checks. In addition, one or more of the unhealthy hosts are running core services, which will result in the NW Server host `cert-reissue` to fail (because of failed triggers explained above). By disabling health checks and trigger errors, you can continue the process and reissue certificates for the remaining hosts. The NW Server host **Status** is reported as `Partial` because the `cert-reissue` command completed for the NW Server but downstream triggers failed for other hosts.
Solution	Manually refresh the failed core hosts (to synchronize trust peers). Submit the following command string to reissue certificates for healthy hosts. `cert-reissue --host-all --skip-health-checks --ignore-trigger-errors`

References

This section describes the NetWitness 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, NetWitness Console utility, and protocols supported in NetWitness).
- Display the current NetWitness 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
  - Health and Wellness View - Alarms View
  - Event Source Monitoring View
  - Health and Wellness Historical Graphs
    - Historical Graph View for Events Collected from an Event Source
    - Historical Graph for System Stats
  - 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
- New Health & Wellness Tab
- System View - System Info Panel
- System Updates Panel - Settings Tab
- System Logging - Settings View
- System Logging - Realtime Tab
- System Logging - Historical Tab

Health and Wellness View

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

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

Health and Wellness View - Alarms View

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

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

What do you want to do?

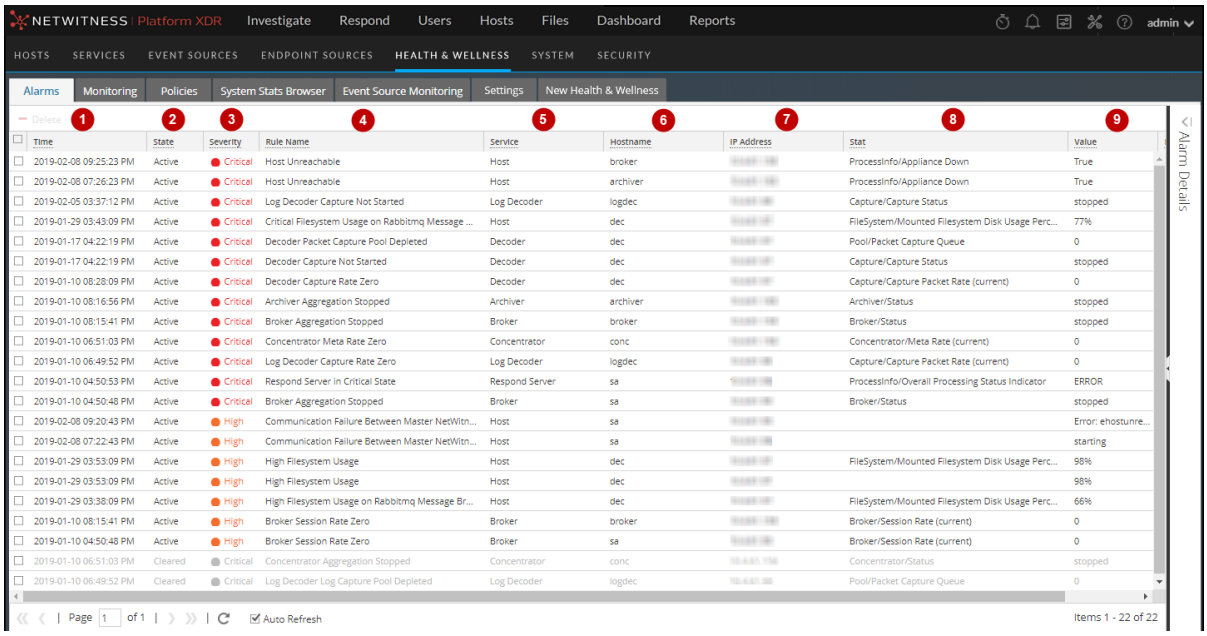
Role	I want to ...	Show me how
Administrator	View the alarm status of NetWitness Servers and services.	Monitor Alarms
Administrator	View detailed information about a specific alarm.	Monitor Alarms

Related Topics

Manage Policies

Quick Look

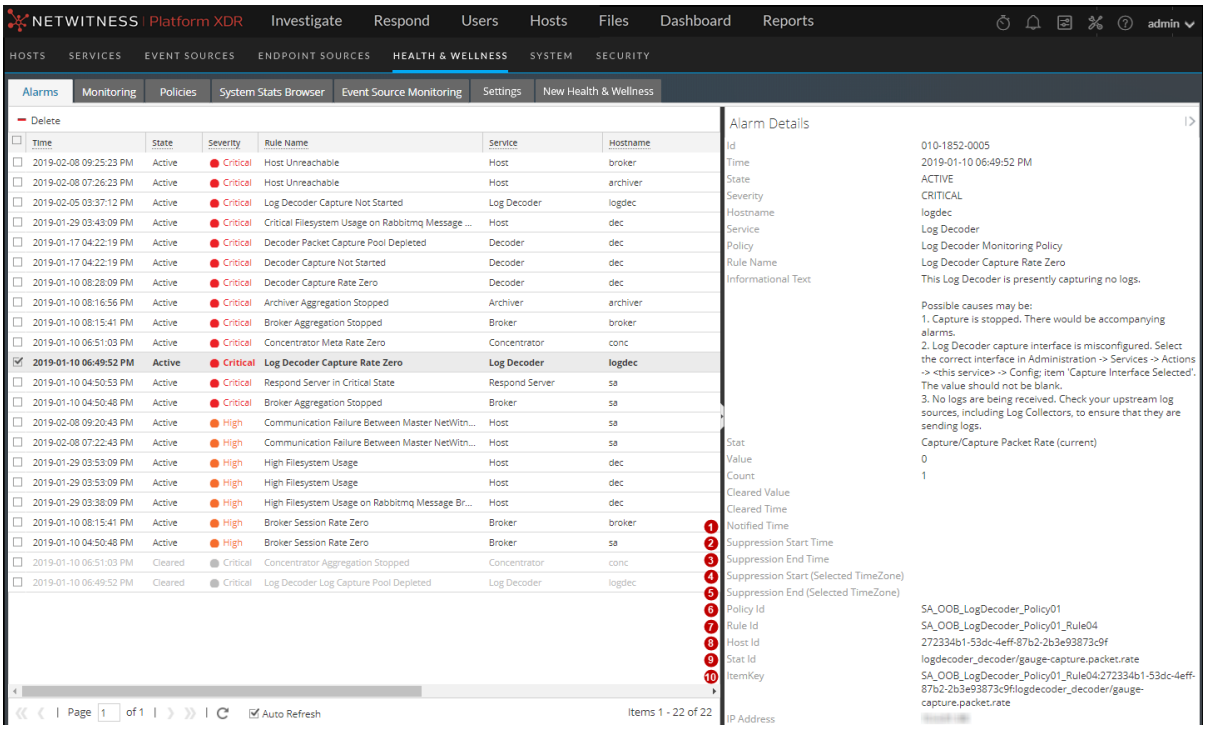
The required permission to access this view is **Manage services**. To access the Alarms view, go to **(Admin)** > **Health & Wellness**. The Health & Wellness view opens with the Alarms tab displayed. The Alarms tab contains an alarms list and an Alarm Details panel.



1	Time when the alarm was triggered.
2	Status of the alarm: • **Active** - the statistical threshold was crossed triggering the alarm. • **Cleared** - the clearing threshold was crossed and the alarm is no longer active.
3	Severity assigned to this alarm: • **Critical** • **High** • **Medium** • **Low**
4	Name of the rule that triggers the alarm.
5	Service defined in the rule.
6	Host on which the alarm is triggered.
7	Statistic selected in the rule that triggers the alarm.
8	Value of the statistic that triggered the alarm.
9	Identification number of the alarm.

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

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



Alarm Details Panel

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

1. Alarm Notified time
2. Suppression start time
3. Suppression end time
4. Suppression start (selected time zone)
5. Suppression end (selected time zone)
6. The Policy ID
7. The Rule ID
8. The Host ID
9. The Stat ID
10. Item key

Event Source Monitoring View

Note: For NetWitness 11.3.1, this view has been deprecated: this functionality is now available in the **(Admin) > Event Sources > Discovery** view. To manage Event Sources, see "About Event Source Management" in the *NetWitness Event Source Management Guide*.

Health and Wellness Historical Graphs

Configuring Archiver monitoring enables you to automatically generate notifications 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

Note: For NetWitness 11.4.1, this view has been deprecated. To manage Event Sources, use the (Admin) > Event Sources view. For details, see "About Event Source Management" in the*NetWitness Event Source Management Guide*.

Historical Graph for System Stats

To access the Historical Graph for the System Stats:

1. Go to **(Admin) > Health & Wellness**.

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

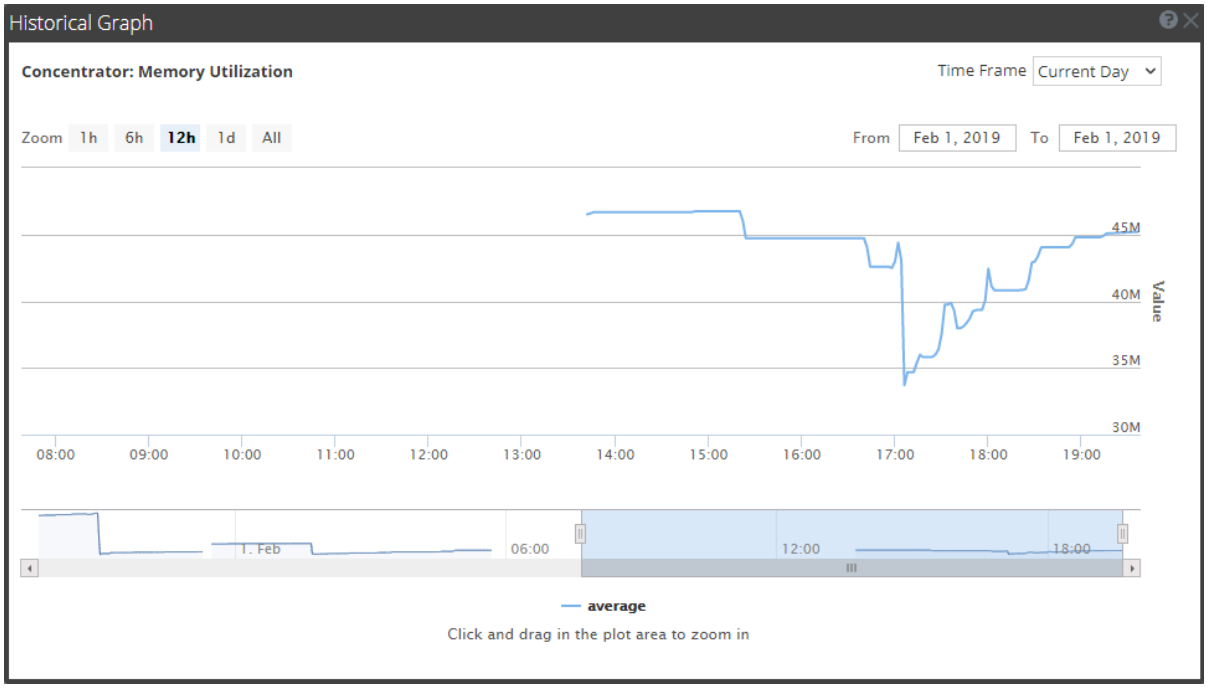
2. Click the **System Stats Browser** tab.

   The System Stats Browser tab is displayed.

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

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

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



Parameters

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

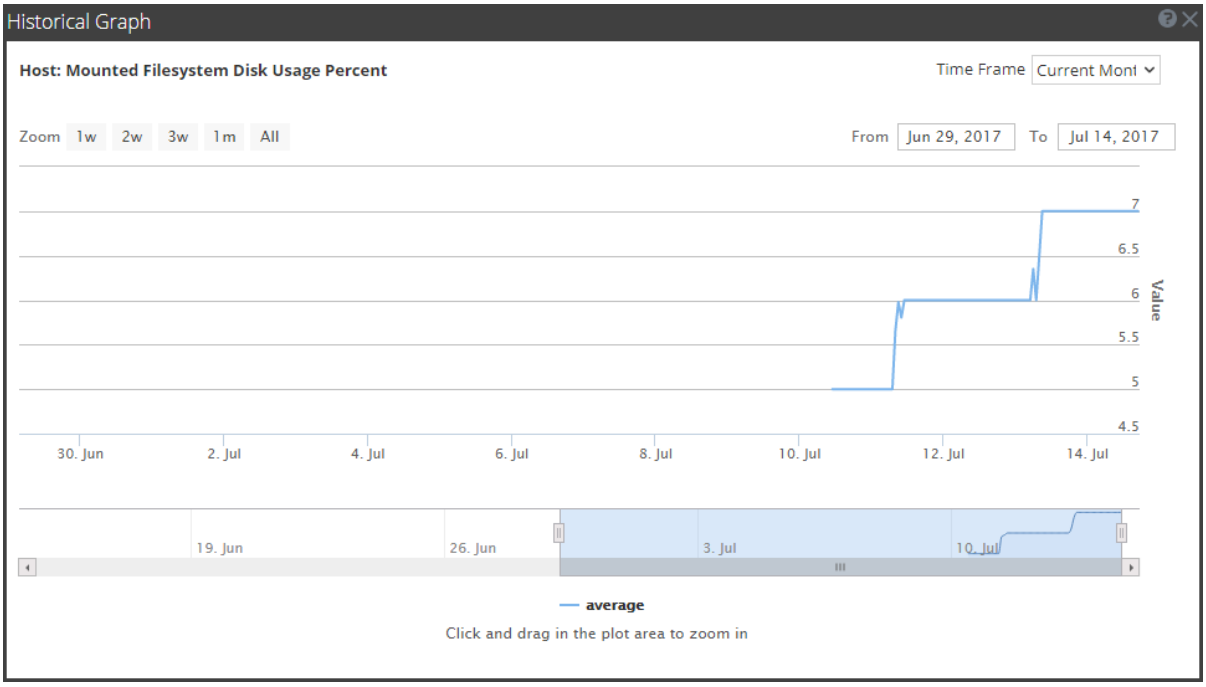
Parameter	Description
Time Frame	Select the time frame for which you want to view the historical data. The available options are: **Current Day**, **Current Week**, **Current Month**, and **Current Year**.
From <date> To <date>	Select the date range for which you want to view the historical data,

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

Zoom in function 1 and 2:

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

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



Zoom in function 3:

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

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

Health and Wellness Settings View - Archiver

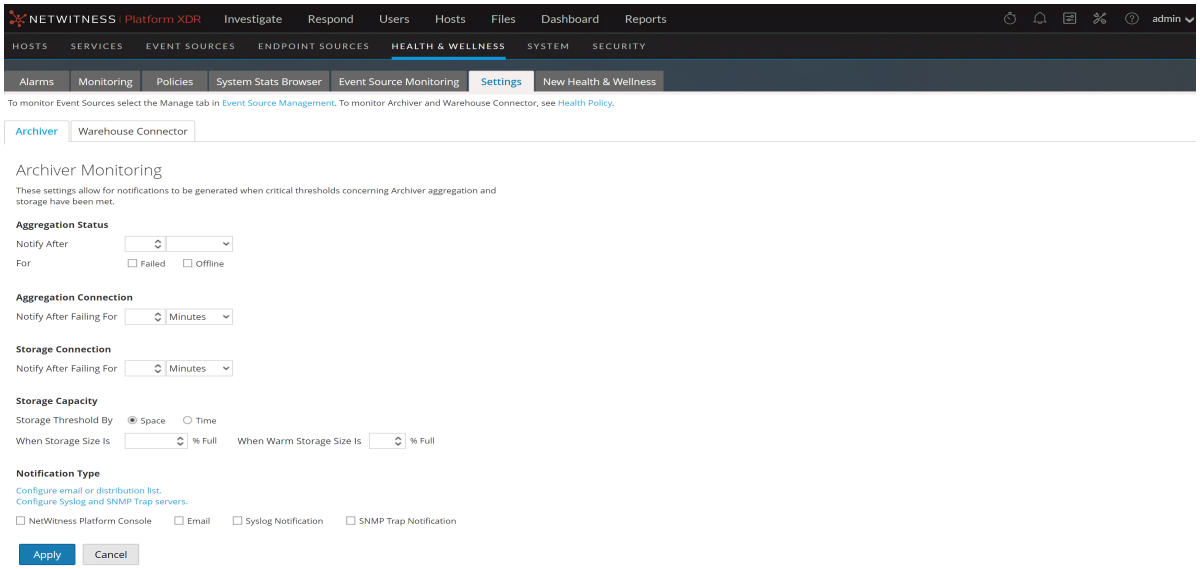
To access the Archiver Monitoring view:

1. Go to **(Admin) > Health & Wellness**.
2. Select **Settings > Archiver**.

What do you want to do?

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

Quick Look



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

Features

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

Parameter	Value	Description
Aggregation Status	Notify After	Number of minutes or hours after which you are notified of aggregation status
	For	Failed - If enabled, you are notified when the Archiver aggregation status is failed for the defined number of minutes or hours. Offline - If enabled, you are notified 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 receive notification if the Archiver aggregation connection fails.
Storage Connection	Notify After Failing for	Number of minutes or hours after which you receive 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 the percentage of used storage to trigger a notification.
	When Warm Storage Size Is	Enter the percentage of used storage on the warm server to trigger a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness.
	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 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: For NetWitness 11.4.1, this view has been deprecated. To manage Event Sources, use the (Admin) > Event Sources view. For details, see "About Event Source Management" in the*NetWitness Event Source Management Guide*.

Health and Wellness Settings View - Warehouse Connector

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

Access the Warehouse Connector Monitoring view

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

What do you want to do?

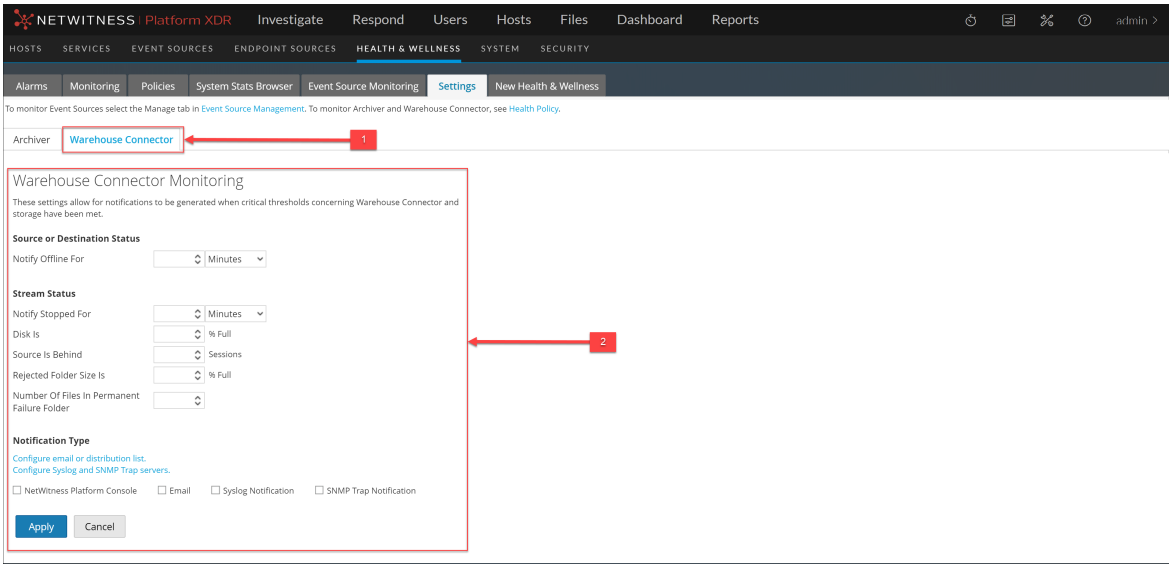
Role	I want to ...	Show me how
Administrator	View the details of Warehouse connector	Warehouse Connector Details View

Related topics

Monitor Service Details

Quick Look

The Warehouse Connector Monitoring view is displayed.



1 Displays the Warehouse Connector Monitoring view panel.
2 Allows you 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 you receive a notification if the source or destination connection fails.
Stream Status	Notify Stopped For	Number of minutes or hours after which you 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 receive a notification.
	Number Of Files in Permanent Failure Folder	Limit on the number of files in the permanent failure folder after which you receive a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in NetWitness.
	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 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 provides detailed statistics and other information about the host and the individual NetWitness services in Details views. You can view the current health of all the hosts and the services running on the hosts in the Monitoring view.

What do you want to do?

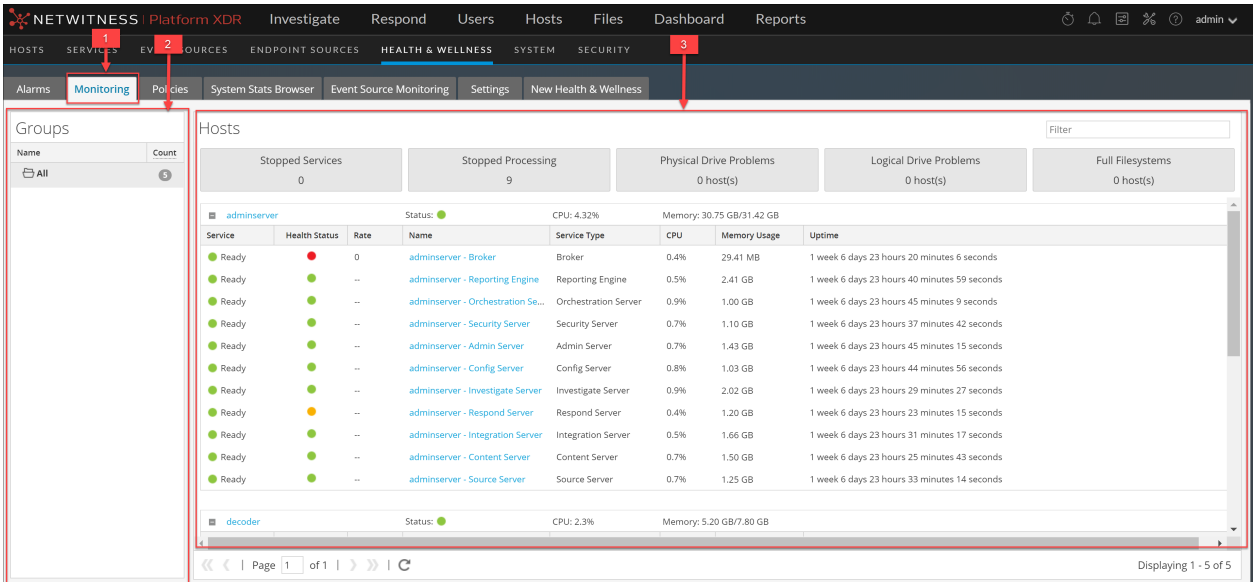
Role	I want to ...	Show me how
Administrator	View and Perform Procedures	Monitor Hosts and Services

Quick Look

To access this view:

1. Go to **(Admin) > Health & Wellness**.
2. Click the **Monitoring** tab.

The Monitoring view is displayed.



1 The Monitoring tab shows health statistics for the NetWitness Platform hosts and services.
2 The Group panel enables you to view statistics for a selected group.
3 The Hosts panel displays operational statistics.

Groups Panel

The Groups panel lists all of 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, 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 of the hosts configured in NetWitness and does not change with the application of filters on the groups.

Below the boxes at the top of the Hosts panel is a list of hosts, the services installed on them, and information regarding the hosts and services.

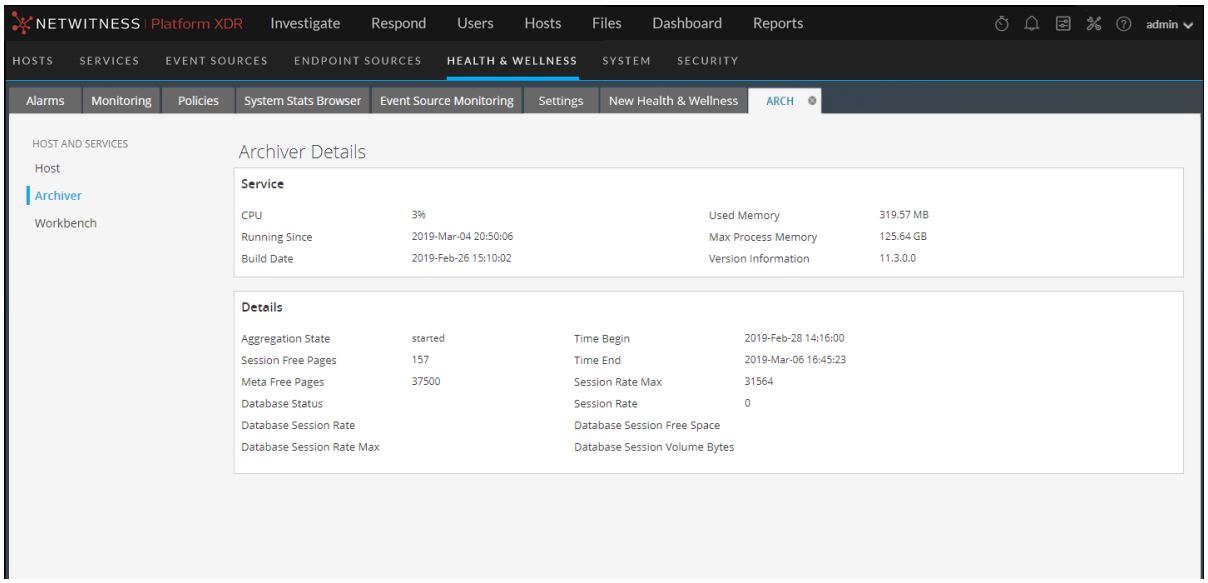
Parameter	Description
Host Name	Displays the host name. If a host has services installed that are not in view, you will see a ⊞ prefixed to the host name. Click ⊞ to view all the services installed on the host.
Status	Displays the status of the Host. ● - The host is active and running. ● - The host is 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 parameters displayed for a service and their description.

Parameter	Description
Service	Displays the status of the service. ● Ready - The service is active and running. ● Stopped - The service is stopped or yet to start processing.
Health Status	Displays the processing status of the service. - The process is running and the data is being processed at a rate greater than zero. ● - The processing is stopped. ● - The processing is turned on but the data is not being processed.
Rate	Shows the rate at which data is being processed.
Name	Name of the service in the format `<host> - <service>`. Click the link in the Name field to get additional service details.
Service Type	Name of the type of service.
CPU	Shows 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 shows the Archiver details.



For the related procedure, see Monitor Service Details

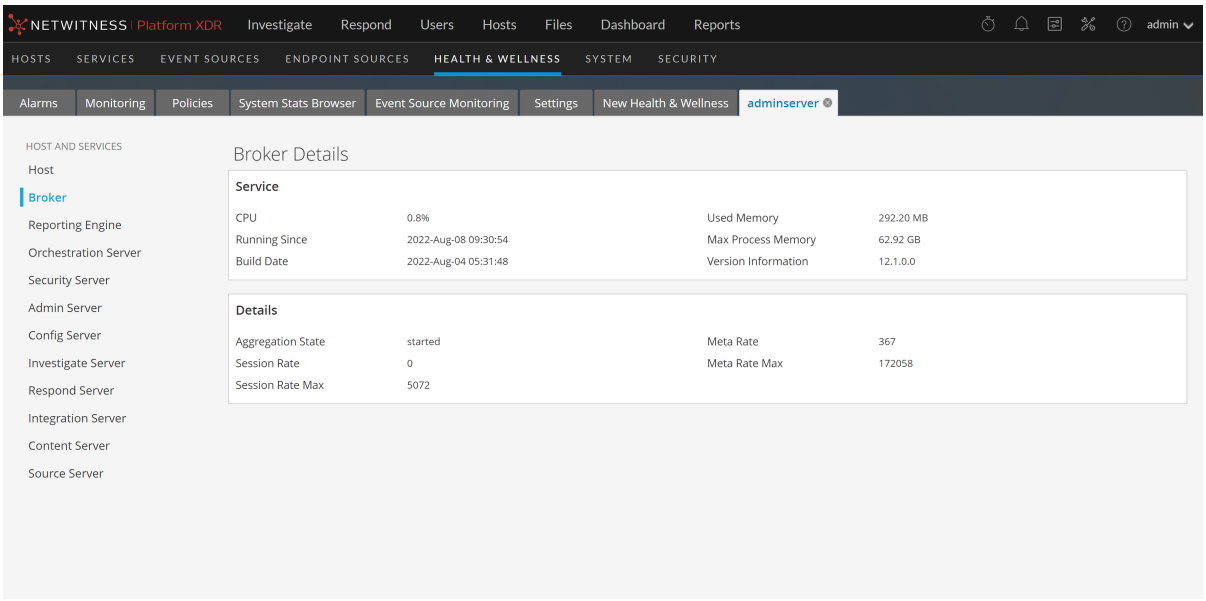
This section displays the current generic statistics for the service.

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

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

Broker Details View

The Broker Details view provides information about the Broker. The following figure shows the Broker details.



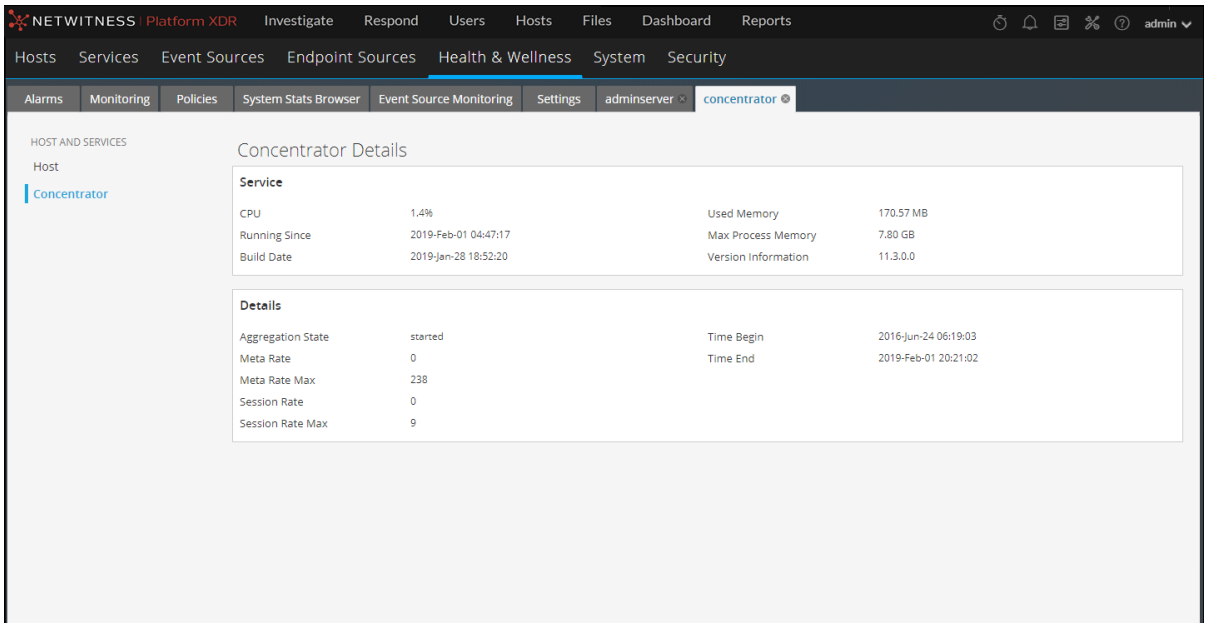
For the related procedure, see Monitor Service Details.

This section displays the current generic statistics for the service.

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

Concentrator Details View

The Concentrator Details view provides information about the Concentrator. The following figure shows the Concentrator details.



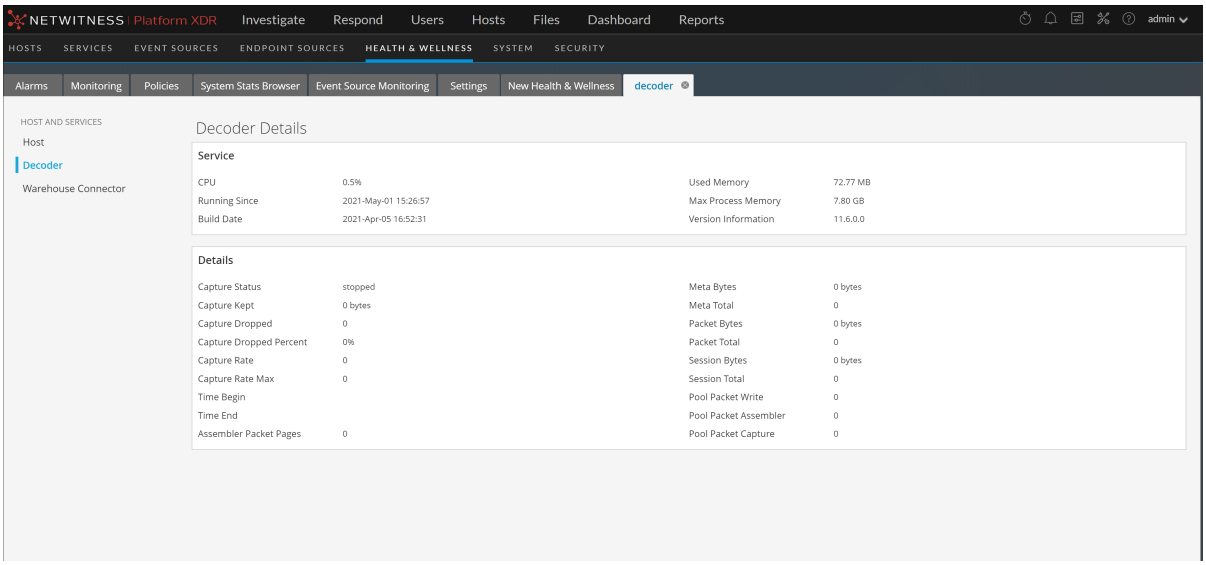
For the related procedure, see Monitor Service Details

The section displays the current generic statistics for the service.

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

Decoder Details View

The Decoder Details view provides information about the Decoder. The following figure shows the Decoder details.



For the related procedure, see Monitor Service Details.

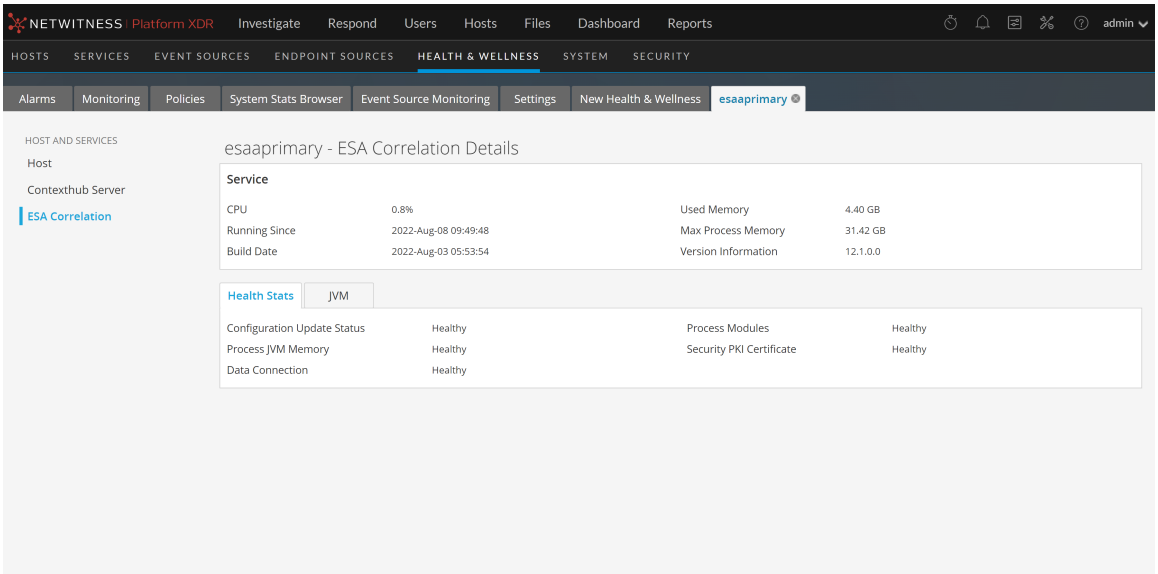
This section displays the current generic statistics for the service.

Statistic	Description
Capture Status	Status of data capture. Valid values are: • `starting` - Starting data capture (not capturing data yet). • `started` - Capturing data. • `stopping` - Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet). • `stopped` - Not capturing data. • `disabled` - Not configured as a Decoder service.
Meta Bytes	Number of meta bytes in the database.
Capture Kept	Number of packets kept during capture.
Meta Total	Amount of metadata in the database.
Capture Dropped	Number of packets reported by the network card as dropped. After the service stops capturing data, the rate is reset to zero.
Packet Bytes	Number of packet bytes in the database.

Statistic	Description
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.
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 pool 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.

ESA Correlation Details View

The ESA Correlation Details view provides information for the ESA Correlation service. The following figure shows the ESA Correlation service details.



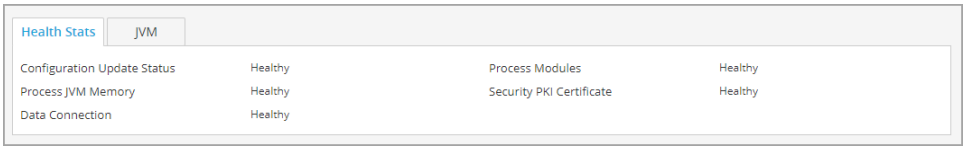
For the related procedure, see Monitor Service Details.

Many services, including the ESA Correlation service, have Health Stats and Java Virtual Machine (JVM) tabs. The Health Stats tab provides information about the health status of the service. The JVM tab shows the total memory used by the selected service and the total memory capacity of the host.

For more information on the ESA Correlation service and ESA Rule memory usage, see the *Alerting with ESA Correlation Rules User Guide*.

Health Stats Tab

The Health Stats tab provides information about the health status of the selected service.



The services on this tab can show one of three states:

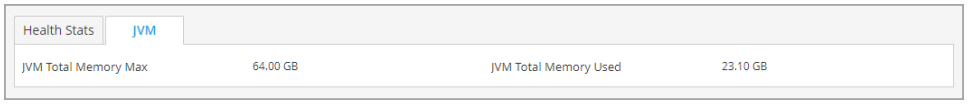
- `Healthy`: The service is healthy.
- `Unhealthy`: The service is mostly functional, but it needs attention to mitigate potential down time.
- `Fatal`: Action needs to be taken to restore the service.

Statistic	Description
Configuration Update Status	Indicates whether the service requires a restart for configuration changes to take effect. If the Configuration Update Status shows as Unhealthy, restart the service.

Statistic	Description
Process JVM Memory	Indicates the memory usage status. An Unhealthy status occurs when heap memory usage is greater than or equal to 80%. A Fatal status occurs when heap memory usage is greater than or equal to 95%. If the service is using too much memory, you can add more memory or move services to other hosts. For more details on memory usage, go to the JVM tab.
Data Connection	Indicates the health of the database connection of the service to MongoDB.
Process Modules	Indicates the health of the service. If a service is starting up, it shows as Unhealthy since its health is not yet determined. A service is Healthy if it is up and running properly. A service shows as Fatal if it is running in upgrade mode or if the service is running in safe or degraded mode.
Security PKI Certificate	Indicates the service certificate health. It shows as Healthy if a given X509 certificate is self-signed.

JVM Tab

The JVM tab shows the total memory used by the selected service and the total memory capacity of the host.

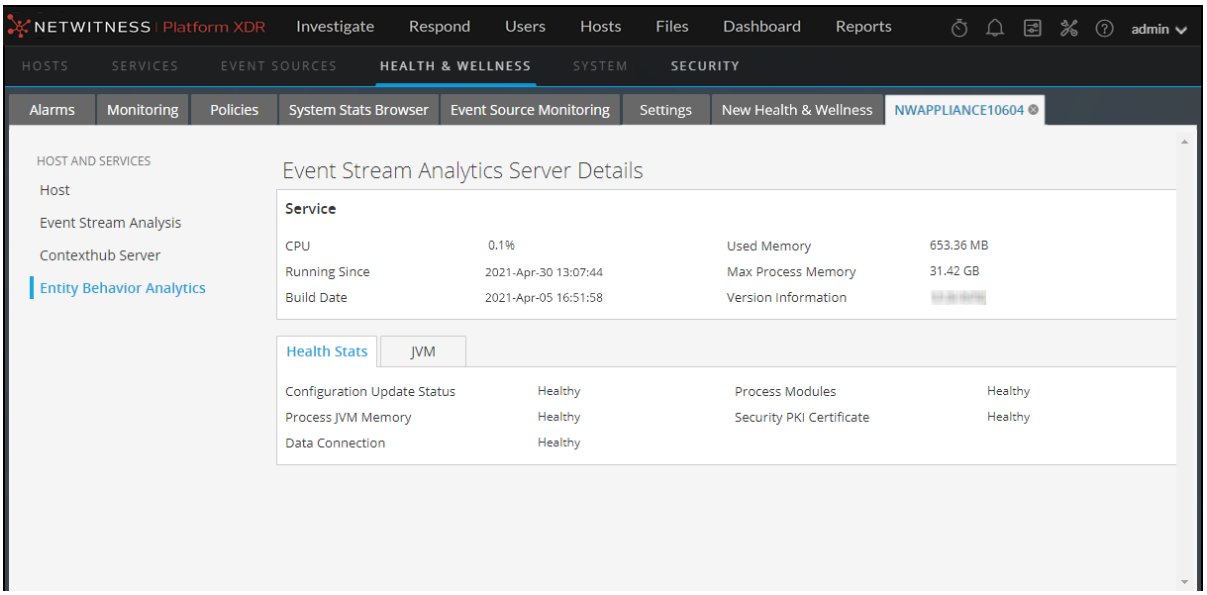


Statistic	Description
JVM Total Memory Max	Shows the total memory capacity for the entire host.
JVM Total Memory Used	Shows the total memory used by all services and processes on the host.

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 item that shows a status other than healthy, so that data processing is not interrupted and critical events are not missed.

The following figure shows the ESA Analytics Details view.



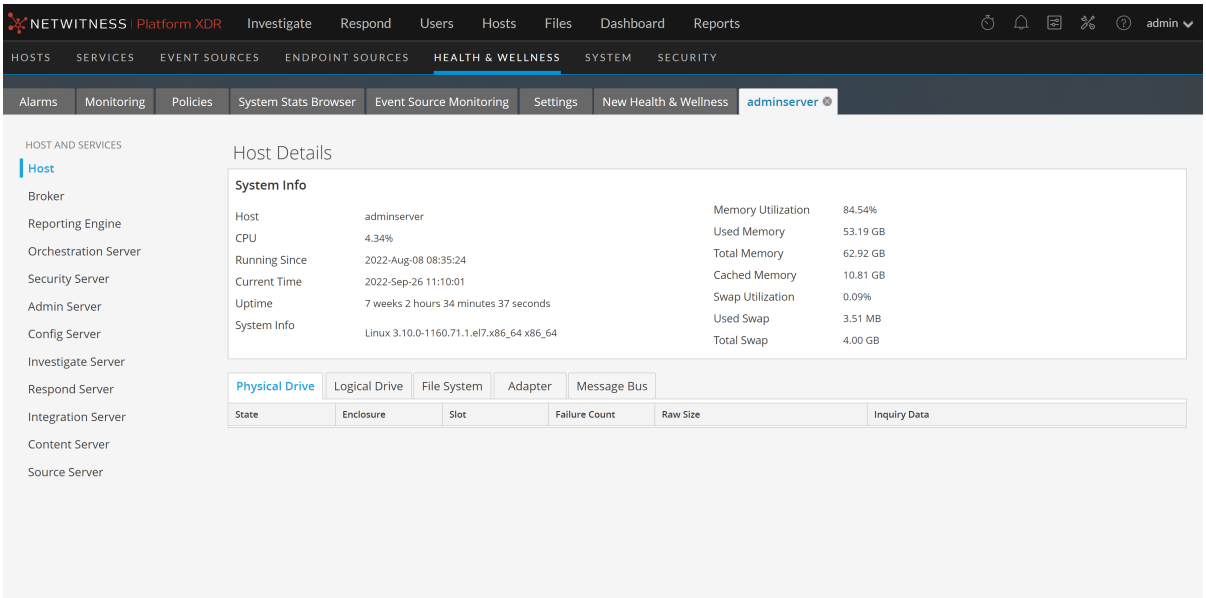
For the related procedure, see Monitor Service Details.

Many services, including the ESA Analytics service, have **Health Stats** and Java Virtual Machine (**JVM**) tabs. The **Health Stats** tab provides information about the health status of the service. The **JVM tab** shows the total memory used by the selected service and the total memory capacity of the host. For more information, see Health Stats Tab and JVM Tab.

For more information on ESA Analytics, see the *Automated Threat Detection Guide* and the *ESA Configuration Guide*.

Host Details View

The Host Details view provides information about a host, as shown in the following figure.



The options panel on the left displays the host and the services installed on the host. You can click on a host or 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

The top 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.
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.

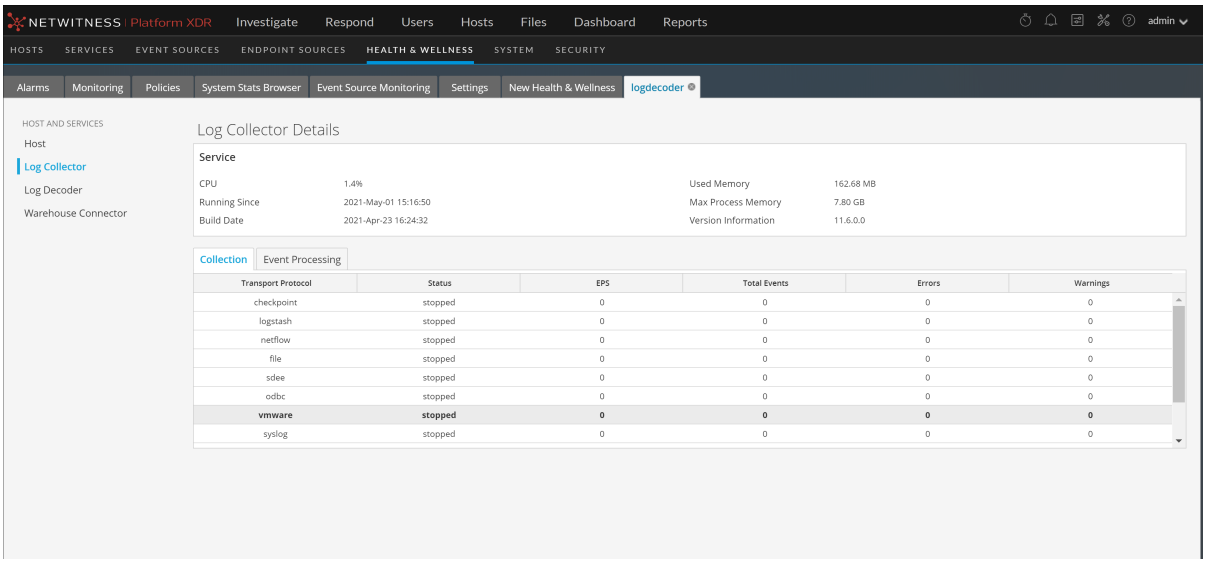
Parameter	Description
Swap Utilization	Percentage of system swap in use.
Used Swap	Swap used in GB.
Total Swap	Capacity of the swap installed on the system.

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.
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 NetWitness 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 NetWitness 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 NetWitness has stopped accepting messages. Memory Alarm - True or False. True indicates that the available memory is below the value set in Memory Limit and NetWitness has stopped accepting messages.

Log Collector Details View

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



For the related procedure, see Monitor Service Details.

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

Collection Tab

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

Event Processing Tab

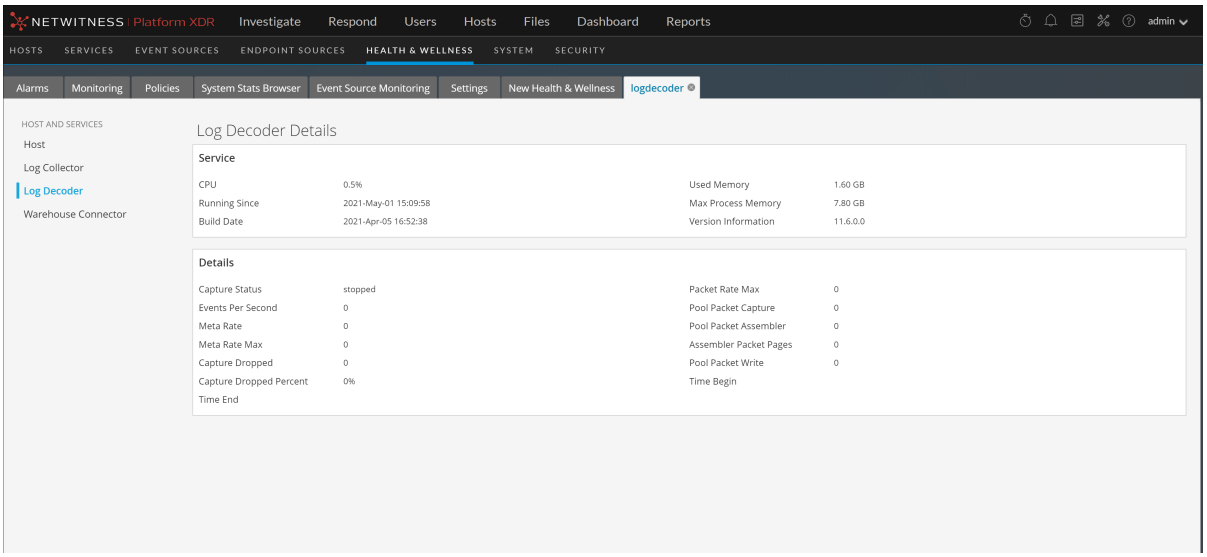
Displays statistics for the NetWitness internal event processing protocol (that is, the Log Decoder) for Log Collection.

Parameter	Description
Transport Protocol	NetWitness 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 shows the Log Decoder Details.



For the related procedure, see Monitor Service Details.

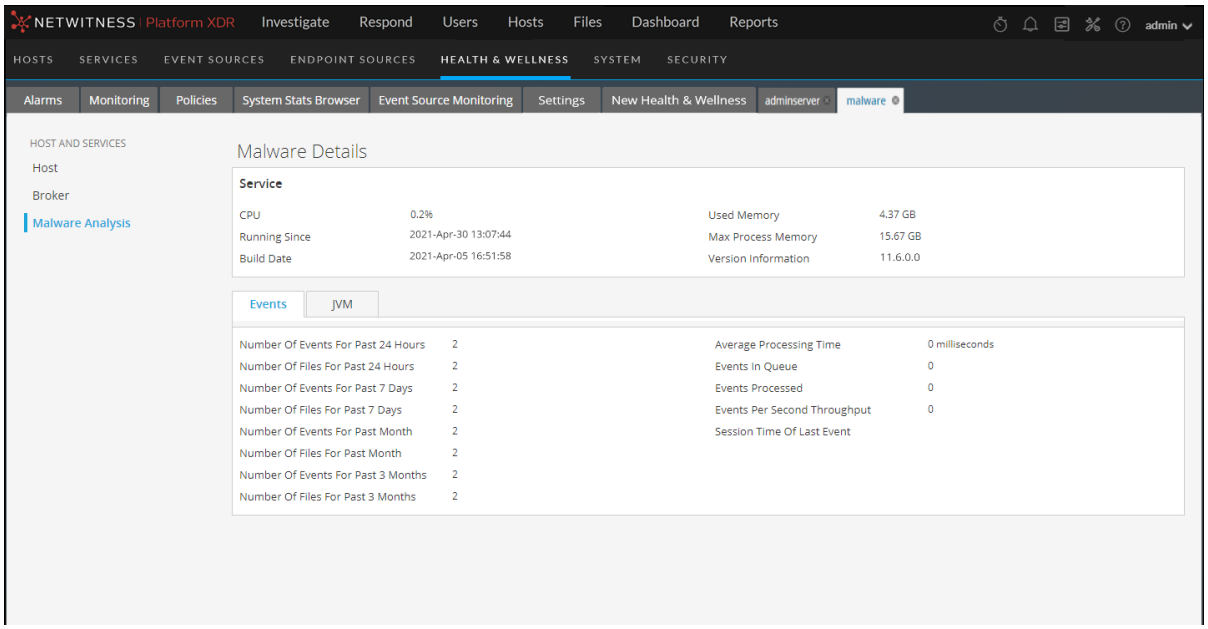
This section displays the current generic statistics for the service.

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

Statistic	Description
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.
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 shows the Malware Details.



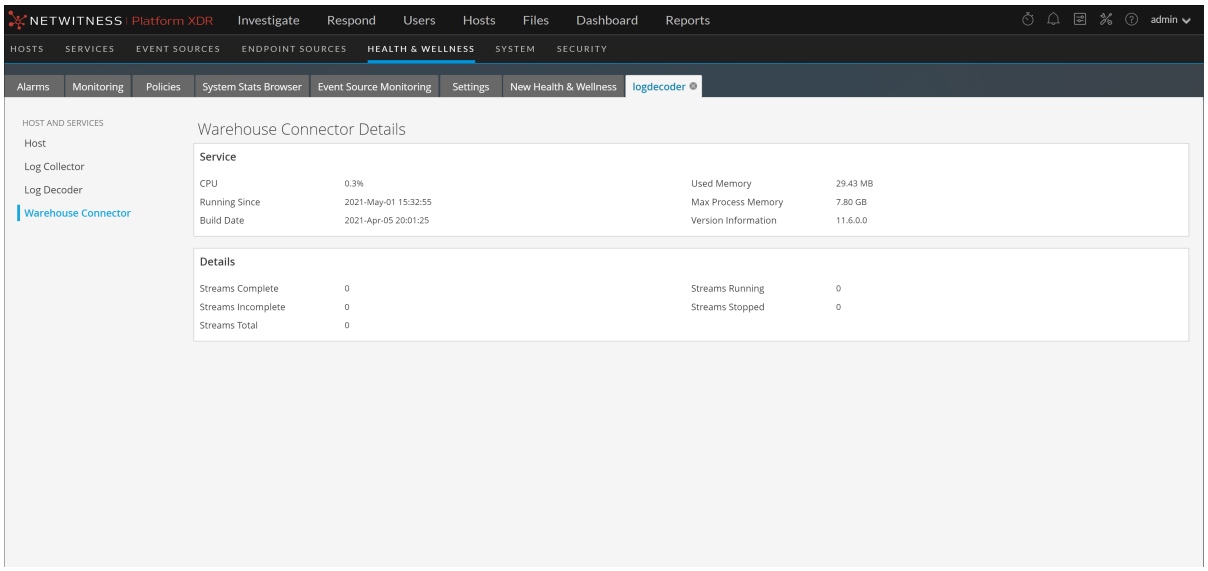
For the related procedure, see Monitor Service Details.

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

- Number of events for the past 24 hours
- Average processing time
- Number of files for the past 24 hours
- Events in queue
- Number of events for the past 7 days
- Events processed
- Number of events for the past 7 days
- Events per second throughput
- Number of events for the past month
- Session time of the last event
- Number of files for the past month
- Number of events for the past 3 months
- Number of files for the past 3 months

Warehouse Connector Details View

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



For the related procedure, see Monitor Service Details.

Policies View

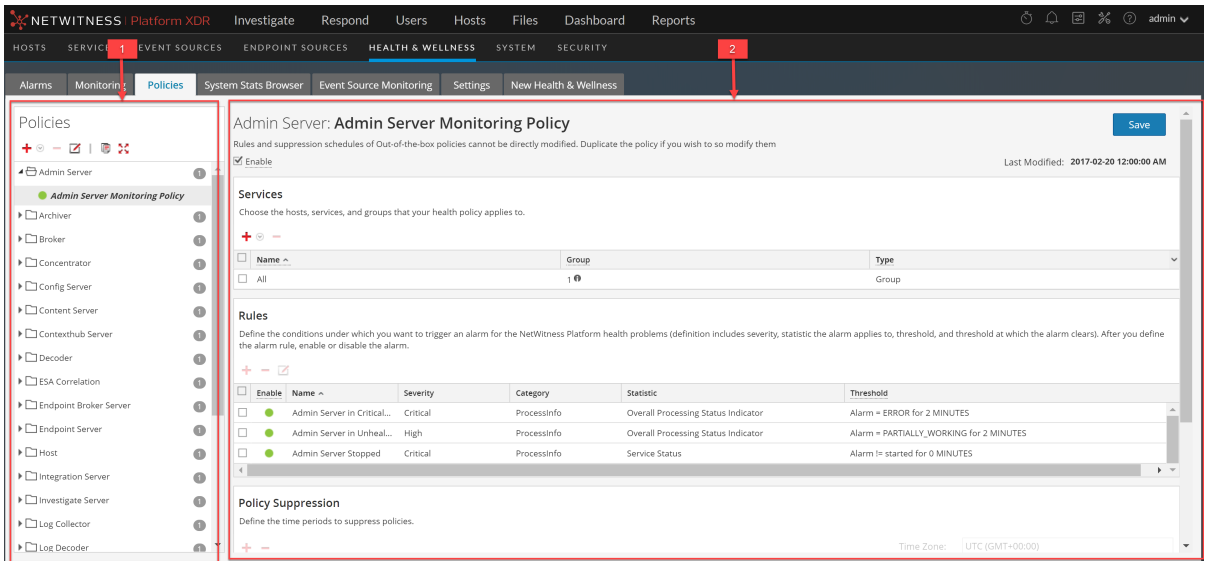
The required permission to access this view is **Manage services**.

What do you want to do?

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

Quick Look

The figure depicts the Policies view.



1 Policies Panel
2 Policy Detail Panel

1. Go to **(Admin) > Health & Wellness**.
2. Click the **Policies** tab.

Policies Panel

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

Feature	Description
	Displays available service types to create a new policy. Select one so that you can define a policy or policies for it.

Feature	Description
	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 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. • NetWitness 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	Enables or disables the policy.
Services	
	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 the policy type is Host, the menu displays Host (and 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.

Feature	Description
	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.
Notification	
	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.
	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	Selects 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	Selects the Template for this EMAIL notification. NetWitness 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	
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

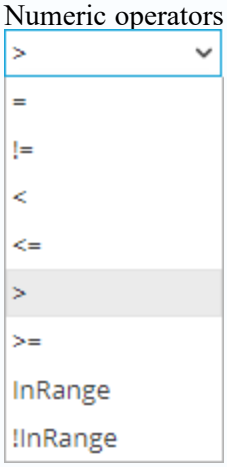
Feature	Description
☐ Enable	Enables or disables the rule for this policy.
Name	Describes the name of the rule.
Description	Describes the rule. Include the following information in this field. • Informational description - purpose of the rule and what problem it monitors. • Remediation - steps to take to resolve the condition that triggers the alarm for this rule.
Severity	Defines the severity of the rule. Valid values are: • Critical • High • Medium • Low

Feature	Description
Statistic	Defines 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. Refer to the System Stats Browser View for examples of the statistics you may want to check with a rule.
Alarm Threshold	Defines he threshold of the rule that triggers the policy alarm: • Amount **Note:** For CRL expiry the supported format is ddddhhmm, for example: - 10000 represents 1 day - 2359 represents 23 hours and 59 minutes - 10023 represents 1 day and 23 minutes - 3650100 represents 365 days and 1 hour • Time in minutes
Recovery	Defines when to clear the threshold of the rule: • Operator • Amount • Time in minutes
Rule Suppression	
	Adds a rule suppression timeframe row.
	Deletes the selected rule suppression time frame row.
	Selects 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	Defines 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	Defines the time range during which the rule is suppressed for the days selected.

Threshold Operators

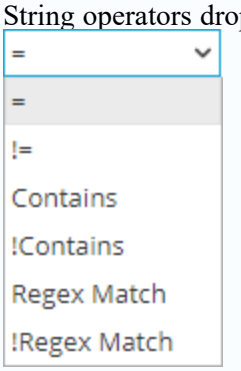
The **Alarm Threshold** and **Recovery Threshold** fields in the Rules dialog prompt you for either numeric or string operators based on the statistic criteria you specify.

Numeric operators drop-down menu:



=
!=
<
<=
>
>=
InRange
!InRange

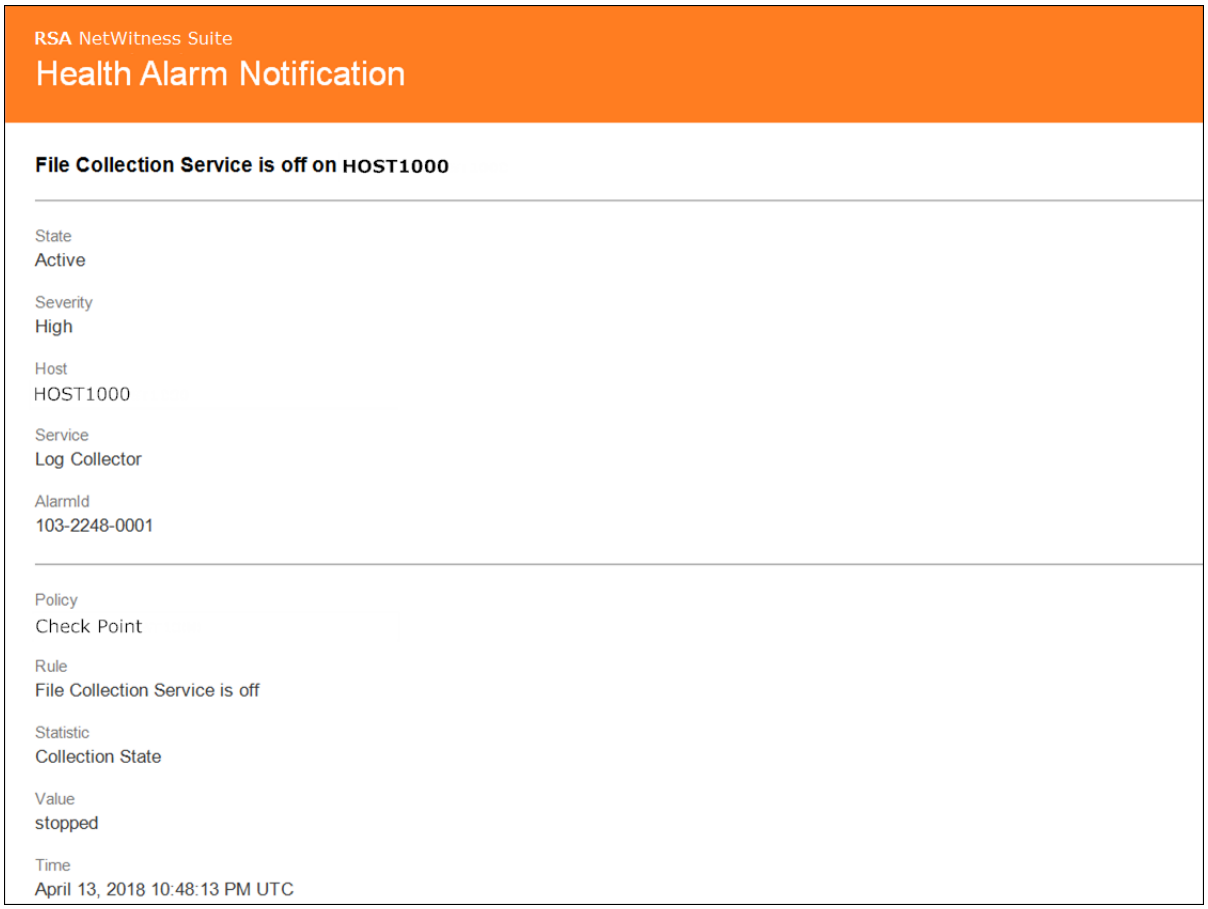
String operators drop-down menu:



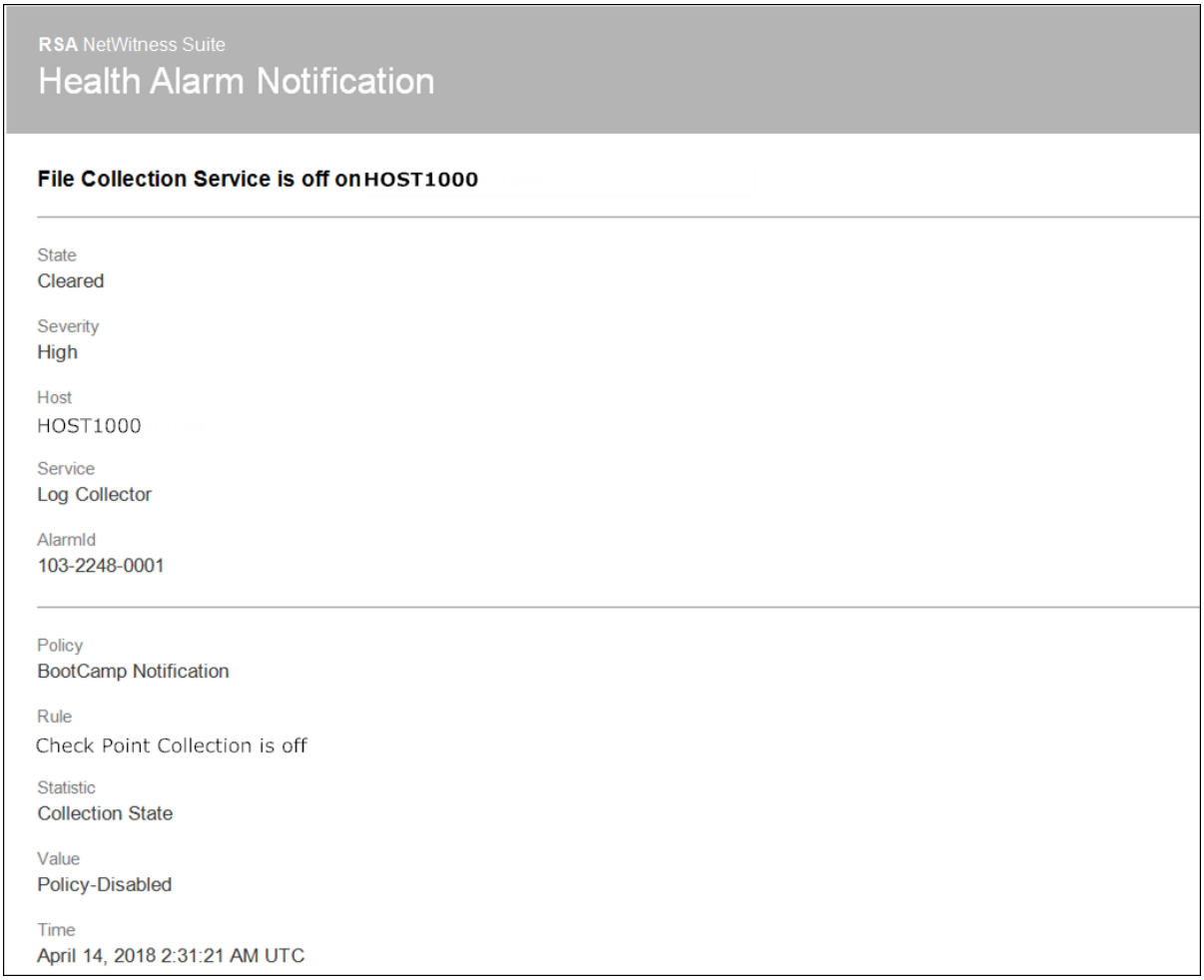
Health & Wellness Email Templates

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

Health & Wellness Default SMTP Template



Alarms Template



NetWitness Platform Out-of-the-Box Policies

The following table lists the NetWitness 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 and group assignments.
- Disable or enable policies.

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 NetWitness Server 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.
	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.

Policy Name	Rule Name	Alarm Triggered
NetWitness 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.
NetWitness 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.
NetWitness 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 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 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.
NetWitness 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 Incident Management Monitoring Policy	Incident Management Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
NetWitness 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.
NetWitness 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 Malware Analysis Monitoring Policy	Malware Analysis Service Stopped	Server Status does not equal started.

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

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

To access the System Stats Browser view:

1. Go to **(Admin) > Health & Wellness**.

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

What do you want to do?

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

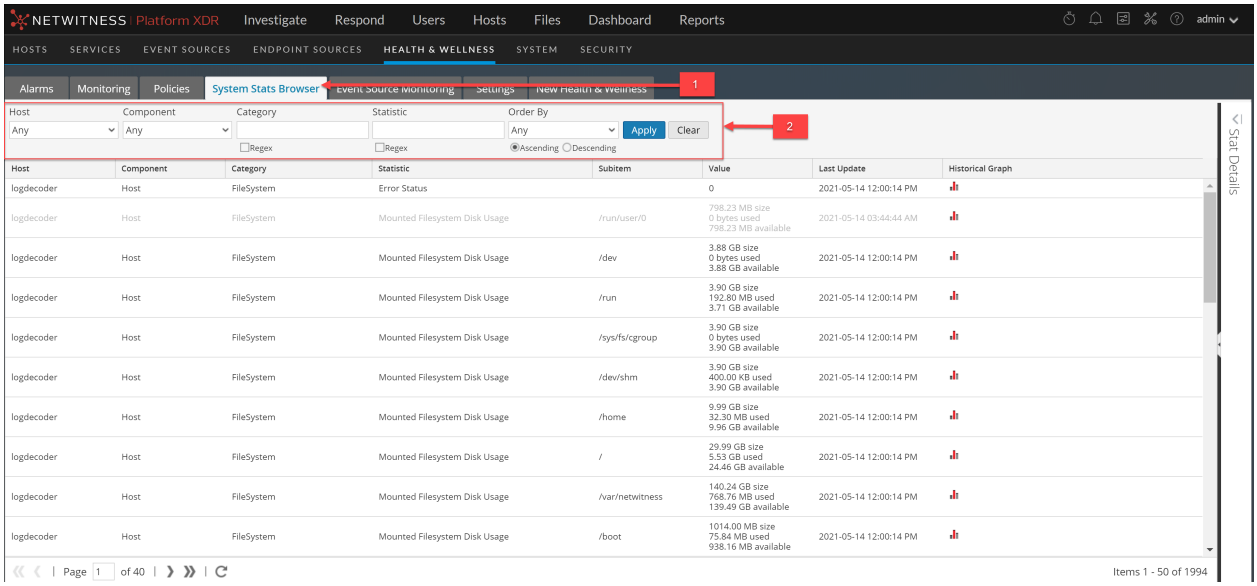
Related Topics

Monitor Service Statistics

Filter System Statistics

Quick Look

The System Stats Browser view is displayed.



1 Displays System Stats Browser View

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

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

Filters

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

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

Commands

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

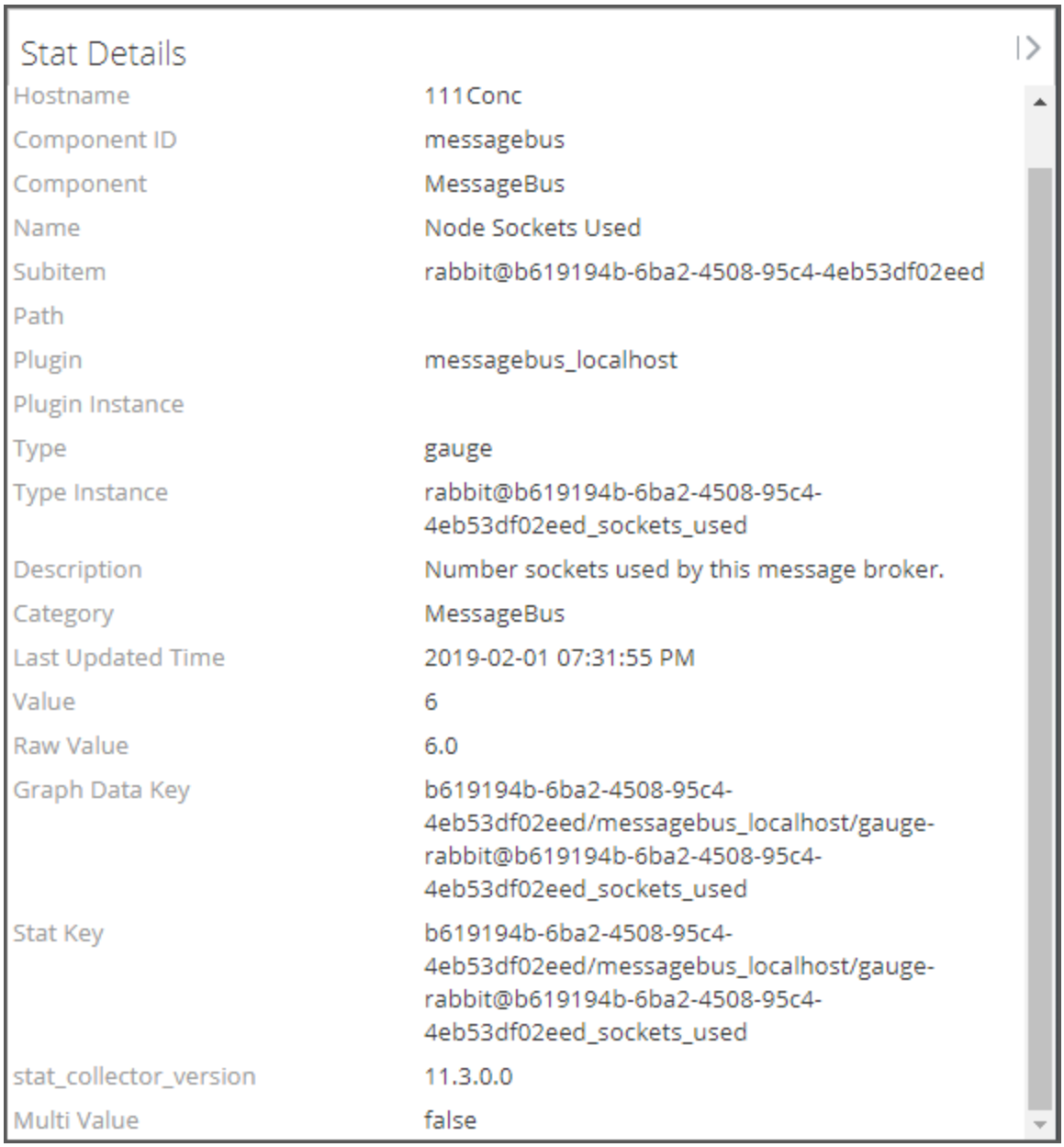
System Stats View Display

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
Hostname
111Conc
Component ID
messagebus
Component
MessageBus
Name
Node Sockets Used
Subitem
rabbit@b619194b-6ba2-4508-95c4-4eb53df02eed
Path
Plugin
messagebus_localhost
Plugin Instance
Type
gauge
Type Instance
rabbit@b619194b-6ba2-4508-95c4-4eb53df02eed_sockets_used
Description
Number sockets used by this message broker.
Category
MessageBus
Last Updated Time
2019-02-01 07:31:55 PM
Value
6
Raw Value
6.0
Graph Data Key
b619194b-6ba2-4508-95c4-4eb53df02eed/messagebus_localhost/gauge-rabbit@b619194b-6ba2-4508-95c4-4eb53df02eed_sockets_used
Stat Key
b619194b-6ba2-4508-95c4-4eb53df02eed/messagebus_localhost/gauge-rabbit@b619194b-6ba2-4508-95c4-4eb53df02eed_sockets_used
stat_collector_version
11.3.0.0
Multi Value
false

New Health & Wellness Tab

In New Health & Wellness tab, you can filter alerts (monitors) and add the notifications which sends a notification message when an alert is triggered, suppress the notification for a time period and pivot to New Health and Wellness dashboards.

To access this view:

1. Go to **(Admin) > Health & Wellness**.
2. Click the **New Health & Wellness** tab.

The figure depicts the New Health & Wellness view.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Manage Notification	Manage Notification and Suppression
Administrator	Manage Suppression	Manage Notification and Suppression

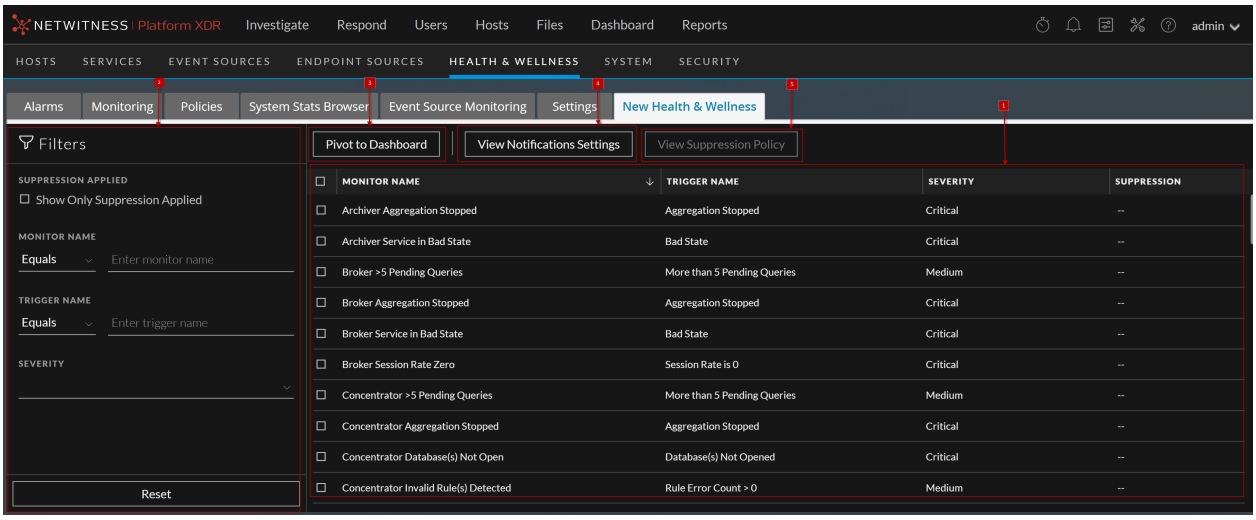
Related Topics

Monitoring through Dashboards

Monitoring through Alerts

Managing Notifications

Quick Look



1 **Notification Panel**: You can view the list of alerts (monitors) along with the trigger name, severity and suppression.

Monitor Name - Name of the monitor.

	Trigger Name - Name of the trigger. **Severity** - Severity assigned to the alert. The options are Critical, High, Medium, and Low. **Suppression** - Indicates whether suppression policy is applied or not. Green tick indicates suppression policy is applied.
2	**Filters Alerts**. You can filter alerts on Suppression Applied, Monitor Name, Trigger Name, and Severity. To reset filters, click **Reset**.
3	**Pivot to Dashboard**. You can view New Health and Wellness Dashboards. For more information, see Accessing New Health and Wellness Dashboards.
4	**View Notification Settings**. You can define notification settings which sends a notification message when an alert is triggered. For more information, see Adding Alert Notifications.
5	**View Suppression Policy**. You can suppress notifications for a time period by specifying a suppression policy. For more information, see Suppressing Notifications.

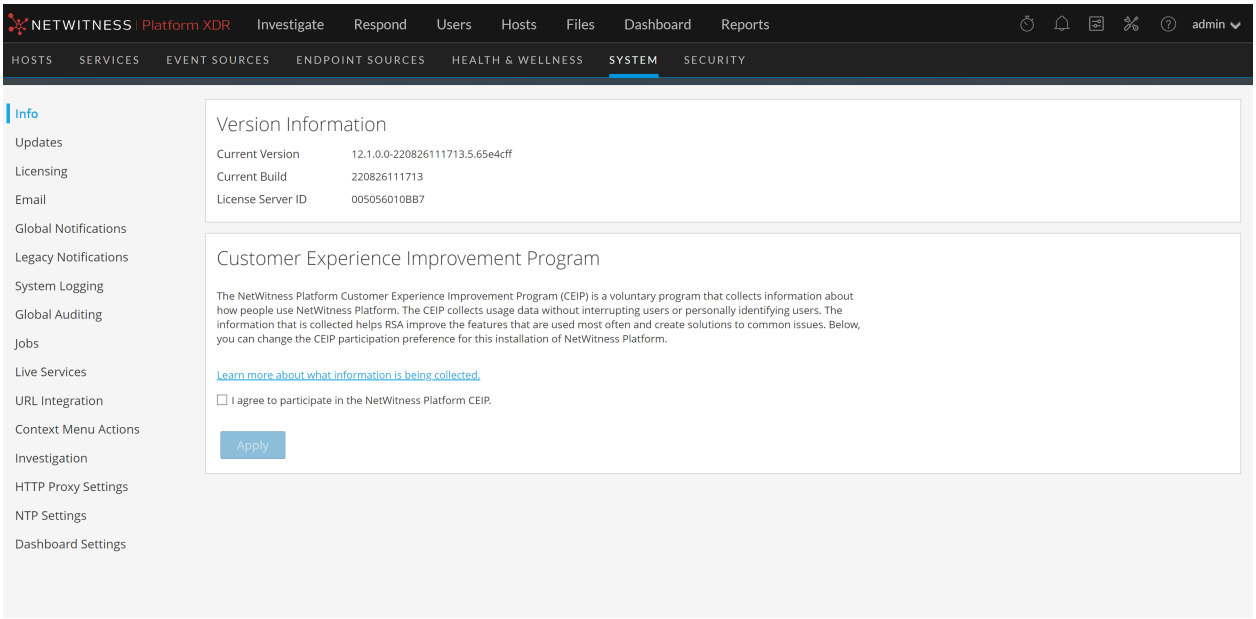
System View - System Info Panel

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 is available in the Notifications tray, click **View**.



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

Name	Description
Current Version	Displays the version of NetWitness 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

Name	Description
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 NetWitness. • 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 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?

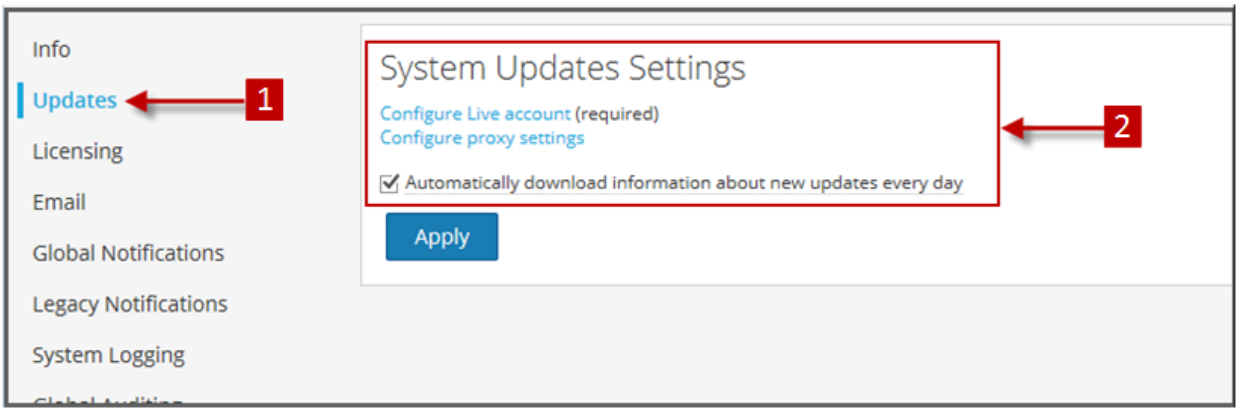
Role	I want to ...	Show me how
Administrator	Automatically download updates	Enable automatic synchronization with the NetWitness update repository.

Related Topics

Manage NetWitness Platform Updates

Quick Look

The System Updates Settings panel is displayed.



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

Features

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

Feature	Description
Configure Live account	Displays the **(Admin)** > **System** > **Live Services** panel in which you can configure your Live Account credentials if they are not configured.
Configure proxy settings	Displays the **(Admin)** > **System** > **HTTP Proxy Settings** panel in which you can configure an HTTP proxy if it is not configured.
Automatically download information about new updates every day	Select to enable automatic synchronization with the NetWitness 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 NetWitness Settings 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. 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?

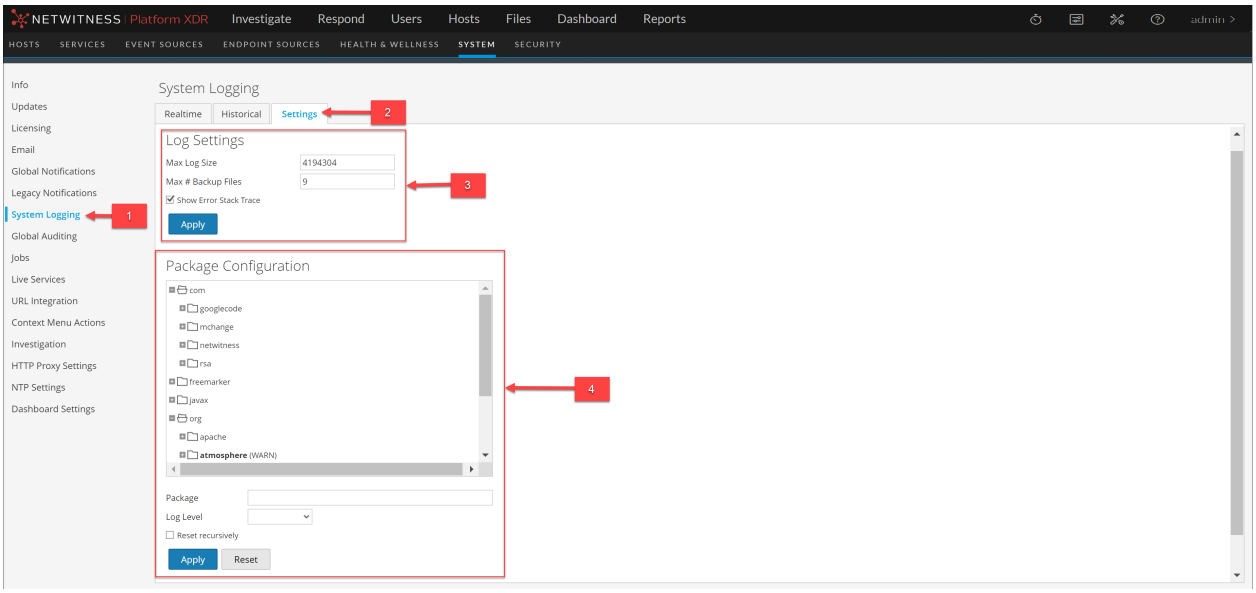
Role	I want to ...	Show me how
Administrator	Configure the size of the Log files	See the "Configure Log File Settings" topic in the *System Configuration Guide*

Related Topics

System Logging - Historical Tab

System Logging - Realtime Tab

Quick Look



1 Displays System Logging Panel
2 Displays Settings Tab
3 Configure Log Settings
4 Configure Packages

Features

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

Log Settings

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

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

Feature	Description
Package tree	Contains all the packages used within NetWitness. 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	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	Resets the log recursively.

Feature	Description
Apply	Puts settings into effect immediately for all future logs.
Reset	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 log 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	Display System and Service Logs

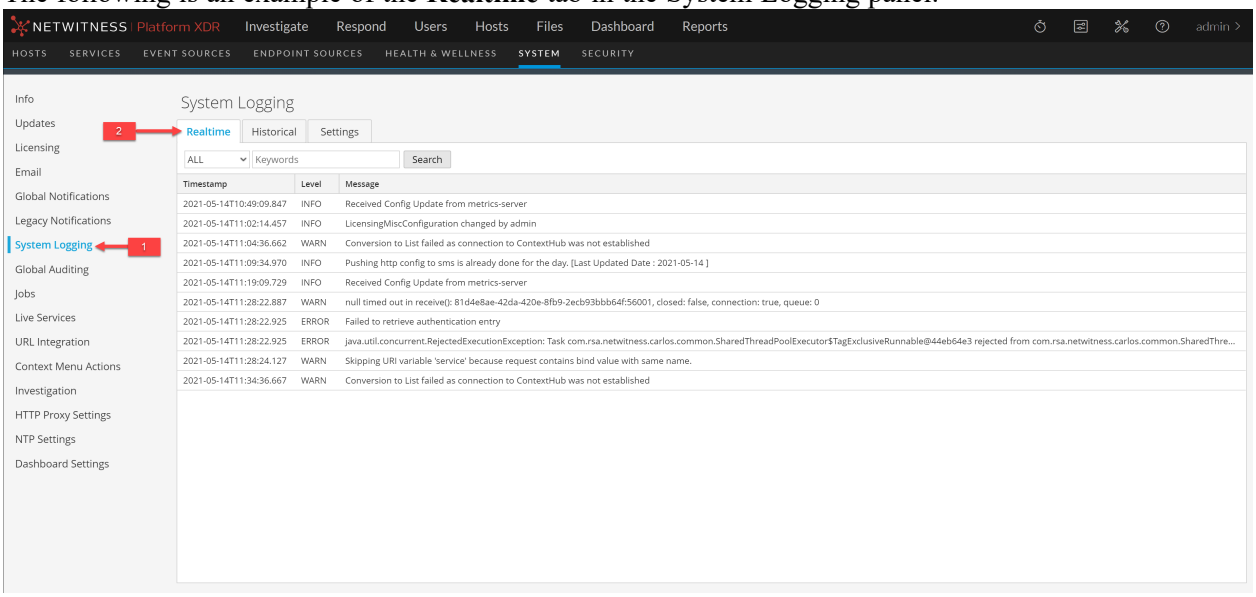
Related Topics

System Logging - Settings View

System Logging - Historical Tab

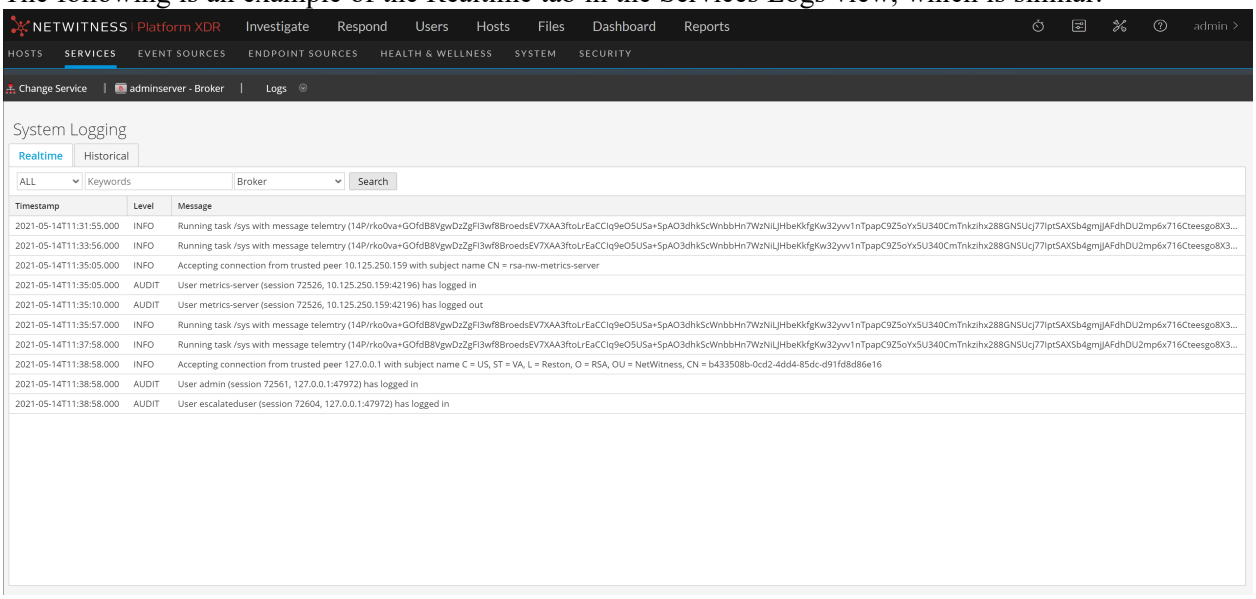
Quick Look

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



1 Displays System Logging Panel
2 Displays Realtime Tab

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



Features

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

Toolbar

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

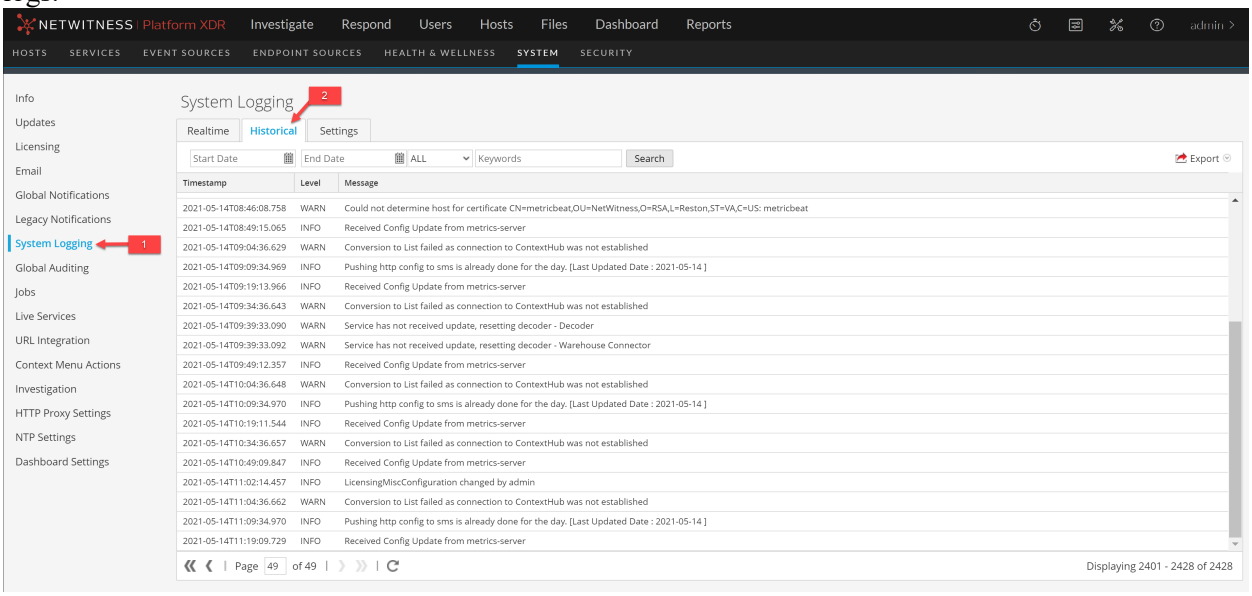
Related Topics

System Logging - Realtime Tab

System Logging - Settings View

Quick Look

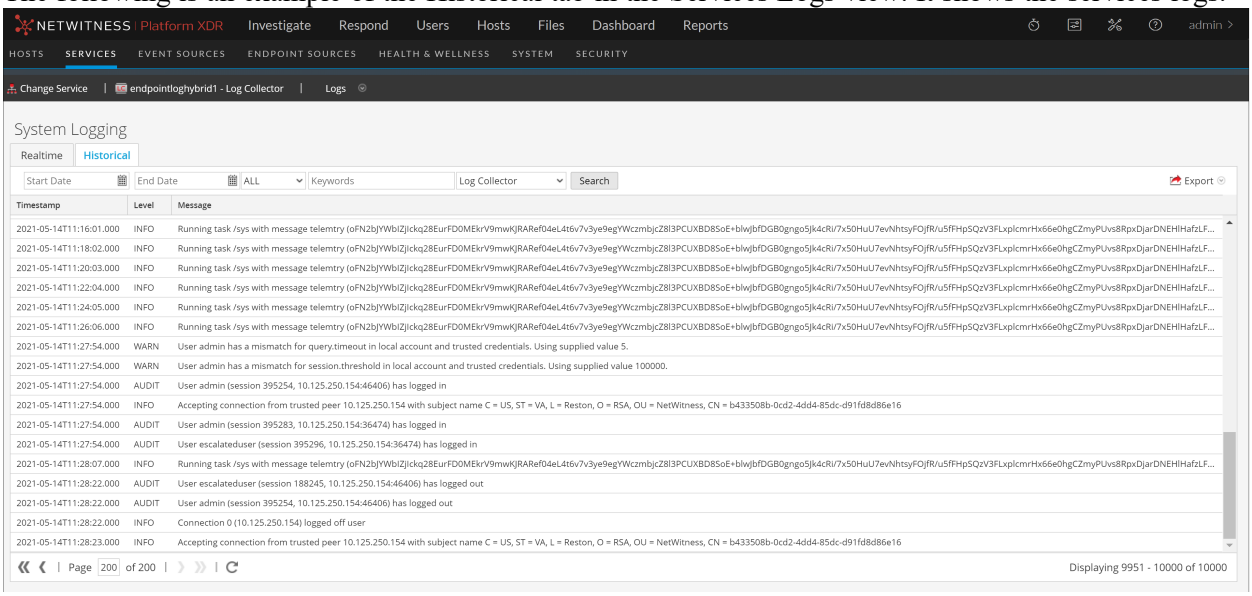
The following is an example of the **Historical** tab in the System Logging panel. It shows the NetWitness logs.



1 Displays System Logging Tab

2 Displays Historical Tab

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



Features

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

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

Feature	Description
Export	Click to export the currently viewed grid entries to a text file. You can select either comma-separated or tab-separated format for the entries in the file.

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

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

Search Log Entries

To search the results shown in the Historical tab:

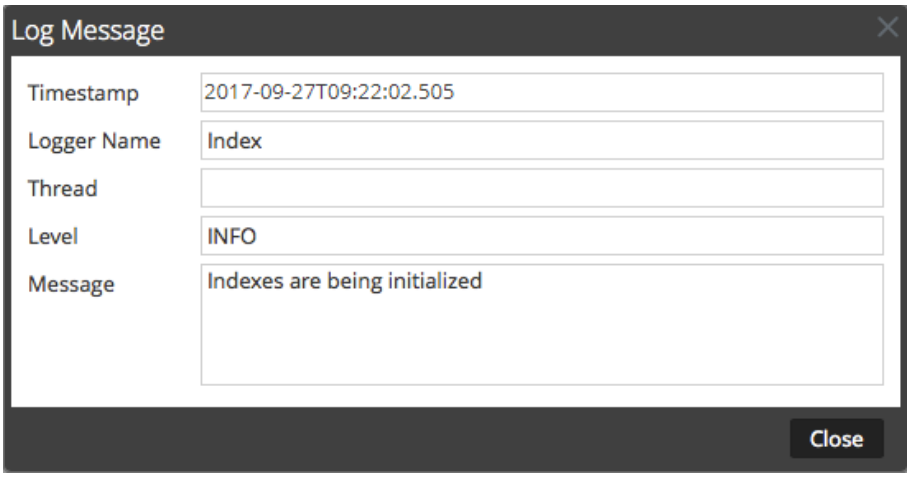
1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both.
3. (Optional) For service logs, select the **Service**: host or service.
4. Click **Search**.
  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

Show Details of a Log Entry

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

1. Double-click a log entry.

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



2. When finished viewing, click **Close**.

Page Through the Entries

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

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

Export

To export the logs in the current view:

Click **Export**, and select one of the drop-down options, **CSV Format** or **Tab Delimited**.
The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a NetWitness 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`.