

RSA | Security Analytics

System Maintenance Guide
for Version 10.6.5

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

November 2018

Contents

Security Analytics System Maintenance	11
Introduction	11
Best Practices	12
Safeguarding Assets with RSA Supplied Policies	12
Safeguarding Assets with Policies Based on Your Environment	12
Creating Rules and Notifications Judiciously	12
Troubleshooting Issues	12
Activate or Deactivate FIPS	13
Important Notes on FIPS	13
Activate, Verify or Deactivate FIPS Using BSAFE	14
Activate FIPS Using BSAFE for the Security Analytics Application Host	14
Activate FIPS Using BSAFE for Services	15
Verify That FIPS Is Activated for Services using BSAFE	16
Verify That FIPS Is Activated for the Reporting Engine on the Application Host	17
Verify that FIPS is Activated for Event Stream Analysis	17
Verify That FIPS Is Activated for Malware Analysis	18
Verify that FIPS Is Activated for Incident Management	18
Deactivate FIPS Using BSAFE for the Security AnalyticsApplication Host	18
Deactivate FIPS Using BSAFE for Services	18
Back Up and Restore Data for Hosts and Services	21
Change IP Address or Hostname of a Host	23
Introduction	23
Prerequisites	23
Syntax	23
Procedure	24
DISA STIG Hardening Guide	25
Introduction	25
How STIG Limits Account Access	25
STIG Compliant Passwords	25

- Procedures26
 - Configure STIG Hardening for 10.6 Updated from Earlier Version26
 - Apply the STIG Hardening Script27
 - (Conditional) Post-STIG Application Task - If You Use Malware Analysis, Update SELinux Parameter28
 - Configure STIG Hardening for New 10.6 Installation28
 - (Conditional) Post-STIG Application Task - If You Use Malware Analysis, Update SELinux Parameter30
 - Generate the OpenSCAP Report30
 - Sample Report31
 - Report Fields31
 - Create the OpenSCAP Report33
 - Create Report in HTML Only33
 - Create Report in XML Only33
 - Create Report in Both XML and HTML34
- Exceptions to STIG Compliance34
 - Key to Elements in Exception Descriptions35
 - Exception Descriptions36
 - Not a Finding54
 - Rules to Be Supported in Future Release85
- Manage Security Analytics Updates94**
 - Software Update Process94
 - Apply Software Version Updates from Hosts View96
 - Populate Local Update Repository96
 - Review Version and License Status99
 - Procedure99
- Monitor Health and Wellness of Security Analytics100**
 - Manage Policies100
 - Procedures102
 - Include the Default Email Subject Line117

Monitor Alarms	119
Monitor Event Sources	120
Configure Event Source Monitoring	121
Configure and Enable Event Monitoring	121
Decommission Event Source Monitoring	123
Filter Event Sources	124
Create Historical Graph of Events Collected for an Event Source	125
Monitor Health and Wellness Using SNMP Alerts	126
Procedures	127
Monitor Hosts and Services	129
Procedure	129
Filter Hosts and Services in the Monitoring View	130
Monitor Host Details	132
Monitor Service Details	133
Monitor Service Statistics	136
Procedure	136
Add Statistics to a Gauge or Chart	137
Create a Gauge for a Statistic	137
Create a Timeline Chart for a Statistic	138
Search for a Statistic in the Chart Stats Tray	139
Edit Properties of Statistics Gauges	140
Edit Properties of a Gauge	141
Add Stats to the Gauges Section	142
Edit Properties of Timeline Charts	142
Edit Properties of a Timeline	143
Edit Properties of a Historical Timeline	143
Add Stats to Timeline Charts	144
Monitor System Statistics	144
Filter System Statistics	145
Create Historical Graph of System Statistics	147

- Troubleshooting Health & Wellness 149
 - Issues Common to All Hosts and Services 149
 - Issues Identified by Messages in the Interface or Log Files 149
 - Issues Not Identified by the User Interface or Logs 154
- Display System and Service Logs 156**
 - Procedures 156
 - View System Logs 156
 - Display Service Logs 156
 - Filter Log Entries 157
 - Show Details of a Log Entry 157
 - Access Reporting Engine Log File 158
 - All Log Files 158
 - Upstart Logs 158
 - Search and Export Historical Logs 158
 - Procedures 159
- Maintain Queries Using URL Integration 162**
 - Procedures 163
 - Edit a Query 163
 - Delete a Query 164
 - Clear All Queries 164
 - Use a Query in a URI 164
 - Examples 165
- Security Analytics System Maintenance Checklist 166**
 - Audience 166
 - All Host Types Health Checks 166
 - Checks for all Host Types Using the Security Analytics UI 166
 - Checks for All Host Types Using SSH-Session/ CLI 167
 - Security Analytics Head Server Health Checks 170
 - Head Server checks using the Security Analytics UI 170
 - Head Server Checks Using SSH-Session/ CLI 170
 - Concentrator Health Checks 171
 - Indexes 171
 - NWDatabase Configuration Verification 172
 - Concentrator Health Checks using the Security AnalyticsUI 173
 - Concentrator Checks Using SSH-Session/ CLI 175

Event Stream Analysis (ESA) Health Checks	176
ESA checks using the Security Analytics UI	176
ESA Checks Using SSH-Session/ CLI	179
Log Collector Health Checks	179
Log Collector checks using the Security Analytics UI	180
Log Collector Checks Using SSH-Session/ CLI	181
Log Decoder Health Checks	181
Log Decoder checks using the Security Analytics UI and Explore/REST	181
Log Decoder Checks Using SSH-Session/ CLI	183
Archiver Health Checks	183
Archiver checks using the Security Analytics UI	183
Packet Decoder Health Checks	184
Packet Decoder checks using the Security Analytics UI	184
Packet Decoder Checks Using SSH-Session/ CLI	185
Log Locations	186
Supported Browsers	187
Task Details	187
Check Services	187
System Log Maintenance	187
Monitor Reporting Engine	188
Malware Analysis Colo Service Failure	188
RabbitMQ Service Report	188
Packet Retention Data Management Script	189
Meta Retention Data Management Script	189
Push Correct Versions of Custom Index Files to Hosts	190
Verify Custom Feeds	190
Validate the List of Enabled Parsers on Decoders	190
Troubleshoot Security Analytics	192
Debugging Information	192
Security Analytics Log Files	192
Files of Interest	193
Error Notification	197
Procedure	198
Miscellaneous Tips	198
Harden the Admin Account	198
Audit Log Messages	198

NwConsole for Health & Wellness	198
Thick Client Error: remote content device entry not found	199
View Example Parsers	199
Harden the Security Analytics Admin Account	199
Upgrade Issues	199
Configure WinRM Event Sources	199
NwLogPlayer	199
Usage	200
Troubleshoot Feeds	201
Overview	201
Details	201
How it Works	201
Feed File	202
Troubleshooting	202
ESMReader	205
ESMAggregator	206
References	209
Health and Wellness	209
Alarms View	210
Alarms List	211
Alarm Details Panel	212
Event Source Monitoring View	212
Filters	213
Commands	214
Event Source Stats view display	214
Health and Wellness Historical Graph Views	215
Overview	215
Features	216
Zoom In Function 1 and 2	217
Zoom In Function 3	218

Parameters	219
Zoom in function 1 and 2:	220
Zoom in function 3:	220
Health and Wellness Settings Tab - Archiver	221
Health and Wellness Settings Tab - Event Sources	224
Event Source Monitoring Panel	225
Decommission Panel	225
Add/Edit Source Monitor Dialog	226
Decommission Dialog	228
Health and Wellness Settings Tab - Warehouse Connector	228
Monitoring View	230
Groups Panel	231
Hosts Panel	231
Details Section	233
Details Section	235
Details Section	236
Details Section	237
Details Section	240
System Info Section	242
Tabs	243
Tabs	245
Details Section	247
Details Section	249
Details Section	250
Features	251
Details Section	251

Policies View	251
Groups dialog	255
Rules Dialog	256
Threshold Operators	258
Health & Wellness Default SMTP Template	259
Alarms Template	260
Security Analytics Out-of-the-Box Policies	260
System Stats Browser View	270
System Info Panel	273
Introduction	273
Features	274
System Updates Panel - Manual Updates Tab	275
Introduction	275
Features	276
System Updates Panel - Repository Space Management Dialog	277
Introduction	277
Features	278
System Updates Panel - Settings Tab	279
Introduction	279
Features	279

Security Analytics System Maintenance

Introduction

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

The following topics show the different system maintenance tasks available to you:

- [Activate or Deactivate FIPS](#)
- [Back Up and Restore Data for Hosts and Services](#)
- [Change IP Address or Hostname of a Host](#)
- [DISA STIG Hardening Guide](#)
- [Manage Security Analytics Updates](#)
- [Monitor Health and Wellness of Security Analytics](#)
- [Security Analytics System Maintenance Checklist](#)
- [Troubleshoot Security Analytics](#)
- [References](#)

Best Practices

Safeguarding Assets with RSA Supplied Policies

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

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

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

Safeguarding Assets with Policies Based on Your Environment

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

Creating Rules and Notifications Judiciously

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

Troubleshooting Issues

RSA recommends that you review "Troubleshooting Health & Wellness" in "Monitor Health and Wellness of Security Analytics" when you receive error messages in the user interface and log files from hosts and services.

Activate or Deactivate FIPS

This topic describes how to activate and deactivate Federal Information Processing Standards (FIPS).

Important Notes on FIPS

When you run the FIPS Enable or Disable script on the Security Analytics Application host, it enables or disables all the services using the BSAFE security library that are running on the Security Analytics Application host, as well as all the connected hosts that use BSAFE security library.

When running Security Analytics in FIPS mode, there are the following requirements for private keys and certificates:

1. There are minimum key sizes for signing and authentication:
 - a. RSA, DSA: Greater than or equal to 2048-bit keys
 - b. ECDSA: Greater than or equal to 224-bit keys (FIPS 186-4 recommends particular EC curves)
2. There are minimum key sizes for verification (legacy use only):
 - a. RSA, DSA: Greater than or equal to 1024-bit keys
 - b. ECDSA: Greater than or equal to 160-bit keys
3. SHA-1 signatures can be verified, but not created.
4. SHA-256 signatures can be verified and created.

If FIPS is enabled, you must complete the following steps before you add an SFTP destination using SSH key-based access after the SSH keys are configured as described in the *Warehouse Connector Configuration Guide*.

1. SSH to the Warehouse Connector host.
2. Run the following commands:

```
cd /root/.ssh/  
mv id_dsa id_dsa.old  
openssl pkcs8 -topk8 -v2 des3 -in id_dsa.old -out id_dsa
```

You are prompted for the old and new pass phrase.

3. Enter the old and new pass phrase.

4. Run the following command:

```
chmod 600 id_dsa
```

The following sections tell you how to activate, deactivate, or verify FIPS.

Activate, Verify or Deactivate FIPS Using BSAFE

This section tells you how to activate, verify, or deactivate FIPS using BSAFE for the Security Analytics Application host and all services that use the BSAFE security library.

Activate FIPS Using BSAFE for the Security Analytics Application Host

To activate FIPS for the Security Analytics Application host using the BSAFE security library:

1. SSH in to the Application host with root permissions.
2. Navigate to the `/etc/puppet/scripts` directory and run the following command:

```
./FIPSEnable.sh
```

The script ONLY runs on the Security Analytics Application host. The

`./FIPSEnable.sh` script:

- Activates FIPS on all the services using the BSAFE security library that are provisioned to the Security Analytics Application host.
- Restarts services on the Security Analytics Application host and all other hosts.

For example: Malware Analysis, Event Stream Analysis (ESA), and Security Analytics core hosts (Broker, Concentrator, Decoder and Log Decoder, and so on) are provisioned to the Security Analytics Application host. When you run the `./FIPSEnable.sh` script on the Security Analytics Application host, it activates FIPS for services (Reporting Engine and Incident Management) running on the Security Analytics Application host and instructs Context Hub, ESA, and services running on other hosts to run in FIPS mode.

After the script completes successfully, it automatically restarts services on the Security Analytics Application, ESA, and Malware hosts. Allow some time for the services to restart.

3. Reboot hosts.

RSA recommends that you reboot all the services using BSAFE that are connected to the Security Analytics Application host, starting with the non-Security Analytics Application hosts first. For example, if you have a Malware Analysis host and a Security Analytics Application host, reboot the Malware Analysis host first and then reboot the Security Analytics Application host.



Note: To activate or deactivate FIPS for the IPDB Extractor and Broker services that are running on the Security Analytics Application host, use the scripts `./NwFIPSEnable.sh` or `./NwFIPSDisable.sh`.

Activate FIPS Using BSAFE for Services

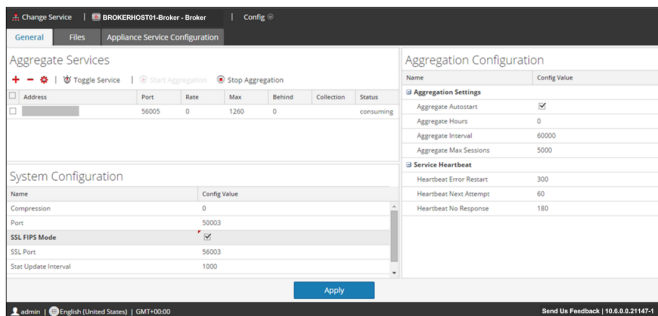
Use these steps to activate FIPS using BSAFE on each service host for the following services:

- Broker
- Concentrator
- Decoder
- Log Decoder
- Warehouse Connector
- IPDB Extractor
- Log Collector(both Local and Remote Collectors)
- Archiver
- Workbench

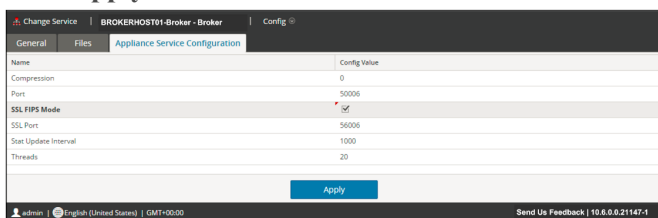
To activate FIPS using BSAFE for these services, on each service host:

1. SSH into the Application services host with root permissions.
2. Navigate to the `/etc/puppet/scripts` directory and run the following command:
`./NwFIPSEnable.sh`
3. Log on to Security Analytics and go to **Administration > Services**.
4. Select the service.
The services that you need to select are Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, IPDB Extractor, Log Collector (both Local and Remote Collectors), Archiver, and Workbench.
5. Click   under **Actions** and select **View > Config**.

- In the **General** tab, select the **SSL FIPS Mode** checkbox in the **System Configuration** panel and click **Apply**.



- In the **Appliance Service Configuration** tab, select the **SSL FIPS Mode** checkbox and click **Apply**.



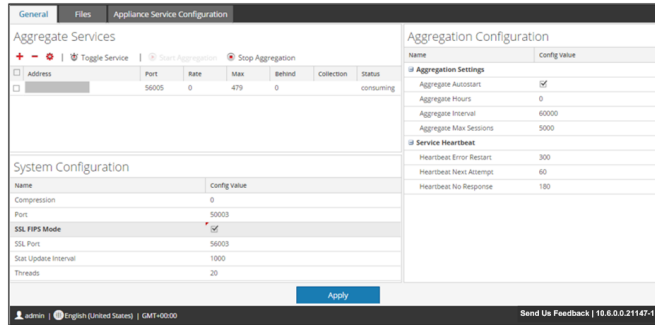
- Reboot the host. The hosts that you need to reboot are the Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, IPDB Extractor, Log Collector (both Local and Remote Collectors), Archiver, and Workbench services.

Verify That FIPS Is Activated for Services using BSAFE

To verify that FIPS is activated for services using the BSAFE security library:


- Log on to Security Analytics and go to **Administration > Services**.
- Select the service. The services that you need to select are the Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, IPDB Extractor, Log Collector (both Local and Remote Collectors), Archiver, and Workbench.
- Under **Actions**, select **View > Config**.
The **General** tab of the **Configuration** view is displayed.
- In the **System Configuration** panel, make sure that the **SSL FIPS Mode** parameter is

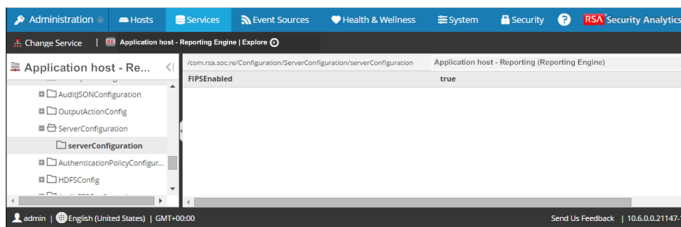
checked.



Verify That FIPS Is Activated for the Reporting Engine on the Application Host


To verify that FIPS using BSAFE is activated for the Reporting Engine:

1. Log onto Security Analytics and go to **Administration > Services**.
2. Select the Reporting Engine service.
3. Click  under **Actions** and select **View > Explore**.
4. Go to **com.rsa.soc.re > Configuration > ServerConfiguration > serverConfiguration**.
5. Make sure that the **FIPSEnabled** parameter is set to **true**.

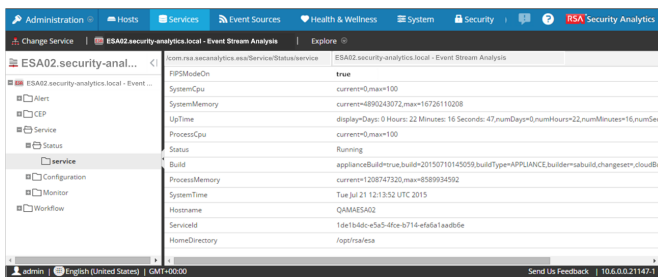


Verify that FIPS is Activated for Event Stream Analysis

To verify that FIPS using BSAFE is activated for Event Stream Analysis (ESA):

1. Log on to Security Analytics and go to **Administration > Services**.
2. Select the ESA service.
3. Click  under **Actions** and select **View > Explore**.
4. Go to **Service > Status > service**.

5. Make sure that the **FIPSMODEON** parameter is set to **true**.



Verify That FIPS Is Activated for Malware Analysis

To verify that FIPS using BSAFE is activated for Malware Analysis, run the following command string:

```
cat /etc/alternatives/jre/lib/security/java.security | grep FIPS
```

The command string returns the following output when FIPS is activated for Malware Analysis:

```
com.rsa.cryptoj.fips140initialmode=FIPS140_MODE
```

Verify that FIPS Is Activated for Incident Management

To verify that FIPS is activated for Incident Management, run the following command string:

```
cat /opt/rsa/im/logs/im.log | grep FIPS
```

The command string returns the following output when FIPS is activated for Incident Management:

```
[WrapperSimpleAppMain] INFO com.rsa.smc.im.ServiceInitializer -  
Running in FIPS mode
```

Deactivate FIPS Using BSAFE for the Security AnalyticsApplication Host

To deactivate FIPS using BSAFE for the Security Analytics Application host:

1. SSH into the Security Analytics Application host with root permissions.
2. Navigate to the `/etc/puppet/scripts` directory and run the following command:


```
./FIPSEnable.sh false
```
3. Reboot the host. RSA recommends that you reboot all hosts that are connected to the Application host starting with the non-Application hosts first. For example, if you have a Malware Analysis host and a Security Analytics Application host, reboot the Malware Analysis host first and then reboot the Security Analytics Application host.

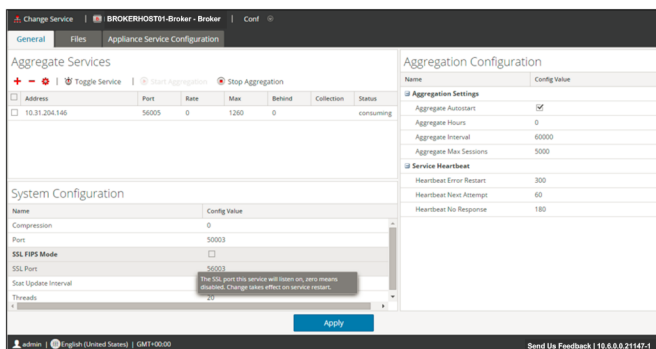
Deactivate FIPS Using BSAFE for Services

Use these steps to deactivate FIPS using BSAFE on each service host for the following services:

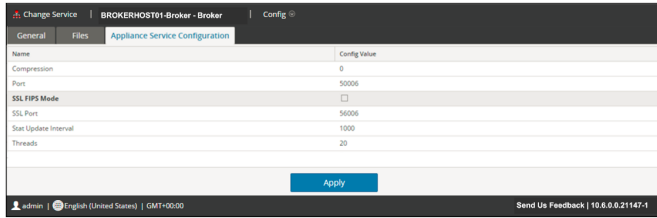
- Broker
- Concentrator
- Decoder
- Log Decoder
- Warehouse Connector
- IPDB Extractor
- Log Collector(both Local and Remote Collectors)
- Archiver
- Workbench

To deactivate FIPS using BSAFE for these services, on each service host:

1. SSH into the services Application host with root permissions.
2. Navigate to the `/etc/puppet/scripts` directory and run the following command:
`./NwFIPSDisable.sh`
3. Log on to Security Analytics and go to **Administration > Services**.
4. Select the service.
 The services that you need to select are Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, IPDB Extractor, Log Collector (both Local and Remote Collectors), Archiver, and Workbench.
5. Click  under **Actions** and select **View > Config**.
6. In the **General** tab, deselect the **SSL FIPS Mode** checkbox in the **System Configuration** panel and click **Apply**.



7. In the **Appliance Service Configuration** tab, deselect the **SSL FIPS Mode** checkbox and click **Apply**.



8. Reboot the host. The hosts that you need to reboot are the Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, IPDB Extractor, Log Collector (both Local and Remote Collectors), Archiver, and Workbench services.

Back Up and Restore Data for Hosts and Services

You can use the **nw-backup.sh** and the **nw-restore.sh** scripts to back up and restore configuration data from the Security Analytics server and Security Analytics hosts for versions 10.6.2.0 and later. The scripts are specifically for restoring systems that fail. You can use the backup and restore scripts for RMAs, hardware refreshes, and general backup and restore requirements. You can download the "RSA Configuration Backup and Restore Scripts" zip file and the documentation from RSA Link:

- Script zip file: <https://community.rsa.com/docs/DOC-79456>
- Documentation: <https://community.rsa.com/docs/DOC-79458>

Caution: When you are ready to restore data that has been backed up, you must work with the RSA Professional Services team or Customer Support. Do not use the restore script without assistance. For information about how to contact Customer Support, go to the "Contact Customer Support" page in RSA Link (<https://community.rsa.com/docs/DOC-1294>).

Caution: The backup script (**nw-backup.sh**) only backs up configuration files that were created by using the Security Analytics console or user interface. RSA recommends that you test the restore process before you delete the original files.

Note: The backup and restore scripts do not support backup and restore for STIG- or FIPS-hardened hosts.

The following hosts can be backed up and restored:

- **Security Analytics Server** (may include Malware Analysis, Incident Management, Health and Wellness, IPDB Extractor, and Reporting Engine)
- **Malware Analysis** (standalone)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and IM database)
- **Concentrator**
- **Log Decoder** (including Local Log Collector and Warehouse Connector, if installed)
- **Log Hybrid**
- **Packet Decoder** (including Warehouse Connector, if installed)
- **Packet Hybrid**

- **Remote Log Collector (VLC)**
- **IPDB Extractor (Stand-Alone)**
- **Warehouse Connector (Stand-Alone)**

You can back up several systems in a single execution of the backup script, but you must restore them one system at a time.

Change IP Address or Hostname of a Host

Introduction

You use the `changePuppetMaster.py` Python script to change the IP Address or hostname of the Security Analytics Server Host or any other host in your Security Analytics deployment. You run this script from the command line on the Security Analytics Server Host.

Prerequisites

You need to apply the 10.6 update package before you can run the `changePuppetMaster.py` script. Verify that the following files exist on the Security Analytics Server Host before you attempt to run the `changePuppetMaster.py` script.

- `/etc/init.d/sa_addrd`
- `/etc/rc.d/rc.local`

Syntax

The following table describes the `changePuppetMaster.py` Python script options.

Options	Description
<code>-h</code> or <code>--help</code>	Displays the following help message and exits.
<code>-a ADDRESS</code> , <code>--address=ADDRESS</code>	Enter the [non-]SA node's [current IP address and] new IP address
<code>-n NAME</code> , <code>--name=NAME</code>	Enter the [non-]SA node's [current hostname and] new hostname
	<code>[root@someSAserver sysSetRPC]#</code>
<code>-a</code> or <code>--address</code>	<p>If you want to change the IP address for:</p> <ul style="list-style-type: none"> • Security Analytics Server Host, specify a single IP address that replaces the existing Security Analytics Server Host IP Address with this option. For example: <code>-a ip-address</code> • Any host other than the Security Analytics Server Host, specify two IP addresses with this option. The first address identifies the current address and the second address identifies the replacement address. For example: <code>-a ip-address ip-address</code>

Options	Description
<code>-n</code> or <code>--name</code>	<p>If you want to change the hostname for:</p> <ul style="list-style-type: none"> • Security Analytics Server Host, specify a single hostname that replaces the existing Security Analytics Server Host hostname with this option. For example: <code>-n hostname</code> • Any host other than the Security Analytics Server Host, specify two hostnames with this option. The first name identifies the current name and the second name identifies the replacement name. For example: <code>-n hostname hostname</code>

Procedure

Complete the following procedure to change the IP address or hostname of a host.

1. SSH to the Security Analytics Server host.
2. Go to the `/etc/puppet/scripts/sysSetRPC` directory.
`cd /etc/puppet/scripts/sysSetRPC`
3. Specify one of the following command strings to change a host IP address or hostname.

Note: You must enter a case-sensitive *hostname* (for `current-hostname` and `newhostname`) that matches the corresponding database record. See the case-sensitive hostname displayed in the Hosts view for the case-sensitive `current-hostname`.

- To change the Security Analytics Server Host IP address:
`python changePuppetMaster.py -a new-ip-address`
- To change the Security Analytics Server Host hostname:
`python changePuppetMaster.py -n newhostname`
- To change any other host IP address:
`python changePuppetMaster.py -a current-ip-address new-ip-address`
- To change any other host hostname:
`python changePuppetMaster.py -n current-hostname new-hostname`

DISA STIG Hardening Guide

This guide tells you:

- What you need to apply STIG Hardening to Security Analytics.
- How to configure STIG Hardening.
- What the OpenSCAP report is and how you generate it.
- What exceptions were discovered in 10.6 and why they occurred.

Note: Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening is fully supported in Security Analytics v10.5.0.1. Security Analytics v10.5 only supported DISA STIG hardening if you applied DISA STIG prior to 10.5.

Introduction

Before you configure your Security Analytics deployment for STIG hardening, you need to know how:

- STIG hardening helps you limit account access.
- To define STIG compliant passwords.

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.

Caution: After you run the STIG hardening rpm, the host is converted to Coordinated Universal Time (UTC).

STIG Compliant Passwords

To be STIG compliant, your organization must implement policies that ensure strong passwords. Your organization:

- Must change user passwords at least every 60 days.
- Must not reuse the last 24 passwords when you reset them.
- Must use SHA-2 family of algorithms or FIPS 140-2 approved algorithms.
- Must employ cryptographic hashes for passwords for the SHA-2 family of algorithms or FIPS 140-2 approved successors. If your organization employs unapproved algorithms, this may result in weak password hashes that are more vulnerable to being compromised.

Each password:

- Must be 14 characters long.
- Must contain at least one of each of the following characters:
 - At least one lower case letter.
 - At least one upper case letter.
 - At least one number.
 - At least one other (non-alphanumeric) character.
- Must not have more than three consecutive characters.
- Must have at least five different characters different from the previous password.

The following password is an example of a STIG compliant password:

Ye@wap2ustavug

Procedures

Follow one of the following two STIG Hardening configuration procedures:

- Configure STIG hardening for a newly-installed Security Analytics 10.6 deployment.
- Configure STIG hardening if a Security Analytics deployment updated from an earlier version to 10.6.

You can also evaluate your environment against the Security Content Automation Protocol (SCAP) rules using the OpenSCAP report.

Configure STIG Hardening for 10.6 Updated from Earlier Version

These instructions describe how to configure Security Analytics hosts that were updated to 10.6 from an earlier version.

Read Before You Run the STIG Script

Please read the following caution statement before you run the STIG hardening script.

Caution: After you run the STIG hardening script, you cannot revert to an unhardened state without performing a build stick on the host. If you want to revert, you must re-image the host and you will lose all of your data. Contact Customer Care to get instructions on how to build stick the host.

Prerequisite

Make sure that the STIG rpm is installed with the CENTOS components required for STIG.

1. SSH to the host and submit the following command string to make sure that the STIG rpm is installed.

```
rpm -qa | grep aqueduct-stig
```

If you receive the following output, the STIG rpm is installed you do not need to complete step 2.

```
aqueduct-stig-10.6.0.0.xxxx-x.el6.noarch
```

2. If the STIG rpm is not installed (that is, no output was displayed in Step 1), use the following command string to install 10.6.0.0 STIG rpm.

```
yum install aqueduct-stig -y
```

Apply the STIG Hardening Script

Complete the following procedure to apply the STIG hardening to a host updated to 10.6.0 from an earlier version:

1. Log on to the host using a normal user account.

Caution: STIG blocks super user access to a host through SSH. You must log on using a normal user account. The STIG script (`Aqueduct-STIG.sh`) creates the `nwadmin` account when you run it logged on with the root password. The password for this account must be at least fourteen characters long and include numbers, letters, and at least one special character. You should change the passwords, including root, every 90 days to avoid expiration and lockout of these passwords. If you are completely locked out, you will need the root password to access the host in single user mode.

In addition, the script adds the `nwadmin` account to the `/etc/sudoers` file.

- a. Check for locks on the account:

```
pam_tally2 --user=<username>
```

- b. Unlock the account, if required:

```
pam_tally2 --user=<username> --reset
```

2. Run the superuser command. You have three options:
 - Run the `sudo <command>`.
 - Run `su` and provide the root password.
 - Run `sudo su` and provide your user password.You can add more user accounts to the `/etc/sudoers` file as needed.
3. Go to the `/opt/rsa/AqueductSTIG/` directory and run the STIG hardening script:
`./Aqueduct-STIG.sh`

Caution: After you run the STIG hardening script you must change all the passwords on the system, including the root password, using the superuser credentials. STIG also applies the SHA512 algorithm to all passwords. This means that when you change all the passwords, they must be STIG compliant and conform to the STIG complex password requirements.

The script prompts you to change `nwadmin` password.

4. Enter new password.
5. Change all the passwords on the system, including the root password, using the superuser credentials:
 - a. Log on to the host using the root credentials.
 - b. Change all the passwords on the system.
6. Restart the host.

(Conditional) Post-STIG Application Task - If You Use Malware Analysis, Update SELinux Parameter

If you use Security Analytics Malware Analysis, you must enable Malware Analysis to communicate with other Security Analytics services. To do this, update the `SELINUX` parameter in the `/etc/selinux/config` file to the following value.

```
SELINUX=disabled
```

Configure STIG Hardening for New 10.6 Installation

These instructions describe how to configure hosts in new 10.6 Security Analytics installations.

Read Before You Run the STIG Script

Please read the following caution statement before you run the STIG hardening script.

Caution: After you run the STIG hardening script, you cannot revert to an unhardened state without performing a build stick on the host. If you want to revert, you must re-image the host and you will lose all of your data. Contact Customer Care to get instructions on how to build stick the host.

Apply the STIG Hardening Script

Complete the following procedure to apply the STIG hardening to a new host:

1. Log on to the host using a normal user account.

Caution: STIG blocks super user access to a host through SSH. You must log on using a normal user account. The STIG script (`Aqueduct-STIG.sh`) creates the `nwadmin` account when you run it logged on with the root password. The password for this account must be at least fourteen characters long and include numbers, letters, and at least one special character. You should change the passwords, including root, every 90 days to avoid expiration and lockout of these passwords. If you are completely locked out, you will need the root password to access the host in single user mode.

In addition, the script adds the `nwadmin` account to the `/etc/sudoers` file.

- a. Check for locks on the account:

```
pam_tally2 --user=<username>
```

- b. Unlock the account, if required:

```
pam_tally2 --user=<username> --reset
```

2. Run the superuser command. You have three options:

- Run the `sudo <command>`.
- Run `su` and provide the root password.
- Run `sudo su` and provide your user password.

You can add more user accounts to the `/etc/sudoers` file as needed.

3. Go to the `/opt/rsa/AqueductSTIG/` directory and run the STIG hardening script:

```
./Aqueduct-STIG.sh
```

Caution: After you run the STIG hardening script you must change all the passwords on the system, including the root password, using the superuser credentials. STIG also applies the SHA512 algorithm to all passwords. This means that when you change all the passwords, they must be STIG compliant and conform to the STIG complex password requirements.

The script prompts you to change `nwadmin` password.

4. Enter new password.
5. Change all the passwords on the system, including the root password, using the superuser credentials:
 - a. Log on to the host using the root credentials.
 - b. Change all the passwords on the system.
6. Restart the host.

(Conditional) Post-STIG Application Task - If You Use Malware Analysis, Update SELinux Parameter

If you use Security Analytics Malware Analysis, you must enable Malware Analysis to communicate with other Security Analytics services. To do this, update the `SELINUX` parameter in the `/etc/selinux/config` file to the following value.

```
SELINUX=disabled
```

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-rhel6-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

For fresh installs, the OpenSCAP report is on the Image.

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			Addresses						
<ul style="list-style-type: none"> NWAPPLIANCE20809 			<ul style="list-style-type: none"> ██████████ ██████████ ██████████ ██████████ 						
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.

Section	Field	Description
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 Security Analytics 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 Security Analytics 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 commands:

```
mkdir -p /opt/rsa/openscap
```
3. Submit the following commands for report upgrades only:

```
sed -i -r -e "s/<platform.*//g" /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```
4. Submit the following commands:

```
oscap xccdf eval --profile "stig-rhel6-server-upstream" --report /tmp/`hostname`-ssg-results.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```
5. Open the report in your browser:

```
/tmp/hostname-ssg-results.html
```

Create Report in XML Only

To create an OpenSCAP report in xml only:

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

```
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-rhel6-xccdf.xml
```

4. Submit the following commands:

```
oscap xccdf eval --profile "stig-rhel6-server-upstream" --results /tmp/`hostname`-ssg-results.xml --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

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 commands:

```
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-rhel6-xccdf.xml
```

4. Submit the following commands:

```
oscap xccdf eval --profile "stig-rhel6-server-upstream" --results /opt/rsa/openscap/`hostname`-ssg-results.xml --report /opt/rsa/openscap/`hostname`-ssg-results.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

Exceptions to STIG Compliance

This topics contains:

- Rule exceptions with reasons for their non-compliance and workarounds if any.
- Rule exceptions that are "Not a Finding" which means that they do not apply to Security Analytics. RSA 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.

Severity

Category	
Category I	Findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. Category I weaknesses must be corrected before an Authorization to Operate (ATO) is granted.
Category II	Findings that have a potential to lead to unauthorized system access or activity. Category II findings can usually be mitigated and will not prevent an Authorization to Operate from being granted.
Category III	Recommendations that will improve IA posture but are not required for an authorization to operate.

Vulnerability ID

Vulnerability identification code assigned to exception by the **Unified Compliance Framework STIG Viewer** (<https://www.stigviewer.com/>).

STIG ID

Security Technical Implementation Guide (STIG) identification code.

Rule ID

Rule identification code.

NIST 800-53 SP 800-53

National Institute of **Standards and Technology (NIST 800-53) Special Publication 800-53 control list** (<https://www.stigviewer.com/controls/800-53>) information provided by the RedHat STIG Viewer.

CCI

DISA Control Correlation Identifier (<https://www.tenable.com/sc-dashboards/disa-control-correlation-identifier-cci-dashboard>).

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:

- **Not a Finding** - Exception does not apply to Security Analytics. RSA has verified that the system meets this requirement.
- **Customer Responsibility** - You are responsible to make sure the system meets this requirement.
- **Required Functionality** - Security Analytics does not meet this requirement.
- **Future Feature** - Security Analytics does not meet this requirement. RSA plans to fix this in a future release of Security Analytics.
- **Mitigation Steps Required** - Lists steps you can take to mitigate the exception.

Exception Descriptions

The following list contains 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.

CCE-26215-4

Severity	Category III
Vulnerability ID	V-38463
STIG ID	RHEL-06-000003
Rule ID	SV-50263r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366

Check	(For the IPDB Extractor only) Verify that <code>/var/log</code> directory on the the host has its own partition or logical volume at installation.
Comments	Customer Responsibility. If the <code>/var/log</code> directory on the the host does not have its own partition or logical volume, use the Logical Volume Manager (LVM) to migrate it to its own partition or logical volume.

CCE-26328-5

Severity	Category III
Vulnerability ID	V-38656
STIG ID	RHEL-06-000272
Rule ID	SV-50457r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	(For the IPDB Extractor on Malware Analysis and SA hosts only) Verify that Client Service Message Block (SMB) packet signing exists on the host if you use using an <code>smbclient</code> . SMB is is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.
Comments	Customer Responsibility. To require samba clients running <code>smbclient</code> to use packet signing, add the following to the <code>[global]</code> section of the Samba configuration file, <code>/etc/samba/smb.conf</code> : <code>client signing = mandatory.</code>

CCE-26435-8

Severity	Category III
Vulnerability ID	V-38455
STIG ID	RHEL-06-000001
Rule ID	SV-50255r1_rule

NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	(For IPDB Extractor only) Verify that /tmp is located on a separate partition.
Comments	Customer Responsibility. Verify that the <code>tmp</code> directory has its own partition or logical volume at installation or migrate it using the Logical Volume Manager (LVM).

CCE-26436-6

Severity	Category III
Vulnerability ID	V-38467
STIG ID	RHEL-06-000004
Rule ID	SV-50267r1_rul
NIST 800-53	NIST SP 800-53 :: AU-4 NIST SP 800-53A :: AU-4.1 (i)
CCI	CCI-000137
Check	Verify that <code>/var/log/audit</code> directory is located on a separate partition on the host.
Comments	Required Functionality. The Security Analytics architecture does not allow the <code>/var/log/audit</code> directory to reside on a separate partition.

CCE-26557-9

Severity	Category III
Vulnerability ID	V-38473
STIG ID	RHEL-06-000007
Rule ID	SV-50273r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b

CCI	CCI-000366
Check	(For IPDB Extractor only) Verify that <code>/home</code> (user home directory) is located on a separate partition.
Comments	Customer Responsibility. If you store user home directories locally, create a separate partition for <code>/home</code> at installation time [or migrate it later using the Logical Volume Manager (LVM)]. If <code>/home</code> is mounted from another system such as an NFS server, you do not need to create a separate partition at installation and you can configure the mount point at a later date.

CCE-26639-5

Severity	Category III
Vulnerability ID	V-38456
STIG ID	RHEL-06-000002
Rule ID	SV-50256r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	(For IPDB Extractor only) Verify that <code>/var</code> is located on a separate partition.
Comments	Customer Responsibility. Verify that the <code>var</code> directory has its own partition or logical volume at installation or migrate it using the Logical Volume Manager (LVM).

CCE-26647-8

Severity	Category III
Vulnerability ID	V-38487
STIG ID	RHEL-06-000015
Rule ID	SV-50288r1_rule
NIST 800-53	NIST SP 800-53 :: SA-7 NIST SP 800-53A :: SA-7.1 (ii)
CCI	CCI-000663

Check	Verify that <code>gpgcheck</code> is enabled for all YUM package repositories (System package management tool must cryptographically verify the authenticity of all software packages during installation.).
Comments	Customer Responsibility. Set to <code>gpgcheck=1</code> .

CCE-26690-8

Severity	Category II
Vulnerability ID	V-38625
STIG ID	RHEL-06-000252
Rule ID	SV-50426r1_rule
NIST 800-53	NIST SP 800-53 :: AC-17 (2) NIST SP 800-53A :: AC-17 (2).1 NIST SP 800-53 Revision 4 :: AC-17 (2)
CCI	CCI-001453
Check	(For Application host only) Verify that the host has the LDAP client configured to use TLS for all transactions.
Comments	Customer Responsibility. Configure LDAP.

CCE-26731-0

Severity	Category III
Vulnerability ID	V-38452
STIG ID	RHEL-06-000518
Rule ID	SV-50252r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI: CCI-000366

Check	Verify and correct file permissions with RPM (System package management tool must verify permissions on all files and directories associated with packages.).
Comments	Customer Responsibility. Reinstate permissions set by the vendor.

CCE-26792-2

Severity	Category III
Vulnerability ID	V-38657
STIG ID	RHEL-06-000273
Rule ID	SV-50458r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that Client Service Message Block (SMB) packet signing exists on the host if you use using an smbclient. SMB is is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.
Comments	Customer Responsibility. To require samba clients running smbclient to use packet signing, add the following to the [global] section of the Samba configuration file, /etc/samba/smb.conf: client signing = mandatory.

CCE-26801-1

Severity	Category II
Vulnerability ID	V-38520
STIG ID	RHEL-06-000136
Rule ID	Rule ID: SV-50321r1_rule
NIST 800-53	NIST SP 800-53 :: AU-9 (2) NIST SP 800-53A :: AU-9 (2).1 (iii) NIST SP 800-53 Revision 4 :: AU-9 (2)
CCI	CCI-001348

Check	Verify that logs are sent to a remote host (Operating system must back up audit records on an organization defined frequency to a different system or media than the system being audited.).
Comments	Customer Responsibility. Forward log messages to a remote log host.

CCE-26812-8

Severity	Category II
Vulnerability ID	V-38518
STIG ID	RHEL-06-000133
Rule ID	SV-50319r2_rule
NIST 800-53	NIST SP 800-53 :: SI-11 c NIST SP 800-53A :: SI-11.1 (iv) NIST SP 800-53 Revision 4 :: SI-11 b
CCI	CCI-001314
Check	Verify that log files are owned by the appropriate user.
Comments	Customer Responsibility. The owner of all log files written by rsyslog should be root. These log files are determined by the second part of each Rule line in <code>/etc/rsyslog.conf</code> and typically all appear in <code>/var/log</code> . For each log file LOGFILE referred to in <code>/etc/rsyslog.conf</code> , run the following command to inspect the file's owner: \$ <code>ls -l LOGFILE</code> If the owner is not root, run the following command to correct this: # <code>chown root LOGFILE</code>

CCE-26910-0

Severity	Category II
Vulnerability ID	V-38643
STIG ID	RHEL-06-000282
Rule ID	SV-50444r3_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b

CCI	CCI-000366
Check	Verify that there are no world-writable files on the system.
Comments	Customer Responsibility. Remove global (other) write access to a file when it is discovered. However, check with documentation for specific applications before making changes. Also, monitor for recurring world-writable files, as these may be symptoms of an application or user account that was not configured correctly.

CCE-26966-2

Severity	
Vulnerability ID	
STIG ID	
Rule ID	
NIST 800-53	
CCI	
Check	Verify that system accounts on the host do not run a shell during login.
Comments	Required Functionality. In Security Analytics, the <code>nwadmin</code> user is the exception.

CCE-26969-6

Severity	Category II
Vulnerability ID	V-51363
STIG ID	RHEL-06-000020
Rule ID	SV-65573r1_rule

NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has the SELinux State set to enforcing. You can set the SELinux State to permissive or enforcing mode. In enforcing mode, the SELinux security subsystem enforces policy decisions.
Comments	Required Functionality. If the SELinux State is set to enforcing, Security Analytics functionality does not work (for example, the Decoder will not function properly).

CCE-26974-6

Severity	Category II
Vulnerability ID	V-38593
STIG ID	RHEL-06-000073
Rule ID	SV-50394r1_rule
NIST 800-53	NIST SP 800-53 :: AC-8 c NIST SP 800-53A :: AC-8.2 (i) NIST SP 800-53 Revision 4 :: AC-8 c 1
CCI	CCI-001384
Check	Verify that the host has the Department of Defense (DoD) login banner displayed immediately prior to, or as part of, console login prompts.
Comments	Required Functionality. Security Analytics allows user to modify system banner.

CCE-27016-5

Severity	Category II
Vulnerability ID	V-38490
STIG ID	RHEL-06-000503
Rule ID	SV-50291r4_rule

NIST 800-53	NIST SP 800-53 :: AC-19 d NIST SP 800-53A :: AC-19.1 (iv)
CCI	CCI-000086
Check	Verify that the host has Modprobe loading of USB storage driver disabled.
Comments	Required Functionality. You need USB to boot from the SD cards onboard Security Analytics hosts.

CCE-27017-3

Severity	Category II
Vulnerability ID	V-38688
STIG ID	RHEL-06-000324
Rule ID	SV-50489r3_rule
NIST 800-53	NIST SP 800-53 :: AC-8 b NIST SP 800-53A :: AC-8.1 (iii) NIST SP 800-53 Revision 4 :: AC-8 b
CCI	CCI-000050
Check	Verify that the host has the graphical user interface warning banner text set (A login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.).
Comments	Required Functionality. Security Analytics does not run an Operating System level graphical user interface, banner is provided upon login through SSH or the console.

CCE-27033-0

Severity	Category III
Vulnerability ID	V-38675
STIG ID	RHEL-06-000308
Rule ID	SV-50476r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b

CCI	CCI-000366
Check	Verify that the host has core dumps for all users disabled.
Comments	<p>Customer Responsibility. The setting is enabled for Security Analytics Customer Care. To disable core dumps for all users, add the following line to <code>/etc/security/limits.conf</code>:</p> <pre>* hard core 0</pre>

CCE-27093-4

Severity	Category II
Vulnerability ID	V-38620
STIG ID	RHEL-06-000247
Rule ID	SV-50421r1_rule
NIST 800-53	NIST SP 800-53 :: AU-8 (1) NIST SP 800-53A :: AU-8 (1).1 (iii)
CCI	CCI-000160
Check	Verify that the system clock on the host is synchronized continuously, or at least daily.
Comments	Customer Responsibility. Configure Network Time Protocol (NTP) servers.

CCE-27153-6

Severity	Category II
Vulnerability ID	V-38546
STIG ID	RHEL-06-000098
Rule ID	SV-50347r2_rule

NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has IPv6 networking support automatic loading disabled.
Comments	Required Functionality. Disabling IPv6 networking support automatic loading causes functionality to fail.

CCE-27186-6

Severity	Category II
Vulnerability ID	V-38686
STIG ID	RHEL-06-000320
Rule ID	SV-50487r1_rule
NIST 800-53	NIST SP 800-53 :: SC-7 (5) NIST SP 800-53A :: SC-7 (5).1 (i) (ii) NIST SP 800-53 Revision 4 :: SC-7 (5)
CCI	CCI-001109
Check	(For Application host only) Verify that the host has certificate directives for LDAP configured to use TLS.
Comments	Customer Responsibility. Configure LDAP.

CCE-27189-0

Severity	Category II
Vulnerability ID	V-38626
STIG ID	RHEL-06-000253
Rule ID	SV-50427r1_rule

NIST 800-53	NIST SP 800-53 :: IA-2 (9) NIST SP 800-53A :: IA-2 (9).1 (ii)
CCI	CCI-000776
Check	Verify that the LDAP client on the host uses a TLS connection that uses trust certificates signed by the site CA.
Comments	Customer Responsibility. Configure LDAP.

CCE-27196-5

Severity	Category III
Vulnerability ID	V-38655
STIG ID	RHEL-06-000271
Rule ID	SV-50456r1_rule
NIST 800-53	NIST SP 800-53 :: AC-19 e NIST SP 800-53A :: AC-19.1 (v)
CCI	CCI-000087
Check	Verfiry that the host has noexec option added to removable media partitions.
Comments	Required Functionality. You need USB to boot from the SD cards.

CCE-27222-9

Severity	Category II
Vulnerability ID	V-38670
STIG ID	RHEL-06-000306
Rule ID	SV-50471r2_rule
NIST 800-53	NIST SP 800-53 :: SI-7 NIST SP 800-53A :: SI-7.1
CCI	CCI-001297
Check	Verify that the host has periodic execution of AIDE configured (Operating system must detect unauthorized changes to software and information.).

Comments	Customer Responsibility. Configure a CRON job to run AIDE or the IDS you use.
-----------------	--

CCE-27239-3

Severity	Category II
Vulnerability ID	V-54381
STIG ID	RHEL-06-000163
Rule ID	SV-68627r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has auditd admin_space_left action on low disk space configured.
Comments	Customer Responsibility. Provide sufficient disk space.

CCE-27283-1

Severity	Category III
Vulnerability ID	V-38692
STIG ID	RHEL-06-000334
Rule ID	SV-50493r1_rule
NIST 800-53	NIST SP 800-53 :: AC-2 (3) NIST SP 800-53A :: AC-2 (3).1 (ii) NIST SP 800-53 Revision 4 :: AC-2 (3)
CCI	CCI-000017
Check	Verify that the host has account expiration following inactivity set (Accounts must be locked upon 35 days of inactivity.).
Comments	Customer Responsibility. Add or correct the <code>INACTIVE=NUM_DAYS</code> lines in <code>/etc/default/useradd</code> , substituting <code>NUM_DAYS</code> appropriately.

CCE-27289-8

Severity	Category II
Vulnerability ID	V-38469
STIG ID	RHEL-06-000047
Rule ID	Rule ID: SV-50269r3_rule
NIST 800-53	NIST SP 800-53 :: CM-5 (6) NIST SP 800-53A :: CM-5 (6).1 NIST SP 800-53 Revision 4 :: CM-5 (6)
CCI	CCI-001499
Check	Verify that all system command files on the host have mode 755 or less permissive.
Comments	Customer Responsibility. Some files deployed by Erlang do not have permissions set according to STIG guidelines. Change permissions to conform to STIG guidelines using the following command: <pre># chmod go-w FILE</pre>

CCE-27365-6

Severity	Category II
Vulnerability ID	V-38660
STIG ID	RHEL-06-000340
Rule ID	SV-50461r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has the SNMP service configured to use only SNMPv3 or a newer version of SNMP.
Comments	Customer Responsibility. Configure SNMPv3.

CCE-27381-3

Severity	Category II
Vulnerability ID	V-38465
STIG ID	RHEL-06-000045
Rule ID	SV-50265r3_rule
NIST 800-53	NIST SP 800-53 :: CM-5 (6) NIST SP 800-53A :: CM-5 (6).1 NIST SP 800-53 Revision 4 :: CM-5 (6)
CCI	CCI-001499
Check	Verify that shared library files on the host have restrictive permissions (Library files must have mode 0755 or less permissive.).
Comments	Customer Responsibility. Fix permissions.

CCE-27409-2

Severity	Category II
Vulnerability ID	V-38667
STIG ID	RHEL-06-000285
Rule ID	SV-50468r2_rule
NIST 800-53	NIST SP 800-53 :: SI-4 (5) NIST SP 800-53A :: SI-4 (5).1 (ii)
CCI	CCI-001263
Check	Verify that the host has intrusion detection software installed.
Comments	Customer Responsibility. Install intrusion detection software. RSA Does not provide this software.

CCE-27529-7

Severity	Category I
Vulnerability ID	V-38666
STIG ID	RHEL-06-000284
Rule ID	SV-50467r2_rule
NIST 800-53	NIST SP 800-53 :: SI-3 a NIST SP 800-53A :: SI-3.1 (ii)
CCI	CCI-001668
Check	Verify that virus scanning software is installed on the host (System must use and update a DoD-approved virus scan program.).
Comments	Customer Responsibility. Install virus scanning software. RSA does not provide this software

CCE-27593-3

Severity	Category I
Vulnerability ID	V-38653
STIG ID	RHEL-06-000341
Rule ID	SV-50454r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host does not use a default password (The <code>snmpd</code> service must not use a default password.).

Comments	Customer Responsibility. Change the default password for SNMP.
CCE-27596-6	
Severity	Category III
Vulnerability ID	V-38659
STIG ID	RHEL-06-000275
Rule ID	SV-50460r2_rule
NIST 800-53	NIST SP 800-53 :: MP-4 (1) NIST SP 800-53A :: MP-4 (1).1
CCI	CCI-001019
Check	Verify that partitions on the host are encrypted.
Comments	Required Functionality. Security Analytics does not encrypt partitions because it degrades performance.

CCE-27635-2

Severity	Category II
Vulnerability ID	V-38481
STIG ID	RHEL-06-000011
Rule ID	SV-50281r1_rule
NIST 800-53	NIST SP 800-53 :: SI-2 (2) NIST SP 800-53A :: SI-2 (2).1 (ii) NIST SP 800-53 Revision 4 :: SI-2 (2)
CCI	CCI-001233
Check	Verify that the host has security software patches installed.

Comments

Customer Responsibility. Make sure that you have applied the Security Analytics security updates.

Not a Finding

The following exceptions do not apply to Security Analytics. RSA has verified that the system meets these requirements.

CCE-26242-8

Severity	Category III
Vulnerability ID	V-38635
STIG ID	RHEL-06-000165
Rule ID	SV-50436r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 a NIST SP 800-53A :: AU-12.1 (ii) NIST SP 800-53 Revision 4 :: AU-12 a
CCI	CCI-000169
Check	Verify that the host records attempts to alter time through adjtimex (Audit system must be configured to audit all attempts to alter system time through adjtimex.).
Comments	Not a Finding. Make sure that you have the correct <code>adjtimex</code> configuration on the host. The following settings are the correct configuration. [root@localhost nwadmin]# <code>grep adjtimex /etc/audit/*</code> <code>/etc/audit/audit.rules:-a exit,always -F arch=b64 -S adjtimex -k audit_time_rules</code> <code>/etc/audit/audit.rules:-a exit,always -F arch=b32 -S adjtimex -k audit_time_rules</code>

CCE-26280-8

Severity	Category III
-----------------	--------------

Vulnerability ID	V-38543
STIG ID	RHEL-06-000184
Rule ID	SV-50344r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - chmod .
Comments	Not a Finding. Make sure that you have the correct chmod configuration on the host. The following settings are the correct configuration. [root@localhost nwadmin]# grep chmod /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-26303-8

Severity	Category II
Vulnerability ID	V-38574
STIG ID	RHEL-06-000062
Rule ID	SV-50375r2_rule

NIST 800-53	NIST SP 800-53 :: IA-7 NIST SP 800-53A :: IA-7.1 NIST SP 800-53 Revision 4 :: IA-7
CCI	CCI-000803
Check	Verify that the host has the password hashing algorithm in /etc/pam.d/system-auth set.
Comments	Not a Finding. Security Analytics has parameter set to 24: [root@localhost nwadmin]# grep remember= /etc/pam.d/* /etc/pam.d/system-auth-ac:password sufficient pam_unix.so sha512 remember=24

CCE-26506-6

Severity	Category I
Vulnerability ID	V-38476
STIG ID	RHEL-06-000008
Rule ID	SV-50276r3_rul
NIST 800-53	NIST SP 800-53 :: CM-5 (3) NIST SP 800-53A :: CM-5 (3).1 (ii)
CCI	CCI-000352
Check	Verify that the Red Hat GPG Key is installed on the host. All Red Hat Enterprise Linux packages are signed with the Red Hat GPG key. GPG stands for GNU Privacy Guard. GnuPG is compliant with RFC 4880, which is the Internet Engineering task Force (IETF) standards track specification of OpenPGP protocol for encrypting email using public key cryptography.
Comments	Not Finding. Security Analytics runs under CentOS so it does not have a Red Hat GPG key.

CCE-26555-3

Severity	Category II
-----------------	-------------

Vulnerability ID	V-38617
STIG ID	RHEL-06-000243
Rule ID	SV-50418r1_rule
NIST 800-53	NIST SP 800-53 :: SC-13 NIST SP 800-53A :: SC-13.1
CCI	CCI-001144
Check	Verify that the host only uses approved ciphers (The SSH daemon must be configured to use only FIPS 140-2 approved ciphers.).
Comments	<p>Not a Finding. Make sure that you have the correct <code>fchmod</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fchmod /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 -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</pre>

CCE-26611-4

Severity	Category II
Vulnerability ID	V-38580
STIG ID	RHEL-06-00020

Rule ID	SV-50381r2_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that auditd collects information on kernel module loading and unloading on the host.
Comments	<p>Not a Finding. Make sure that you have the correct auditd configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep module /etc/audit/audit.rules -a exit,always -F arch=b64 -S init_module -S delete_module -k modules -a exit,always -F arch=b32 -S init_module -S delete_module -k modules -w /sbin/insmod -p x -k modules -w /sbin/modprobe -p x -k modules -w /sbin/rmmod -p x -k modules</pre>

CCE-26648-6

Severity	Category III
Vulnerability ID	V-38540
STIG ID	RHEL-06-000182
Rule ID	SV-50341r3_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366

Check	Verify that the host records events that modify its network environment.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep audit_network_modifications /etc/audit/* /etc/audit/audit.rules:-w /etc/issue -p wa -k audit_network_modifications /etc/audit/audit.rules:-w /etc/issue.net -p wa -k audit_network_modifications /etc/audit/audit.rules:-w /etc/hosts -p wa -k audit_network_modifications /etc/audit/audit.rules:-w /etc/sysconfig/network -p wa -k audit_network_modifications /etc/audit/audit.rules:-a exit,always -F arch=b64 -S sethostname -S setdomainname -k audit_network_modifications /etc/audit/audit.rules:-a exit,always -F arch=b32 -S sethostname -S setdomainname -k audit_network_modifications</pre>

CCE-26651-0

Severity	Category III
Vulnerability ID	V-38575
STIG ID	RHEL-06-000200
Rule ID	SV-50376r4_rule
NIST 800-53	<p>NIST SP 800-53 :: AU-12 c</p> <p>NIST SP 800-53A :: AU-12.1 (iv)</p> <p>NIST SP 800-53 Revision 4 :: AU-12 c</p>
CCI	CCI-000172

Check	Verify that auditd collects file deletion events by user on the host.
Comments	<p>Not a Finding. Make sure that you have the correct auditd configuration on the host. The following settings are the correct configuration. [root@localhost nwadmin]# grep unlink /etc/audit/audit.rules-a</p> <pre>exit,always -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid=0 -k delete-a exit,always -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid=0 -k delete-a exit,always -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete-a exit,always -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete</pre> <p>[root@localhost nwadmin]#</p>

CCE-26712-0

Severity	Category III
Vulnerability ID	V-38566
STIG ID	RHEL-06-000197
Rule ID	SV-50367r2_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that auditd collects unauthorized access attempts to files (unsuccessful) on the host.

Comments

Not a Finding. Make sure that you have the correct configuration on the host. You must add the following settings to `/etc/audit/audit.rules` on the host. Set `arch` to either `b32` or `b64` as appropriate for your system. The following settings are the correct configuration.

```
[root@localhost nwadmin]# grep creat
/etc/audit/audit.rules
-a exit,always -F arch=b64 -S creat -S open -S openat -S
truncate -S ftruncate -F exit=-EACCES -F auid=500 -F
auid!=4294967295 -k access
-a exit,always -F arch=b64 -S creat -S open -S openat -S
truncate -S ftruncate -F exit=-EPERM -F auid=500 -F auid!-
!=4294967295 -k access
-a exit,always -F arch=b32 -S creat -S open -S openat -S
truncate -S ftruncate -F exit=-EACCES -F auid=500 -F
auid!=4294967295 -k access
-a exit,always -F arch=b32 -S creat -S open -S openat -S
truncate -S ftruncate -F exit=-EPERM -F auid=500 -F auid!-
!=4294967295 -k access
```

CCE-26741-9

Severity	Category II
Vulnerability ID	V-38658
STIG ID	RHEL-06-000274
Rule ID	SV-50459r2_rule
NIST 800-53	NIST SP 800-53 :: IA-5 (1) (e) NIST SP 800-53A :: IA-5 (1).1 (v) NIST SP 800-53 Revision 4 :: IA-5 (1) (e)
CCI	CCI-000200

Check	Verify that the host limits password reuse.
Comments	Not a Finding. Security Analytics has <code>password remember</code> set to 24. The following settings are the correct configuration. <code>[root@localhost ~]# grep remember= /etc/pam.d/*/etc/pam.d/system-auth-ac:password sufficient pam_unix.so sha512 remember=24</code>

CCE-27567-7

Severity	Category I
Vulnerability ID	V-38668
STIG ID	RHEL-06-000286
Rule ID	SV-50469r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has the Ctrl-Alt-Del reboot activation disabled (The x86 Ctrl-Alt-Delete key sequence must be disabled.).
Comments	Not a Finding. Make sure that you have the correct configuration on the host. <code>/etc/inittab</code> must have: <code>ca:nil:ctrlaltdel:/usr/bin/logger -p security.info "Ctrl-Alt-Del was pressed".</code>

CCE-26763-3

Severity	Category II
Vulnerability ID	V-38682
STIG ID	RHEL-06-000315

Rule ID	SV-50483r3_rule
NIST 800-53	NIST SP 800-53 :: AC-19 c NIST SP 800-53A :: AC-19.1 (iii)
CCI	CCI-000085
Check	Verify the host has bluetooth kernel modules disabled.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep net-pf-31 /etc/modprobe.d/* /etc/modprobe.d/stig.conf:install net-pf-31 /bin/true [root@localhost nwadmin]# grep bluetooth /etc/modprobe.d/* /etc/modprobe.d/stig.conf:install bluetooth /bin/false</pre>

CCE-26774-0

Severity	Category III
Vulnerability ID	V-51379
STIG ID	RHEL-06-000025
Rule ID	SV-65589r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host does not have any device files unlabeled by SELinux.

Comments	<p>Not a Finding. Security Analytics requires that device files are labeled with proper SELinux types for communication.</p> <p>Run the following command string on the host to check for unlabeled device files.</p> <pre>ls -RZ /dev grep unlabeled_t</pre> <p>It should produce no output in a correctly configured host.</p>
-----------------	---

CCE-26785-6

Severity	Category III
Vulnerability ID	V-38438
STIG ID	RHEL-06-000525
Rule ID	SV-50238r2_rule
NIST 800-53	<p>NIST SP 800-53 :: AU-12 a</p> <p>NIST SP 800-53A :: AU-12.1 (ii)</p> <p>NIST SP 800-53 Revision 4 :: AU-12 a</p>
CCI	CCI-000169
Check	Verify that host has auditing for processes which start prior to the audit daemon enabled.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep audit /etc/grub.conf kernel /boot/vmlinuz-2.6.32-504.1.3.el6.x86_64 ro root- t=UUID=03632221-29ef-4fac-b5d5-b5af0b925389 rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latacyrheb- sun16 crashkernel=auto KEYBOARDTYPE=pc KEYTABLE=us rd_ NO_DM rhgb quiet audit=1</pre>

CCE-26801-1

Severity	Category II
-----------------	-------------

Vulnerability ID	V-38520
STIG ID	RHEL-06-000136
Rule ID	SV-50321r1_rule
NIST 800-53	NIST SP 800-53 :: AU-9 (2) NIST SP 800-53A :: AU-9 (2).1 (iii) NIST SP 800-53 Revision 4 :: AU-9 (2)
CCI	CCI-001348
Check	Verify that logs on the host are sent to remote host.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host.</p> <p>To configure <code>rsyslog</code> to send logs to a remote log server, open <code>/etc/rsyslog.conf</code> and read and understand the last section of the file, which describes the multiple directives necessary to activate remote logging. Comply with these directives and configure the host to forward its logs to a particular log server by adding or correcting one of the following lines, substituting <code>loghost.example.com</code> for your host. You choose a protocol depending on the environment of the host. TCP and RELP provide more reliable message delivery, but they may not be supported in all environments.</p> <p>Insert <code>.@</code> as a prefix to use UDP for log message delivery: <code>.@loghost.example.com</code></p> <p>Insert <code>.@@</code> as a prefix to use TCP for log message delivery: <code>.@@loghost.example.com</code></p> <p>Insert <code>. :omrelp:</code> as a prefix to use RELP for log message delivery: <code>. :omrelp:loghost.example.com</code></p> <p>A log server (loghost) receives syslog messages from one or more systems. You can use this data as an additional log source if a system is compromised and its local logs are suspect. Forwarding log messages to a remote loghost also provides system administrators with a centralized place to view the status of multiple hosts within the enterprise.</p>

CCE-26828-4

Severity	Category II
Vulnerability ID	V-38629
STIG ID	RHEL-06-000257
Rule ID	SV-50430r3_rule
NIST 800-53	NIST 800-53 SP 800-53 :: AC-11 a NIST 800-53 SP 800-53A :: AC-11.1 (ii) NIST 800-53 SP 800-53 Revision 4 :: AC-11 a
CCI	CCI-000057
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. Security Analytics does not use Gnome Graphical User Interface (GUI) Desktop.

CCE-26840-9

Severity	Category III
Vulnerability ID	V-38697
STIG ID	RHEL-06-000336
Rule ID	SV-50498r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has sticky bits set for all world-writable directories.
Comments	Not a Finding.

CCE-26844-1

Severity	Category II
Vulnerability ID	V-38573
STIG ID	RHEL-06-000061
Rule ID	SV-50374r4_rule
NIST 800-53	NIST SP 800-53 :: AC-7 a NIST SP 800-53A :: AC-7.1 (ii) NIST SP 800-53 Revision 4 :: AC-7 a
CCI	CCI-000044
Check	Verify that the host has deny for failed password attempts set.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fail_interval=900 /etc/pam.d/* /etc/pam.d/system-auth-ac:auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800 fail_interval=900 /etc/pam.d/system-auth-ac:auth required pam_faillock.so authsucc deny=3 unlock_time=604800 fail_interval=900</pre>

CCE-26872-2

Severity	
Vulnerability ID	
STIG ID	
Rule ID	
NIST 800-53	

CCI	
Check	Verify that all files on the host are owned by a group.
Comments	<p>Not a Finding. No files are owned by a group and this finding is a false positive.</p> <pre>[root@localhost nwadmin]# rpm -V audit grep '^.....G' [root@localhost nwadmin]#</pre>

CCE-27031-4

Severity	Category III
Vulnerability ID	V-38642
STIG ID	RHEL-06-000346
Rule ID	SV-50443r1_rule
NIST 800-53	<p>NIST SP 800-53 :: CM-6 b</p> <p>NIST SP 800-53A :: CM-6.1 (iv)</p> <p>NIST SP 800-53 Revision 4 :: CM-6 b</p>
CCI	CCI-000366
Check	Verify that host has daemon umask set.
Comments	<p>Not a Finding. Security Analytics has daemon umask set to 022. Make sure that the host has umask set to 022.</p> <pre>[root@localhost nwadmin]# grep umask /etc/in- it.d/functions</pre>

CCE-27110-6

Severity	Category II
Vulnerability ID	V-38592

STIG ID	RHEL-06-000356
Rule ID	SV-50393r4_rule
NIST 800-53	NIST SP 800-53 :: AC-7 b NIST SP 800-53A :: AC-7.1 (iv)
CCI	CCI-000047
Check	Verify that host has lockout time for failed password attempts set.
Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fail_interval=900 /etc/pam.d/* /etc/pam.d/system-auth-ac:auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800 fail_interval=900 /etc/pam.d/system-auth-ac:auth required pam_faillock.so authsucc deny=3 unlock_time=604800 fail_interval=900</pre>

CCE-27123-9

Severity	
Vulnerability ID	
STIG ID	
Rule ID	
NIST 800-53	
CCI	
Check	Verify that the host has password retry prompts permitted per session set.

Comments	<p>Not a Finding. Make sure that you have the correct configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep retry=3 /etc/pam.d/* /etc/pam.d/system-auth-ac:#password requisite pam_cracklib.so try_first_pass retry=3 type=</pre>
-----------------	---

CCE-27142-9

Severity	Category III
Vulnerability ID	V-38702
STIG ID	RHEL-06-000339
Rule ID	SV-50503r1_rule
NIST 800-53	NIST SP 800-53 :: AU-3 NIST SP 800-53A :: AU-3.1 NIST SP 800-53 Revision 4 :: AU-3
CCI	CCI-000130
Check	Verify that the host has logging of all FTP transactions enabled.
Comments	Not a Finding. Security Analytics does not use FTP.

CCE-27145-2

Severity	Category II
Vulnerability ID	V-38599
STIG ID	RHEL-06-000348
Rule ID	SV-50400r2_rule
NIST 800-53	NIST SP 800-53 :: AC-8 a NIST SP 800-53A :: AC-8.1 (ii) NIST SP 800-53 Revision 4 :: AC-8 a
CCI	CCI-000048
Check	Verify that the host has warning banners for All FTP users created (The FTPS/FTP service on the system must be configured with the Department of Defense (DoD) login banner.).

Comments	Not a Finding. Security Analytics does not use FTP.
CCE-27170-0	
Severity	Category III
Vulnerability ID	V-38527
STIG ID	RHEL-06-000171
Rule ID	SV-50328r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 a NIST SP 800-53A :: AU-12.1 (ii) NIST SP 800-53 Revision 4 :: AU-12 a
CCI	CCI-000169
Check	Verify that the host records attempts to alter time through <code>clock_settime</code> .
Comments	Not a Finding. Make sure that you have the correct <code>clock_settime</code> configuration on the host. The following settings are the correct configuration. [root@localhost nwadmin]# grep clock_settime /etc/audit/* /etc/audit/audit.rules:-a exit,always -F arch=b64 -S clock_settime -k audit_time_rules /etc/audit/audit.rules:-a exit,always -F arch=b32 -S clock_settime -k audit_time_rules

CCE-27173-4

Severity	Category III
Vulnerability ID	V-38545
STIG ID	RHEL-06-000185
Rule ID	SV-50346r3_rule

NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - chown.
Comments	<p>Not a Finding. Make sure that you have the correct <code>chown</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[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 fchow- nat -S fremovexattr -S fsetxattr -S lchown -S lre- movexattr -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 fre- movexattr -S fsetxattr -S lchown -S lremovexattr -S lre- movexattr -S lsetxattr -S removexattr -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod</pre>

CCE-27174-2

Severity	Category III
Vulnerability ID	V-38547
STIG ID	RHEL-06-000186
Rule ID	SV-50348r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172

Check	Verify that the host records events that modify the system's discretionary access controls - fchmod.
Comments	<p>Not a Finding. Make sure that you have the correct fchmod configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fchmod /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 -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</pre>

CCE-27175-9

Severity	Category III
Vulnerability ID	V-38550
STIG ID	RHEL-06-000187
Rule ID	SV-50351r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - fchmodat.

Comments	<p>Not a Finding. Make sure that you have the correct <code>fchmodat</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fchmodat /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 -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</pre>
-----------------	--

CCE-27177-5

Severity	Category III
Vulnerability ID	V-38552
STIG ID	RHEL-06-000188
Rule ID	SV-50353r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>fchown</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>fchown</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fchown /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 -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</pre>
-----------------	--

CCE-27178-3

Severity	Category III
Vulnerability ID	V-38554
STIG ID	RHEL-06-000189
Rule ID	SV-50355r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>fchownat</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>fchownat</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fchownat /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 -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</pre>
-----------------	--

CCE-27179-1

Severity	Category III
Vulnerability ID	V-38556
STIG ID	RHEL-06-000190
Rule ID	SV-50357r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>fremovexattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>fremovexattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fremovexattr /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 -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</pre>
-----------------	--

CCE-27180-9

Severity	Category III
Vulnerability ID	V-38557
STIG ID	RHEL-06-000191
Rule ID	SV-50358r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>fsetxattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>fsetxattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fsetx- attr/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 fsetx- attr -S lchown -S lremovexattr -S lremovexattr -S lsetx- attr -S removexattr -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod -a exit,always -F arch=b32 -S chown -S fchmod -S fch- modat -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</pre>
-----------------	--

CCE-27181-7

Severity	Category III
Vulnerability ID	V-38558
STIG ID	RHEL-06-000192
Rule ID	SV-50359r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>lchown</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>lchown</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep lchown /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 -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</pre>
-----------------	--

CCE-27182-5

Severity	Category III
Vulnerability ID	V-38559
STIG ID	RHEL-06-00019
Rule ID	SV-50360r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>lremovexattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>lremovexattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep lremovexattr /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 -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</pre>
-----------------	--

CCE-27183-3

Severity	Category III
Vulnerability ID	V-38561
STIG ID	RHEL-06-000194
Rule ID	V-50362r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>lsetxattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>lsetxattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep lsetxattr /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 -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</pre>
-----------------	--

CCE-27184-1

Severity	Category III
Vulnerability ID	V-38563
STIG ID	RHEL-06-000195
Rule ID	SV-50364r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>removexattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>removexattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep removexattr /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 -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</pre>
-----------------	--

CCE-27185-8

Severity	Category III
Vulnerability ID	V-38565
STIG ID	RHEL-06-000196
Rule ID	SV-50366r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv) NIST SP 800-53 Revision 4 :: AU-12 c
CCI	CCI-000172
Check	Verify that the host records events that modify the system's discretionary access controls - <code>setxattr</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>setxattr</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep setxattr /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 -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</pre>
-----------------	--

CCE-27203-9

Severity	Category III
Vulnerability ID	V-38522
STIG ID	RHEL-06-000167
Rule ID	SV-50323r3_rule
NIST 800-53	NIST SP 800-53 :: AU-12 a NIST SP 800-53A :: AU-12.1 (ii) NIST SP 800-53 Revision 4 :: AU-12 a
CCI	CCI-000169
Check	Verify that the host records attempts to alter time through <code>settimeofday</code> .

Comments	<p>Not a Finding. Make sure that you have the correct <code>settimeofday</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep settimeofday /etc/audit/* /etc/audit/audit.rules:-a exit,always -F arch=b64 -S settimeofday -k audit_time_rules /etc/audit/audit.rules:-a exit,always -F arch=b32 -S settimeofday -k audit_time_rules</pre>
-----------------	---

CCE-27215-3

Severity	Category III
Vulnerability ID	V-38501
STIG ID	RHEL-06-000357
Rule ID	SV-50302r4_rule
NIST 800-53	NIST SP 800-53 :: AC-7 a NIST SP 800-53A :: AC-7.1 (ii)
CCI	CCI-001452
Check	Verify that the host has interval for counting failed password attempts set.
Comments	<p>Not a Finding. Make sure that you have the correct <code>fail_interval</code> configuration on the host. The following settings are the correct configuration.</p> <pre>[root@localhost nwadmin]# grep fail_interval=900 /etc/pam.d/* /etc/pam.d/system-auth-ac:auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800 fail_interval=900 /etc/pam.d/system-auth-ac:auth required pam_faillock.so authsucc deny=3 unlock_time=604800 fail_interval=900</pre>

CCE-27291-4

Severity	Category II
Vulnerability ID	V-51875
STIG ID	RHEL-06-000372
Rule ID	SV-66089r1_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has the last logon/access notification set.
Comments	Not a Finding. Make sure that you have the correct <code>lastlog</code> configuration on the host. The following settings are the correct configuration. <pre>[root@localhost nwadmin]# grep lastlog /etc/pam.d/* /etc/pam.d/password-auth:session required pam_lastlog.so showfailed /etc/pam.d/password-auth-local:session required pam_lastlog.so showfailed</pre>

Rules to Be Supported in Future Release

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

CCE-26282-4

Severity	Category III
Vulnerability ID	V-38610
STIG ID	RHEL-06-000231

Rule ID	SV-50411r1_rule
NIST 800-53	NIST SP 800-53 :: MA-4 e NIST SP 800-53A :: MA-4.1 (vi) NIST SP 800-53 Revision 4 :: MA-4 e
CCI	CCI-000879
Check	(For Log Decoder and Remote Collector hosts only) Verify that the host has the SSH Client alive count set.
Comments	Future Feature

CCE-26444-0

Severity	Category II
Vulnerability ID	V-38513
STIG ID	RHEL-06-000120
Rule ID	SV-50314r1_rule
NIST 800-53	NIST 800-53 SP 800-53 :: AC-17 e NIST 800-53 SP 800-53A :: AC-17.1 (v)
CCI	CCI-000066
Check	Verify that the host has default iptables policy for incoming packets set (Local IPv4 firewall must implement a deny-all, allow-by-exception policy for inbound packets).
Comments	Future Feature

CCE-26457-2

Severity	Category III
Vulnerability ID	V-38567

STIG ID	RHEL-06-000198
Rule ID	SV-50368r4_rule
NIST 800-53	NIST SP 800-53 :: AC-6 (2) NIST SP 800-53A :: AC-6 (2).1 (iii)
CCI	CCI-000040
Check	Verify that auditd collects information on the Use of Privileged commands on the host.
Comments	Future Feature

CCE-26638-7

Severity	Category III
Vulnerability ID	V-38639
STIG ID	RHEL-06-000260
Rule ID	SV-50440r3_rule
NIST 800-53	NIST 800-53 SP 800-53 :: AC-11 (1) NIST 800-53 SP 800-53A :: AC-11 (1).1 NIST 800-53 SP 800-53 Revision 4 :: AC-11 (1)
CCI	CCI-000060
Check	Verify that the blank screen saver is implemented on the host (System must display a publicly-viewable pattern during a graphical desktop environment session lock.).
Comments	Future Feature

CCE-26821-9

Severity	Category III
Vulnerability ID	V-38699
STIG ID	RHEL-06-000337

Rule ID	SV-50500r2_rule
NIST 800-53	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that log files on the host are owned by appropriate group (All public directories must be owned by a system account.).
Comments	Future Feature

CCE-26887-0

Severity	Category I
Vulnerability ID	V-38614
STIG ID	RHEL-06-000239
Rule ID	SV-50415r1_rule
NIST 800-53	NIST SP 800-53 :: IA-2 (2) NIST SP 800-53A :: IA-2 (2).1 NIST SP 800-53 Revision 4 :: IA-2 (2)
CCI	CCI-000766
Check	(For Log Decoder and Remote Collector hosts only) Verify that the host has the SSH access through empty passwords disabled.
Comments	Future Feature

CCE-26919-1

Severity	Category III
Vulnerability ID	V-38608

STIG ID	RHEL-06-000230
Rule ID	SV-50409r1_rule
NIST 800-53	NIST SP 800-53 :: SC-10 NIST SP 800-53A :: SC-10.1 (ii) NIST SP 800-53 Revision 4 :: SC-10
CCI	CCI-001133
Check	(For Log Decoder and Remote Collector hosts only) Verify that the host has the SSH idle timeout interval set.
Comments	Future Feature

CCE-27167-6

Severity	Category I
Vulnerability ID	V-38677
STIG ID	RHEL-06-00030
Rule ID	SV-50478r1_rule
NIST 800-53	NIST 800-53 SP 800-53 :: IA-2 NIST 800-53 SP 800-53A :: IA-2.1 NIST 800-53 SP 800-53 Revision 4 :: IA-2
CCI	CCI-000764
Check	Verify that the host prohibits insecure file locking (The NFS server must not have the insecure file locking option enabled.).
Comments	Future Feature

CCE-27190-8

Severity	Category II
-----------------	-------------

Vulnerability ID	V-38623
STIG ID	RHEL-06-000135
Rule ID	SV-50424r2_rule
NIST 800-53	NIST SP 800-53 :: SI-11 c NIST SP 800-53A :: SI-11.1 (iv) NIST SP 800-53 Revision 4 :: SI-11 b
CCI	CCI-001314
Check	Verify that host has correct permissions configured for system log files (All rsyslog-generated log files must have mode 0600 or less permissive.).
Comments	Future Feature

CCE-27201-3

Severity	Category III
Vulnerability ID	V-38616
STIG ID	RHEL-06-000241
Rule ID	SV-50417r1_rule
NIST 800-53	NIST SP 800-53 :: AC-4 NIST SP 800-53A :: AC-4.1 (iii) NIST SP 800-53 Revision 4 :: AC-4
CCI	CCI-001414
Check	(For Log Decoder and Remote Collector hosts only) Verify that the host does not allow SSH environment options.
Comments	Future Feature

CCE-27227-8

Severity	Category III
Vulnerability ID	V-38693
STIG ID	RHEL-06-000299
Rule ID	SV-50494r2_rule
NIST 800-53	NIST 800-53 SP 800-53 :: CM-6 b NIST 800-53 SP 800-53A :: CM-6.1 (iv) NIST 800-53 SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366
Check	Verify that the host has the password set to a maximum of three consecutive repeating characters (The system must require passwords to contain no more than three consecutive repeating characters.).
Comments	Future Feature

CCE-27379-7

Severity	Category III
Vulnerability ID	V-38681
STIG ID	RHEL-06-000294
Rule ID	SV-50482r2_rule
NIST 800-53	NIST 800-53 SP 800-53 :: CM-6 b NIST 800-53 SP 800-53A :: CM-6.1 (iv) NIST 800-53 SP 800-53 Revision 4 :: CM-6 b
CCI	CCI-000366

Check	Verify that the host has all GIDs referenced in <code>/etc/passwd</code> defined in <code>/etc/group</code> (All GIDs referenced in <code>/etc/passwd</code> must be defined in <code>/etc/group</code>).
Comments	Future Feature

CCE-27440-7

Severity	Category II
Vulnerability ID	V-38595
STIG ID	RHEL-06-000349
Rule ID	SV-50396r3_rule
NIST 800-53	NIST SP 800-53 :: IA-2 (1) NIST SP 800-53A :: IA-2 (1).1 NIST SP 800-53 Revision 4 :: IA-2 (1)
CCI	CCI-000765
Check	Verify that the host has smart card login enabled (System must be configured to require the use of a CAC, PIV compliant hardware token, or Alternate Logon Token (ALT) for authentication.).
Comments	Future Feature

CCE-27474-6

Severity	Category III
Vulnerability ID	V-38685
STIG ID	RHEL-06-000297
Rule ID	SV-50486r1_rule

NIST 800-53	NIST 800-53 SP 800-53 :: AC-2 (2) NIST 800-53 SP 800-53A :: AC-2 (2).1 (ii) NIST 800-53 SP 800-53 Revision 4 :: AC-2 (2)
CCI	CCI-000016
Check	Verify that the host has an expiration date assigned to temporary accounts (Temporary accounts must be provisioned with an expiration date.).
Comments	Future Feature

CCE-27609-7

Severity	Category III
Vulnerability ID	V-38683
STIG ID	RHEL-06-000296
Rule ID	SV-50484r1_rule
NIST 800-53	NIST SP 800-53 :: IA-8 NIST SP 800-53A :: IA-8.1 NIST SP 800-53 Revision 4 :: IA-8
CCI	CCI-000804
Check	Verify that all accounts on the host have unique names (All accounts on the system must have unique user or account names.).
Comments	Future Feature

Manage Security Analytics Updates

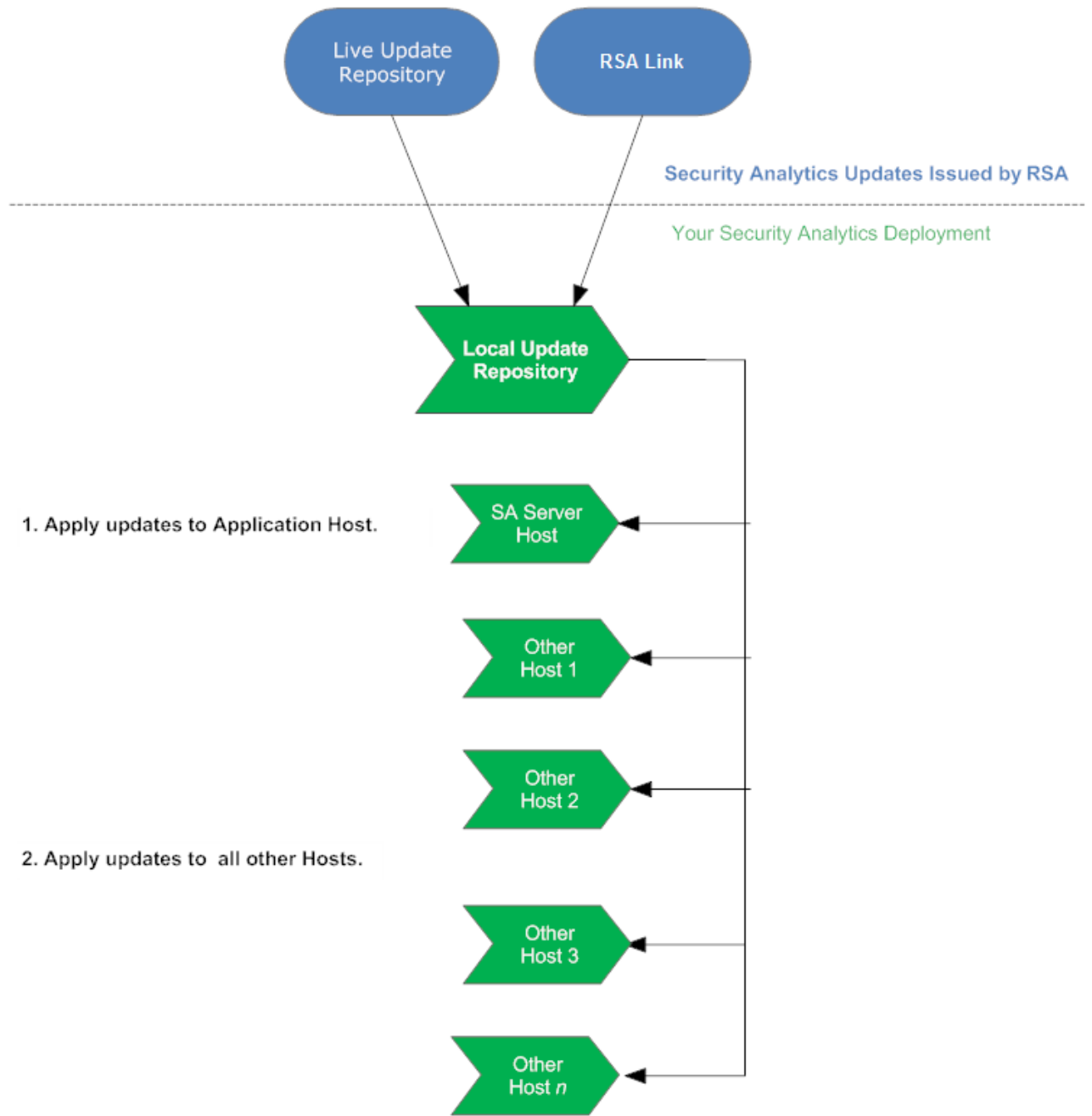
RSA issues Security Analytics software version updates on a regular basis as it strives to continually improve the product. A software version update consists of a release, service pack, or patch (including security patch) and ancillary software on which the release, service pack, or patch depends.

Software Update Process

The following figure illustrates how to:

- Populate the Local Update Repository with software version updates issued by RSA. You have the following two options:
 - Ongoing connection to the Live Update Repository.
 - Download RSA Link
- Apply these updates.

Security Analytics Software Update Process



- [Review Version and License Status](#)

Apply Software Version Updates from Hosts View

Note: The Hosts view update feature requires that you have the desired software version updates in the Local Update Repository.

After you have populated the Local Update Repository, you apply these updates using the Hosts view when you want to:

- Add or update a host.
- Check and apply updates to a host.

Note: If you need to restore the previous version, refer to **Back Up and Restore Data for Hosts and Services** in the *RSA Security Analytics Host and Services Configuration Guide*.

Populate Local Update Repository

The Local Update Repository is the staging area in your Security Analytics deployment from which you apply version updates to your hosts. The Live Update Repository is the location to which RSA posts the latest Security Analytics version updates. This topic describes the following two options of populating the Local Update Repository in your Security Analytics deployment from the Live Update Repository:

- Option 1 - Connect to the Live Update Repository.
This connects your Security Analytics Local Update Repository to the RSA Live Update Repository through the Internet using your LIVE account.
- Option 2 - Download version updates from RSA Link (<https://community.rsa.com/>).
If you do not allow your Security Analytics deployment to connect to the Internet, you must download the update packages from RSA Link to a local directory and then upload them to your Security Analytics Local Update Repository.

Option 1 - Connect to Live Update Repository

Access to the Live Update Repository requires and uses the Live Account credentials configured under **Administration > System > Live**.

Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 6 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your Security Analytics Server's Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository.

To connect to the Live Update Repository:

Note: If you need to use a proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. Refer to *Configure Proxy for Security Analytics* in the *Security Analytics System Configuration Guide* in the help on RSA Link (<https://community.rsa.com/>).

1. Navigate to the **Administration > System** view, select **Live Services** in the options panel and ensure that credentials are configured. If they are not configured, do so now, click **Test Connection**, and click **Apply**.
Make sure that Test Connection is successful because this account is used to access the Live Update Repository.
2. Select the **Updates > Settings** tab.
3. Select the **Enable** check box and click **Apply**.
4. Use the **Test Connection** button to check for connectivity. Make sure that this is successful. An **RSASoftware.repo** file is automatically created in the Security Analytics Server Host **/etc/yum.repos.d/** directory, which is used by your Local Update Repository to communicate with the Live Update Repository.
After it is enabled, the Local Update Repository will synchronize and download all available packages from the Live Update Repository on the next scheduled event. You can also force a synchronize job from the **Updates Repository** tab using the **Synchronize Now** option.
After you update both of the Update Repositories (Live and Local), you can see all downloaded RPM packages in the **Updates Repository** tab of the **Administration > Updates** panel.
5. In the Security Analytics menu, select **Administration > System**.
The Info view is displayed.
6. In the left panel, select **Updates**.
7. In the **Updates Repository** tab, click **Synchronize Now**. A message similar to the following is displayed.

The **Updates Repository** tab is displayed with the updates you retrieved by synchronizing.

Option 2 - Download Version Updates from RSA Link

You would need to populate Security Analytics update repository from RSA Link (<https://community.rsa.com/>) for the following reasons:

- If the version updates that you want are not in your Local Update Repository (that is, they are not listed in the **Updates Available** list for a host in the **Updates** column in the Hosts view).

- If your Security Analytics deployment does not have Internet access.

Warning: After you update a host from the Local Update Repository, you may not be able to access earlier versions to update other hosts. This is determined by the amount of available space in your Local Update Repository and the size of the update packages. For example, if you updated the Security Analytics Server Host to 10.5.2.0 and then to 10.6.3.0, 10.5.2.0 may have been removed and will not be available to update other hosts. If you needed to update another system to 10.5.2.0 (before updating to 10.6.3.0), you would need to download 10.5.2.0 from RSA Link and manually update the Local Update Repository again.

To populate your Local Update Repository from RSA Link:

1. Download the zip files for the release you are installing from RSA Link (<https://community.rsa.com/>) to a local directory.
2. In the Security Analytics menu, select **Administration > System**.
3. In the left panel, select **Updates**.
4. In the **Settings** tab, make sure the **Enable** checkbox is not selected.
5. In the **Manual Updates** tab, click **Upload Files**.
The Upload File dialog is displayed.
6. Click **+** and browse to the local directory where you put the zip files and select the files.
The Update RPMs display in the **Manual Updates** tab.
The upload status is displayed in the lower left corner. When the upload is complete, Security Analytics server unzips all the RPM packages and displays them in the **Manual Updates** tab.
7. Select all files in the Manual Updates list and click **Apply**.
This moves the RPM files into the Local Update Repository on the Security Analytics Server and makes them available to hosts.
8. If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening RPM in Security Analytics, you must perform the following tasks on all components, including the Security Analytics server, to migrate it to 10.6.3.0.

Note: These steps apply only to STIG. Do not perform these steps for any non-STIG system, including FIPS.

- a. SSH to the host.
- b. `yum update glibc`

c. `reboot`

Review Version and License Status

Procedure

You display the Security Analytics software version, RSA license, and if there are new updates available.

To view the current status of Security Analytics:

1. In the **Security Analytics** menu, select **Administration > System**.
The System Information panel is displayed by default.
2. Click **Enable**.
If an update is found, the version is listed.

Monitor Health and Wellness of Security Analytics

The Health & Wellness module of Security Analytics provides an ability to:

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

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

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

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

The screenshot shows the Security Analytics user interface with the 'Health & Wellness' module selected. The interface includes a navigation bar with tabs for Administration, Hosts, Services, Event Sources, Health & Wellness, System, Security, and RSA Security Analytics. Below the navigation bar, there are sub-tabs for Alarms, Monitoring, Policies, System Stats Browser, Event Source Monitoring, and Settings. The 'Alarms' tab is active, displaying a table of alarm events.

Time	State	Severity	Rule Name	Service	Hostname	Stat
2015-05-04 11:57:46 PM	Cleared	High	Rule1430471443	Host		CPU Utilization
2015-04-29 06:13:24 PM	Active	High	Rule1430327310	Reporting Engine	SA	Garbage Collection Coun
2015-04-29 06:01:31 PM	Cleared	High	Rule1430326582	Log Decoder		Capture Packets Received
2015-04-24 05:41:59 AM	Active	Critical	IPDB Extractor Service in Bad State	IPDB Extractor	SA	Service State

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and an 'Auto Refresh' checkbox. The status bar at the bottom indicates the user is 'admin', the language is 'English (United States)', and the time zone is 'GMT+00:00'. There is also a 'Send Us Feedback' link.

Manage Policies

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

- Services and hosts to which the policy applies.
- Rules that specify statistical thresholds that govern alarms.

- When to suppress the policy.
- Who to notify when an alarm triggers and when to notify them.

For the related reference topics, see [Security Analytics Out-of-the-Box Policies](#)

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

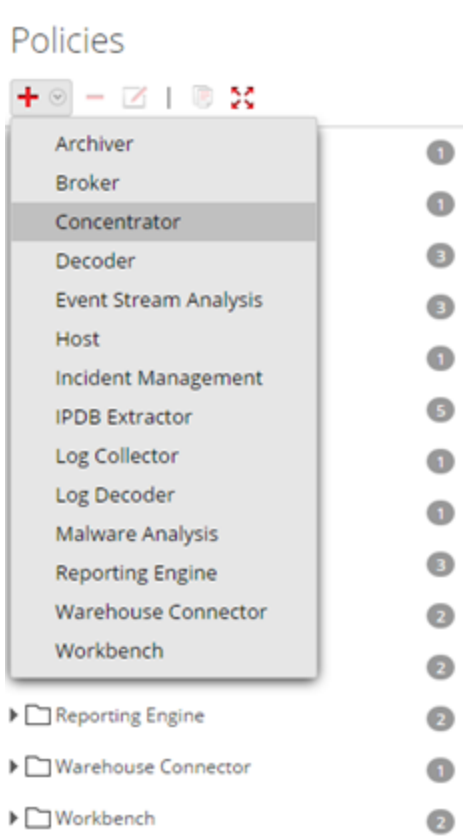
Procedures

Add a Policy

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.

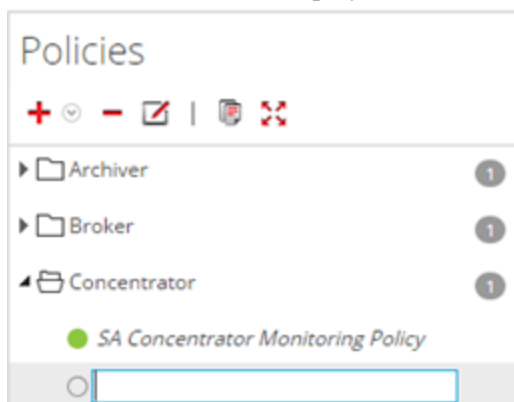
3. Click  in the **Policies** panel.

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

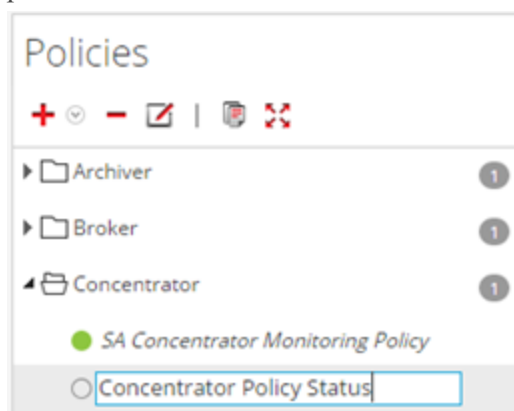


4. Select a host or service (for example, **Concentrator**).
For PKI policy, you must select a host (for example, Host).

The host or service is displayed in the Policies panel with a blank Policy Detail panel.



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

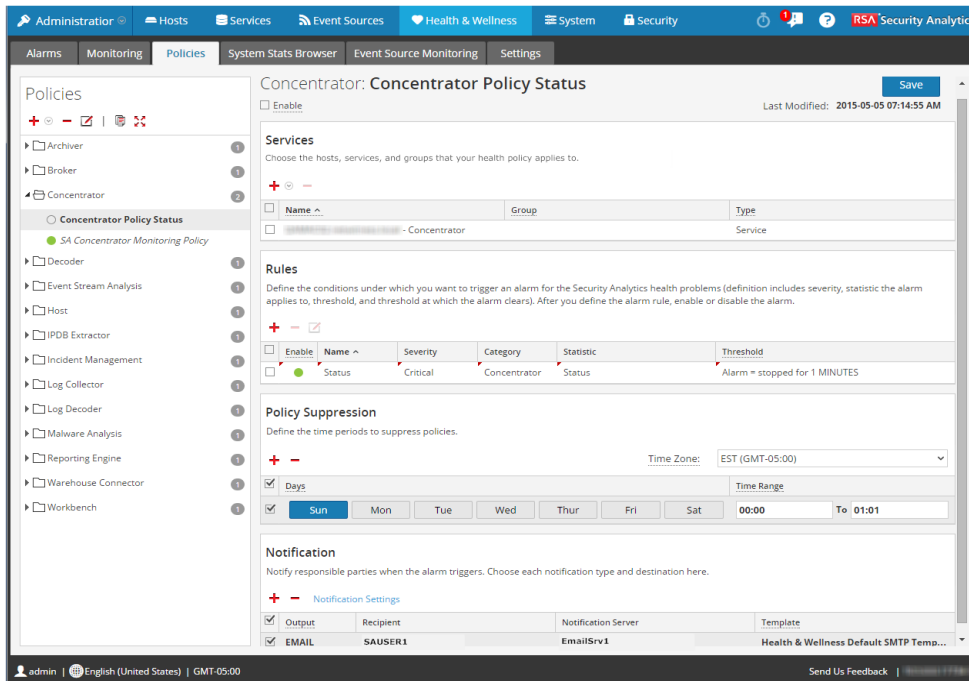


The name (for example, **Concentrator Policy Status**) is now displayed as the policy name in Policy Detail panel.

6. Create a Policy in the Policy Detail panel:
 - a. Select the **Enable** checkbox.
 - b. Add relevant services (in this example, any relevant Concentrator services) that you want to monitor for health statistics.

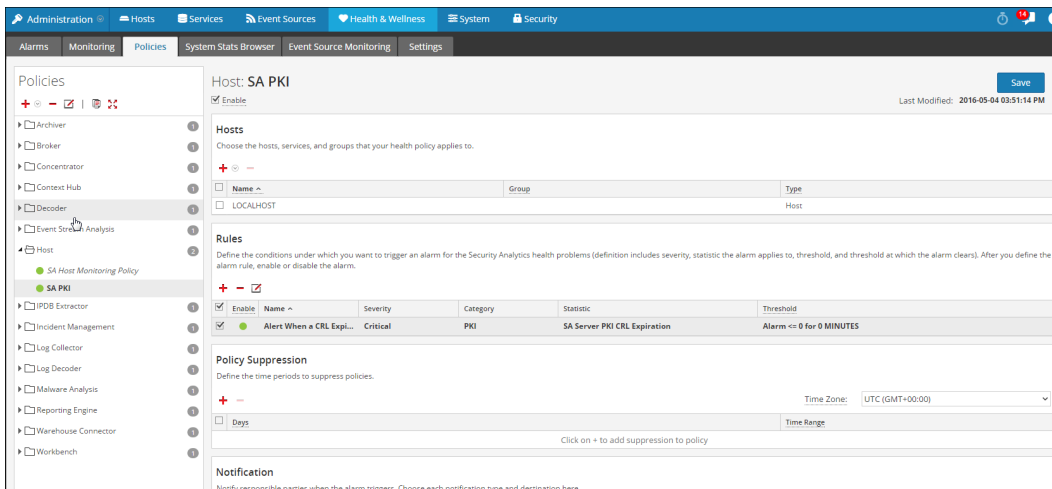
For PKI policy, you must select the LOCALHOST to monitor for health statistics.
 - c. Add relevant rule conditions you want to configure for the policy.
 - d. Suppress enforcement of the policy for the time periods you want.
 - e. Add any email notifications you want for the policy.

- f. Click **Save** in the Policy Detail panel.
The Policy is added.



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

1. Add a new PKI policy.



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

The 'Add Rule' dialog box is shown with the following configuration:

- Enable:**
- Name:** Trusted CA Certificate Expiry Time
- Description:** Enter Informational Text For This Rule And Any Possible Remediation Actions
- Severity:** High
- Statistic:** PKI, SA Server PKI Certificate Expiration, TRUSTED_CA
- Alarm Threshold:** <= 2400 For 0 Minutes
- Recovery Threshold:** > 2400 For 1 Minutes
- Rule Suppression:** + - Time Zone: UTC (GMT+00:00)
- Days:** Time Range:

Buttons: Cancel, Save

- For CRL Expiration

The 'Add Rule' dialog box is shown with the following configuration:

- Enable:**
- Name:** CRL Expiration Based On Time
- Description:** Enter Informational Text For This Rule And Any Possible Remediation Actions
- Severity:** High
- Statistic:** PKI, SA Server PKI CRL Expiration
- Alarm Threshold:** <= 2400 For 0 Minutes
- Recovery Threshold:** > 1 For 1 Minutes
- Rule Suppression:** + - Time Zone: UTC (GMT+00:00)
- Days:** Time Range:

Buttons: Cancel, Save

- For CRL Status


The 'Add Rule' dialog box is shown with the following configuration:

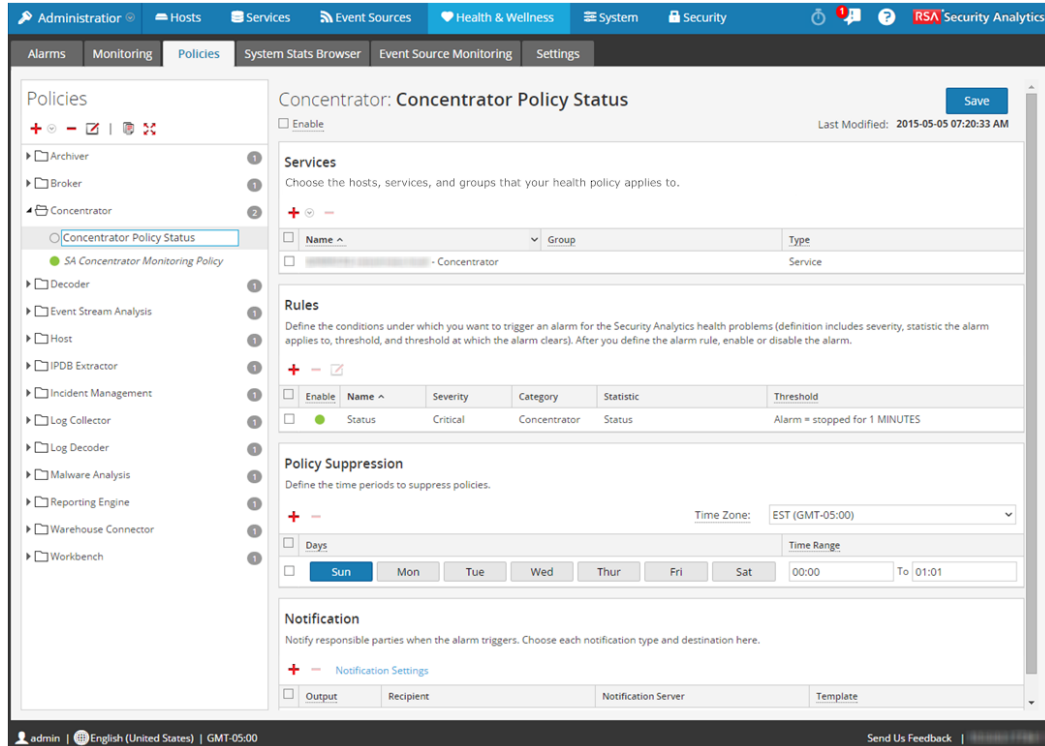
- Enable:**
- Name:** CRL Status
- Description:** Enter Informational Text For This Rule And Any Possible Remediation Actions
- Severity:** High
- Statistic:** PKI, SA Server PKI CRL Status
- Alarm Threshold:** != Valid For 0 Minutes
- Recovery Threshold:** = Valid For 1 Minutes
- Rule Suppression:** + - Time Zone: UTC (GMT+00:00)
- Days:** Time Range:

Buttons: Cancel, Save

- For Server Certificate Expiration

Edit a Policy

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **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, **Concentrator Performance Status**) and policy detail panel become editable.



5. Make the required changes and click **Save** in the Policy Detail panel. You can:

- Edit the Policy name.
- Enable or disable the policy.
- Add or delete hosts and services in the policy.
- Add, delete or modify rules in the policy.
- Add/Edit/Delete suppressions in the policy.
- Add/Edit/Delete notifications in the policy.

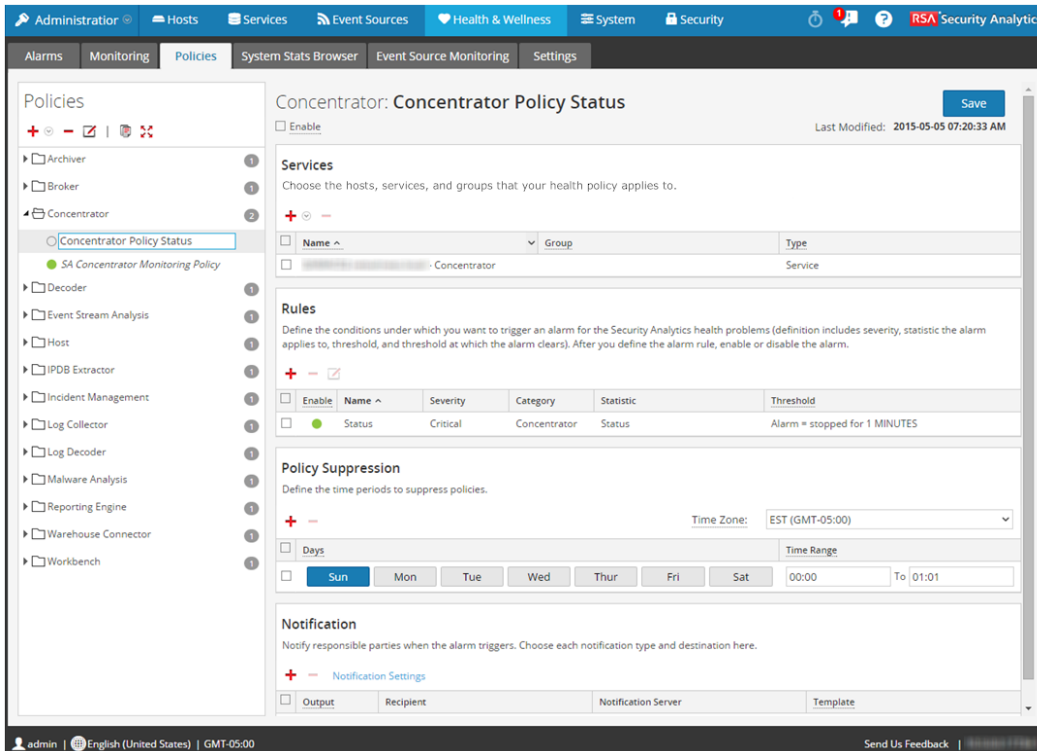
Note: **Save** applies the policy rules based on the selection of enable/disable. It also resets the rule condition timers for changed rules, and the entire Policy.


Duplicate a Policy

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.
3. Select a policy (for example, **Concentrator Policy Status**) under a host or service.

- Click .

Security Analytics copies the policy and lists it with **(1)** appended to the original policy's name.



- Click  and rename the Policy [for example, rename **Concentrator Policy Status (1)** to **Concentrator Policy Status 2**].

Note: A duplicated policy is disabled by default and the host and service assignments are not duplicated.
Please assign any relevant hosts and services to the duplicated policy before you use it to monitor health and wellness of the Security Analytics infrastructure.

Assign Services or Groups

To assign hosts or services to a policy:

- In the **Security Analytics** menu, select **Administration > Health & Wellness**.
- Click **Policies** tab.
The Policies view is displayed.
- Select a policy (for example, **First Policy**) under a host or service.
The Policy Detail is displayed.

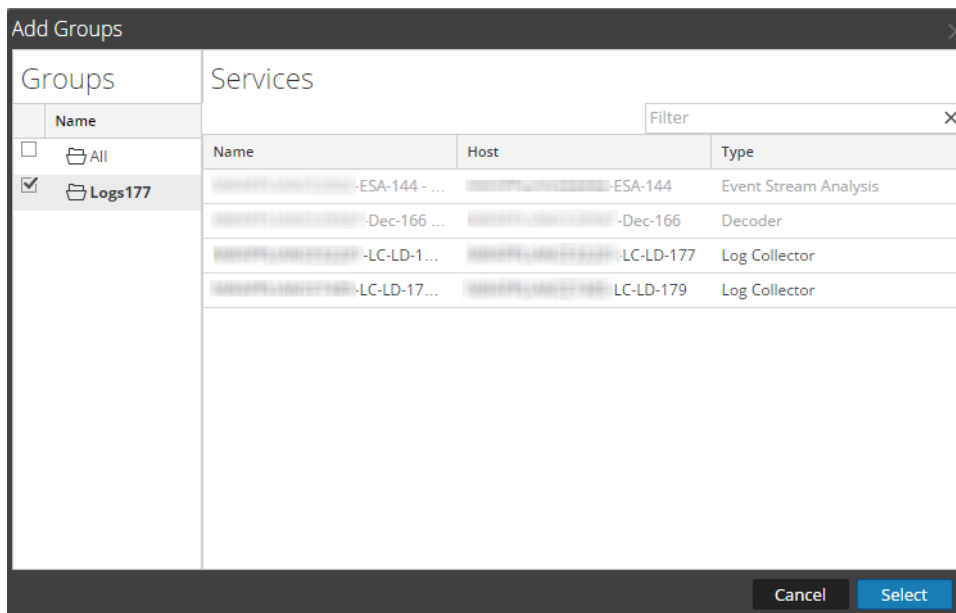
4. Click  in the Services and Groups list toolbar.

5. For:

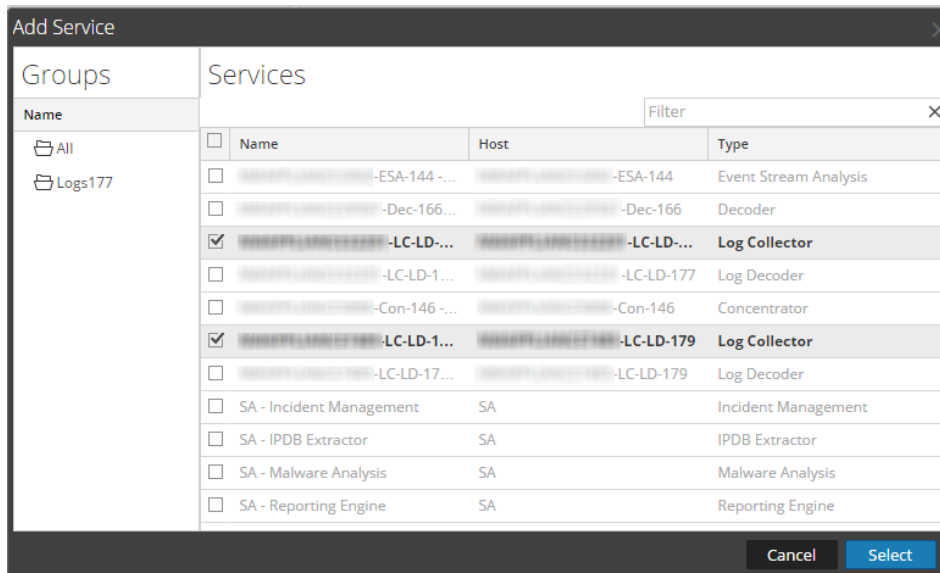
- Hosts, select **Groups** or **hosts** from the selection menu.
- Services, select **Groups** or **Services** from the selection menu.

If you selected:

- **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.



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

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

Remove Services or Groups

To remove a host or service from a policy:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.
3. Select a policy under a service.
The Policy Detail is displayed.
4. Select a host or service.

Services

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

+ ⓘ -

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	All	Group
<input checked="" type="checkbox"/>	CONCENTRATOR SERVICES - Concentrator	Service

5. Click **-**.
The host or service is removed from the policy.

Services

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

+ ⓘ -

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	All	Group

Add a Rule

To add a rule to a policy:

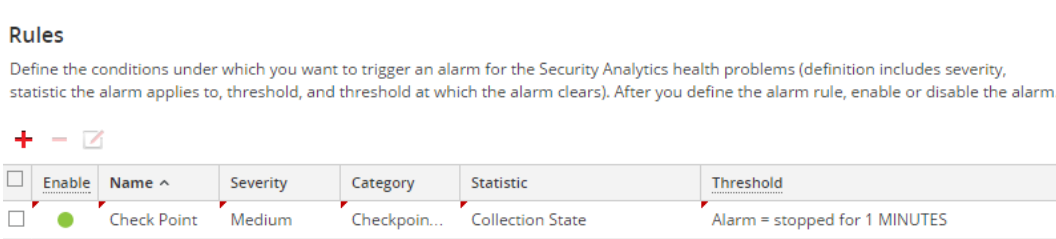
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.

3. Select a policy (for example, **Checkpoint**) under a host or service.
The Policy Detail is displayed.
4. Click **+** in the Rules list toolbar.
The Add Rule dialog is displayed.
5. Complete the dialog to define the rule.

In Security Analytics 10.5.0.1, add the **Description** field as shown in the following example.

6. Click **OK**.

The rule is added to the policy.



Edit a Rule

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

2. Click **Policies** tab.

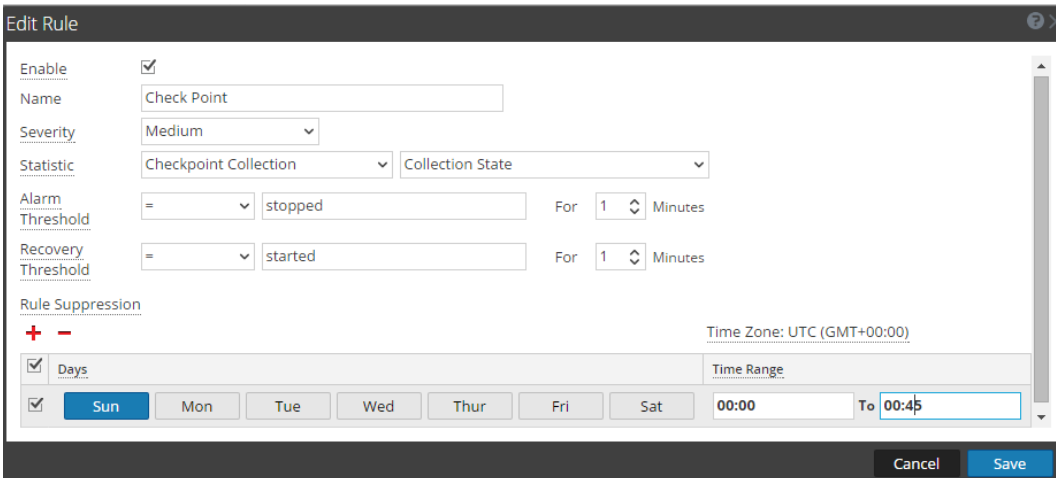
The Policies view is displayed.

3. Select a policy under a host or service.

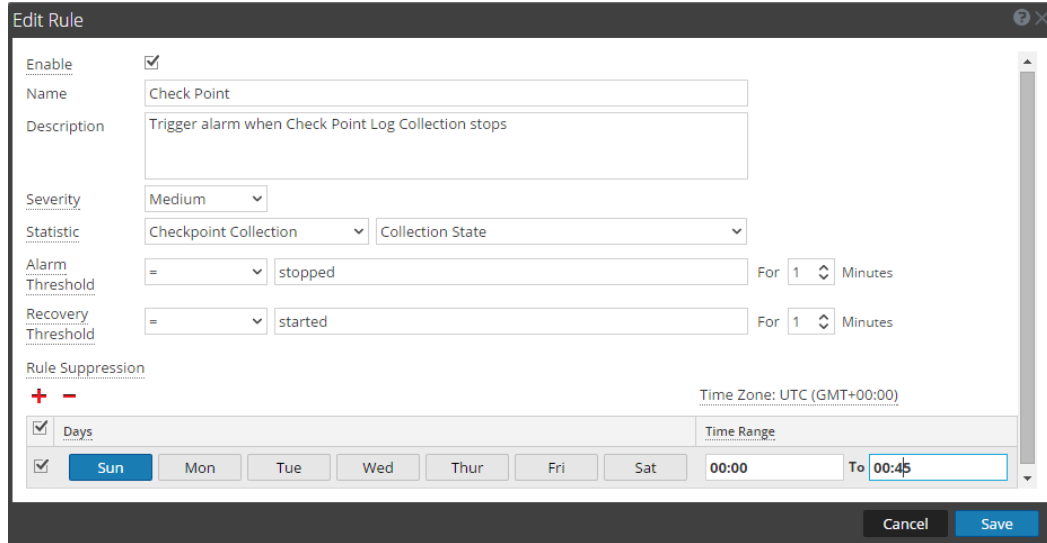
The Policy Detail is displayed.

4. Select a rule from the Rules list and click .

The Edit Rule dialog is displayed.



In Security Analytics 10.5.0.1, added the **Description** field in as shown in the following example.

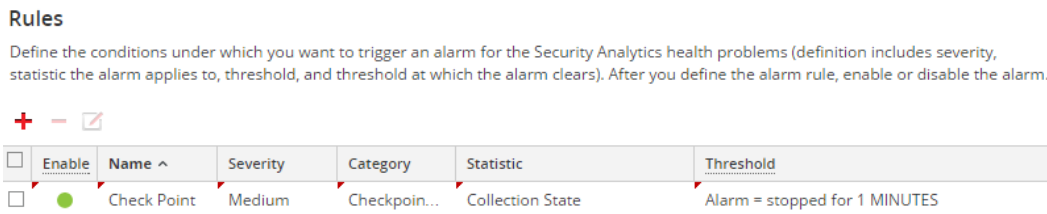


5. Make the required changes and click **Save**.

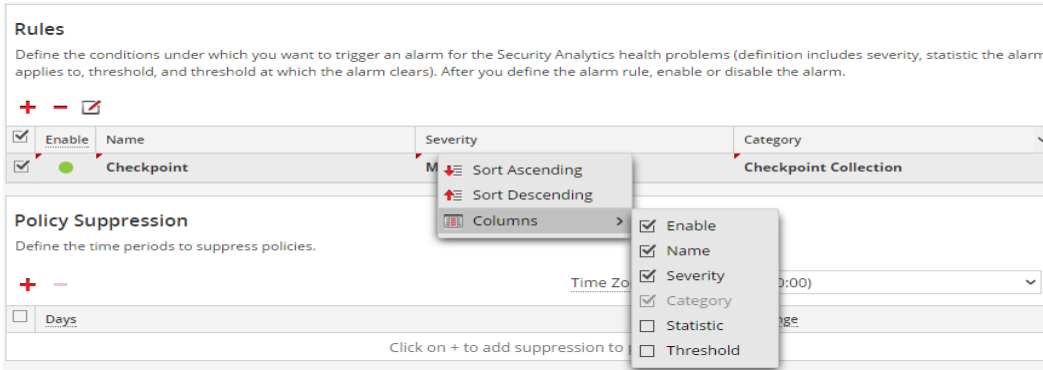
Hide/Show Rule Conditions

To hide or show rule conditions:

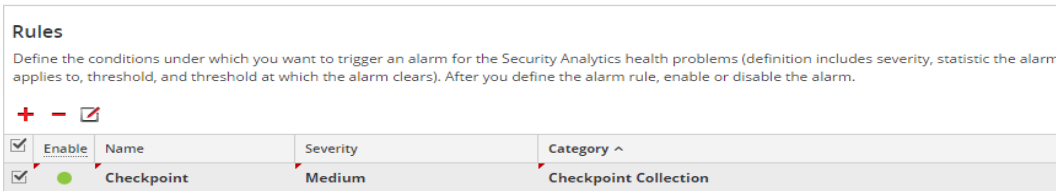
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.
3. Select a policy under a service.
The Policy Detail is displayed.
4. Go to the **Rules** panel.



5. Click **✓** to the the right of **Category** and uncheck the **Static** and **Threshold** rule conditions.
You can check or uncheck any Rules column to show or hide it.



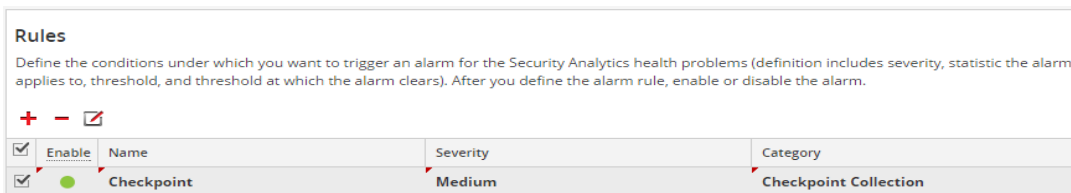
The **Rules** panel displays without the rule conditions.



Delete a Rule

To remove a host or service from a policy:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click **Policies** tab.
The Policies view is displayed.
3. Select a policy under a service.
The Policy Detail is displayed.
4. Select a rule from the **Rules** list (for example, **Checkpoint**).



5. Click **[-]**.
The rule is removed from the policy.

Suppress a Rule

1. Click the **Policies** tab.
The Policies view is displayed.

2. Select a policy under a service.
The Policy Detail is displayed. You can specify rule suppressions time ranges when you initially add it or you can edit the rule and specify suppression time ranges.
3. Add or edit a rule.
4. In the **Rules Suppression** panel of the **Add** or **Edit Rule** dialog, specify the days and time ranges during which you want the rule suppressed. In the following example, the rule is suppressed on Sundays from 12AM to 12:30AM and on Saturdays from 2:30AM to 3:30 AM.

Rule Suppression

+ **-** Time Zone: UTC (GMT+00:00)

<input type="checkbox"/> Days	Time Range
<input type="checkbox"/> Sun Mon Tue Wed Thur Fri Sat	00:00 To 00:30
<input checked="" type="checkbox"/> Sun Mon Tue Wed Thur Fri Sat	02:30 To 03:30

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. In the following example, the policy is suppressed on Fridays from 7:30AM to 7:45AM.

Policy Suppression

Define the time periods to suppress policies.

+ **-** Time Zone: UTC (GMT+00:00)

<input checked="" type="checkbox"/> Days	Time Range
<input checked="" type="checkbox"/> Sun Mon Tue Wed Thur Fri Sat	07:30 To 07:45

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.

Notification			
Notify responsible parties when the alarm triggers. Choose each notification types and destinations here.			
+ - Notification Settings			
<input type="checkbox"/>	Type	Recipient	Notification Server
<input type="checkbox"/>	EMAIL	Select Notification	Select Notification Server
			Select Template

b. Select the email:

- Notification types in the Notification column (see **Configure Notification Outputs** in the *RSA Security Analytics 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 *RSA Security Analytics System Configuration Guide* for the source of the values in this drop-down list).
- Template server in the Notification Server column (see **Configure Notification Templates** in the *RSA Security Analytics System Configuration Guide* for the source of the values in this drop-down list).

Notification			
Notify responsible parties when the alarm triggers. Choose each notification type and destination here.			
+ - Notification Settings			
<input checked="" type="checkbox"/>	Output	Recipient	Notification Server
<input checked="" type="checkbox"/>	EMAIL	SAUSER1	EmailSrv1
			Health & Wellness Default SMTP ...

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.

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.

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

+ - [Notification Settings](#)

<input checked="" type="checkbox"/> Output	Recipient	Notification Server	Template
<input checked="" type="checkbox"/> EMAIL	SAUSER1	EmailSrv1	Health & Wellness Default SMTP ...

- b. Click - .

The notification is removed.

Include the Default Email Subject Line

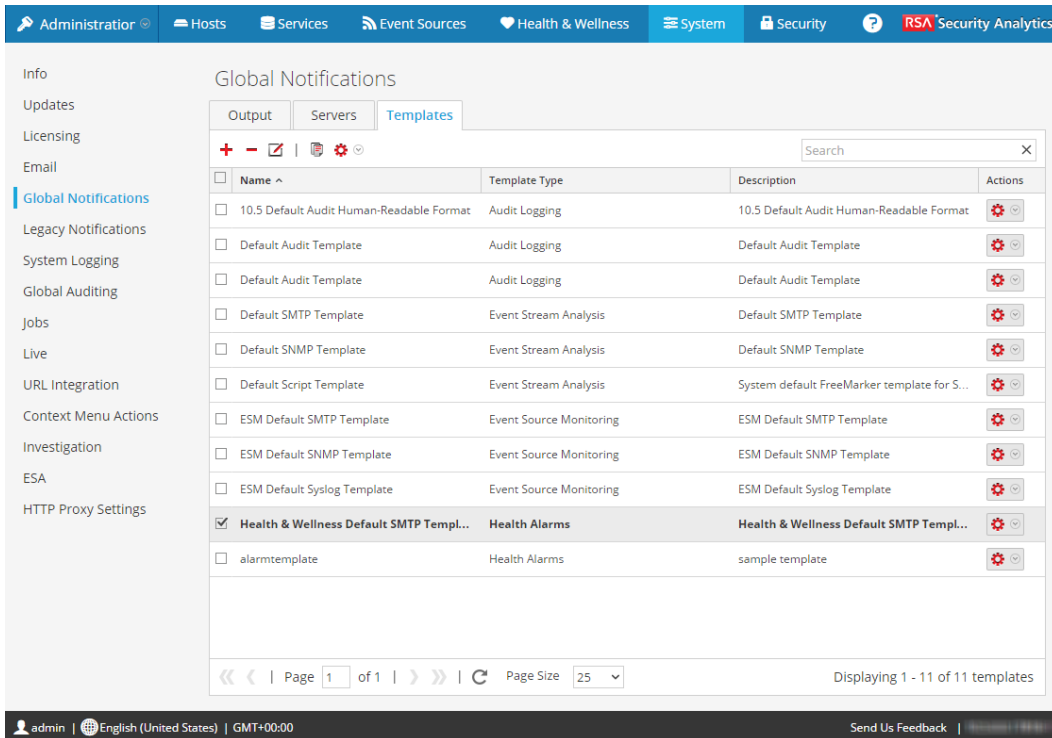
The emails generated by the notifications you set up for policies do not include the subject line from the Health & Wellness Default Email Notification templates. You need to specify the subject line in the do not include subject lines. This procedure shows you how to insert a subject line into the templates.

For related reference topics, see [Policies View](#) and [Security Analytics Out-of-the-Box Policies](#)

Procedure

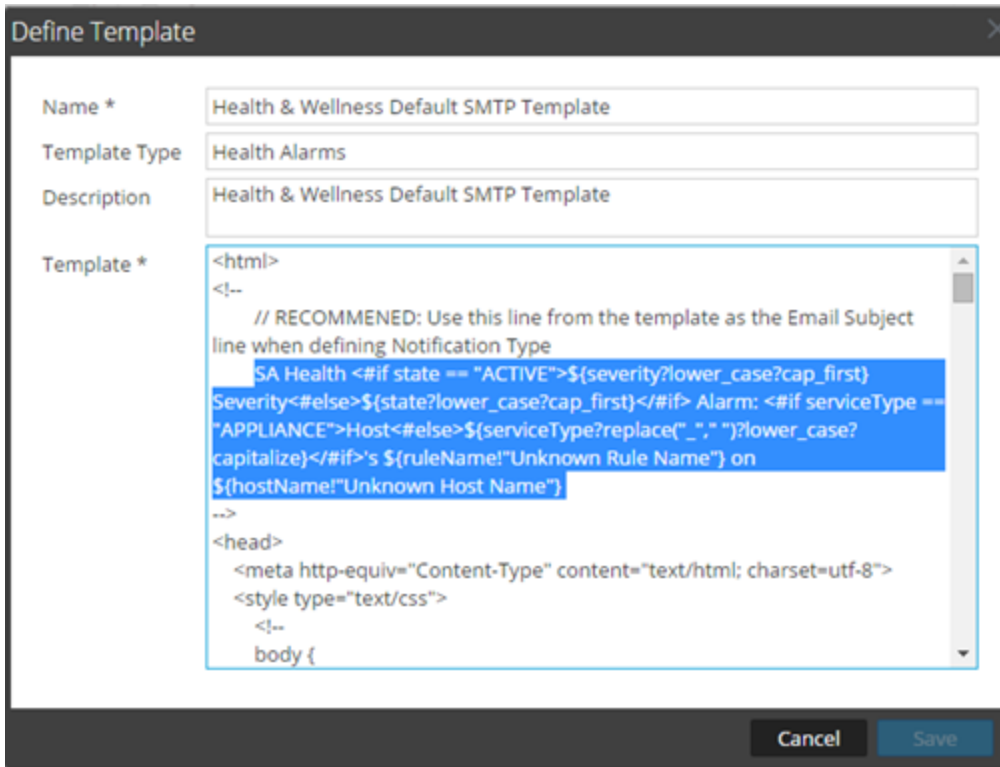
To include the subject line from a Health & Wellness email template in your email notification:

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

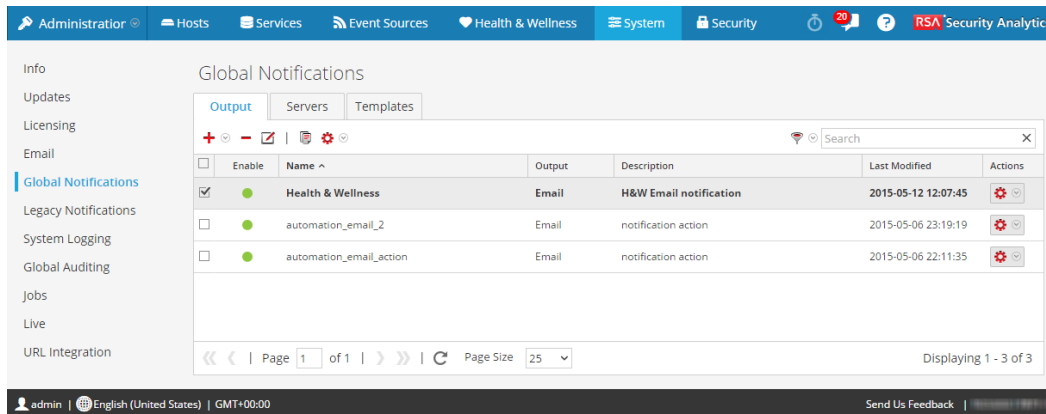


The Define Template dialog is displayed.

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



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



- Click

The **Define Email Notification** dialog is displayed.

- Replace the value in **Subject** field text box with the subject line that you have in the buffer (highlight the existing text and press **Ctrl-V**).

Define Email Notification

Enable

Name *

Description

To Email Addresses *

Subject *

Cancel Save

- Click **Save**.

Monitor Alarms

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

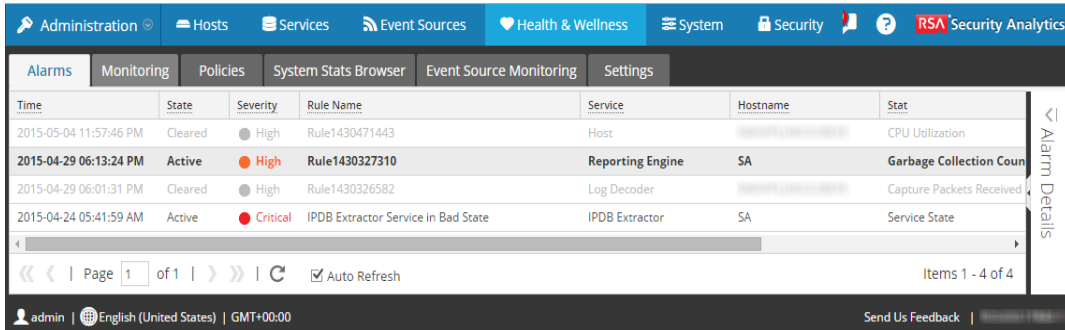
You set up the parameters for alarms in [Manage Policies](#)

For the related reference topic, see [Alarms View](#).

To monitor the alarms set up in Security Analytics:

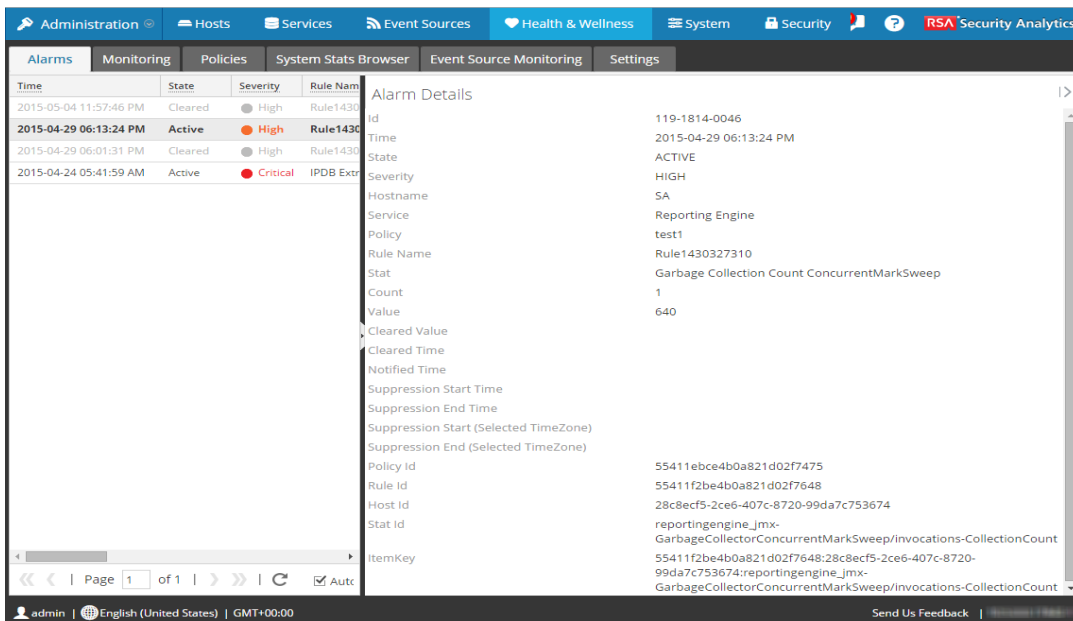
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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 Event Sources

The event source monitoring feature of Security Analytics provides the following functionalities:

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

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

Configure Event Source Monitoring

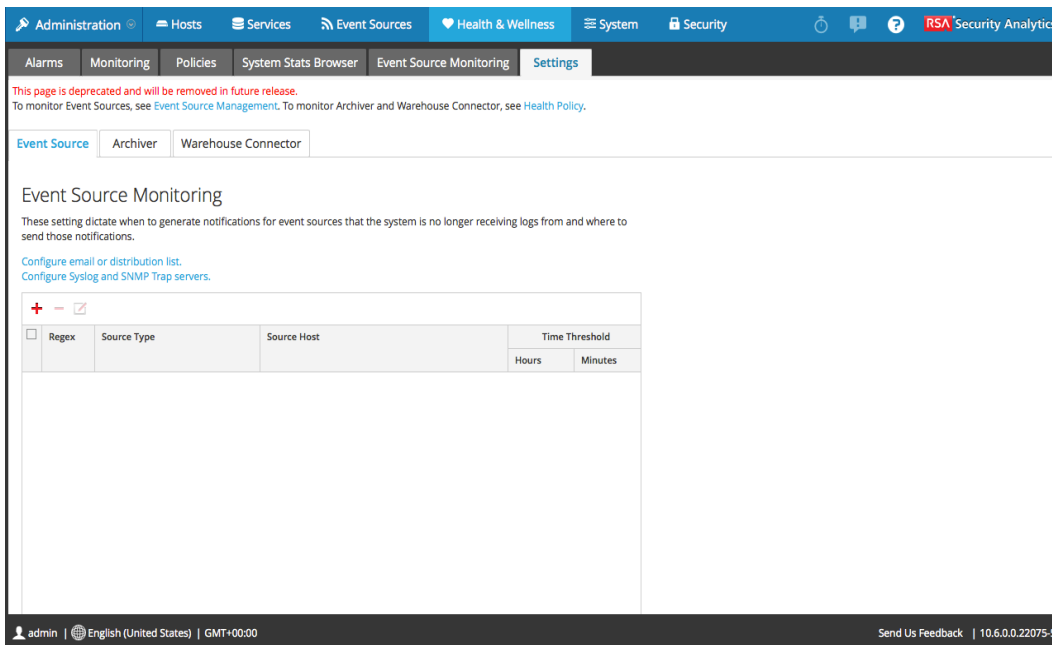
To monitor event sources you have to configure the event sources so that they generate and send out notifications when required. For the related reference topic, see [Health and Wellness Settings Tab - Event Sources](#)

Procedures

Configure and Enable Event Monitoring

To configure and enable event monitoring in Security Analytics:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Select **Settings > Event Source**.
The Event Source tab is displayed.



3. Under **Event Source Monitoring**, click **+** .
The Add/Edit Source Monitor dialog is displayed.
4. Define the **Source Type**, **Source Host**, and **Time Threshold** for the source of the event source that you want to monitor to detect when Security Analytics stops receiving logs from it. If you do not specify a **Time Threshold**, Security Analytics monitors the event source until you set a threshold.

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

The screenshot shows a dialog box titled "Add/Edit Source Monitor". It includes a checkbox for "Regex", a text input field for "Source Type *", a larger text input field for "Source Host *", and two spinners for "Time Threshold *" with labels "Hours" and "Minutes". At the bottom are "Cancel" and "OK" buttons.

5. Click **OK**.

The event source is displayed in the panel.

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

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

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

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

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

7. Click **Apply**.

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

For details on various parameters and description in the Event Source Monitoring settings view, see [Event Source Monitoring View](#).

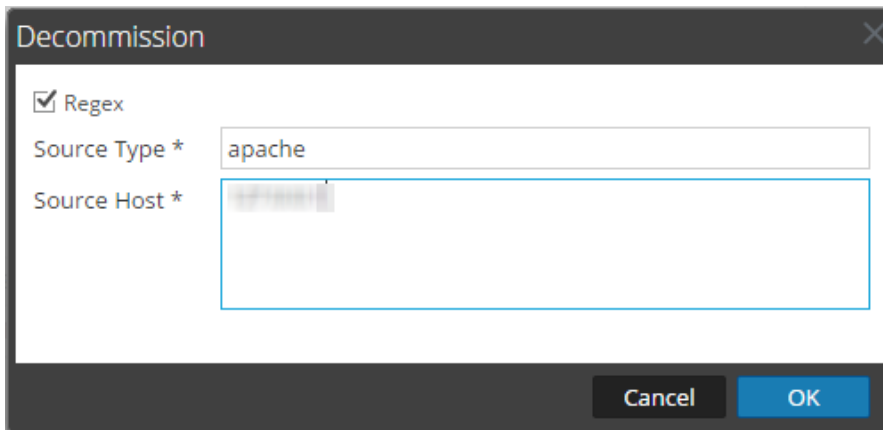
Decommission Event Source Monitoring

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

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

To decommission event source monitoring for an event source:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Select **Settings > Event Source**.
The **Event Source** tab is displayed.
3. Under **Decommission**, click **+**.
The **Decommission** dialog displays.
4. Define the **Source Type** and the **Source Host** for the source for which you want to decommission event monitoring notifications.



The screenshot shows a dialog box titled "Decommission". It has a close button in the top right corner. Inside the dialog, there is a checked checkbox labeled "Regex". Below this, there are two text input fields. The first is labeled "Source Type *" and contains the text "apache". The second is labeled "Source Host *" and is currently empty. At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

Filter Event Sources

You can choose a filter to display:

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

Procedure

To filter the list of event sources:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Select **Event Source Monitoring**.
3. Filter the list in one of the following ways:

- To view the events generated by a particular event source, type the required event source in the **Event Source** field. Select **Regex** to enable Regex filter and click **Apply**. It performs a regular expression search against text and lists out the specified category. This field also supports globbing pattern matching.

All events generated by the Event Source specified are displayed.

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Last Update	Historical
1.1.1.5	unknown	0	NWAPPLIANCE32201-LC-LD-177	200	33 days, 5 hours, 49 ...	2015-01-29 11:13:1...	2015-03-03 01:58:28 ...	
10.63.21.23	checkpointfw1	NWAPPLIANCE32201-LC-LD-177	NWAPPLIANCE32201-LC-LD-177	17756318	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	
10.63.21.23	unknown	NWAPPLIANCE32201-LC-LD-177	NWAPPLIANCE32201-LC-LD-177	3900429	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	
10.63.21.23	winevent_nic	NWAPPLIANCE32201-LC-LD-177	NWAPPLIANCE32201-LC-LD-177	2701253	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	
10.31.204.100	apache	NWAPPLIANCE32201	NWAPPLIANCE32201-LC-LD-177	3564600	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	
127.0.0.1	apache	NWAPPLIANCE32201	NWAPPLIANCE32201-LC-LD-177	9969924	8 days, 12 hours, 54 ...	2015-02-23 04:07:3...	2015-03-03 01:58:28 ...	
10.31.204.100	unknown	NWAPPLIANCE32201	NWAPPLIANCE32201-LC-LD-177	223976	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	
10.31.204.20	unknown	NWAPPLIANCE32201	NWAPPLIANCE32201-LC-LD-177	82000	39 days, 9 hours, 27 ...	2015-01-23 07:34:4...	2015-03-03 01:58:28 ...	

- To view events collected from a particular Log Collector, select a Log Collector from the drop-down list and click **Apply**.

A list of all events being collected from the specified Log Collector from various event sources is displayed.

Note: Similarly you can also choose the following filters:

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

For details on various parameters and description see [Event Source Monitoring View](#) .

Create Historical Graph of Events Collected for an Event Source

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

Procedure

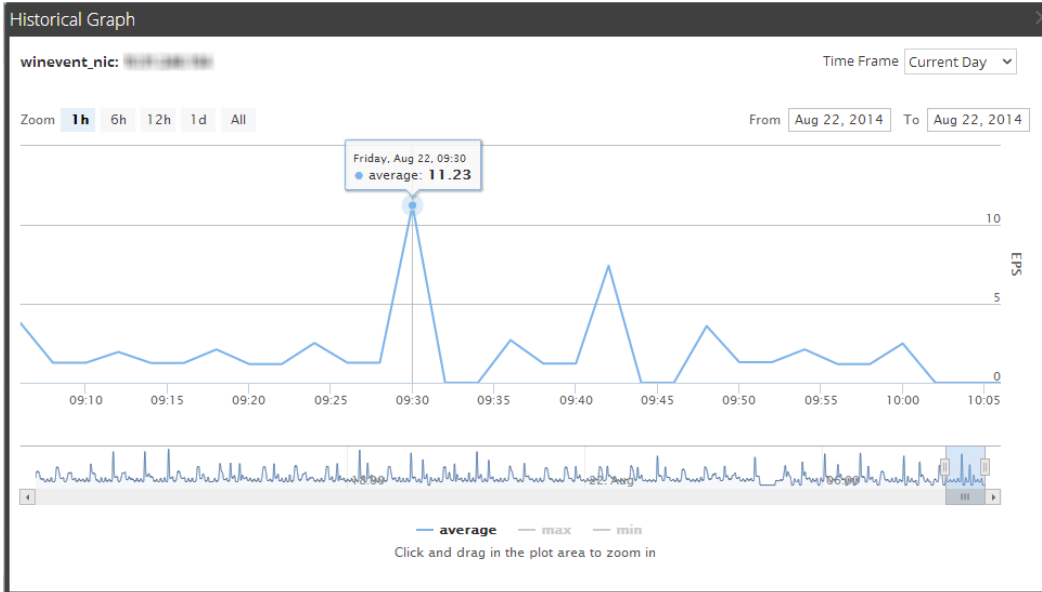
To create an historical graph:

- In the **Security Analytics** menu, select **Administration > Health & Wellness**.
The Health & Wellness view is displayed with the Monitoring tab open.
- Click **Event Source Monitoring**.
The Event Source Monitoring view is displayed.

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

The Historical graph for the selected event source is displayed.

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



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

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

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

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

Monitor Health and Wellness Using SNMP Alerts

You can monitor a Security Analytics component to proactively alert using Simple Network Management Protocol (SNMP) based on the thresholds or system failures.

You can monitor the following for Security Analytics components:

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

SNMP Configuration

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

Thresholds

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

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

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

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

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

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

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

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

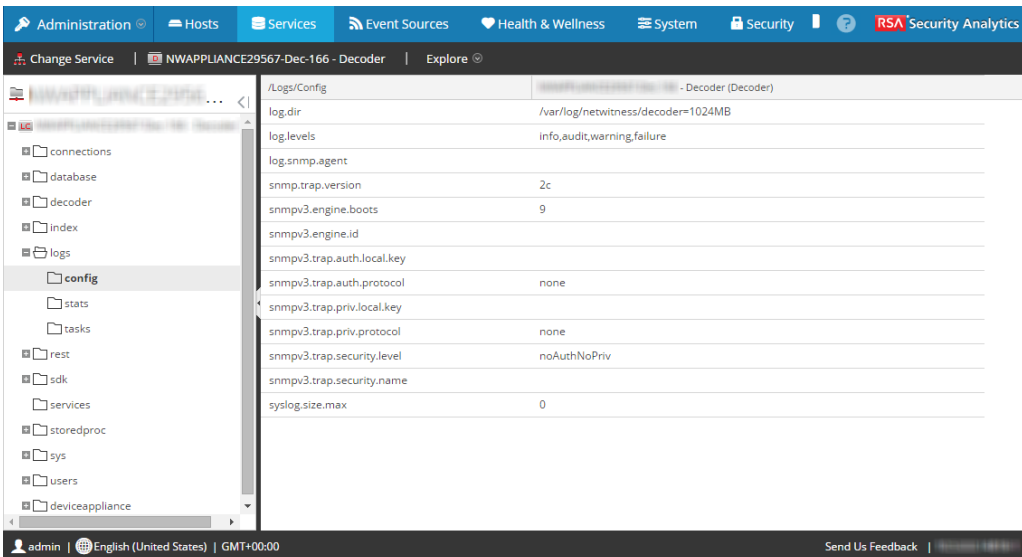
```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu  
old=77% new=91
```

Procedures

Configure SNMPv3 for a Host

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.
2. Select the service.
3. In the Actions column, select **View > Explore**.

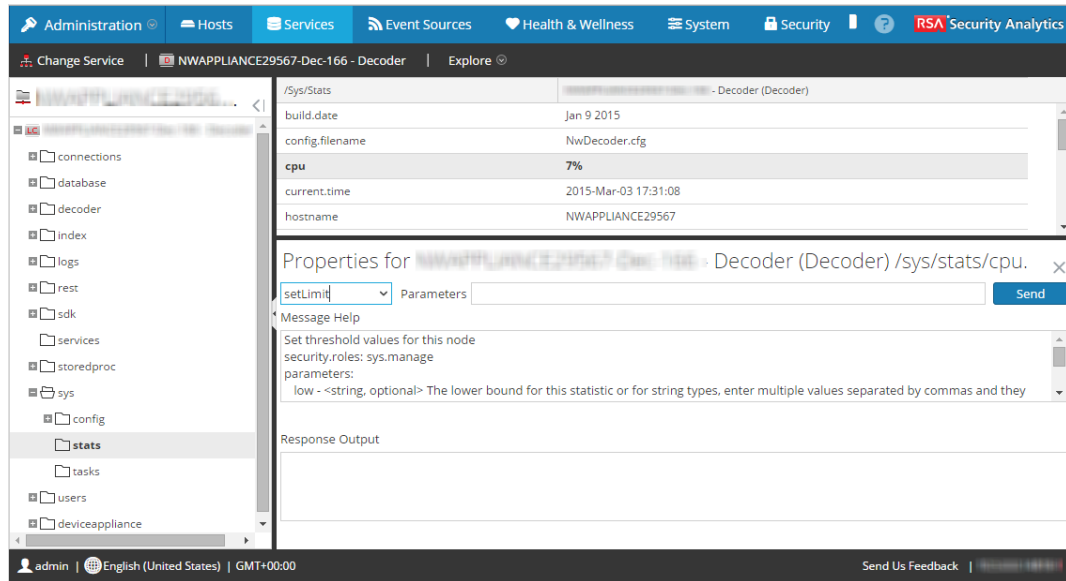
- In the nodes list, expand the list and select a config folder. For example, **log > config**
- Set the SNMPv3 configuration.



Set the Threshold for a Service

- In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.
- Select the service.
- In the Actions column, select **View > Explore**.
- In the nodes list, expand the list and select a stat folder.
- Select a stat, for example, **cpu**, and right-click.
- From the drop-down menu, select **Properties**.
The Properties dialog is displayed. The Properties dialog has a drop-down list of available

messages for the parameter.



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

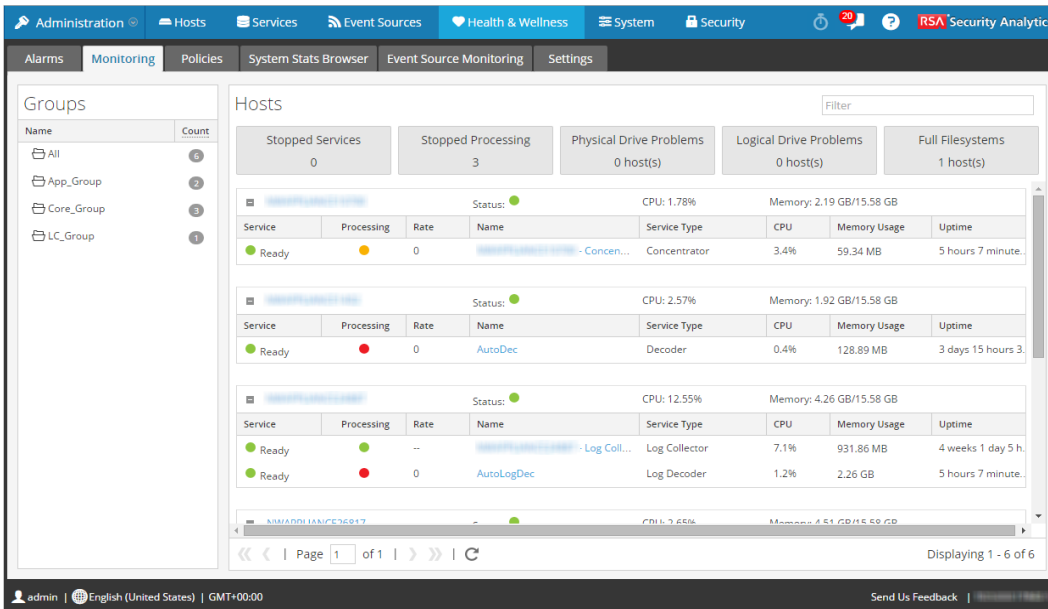
Monitor Hosts and Services

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

Procedure

To monitor hosts and services in Security Analytics:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
The Health & Wellness view is displayed with the Alarms tab open.
2. Select the **Monitoring** tab.
A list of all hosts and their associated services that belong to the group **All** is displayed by default.
The operational status, CPU usage, and memory usage for each host is displayed.



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

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

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

Filter Hosts and Services in the Monitoring View

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

- Hosts belonging to a particular group
- Specific host and its associated services
- Hosts whose services are stopped
- Hosts whose services have stopped processing or processing has been turned off
- Hosts that have Physical drive problems
- Hosts that have Logical drive problems
- Hosts that have Full File systems

For the related reference topic, see [Monitoring View](#)

Procedure

To filter hosts and services:

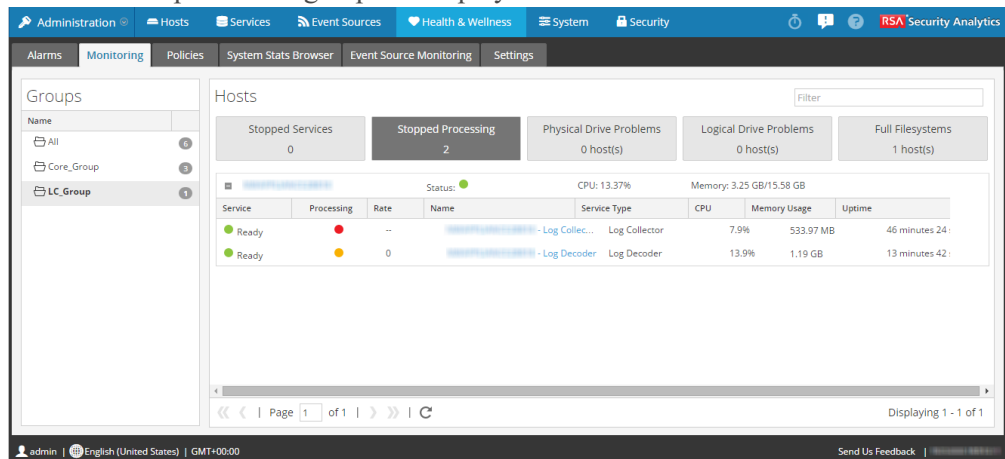
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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

2. Select the **Monitoring** tab.
3. Filter the hosts and services in one of the following ways:
 - To view a list of hosts and their associated services belonging to a particular group, select the group in the Groups panel.
All hosts and their associated services belonging to the specified group are displayed in the Hosts panel.

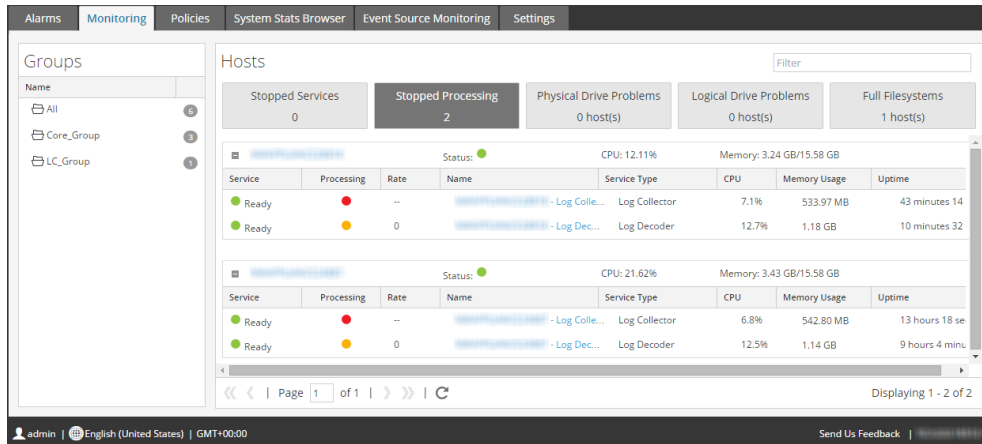
Note: The grouping of hosts is derived from the groups created in the Administration page. Any/All groups created in the Administration page are displayed here.

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



- To view a list of all services that have stopped processing, click **Stopped Processing** in the Hosts panel.
A list of all the hosts that have at least one service with the status as stopped processing is displayed.

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



Note: In a similar way you can filter the list of hosts and the associated services by choosing the right filter

- Click Stopped Services to display a list of all stopped services.
- Click Physical Drive Problems to display a list of host with Physical Drive Problems.
- Type the host name in the Filter box to display only the required host and the services running on the host.

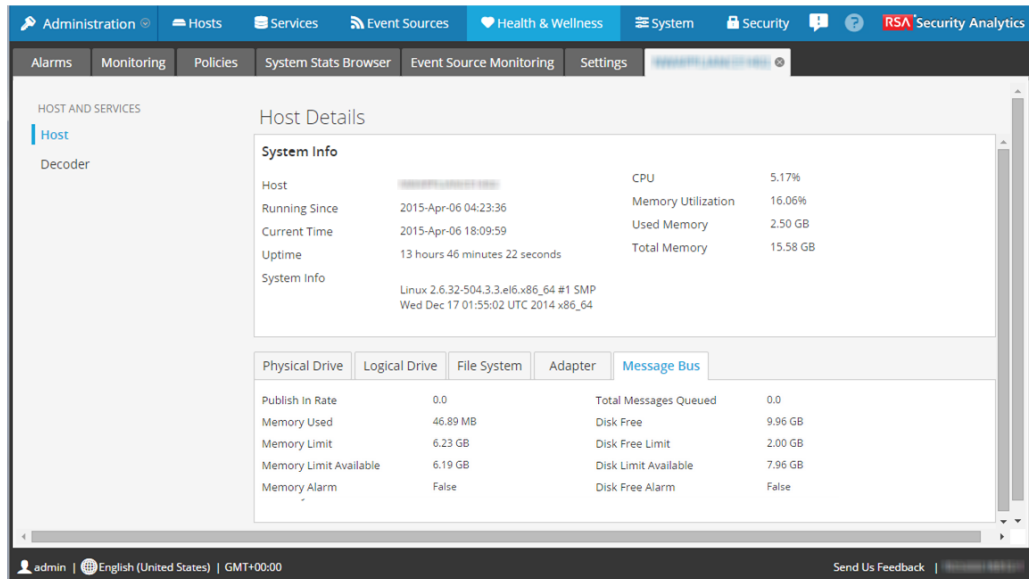
Monitor Host Details

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

Procedure

To view host details:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
The Health & Wellness view is displayed with the Alarms tab open.
2. Select the **Monitoring** tab.
3. Click a host in the **Hosts** panel.
The Host Details view is displayed as a new page.




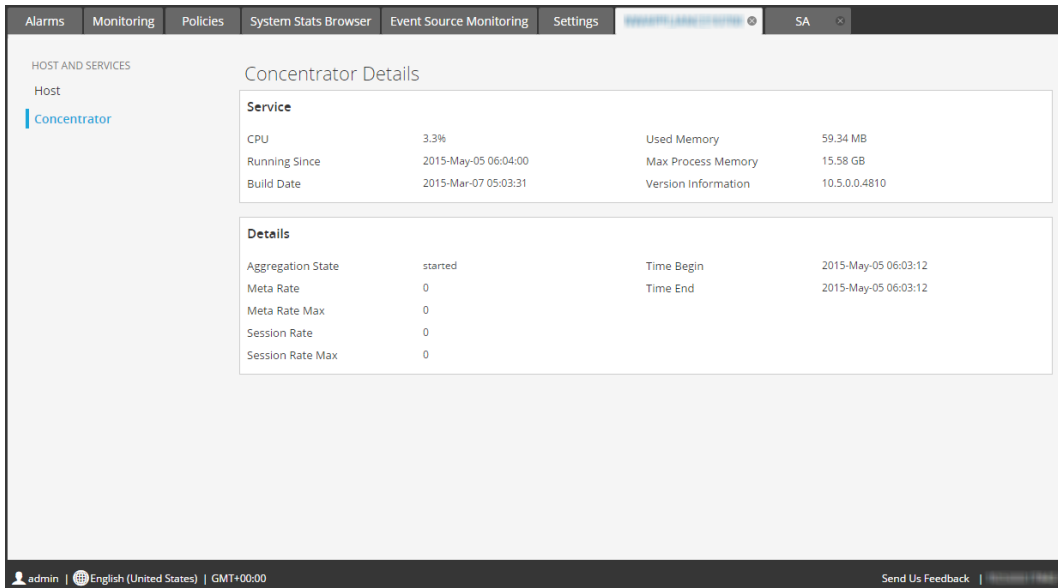
Monitor Service Details

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

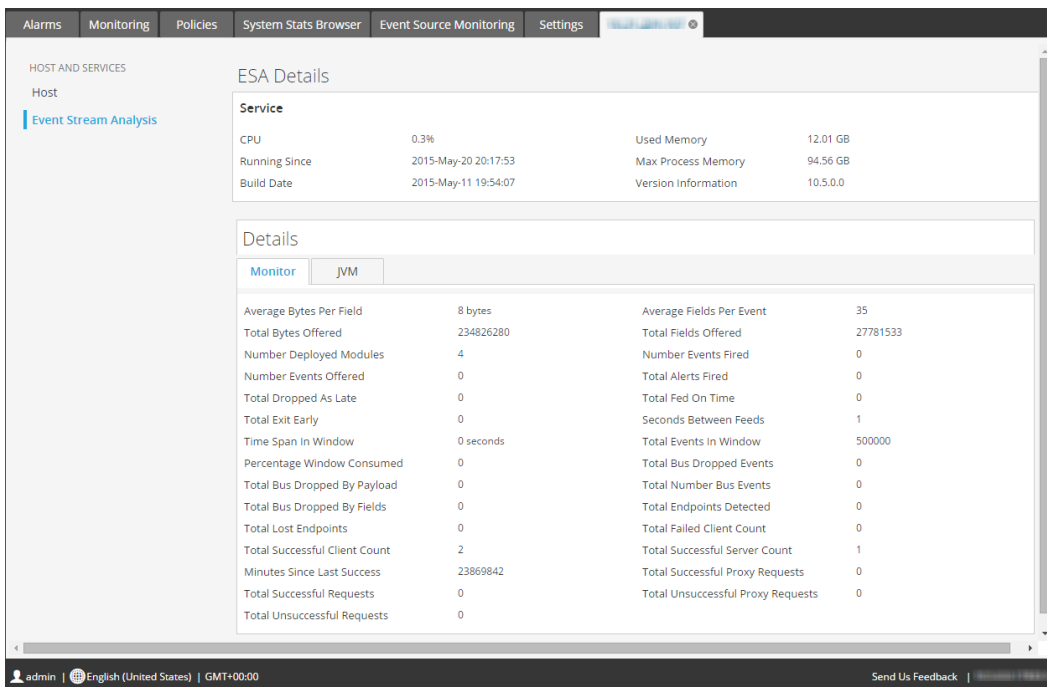
Procedure

To view service details:

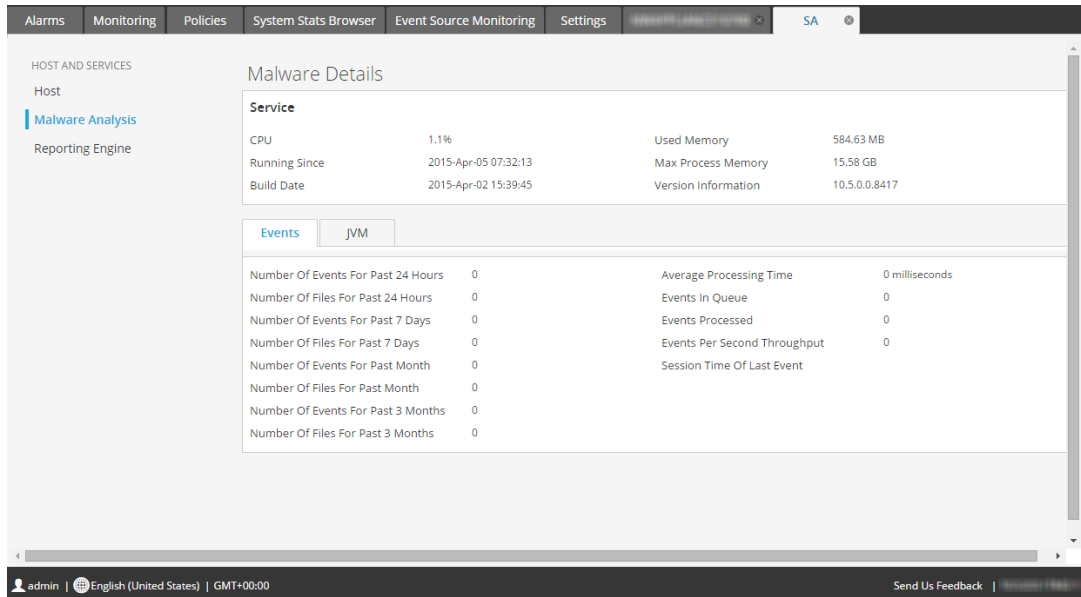
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
The Health & Wellness view is displayed with the Alarms tab open.
2. Select the **Monitoring** tab.
3. Click  for a host in the Hosts panel.
A list of services running on the host is displayed.
4. Click on any service.
The service details view is displayed as a new page. The Archiver, Broker, Concentrator, and Decoder service details views have the **Service** and **Details** panels.



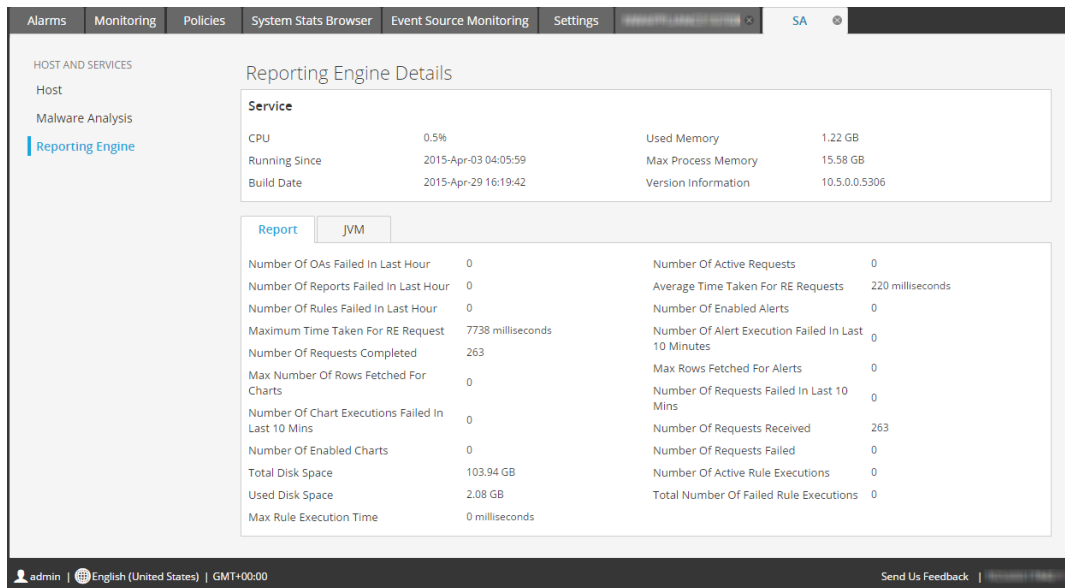
The Event Stream Analysis (ESA) service details view has the **Service** panel plus the **Monitor** and **JVM** tabs that show additional statistics.



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



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



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

Refer to [Monitoring View](#) for a detailed description of the Details view for each service.

Monitor Service Statistics

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

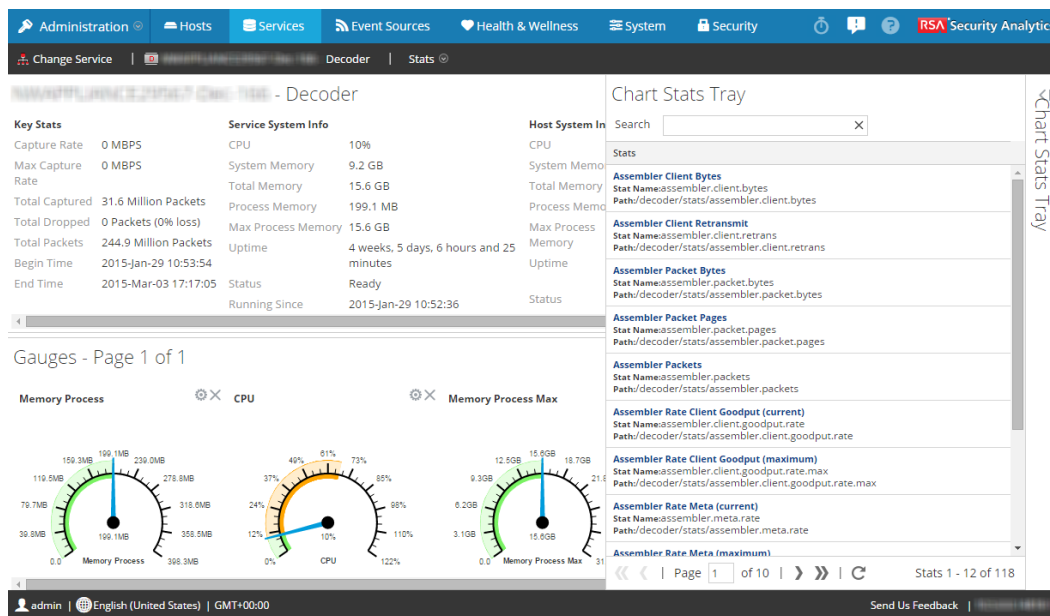
Although different statistics are available for different types of services, certain elements are common for any Core device.

Procedure

To monitor service statistics in Security Analytics:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.
2. Select a service, and select **View > Stats** in the Actions column.





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


Add Statistics to a Gauge or Chart

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

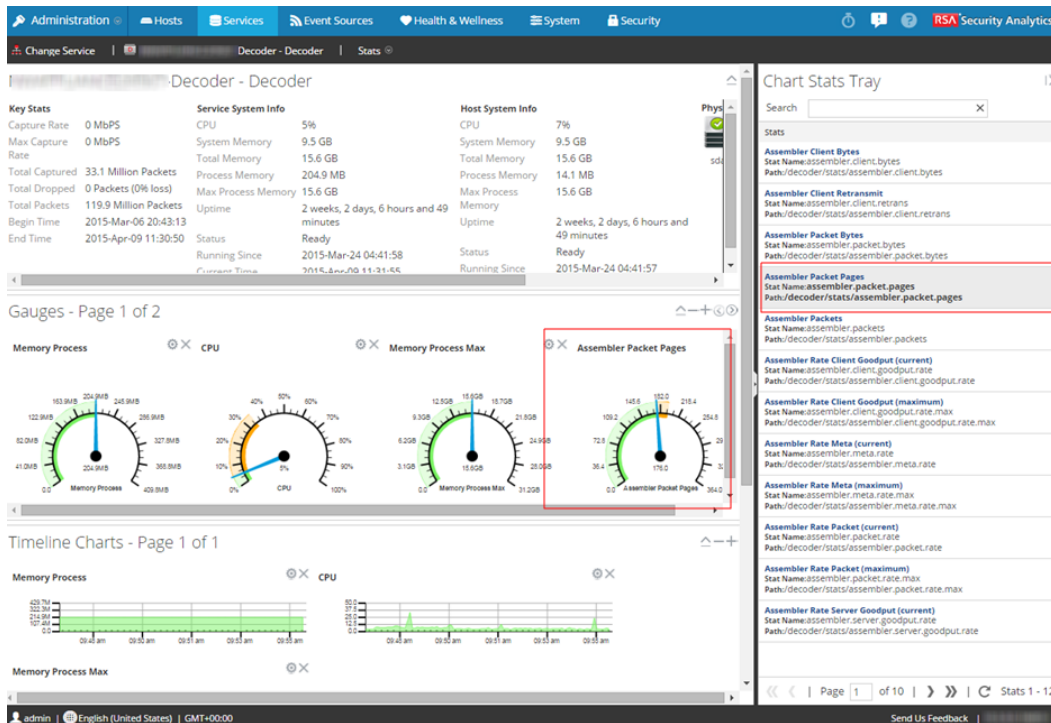
Procedures

Create a Gauge for a Statistic

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

- In the **Security Analytics** menu, select **Administration > Services**.
The Administration Services View is displayed.
- Select a service and select **View > Stats** in the Actions column.
The Chart Stats Tray is displayed on the right side.
- If the tray is collapsed, click  to view the list of available statistics.
- From the **Chart Stats Tray**, click on any statistic and drag it into the **Gauges** section.
A gauge is created for the statistic. If there is no space for the gauge, a new page is created

on the Gauges section and the gauge is added to the new page. In the example, the Assembler Packet Packages chart was added to the Gauges section by dragging it from the Chart Stats Tray.

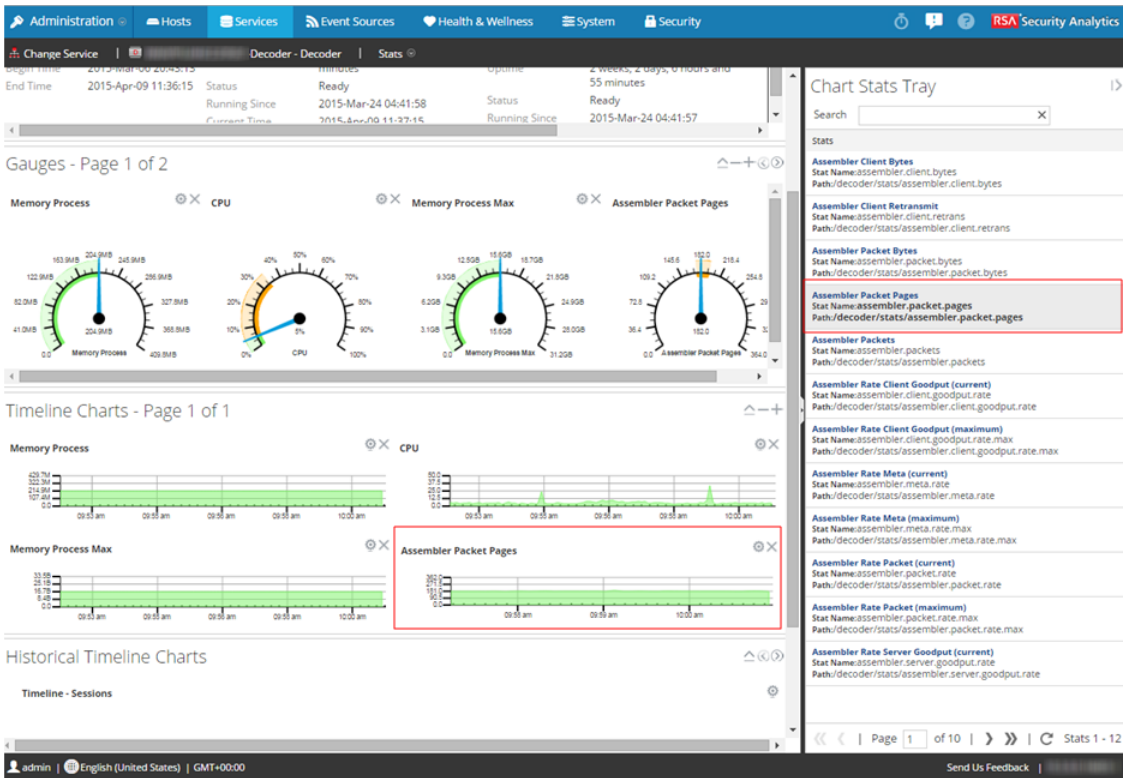


Create a Timeline Chart for a Statistic

To create a timeline for a statistic:

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

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



Search for a Statistic in the Chart Stats Tray

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

Chart Stats Tray >	
Search	<input type="text" value="session"/> X
Stats	
Assembler Sessions	Stat Name: assembler.session Path: /decoder/stats/assembler.session
Session Bytes	Stat Name: session.bytes Path: /database/stats/session.bytes
Session Bytes Last Hour	Stat Name: session.bytes.last.hour Path: /database/stats/session.bytes.last.hour
Session Completion Queue	Stat Name: pool.session.complete Path: /decoder/parsers/stats/pool.session.complete
Session Correlation Queue	Stat Name: pool.session.correlate Path: /decoder/stats/pool.session.correlate
Session Decrement Queue	Stat Name: pool.session.decrement Path: /decoder/stats/pool.session.decrement
Session Export Cache Files	Stat Name: export.session.cache.files Path: /decoder/stats/export.session.cache.files
Session Export Cache Percent Usage	Stat Name: export.session.percent.usage Path: /decoder/stats/export.session.percent.usage
Session Export Queue	Stat Name: pool.session.export Path: /decoder/stats/pool.session.export
Session First ID in hot storage	Stat Name: session.first.id.hot Path: /index/stats/session.first.id.hot
Session Free Space	Stat Name: session.free.space Path: /database/stats/session.free.space
Session Parse Queue	Stat Name: pool.session.parse Path: /decoder/parsers/stats/pool.session.parse
<< < Page <input type="text" value="1"/> of 2 > >> Stats 1 - 12 of 24	

Edit Properties of Statistics Gauges

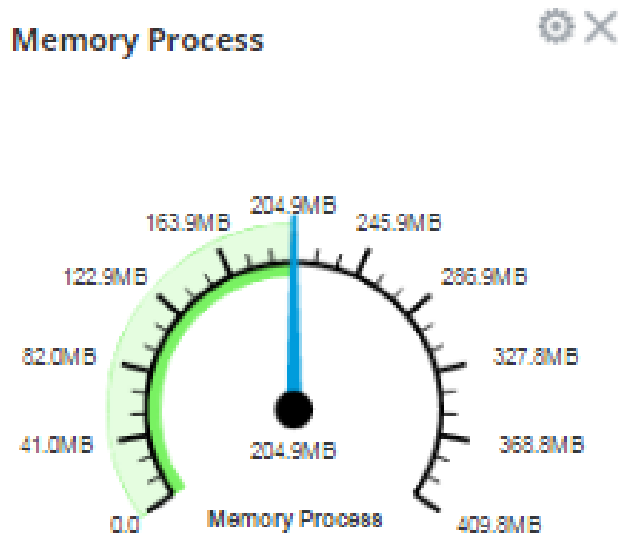
The Gauges section of the Service Stats view presents statistics in the form of an analog gauge. The properties of each individual gauge are editable; all gauges have an editable title and some have additional editable properties.


Procedures

Edit Properties of a Gauge

1. In the **Security Analytics** menu, select **Administration > Services**
The Administration 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**).



Gauges - Page 1 of 2



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.

Gauges - Page 1 of 2

Memory Process  


Name	Value ^
Path	/sys/stats/memor...
Display Name	Memory Process
Stat Name	memory.process

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

The new title replaces **Memory Process**.

Add Stats to the Gauges Section

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

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

The new gauge is displayed in the Gauges section.

Edit Properties of Timeline Charts

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

To access the charts:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a service and click **Stats**.

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

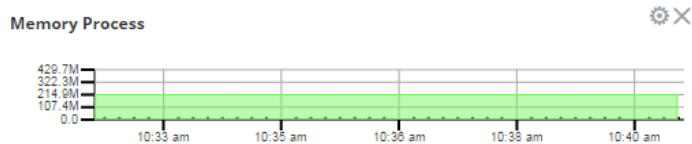
Procedures


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**).


Timeline Charts - Page 1 of 1



2. Click the **Properties** icon () to display the parameter names and values.
3. Double-click on a value (for example, the **Display Name** field).


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

Name ^	Value
Display Name	Memory Process
Path	/sys/stats/memory.process
Stat Name	memory.process

4. Type a new value and click the **Properties** icon ().
The timeline chart is displayed with new values.


Edit Properties of a Historical Timeline


To edit properties of a historical timeline chart:

1. Go to Historical Timeline Charts.
2. Click the **Properties** icon () to display the parameter names and values.
3. Click on a value (for example, **01/27/2015** for the **Begin Date** field).

Historical Timeline Charts

Timeline - Sessions

Name ^	Value
Begin Date	01/27/15 
Display Name	Timeline - Sessions
End Date	04/09/2015


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 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.

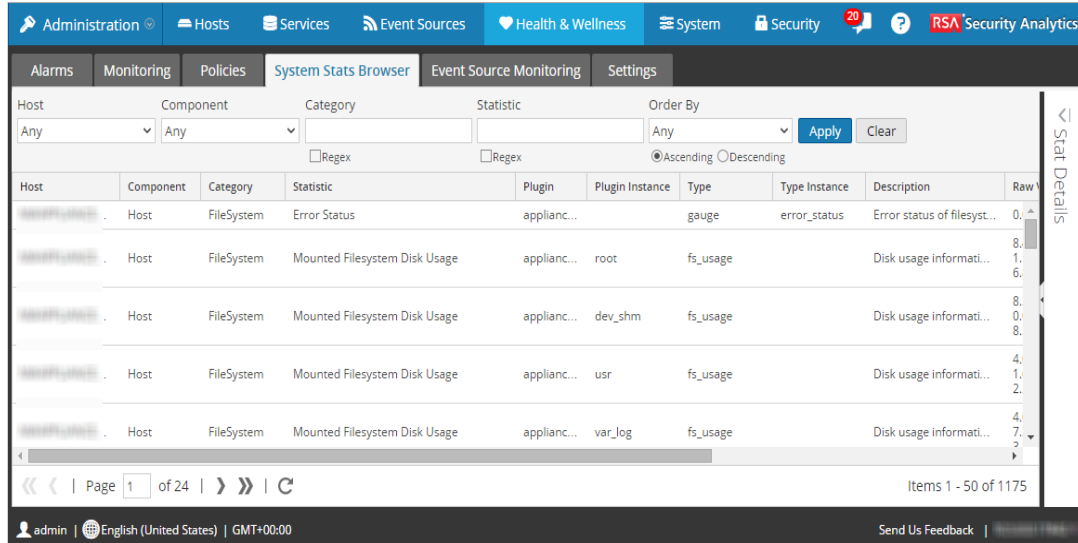
To access the system browser:

1. In the Security Analytics menu, select **Administration > Health & Wellness**.

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

2. Click **System Stats Browser**.

The System Stats Browser tab is displayed.



Filter System Statistics

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

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

Procedure

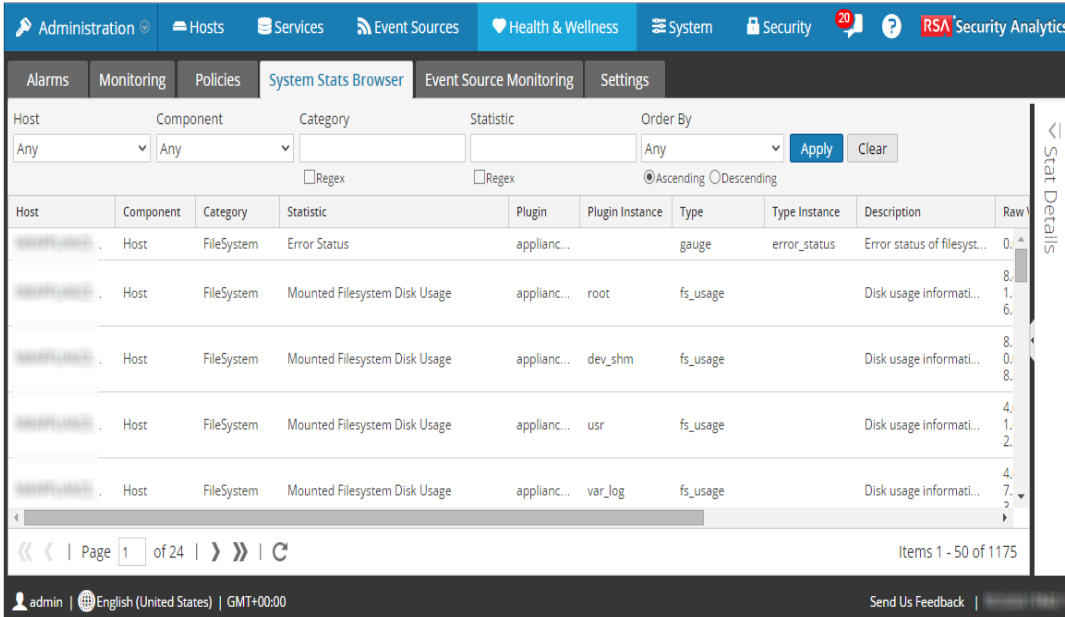
To filter the list of system statistics:

1. In the Security Analytics menu, select **Administration > Health & Wellness**.

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

2. Click **System Stats Browser**.

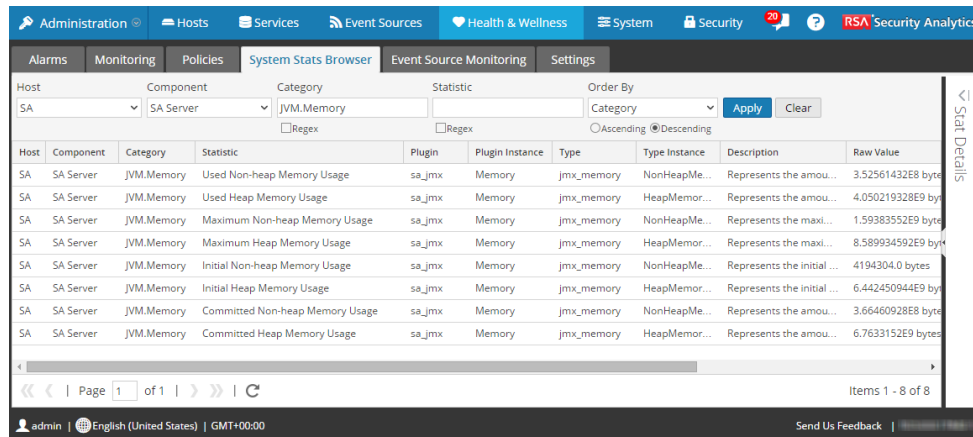
The System Stats Browser tab is displayed.



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

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

descending statistical category order.

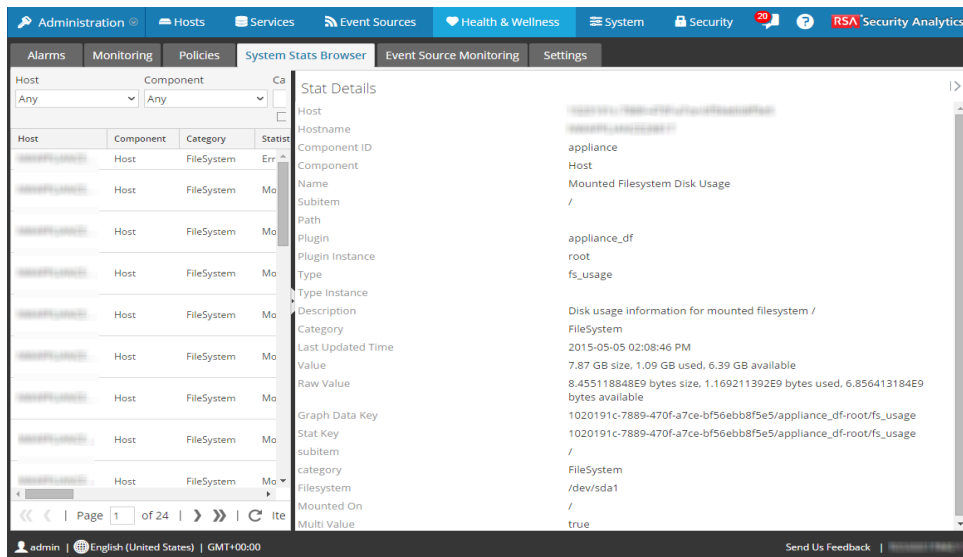


4. To view the details for an individual statistic:

a. Select a row to select a statistic.

b. Click  to the left of Stat Details.

The Stat Details section is displayed.



For details on various parameters and description in the **Administration > Health & Wellness > System Stats Browser** view, see [System Stats Browser View](#)

Create Historical Graph of System Statistics

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

Procedure

To create a historical graph:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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

2. Click **System Stats Browser**.

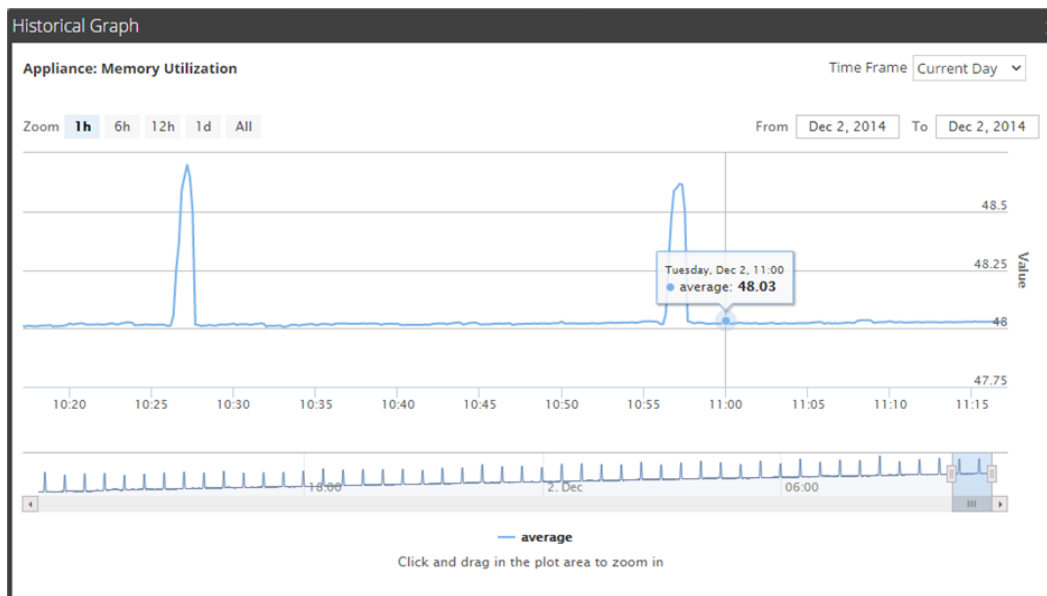
The System Stats Browser panel is displayed.

3. Specify the filter criteria to display the statistics you want.

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

The Historical graph for the selected statistic is displayed.

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



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

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

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 Security Analytics 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 Security Analytics displays in the Health & Wellness Interface or includes in the Health & Wellness log files.

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.
uninterruptibleGetValue (BlockingValueOrException.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
```

Message

```
(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 Security Analytics host.
Solution	Restart RabbitMQ service using the following commands. service rabbitmq-server restart

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

Run the following commands on Security Analytics server to make sure all these services are running.

```
[root@saserver ~]# service rsa-sms status
RSA NetWitness SMS :: Server is not running.
[root@saserver ~]# service rsa-sms start
Starting RSA NetWitness SMS :: Server...
[root@saserver ~]# service rsa-sms status
RSA NetWitness SMS :: Server is running (5687).
Solution [root@saserver ~]# service tokumx status
tokumx (pid 2779) is running...
service rabbitmq-server status
Status of node sa@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 Security Analytics services may be in a **stopped** state.

Solution	<p>Make sure that the following services are running then restart the Security Analytics server:</p> <p>Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.</p>
Message/ Problem	<p>User Interface: Server Unavailable.</p>
Possible Cause	<p>One or more Security Analytics services may be in a stopped state.</p>
Solution	<p>Make sure that the following services are running then restart the Security Analytics server: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.</p>
Message/ Problem	<p>User Interface: Server Unavailable</p>
Possible Cause	<p>System Management Service (SMS), RabbitMQ, or Tokumx service is not running.</p>

Run the following commands on Security Analytics server to make sure all these services are running.

```
[root@saserver ~]# service rsa-sms status
RSA NetWitness SMS :: Server is not running.
[root@saserver ~]# service rsa-sms start
Starting RSA NetWitness SMS :: Server...
[root@saserver ~]# service rsa-sms status
RSA NetWitness SMS :: Server is running (5687).
[root@saserver ~]# service tokumx status
tokumx (pid 2779) is running...
service rabbitmq-server status
Status of node sa@localhost ...
[{pid,2501},
 {running_applications,
  [{rabbitmq_federation_management,"RabbitMQ Federation
Management",
  "3.3.4"}],
```

Solution 1

Solution 2

Make sure /var/lib/rabbitmq partition is less than 75% full

Solution 3

Check Security Analytics host log files (var/lib/net-witness/uax/logs/sa.log) for any errors.

Issues Not Identified by the User Interface or Logs

This section provides troubleshooting information for issues that are not identified by messages Security Analytics 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	Puppet service not running. Puppet service must be running on all services.
Solution	Restart Puppet service.

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

Problem	Security Analytics does not show version to which you upgraded until you restart jettysrv (jeTTY server).
Possible Cause	When Security Analytics 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	<ol style="list-style-type: none"> 1. Manually stop the service. 2. Wait until you see that it is it offline. 3. Restart the service. <p>Security Analytics displays the correct version.</p>

Problem	Security Analytics server does not display Service Unavailable page.
Possible Cause	After you upgrade to Security Analytics 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 Security Analytics server cannot display the Service Unavailable page.
Solution	Restart jeTTY server.

Display System and Service Logs

RSA Security Analytics provides views into system logs and service logs. The views and procedures are similar; the only difference is that when viewing service logs, you can also select messages for the service or host.

Procedures

View System Logs

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **System Logging**.

Timestamp	Level	Message
2015-05-05T18:34:00.560	INFO	Valid license not found for service [REDACTED] - Event Stream Analysis
2015-05-05T18:34:00.562	INFO	Looking for valid license for service AutoDec
2015-05-05T18:34:00.562	INFO	Valid license not found for service AutoDec
2015-05-05T18:34:43.987	WARN	Unknown system monitoring component type getIPDBEndpointLabel
2015-05-05T18:39:43.987	WARN	Unknown system monitoring component type getIPDBEndpointLabel
2015-05-05T18:44:43.987	WARN	Unknown system monitoring component type getIPDBEndpointLabel
2015-05-05T18:46:48.424	INFO	Running resource subscription job
2015-05-05T18:46:49.115	ERROR	No service groups for resource : fingerprint_msi_lua
2015-05-05T18:46:49.245	ERROR	No service groups for resource : Netwitness Lua Library
2015-05-05T18:49:43.987	WARN	Unknown system monitoring component type getIPDBEndpointLabel

Display Service Logs

To display Security Analytics service logs:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a service.

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

The screenshot shows the 'System Logging' interface. At the top, there is a navigation bar with tabs for Administrator, Hosts, Services, Event Sources, Health & Wellness, System, Security, and Analytics. Below this, there is a sub-navigation bar with 'Change Service', 'NWAPPLIANCE28818 - Log Decoder', and 'Logs'. The main content area is titled 'System Logging' and has two tabs: 'Realtime' (selected) and 'Historical'. Below the tabs, there is a search bar with a dropdown menu set to 'ALL', a 'Keywords' input field, a 'Log Decoder' dropdown, and a 'Search' button. The main area contains a table with the following columns: 'Timestamp', 'Level', and 'Message'. The table lists several log entries, including a warning about a mismatch for query.timeout and several audit and info messages about user logins and database tasks.

Timestamp	Level	Message
2015-05-06T12:27:49.0	WARN	User admin has a mismatch for query.timeout in local account and trusted credentials. Using supplied value 5.
2015-05-06T12:27:49.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 1000.
2015-05-06T12:27:49.0	AUDIT	User admin (session 879, [REDACTED] 61) has logged in
2015-05-06T12:27:51.0	AUDIT	User escalateduser (session 904, [REDACTED] 661) has logged in
2015-05-06T12:28:22.0	AUDIT	User admin (session 853, 10.63.0.15:35640) has logged out
2015-05-06T12:56:03.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2015-05-06T13:26:04.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2015-05-06T13:56:04.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2015-05-06T14:26:05.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2015-05-06T14:56:06.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited

At the bottom of the interface, there is a footer bar with 'admin | English (United States) | GMT+00:00' and a 'Send Us Feedback' link.

Filter Log Entries

To filter the results shown in the Realtime tab:

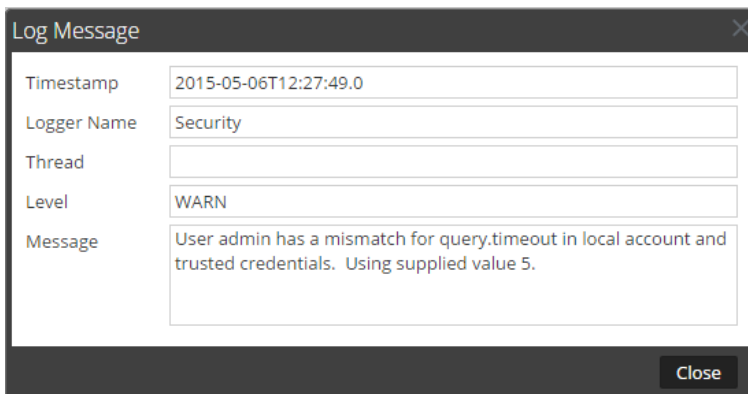
1. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both. System logs have seven log levels. Service logs have only six log levels because they do not include the **TRACE** level. The default is **ALL** log entries.
2. (Optional) For service logs, select the Service: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

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

Show Details of a Log Entry

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

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



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

Access Reporting Engine Log File

All Log Files

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

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

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

Upstart Logs

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

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

Search and Export Historical Logs

Security Analytics provides a searchable view of the **Security Analytics** 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.

Procedures

Display the Historical System Log

To display the historical log for the system:

1. In the **Security Analytics** menu, select **Administration > 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.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes Administrator, Hosts, Services, Event Sources, Health & Wellness, System, Security, and RSA Security Analytics. The left sidebar lists various system components, with System Logging selected. The main content area is titled 'System Logging' and has tabs for Realtime, Historical, and Settings. The Historical tab is active, showing a table of log entries with columns for Timestamp, Level, and Message. The table contains 10 entries, all with an INFO level. The messages include 'Valid license not found for service', 'Looking for valid license for service', and 'Log Decoder'. The interface also includes search filters for Start Date, End Date, and Keywords, and a search button. At the bottom, it shows 'Page 200 of 200' and 'Displaying 9951 - 10000 of 10000'.

Timestamp	Level	Message
2015-05-06T18:51:15.636	INFO	Valid license not found for service [REDACTED] - Log Decoder
2015-05-06T18:51:15.639	INFO	Looking for valid license for service AutoLogDec
2015-05-06T18:51:15.639	INFO	Valid license not found for service AutoLogDec
2015-05-06T18:51:15.643	INFO	Looking for valid license for service [REDACTED] - Concentrator
2015-05-06T18:51:15.643	INFO	Valid license not found for service [REDACTED] - Concentrator
2015-05-06T18:51:15.646	INFO	Looking for valid license for service [REDACTED] - Event Stream Analysis
2015-05-06T18:51:15.646	INFO	Valid license not found for service [REDACTED] - Event Stream Analysis
2015-05-06T18:51:15.649	INFO	Looking for valid license for service AutoDec
2015-05-06T18:51:15.649	INFO	Valid license not found for service AutoDec
2015-05-06T18:54:54.930	INFO	Looking for valid license for service [REDACTED] - Log Decoder
2015-05-06T18:54:54.931	INFO	Valid license not found for service [REDACTED] - Log Decoder

Display a Historical Service Log

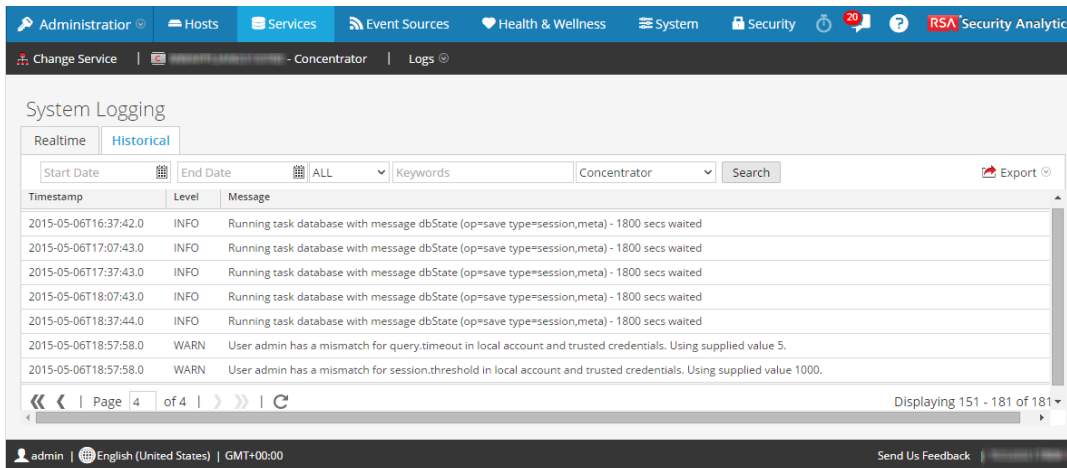
To display the historical log for services:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a service.
3. In the **Actions** column, select **View > Logs**.

The service logs view is displayed with the Realtime tab open.

4. Click the **Historical** tab.

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



Search Log Entries

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

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

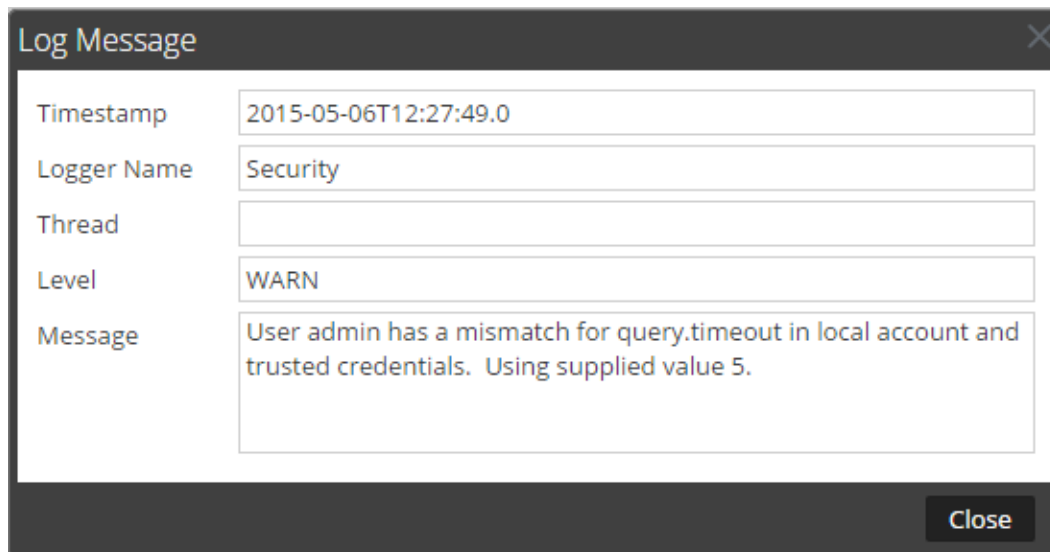
The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

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

1. Double-click a log entry.

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



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

The dialog closes.

Page Through Log Entries

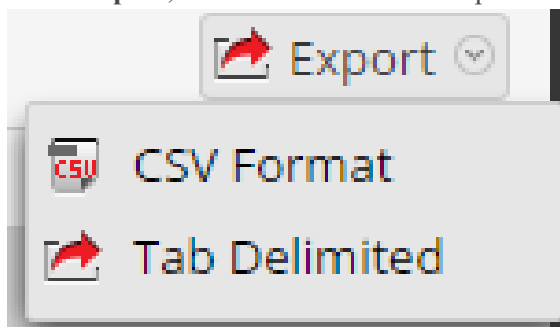
To peruse the different pages of the grid, use the paging controls on the bottom of the grid as follows:

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

Export a Log File

To export the logs in the current view:

Click **Export**, and select one of the drop-down options, **CSV Format** or **Tab Delimited**.



The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a Security Analytics 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 provide a way to represent the bread crumbs, or query path, you take when actively investigating a service in the Navigation view. You do not need to display and edit these objects very often.

A URL integration maps between 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 appears in the bread crumb in the Values panel.

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 Security Analytics 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.

Procedures

Edit a Query

1. In the **Security Analytics** menu, click **Administration > System**.
2. In the options panel, select **URL Integration**.

ID	Display Name	Query	Username	When Created
1		ip.src = '...'	admin	Fri Jan 30 2015 02:06:08 GMT-0500 (Easte...)
2		ip.dst = '...'	admin	Mon Feb 02 2015 10:33:45 GMT-0500 (Ea...)
3	304	result.code = '304'	admin	Wed Feb 25 2015 22:12:58 GMT-0500 (Ea...)
4		did = '...'	admin	Wed Feb 25 2015 22:13:10 GMT-0500 (Ea...)

3. Select the row in the grid and either double-click the row or click . The **Edit Query Dialog** is displayed.

Edit Query ✕

Display Name


Query

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 Security Analytics 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 Security Analytics 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 Security Analytics.

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

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

- **<sa host: port>** is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is only needed if access is configured over a non-standard port through a proxy.
- **<serviceId>** is the internal Service ID in the Security Analytics 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 Security Analytics. This value will change based on the service being connected to for analysis.
- **<encoded query>** is the URL-encoded Security Analytics query. The length of query is limited by the HTML URL limitations.

- **<start date>** and **<end date>** define the date range for the query. The format is **<yyyy-mm-dd>T<hh:mm>**. The start and end dates are required. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.

For example:

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

Examples

These are query examples where the Security Analytics server is 192.168.1.10 and the serviceID is identified as 2.

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

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

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

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

Additional Notes

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

Security Analytics System Maintenance Checklist

This checklist is intended for troubleshooting system issues as well as regular maintenance that can improve the health of your systems. For example, if you run into issues with disk space (such as disk space filling up regularly), refer to this document. It is not mandatory that you perform these tasks as suggested here, but these steps are designed to help with troubleshooting. This checklist is intended for reference purposes.

Several of the following troubleshooting tasks suggest restarting services. Please check with your organization's policies on restarting services before you perform those tasks.

If you need assistance with these tasks, contact Customer Support. For information about how to contact Customer Support, go to the "Contact Customer Support" page in RSA Link (<https://community.rsa.com/docs/DOC-1294>).

Audience

The primary audience for this guide is members of the Administration team who are responsible for maintaining Security Analytics.

All Host Types Health Checks

In this section, we describe the most common health checks that apply across all the Security Analytics platforms. You perform these tasks using both the Security Analytics user interface and SSH-Session/ CLI.

Checks for all Host Types Using the Security Analytics UI

Task Title	Description	✓
Check services	<ol style="list-style-type: none"> Go to Administration > Hosts and ensure that all the boxes in the Services column are green. Go to Administration > Services and ensure that all the services that are listed include green circles (●). 	
Check alarms	In the Security Analytics UI, go to Administration > Health & Wellness and click the Alarms tab. For information about interpreting the alarms, see Monitor Alarms .	

Checks for All Host Types Using SSH-Session/ CLI

Task Title	Description	✓
Check memory usage	Run the following command: <code>free -g ; top</code>	
Check CPU usage	Run the following command: <code>iostat</code>	
Check for any Security Analytics configuration changes	Run the following command: <code>puppet agent -t</code>	
Check the status of mcollective and collectd services	Run the following commands: <code>service mcollective status</code> <code>service collectd status</code>	
Log maintenance	It is a best practice to monitor service and system logs for content and physical size on a daily basis. It is important to verify that logs are being rolled over to keep disk partitions from getting full. (A log is rotated after it reaches a certain size, for example, 50 MB, and a log control tool such as <code>logrotate</code> creates a new file in its place for logging purposes.) Some of the services might not function properly if the root partition runs over 80%. Follow the steps in System Log Maintenance to address problems that can arise if the root partition runs over 80%.	
Monitor Reporting Engine	Monitor the Reporting Engine to ensure that it does not fill up the <code>/home/rsasoc/</code> partition. For information about how to monitor Reporting Engine, see Monitor Reporting Engine .	
Monitor Malware Co-Located service	The Malware Analysis <code>colo</code> service may fail if the <code>spectrum.h2.db</code> database size is over 10 GB. Avoid running the Malware Analysis <code>colo</code> service for continuous scans and check the size of the database frequently. This service is located on all Security Analytics servers. Do not confuse it with the stand-alone Malware Analysis appliance or virtual machine. If the service fails due to unavailable disk space, follow the steps described in Malware Analysis Colo Service Failure .	

Task Title	Description	✓
Monitor RabbitMQ server	Security Analytics servers use the <code>RabbitMQ</code> service for features such as federation, Health and Wellness, and Incident Management. Ensure that the <code>RabbitMQ</code> service is in a healthy state by running a report and looking for alarms, memory usage, and sockets used. To run this report, follow the steps described in RabbitMQ Service Report .	
Back up host systems and services	<p>Scheduled daily backups of all essential Security Analytics configurations should be taken for each of the following components:</p> <ul style="list-style-type: none"> • Log Decoder • Archiver • Concentrator • Broker • ESA • Remote Log Collectors (VLC) • Reporting Engine • Security Analytics server <p>For information about backing up these components, see Back Up and Restore Data for Hosts and Services.</p>	
Check Storage Usage	Run the following command: <code>df -h</code>	
Sort the files consuming the largest amount of disk space	Run the following command: <code>du -hsh * sort -rh</code>	
Check for core service dump files	In the Security Analytics console, run the following command: <code>find /var/netwitness/ -iname core*</code>	
Check for any process claiming space for a deleted file	Run the following command: <code>lsdf grep -i deleted</code>	

Task Title	Description	✓
Check for date and time to make sure they are synchronized	In the Security Analytics console, run the following command: date	
Check size of H2 database	Security Analytics uses an in-memory H2 database. If the H2 database is over 5 GB, and the user interface is slow, contact Customer Support.	
Check for Security Analytics current version	Run the following command: rpm -qa grep -i -nwappliance	
Check for all attached storage disks status and RAID configurations	Run the following command: /usr/sbin/nwraidutil.pl	
Check for NTP operations	Run the following command: ntpstat	
Check for kernel version	Run the following command: uname -a	
Check for kernel version	Run the following command: uname -a	
Verify Custom Index File Configurations	<p>Validate that the following files are consistent across all of the same type of host, for example, all Concentrators have a consistent <code>index-concentrator-custom.xml</code> file.</p> <ul style="list-style-type: none"> • Decoders: <code>/etc/netwitness/ng/index-decoder-custom.xml</code> • Concentrators: <code>/etc/netwitness/ng/index-concentrator-custom.xml</code> <p>If there are any file discrepancies, verify which host has the correct version and push that version to the other hosts. For instructions, see Push Correct Versions of Custom Index Files to Hosts.</p>	
Verify Custom Feeds	Verify that custom feeds are correctly deployed to hosts. For instructions, see Verify Custom Feeds .	

Task Title	Description	✓
Back Up Feeds, Rules and Parsers	Backing up feeds, correlation rules, parsers, and application rules regularly ensures that your configuration is correct if recovery is necessary and makes the recovery procedure easier and faster. If these items are not changed often, they can be backed up less frequently, but you should back them up regularly. You can use the backup scripts to back up these artifacts. For more information, see Back Up and Restore Data for Hosts and Services .	

Security Analytics Head Server Health Checks

In this section, we describe regular health checks to perform on the Security Analytics Head Server. You perform these tasks using the Security Analytics user interface and `SSH-Session/CLI`.

Head Server checks using the Security Analytics UI

Task Title	Description	✓
List Health and Wellness alarms for false and true positive	Create a list of Health and Wellness alarms and filter for false-positive and true-positive alarms, so that you can address them. Go to Administration > Health & Wellness and select the Alarms tab.	

Head Server Checks Using SSH-Session/ CLI

Task Title	Description	✓
Test connectivity of SA Head Server with other hosts	Run the command: <code>mco ping</code>	
Check for Reporting Engine critical errors	Run the command: <code>tailf /home/rsasoc/rsa/soc/reporting-engine/logs/reporting-engine.log grep -i error</code>	

Task Title	Description	✓
Check for Mcollective errors	Run the command: <code>tailf /var/log/mcollective.log grep -i error</code>	
Check SA certificates keystore contents	Run the command: <code>keytool -list -keystore /etc/pki/java/cacerts -storetype JKS -storepassword changeit</code>	
Check for any SA Jetty server critical errors	Run the command: <code>more /var/lib/netwitness/uax/logs/sa.log grep -i error</code>	
Verify all attached storage disks	Run the command: <code>nwraidutil.pl</code>	
Verify network connectivity	<ul style="list-style-type: none"> • Run the command: <code>curl host_IP:port</code> • With outgoing SMTP servers, run the command: <code>curl smtp_server_IP:25</code> 	
Verify required Security Analytics ports are open	Run the command: <code>netstat -alnp grep "port_no"</code>	

Concentrator Health Checks

Indexes

By default, Security Analytics hosts create index slices based on index save session count. The option `/index/config/save.session.count` enables you to configure the system to perform automatic checkpoint saves. "0" (zero) means that no checkpoint saves will occur based on sessions that are added. "auto" means that a save will occur at an interval chosen automatically based on available resources.

Older versions of Security Analytics Core, or systems that have been upgraded from Security Analytics versions prior to 10.5, use a time-based save schedule that saves the index every eight hours. You can see the current save interval by using the scheduler editor in the Security Analytics Administration UI for the service.

Within the index slice window there is a maximum limit of a unique number of values that can be indexed for a meta key. The number of values is defined by the setting `valueMax` in the `index-concentrator-custom.xml` file. If the meta key is indexed by index values, and if there is no `valueMax` setting, or if it is set to 0, then the meta key maximum number of unique values is limitless, which can cause higher index usage and degrade the Concentrator performance. Therefore, RSA recommends that you to set `valueMax` for the meta keys with index values.

It is also important to monitor the number of slices created on a Hybrid or Concentrator host. If the slices reach a certain number, the Concentrator service will have a detrimental impact on query performance, since more slices are created. When hosts reach the following number of index slices, an index reset is recommended if overall query performance is reduced:

- LogHybrid: 250 index-slices
- LogConcentrator: 500 index-slices

Caution: Be aware that a full re-index takes days to complete on a fully-loaded Concentrator .

NWDatabase Configuration Verification

Professional Services usually configures the Core NW database parameters and handles related issues. The information below is quoted from an internal support document: "The Core Database Tuning Guide" and provides information about the syntax that can be used and configuration best-practice for the core NW database.

Syntax used

The following example shows the syntax for NW database configuration:

```
/var/netwitness/decoder/packetdb=10tb; /var/netwitness/decoder0/packetdb  
==20.5tb
```

The size values are optional. If set, they indicate the maximum total size of files stored before databases roll over. If the size is not present, the database does not automatically roll over, but its size can be managed using other mechanisms.

The use of `=` or `==` is significant. The default behavior of the databases is to automatically create directories specified when the Core service starts. However, this behavior can be overridden by using the `==` syntax. If `==` is used, the service does not create any directories. If the directories do not exist when the service starts, the service does not successfully start processing. This gives the service resilience against file systems that are missing or unmounted when the host boots.

Verification of the 95% threshold

To ensure that the NW database directory sizes are configured with the correct 95% threshold, in the Security Analytics UI:

1. Go to the Security Analytics service Explore view, right-click on **Properties** and select **reconfig**.

2. In the **parameters** field, type `Update=0` and click **Send**. The response output will check the host storage and attached storage, and automatically calculates what the 95% threshold is.
3. When you type `Update=1` and click **Send**, the response output displays the same response as in the previous step, but when you refresh the Explore view, you will see that the session, meta, and packet database directories size have been updated to 95% of the current available storage.
4. Restart the Concentrator or Decoder service for the changes to take effect.

Concentrator Health Checks using the Security AnalyticsUI

Task Title	Description	✓
Check Health and Wellness for any related errors to hosts.	Go to Administration > Health & Wellness and click on the Alarms tab.	
Check aggregation status, rate and auto start	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service. 2. Click View > Config. From the Config drop-down menu at the top of the page, select Stats. 3. In Key Stats, check the values Rate, Behind and Status and make sure sessions-behind are less than 100,000. 	
Confirm metadata at the Concentrator is available for investigation	Go to Investigation > Navigate and select Load Values .	
Set query.parse to strict	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service. 2. In the Actions menu, click View > Explore. 3. In the left pane, expand sdk and select config. Ensure that query.parse is set to <code>strict</code>. 	
Review configured storage for NWDB	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service. 2. In the Actions menu, click View > Explore and in the left pane, select database > config. 3. Look in the configured storage for NWDB (<code>meta.dir</code>, <code>session.dir</code>, <code>index.dir</code>), which should be using up to 95% of available storage (local storage and DAC). 	

Task Title	Description	✓
Index-check: Check the number of slices	<p>The number of slices should be 400 or less. Run the command: <code>/index/stats/slices.total</code> (Index Slice Total)</p> <p>The number of slices should be less than 500 to avoid slowing down query performance.</p>	
Ensure NWDB storage configuration is correct	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service. 2. In the Actions menu, click View > Explore. 3. In the left panel, right-click on database and select Properties. 4. From the drop down menu, select reconfig, and in Parameters, type <code>update=0</code>, and click Send. This calculates what the NWDB size-configuration should be for all available storage to the server. 5. If this configuration does not match the current configuration, in Parameters, type <code>update=1</code> and then restart the <code>nwconcentrator</code> service to implement the correct NWDB storage configuration. 	
Verify all meta keys are configured with correct format and valueMax entries	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service. 2. In the Actions menu, click View > Config. 3. Select the Files tab, and from the drop down list, select the <code>index-concentrator-custom.xml</code> file and verify that all the meta keys are configured with the correct format and <code>valueMax</code> entries. 	

Task Title	Description	✓
Check /index/config/save.session.count	<ol style="list-style-type: none"> 1. Go to Administration > Services and select a Concentrator service 2. In the Actions menu, click View > Config. 3. From the Config menu at the top of the page, select Explore. 4. In the left pane, select index > config. save.session.count is displayed in the right pane. save.session.count is 600000000 by default (in 10.5.X and later). If save.session.count=0, then index slice creation is still controlled by the service scheduler. 5. In View > Config, select the Files tab and from the drop down list, select scheduler. Scheduler should look similar to : <pre>/sys/config/scheduler/351 = hours=8 pathname=/index msg=save</pre> 6. If <code>/index/config/save.session.count=0</code> and the index save schedule is every 8 hours, there are at least 21 index slices created every week. Assuming that the majority of queries are two weeks or less, update the index slice to: <pre>/index/config/index.slices.open (Index Open Slice Count) = 0 to 42 (42 is the default open slice count).</pre> <p>This change should reduce the maximum amount of memory that the Concentrator service can use for queries.</p> <p>Note: The change is immediate and does not require a service restart.</p>	

Concentrator Checks Using SSH-Session/ CLI

Task Title	Description	✓
Check storage usage	Run the command: <code>df -h</code>	
Check memory usage	Run the command: <code>free -g</code>	
Check for meta keys exceeding their valueMax per slice	Run the command: <pre>cat /var/log/messages grep -i index grep -i max</pre>	

Task Title	Description	✓
Test execution of Puppet provisioning script	Run the command: <code>puppet agent -t</code>	
Verify required ports are open	Run the command <code>netstat -alnp grep "port_no"</code>	
Index check: Check size of index slices	<p>Run the command:</p> <pre>cd /var/netwitness/concentrator ; du -h index</pre> <p>Note: RSA recommends that index slice size should be less than 20 GB for optimal performance. If you see very large index slices, you can verify the following index configuration settings:</p> <ul style="list-style-type: none"> • Proper <code>valueMax</code> values are set for meta keys with the format <code>IndexValues</code> in <code>index-concentrator-custom.xml</code>. • Index <code>save scheduler</code> entry is set to <code>8hr</code>, or • Index <code>config /index/config/save.session.count</code> is set to <code>auto</code> or <code>600000000</code> (600 Million). 	

Event Stream Analysis (ESA) Health Checks

In this section, we describe regular health checks to perform for ESA. You perform these tasks using both the Security Analytics user interface and `SSH-Session/ CLI`.

ESA checks using the Security Analytics UI

Task Title	Description	✓
Check the Events per Second (EPS) rate	<p>Monitor EPS for an ESA host at the following location:</p> <p>Alerts > Configure > Services, select an ESA host and check Offered Rate.</p> <p>Compare your current ESA EPS rates to previous results, and if there is a significant difference, call Customer Support. If you are using a virtual system, you can also refer to the "Basic Deployment" topic in the <i>Virtual Host Setup Guide</i> (https://community.rsa.com/docs/DOC-83321) for more information.</p>	

Task Title	Description	✓
Check Mongo database status	<p>The Mongo database on the ESA host is responsible for storing the alerts and incident management information. After a period of time, it is possible for this database to grow large and cause performance issues. RSA recommends that the Mongo database does not exceed 5 GB in size. Ensure that you set up database maintenance to prevent it from exceeding 5 GB at the following location:</p> <p>Administration > Services, select an ESA service. From the Actions menu, select View > Explore > Alert > Storage > Maintenance.</p>	
Ensure that all data source connections are enabled	<ol style="list-style-type: none"> 1. Go to Services and select an ESA service. 2. From the Actions menu, select View > Config. 	
Ensure that ESA rules resource-usage monitoring is enabled	<ol style="list-style-type: none"> 1. Go to Administration > Services, select an ESA service. From the Actions menu, select View > Explore. 2. In the left pane, expand CEP and go to Metrics > configuration, and ensure that EnabledMemoryMetric, EnabledCaptureSnapshot and EnableStats are set to true. 3. Restart the ESA service. 	
Monitor ESA rules memory usage	<ol style="list-style-type: none"> 1. Go to Administration > Health & Wellness > System Stats Browser. 2. Enter the following options in the fields at the top of the page: Host = ESA Component = Event Stream Analytics Category, type <code>esa-metrics</code> 3. Click Apply. 	
Ensure that the correct Concentrators are added to the ESA service as data sources	<ol style="list-style-type: none"> 1. Go to Administration > Services and select an ESA service. 2. From the Actions menu, select View > Config and ensure that the list of Concentrators is correct. 3. Ensure that all Concentrators are enabled and that the default port is set to 56005. 	

Task Title	Description	✓
Ensure that the number of enabled rules meets requirements	Go to Alerts > Configure > Services > Rule Stats .	
Ensure all ESA rules are deployed after updates	<ol style="list-style-type: none">1. Go to Alerts > Configure > Rules.2. Ensure that there is no exclamation mark beside the deployment.	

ESA Checks Using SSH-Session/ CLI

Task Title	Description
Make sure that there are NO sessions-behind between ESA and downstream data-sources like (concentrator, decoders)	SSH to the ESA host and run the following commands Note: The commands in RED are user inputs and the ones in BLACK are system outputs. <pre> root@ESA]# /opt/rsa/esa/client/bin/esa-client --profiles carlos carlos:offline jmx:localhost:com.rsa.netwitness.esa:/> carlos-connect RemoteJmsDirectEndpoint { jms://localhost:50030?carlos.useSSL=true } ; running = true carlos:localhost jmx:localhost:com.rsa.netwitness.esa:/>cd nextgen /Workflow/Source/nextgenAggregationSource carlos:localhost jmx:localhost:com.rsa.netwitness.esa:/Workflow/Source/nextgenAggregationSource> get . "name" : "10.xx.xx.xx:56005", "note" : "", "sessionId" : 24462390949, "sessionsBehind" : 58501036, "state" : "IDLE_QUEUED", "status" : "Streaming", "time" : 1459508373000 }, { </pre>

Log Collector Health Checks

In this section, we describe regular health checks to perform for Log Collector. You perform these tasks using both the Security Analytics user interface and SSH-Session/ CLI.

Log Collector checks using the Security Analytics UI

Task Title	Description	✓
Ensure all subcollections are started	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Collector service. 2. From the Actions menu, select View > System and check the collection status to ensure that the relevant collections have been started. 	
Check the Start collection on service startup status	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Collector service. 2. From the Actions menu, select View > Config > Collector Configuration. 	
Ensure Remote Log Collectors (VLCs) are configured	<p>If VLCs are available and their configuration is the Pull model, ensure that VLCs are included in the Log Collector configuration.</p> <ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Collector service. 2. In the Actions menu, select View > Config > Remote Collectors. 	
Ensure the Decoder is defined for the Log Collector in Event Destinations	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Collector service. 2. In the Actions menu, select View > Config > Event Destinations and make sure the status is “started”. 	
Ensure ports are set to default 50001 and 56001 for SSL	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Collector service. 2. In the Actions menu, select View > Config. Select the General tab and ensure that: <ul style="list-style-type: none"> Port is set to 50001 SSL Port is set to 56001 	

Log Collector Checks Using SSH-Session/ CLI

Task Title	Description	✓
Ensure rabbitmq-server is started	From logcollector SSH, run the command: <code>service rabbitmq-server status</code>	
Ensure nwlogcollector service is up and running	From logcollector SSH, run the command: <code>status nwlogcollector</code>	
Make sure all queues have at least one consumer	Run the command: <code>rabbitmqctl list_queues -p logcollection messages_ready name consumers</code>	
Ensure that there are no stuck rdq files	Navigate to the following location and ensure that <code>msg_store_persistent</code> does not have the rdq files backed up: <code>/var/netwitness/logcollector/rabbitmq/mnesia/sa@localhost/msg_store_persistent</code>	
If host is VLC, verify that the logCollectionType is set to RC	Run the command: <code>cat /etc/netwitness/ng/logcollection/{logCollectionType}</code>	
	Note: If you are deploying new plugin collection content on a VLC, you must deploy it on the local Log Collector as well.	

Log Decoder Health Checks

In this section, we describe regular health checks to perform for Log Decoder. You perform these tasks using both the Security Analytics user interface and SSH-Session/ CLI.

Log Decoder checks using the Security Analytics UI and Explore/REST

Task Title	Description	✓
Ensure that capture has been started.	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. 2. From the Actions menu, select View > System and check the capture status. 	

Task Title	Description	✓
Ensure that the capture rate is within the EPS range	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. 2. From the Actions menu, select View > Config. 3. From the Config dropdown menu, select Stats. 	
Ensure that parsers are enabled	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. 2. From the Actions menu, select View > Config and on the General tab, check the Parsers Configuration section. 	
Ensure that the ports are set to default 50002 and 56002 for SSL	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. 2. From the Actions menu, select View > Config and on the General tab in the System Configuration section, ensure that: Port is set to 50002 SSL Port is set to 56002 	
Ensure that the correct capture interface is selected	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. 2. From the Actions menu, select View > Config. 3. On the General tab, check the Decoder Configuration section. 	
Ensure that databases are correctly configured	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Log Decoder service. From the Actions menu, select View > Explore. 2. In the left pane, right-click on database and select Properties, and from the drop-down menu, select reconfig. 3. In Parameters, type <code>update=0</code>, and then click Send. 4. Compare the response output with the current configuration. 	
Ensure Decoders are Synchronized with Enabled Parsers	<p>To ensure accurate analysis and that forensic data is available to analysts, Decoders must be in sync with enabled parsers. Because the list of enabled parsers can grow in a typical installation, the easiest way to validate the list of parsers that are enabled on Decoders is to check which parsers are currently disabled by using the <code>parsers.disabled</code> attribute in the Explore/REST interface. Perform the steps in Validate the List of Enabled Parsers on Decoders.</p>	

Log Decoder Checks Using SSH-Session/ CLI

Task Title	Description	✓
Ensure that Log Decoder is listening on port 514	Run the command: <code>netstat -anp grep 514</code>	

Archiver Health Checks

In this section, we describe regular health checks to perform for Archiver. You perform these tasks using both the Security Analytics user interface and `SSH-Session/ CLI`.

Archiver checks using the Security Analytics UI

Task Title	Description	✓
Ensure that aggregation has started	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. 2. From the Actions menu, select View > System and check the aggregation status. 	
Ensure that Log Decoder aggregation is correct and status is consuming	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. 2. From the Actions menu, select View > Config and check the General tab. 	
Ensure that aggregation is automatically started	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. 2. From the Actions menu, select View > Config. 3. On the General tab, under Aggregation Configuration > Aggregation Settings, ensure that Aggregate Autostart is selected. 	
Ensure that all metas are added to Meta Include	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. 2. From the Actions menu, select View > Config and on the General tab, check the Meta Include column. 	

Task Title	Description	✓
Ensure that ports are set to default 50008 and SSL 56008	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. 2. In the Actions menu, select View > Config. Ensure that: <ul style="list-style-type: none"> Port is set to 50008 SSL Port is set to 56008 	
Ensure that all database directories are set to 0 B	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. From the Actions menu, select View > Explore. 2. In the left pane, expand archiver > collections > default > database > config. 3. In the right pane, check meta.dir, packet.dir, and session.dir and ensure that they are set to 0 B. 	
Ensure that 95% of usable storage is set	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select an Archiver service. In the Actions menu, select View > Config. 2. Select the Data Retention tab, and under Collections, check the values for Hot Storage, Warm Storage, and Cold Storage. 	

Packet Decoder Health Checks

In this section, we describe regular health checks to perform for Packet Decoders. You perform these tasks using both the Security Analytics user interface and `SSH-Session/ CLI`.

Packet Decoder checks using the Security Analytics UI

Task Title	Description	✓
Ensure that capture has been started.	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. From the Actions menu, select View > System and check the capture status. 	
Ensure that the correct capture interface is selected	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. From the Actions menu, select View > Config and on the General tab, check the Decoder Configuration section. 	

Task Title	Description	✓
Ensure that parsers are enabled	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. From the Actions menu, select View > Config and on the General tab, check the Parsers Configuration section. 	
Ensure that the capture rate is within the Mbps range	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. From the Actions menu, select View > Config. 3. From the Config dropdown menu, select Stats. 	
Ensure that ports are set to default 50004 and SSL 56004	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. In the Actions menu, select View > Config. 3. Ensure that: <ul style="list-style-type: none"> Port is set to 50004 SSL Port is set to 56004 	
Ensure that there are no Flex parsers or duplicate parsers enabled	<ol style="list-style-type: none"> 1. Go to Administration > Services, and select a Packet Decoder service. 2. From the Actions menu, select View > Config and on the General tab, check the Parsers Configuration section. 	

Packet Decoder Checks Using SSH-Session/ CLI

Task Title	Description	✓
Monitor current transmission rate, packet-drops and errors on all interfaces	Run the command: <code>netstat -i</code>	

Log Locations

If issues arise with any component of the Security Analytics platform, the following table will help you find component log files to assist with troubleshooting.

You can also export logs from the user interface, for example, from Decoders and Log Collectors. For information about viewing and exporting logs, see the "Search and Export Historical Logs" topic in the *System Maintenance Guide* (<https://community.rsa.com/docs/DOC-84570>).

Component	Log Location
SA Server UI	/var/lib/netwitness/uax/logs/sa.log
SA Server Jetty	/var/lib/netwitness/uax/logs/sa.log /opt/rsa/jetty9/logs/<YYYY>_<MM>_<DD>.stderrout.log
RabbitMQ	/var/log/rabbitmq/sa@localhost.log /var/log/rabbitmq/startup.log /var/log/rabbitmq/sa@localhost-sasl.log
Reporting Engine	/home/rsasoc/rsa/soc/reporting-engine/logs/reporting-engine.log
Upgrading	/var/log/yum.log
CollectD	/var/log/messages
Puppet	/var/log/messages
Puppet Master	/var/log/puppet/masterhttp.log
MCollective	/var/log/mcollective.log
ESA	/opt/rsa/esa/logs/esa.log
General	/var/log/messages
Host	Number of DACs
Series 4 Log Decoder	Up to 5, or one UltraDAC.
Series 5 Log Decoder	Up to 8, or one UltraDAC.

Supported Browsers

When using the Security Analytics user interface, RSA recommends that you use the following browsers:

- Google Chrome
- Firefox

Task Details

This section contains detailed procedures for some of the tasks in the checklist.

Check Services

To check the health of services using Health and Wellness:

1. Log into the Security Analytics user interface.
2. Select **Administration > Health & Wellness** and then click the **Policies** tab.
3. Ensure that the Broker, Concentrator and Decoder services are displayed as green (enabled) and that the services indicate **All** with the correct number of devices for our environment.

To learn more about health and wellness, read the "Health and Wellness" topic in the *System Maintenance Guide* in RSA Link (<https://community.rsa.com/>).

System Log Maintenance

To address issues if the root partition runs over 80%:

1. Check disk volume partition space and ensure that the root partition is not over 80%. Run the following command:

```
df
```

2. Check the size of the logs in the `/etc/logrotate.conf` and `/etc/logrotate.d` directories. Ensure that the logs are being rolled over. Most services use `logrotate` to manage the logs. `logrotate` configurations are in the `/etc/logrotate.conf` and `/etc/logrotate.d` directories. The following list of logs should be monitored:

```
/var/log/tokumx/
```

```
/var/log/puppet/
```

```
/var/log/logstash/
```

```
/var/log/audit/
```

```
/var/log/rabbitmq/
```

```
/var/lib/netwitness/uax/logs
```

```
/var/lib/netwitness/rsamalware/jetty/logs
```

```
/opt/rsa/im/  
/opt/rsa/jetty9/logs/  
/home/rsasoc/rsa/soc/reporting-engine/logs  
/opt/rsa/sms/  
/opt/rsa/sms/logs  
/var/lib/netwitness/rsamalware/spectrum/logs
```

3. Pay special attention to the `/var/lib/netwitness/uax/scheduler/` directory. This is where Security Analytics stores all PCAPS that are generated from analysts using the Investigation module. Ensure that this directory does not fill up all the available space in the partition.

Monitor Reporting Engine

To resolve Reporting Engine issues, run a `df` command. If the command shows that the partition is getting full, the most common directories that cause this are:

- `/home/rsasoc/rsa/soc/reporting-engine/formattedReports`
- `/home/rsasoc/rsa/soc/reporting-engine/resultstore`

Recovery steps: Open a ticket with Customer Support, as this can indicate a unique situation that should be evaluated by Support.

Malware Analysis Colo Service Failure

To resolve a Malware Analysis Colo service failure:

1. Run `stop rsaMalwareDevice`
2. Move the contents of `/var/lib/netwitness/rsamalware/spectrum/db/` to a backup location.
3. Run `start rsaMalwareDevice`

RabbitMQ Service Report

To run the RabbitMQ service report and recover if RabbitMQ is down:

1. SSH to the Security Analytics server.
2. Run `rabbitmqctl status`.

Recovery Steps: If **RabbitMQ** is down, follow these steps:

1. Collect the logs under `/var/log/rabbitmq/`
2. Run the following commands:
`service puppet stop`

```
service rsa-sms stop
service rabbitmq-server stop
service rabbitmq-server start
service rsa-sms start
service puppet start
```

Packet Retention Data Management Script

To run the `rest_packet_retention.py` script that provides packet retention data:

1. Copy the `rest_packet_retention.py` to a server that has access to the other Security Analytics hosts.
2. Make the script executable by running the following command (this is a one-time task):
`chmod +x rest_packet_retention.py`
3. Create a host `.csv` file named `decoders.csv` that contains a list of all Decoders, one per line, with IP addresses or hostnames (this is a one-time task).

4. Run the following command:

```
./rest_packet_retention.py
```

5. Enter the user name (the local admin account, not root) for the host and press **ENTER**.
6. Enter the password for the host and press **ENTER**.
7. The following example shows output from the `rest_packet_retention.py` script:

```
Username: admin
Password for admin:
Host: 172.16.0.0 Packet Oldest Time: 2017-05-10 15:06:49 Days
(Retention): 10 days, 10:28:47
```

Meta Retention Data Management Script

To run the `rest_meta_retention.py` script that provides meta retention data:

1. Copy the `rest_meta_retention.py` script to a server that has access to the other Security Analytics hosts.
2. Make the script executable by running the following command (this is a one-time task):
`chmod +x rest_meta_retention.py`
3. Create a host `.csv` file named `concentrators.csv` that contains a list of all Concentrators, one per line, with IP addresses or hostnames (this is a one-time task).

4. Run the following command:

```
./rest_meta_retention.py
```

5. Enter the user name (the local admin account, not root) for the host and press **ENTER**.
6. Enter the password for the host and press **ENTER**.
7. The following example shows output from the `rest_packet_retention.py` script:

```
Username: admin
Password for admin:
Host: 172.16.0.0 Meta Retention: 10 days, 20:27:46
```

Push Correct Versions of Custom Index Files to Hosts

To verify which host has the correct version of custom index files, and then push them to the other hosts, follow the steps in this example (which is a Concentrator with an inconsistent file):

1. Log into the Security Analytics user interface.
2. From the main menu, select **Administration > Services**.
3. Select a Concentrator that has the correct version of the custom index file and click **View > Config**.
4. Select the **Files** tab.
5. Select the `index-concentrator-custom.xml` from the drop-down list and click **Push** to push this file to a Concentrator with a known bad configuration.

Verify Custom Feeds

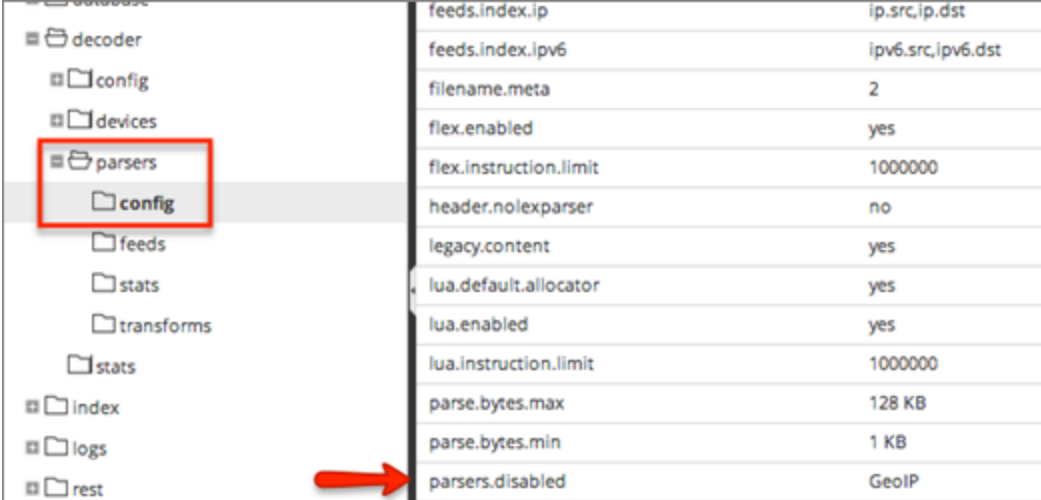
To verify that custom feeds are deployed correctly to hosts:

1. Log into the Security Analytics user interface.
2. From the main menu, select **Live > Feeds**.
3. Check the **Status** column for any failed feeds and remediate them.

Validate the List of Enabled Parsers on Decoders

To validate enabled parsers for each Decoder and then compare the list of disabled parsers to ensure uniformity across all Decoders:

1. Log into the Security Analytics user interface.
2. Select **Administration > Services**.
3. Select a Decoder and click **View > Explore**.
4. In the left pane, navigate to **decoder > parsers > config**.
The `parsers.disabled` attribute is displayed on the right and lists the parsers that are disabled as shown in the following figure.



feeds.index.ip	ip.src,ip.dst
feeds.index.ipv6	ipv6.src,ipv6.dst
filename.meta	2
flex.enabled	yes
flex.instruction.limit	1000000
header.nolexer	no
legacy.content	yes
lua.default.allocator	yes
lua.enabled	yes
lua.instruction.limit	1000000
parse.bytes.max	128 KB
parse.bytes.min	1 KB
parsers.disabled	GeoIP

5. Compare the `disabled.parsers` attribute to other Decoders in your environment. Any discrepancies can be cleared up by copying and pasting settings from a known good Decoder configuration to one with errors. You can also manually enable or disable parsers using **View > Config**.

Troubleshoot Security Analytics

For information about troubleshooting Security Analytics, see the following topics:

- [Debugging Information](#)
- [Error Notification](#)
- [Miscellaneous Tips](#)
- [NwLogPlayer](#)
- [Troubleshoot Feeds](#)

Debugging Information

Security Analytics Log Files

The following files contain Security Analytics log information.

Component	File
puppet	/var/log/messages
rabbitmq	/var/log/rabbitmq/sa@localhost.log /var/log/rabbitmq/sa@localhost-sasl.log
mcollective	/var/log/mcollective.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
Security Analytics	/var/lib/netwitness/uax/logs/sa.log
Security Analytics	/var/lib/netwitness/uax/logs/ audit/audit.log

Component	File
Security Analytics	/opt/rsa/jetty9/logs

Files of Interest

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

Component	File	Description
puppet	/etc/puppet/puppet.conf	Puppet configuration file. This configuration file drives the behavior of both the Puppet Agent (all nodes) and the Puppet Master (SA node only). This file is modified by upgrade scripts when the system is upgraded, and at installation time for new installs.
puppet	/etc/sysconfig/puppet	Service configuration file for puppet agent.
puppet	/var/lib/puppet/ssl	This is where Puppet stores keys and certificates (among other PKI artifacts). Caution: Tread very carefully in this directory, as destroying artifacts in this directory can cause Puppet to stop functioning.
puppet	/var/lib/puppet/node_id	This is where we store the SA node ID persistently. Do not delete or modify this file, or you may end up breaking your puppet installation.

Component	File	Description
puppet	/etc/puppet/scripts	This directory contains common scripts we have created that simplify our use of Puppet. Typically you do not need to use these scripts, except for some very arcane troubleshooting scenarios.
puppet	/var/lib/puppet	Runtime Puppet artifacts. Most of the time you do not need to inspect this directory, except as listed below.
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQ configuration file. This configuration file partially drives the behavior of RabbitMQ, particularly around network/SSL settings. This file is downloaded and synchronized through Puppet.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQ environment configuration file. This file specifies the RabbitMQ node name and location of the enabled plugins file.
rabbit	/etc/rabbitmq/rsa_enabled_plugins	This file specifies the list of enabled plugins in RabbitMQ. This file is managed by the RabbitMQ server, via the rabbitmq-plugins command. This file overrides the /etc/rabbitmq/rsa_enabled_plugins path, in order to work around issues with upgrading the Log Collector from 10.3.

Component	File	Description
rabbit	<code>/etc/rabbitmq/ssl/server/key.pem</code>	The RabbitMQ private key, as a PEM-encoded RSA private key. This file is a symbolic link to the Puppet node ID private key.
rabbit	<code>/etc/rabbitmq/ssl/server/cert.pem</code>	The RabbitMQ server certificate, as a PEM-encoded X.509 certificate. This file is a symbolic link to the Puppet node ID certificate.
rabbit	<code>/etc/rabbitmq/ssl/truststore.pem</code>	The RabbitMQ trust store. This file contains a sequence of PEM-encoded X.509 certificates, represented trust CAs. Any clients that connect to RabbitMQ and present a certificate that is signed by a CA in this list is considered a trusted client.

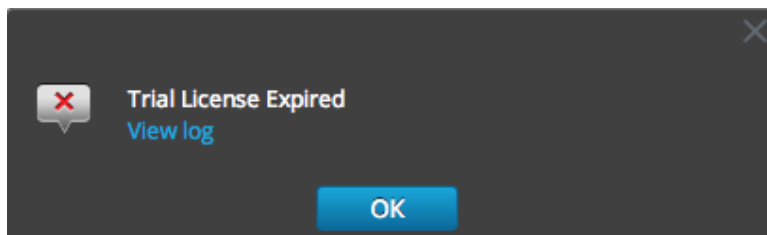
Component	File	Description
rabbit	/var/log/rabbitmq/mnesia/sa@localhost	<p>The RabbitMQ Mnesia directory. Mnesia is the Erlang/OTP database technology, for storing Erlang objects persistently. RabbitMQ uses this technology for storing information such as the current set of policies, persistent exchanges and queues, and so forth.</p> <p>Importantly, the <code>msg_store_persistent</code> and <code>msg_store_transient</code> directories are where RabbitMQ stores messages that have been spooled to disk, e.g., if messages are published as persistent messages, or which have paged off to disk due to memory limitations. Keep a close eye on this directory, if the disk or memory alarms have tripped in RabbitMQ.</p> <div style="border: 1px solid yellow; padding: 5px;">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.</div>
mcollective	/etc/mcollective/client.cfg	MCollective client configuration file. This file is generally only applicable to the SA node.

Component	File	Description
mcollective	/etc/mcollective/server.cfg	MCollective server configuration file. The configuration file applies to all nodes, including the SA server node.
mcollective	/etc/mcollective/ssl/mcollective_server_public.pem	MCollective server public key. This file is file is generated on the SA Server and distributed via Puppet.
mcollective	/etc/mcollective/ssl/mcollective_server_private.pem	MCollective server private key. This file is file is generated on the SA Server and distributed via Puppet.
mcollective	/etc/mcollective/ssl/mcollective_client_private.pem	MCollective client private key. This file is file is only resident on the SA Server.
mcollective	/etc/mcollective/clients/mcollective_client_public.pem	MCollective client public key. This file is file is generated on the SA Server and distributed via Puppet.

Error Notification

Security Analytics has a set of error message types associated with different components and operations. Security Analytics 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.



Procedure

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

Timestamp	Level	Message
2014-03-14T19:01:49.501	WARN	Failed setup yum service for device
2014-03-14T19:02:53.907	ERROR	Unable to connect to endpoint vives://
2014-03-14T19:02:53.913	WARN	Failed setup yum service for device
2014-03-14T19:03:23.925	ERROR	Timeout waiting for task. java.util.concurrent.TimeoutException: Timeout waiting for task. at c
2014-03-14T19:03:23.926	WARN	Failed setup yum service for device
2014-03-14T19:03:23.941	ERROR	Unable to connect to endpoint
2014-03-14T19:03:23.942	WARN	Failed setup yum service for device
2014-03-14T19:03:36.2	ERROR	Unable to connect to endpoint
2014-03-14T19:03:36.11	WARN	Error occurred during applying system updates
2014-03-14T19:05:44.120	ERROR	java.lang.Exception: Trial license does not match

Miscellaneous Tips

Harden the Admin Account

The STIG Hardening Guide in the SA 10.4 Documentation on SCOL (<https://knowledge.rsasecurity.com/scolcms/set.aspx?id=10407>) has this information.

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 Security Analytics Parser v2.0.zip archive lists the event categories and the event parser lines to help with building reports, alerts, and queries.

NwConsole for Health & Wellness

RSA has added a command option called **logParse** in **NwConsole**. This command option supports log parsing, a convenient way to check log parser without setting up the full system to do log parse.

Note: Does anyone know of any documentation for this command?

Usage

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

<code>--priority arg</code>	set log priority level
<code>-h [--help]</code>	show this message
<code>-f [--file] arg</code> (=stdin)	input message; defaults to stdin
<code>-d [dir] arg</code>	input directory
<code>-s [--server] arg</code> (=localhost)	remote server; defaults to localhost
<code>-p [--port] arg</code> (=514)	remote port; defaults to 514
<code>-r [--raw] arg</code> (=0)	Determines raw mode. <ul style="list-style-type: none"> • 0 = add priority mark (default) • 1= File contents will be copied line by line to the server. • 3 = auto detect • 4 = enVision stream • 5 = binary object
<code>-m [--memory] arg</code>	Speed test mode. Read up to 1 Megabyte of messages from the file content and replays.
<code>--rate arg</code>	Number of events per second. This argument has no effect if rate > eps that the program can achieve in continuous mode.
<code>--maxcnt arg</code>	maximum number of messages to be sent
<code>-c [--multiconn]</code>	multiple connection
<code>-t [--time] arg</code>	simulate time stamp time; format is <code>yyyy-m-d-hh:mm:ss</code>
<code>-v [--verbose]</code>	If true , output is verbose
<code>--ip arg</code>	simulate an IP tag

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

Troubleshoot Feeds

Overview

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

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

Details

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

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

How it Works

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

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

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, Security Analytics 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", "Apache  
grp"
```

Troubleshooting

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

10.5 Log Decoders

Are your Security Analytics Log Decoders at version 10.5? If not, you need to upgrade them. For Security Analytics version 10.5, feeds are sent only to version 10.5 Log Decoders.

Feed File Existence

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

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

Do not modify this file.

Group Meta Populated on LD

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

```
http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=e=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=
t=1301 lastSeenTime=2015-Feb-04 22:30:19 lastUpdatedTime=2015-Feb-04
22:30:19 groups=AllOtherGroup, ApacheTomcatGroup
```

In the above text, the group information is bolded.

Device Group Meta on Concentrator

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

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

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

SMS Log File

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

The following are example informational messages:

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

The following are example error messages:

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

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

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

ESMReader

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

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

    <Module "NgEsmReader" "all">        port        "56002"
        ssl            "yes"
        keypath        "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-4838-a2f7-ba7e9a165aae.pem"
        certpath       "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-a2f7-ba7e9a165aae.pem"
        interval       "600"
        query          "all"
    <stats>            </stats>        </Module>    <Module "NgEsmReader" "update">        port        "56002"
        ssl            "yes"
        keypath        "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-4838-a2f7-ba7e9a165aae.pem"
        certpath       "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-a2f7-ba7e9a165aae.pem"
        interval       "60"
        query          "update"
    <stats>            </stats>        </Module></Plugin>
```

2. Run the command:

```
collectd service restart
```

3. Run the following command:

```
tail -f /var/log/messages | grep collectd
```

Verify that ESMReader is reading logstats and there are no errors. If there are any read issues, you will see errors similar to the following:

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

ESMAggregator

1. On Security Analytics, uncomment the verbose flag in `/etc/collectd.d/ESMAggregator.conf`:

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

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

<Module "ESMAggregator">
    verbose 1
    interval "60"
    cache_save_interval "600"
    persistence_dir "/var/lib/netwitness/collectd"
</Module>    </Plugin>
```

2. Run the following:

```
collectd service restart.
```

3. Run the following command:

```
run "tail -f /var/log/messages | grep ESMA"
```

Look for for ESMAggregator data and make sure your logstat entry is available in logs.

Sample output:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
```

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelfff,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: Dis-
patching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelfff/esm_
counter-3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cache-
flowelfff/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-52e4f4d8bffff
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 = Cacheflowelfff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bffff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dis-
patching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelfff/esm_counter-
3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cacheflowelfff/esm_
counter-3.3.3.3 aggregated from 1 log
```

Configure JMX Feed Generator Job Interval

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

To change the feed generator job interval:

1. Open **jconsole** for the SMS service.
2. On the MBeans tab, navigate to **com.rsa.netwitness.sms > API > esmConfiguration > Attributes**.
3. Modify the value for the property **FeedGeneratorJobIntervalInMinutes**.

4. Go to **Operations** under the same navigation tree, and click **commit()**. This persists the new value in the corresponding json file under `/opt/rsa/sms/conf`, and uses the value if SMS is restarted.

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

References

This section describes the System Maintenance user interface. You use this interface to:

- Monitor and maintain services (settings, statistics, command and message syntax, REST API, RSA Console utility, and protocols supported in RSA Security Analytics).
- Display the current Security Analytics 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](#)
- [System Info Panel](#)
- [System Updates Panel - Manual Updates Tab](#)
- [System Updates Panel - Repository Space Management Dialog](#)
- [System Updates Panel - Settings Tab](#)

Health and Wellness

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:

- [Alarms View](#)
- [Event Source Monitoring View](#)
- [Health and Wellness Historical Graph Views](#)
- [Health and Wellness Settings Tab - Archiver](#)
- [Health and Wellness Settings Tab - Event Sources](#)
- [Health and Wellness Settings Tab - Warehouse Connector](#)
- [Monitoring View](#)
- [Policies View](#)
- [System Stats Browser View](#)

Alarms View

Alarms help you monitor hosts and services installed in the Health and Wellness interface. Policy rules, that you define or assign to hosts and services, in the **Policies view** (see [Manage Policies](#)) trigger these alarms.

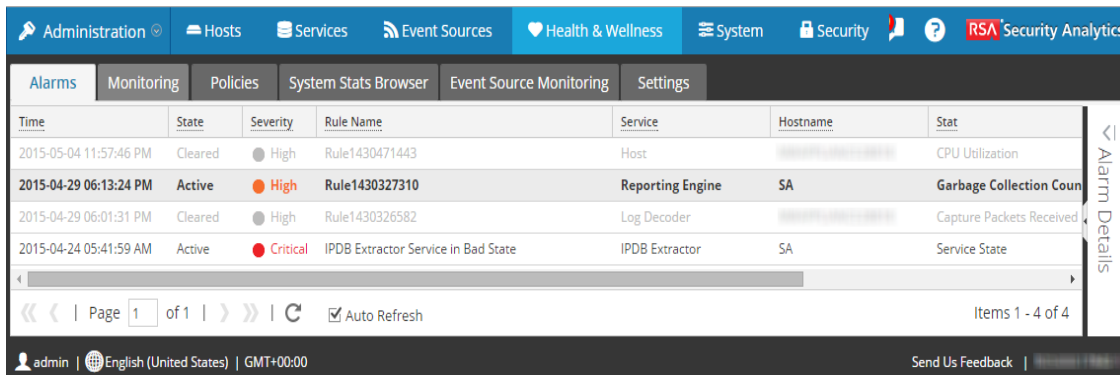
The Alarms view displays the alarms you have set up to alert you when when the user-defined limitations for hosts and services are reached.

The required permission to access this view is **Manage services**. To access the Alarms view:

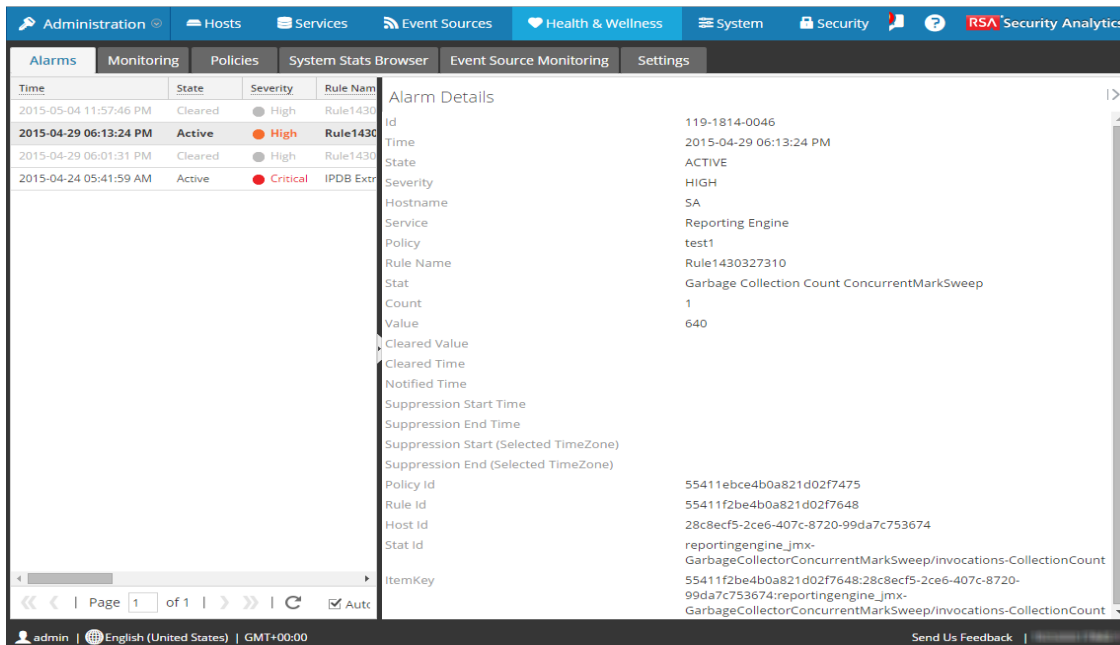
1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

The Health & Wellness Interface opens with the Alarms view displayed. The Alarms view contains an alarms list and an Alarm Details panel.

This figure depicts the Alarms view.



This figure depicts the Alarms tab with the Alarms Details panel expanded.



For the related procedure, see [Monitor Alarms](#)

Alarms List

The alarms list displays all the alarms that you have configured in Security Analytics. You set up the parameters for alarms in [Manage Policies](#). It contains the following information for each alarm.

Note: Security Analytics sorts the alarms in time order. There is no filtering in this view.

Column	Description
Time	Time when alarm was triggered.
State	Status of the alarm: <ul style="list-style-type: none"> • Active - the statistical threshold was crossed triggering the alarm. • Cleared - the clearing threshold was crossed and the alarm is no longer active.
Severity	Severity assigned to this alarm: <ul style="list-style-type: none"> • Critical • High • Medium • Low
Policy	Name of the policy in which the rule that triggers the alarms is defined.
Rule Name	Name of the rule that triggers the alarm.
Service	Service defined in the rule.
Hostname	Host on which the alarm is triggered.
Stat	Statistic selected in the rule that triggers the alarm.
Value	Value of the statistic that triggered the alarm.
Cleared Value	Value of the statistic in the rule that forced the alarm to a cleared state.
Cleared Time	Time when the alarm was forced to a cleared state.
Id	Identification number of the alarm.

From 10.6.3 onwards, the relevant parameters can be sorted in ascending or descending order.

Alarm Details Panel

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

- Notified Time
- Suppression Start Time
- Suppression Start Time
- Suppression Start (Selected TimeZone)
- Suppression End (Selected TimeZone)
- Policy Id
- Rule Id
- Host Id
- Stat Id
- ItemKey

Event Source Monitoring View

Note: This panel is being deprecated. To manage Event Sources, see **About Event Source Management** in the *RSA Security Analytics Event Source Management Guide*.

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

To access the Event Source Monitoring view:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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

2. Click **Event Source Monitoring**.

The Event Source Monitoring view is displayed.

For related procedures, see [Monitor Event Sources](#), [Filter Event Sources](#), and [Create Historical Graph of Events Collected for an Event Source](#).

Filters

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

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

Parameter	Description
Time Frame	Select the time frame for which you want the stats. Select Received if you need the query results to contain only event sources that logs have been received from within the selected time. or Select Not Received if you need the query results to contain only event sources that logs have not been received from within the selected time
Order By	Select the order in which the list needs to be filtered. Select Ascending to filter it in an ascending order.


From 10.6.3 onwards, the relevant parameters can be sorted in ascending or descending order.

Commands

Command	Action
Apply	Click to apply the filters chosen and display the list accordingly.
Clear	Click to clear the chosen filters.
Export as CSV	Click to export the information as a csv file.

Event Source Stats view display

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

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

Health and Wellness Historical Graph Views

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

See the following topics for more details:

- [Overview](#)
- [Parameters](#)


Historical Graph View for Events Collected from an Event Source

Overview

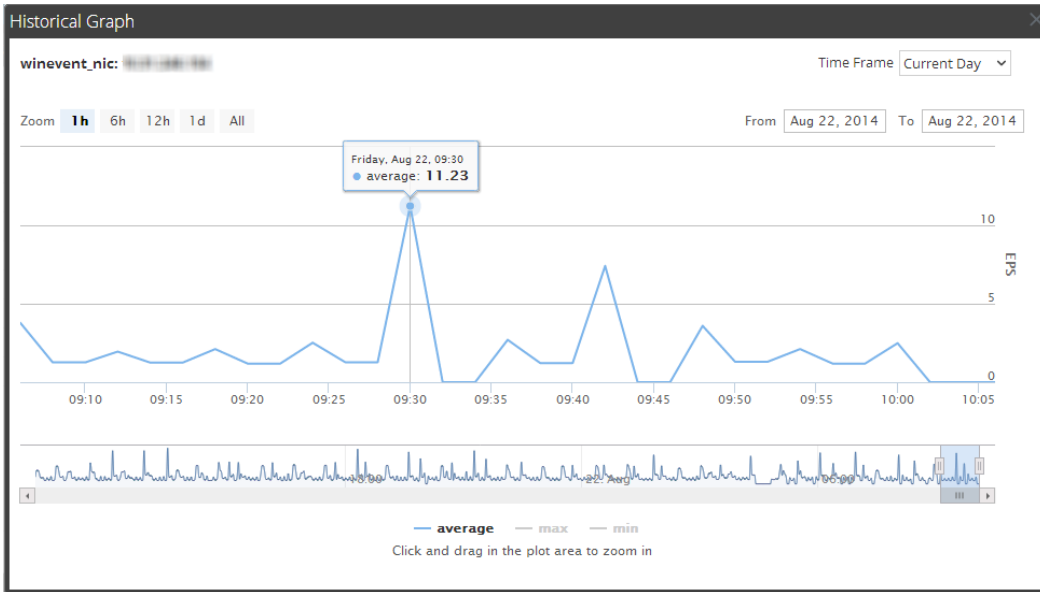
Note: This view is being deprecated. To manage Event Sources, see **About Event Source Management** in the *Event Source Management Guide*.

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

To access this view:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
The Health & Wellness view is displayed with the Monitoring tab open.
2. Click **Event Source Monitoring**.
The **Event Source Monitoring** view is displayed.
3. In the **Historical Graph** column, select .
The Historical graph for the selected event source type is displayed.

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



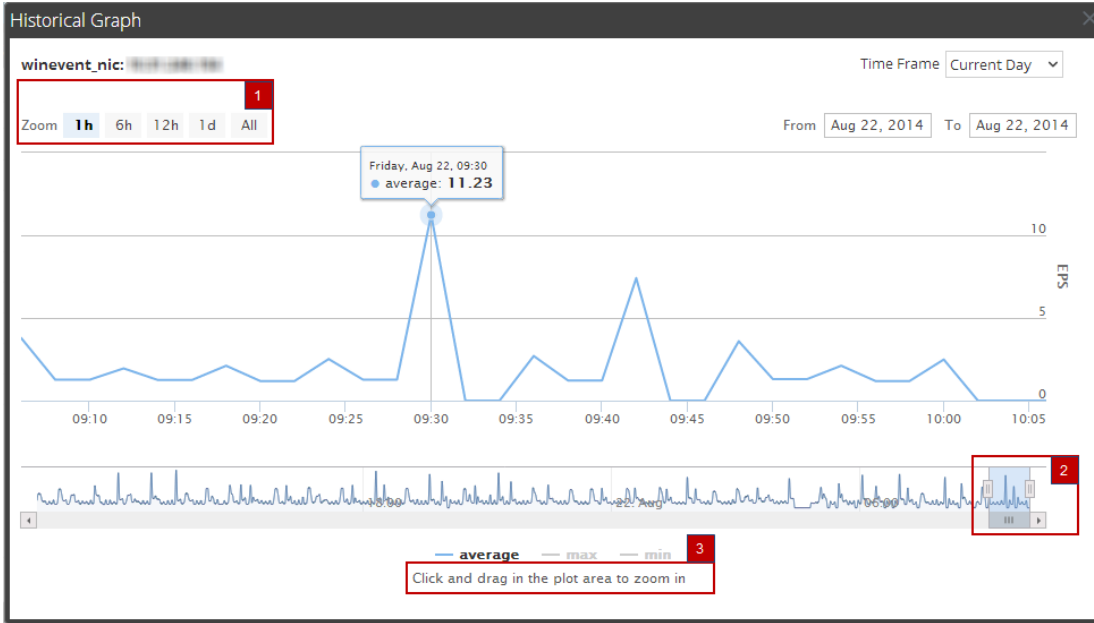
Features

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.
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.

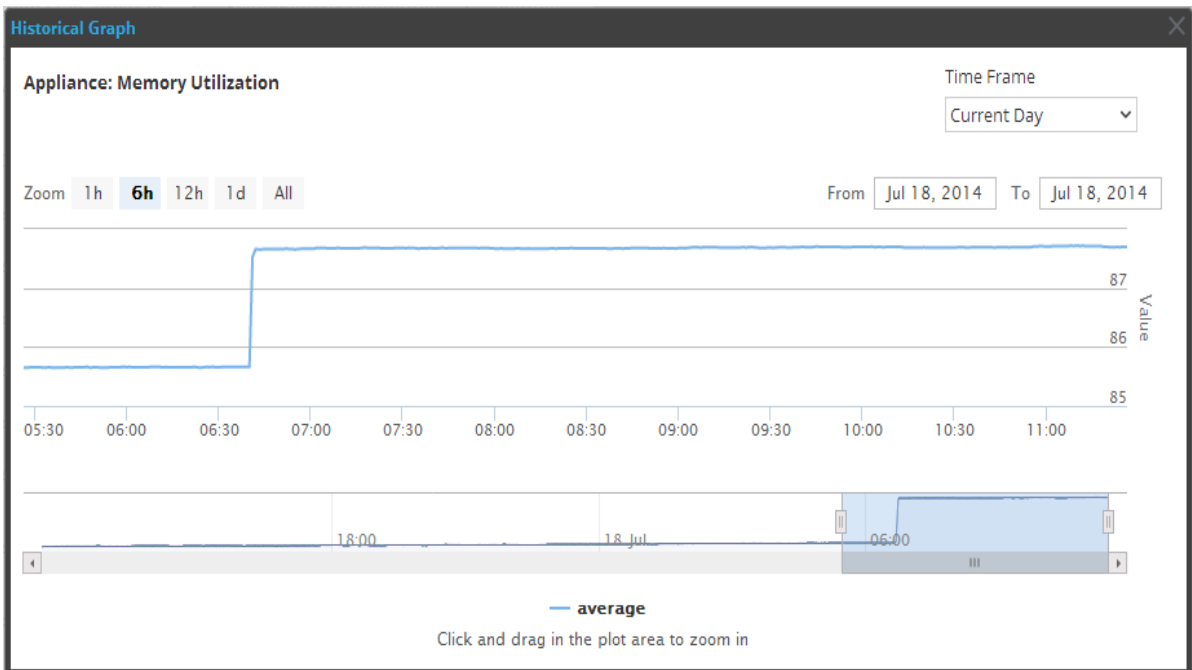
The following figure displays the various zoom functions available.



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

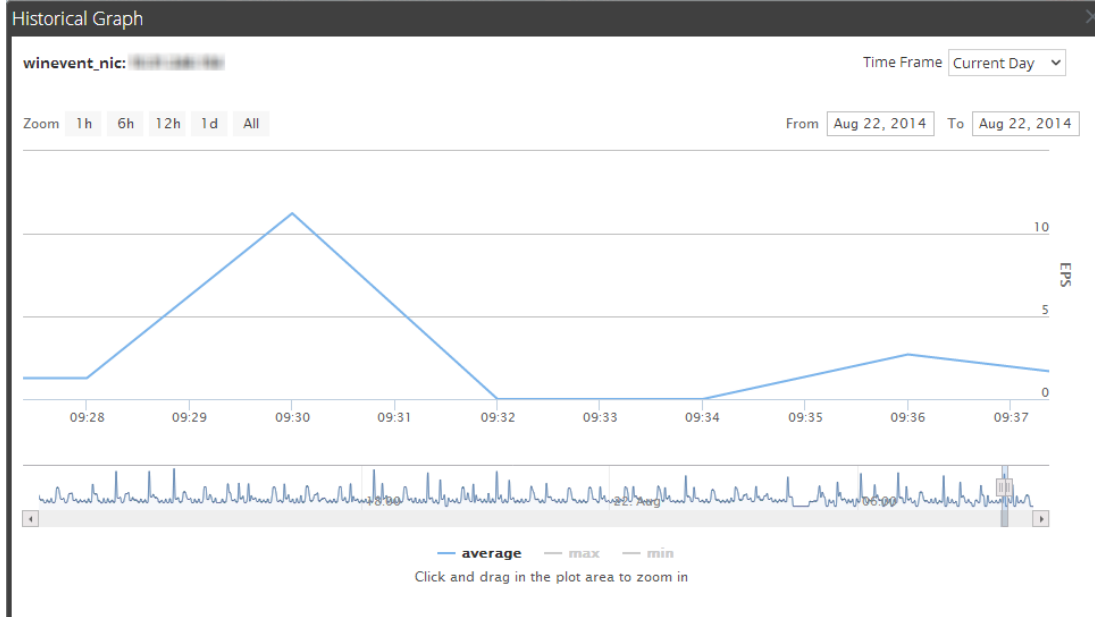
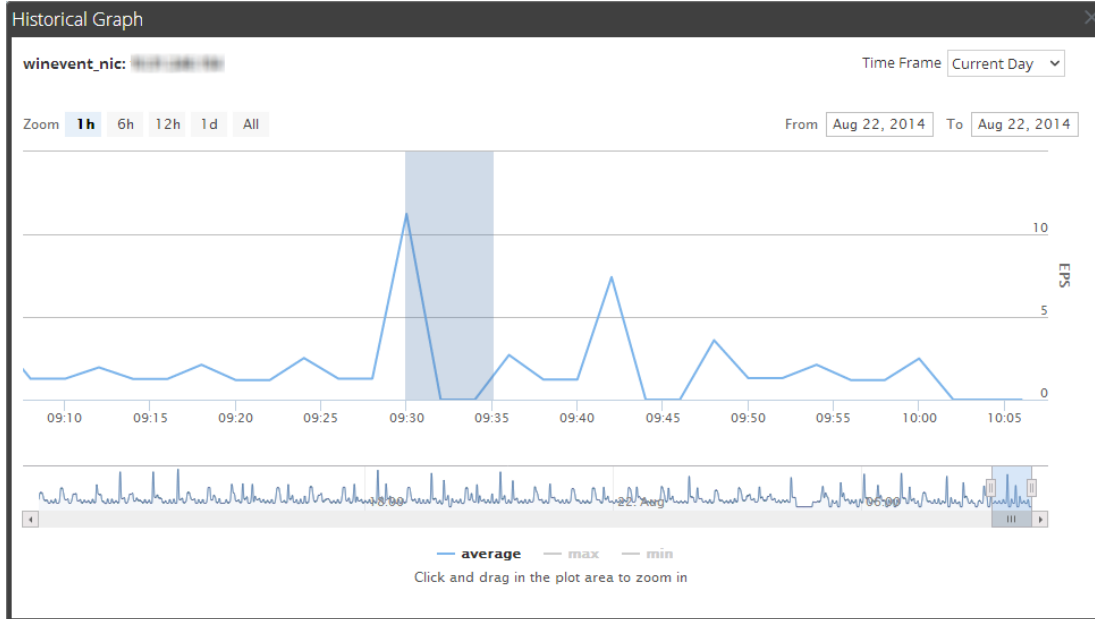
Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.



Zoom In Function 3

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

The figures below display an example of selecting a 5 minute frame and the displaying data in the 5 minute frame.



Historical Graph View for System Stats

To access the Historical Graph view for the System Stats:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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

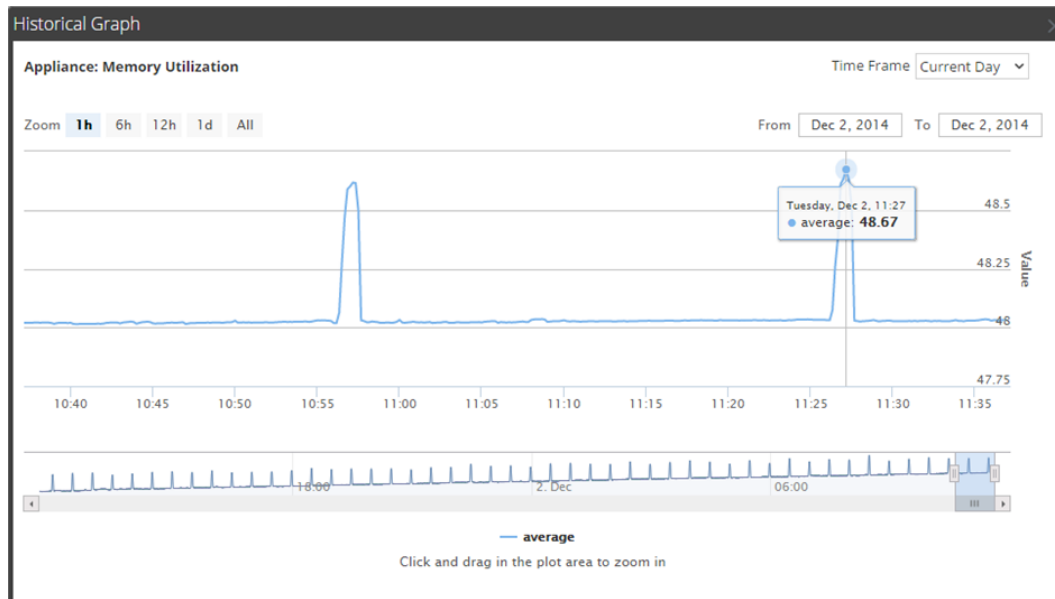
2. Click **System Stats Browser**.

The System Stats Browser view 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.

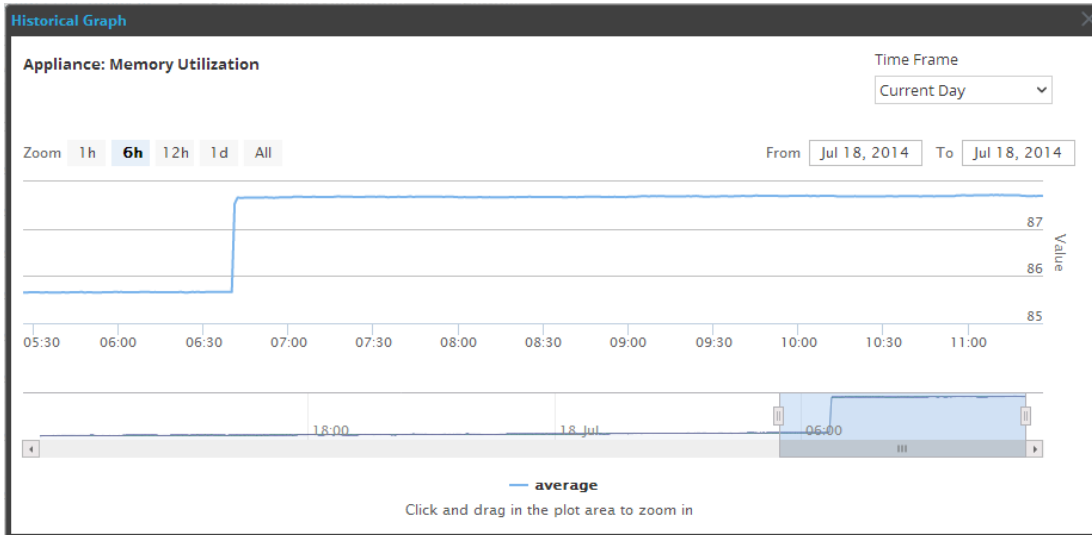
The following figure displays the various zoom functions available.



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.

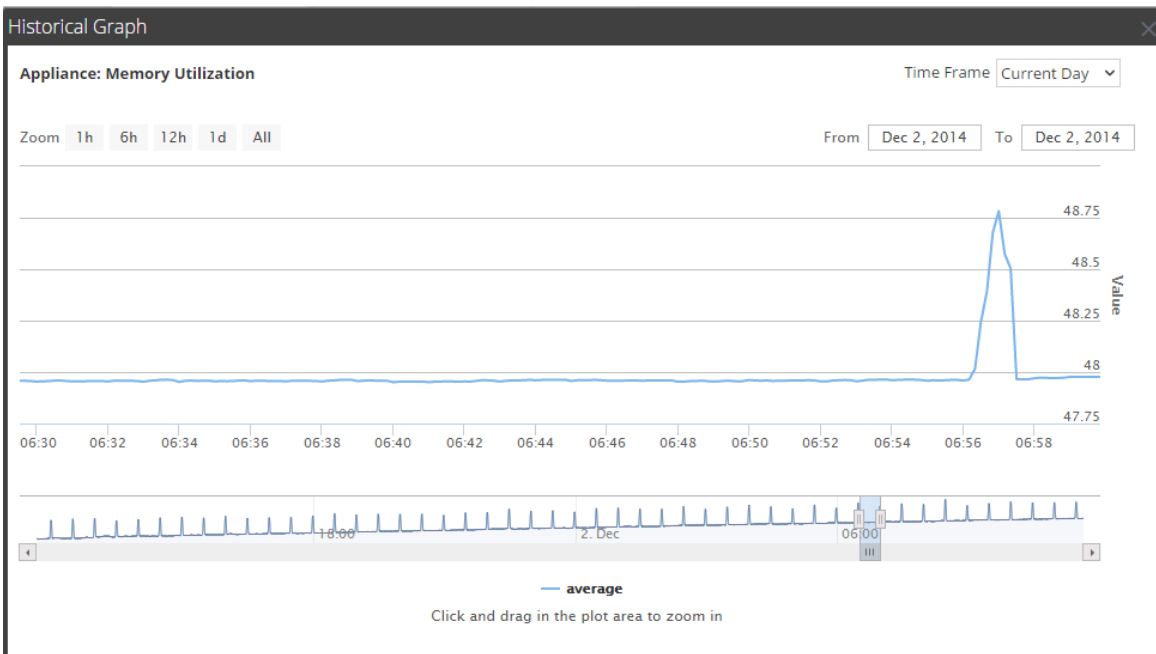
Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.



Zoom in function 3:

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

The figures below display an example of selecting a 30 minute frame and the displaying data in the 30 minute frame.



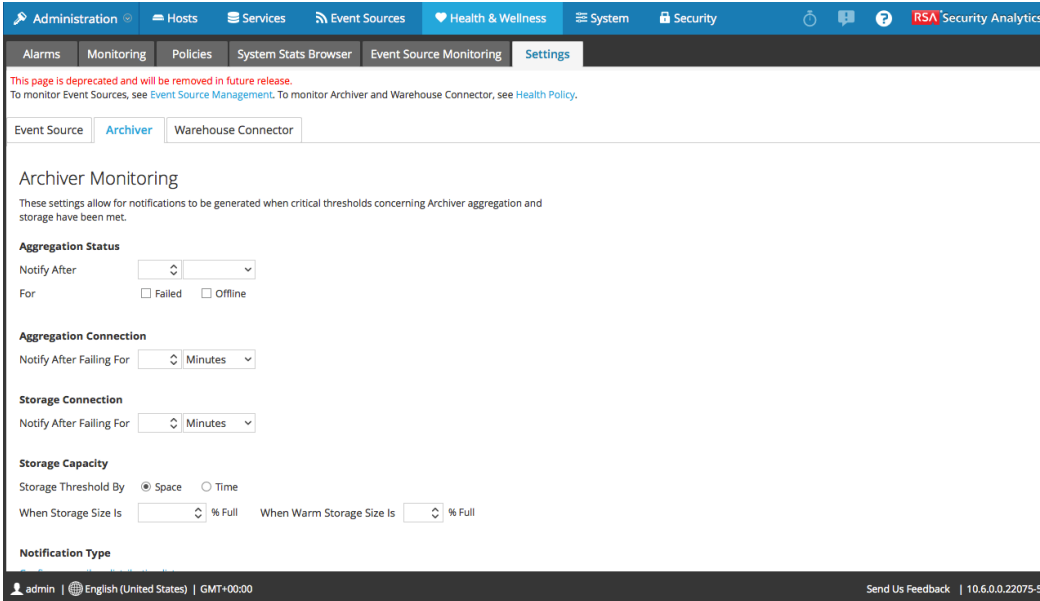
Health and Wellness Settings Tab - Archiver

To access the Archiver Monitoring view:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

2. Select **Settings > Archiver**.

The Archiver Monitoring view is displayed.



Features

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

Parameter	Value	Description
Aggregation Status	Notify After	Number of minutes or hours after which the you will get notified of the Aggregation status
	For	Failed - If enabled, you get notification when the Archiver aggregation status is failed for the defined number of minutes or hours. Offline - If enabled, you get a notification when the Archiver aggregation status is offline for the defined number of minutes or hours
Aggregation Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver aggregation connection fails.

Parameter	Value	Description
Storage Connection	Notify After Failing for	Number of minutes or hours after which you will receive a notification if the Archiver storage connection fails.
Storage Capacity	Storage Threshold By	Select Space , if you want to receive a notification when the Archiver storage capacity exceeds the percentage defined in the When Storage Size Is field. Select Time , if you want to receive a notification when the files stored in the Archiver exceeds the defined number of days in the When Oldest Storage File Is field
	When Storage Size Is	Enter what percent full the storage size should be if you want to receive a notification.
	When Warm Storage Size Is	Enter what percent full the warm storage size should be if want to receive a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in Security Analytics.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.
	SA Console, Email, Syslog Notification, SNMP Trap Notification	Enable SA Console to get notifications on the Security Analytics 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 Tab - Event Sources

Note: This tab is being deprecated. To manage Event Sources, see **About Event Source Management** in the *RSA Security Analytics Event Source Management Guide*.

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

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

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

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Select **Settings > Event Source**.



The Event Source tab is displayed.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Administration', 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' section is active, and the 'Settings' tab is selected. Below the navigation, there are tabs for 'Alarms', 'Monitoring', 'Policies', 'System Stats Browser', 'Event Source Monitoring', and 'Settings'. The 'Event Source Monitoring' tab is active, and the 'Event Source' sub-tab is selected. The main content area displays the 'Event Source Monitoring' configuration page. It includes a warning message: 'This page is deprecated and will be removed in future release. To monitor Event Sources, see Event Source Management. To monitor Archiver and Warehouse Connector, see Health Policy.' Below the warning, there are links for 'Configure email or distribution list' and 'Configure Syslog and SNMP Trap servers'. The main configuration area contains a table with columns for 'Regex', 'Source Type', 'Source Host', and 'Time Threshold' (subdivided into 'Hours' and 'Minutes'). The table is currently empty.


For the related procedure, see [Configure Event Source Monitoring](#).



Features

Event Source Monitoring Panel

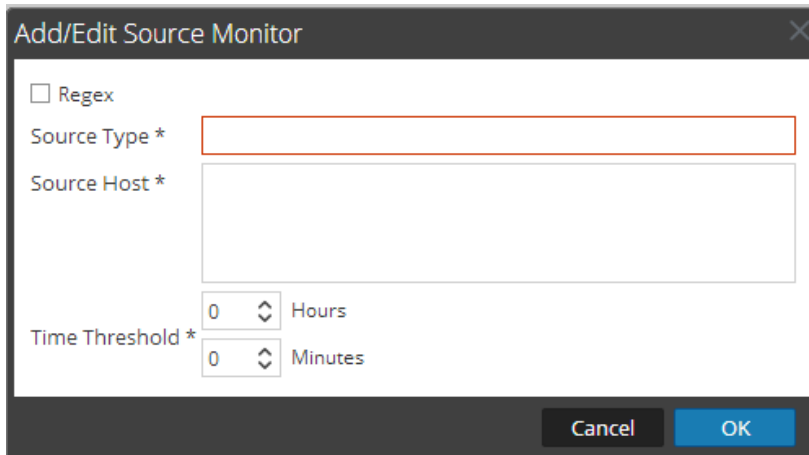
Feature	Description
Configure email or distribution list.	Opens the Administration > System > Email view so you can adjust the email distribution for the Event Source Monitoring output, if necessary.
Configure Syslog and SNMP Trap servers.	Opens the Administration > System > Auditing view so you can adjust the Syslog and SNMP trap distribution for the Event Source Monitoring output, if necessary.
	Displays the Add/Edit Source Monitor dialog in which you add or modify event sources to monitor.
	Deletes the selected event sources from monitoring.
	Selects an event source.
Source Type	Displays the source type of the event source.
Source Host	Displays the source host of the event source.
Time Threshold	Displays the time period after which Security Analytics stops sending notifications (Time Threshold).
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancels any additions, deletion, or changes.

Decommission Panel

Feature	Description
	Displays the Decommission dialog in which you add or modify event sources to decommission.

Feature	Description
	Deletes the selected event sources from decommissioning.
	Selects an event source.
Regex	Displays if you choose to use regular expressions
Source Type	Displays the source type of the decommissioned event source.
Source Host	Displays the source host of the decommissioned event source.
Apply	Applies any additions, deletions, or changes and they become effective immediately.
Cancel	Cancel any additions, deletions, or changes.

Add/Edit Source Monitor Dialog



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

Source Type	Source Host
ciscopix	1.1.1.1
*	1.1.1.1

Source Type	Source Host
*	*
*	1.1.1.1 1.1.1.2
*	1.1.1.[1 2]
*	1.1.1.[123]
*	1.1.1.[0-9]
*	1.1.1.11[0-5]
*	1.1.1.1,1.1.1.2
*	1.1.1.[0-9] 1.1.1.11[0-5]
*	1.1.1.[0-9] 1.1.1.11[0-5],10.31.204.20
*	1.1.1.*
*	1.1.1.[0-9]{1,3}

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

Decommission Dialog

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

Health and Wellness Settings Tab - Warehouse Connector

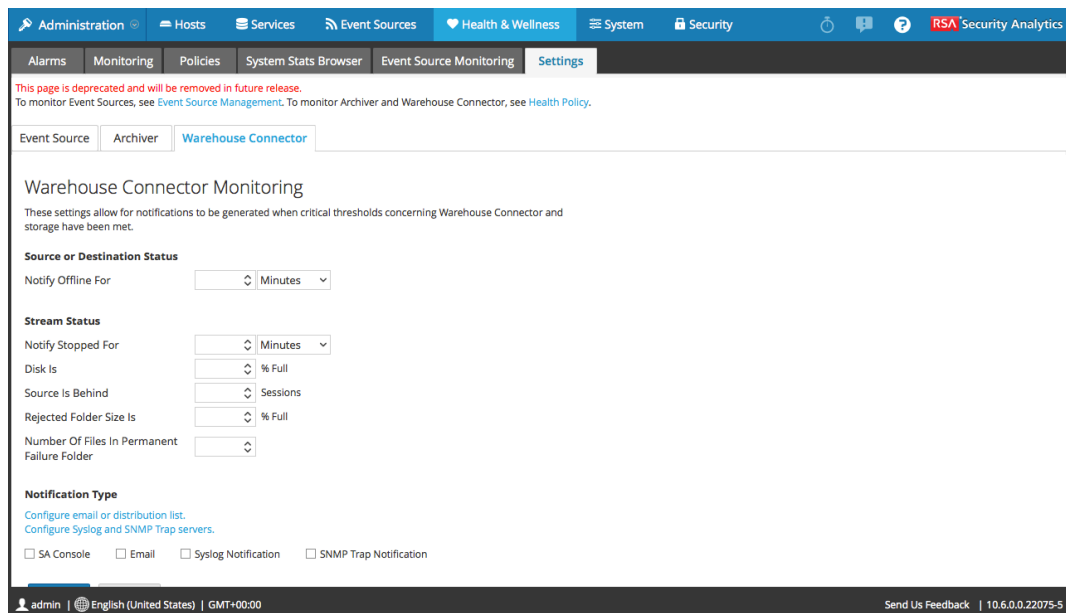
Introduction

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. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Select **Settings > Warehouse Connector**.

The Warehouse Connector Monitoring view is displayed.



Warehouse Connector Monitoring parameters

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

Parameter	Value	Description
Source or Destination Status	Notify Offline For	Number of minutes or hours after which the you will receive a notification if the source or destination connection fails.
Stream Status	Notify Stopped For	Number of minutes or hours after which you would like to receive a notification when the Stream goes offline.
	Disk Is	The limit on the percentage of disk usage after which you would like to receive a notification.
	Source Is Behind	Number of sessions after which a notification is raised if the source goes behind the defined number of sessions.
	Rejected Folder Size Is	Limit on the percentage of folder usage after which you would like to receive a notification.

Parameter	Value	Description
	Number Of Files in Permanent Failure Folder	Limit on the number of files in the permanent failure folder after which you would like to receive a notification.
Notification Type	Configure email or distribution list	Click to configure email so that you can receive notifications in Security Analytics.
	Configure Syslog and SNMP Trap servers	Click to configure audit logs.
	SA Console, Email, Syslog Notification, SNMP Trap Notification	<p>Enable SA Console to get notifications on the Security Analytics UI notification toolbar.</p> <p>Enable Email to get email notifications.</p> <p>Enable Syslog Notification to generate syslog events.</p> <p>Enable SNMP Trap Notification to get audit events as SNMP traps.</p>

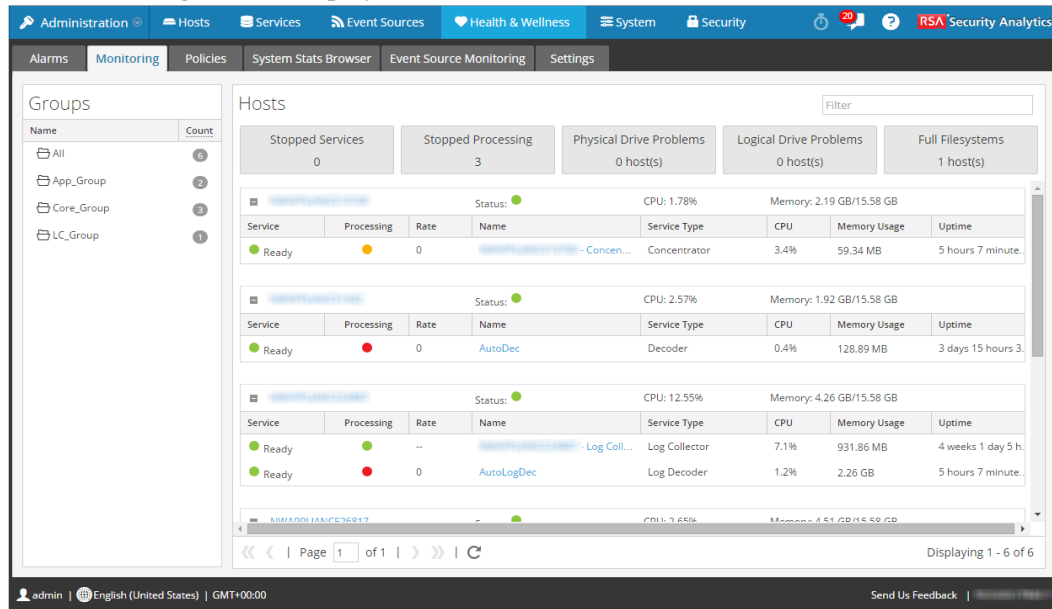
Monitoring View

Security Analytics provides detailed statistics and other information about the host and the individual Security Analytics services on Details views. You can view the current health of all the hosts, services running on the hosts, various aspects of the hosts' health, host details and service details in the Monitoring view. Procedures that you can perform in this view are provided here: [Monitor Hosts and Services](#)

To access this view:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click the **Monitoring** tab.

The Monitoring view is displayed.



Features

Groups Panel

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

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

Hosts Panel


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






Parameter	Description
<input type="text" value="Filter"/>	Type a host name or a service name in the Search box 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.

Parameter	Description
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 filesystems.

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

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

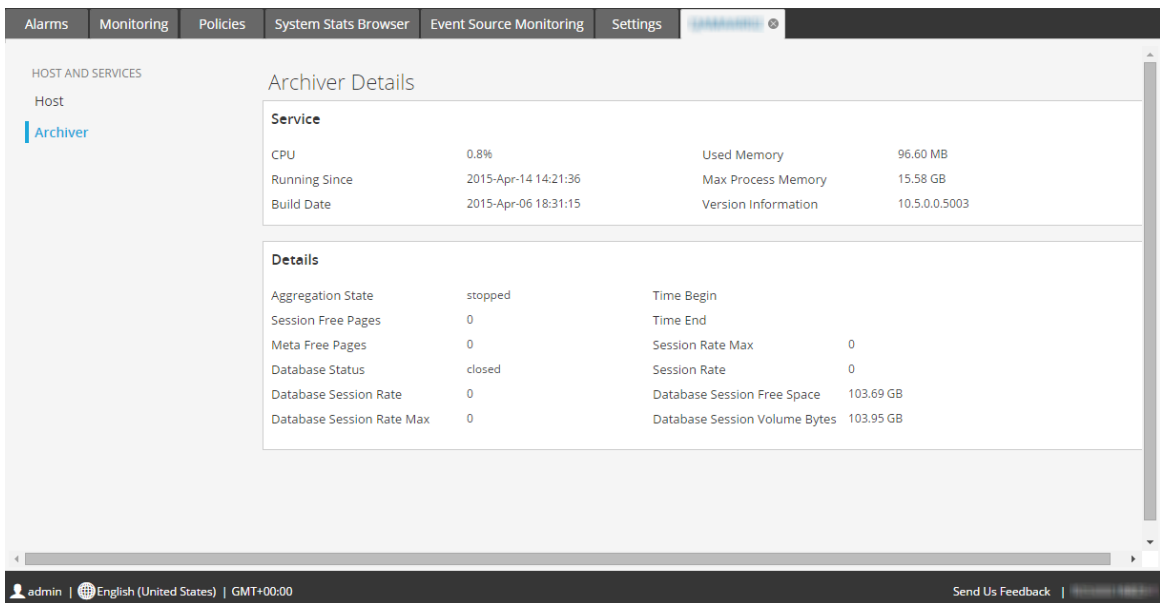
When you click  prefixed to the host name, a list of all the services installed on the host is displayed. The table below describes various parameters displayed for a service and their description.

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

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

Archiver Details View

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



For the related procedure, see [Monitor Service Details](#)

Details Section

This section displays the current generic statistics for the service.

Statistic	Description
Aggregation State	State of data aggregation.

Statistic	Description
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.
Database Status	<p>Status of databases. Valid values are:</p> <ul style="list-style-type: none"> • 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.

Statistic	Description
Database Session Volume Bytes	Number of session bytes in the database.

Broker Details View

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

For the related procedure, see [Monitor Service Details](#).

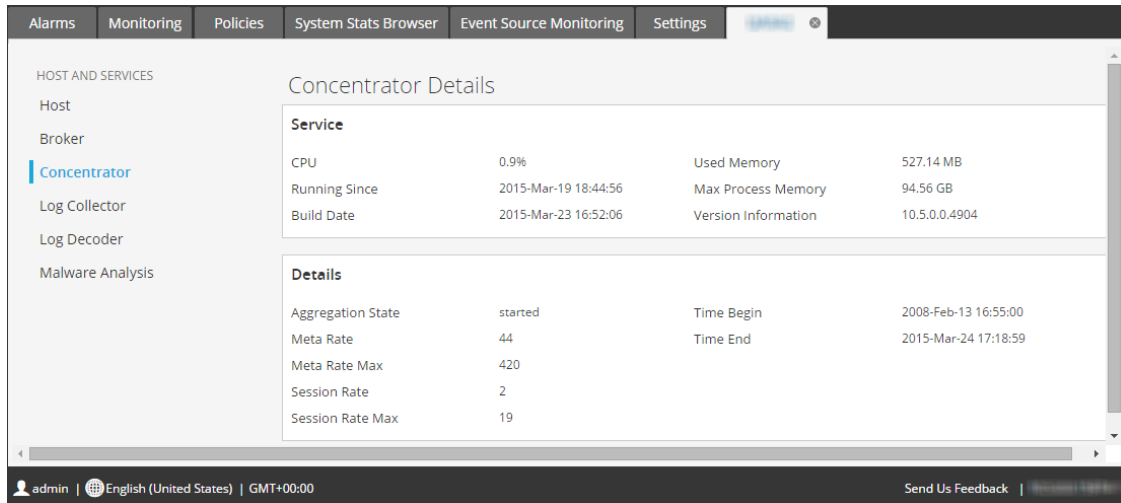
Details Section

This section displays the current generic statistics for the service.

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

Concentrator Details View

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



For the related procedure, see [Monitor Service Details](#)

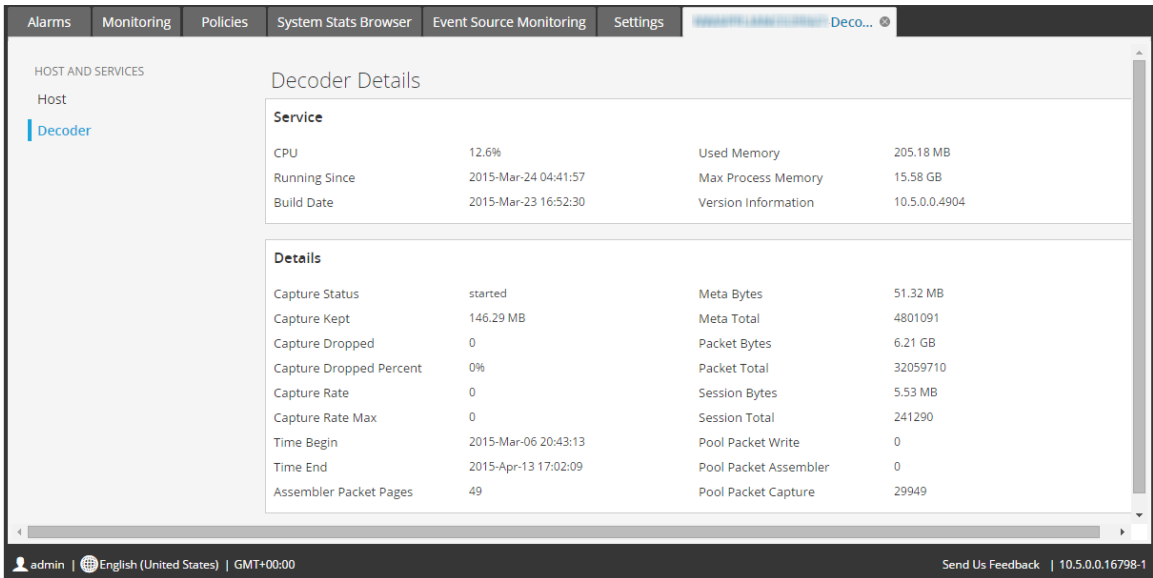
Details Section

The section displays the current generic statistics for the service.

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

Decoder Details View

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



For the related procedure, see [Monitor Service Details](#).

Details Section

This section displays the current generic statistics for the service.

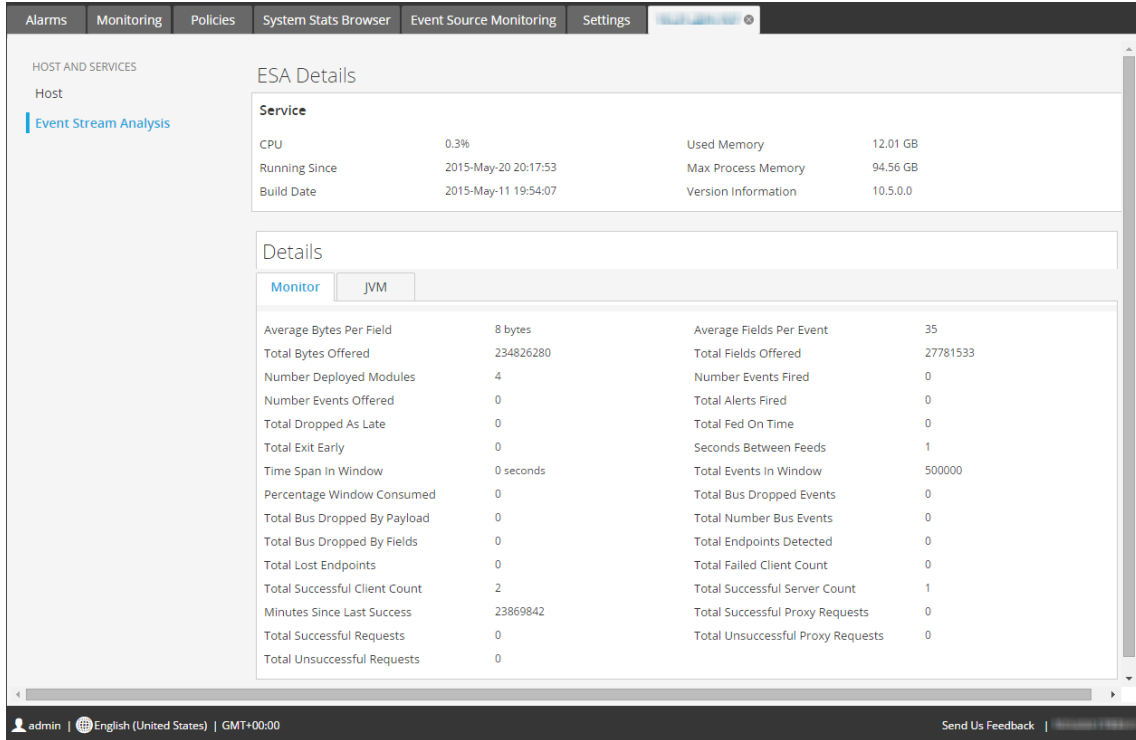
Statistic	Description
Capture Status	Status of data capture. Valid values are: <ul style="list-style-type: none"> • starting - Starting data capture (not capturing data yet). • started- Capturing data. • stopping- Stopping data capture (received request to stop data capture, but not have not stopped 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	Number of metadata in the database.

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

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

Event Stream Analysis (ESA) Details View

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



For the related procedure, see [Monitor Service Details](#).

Details Section

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

Monitor tab

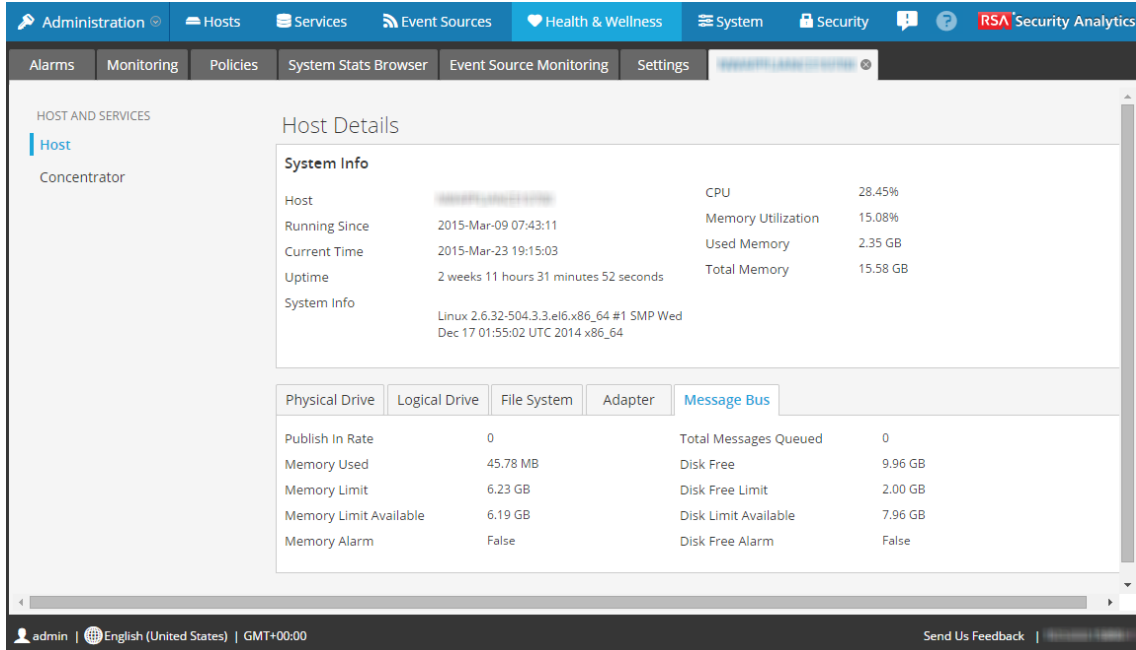
Displays the following generic statistical information for the Event Stream Analysis service:

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

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

Host Details View

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



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

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

For the related procedure, see [Monitor Service Details](#).

System Info Section

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

Parameter	Description
Host	Hostname.
CPU	Current CPU usage of the host.
Running Since	Time when the host was started.
Memory Utilization	Percentage of memory utilized by the host.
Current Time	Current time on the host
Used Memory	Memory used in GB.
Uptime	Time for which the host has been active.

Parameter	Description
Total Memory	Capacity of the memory installed on the system.
System Info	OS version installed on the host.

Tabs

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

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

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

Log Collector Details View

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

The screenshot shows the 'Log Collector Details' view. On the left, there is a navigation pane with 'Log Collector' selected. The main area displays service statistics and a table of collection protocols.

Service Statistics:

Parameter	Value	Parameter	Value
CPU	8.1%	Used Memory	549.69 MB
Running Since	2015-Mar-24 10:15:23	Max Process Memory	15.58 GB
Build Date	2015-Mar-21 01:21:58	Version Information	10.5.0.0.13893

Collection Table:

Transport Protocol	Status	EPS	Total Events	Errors	Warnings
checkpoint	stopped	0	0	0	0
netflow	stopped	0	0	0	0
file	started	0	3200	0	0
sdee	stopped	0	0	0	0
odbc	stopped	0	0	0	0
vmware	stopped	0	0	0	0
syslog	stopped	0	0	0	0
windows	stopped	0	0	0	0

For the related procedure, see [Monitor Service Details](#).

Tabs

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 Security Analytics (see the *Log Collection Getting Started Guide* in the *Log Collection Guides*).

Event Processing tab

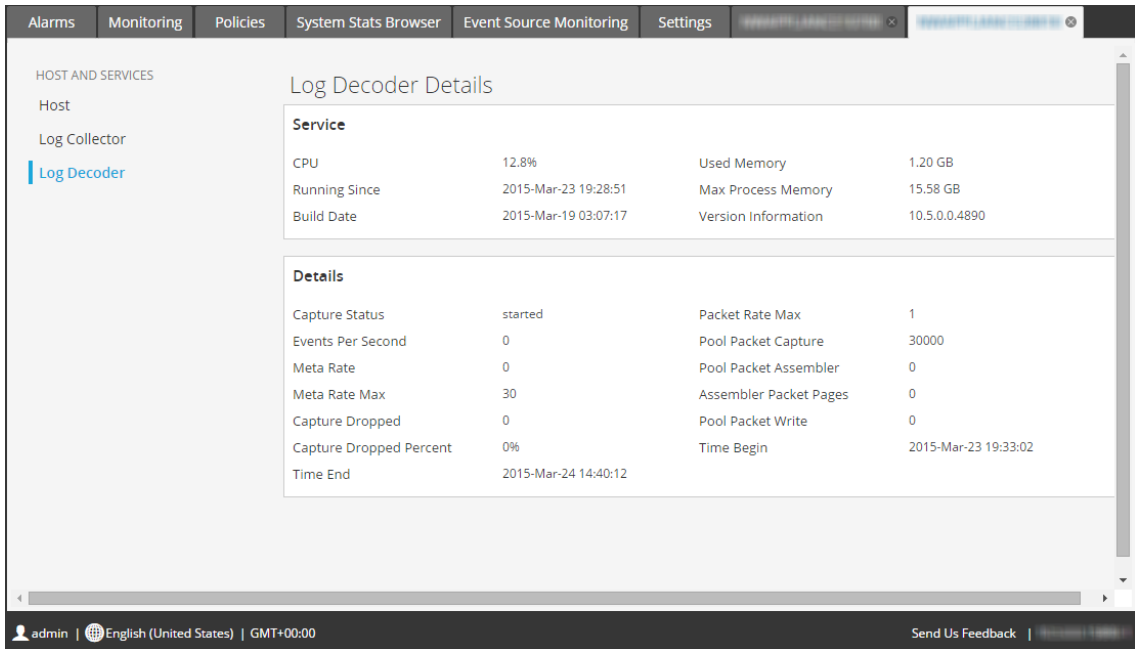
Displays statistics for the Security Analytics internal event processing protocol (that is, the Log Decoder) for Log Collection.

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

Parameter	Description
Status	Status of the Log Decoder. Valid values are: <ul style="list-style-type: none">• starting - Starting data capture (not capturing data yet).• started- Capturing data.• stopping- Stopping data capture (received request to stop data capture, but not have not stopped capturing data yet).• stopped - Not capturing data.• disabled - Not configured as a Decoder service.
EPS	Rate (events per second) at which this the Log Decoder is processing events from the Log Collector.
Total Events	Total events processed by the Log Decoder.
Errors	Number of errors encountered.
Warnings	Number of warnings encountered.
Byte Rate	Current throughput in bytes per second.

Log Decoder Details View

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



For the related procedure, see [Monitor Service Details](#)

Details Section

This section displays the current generic statistics for the service.

Statistic	Description
Capture Status	Status of data capture. Valid values are: <ul style="list-style-type: none"> • 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.

Statistic	Description
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.
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.

Statistic	Description
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 depicts the Malware Details view.

The screenshot shows the Malware Details view with the following data:

Service			
CPU	0.1%	Used Memory	373.98 MB
Running Since	2015-Mar-19 18:44:57	Max Process Memory	94.56 GB
Build Date	2015-Mar-17 20:24:59	Version Information	10.5.0.0.8411

Events			
Number Of Events For Past 24 Hours	0	Average Processing Time	0 milliseconds
Number Of Files For Past 24 Hours	0	Events In Queue	0
Number Of Events For Past 7 Days	0	Events Processed	0
Number Of Files For Past 7 Days	0	Events Per Second Throughput	0
Number Of Events For Past Month	0	Session Time Of Last Event	
Number Of Files For Past Month	0		
Number Of Events For Past 3 Months	1		
Number Of Files For Past 3 Months	1		

For the related procedure, see [Monitor Service Details](#).

Details Section

Events Tab

Displays the following event-related statistical information for the MalwareAnalysis service.

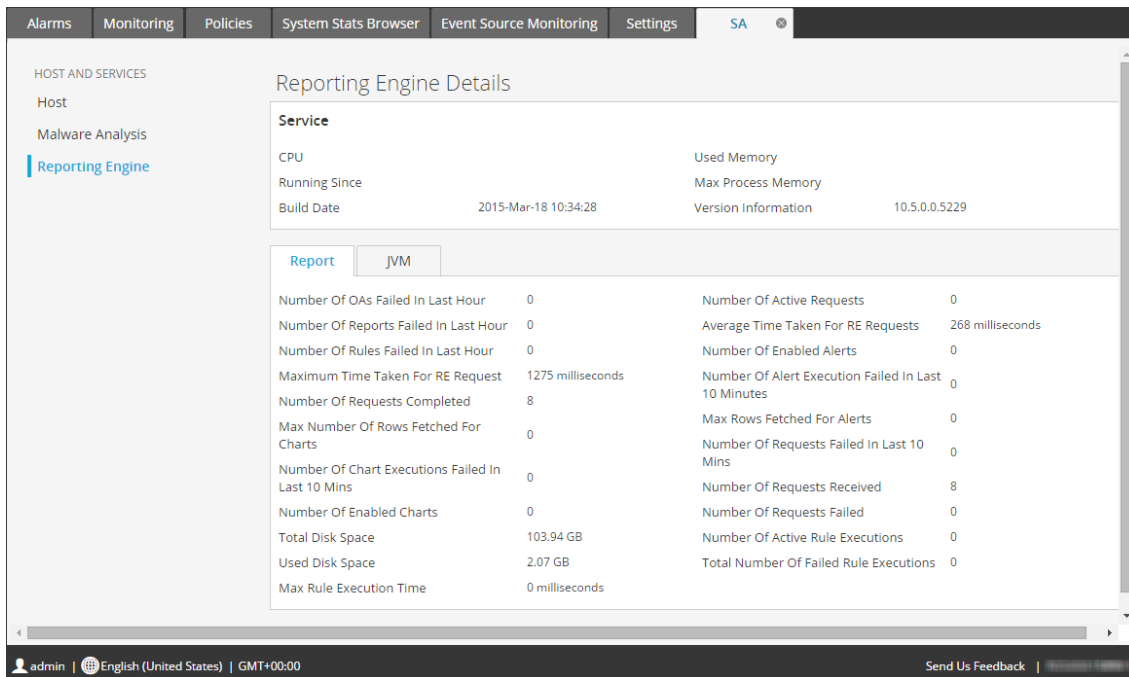
- Number of events for the past 24 hours
- Average processing time
- Number of files for the past 24 hours
- Events in queue

- 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

Reporting Engine Details View

The Reporting Engine Details view provides information for the Reporting Engine, such as the version information, number of active requests, or number of enabled alerts.

The following figure depicts the Reporting Engine Details view.



For the related procedure, see [Monitor Service Details](#).

Details Section

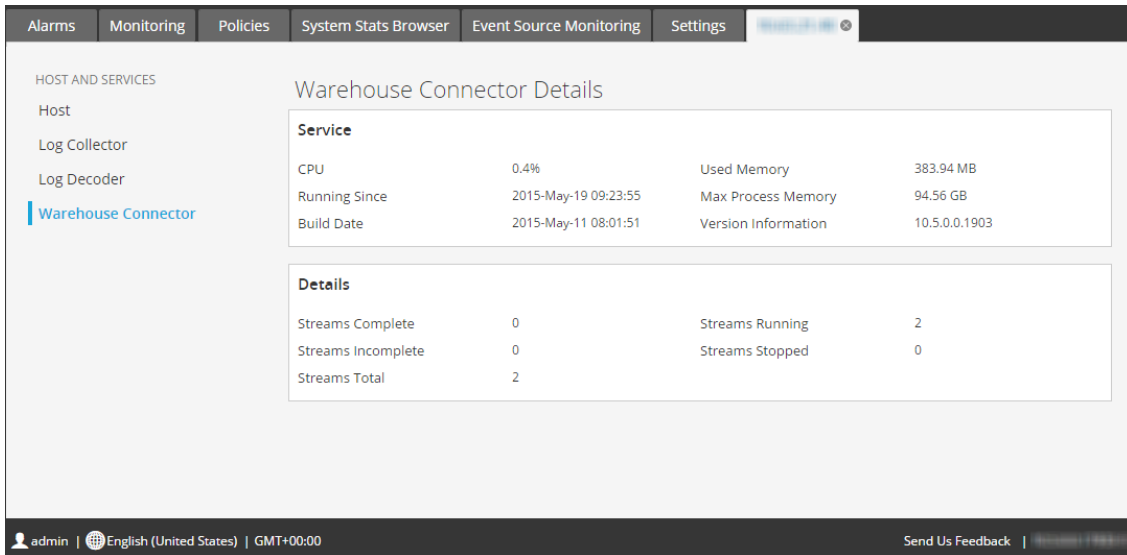
This section consists of the **Report** and **JVM** tabs that show additional statistics.

Report tab

Displays report-related statistical information for the Reporting Engine service.

Warehouse Connector Details View

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



The screenshot displays the 'Warehouse Connector Details' view. The left sidebar lists 'HOST AND SERVICES' including Host, Log Collector, Log Decoder, and Warehouse Connector (selected). The main content area is titled 'Warehouse Connector Details' and contains two data tables.

Service			
CPU	0.4%	Used Memory	383.94 MB
Running Since	2015-May-19 09:23:55	Max Process Memory	94.56 GB
Build Date	2015-May-11 08:01:51	Version Information	10.5.0.0.1903

Details			
Streams Complete	0	Streams Running	2
Streams Incomplete	0	Streams Stopped	0
Streams Total	2		

The bottom status bar shows: admin | English (United States) | GMT+00:00 | Send Us Feedback | 1903

For the related procedure, see [Monitor Service Details](#).

Features

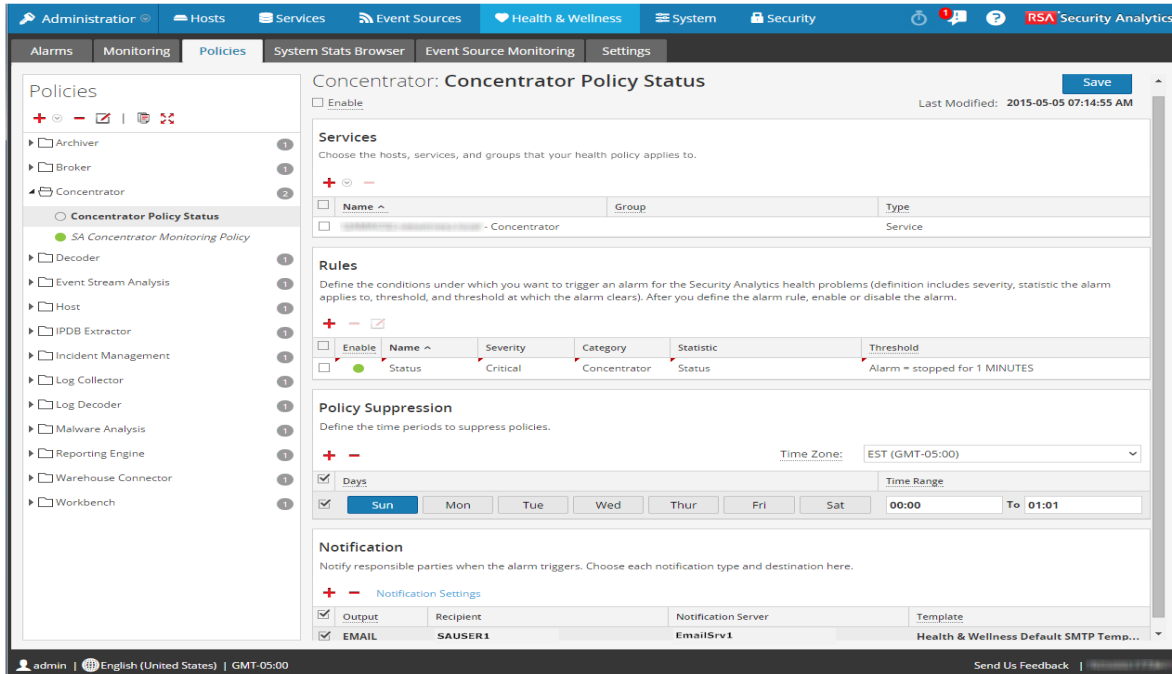
Details Section

This section displays the current generic statistics for the service.

Policies View

Policies view

This figure depicts the Policies view.








How to Access



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

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.
2. Click the **Policies** tab.

Policies Panel


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

Feature	Description
	Displays available service types to create a new policy . Select one so that you can define a policy or policies for it.
	Deletes the selected policy from the Policies panel. You can only delete one policy at a time.
	Allows you to change the name of the policy.
	Creates a copy of the selected policy. For example, if you select First Policy and click  , Security Analytics creates a copy of this policy and names it First Policy (1).





Feature	Description
	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: <ul style="list-style-type: none"> • services and hosts for which you have defined policies. • RSA standard policies that you can apply to hosts and services.

Policy Detail Panel


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

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

Services

	 <p>Displays  menu. Select:</p> <ul style="list-style-type: none"> • Groups to display the Groups dialog from which you select service groups to this policy. • Service/Host to display the Services/Hosts dialog from which you select services to add to this policy. If policy type is Host, the menu will have Host not Service. You can select services based on policy type.
	Deletes the selected service or group from this policy.

Feature	Description
Rules	
	Displays the Add Rule dialog in which you define a rule for this policy.
	Deletes the selected rule from this policy.
	Displays the Edit Rule dialog for the selected rule.
Policy Suppression	
	Adds a policy suppression timeframe row.
	Deletes the selected policy suppression timeframe row.
Time Zone	Select the time zone for the Policy from the drop-down list. This time zone applies to both Policy Suppression and Rule Suppression.
	Select the checkbox to select a policy suppression timeframe row.
Days	Days of the week that you want to suppress the policy according to the time range specified. Click on the day of the week that you want to suppress the policy. You can select any combination of days including all days.
Time Range	Time range during which the policy is suppressed for the days selected.
Notifications	
	Adds a 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.

Feature	Description
	Select the checkbox to select a policy suppression timeframe row.
Type	Display EMAIL . EMAIL is the only type of notification available in this release.
Notification	Select the type of EMAIL notification. See Configure Notification Types in the <i>System Configuration Guide</i> for the source of the values in this drop-down list.
Notification Server	Select the EMAIL notification server. See Configure Notification Servers in the <i>System Configuration Guide</i> for the source of the values in this drop-down list.
Template	Select the Template for this EMAIL notification. RSA provides the Health & Wellness Default SMTP Template and the alarms template. See Configure Notification Templates in the <i>System Configuration Guide</i> for the source of the other values in this drop-down list.
	<p>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.</p>

Groups dialog




Feature	Description
Groups panel	
Name	Displays the service groups you have define. Select: <ul style="list-style-type: none"> • 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.

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

Rules Dialog

Feature	Description
<input type="checkbox"/> Enable	Select and deselect this checkbox to enable and disable the rule for this policy.
Name	Enter the name of the rule.
Description	<p>Added this field in Security Analytics 10.5.0.1.</p> <p>Enter the description of the rule. RSA suggests that you include the following information in this field.</p> <ul style="list-style-type: none"> • 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	<p>Select the severity of the rule. Valid values are:</p> <ul style="list-style-type: none"> • Critical • High • Medium • Low

Feature	Description
Statistic	<p>Select the statistics you want to check with this rule. Select a:</p> <ul style="list-style-type: none"> • statistical category from the left drop-down list. • statistic from the right drop-down list. <div data-bbox="472 470 1414 753" style="border: 1px solid green; padding: 5px;"> <p>Note: For Public Key Infrastructure (PKI) policy, select PKI in the category and statistics as any one of the following:</p> <ul style="list-style-type: none"> - SA Server PKI Certificate Expiration - Displays the time left before the certificate expires. - SA Server PKI CRL Expiration - Displays the time left before the Certificate Revocation List (CRL) expires. - SA Server PKI CRL Status - Displays the current status of the CRL. </div> <p>SA Server PKI Certificate Expiration - Displays the time left before the certificate expires.</p> <p>SA Server PKI CRL Expiration - Displays the time left before the Certificate Revocation List (CRL) expires.</p> <p>SA Server PKI CRL Status - Displays the current status of the CRL.</p> <p>Please refer to the System Stats Browser View for examples of the statistics you may want to check with a rule.</p>
Alarm Threshold	<p>Define the threshold of the rule that will trigger the policy alarm:</p> <ul style="list-style-type: none"> • operator: <ul style="list-style-type: none"> • For Security Analytics 10.5 (=, !=, <, <=, >, or >=) • For Security Analytics 10.5.0.1 and later (See Threshold Operators below) • amount <div data-bbox="472 1451 1414 1661" style="border: 1px solid green; padding: 5px;"> <p>Note: For CRL expiry the supported format is ddddhhmm, for example:</p> <ul style="list-style-type: none"> - 10000 represent 1 day - 2359 represent 23 hours and 59 minutes - 10023 represent 1 day and 23 minutes - 3650100 represent 365 days and 1 hour </div> <ul style="list-style-type: none"> • time in minutes

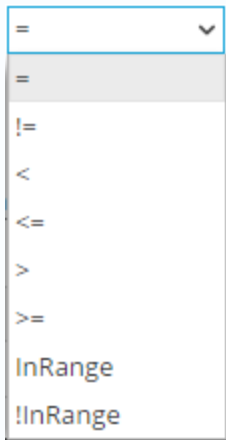
Feature	Description
Recovery	Define the when to clear the threshold of the rule: <ul style="list-style-type: none"> operator: <ul style="list-style-type: none"> For Security Analytics 10.5 (=, !=, <, <=, >, or >=) For Security Analytics 10.5.0.1 and later (See Threshold Operators below) amount time in minutes
Rule Suppression	
	Adds a rule suppression timeframe row.
	Deletes the selected rule suppression timeframe row.
	Select the checkbox to select a rule suppression timeframe row.
Time Zone:	Displays the Policy time zone. You select the time zone for a policy in the <i>time-zone</i> Policy Suppression panel.
Days	Days of the week that you want to suppress the rule according to the time range specified. Click on the day of the week that you want to suppress the rule. You can select any combination of days including all days.
Time Range	Time range during which the rule is suppressed for the days selected.

In Security Analytics 10.5.0.1, RSA added threshold operator support as described in the following **Threshold Operators** section.

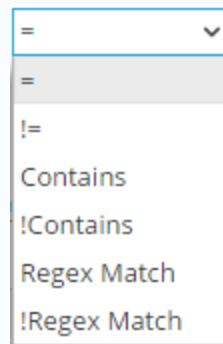
Threshold Operators

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 drown-down menu:



String operators drop-down menu:



RSA Health & Wellness Email Templates

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

Health & Wellness Default SMTP Template



File Collection Service is off on HOST1000

State
Active

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
Check Point

Rule
File Collection Service is off

Statistic
Collection State

Value
stopped

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

Alarms Template

RSA Security Analytics

Health Alarm Notification

File Collection Service is off on HOST1000

State
Cleared

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
BootCamp Notification

Rule
Check Point Collection is off

Statistic
Collection State

Value
Policy-Disabled

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

Security Analytics Out-of-the-Box Policies

Security Analytics Out-of-the-Box Policies

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

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

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

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

- Delete them.
- Edit Policy names.

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

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

Policy Name	Rule Name	Alarm Triggered
SA Host Monitoring Policy	Critical Usage on Rabbitmq Message Broker Filesystem	For <code>var/lib/rabbitmq</code> , 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 96%.
	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 <code>var/lib/rabbitmq</code> goes over 60%.
	Host Unreachable	Host down.
	LogCollector Event Processor Exchange Bindings Status	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Bindings	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	LogCollector Event Processor Queue with No Consumers	Issue with Log Collection Message Broker Queues for 10 minutes or more.
	Power Supply Failure	Host not receiving power.
RAID Logical Drive Degraded	For Raid Logical Drive, Drive State equals Degraded or Partially Degraded.	

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

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

Policy Name	Rule Name	Alarm Triggered
Security Analytics 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
Security Analytics 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.
Security Analytics Event Steam Analysis Monitoring Policy	ESA Overall Memory Utilization > 85%	Total ESA Memory Usage % is greater than or equal to 85 %.
	ESA Overall Memory Utilization > 95%	Total ESA Memory Usage % is greater than or equal to 95 %.
	ESA Service Stopped	Server Status does not equal started.
	ESA Trial Rules Disabled	Trial Rules Status does not equal enabled.

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

Policy Name	Rule Name	Alarm Triggered
Security Analytics 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.
Security Analytics Malware Analysis Monitoring Policy	Malware Analysis Service Stopped	Server Status does not equal started.

Policy Name	Rule Name	Alarm Triggered
Security Analytics 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 <20%	Available disk space is less than 20% with medium severity.
	Reporting Engine Available Disk <10%	Available disk space is less than 10% with high severity.
	Reporting Engine Available Disk <5%	Available disk space is less than or equal to 5% with critical severity.
	Reporting Engine Charts Critical Utilization	Charts Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Rules Critical Utilization	Rules Utilization is greater than or equal to 10 for 5 minutes or more.
	Reporting Engine Schedule Task Pool Critical Utilization	Schedule Task Pool Utilization is greater than or equal to 10 for 15 minutes or more.
	Reporting Engine Service Stopped	Server Status does not equal started.
	Reporting Engine Shared Task Critical Utilization	Shared Task Pool Utilization is greater than or equal to 10 for 5 minutes or more.

Policy Name	Rule Name	Alarm Triggered
Security Analytics 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 or 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%.
Security Analytics 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

Security Analytics 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.

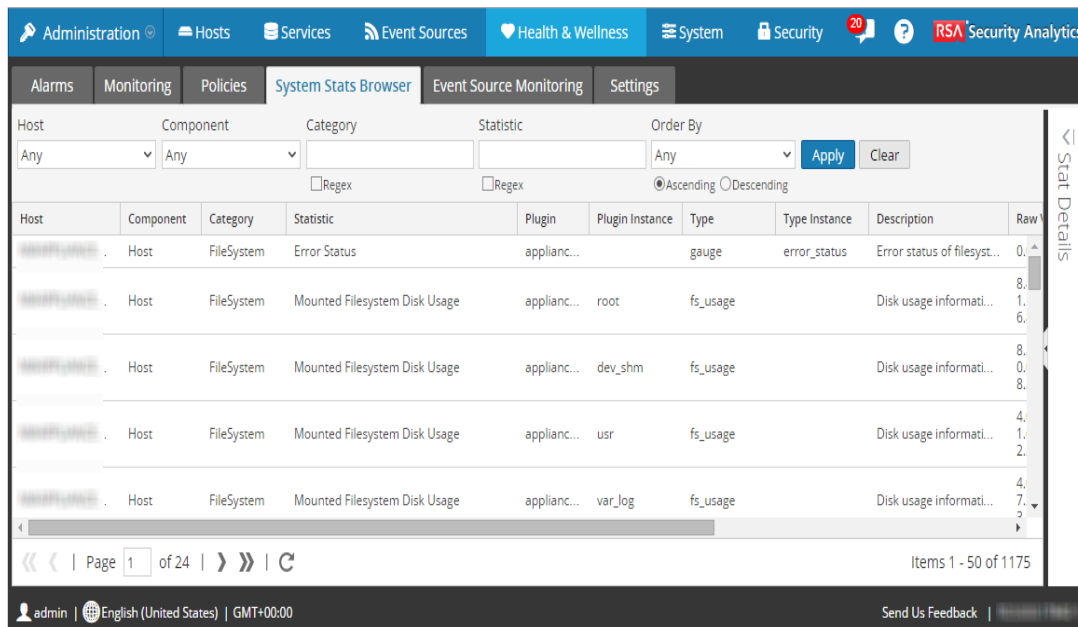
To access the System Stats Browser view:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**.

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

2. Click **System Stats Browser**.

The System Stats Browser view is displayed.



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.

Parameter	Description
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.

From 10.6.3 onwards, the relevant parameters can be sorted in ascending or descending 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 section appears with details of the selected stats.

The screenshot displays the RSA Security Analytics interface, specifically the System Stats Browser. The top navigation bar includes tabs for Administration, Hosts, Services, Event Sources, Health & Wellness, System, Security, and RSA Security Analytics. Below this, there are sub-tabs for Alarms, Monitoring, Policies, System Stats Browser, Event Source Monitoring, and Settings. The System Stats Browser is active, showing a table of statistics and a detailed view on the right. The table has columns for Host, Component, Category, and Statist. The detailed view shows fields like Hostname, Component ID, Name, Subitem, Path, Plugin, Plugin Instance, Type, Type Instance, Description, Category, Last Updated Time, Value, Raw Value, Graph Data Key, Stat Key, subitem, category, Filesystem, Mounted On, and Multi Value.

System Info Panel

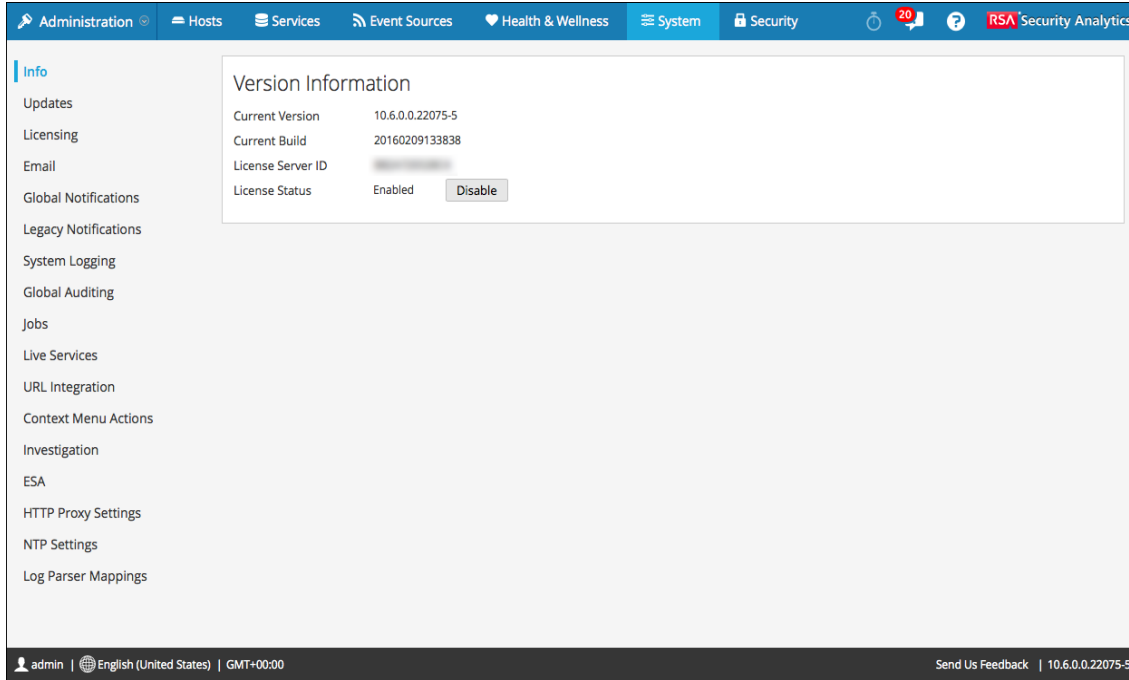
Introduction

This topic describes the System Information panel that 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:

- In the **Security Analytics** menu, select **Administration > System**.
- From the **Administration** module, click **System** in the **Security Analytics** toolbar.
The System Information panel is displayed by default.
- When you receive a notification that a new version of Security Analytics is available in the Notifications tray, click **View**.



Features

The Version Information section displays version information about the version of Security Analytics that is currently installed.

The following table describes the features of the Version Information section.

Name	Description
Current Version	<p>Displays the version of Security Analytics that is currently running. The format of the version is <i>major-release.minor-release.stability-id.build-number</i>. Possible values for the <i>stability-id</i> are:</p> <ul style="list-style-type: none"> • 1 - Development • 2 - Alpha • 3 - Beta • 4 - RC • 5 - Gold
Current Build	Identifies the current build revision for use in troubleshooting situations.

Name	Description
License Server ID	<p>Each client host is shipped with the Local Licensing Server (LLS) installed to manage host licenses. This field indicates whether the LLS is installed for this instance of Security Analytics.</p> <ul style="list-style-type: none"> When the LLS is installed, the Licensing Server ID is displayed. Unknown indicates that the LLS is not installed.
License Status	<p>Indicates whether or not the license is enabled. If the license is:</p> <ul style="list-style-type: none"> 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 - Manual Updates Tab

Introduction

This topic describes the interface tab that you use to upload RSA software updates to your Local Update Repository. If you are connected to the Live Update Repository, Security Analytics automatically makes the latest software updates available in the Hosts View. If you are not connected to the Live Update Repository, or you cannot find the software version you want in the Hosts view, you can upload version updates manually using the **Manual Updates** tab.

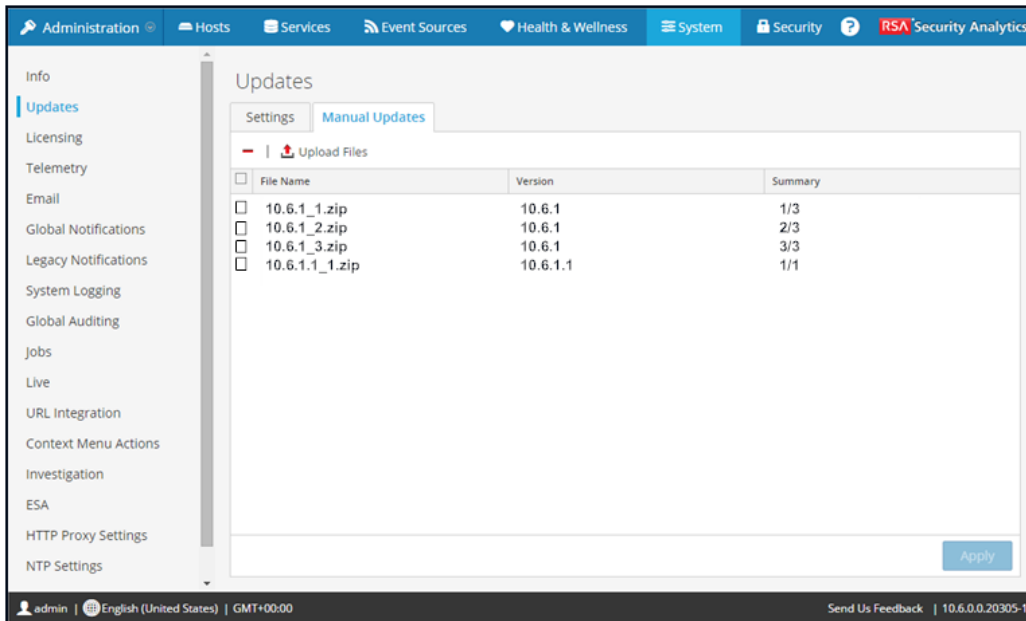
The required permission to access this view is **Apply System Updates**.

To access this view:

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Updates**.





The System Updates panel is displayed with the Updates Repository tab open.

3. Select the **Manual Updates** tab.



Features

This table describes the Manual Updates tab features.

Feature	Description
	Deletes selected zip files.
 Upload Files	<p>Opens the Upload Files dialog. Use this dialog to upload software version update package zip files downloaded to your the local file system to the Manual Updates tab. The features of this dialog are:</p> <ul style="list-style-type: none">  - Opens the last local directory accessed from this computer. If the downloaded software version update package zip files are not in this directory, browse to the correct directory. Select the package zip file or files you want and click Open.  - Deletes the selected zip file. <p>File Name - The software version update package zip filename.</p> <p>Upload - Uploads the software version update zip package file or files that you selected from your local directory to the Manual Updates tab.</p> <p>Close - Closes the dialog.</p>
File Name	The software update version zip filename.

Feature	Description
Version	The version update in the zip file.
Summary	A description of the version zip file. For example, 1/3 if the zip file is the first of three zip files for that update.
Apply	Adds the selected zip files to your Local Update Repository for use in updating hosts. Security Analytics unzips them and displays Updates Available under Status the Hosts view. You can select and apply these software version updates to a host from the Hosts view.

System Updates Panel - Repository Space Management Dialog

Introduction

This topic describes Repository Management dialog that you use to manage the disk space in your Local Update Repository.

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

To access this view:

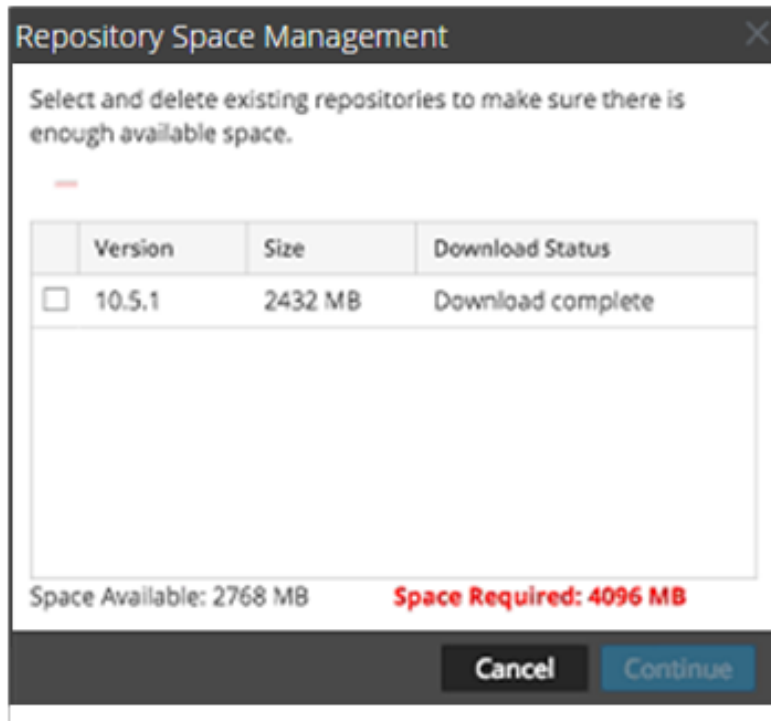
1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Updates**.

The System Updates panel is displayed with the Settings tab open.

3. Click **Manage Repository**.


The Repository Space Management dialog is displayed with the contents of your Local

Update Repository and the space available.



Features

This table describes the features in the Settings tab.

Feature	Description
	Deletes selected versions.
Version	Displays the version updates in your Local Update Repository.
Size	Displays the size of each version update in your Local Update Repository.
Download Status	Displays the download status of each version update in your Local Update Repository.
Cancel	Closes the dialog without making any changes (Displayed when the Local Update Repository is empty).
Continue	Deletes the selected version updates.

Feature	Description
Close	If there are no version updates in your Local Update Repository, closes the dialog.

System Updates Panel - Settings Tab

Introduction

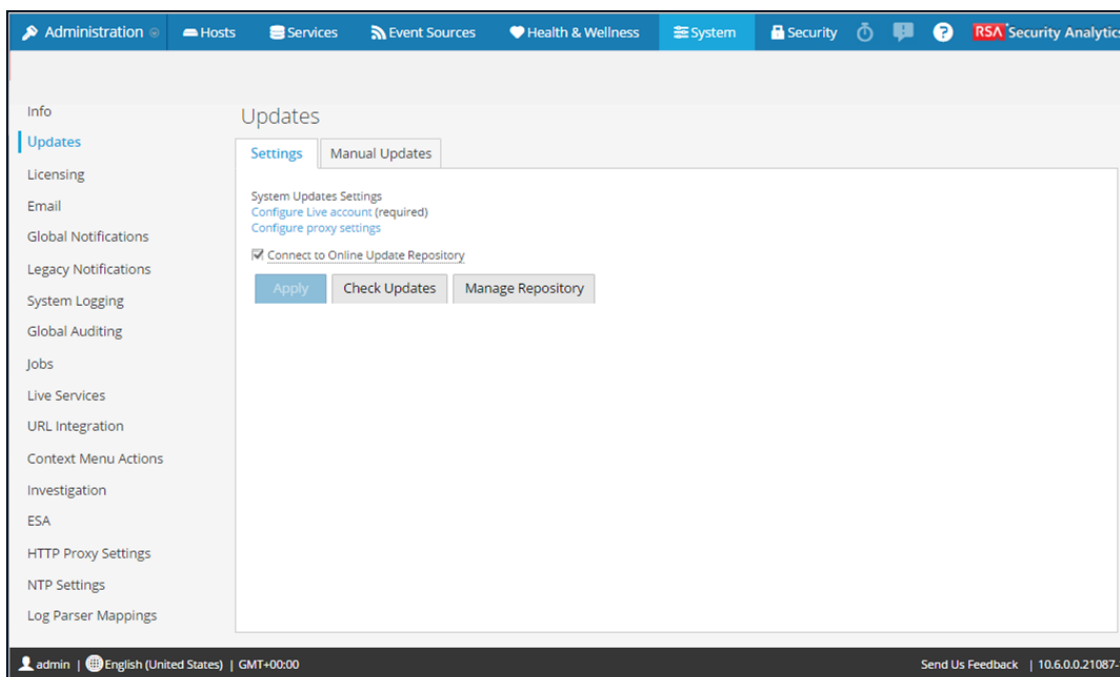
This topic describes the interface that you use to set up a connection to Live Update Repository. These settings ensure that Security Analytics can reach the Live Update Repository and synchronize it with your Local Update Repository.

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

To access this view:

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Updates**.

The System Updates panel is displayed with the Settings tab open.



Features

This table describes the features in the Settings tab.

Feature	Description
Configure Live account	Displays the Administration > System > Live panel in which you can configure your Live Account credentials if they are not configured.
Configure proxy settings	Displays the Administration > System > HTTP Proxy Settings panel in which you can configure an HTTP proxy if it is not configured.
Connect to Live Update Repository	Select to enable automatic synchronization with the RSA update repository. The default value is not connected.
Apply	Applies the settings in this tab.
Check Updates	Checks the Live Update Repository to determine if there are any updates available.
Manage Repository	Opens the Repository Space Management dialog in which you can manage the disk space of your Local Update Repository.