RSA NETWITNESS® PLATFORM

Upgrade Guide

for RSA NetWitness® Platform 11.4.1

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

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

Distribution

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

May 2020

Contents

Upgrade Overview

RSA NetWitness® Platform 11.4.1.0 provides enhancements and fixes for all products in the Platform. The components of the platform are: The NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, Security server, and Source server), Archiver, Broker, Concentrator, Context Hub, Decoder, Standalone Endpoint server, Endpoint Broker, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Health & Wellness Beta, Log Collector, Log Decoder, Log Hybrid, Log Hybrid Retention, Malware Analysis, Network Decoder, Network Hybrid, Reporting Engine, UEBA, and Warehouse Connector.

Note: The Reporting Engine is installed on the NetWitness Server (NW Server) host, Workbench is installed on the Archiver host, and Warehouse Connector can be installed on the Decoder host or Log Decoder host.

The instructions in this guide apply to both physical and virtual hosts (including AWS and Azure Public Cloud) unless stated to the contrary.

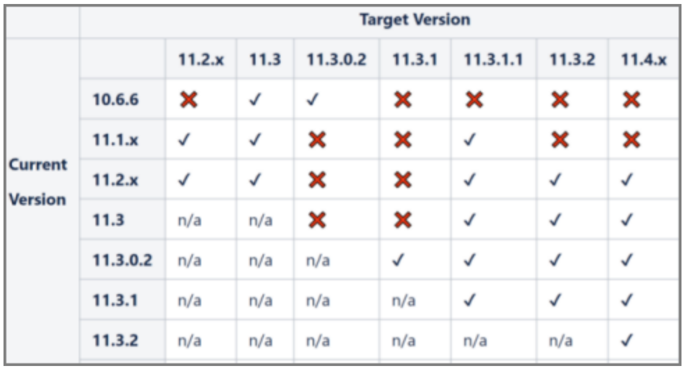
Upgrade Path

The following upgrade paths are supported for NetWitness Platform 11.4.1.0:

- RSA NetWitness® Platform 11.2.x.x to 11.4.1.0
- RSA NetWitness® Platform 11.3.0.x to 11.4.1.0
- RSA NetWitness® Platform 11.3.1.x to 11.4.1.0
- RSA NetWitness® Platform 11.3.2.x to 11.4.1.0
- RSA NetWitness® Platform 11.4.0.x to 11.4.1.0

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.
If you are upgrading from NetWitness Platform version 10.6.6.x, you must upgrade to 11.3.0.2, upgrade to 11.4.0.0, and then upgrade from 11.4 to 11.4.1.0. See the *RSA NetWitness Platform 10.6.6.x to 11.3 Physical Host Upgrade Guide* and *RSA NetWitness Platform 10.6.6.x to 11.3 Virtual Host Upgrade Guide* for instructions on how to upgrade 10.6.6.x to 11.3.0.2.

The following matrix shows all the supported upgrade paths.



		Target Version						
		11.2.x	11.3	11.3.0.2	11.3.1	11.3.1.1	11.3.2	11.4.x
Current Version	10.6.6	✗	✓	✓	✗	✗	✗	✗
	11.1.x	✓	✓	✗	✗	✓	✗	✗
	11.2.x	✓	✓	✗	✗	✓	✓	✓
	11.3	n/a	n/a	✗	✗	✓	✓	✓
	11.3.0.2	n/a	n/a	n/a	✓	✓	✓	✓
	11.3.1	n/a	n/a	n/a	n/a	✓	✓	✓
	11.3.2	n/a	n/a	n/a	n/a	n/a	n/a	✓

Running in Mixed Mode

Running in mixed mode occurs when some services are upgraded to the latest version and some services are on older versions. See "Running in Mixed Mode" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for further information.

Upgrade Considerations for ESA Rule Deployments

Caution: In NetWitness Platform 11.3 and later versions, the ESA Correlation service contains data source changes that require changes to migrated ESA rule deployments. The newer ESA Correlation service replaces the Event Stream Analysis service in 11.2.x.x versions.

If you are upgrading from 11.2.x.x to 11.4 or later, migrated ESA rule deployments have the following changes.

1. If an ESA rule deployment contains two services before you upgrade to 11.4 or later, the deployment splits into two deployments. You can only have one ESA Correlation service in an ESA rule deployment in version 11.4 or later.
2. If an ESA service has multiple ESA rule deployments before you upgrade to 11.4 or later, they are combined into one deployment in version 11.4 or later.

You can still access your old deployments. For a detailed example, see the *ESA Configuration Guide for RSA NetWitness Platform 11.4*.

Change to Column Groups in the Events View

To improve consistency when loading results in the Events view, the number of columns in a column group is limited to 40.

After you upgrade to 11.4 or later, column groups migrated to the Events view from the Legacy Events view still function with more than 40 columns. However, when you edit those groups, you receive a warning that tells you to reduce the number of columns below the limit of 40 columns.

Feedback on Product Documentation

You can send an email to sahelpfeedback@emc.com to provide feedback on NetWitness Platform documentation.

Contacting Customer Care

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com/

Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/rsa-customer-support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Enhanced Support Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Upgrade or Install Windows Legacy Collection

IMPORTANT: If you are currently running NW 11.2.0 with a Windows Legacy Collector (WLC) in your environment and are planning on upgrading to NW 11.4.x, you must first upgrade all components including WLC to 11.2.1 or 11.3, and then you can upgrade all components and WLC to NW 11.4.x.

Refer to the *Windows Legacy Collection Guide for RSA NetWitness 11.x* (https://community.rsa.com/docs/DOC-103165).

Note: After you update or install Windows Legacy Collection, reboot the system to ensure that Log Collection functions correctly.

Upgrade Tasks

> **Note:** For RSA NetWitness Endpoint customers only, Endpoint Hybrid is not supported in 11.3.0.0 and later releases.
> If you have deployed an Endpoint Hybrid host in 11.2.x.x and did not install an Endpoint Log Hybrid host in 11.3.x.x or 11.4.0.x, you must install an Endpoint Log Hybrid host in 11.4.1. See the *Physical Host Installation Guide for RSA NetWitness Platform* or the *Virtual Host Installation Guide for RSA NetWitness Platform* for instructions on how to install an 11.4 Endpoint Log Hybrid on a physical host.

> **Note:** After upgrading the primary NW Server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4.1. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

> **Note:** If you are using S4s devices that use SD cards, SSH to NW Server and run the following command before starting the upgrade process.
> ```
> manage-stig-controls --disable-control-groups 7 --host-id <node uuid>
> ```

> **Note:** Before upgrading the hosts make sure that the time on each host is synchronized with the time on the NetWitness Server.
> To synchronize the time do one of the following:
> - Configure the NTP Server. For more information, see "Configure NTP Servers" in the *System Configuration Guide*.
> - Run the following commands on each hosts:
> 1. SSH to NW host.
> 2. Run the following commands.
> ```
> systemctl stop ntpd
> ntpdate nw-node-zero
> systemctl start ntpd
> ```

You can choose one of the following upgrade methods based on your Internet connectivity. They are listed in the order recommended by RSA.

- User Interface Method with Connectivity to the Internet
- User Interface with No Connectivity to the Internet (available for upgrades from 11.3.1 or later)
- Command Line Interface (CLI) with No Connectivity to the Internet

The following rules apply when you are upgrading hosts for all of these upgrade methods:

- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.

User Interface Method with Connectivity to the Internet

You can use this method if the NW Server host is connected to Live Services and if you are able to obtain the package.

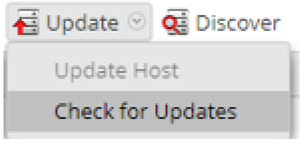
Prerequisites

Make sure that:

1. The **Automatically download information about new upgrades every day** option is selected and is applied in **ADMIN** > **System** > **Updates**.
2. Go to **Admin** > **HOSTS** > **Update** > **Check for Updates** to check for updates. The Host view displays the **Update Available** status.
3. 11.4.1.0 is available in the **Update Version** column.

Procedure

1. Go to **Admin** > **HOSTS**.
2. Select the NW Server (`nw-server`) host.
3. Check for the latest updates.

4. Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.
5. Select **11.4.1.0** from the **Update Version** column. If you:
   - Want to view a dialog with the major features in the upgrade and information on the updates, click the information icon (ⓘ) to the right of the upgrade version number.
   - Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show Update Available. By default, only supported updates for the selected host are displayed.
6. Click **Update** > **Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click **Reboot Host**.
9. Repeat steps 6 to 8 for other hosts.

Note: You can select multiple hosts to upgrade at the same time only after updating and rebooting the NW Server host. All ESA, Endpoint, and Malware Analysis hosts should be upgraded to the same version as that of the NW Server host.

User Interface with No Connectivity to the Internet

Caution: The offline User Interface method is only available if you are upgrading a host from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1 to 11.4.1.0. If you are upgrading a host on an earlier version, you must use the Command Line Interface (CLI) with No Connectivity to the Internet method. After you complete Step 5 in Task 2. Apply Upgrades from the Staging Area to Each Host, go to Upgrading from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1.

Caution: If you are upgrading a host from 11.4.0.0 or 11.4.0.1 to 11.4.1.0 using the offline User Interface method, in Step 5 of Task 2. Apply Upgrades from the Staging Area to Each Host, the upgrade will fail with the message Download error. You can still complete the upgrade successfully by following the steps in Upgrading from 11.4.0.0 or 11.4.0.1 to 11.4.1.0 .

Task 1. Populate Staging Folder (`/var/lib/netwitness/common/update-stage/`) with Version Upgrade Files

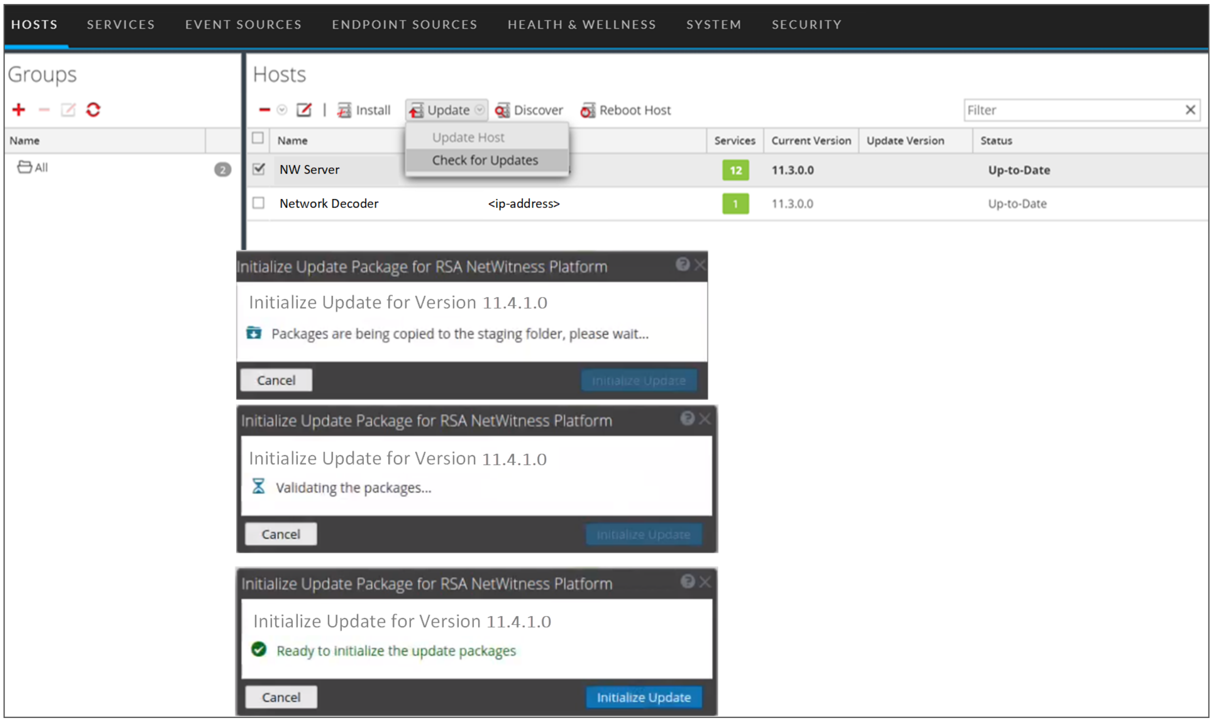
1. Download the upgrade package from RSA Link (https://community.rsa.com/) > Downloads > NetWitness Platform > Version 11.4 to a local directory:
    - If you are upgrading from 11.2.x.x or 11.3.x.x, download `netwitness-11.4.0.0.zip` and `netwitness-11.4.1.0.zip`
    - If you are upgrading from 11.4.x.x, download `netwitness-11.4.1.0.zip`
2. SSH to the NW Server host.
3. Copy `netwitness-11.4.1.0.zip` (and `netwitness-11.4.0.0.zip` if upgrading from 11.2.x.x or 11.3.x.x) from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.
   For example:
   ```
   sudo cp /tmp/netwitness-11.4.1.0.zip /var/lib/netwitness/common/update-stage/
   ```

   Note: NetWitness Platform unzips the file automatically.

Task 2. Apply Upgrades from the Staging Area to Each Host

Caution: You must upgrade the NW Server host before upgrading any non-NW Server host.

1. Log in to NetWitness Platform.
2. Go to **Admin** > **HOSTS**.
3. Check for updates and wait for the upgrade packages to be copied, validated, and ready to be initialized.



	Name		Services	Current Version	Update Version	Status
☑	NW Server		12	11.3.0.0		Up-to-Date
□	Network Decoder	<ip-address>	1	11.3.0.0		Up-to-Date

Initialize Update Package for RSA NetWitness Platform

Initialize Update for Version 11.4.1.0

Packages are being copied to the staging folder, please wait...

Initialize Update Package for RSA NetWitness Platform

Initialize Update for Version 11.4.1.0

Validating the packages...

Initialize Update Package for RSA NetWitness Platform

Initialize Update for Version 11.4.1.0

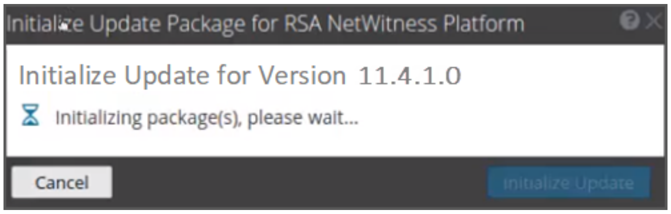
Ready to initialize the update packages

"Ready to initialize packages" is displayed if:

- NetWitness Platform can access the upgrade package.
- The package is complete and has no errors.

Refer to Troubleshooting Version Installations and Updates for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

4. Click **Initialize Update**.



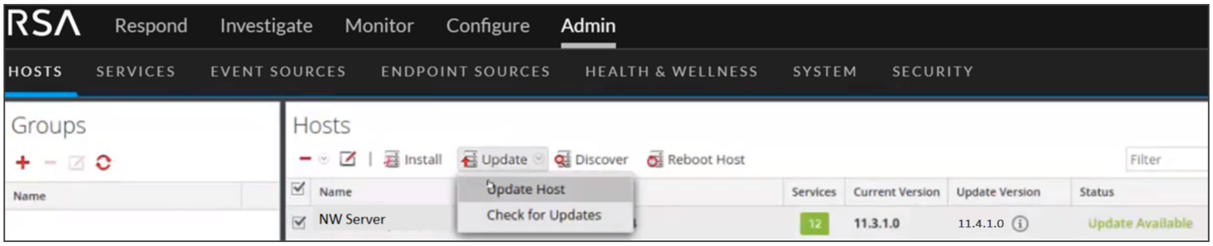
Initialize Update Package for RSA NetWitness Platform

Initialize Update for Version 11.4.1.0

Initializing package(s), please wait...

It takes some time to initialize the packages because the files are large and need to be unzipped. After the initialization is successful, the **Status** column displays Update Available and you complete the rest of the steps in this procedure to finish the upgrade of the host.

5. Click **Update** > **Update Hosts** from the toolbar.



	Name	Services	Current Version	Update Version	Status
☑	NW Server	12	11.3.1.0	11.4.1.0 ⓘ	Update Available

Upgrading from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1

After you click **Update Hosts** in step 5, complete these steps:

1. Click **Begin Update** from the Update Available dialog.
   After the host is upgraded, it prompts you to reboot the host.
2. Click **Reboot Host** from the toolbar.

Upgrading from 11.4.0.0 or 11.4.0.1 to 11.4.1.0

After you click **Update Hosts** in step 5, the upgrade will fail with the message Download error. You can successfully complete the upgrade by following these steps.

1. In the Command Line Interface (CLI):
   a. SSH to NW Server.
   b. Run the following command:
   ```
   upgrade-cli-client –-upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.0
   ```
2. After the NW Server is successfully updated, log in to the NW Server user interface and go to **Admin** > **HOSTS**, where you are prompted to reboot the host.
3. Click **Reboot Host** from the toolbar.

You can upgrade all the other hosts directly from the user interface:

1. Click **Begin Update** from the Update Available dialog.
   After the host is upgraded, it prompts you to reboot the host.
2. Click **Reboot Host** from the toolbar.

Command Line Interface (CLI) with No Connectivity to the Internet

Follow the instructions in Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface .

Post Upgrade Tasks

This topic is divided into two sections. Complete the tasks in one of the following sections based on your upgrade path:

- Post Upgrade Tasks for Customers Upgrading From 11.3.x.x or 11.4.0.x
- Post Upgrade Tasks for Customers Upgrading From 11.2.x.x

Post Upgrade Tasks for Customers Upgrading From 11.3.x.x or 11.4.0.x

Perform all the tasks in this section if you are upgrading from 11.3.x.x or 11.4.0.x to 11.4.1.0

- General
- Event Stream Analysis
- Investigate
- Respond

General

Task 1. Make Sure Services Have Restarted and Are Capturing and Aggregating Data

Make sure that services have restarted and are capturing data (this depends on whether or not you have auto-start enabled).

If required, restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Start Network Capture

1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under ⚙ (actions), select **View** > **System**.
4. In the toolbar, click ● Start Capture

Start Log Capture

1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.
2. Select each **Log Decoder** service.

3. Under ⚙ (actions), select **View** > **System**.

4. In the toolbar, click ● Start Capture

Start Aggregation

1. In the NetWitness Platform menu, go to **Admin** > **Services**.

   The Services view is displayed.

2. For each **Concentrator**, **Broker**, and **Archiver** service:

   a. Select the service.

   b. Under ⚙ (actions), select **View** > **Config**.

   c. In the toolbar, click ▶ Start Aggregation

Event Stream Analysis

Note: These Event Stream Analysis (ESA) tasks are for upgrades from 11.3.x.x.

Task 2. Verify the Status of the ESA Rule Deployments

Check the status of the ESA rule deployments.

1. Go to **Configure** > **ESA Rules** > **Services** tab.
   The Services view is displayed, which shows the status of your ESA services and deployments.

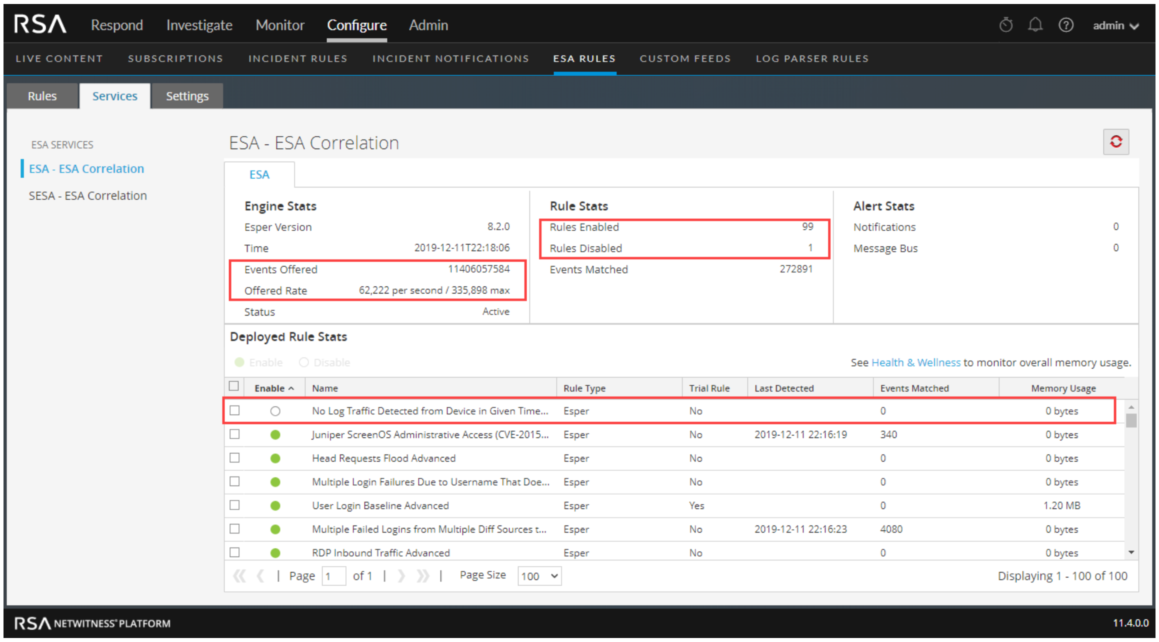
2. In the options panel on the left, select an ESA service.

3. For each service listed, look at the deployment tabs in the panel on the right. Each tab represents a separate ESA rule deployment.

4. For each ESA rule deployment:

   a. In the **Engine Stats** section, look at the **Events Offered** and the **Offered Rate**. They confirm that the data is being aggregated and analyzed properly. If you see 0 for Events Offered, nothing is coming in for the deployment.

   b. In the **Rule Stats** section, look at the **Rules Enabled** and **Rules Disabled**. If there are any disabled rules, look in the **Deployed Rule Stats** section below to view the details of the disabled rules. Disabled rules show a white circle. Enabled rules show a green circle.



ESA - ESA Correlation

Engine Stats	
Esper Version	8.2.0
Time	2019-12-11T22:18:06
Events Offered	11406057584
Offered Rate	62,222 per second / 335,898 max
Status	Active

Rule Stats	
Rules Enabled	99
Rules Disabled	1
Events Matched	272891

Alert Stats	
Notifications	0
Message Bus	0

Deployed Rule Stats

See Health & Wellness to monitor overall memory usage.

□	Enable	Name	Rule Type	Trial Rule	Last Detected	Events Matched	Memory Usage
□	○	No Log Traffic Detected from Device in Given Time...	Esper	No		0	0 bytes
□	●	Juniper ScreenOS Administrative Access (CVE-2015...	Esper	No	2019-12-11 22:16:19	340	0 bytes
□	●	Head Requests Flood Advanced	Esper	No		0	0 bytes
□	●	Multiple Login Failures Due to Username That Doe...	Esper	No		0	0 bytes
□	●	User Login Baseline Advanced	Esper	Yes		0	1.20 MB
□	●	Multiple Failed Logins from Multiple Diff Sources t...	Esper	No	2019-12-11 22:16:23	4080	0 bytes
□	●	RDP Inbound Traffic Advanced	Esper	No		0	0 bytes

Page 1 of 1 | Page Size 100 | Displaying 1 - 100 of 100

5. If you notice any disabled rules that should be enabled:

   a. Go to **Configure** > **ESA Rules** > **Rules** tab and redeploy the ESA rule deployments that contain disabled rules.

   b. Go back to the **Services** tab and check to see if the rules are still disabled. If the rules are still disabled, check the ESA Correlation service log files, which are located at `/var/log/netwitness/correlation-server/correlation-server.log`.

Task 3. (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the Latest Endpoint, UEBA, and RSA Live Content Rules

Note: If you have already completed this task during an upgrade to 11.3.0.2, 11.3.1.1, 11.3.2, or 11.4.0.x, you do not need to do it again.

To use the latest Endpoint, UEBA, and Live content rules, you must update the **multi-valued** parameter field on the ESA Correlation service to include all of the meta keys in the **default-multi-valued** field. You must also update the **single-valued** parameter field to include all of the meta keys in the **default-single-valued** field.

The **multi-valued** parameter shows the string array meta keys used for your ESA rules. This parameter is equivalent to the Event Stream Analysis service **ArrayFieldNames** parameter in NetWitness Platform versions 11.2 and earlier.

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. You can update the `multi-valued` parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

Note: If you see a warning message in the ESA Correlation server error logs that means there is a difference between the `default-multi-valued` parameter and `multi-valued` parameter meta key values, the new Endpoint, UEBA, and Live content rules will not work. Completing this procedure should fix the issue. For example warning messages, see Example ESA Correlation Server Warning Message for Missing Meta Keys.

1. After you upgrade to 11.4.1, go to **Admin** > **Services**, and in the Services view, select an ESA Correlation service and then select ⚙ ⌄ > **View** > **Explore**.
2. In the Explore view node list for the ESA Correlation service, select **correlation** > **stream**.
3. Compare the **`multi-valued`** parameter meta keys with the required **`default-multi-valued`** meta keys. Copy and paste the missing string array meta keys from the **`default-multi-valued`** parameter to the **`multi-valued`** parameter. (You may want to copy only a couple meta keys at one time to reduce the number of reported errors).
4. Copy and paste the string meta keys from the **`default-single-valued`** parameter to the **`single-valued`** parameter.
5. Apply the changes on the ESA Correlation service:
6. Go to **Configure** > **ESA Rules** and click the **Settings** tab.
   - In the Meta Key References, click the Meta Re-Sync (Refresh) icon (⟳).
   - If you have multiple ESA Correlation services, make the same meta key changes on each ESA Correlation service.
7. If you are using any of the **`default-multi-valued`** or **`default-single-valued`** meta keys in your ESA Advanced rules, update the rule syntax. See also Task 4. (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules .
8. If you used any meta keys in the ESA rule notification templates from the **`default-multi-valued`** parameter list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*.
9. Deploy your ESA rule deployments.
10. Check your rules for error messages in the ESA Rules section of the ESA rule deployment or check the ESA Correlation error logs for errors.
    - To access the error messages in the ESA rule deployment, go to **Configure** > **ESA Rules** > **Rules** tab, select a deployment in the options panel on the left, and go to the **ESA Rules** section.
    - To access the ESA Correlation service logs, you can use SSH to get in the system and go to: `/var/log/netwitness/correlation-server/correlation-server.log`.

Task 4. (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules

Note: If you have already completed this task during an upgrade to 11.3.0.2, 11.3.1.1, 11.3.2, or 11.4.0.x, you do not need to do it again.

Update your ESA Rule Builder and ESA Advanced rules to work with the string and string array meta keys listed in the `default-multi-valued` and `default-single valued` parameter fields for the ESA Correlation service. You can add additional meta keys to the `multi-valued` and `single-valued` parameters.

For example, if you use `ec.outcome` as a single-valued meta key in your ESA rule as shown below:

```
@RSAAlert

SELECT * FROM Event((ec_outcome IN ( 'Success' )))

.win:time_length_batch(2 Minutes, 2)

HAVING COUNT(*) >= 2;
```

If you add `ec.outcome` to the **`multi-valued`** parameter field, you need to update your rule as shown below:

```
@RSAAlert

SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))

.win:time_length_batch(2 Minutes, 2)

HAVING COUNT(*) >= 2;
```

For more information, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*.

ESA Troubleshooting information

For more information, see ESA Troubleshooting Information.

Investigate

Task 5. (Conditional - For Custom Roles Only) Adjust investigate-server Permissions for Custom User Roles

After upgrading to Version 11.4.1.0, the built-in user roles for analysts using Investigate have the following permissions enabled:

- `investigate-server.columngroup.read`
- `investigate-server.metagroup.read`
- `investigate-server.profile.read`

After you upgrade to 11.4.1.0, NetWitness Platform does not add these permissions to custom analyst roles so you must enable them for your custom roles as described in this procedure (see the *System Security and User Management Guide* for comprehensive information about user roles).

Users who are assigned a custom user role that does not have these permissions will see issues in the Navigate view and Legacy Events view. If any of the three permissions are disabled, the Load Values button is not displayed in the Navigate view. When column groups permission is disabled, there is an additional issue in the Legacy Events view: Only the Detail view is visible and you cannot select different views and column groups.

To enable the permissions for a user role:

1. Go to **Admin** > **Security** and click the **Roles** tab.
2. Select the custom user role that needs to be edited and click ✎ (edit icon).
3. In the Edit Role dialog, ensure that these three permissions are enabled:
   ```
   investigate-server.columngroup.read
   investigate-server.metagroup.read
   investigate-server.profile.read
   ```
4. Click **Save** to save your changes. When analysts with the custom user role log in to the NetWitness Platform, the changes will be in effect.

Respond

The Primary ESA server must be upgraded to 11.4.1 before you can complete these tasks.

Note: After upgrading the primary NW Server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4.1. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Task 6. (Conditional) Restore any Respond Service Custom Keys in the Aggregation Rule Schema

Note: If you did not manually customize the incident aggregation rule schema, you can skip this task.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.x, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file.

The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format:
`aggregation_rule_schema.json.bak-<time of the backup>`

Task 7. (Conditional) Restore any Customized Respond Service Normalization Scripts

Note: If you did not manually customize any alert normalization scripts, you can skip this task.

To prevent overwriting future customizations, custom normalization script files are available in NetWitness Platform 11.4 and later. Add any custom logic to the **`custom_normalize_<alert type>.js`** files.

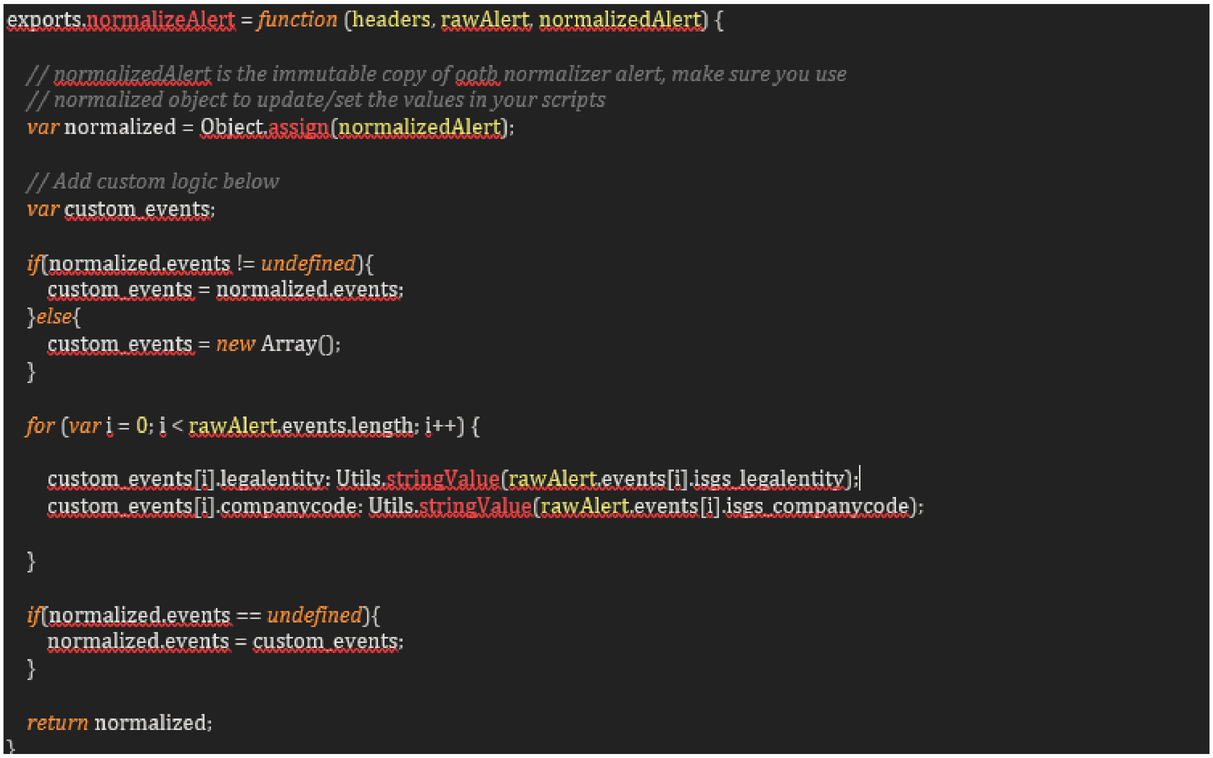
1. Locate any custom logic from the backup Respond normalization scripts located in the **`/var/lib/netwitness/respond-server/scripts.bak-<timestamp>`** directory, where `<timestamp>` is the time that the backup completed:
   ```
   data_privacy_map.js
   normalize_alerts.js
   ```

```
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_ueba_alerts.js
normalize_wtd_alerts.js
utils.js
```

2. Edit the new 11.4 or later script files in the **`/var/lib/netwitness/respond-server/scripts`** directory to include any logic from the back up files. If you have any customizations in the normalization files, add them to the normalization files with the `"custom"` prefix.

```
data_privacy_map.js
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
utils.js
```

For Example, the `custom_normalize_core_alerts.js` is the normalization script for ESA to add up any custom logic. This java script file has a function '`normalizeAlert`' with parameters headers, rawAlert, and normalizedAlert. The variable '`normalized`' is a immutable copy object which has an embedded object of list of normalized events. So if you have any custom meta keys configured for the events then you have to iterate through the '`normalized.events`' to populate the appropriate meta keys with values from the '`rawAlert.events`' object. Below is the sample code.



```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {

  // normalizedAlert is the immutable copy of ooth normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

  if(normalized.events != undefined){
    custom_events = normalized.events;
  }else{
    custom_events = new Array();
  }

  for (var i = 0; i < rawAlert.events.length; i++) {

    custom_events[i].legalentity: Utils.stringValue(rawAlert.events[i].isgs_legalentity);
    custom_events[i].companycode: Utils.stringValue(rawAlert.events[i].isgs_companycode);

  }

  if(normalized.events == undefined){
    normalized.events = custom_events;
  }

  return normalized;
}
```

Task 8. (Conditional) Add Respond Notification Settings Permissions

Note: If you already configured these permissions in 11.2 or later, you can skip this task.

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**Configure** > **RespondNotifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you must add additional permissions to your existing built-in NetWitness Platform user roles. You must also add permissions to your custom roles.

See the “Respond Notification Settings Permissions” topic in the *NetWitness Respond Configuration Guide*.

For detailed information about user permissions, see the *System Security and User Management Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Post Upgrade Tasks for Customers Upgrading From 11.2.x.x

Perform all the tasks in this section if you are upgrading from 11.2.x.x to 11.4.1.

- General
- Event Stream Analysis
- Investigate
- Respond
- Decoder and Log Decoder

General

Task 1. Make Sure Services Have Restarted and Are Capturing and Aggregating Data

Make sure that the services have restarted and capturing data (this depends on whether or not you have auto-start enabled).

If required, restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Start Network Capture

1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.
3. Under ⚙ (actions), select **View** > **System**.
4. In the toolbar, click ● Start Capture

Start Log Capture

1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.

2. Select each **Log Decoder** service.

3. Under ⚙ (actions), select **View** > **System**.

4. In the toolbar, click ● Start Capture

Start Aggregation

1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.

2. For each **Concentrator**, **Broker**, and **Archiver** service:

   a. Select the service.

   b. Under ⚙ (actions), select **View** > **Config**.

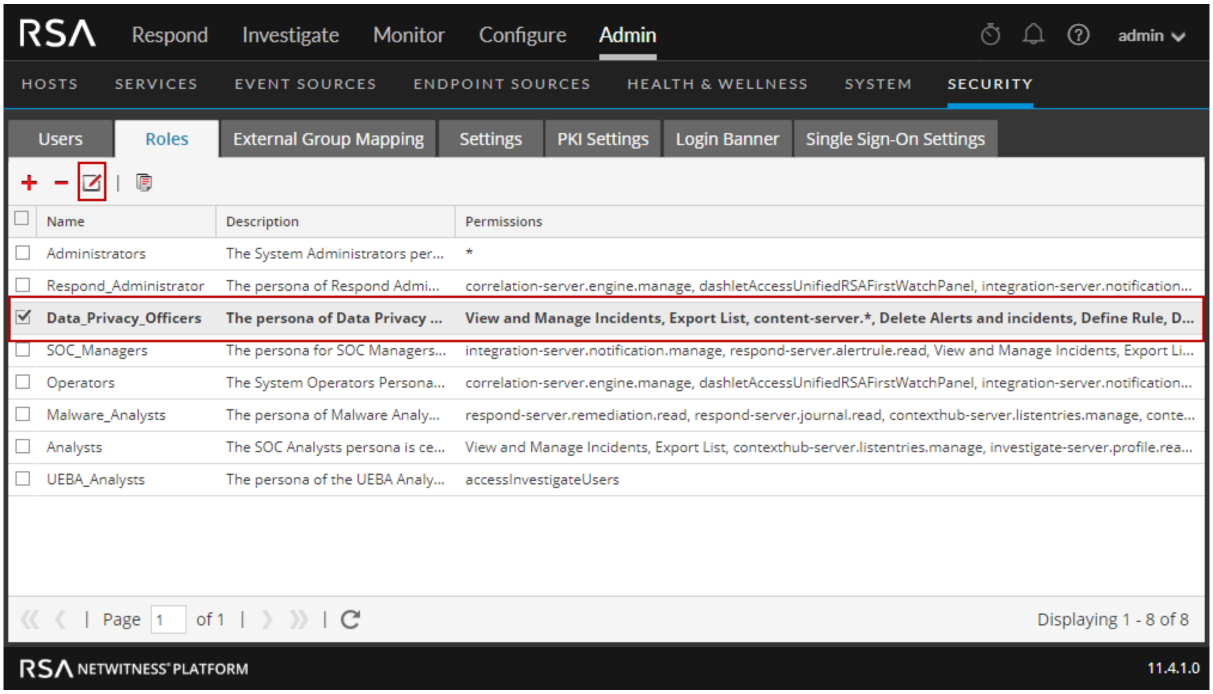
   c. In the toolbar, click ▶ Start Aggregation

Task 2. Set Up Context Menu Actions User Permissions

Complete the following steps for **Analysts**, **SOC Managers**, **Data Privacy Officers** roles to set up their Context Menu Actions. You must complete these steps for the **Analysts**, **SOC Managers**, and **Data Privacy Officers** roles.

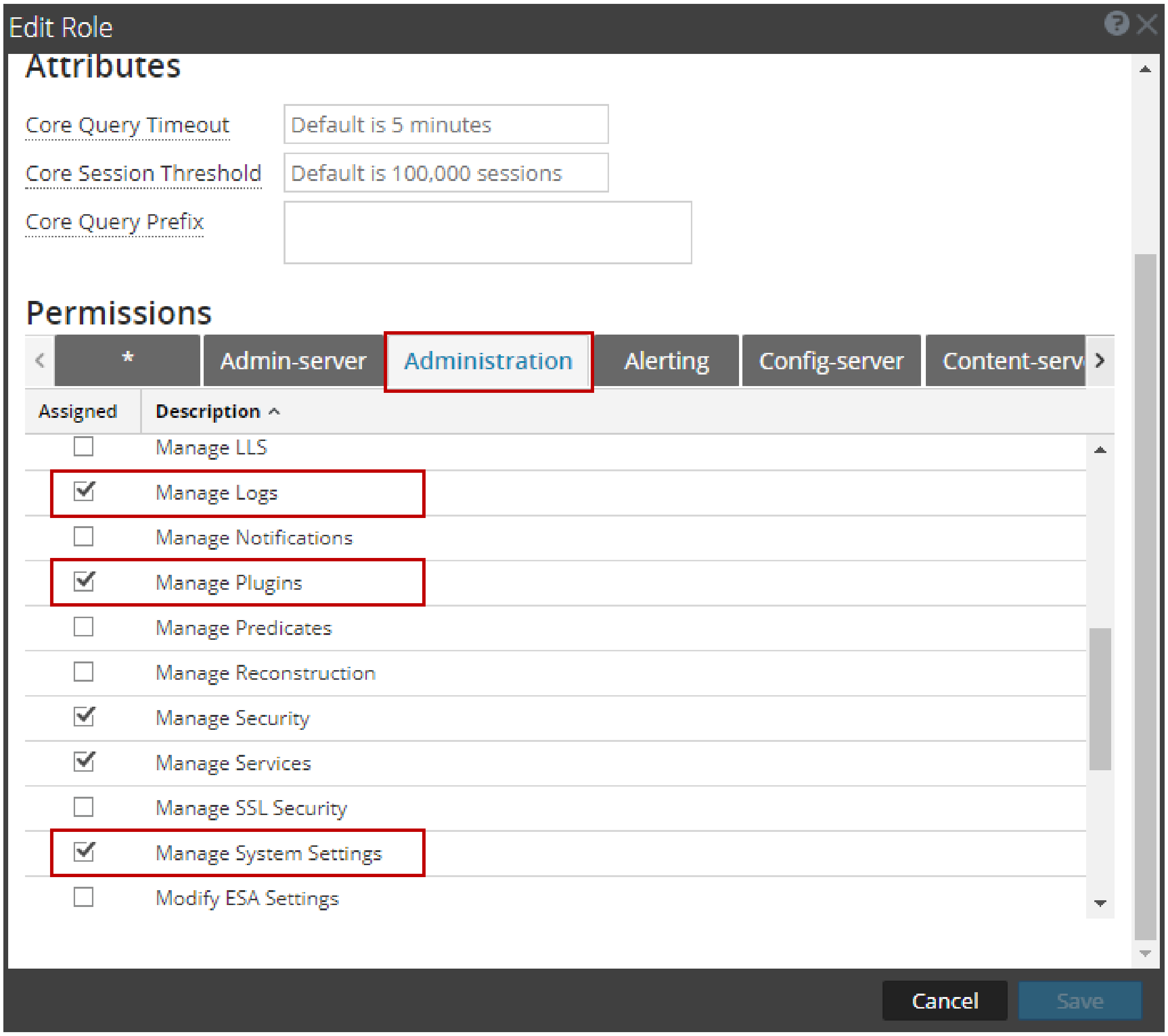
1. In the **NetWitness Platform** menu, go to **Admin** > **Security** > **Roles**.

2. Double-click on the user role (for example, **Data Privacy Officers**), or click to select the role and click ✎ (Edit).



□	Name	Description	Permissions
□	Administrators	The System Administrators per...	*
□	Respond_Administrator	The persona of Respond Admi...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
☑	**Data_Privacy_Officers**	**The persona of Data Privacy ...**	**View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, D...**
□	SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
□	Operators	The System Operators Persona...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
□	Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
□	Analysts	The SOC Analysts persona is ce...	View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.profile.rea...
□	UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

3. In the **Edit Role** view, under **Permissions** on the **Administration** tab, select the **Manage Logs**, **Manage Plugins**, and **Manage System Settings** check boxes and click **Save**.



Core Query Timeout	Default is 5 minutes
Core Session Threshold	Default is 100,000 sessions
Core Query Prefix	

Assigned	Description ^
□	Manage LLS
☑	Manage Logs
□	Manage Notifications
☑	Manage Plugins
□	Manage Predicates
□	Manage Reconstruction
☑	Manage Security
☑	Manage Services
□	Manage SSL Security
☑	Manage System Settings
□	Modify ESA Settings

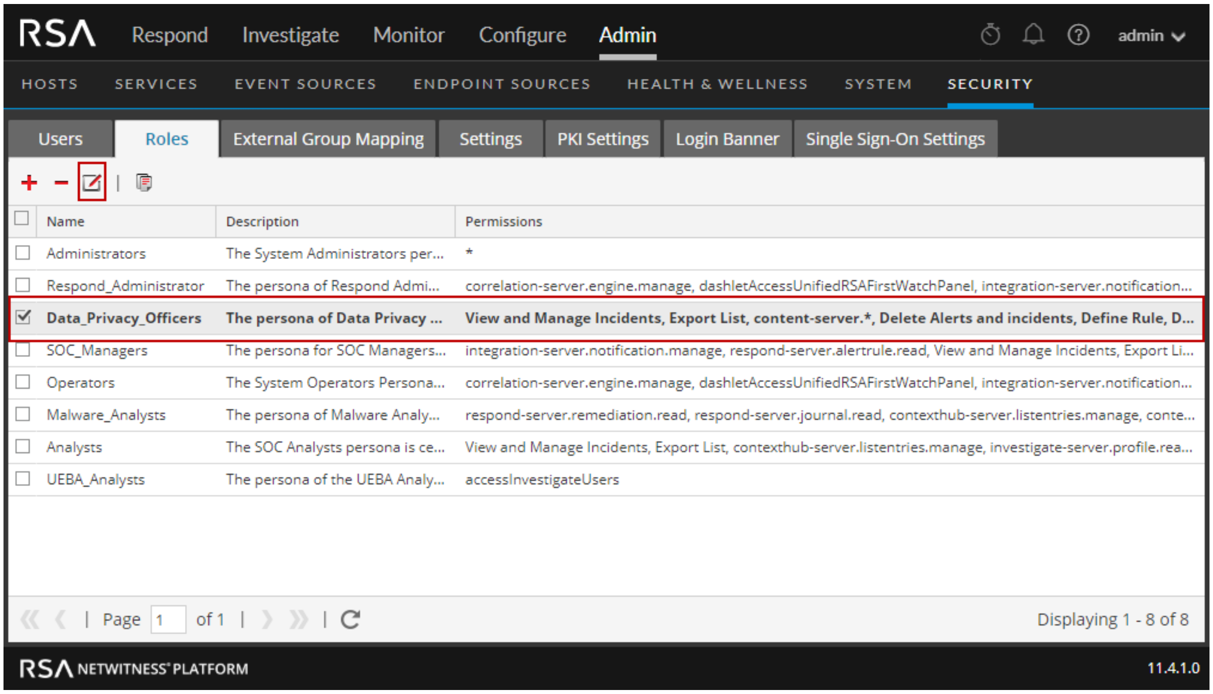
4. Complete steps 1 through 3 for the **Analysts** and **SOC Managers** roles in addition to **Data Privacy Officers**.

Task 3. Add "Manage Jobs" Permission to Roles Missing this Permission

Add the 'Manage Jobs' Administration permission to the following roles:

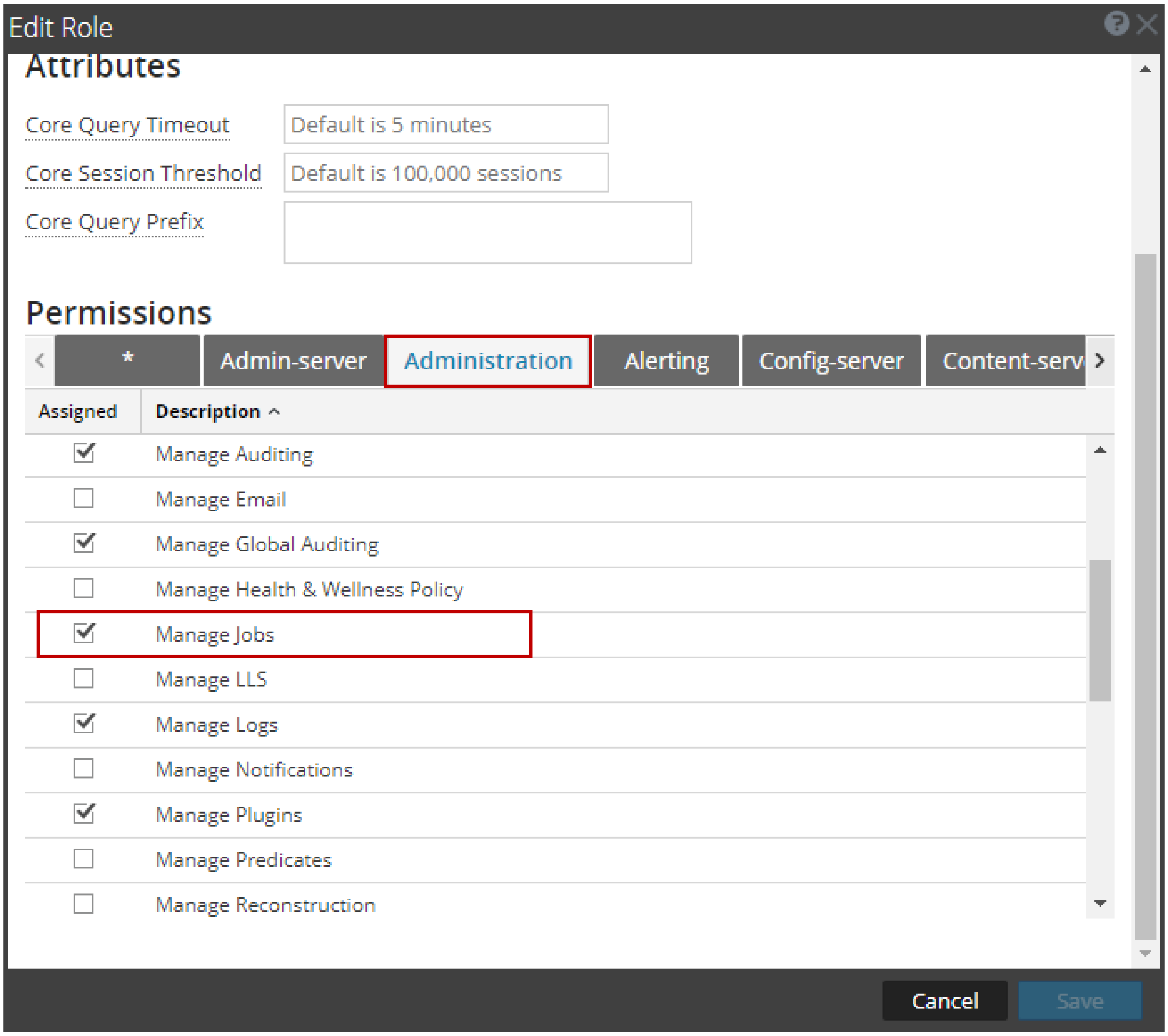
- SOC_Managers
- Operators
- Data_Privacy_Officers

1. In the **NetWitness Platform** menu, go to **Admin** > **Security** and click **Roles**.
2. Select the role you need to update (that is, **SOC_Managers**, **Operators**, or **Data_Privacy_Officers**) and click Edit .



□	Name	Description	Permissions
□	Administrators	The System Administrators per...	*
□	Respond_Administrator	The persona of Respond Admi...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
☑	**Data_Privacy_Officers**	**The persona of Data Privacy ...**	**View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, D...**
□	SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
□	Operators	The System Operators Persona...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
□	Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
□	Analysts	The SOC Analysts persona is ce...	View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.profile.rea...
□	UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

3. Click **Administration**, select the **Manage Jobs** checkbox, and click **Save**.



Attributes

Core Query Timeout: Default is 5 minutes

Core Session Threshold: Default is 100,000 sessions

Core Query Prefix:

Assigned	Description
☑	Manage Auditing
□	Manage Email
☑	Manage Global Auditing
□	Manage Health & Wellness Policy
☑	Manage Jobs
□	Manage LLS
☑	Manage Logs
□	Manage Notifications
☑	Manage Plugins
□	Manage Predicates
□	Manage Reconstruction

4. Complete steps 1 through 3 inclusive for all three roles (**SOC_Managers**, **Operators**, and **Data_Privacy_Officers**).

Task 4. (Conditional) Reissue Certificates for Your Hosts

Before you upgrade, you must ensure that the internal RSA-issued certificates, such as CA Certificate and Service certificates, are renewed.

The validity for NetWitness Platform certificates are as follows:

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

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

To renew the CA certificates or service certificates, see the Reissue root CA security certificates on RSA NetWitness Platform 11.x.

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

For more information, see the "Reissue Certificates" topic in the *System Maintenance Guide*.

Task 5. Modify the Analyst Role `investigate-server` Permissions

The default permissions for the **SOC Managers**, **Malware Analysts**, and **Analysts** roles in 11.3 or later have specific permissions required to view and work in the Event Analysis view. Prior to 11.3, the default permissions were different.

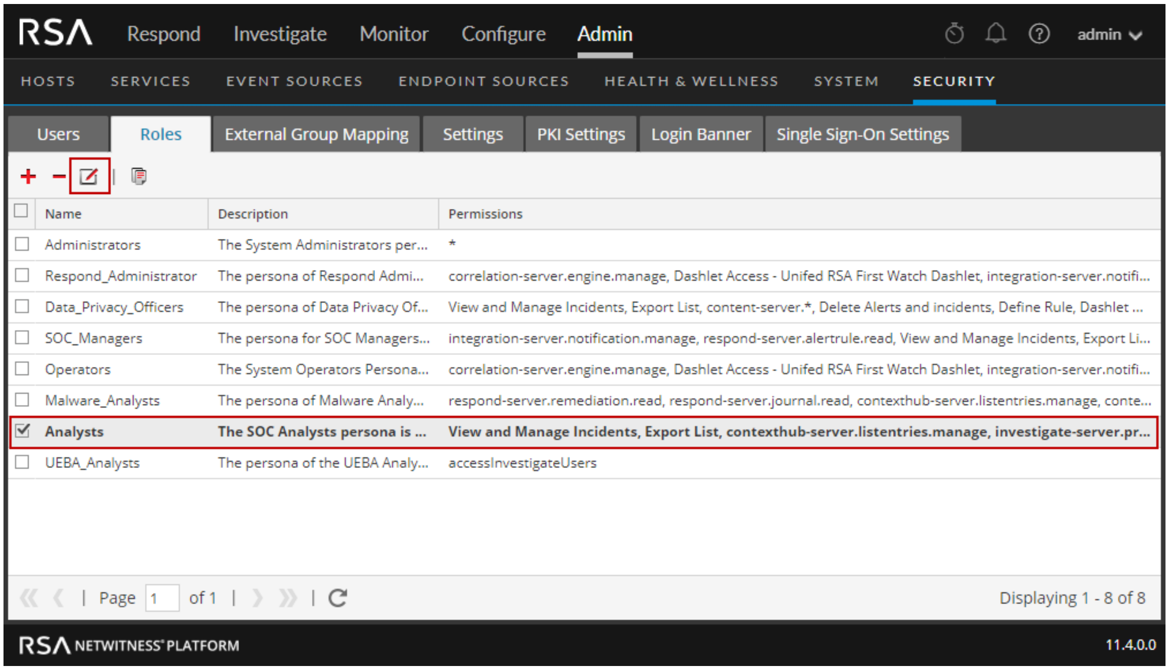
In addition, the `predicate.manage` permission should not be assigned to the **SOC Managers**, **Malware Analysts**, and **Analysts** roles because it grants them access to `get-predicates`, `edit-predicates`, `remove-predicates`, `remove-all-predicates` and so on. This access could be a security risk because it allows them to circumvent settings that restrict access to certain data.

As a result, if you are upgrading from version 11.2.x.x to 11.4 or later, you must update the default permissions to match the new default permissions, as described in the following procedure.

1. Go to **Admin** > **Security** > **Roles**.

2. Complete the following steps for **SOC Managers**, **Malware Analysts**, and **Analysts** roles.

   a. Select the user role checkbox (for example, **Analysts**) and click Edit.



☐	Name	Description	Permissions
☐	Administrators	The System Administrators per...	*
☐	Respond_Administrator	The persona of Respond Admi...	correlation-server.engine.manage, Dashlet Access - Unifed RSA First Watch Dashlet, integration-server.notifi...
☐	Data_Privacy_Officers	The persona of Data Privacy Of...	View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, Dashlet ...
☐	SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
☐	Operators	The System Operators Persona...	correlation-server.engine.manage, Dashlet Access - Unifed RSA First Watch Dashlet, integration-server.notifi...
☐	Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
☑	**Analysts**	**The SOC Analysts persona is ...**	**View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.pr...**
☐	UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

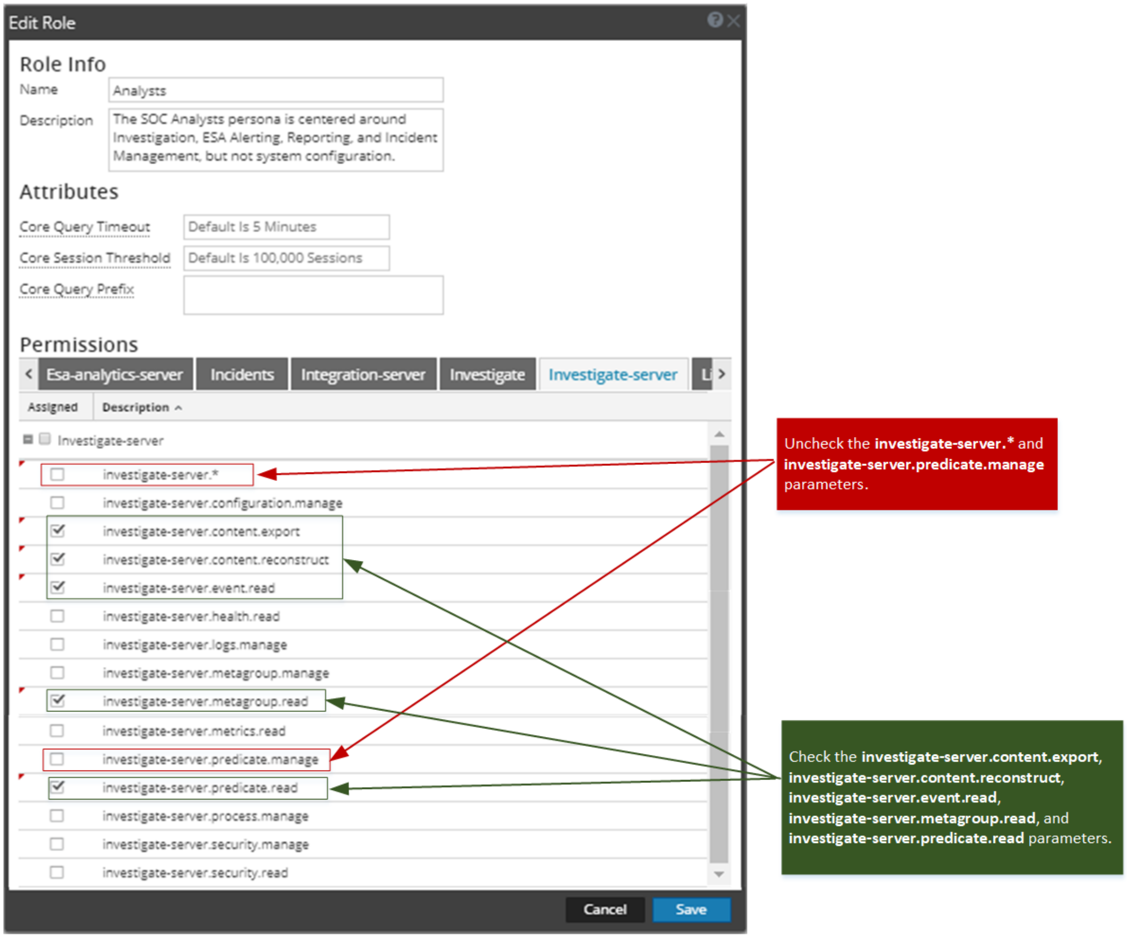
b. Under **Permissions**, click the **Investigate-server** tab.

c. Make sure that the following permissions are not selected.

- `investigate-server.*`
- `investigate-server.predicate.manage`

d. Select the following permissions.

- `investigate-server.content.export`
- `investigate-server.content.reconstruct`
- `investigate-server.event.read`
- `investigate-server.metagroup.read`
- `investigate-server.predicate.read`



Edit Role

Role Info

Name: Analysts

Description: The SOC Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Incident Management, but not system configuration.

Attributes

Core Query Timeout: Default Is 5 Minutes

Core Session Threshold: Default Is 100,000 Sessions

Core Query Prefix:

Permissions

□ Investigate-server

□ investigate-server.*

□ investigate-server.configuration.manage

☑ investigate-server.content.export

☑ investigate-server.content.reconstruct

☑ investigate-server.event.read

□ investigate-server.health.read

□ investigate-server.logs.manage

□ investigate-server.metagroup.manage

☑ investigate-server.metagroup.read

□ investigate-server.metrics.read

□ investigate-server.predicate.manage

☑ investigate-server.predicate.read

□ investigate-server.process.manage

□ investigate-server.security.manage

□ investigate-server.security.read

Uncheck the **investigate-server.*** and **investigate-server.predicate.manage** parameters.

Check the **investigate-server.content.export**, **investigate-server.content.reconstruct**, **investigate-server.event.read**, **investigate-server.metagroup.read**, and **investigate-server.predicate.read** parameters.

e. Click **Save**.

Task 6. (Conditional) Reconfigure PAM RADIUS Authentication

If you configured PAM RADIUS authentication in 11.2.x.x using the `pam_radius` package, you must reconfigure it in 11.4 or later using the `pam_radius_auth` package.

Run the following commands on the NW Server host.

Note: If you configured `pam_radius` in 11.2.x.x, perform step 1 to uninstall the existing version. If not, you can proceed with step 2.

1. Verify the existing page and uninstall the existing `pam_radius` file:
   ```
   rpm -qa |grep pam_radius
   yum erase pam_radius
   ```
2. To install the `pam_radius_auth` package, run the following command:
   ```
   yum install pam_radius_auth
   ```
3. Edit the RADIUS configuration file, `/etc/raddb/server`, as follows and add the configurations for the RADIUS server:
   ```
   # server[:port] shared_secret timeout (s)
   server secret 3
   ```
   For example: `111.222.33.44 secret 1`
4. Edit the NW Server host PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   ```
   auth sufficient pam_radius_auth.so
   ```
5. Provide write permission to `/etc/raddb/server` files by running the following command:
   ```
   chown netwitness:netwitness /etc/raddb/server
   ```
6. Copy the `pam_radius_auth` library by running the following command:
   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```
7. After making the changes to the `pam_radius_auth` configurations, restart the Jetty server by running the following command:
   ```
   systemctl restart jetty
   ```

Task 7. (Conditional) If NetWitness Platform Has No Web Access, Upload Response .bin File Again (License Server)

If your NetWitness deployment does not have Internet access, after you upgrade to 11.4 or later, you must upload the response `.bin` file again to view the license information in the **Admin** > **System** > **Licensing** view in the NetWitness Platform User Interface. See “Upload an Offline Capability Response to NetWitness Platform” in the *Licensing Management Guide* for instructions. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Task 8. Change Minimum Password Length from Eight Characters to Nine Characters

In versions 11.2.x.x, the NetWitness Platform minimum password length is eight characters. In 11.3.x.x and later, the minimum length is nine characters. After you upgrade from 11.2.x.x to 11.4 or later, set the minimum password length to nine characters as described under "Configure Password Complexity" in the *System Security and User Management Guide*.

Event Stream Analysis

Note: These Event Stream Analysis (ESA) tasks are for upgrades from 11.2.x.x.

Task 9. View the String Array Type Meta Keys on the ESA Correlation Service and Next Steps

To support Endpoint, UEBA, and RSA Live content, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service for 11.3 and later. Additional string meta keys are also required.

If the meta keys used for your ESA rules are different from the required default multi-value meta keys, your ESA rules continue to work, but you should update your ESA rules to use the required meta keys as soon as possible to ensure that your rules continue to deploy properly.

The ESA Correlation service has the following multi-valued (string array) and single-valued (string) parameters:

- **`multi-valued`** - Shows the string array meta keys currently used for your ESA rules. For an upgrade to NetWitness Platform 11.4 or later, it shows the existing string array meta keys before the upgrade. (This parameter is equivalent to the Event Stream Analysis service `ArrayFieldNames` parameter in NetWitness Platform versions 11.2 and earlier.)
- **`single-valued`** - Shows the string meta keys currently used for your ESA rules. For an upgrade to NetWitness Platform 11.4 or later, this parameter value is empty.
- **`default-multi-valued`** - Shows the required string array meta keys for the latest version.
- **`default-single-valued`** - Shows the required string meta keys for the latest version.

Note: If you have the same value in the `single-valued` and `multi-valued` parameter fields, the `single-valued` meta key value takes precedence over the `multi-valued` meta key value.

1. View the `multi-valued` and `single-valued` meta key parameters on the ESA Correlation service:
   a. Go to **Admin** > **Services**, and in the Services view, select an ESA Correlation service and then select ⚙ ⌄ > **View** > **Explore**.
   b. In the Explore view node list for an ESA Correlation service, select **correlation** > **stream**.
2. Your ESA rules continue to work, but if you are using Live, UEBA, or Endpoint rules, follow the Task 12. (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules procedure.

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. You can update the `multi-valued` parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

Note: If you are using multiple ESA Correlation services, the `multi-valued` and `single-valued` parameters should be the same on each ESA Correlation service.

Task 10. (Conditional) Update RSA Live ESA Rules with Meta Type Changes from String to Array

The following table lists ESA rules from RSA Live that had meta key type changes from String to Array in NetWitness Platform 11.3.x and 11.4.

Rule #	Rule Name	Array Type Meta Keys in 11.3.x and 11.4
1	RIG Exploit Kit	threat_category
2	AWS Critical VM Modified	alert
3	Multiple Successful Logins from Multiple Diff Src to Same Dest	host.src and host.dst
4	Multiple Successful Logins from Multiple Diff Src to Diff Dest	host.src and host.dst
5	Multiple Failed Logins from Multiple Diff Sources to Same Dest	host.src and host.dst
6	Multiple Failed Logins from Multiple Users to Same Destination	host.src and host.dst
7	User Login Baseline	host.src and host.dst

1. If you:
   - Deployed these rules before version 11.3:
     a. Note any rule parameters that you have changed so you can adjust the rules for your environment.
     b. Download the updated rules from RSA Live.
     c. Reapply any changes to the default rule parameters and deploy the rules.
        (For instructions, see “Download RSA Live ESA Rules” in the *Alerting with ESA Correlation Rules User Guide*.)
   - Are deploying these rules for the first time in version 11.4 or later, follow the customization directions within the ESA rule descriptions. Rules 3 to 7 in the above table require that the Context Hub lists for `User_Whitelist`, `Host_Whitelist` and `IP_Whitelist` to be added as enrichments to ESA. (See “Configure Context Hub List as an Enrichment Source” in the *Alerting with ESA Correlation Rules User Guide*.)
2. Deploy the ESA rule deployment that contains these rules. (See “ESA Rule Deployment Steps” in the *Alerting with ESA Correlation Rules User Guide*.)

Task 11. Verify the ESA Rule Deployments

After you upgrade to 11.4 or later, verify your ESA rule deployments. For every ESA host, a new deployment is created in the format "`<ESA-Hostname>` – ESA Correlation".

1. Make sure that a new deployment was created.
2. Make sure that the new deployment contains an ESA Correlation service, data sources, and rules for all previous deployments on that ESA host.
3. Make sure that the ESA Correlation service has status of "Deployed".
4. If an ESA rule status incorrectly shows as "Disabled" or shows the ❗ icon in the Status column, you need to determine the issue to fix the rule. If a disabled rule has an error message, it now shows ❗ in the Status field. You can hover over the rule to view the error message tooltip without going to the error log. (The ESA Correlation Service log files are located at `/var/log/netwitness/correlation-server/correlation-server.log`)
   See ESA Troubleshooting Information.
5. Check the status of the overall ESA rule deployment. If the ESA rule deployment is successful, the ESA Services and ESA Rules show a status of "Deployed," the Data Sources show a green circle, and the **Deploy Now** button is disabled.

For a detailed example, see the *ESA Configuration Guide*. For Deployment information, see "ESA Rule Deployment Steps" in the *Alerting with ESA Correlation Rules User Guide*. For troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Task 12. (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules

To use the latest Endpoint, UEBA, and Live content rules, you must update the **multi-valued** parameter field on the ESA Correlation service to include all of the meta keys in the **default-multi-valued** field. You must also update the **single-valued** parameter field to include all of the meta keys in the **default-single-valued** field.

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. You can update the `multi-valued` parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

Note: If you see a warning message in the ESA Correlation server error logs that means there is a difference between the `default-multi-valued` parameter and `multi-valued` parameter meta key values, the new Endpoint, UEBA, and Live content rules will not work. Completing this procedure should fix the issue. For example warning messages, see Example ESA Correlation Server Warning Message for Missing Meta Keys.

1. After an upgrade to 11.4 or later, go to **Admin** > **Services**, and in the Services view, select an ESA Correlation service, and then select ⚙ ⌄ > **View** > **Explore**.
2. In the Explore view node list for the ESA Correlation service, select **correlation** > **stream**.
3. Compare the **`multi-valued`** parameter meta keys with the required **`default-multi-valued`** meta keys. Copy and paste the missing string array meta keys from the **`default-multi-valued`** parameter to the **`multi-valued`** parameter. (You may want to copy only a couple meta keys at one time to reduce the number of reported errors).
4. Copy and paste the string meta keys from the **`default-single-valued`** parameter to the **`single-valued`** parameter.
5. Apply the changes on the ESA Correlation service:
6. Go to **Configure** > **ESA Rules** and click the **Settings** tab.
   - In the Meta Key References, click the Meta Re-Sync (Refresh) icon (⟳).
   - If you have multiple ESA Correlation services, make the same meta key changes on each ESA Correlation service.
7. If you are using any of the **`default-multi-valued`** or **`default-single-valued`** meta keys in your ESA Advanced rules, update the rule syntax. See also Task 13. (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules
8. If you used any meta keys in the ESA rule notification templates from the **`default-multi-valued`** parameter list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.
9. Deploy your ESA rule deployments.
10. Check your rules for error messages in the ESA Rules section of the ESA rule Deployment or check the ESA Correlation error logs for errors.
    - To access the error messages in the ESA rule deployment, go to **Configure** > **ESA Rules** > **Rules** tab, select a deployment in the options panel on the left, and go to the **ESA Rules** section.
    - To access the ESA Correlation service logs, you can use SSH to get in the system and go to: `/var/log/netwitness/correlation-server/correlation-server.log`.

Task 13. (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules

Update your ESA Rule Builder and ESA Advanced rules to work with the string and string array meta keys listed in the `default-multi-valued` and `default-single valued` parameter fields for the ESA Correlation service. You can add additional meta keys to the `multi-valued` and `single-valued` parameters.

For example, if you use `ec.outcome` as a single-valued meta key in your ESA rule as shown below:

```
@RSAAlert
SELECT * FROM Event((ec_outcome IN ( 'Success' )))
```

```
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

If you add `ec.outcome` to the **`multi-valued`** parameter field, you need to update your rule as shown below:

```
@RSAAlert
SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

For more information, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

ESA Troubleshooting Information

> **Note:** To avoid unnecessary processing overhead, the Ignore Case option has been removed from the ESA Rule Builder - Build a Statement dialog for meta keys that do not contain text data values. During the upgrade to 11.4 or later, NetWitness Platform does not modify existing rules for the Ignore Case option. If an existing Rule Builder rule has the Ignore Case option selected for a meta key that no longer has the option available, an error occurs if you try to edit the statement and try to save it again without clearing the checkbox.

To support Endpoint and UEBA content as well as changes to ESA rules from Live, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service. In NetWitness Platform 11.4 or later, ESA automatically adjusts the operator in the rule statement when there is a change from string to string array, but you still may need to make manual adjustments to adjust for the string array changes.

To change the string type meta keys to string array type meta keys manually in 11.4 or later, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*.

To use the latest Endpoint, UEBA, and Live content rules, the following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform version 11.4 or later:

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file
, analysis.service , analysis.session , boc , browserprint , cert.thumbprint ,
checksum , checksum.all , checksum.dst , checksum.src , client.all , content ,
context , context.all , context.dst , context.src , dir.path , dir.path.dst ,
dir.path.src , directory , directory.all , directory.dst , directory.src ,
email , email.dst , email.src , eoc , feed.category , feed.desc , feed.name ,
file.cat , file.cat.dst , file.cat.src , filename.dst , filename.src , filter
, function , host.all , host.dst , host.orig , host.src , host.state ,
inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param
, param.dst , param.src , registry.key , registry.value , risk , risk.info ,
risk.suspicious , risk.warning , threat.category , threat.desc , threat.source
, user.agent , username
```

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform 11.4 or later:

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

If you used any meta keys in the ESA rule notification templates from the Required String Array or String Meta Keys list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Note: Advanced EPL rules may get disabled and are not automatically updated so they must be fixed manually.

For additional troubleshooting information, see "Troubleshoot ESA" in the *Alerting with ESA Correlation Rules User Guide for RSA NetWitness Platform*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Example ESA Correlation Server Warning Message for Missing Meta Keys

If you see a warning message in the ESA Correlation server error logs that means there is a difference between the `default-multi-valued` parameter and `multi-valued parameter` meta key values, the new Endpoint, UEBA, and Live content rules will not work. Completing the Task 12. (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules procedure should fix the issue.

Multi-Valued Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_
src, client_all, content, context, context_all, context_dst, context_src, dir_
path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst,
directory_src, email_dst, email_src, feed_category, feed_desc, feed_name,
file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter,
function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_
orig, OS, param, param_dst, param_src, registry_key, registry_value, risk,
risk_info, risk_suspicious, risk_warning, threat_category, threat_desc,
threat_source, user_agent] are still MISSING from multi-valued
```

Single Value Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target,
file_attributes, logon_type_desc, packets] are still MISSING from single-
valued
```

Investigate

Task 14. (Conditional - For Custom Roles Only) Adjust investigate-server Permissions for Custom User Roles

After upgrading to Version 11.4 or later, the built-in user roles for analysts using Investigate have the following permissions enabled:

- `investigate-server.columngroup.read`
- `investigate-server.metagroup.read`
- `investigate-server.profile.read`

After you upgrade to 11.4 or later, NetWitness Platform does not add these permissions to custom analyst roles so you must enable them for your custom roles as described in this procedure (see the *System Security and User Management Guide* for comprehensive information about user roles).

Users who are assigned a custom user role that does not have these permissions will see issues in the Navigate view and Legacy Events view. If any of the three permissions are disabled, the Load Values button is not displayed in the Navigate view. When column groups permission is disabled, there is an additional issue in the Legacy Events view: Only the Detail view is visible and you cannot select different views and column groups.

To enable the permissions for a user role:

1. Go to **Admin** > **Security** and click the **Roles** tab.
2. Select the custom user role that needs to be edited and click ✎ (edit icon).
3. In the Edit Role dialog, ensure that these three permissions are enabled:
   `investigate-server.columngroup.read`
   `investigate-server.metagroup.read`
   `investigate-server.profile.read`
4. Click **Save** to save your changes. When analysts with the custom user role log in the NetWitness Platform, the changes will be in effect.

Respond

The Primary ESA server must be upgraded to 11.4.1 before you can complete these tasks.

> **Note:** After upgrading the primary NW Server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4.1. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Task 15. (Conditional) Restore any Respond Service Custom Keys in the Aggregation Rule Schema

> **Note:** If you did not manually customize the incident aggregation rule schema, you can skip this task.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.x, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file.

The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format:
`aggregation_rule_schema.json.bak-<time of the backup>`

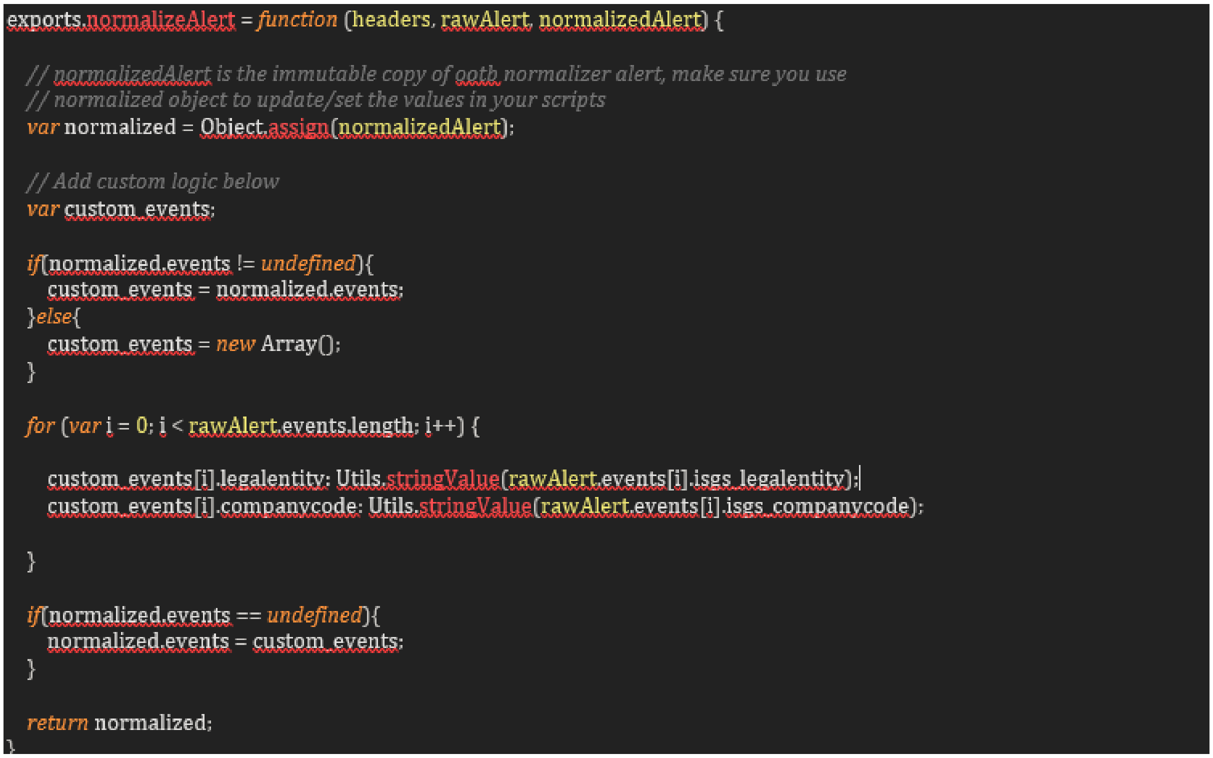
Task 16. (Conditional) Restore any Customized Respond Service Normalization Scripts

> **Note:** If you did not manually customize any alert normalization scripts, you can skip this task.

To prevent overwriting future customizations, custom normalization script files are available in NetWitness Platform 11.4 and later. Add any custom logic to the **custom_normalize_<alert type>.js** files.

1. Locate any custom logic from the backup Respond normalization scripts located in the **/var/lib/netwitness/respond-server/scripts.bak-<timestamp>** directory, where `<timestamp>` is the time that the backup completed:
   ```
   data_privacy_map.js
   normalize_alerts.js
   normalize_core_alerts.js
   normalize_ecat_alerts.js
   normalize_ma_alerts.js
   normalize_ueba_alerts.js (11.3 and later versions)
   normalize_wtd_alerts.js
   utils.js
   ```
2. Edit the new 11.4 script files in the **/var/lib/netwitness/respond-server/scripts** directory to include any logic from the back up files. If you have any customizations in the normalization files, add them to the normalization files with the “custom” prefix.
   ```
   data_privacy_map.js
   custom_normalize_alerts.js
   custom_normalize_core_alerts.js
   custom_normalize_ecat_alerts.js
   custom_normalize_ma_alerts.js
   custom_normalize_ueba_alerts.js
   custom_normalize_wtd_alerts.js
   utils.js
   ```

   For Example, the `custom_normalize_core_alerts.js` is the normalization script for ESA to add up any custom logic. This java script file has a function ‘`normalizeAlert`’ with parameters headers, rawAlert, and normalizedAlert. The variable ‘`normalized`’ is a immutable copy object which has an embedded object of list of normalized events. So if you have any custom meta keys configured for the events then you have to iterate through the ‘`normalized.events`’ to populate the appropriate meta keys with values from the ‘`rawAlert.events`’ object. Below is the sample code.



```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {

  // normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

  if(normalized.events != undefined){
    custom_events = normalized.events;
  }else{
    custom_events = new Array();
  }

  for (var i = 0; i < rawAlert.events.length; i++) {

    custom_events[i].legalentity: Utils.stringValue(rawAlert.events[i].isgs_legalentity);
    custom_events[i].companycode: Utils.stringValue(rawAlert.events[i].isgs_companycode);

  }

  if(normalized.events == undefined){
    normalized.events = custom_events;
  }

  return normalized;
}
```

Task 17. (Conditional) Add Respond Notification Settings Permissions

Note: If you already configured these permissions in 11.2 or later, you can skip this task.

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**Configure** > **Respond Notifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you must add additional permissions to your existing built-in NetWitness Platform user roles. You must also add permissions to your custom roles.

See the “Respond Notification Settings Permissions” topic in the *NetWitness Respond Configuration Guide*.

For detailed information about user permissions, see the *System Security and User Management Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Decoder and Log Decoder

Task 18. Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

You must reconfigure the Legacy Endpoint recurring feed due to the change in Java version. Complete the following step to fix this problem.

- Import the NetWitness Endpoint CA certificate into the NetWitness Platform Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness Endpoint Integration Guide* to import the certificate. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Endpoint Installation Tasks

Install the 11.4 Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 11.4 by downloading the Relay Server installer from the upgraded Endpoint Server. For more information see "(Optional) Installing and Configuring Relay Server" section in the *Endpoint Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.
2. Restart the Endpoint Server using the command:

   ```
   systemctl restart rsa-nw-endpoint-server
   ```

Upgrade Endpoint Agents

See "Upgrade Agents" in the *Endpoint Agent Installation Guide for NetWitness Platform 11.4* for instructions on how to upgrade agents.

NetWitness UEBA Post Upgrade Tasks

The following sections describe the tasks for installing and upgrading NetWitness UEBA.

- (Optional) – Update UEBA configuration
- (Optional) Add Packets Schema
- (Optional) Enable Endpoint Data Sources
- (Optional) Enable UEBA Indicator Forwarder
- (Mandatory) Update Airflow Configuration

(Optional) – Update UEBA configuration

To get the UEBA configuration main parameters, run the following curl command from the UEBA machine:

```
curl http://localhost:8888/application-default.properties
```

The main parameters that will be returned are as follows:

- `uiIntegration.brokerId`: Service ID of the NW data source (Broker / Concentrator).
- `dataPipeline.schemas`: List of schemas processed by the UEBA.
- `dataPipeline.startTime`: Date when UEBA started consuming data from the NetWitness data source.
- `outputForwarding.enableForwarding`: UEBA Forwarder status.

(Optional) Add Packets Schema

If NetWitness Platform 11.4 is configured to perform packet capturing, you can add packet schemas to NetWitness UEBA.

To add packet schemas, run the following command on the UEBA server:

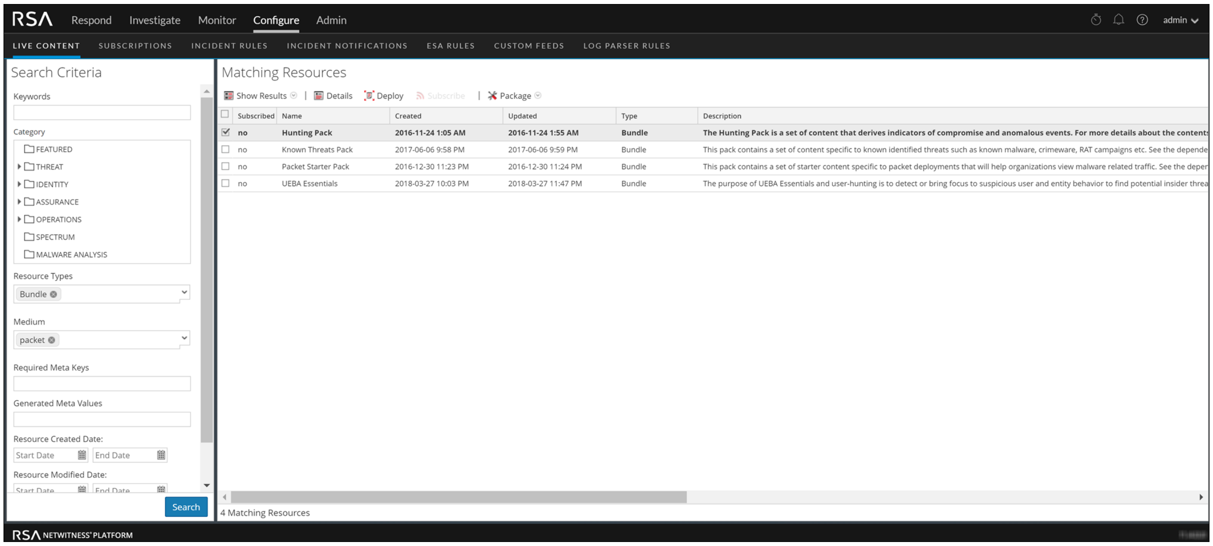
```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"add","path":"/dataPipeline/schemas/-","value":"TLS"}]}'
```

Add the Hunting Pack

In NetWitness Platform, add the hunting pack or verify if it is available:

1. Log in to NetWitness Platform
2. Go to **ADMIN** and select **Admin Server**

3. Click and select **Configure** > **Live Content**



Resource Types: Bundle

Medium: packet

	Subscribed	Name	Created	Updated	Type	Description
☑	no	Hunting Pack	2016-11-24 1:05 AM	2016-11-24 1:55 AM	Bundle	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the content:
□	no	Known Threats Pack	2017-06-06 9:58 PM	2017-06-06 9:59 PM	Bundle	This pack contains a set of content specific to known identified threats such as known malware, crimeware, RAT campaigns etc. See the depende
□	no	Packet Starter Pack	2016-12-30 11:23 PM	2016-12-30 11:24 PM	Bundle	This pack contains a set of starter content specific to packet deployments that will help organizations view malware related traffic. See the deper
□	no	UEBA Essentials	2018-03-27 10:03 PM	2018-03-27 11:47 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focus to suspicious user and entity behavior to find potential insider threa

.

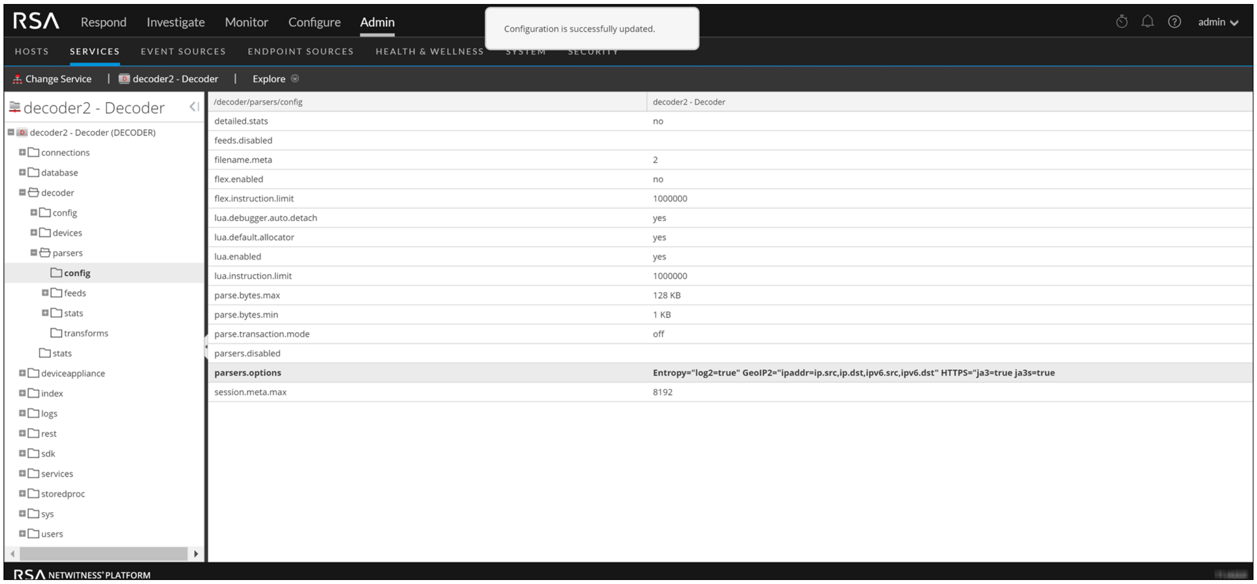
4. In the Search Criteria, select the following:
   a. **Bundle** under Resources Type.
   b. **Packet** under Medium.
5. Click **Search**.
   A list of matching resources is displayed.
6. Select **Hunting Pack** from the list and click **Deploy**.
   The hunting pack is added.

Add JA3 and JA3s

The JA3 and JA3s fields are supported by the Network Decoder in 11.3.1 and later. Verify that your Network Decoder is upgraded to one of these versions.

To add JA3 and JA3s:

1. Log in to NetWitness Platform.
2. Go to **ADMIN** and select **Decoder**.
3. Navigate to `/decoder/parsers/config/parsers.options`.
4. Add `HTTPS="ja3=true ja3s=true`.
   The JA3 and JA3s fields are configured.



Configuration is successfully updated.

/decoder/parsers/config	decoder2 - Decoder
detailed.stats	no
feeds.disabled	
filename.meta	2
flex.enabled	no
flex.instruction.limit	1000000
lua.debugger.auto.detach	yes
lua.default.allocator	yes
lua.enabled	yes
lua.instruction.limit	1000000
parse.bytes.max	128 KB
parse.bytes.min	1 KB
parse.transaction.mode	off
parsers.disabled	
parsers.options	**Entropy="log2=true" GeoIP2="ipaddr=ip.src,ip.dst,ipv6.src,ipv6.dst" HTTPS="ja3=true ja3s=true**
session.meta.max	8192

(Optional) Enable Endpoint Data Sources

If NetWitness Endpoint Server is configured in NetWitness Platform 11.4, you can enable the Endpoint data sources such as Process and Registry to generate alerts in UEBA.

To enable Endpoint data sources, run the following commands on the UEBA server :

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"add","path":"/dataPipeline/schemas/-","value":"PROCESS"},
{"op":"add","path":"/dataPipeline/schemas/-","value":"REGISTRY"}]}'
```

(Optional) Enable UEBA Indicator Forwarder

If the NetWitness Respond Server is configured in NetWitness Platform 11.4, you can transfer the NetWitness UEBA indicators to the NetWitness Respond Server and to the correlation server to create incidents.

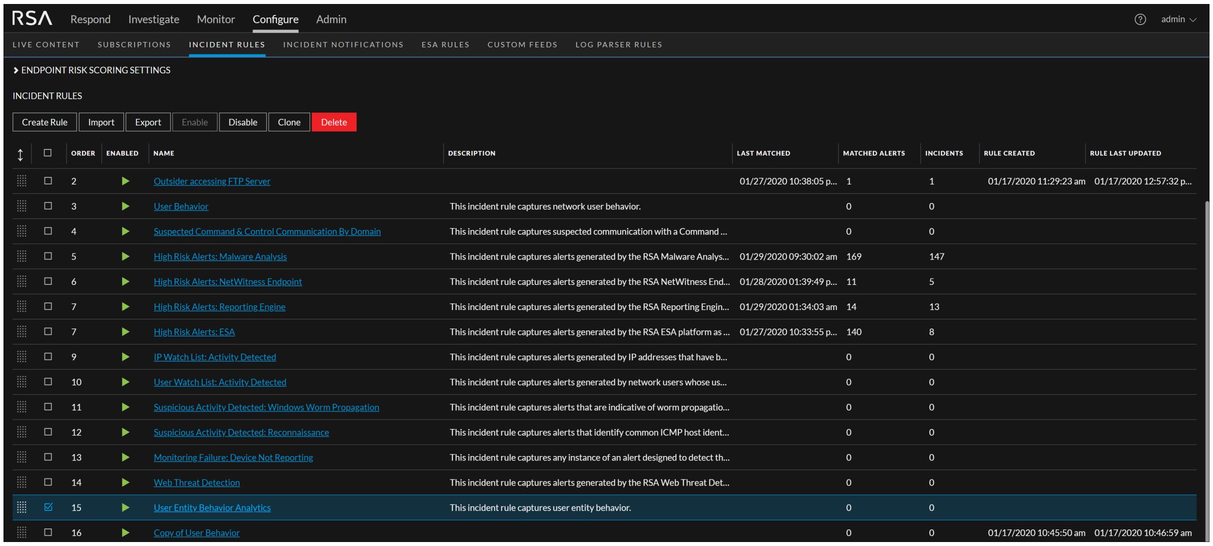
To enable the UEBA indicator forwarder, run the following command:

```
curl -X PATCH http://localhost:8881/configuration -H ', content-type:
application/json' -d '{"operations":
[{"op":"replace","path":"/outputForwarding/enableForwarding","value":true}]}'
```

To view the incidents in Respond:

1. Log in to NetWitness Platform.
2. Go to **Configure** > **INCIDENT RULES**

3. Select the **User Entity Behavior Analytics** rule checkbox.



INCIDENT RULES

↕	□	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS	RULE CREATED	RULE LAST UPDATED
	□	2	▶	Outsider accessing FTP Server		01/27/2020 10:38:05 p...	1	1	01/17/2020 11:29:23 am	01/17/2020 12:57:32 p...
	□	3	▶	User Behavior	This incident rule captures network user behavior.		0	0		
	□	4	▶	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication with a Command ...		0	0		
	□	5	▶	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware Analys...	01/29/2020 09:30:02 am	169	147		
	□	6	▶	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA NetWitness End...	01/28/2020 01:39:49 p...	11	5		
	□	7	▶	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting Engin...	01/29/2020 01:34:03 am	14	13		
	□	7	▶	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platform as ...	01/27/2020 10:33:55 p...	140	8		
	□	9	▶	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that have b...		0	0		
	□	10	▶	User Watch List: Activity Detected	This incident rule captures alerts generated by network users whose us...		0	0		
	□	11	▶	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of worm propagatio...		0	0		
	□	12	▶	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common ICMP host ident...		0	0		
	□	13	▶	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert designed to detect th...		0	0		
	□	14	▶	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Threat Det...		0	0		
	☑	15	▶	User Entity Behavior Analytics	This incident rule captures user entity behavior.		0	0		
	□	16	▶	Copy of User Behavior			0	0	01/17/2020 10:45:50 am	01/17/2020 10:46:59 am

(Mandatory) Update Airflow Configuration

After you upgrade to NetWitness Platform 11.4.1, make sure you update the Airflow configurations. However before you update the Airflow configurations, you must perform the following mandatory steps:

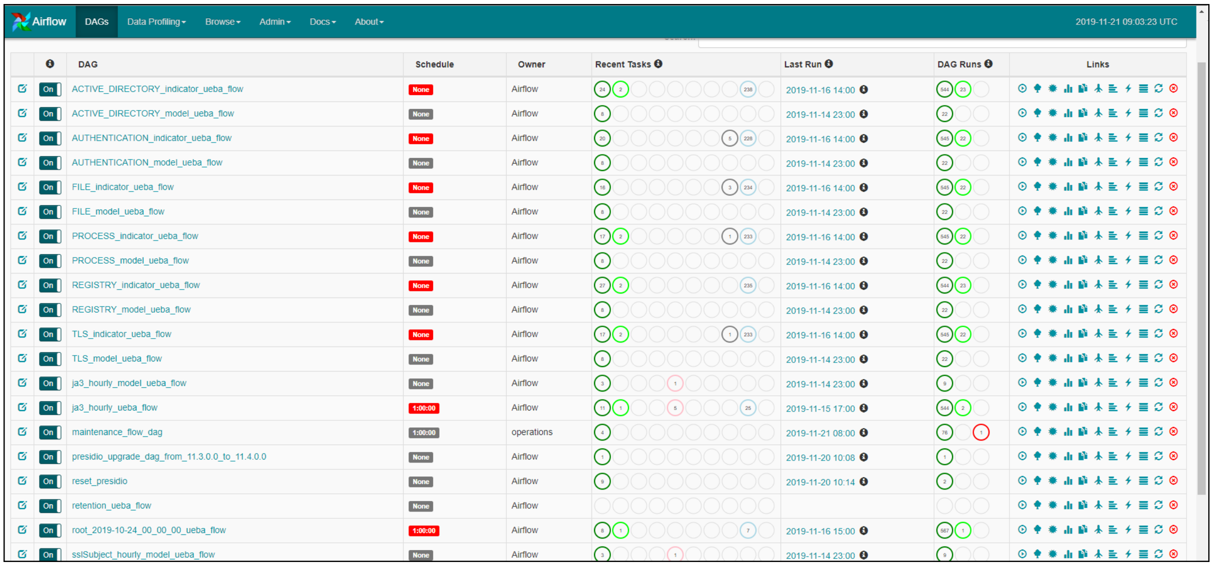
- Run the script as root user from the UEBA machine:
  `python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_server_config.py`.

To update the Airflow Configurations:

1. Access Airflow web server UI (`https://<UEBA_host>/admin/`) and enter the username and password.

   > **Note:** The Airflow web server UI username is admin, and the password is same as the `deploy_Admin` password.

   > **Note:** Mismatched tasks between NetWitness Platform 11.3 and NetWitness Platform 11.4 in the full flow DAG can be marked in red.



		DAG	Schedule	Owner	Recent Tasks	Last Run	DAG Runs	Links
	On	ACTIVE_DIRECTORY_indicator_ueba_flow	None	Airflow	24 2 238	2019-11-16 14:00	544 23	
	On	ACTIVE_DIRECTORY_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	AUTHENTICATION_indicator_ueba_flow	None	Airflow	20 5 228	2019-11-16 14:00	545 22	
	On	AUTHENTICATION_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	FILE_indicator_ueba_flow	None	Airflow	16 3 234	2019-11-16 14:00	545 22	
	On	FILE_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	PROCESS_indicator_ueba_flow	None	Airflow	17 2 1 233	2019-11-16 14:00	545 22	
	On	PROCESS_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	REGISTRY_indicator_ueba_flow	None	Airflow	27 2 235	2019-11-16 14:00	544 23	
	On	REGISTRY_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	TLS_indicator_ueba_flow	None	Airflow	17 2 1 233	2019-11-16 14:00	545 22	
	On	TLS_model_ueba_flow	None	Airflow	8	2019-11-14 23:00	22	
	On	ja3_hourly_model_ueba_flow	None	Airflow	3 1	2019-11-14 23:00	9	
	On	ja3_hourly_ueba_flow	1:00:00	Airflow	11 1 5 25	2019-11-15 17:00	544 2	
	On	maintenance_flow_dag	1:00:00	operations	4	2019-11-21 08:00	76 1	
	On	presidio_upgrade_dag_from_11.3.0.0_to_11.4.0.0	None	Airflow	1	2019-11-20 10:08	1	
	On	reset_presidio	None	Airflow	9	2019-11-20 10:14	2	
	On	retention_ueba_flow	None	Airflow				
	On	root_2019-10-24_00_00_00_ueba_flow	1:00:00	Airflow	8 1 7	2019-11-16 15:00	567 1	
	On	sslSubject_hourly_model_ueba_flow	None	Airflow	3 1	2019-11-14 23:00	9	

2. Click ▶ on `presidio_upgrade_dag_from_11.*_to_11.4.0.1` to pause the full flow DAG.

> **Note:** This step creates a new full flow DAG where the start date is 27 days ago, removes the old full flow DAG and starts a new flow DAG.

3. Once the DAG update is successful, the `presidio_upgrade DAG` task is marked with green circle in the **Recent Tasks** column.

Enable New Features

This section describes the new features that you can enable in 11.4.1. For a complete list of new features in this release, see the *Release Notes for RSA NetWitness Platform 11.4.1*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Customer Experience Improvement Program

The RSA NetWitness Platform Customer Experience Improvement Program (CEIP) is an initiative to continuously improve RSA NetWitness Platform. When enabled by the customer, the CEIP performs analytics about how individual users work in RSA NetWitness Platform without interrupting their workflow or personally identifying users. RSA considers these analytics when making decisions about new features and enhancements to prioritize in upcoming releases. For more information, see "Configure the Customer Experience Improvement Program" in the *System Configuration Guide*.

Improved Email Reconstruction in the Events View

Analysts can now reconstruct email sessions directly in the Events view. For more information, see "Reconstruct an Event in the Events View" in the *Investigate User Guide*.

Intra-session and Related Events Grouped in the Events View

To more easily detect relationships in captured data, you can group events from split and related sessions in the Events and Legacy Events views. The user interface helps you identify the leading event and subsequent events by nesting subsequent events under the leading event. For more information, see "Group Events from Split and Related Sessions in the Events and Legacy Events Views" in the *Investigate User Guide*.

Configurable Event Analysis View Event Limit

To optimize performance in Event Analysis, administrators can configure the default number of events loaded in the Events panel, and then configure a lower limit for different user roles. For more information, see "Configure Event Analysis View Settings" in the *System Configuration Guide for RSA NetWitness Platform*.

Faster and Easier Query Building in the Events View

The user interface for creating filters and building queries continues to evolve to support faster creation of filters with several new time-saving features. For more information, see "Filter Events in the Events View" in the *Investigate User Guide*.

Configure Custom Certificates on Log Collectors and Log Decoders

You can configure custom certificates for the syslog listener on Log Collectors and Log Decoders. This enables you to put your own trusted certificate in place for the syslog listener, while all other functionality uses the pre-installed certificates. For more information, see "(Optional) Configure Custom Certificates on Log Collectors" in the *Log Collection Configuration Guide* and "(Optional) Configure Custom Certificates on Log Decoders" in the *Decoder Configuration Guide*.

Event Source Visualization and Search Improvements

You can search event sources using IP or hostname addresses, or by Name, on Log Collectors to easily view required sources. Historical graphs and other information have been moved to Event Sources Management from Health & Wellness. For more information, see the *Event Sources Management User Guide*.

SSO Authentication is Supported for Analyst UI Deployments

Single Sign-On (SSO) is supported for analysts in a multiple NetWitness Platform User Interface instances deployment.

Simplified Management of the deploy_admin Account

The `deploy_admin` account is a password-based system account that is used on every NetWitness Platform host, and must be kept synchronized between all hosts. It can require periodic updating depending on your deployment environment policies. Starting with 11.4.1, the `deploy_admin` password is centrally managed with the `nw-manage` script on the NW Server. The `nw-manage` script execution updates the password on all NetWitness Platform component hosts that use the `deploy_admin` account. For more information, see "Manage the deploy_admin Account" in the *System Maintenance Guide*.

Change the IP Address of the Warm Standby NW Server

If your secondary NW Server must have a different IP address from your primary NW Server, you can use a manual procedure for failover that enables you to change the IP address of the Warm Standby NW Server. This procedure is documented in "Fail Over Primary NW Server to Secondary NW Server with Different IP Address" in the *Deployment Guide*.

Support to Forward High-Risk Usernames to RSA SecurID Access

With the NetWitness Platform Integration with RSA SecurID Access, the NetWitness Respond server can now also send the Active Directory username of high-risk users from incidents to RSA SecurID Access. To configure this metadata on the Respond Server, see the *Respond Configuration Guide*.

ESA Rule Deployment Troubleshooting Metrics are Available Through Nw-Shell

You can use Nw-Shell to view ESA Correlation Server metrics for each of your ESA rule deployments. These metrics show the number of sessions behind for the deployment data sources as well as the memory usage for the rules in the deployment. For more information, see “Obtain Correlation Server Metrics for ESA Rule Deployment Troubleshooting Using Nw-Shell” in the *Alerting with ESA Correlation Rules User Guide*.

Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface

You can use this method if the NW Server host is not connected to Live Services.

Prerequisites

Make sure that you have downloaded the following files from RSA Link (https://community.rsa.com/) > **NetWitness Platform** > **RSA NetWitness Logs and Network** > **Downloads** > RSA Downloads to a local directory:

- If you are upgrading from an 11.2.x.x or 11.3.x.x release to 11.4.1.0, download:
  ```
  netwitness-11.4.0.0.zip
  netwitness-11.4.1.0.zip
  ```
- If you are upgrading from an 11.4.0.x release to 11.4.1.0 release, download:
  ```
  netwitness-11.4.1.0.zip
  ```
- If you are using external repository, you can update the external repository with the latest upgrade content. For more information, see External Repo Instructions for CLI upgrade.

Procedure

You must perform the upgrade steps for NW Server hosts and for component servers.

Note: If you copy and paste the commands from PDF to Linux SSH terminal, the characters do not work. It is recommended to type the commands.

1. Stage the 11.4.1.0 files to prepare them for the upgrade:
   - **If you are upgrading from 11.2.x.x or 11.3.x.x**, you must stage 11.4.0.0 and 11.4.1.0. Log into the NW Server as `root` and create the following directories:
     ```
     /tmp/upgrade/11.4.0.0
     /tmp/upgrade/11.4.1.0
     ```
     and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:
     ```
     unzip netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0
     unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
     ```
   - **If you are upgrading from 11.4.0.0 to 11.4.1.0**, you only need to stage 11.4.1.0. Log into the NW Server as `root` and create the following directory:
     ```
     /tmp/upgrade/11.4.1.0
     ```
     and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:
     ```
     unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
     ```

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

2. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.4.1.0 --stage-dir /tmp/upgrade
   ```

3. Upgrade the NW Server host, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.0
   ```

4. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.

5. Repeat steps 3 through 5 for each component host, changing the IP address to the component host which is being upgraded.

Note: You can check versions of all the hosts, using the command `upgrade-cli-client --list` on the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

Note: If the following error is displayed during the upgrade process:

```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support for assistance (https://community.rsa.com/docs/DOC-1294).

External Repo Instructions for CLI upgrade

1. Stage the 11.4.1.0 files to prepare them for the upgrade:

   - **If you are upgrading from 11.2.x.x or 11.3.x.x**, you must stage 11.4.0.0 and 11.4.1.0. Log into the NW Server as `root` and create the following directories:
     ```
     /tmp/upgrade/11.4.0.0
     /tmp/upgrade/11.4.1.0
     ```
     and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:
     ```
     unzip netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0
     unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
     ```

   - **If you are upgrading from 11.4.0.0 to 11.4.1.0**, you only need to stage 11.4.1.0. Log into the NW Server as `root` and create the following directory:
     ```
     /tmp/upgrade/11.4.1.0
     ```
     and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:
     ```
     unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
     ```

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

2. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.4.1.0 --stage-dir /tmp/upgrade
   ```

3. Upgrade the NW Server host using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.4.1.0
   ```
4. When the NW Server host upgrade is successful, reboot the host from NetWitness UI.
5. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being upgraded.

> **Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

> **Note:** If the following error displays during the upgrade process:
> ```
> 2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
> o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
> protocol method: #method<connection.close>(reply-code=320, reply-
> text=CONNECTION_FORCED - broker forced connection closure with reason
> 'shutdown', class-id=0, method-id=0)
> ```
> the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support for assistance (https://community.rsa.com/docs/DOC-1294).

Appendix B. Troubleshooting Version Installations and Upgrades

This section describes the error messages displayed in the Hosts view when it encounters problems updating host versions and installing services on hosts in the Hosts view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

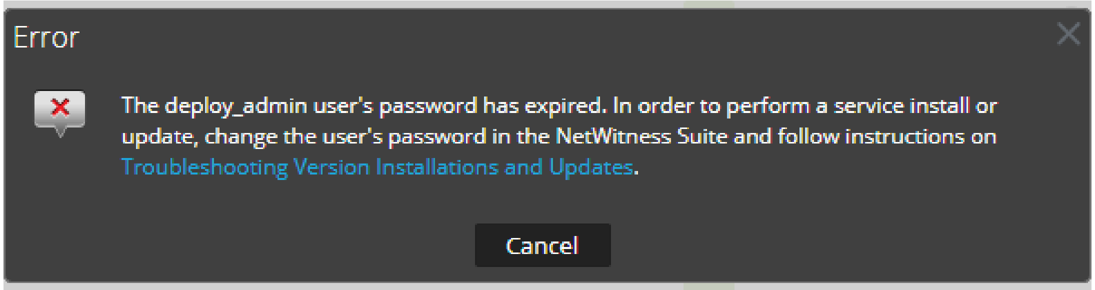
Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

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

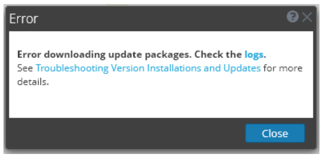
Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

- Log Collector Service
- NW Server
- Orchestration
- Reporting Engine

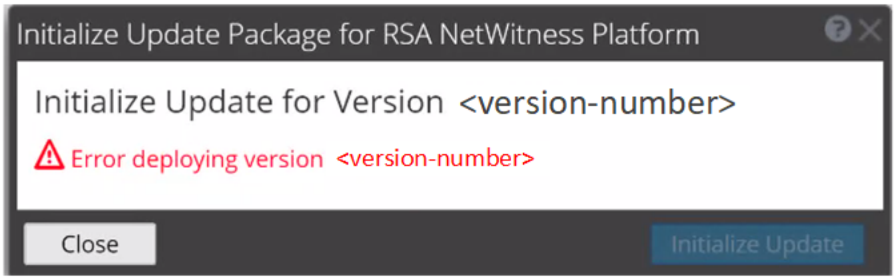
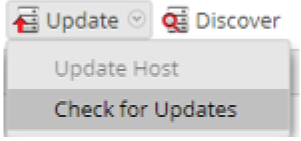
deploy_admin User Password Has Expired Error

Error Message	 Error The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on Troubleshooting Version Installations and Updates.
Cause	The `deploy_admin` user password has expired.
Solution	Reset your `deploy_admin` password password. 1. On all component hosts (not including the NW Server host), run the following command. `/opt/rsa/saTools/bin/set-deploy-admin-password` 2. After all the component hosts have been updated, run this command on the NW Server host. `/opt/rsa/saTools/bin/set-deploy-admin-password` 3. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

Downloading Error

Error Message	 Error **Error downloading update packages. Check the logs.** See Troubleshooting Version Installations and Updates for more details.
Problem	When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete.
Cause	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
Solution	1. Try to update again. 2. If it fails again with the same error, try to update using the offline methods as described in "Offline Method from Hosts View" or "Offline Method Using Command Line Interface" in the *Upgrade Guide for NetWitness Platform 11.4*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents. 3. If you are still not able to update, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Deploying Version <version-number> Missing Update Packages

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

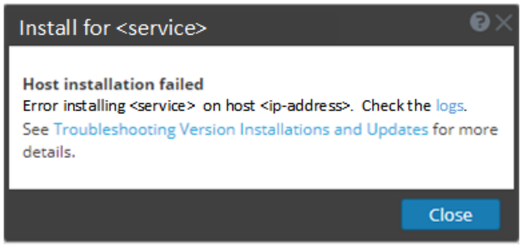
External Repo Update Error

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

	• the URL does exist on the NW Server host. • you used the correct path and remove any spaces from it.

Host Installation Failed Error

Error Message



Install for <service>

Host installation failed

Error installing <service> on host <ip-address>. Check the logs.

See Troubleshooting Version Installations and Updates for more details.

Problem

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

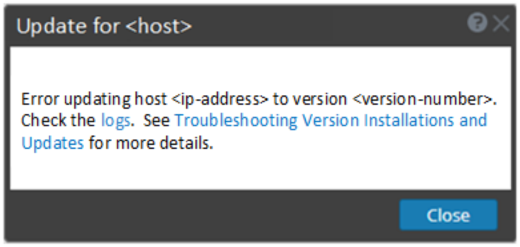
Solution

1. Try to install the service again.
   Often this is all you need to do.
2. If you still cannot install the service:
   a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):
      ```
      /var/netwitness/uax/logs/sa.log
      /var/log/netwitness/orchestration-server/orchestration-server.log
      /var/log/netwitness/deployment-upgrade/chef-solo.log
      /var/log/netwitness/config-management/chef-solo.log
      /var/lib/netwitness/config-management/cache/chef-stacktrace.out
      ```
      The error appears in one or more of these logs.

   b. Try to resolve the issue and reinstall the service.
      - Cause 1 - Entered the wrong `deploy_admin` password in the nwsetup-tui.
        Solution - Reset your `deploy_admin` password password.
        1. On the NW Server host and all other hosts on 11.x, run the following command.
           `/opt/rsa/saTools/bin/set-deploy-admin-password`
        2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.
      - Cause 2 -The `deploy_admin` password has expired.
        Solution - Reset your `deploy_admin` password password.
        1. On the NW Server host and all other hosts on 11.x, run the following command.
           `/opt/rsa/saTools/bin/set-deploy-admin-password`
        2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

	3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).

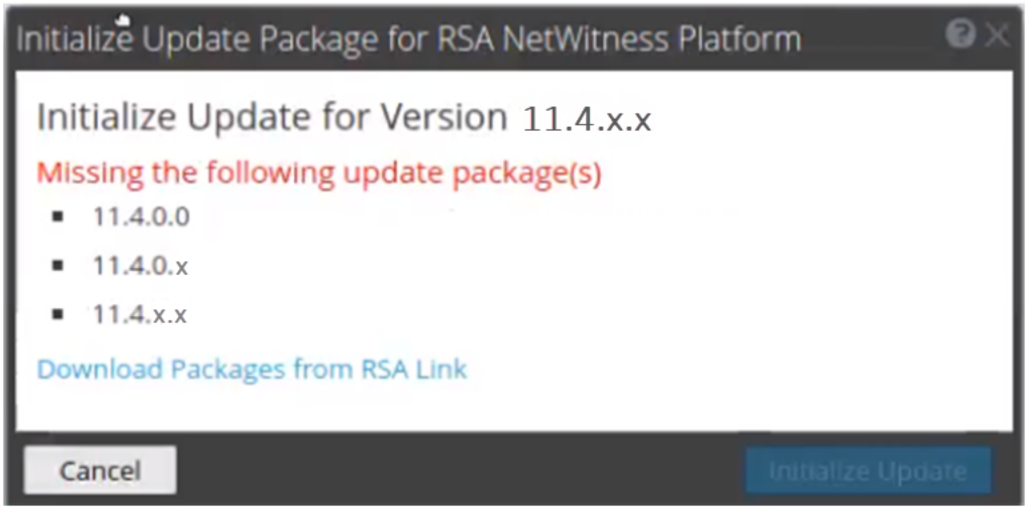
Host Update Failed Error

Error Message	Update for <host> Error updating host <ip-address> to version <version-number>. Check the logs. See Troubleshooting Version Installations and Updates for more details. Close
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.

Solution	1. Try to apply the version update to the host again.
	Often this is all you need to do.
	2. If you still cannot apply the new version update:
	a. Monitor the following logs on NW Server as it progresses (for example, run the `tail -f` command from the command line):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error appears in one or more of these logs.
	b. Try to resolve the issue and reapply the version update.
	• Cause 1 - `deploy_admin` password has expired.
	Solution - Reset your `deploy_admin` password .
	Complete the following steps to resolve Cause 1.
	1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
	2. Select the `deploy_admin` and click **Reset Password**.
	3. (Conitional) If NetWitness Suite does not allow you to expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
	a. Reset `deploy_admin` to use a new password.
	b. On all non-NW Server hosts on 11.x , run the following command using

<table>
<tr><td></td><td>
the matching <code>deploy_admin</code> password from NW Server host.
<code>/opt/rsa/saTools/bin/set-deploy-admin-password</code>
<ul>
<li>Cause 2 -The <code>deploy_admin</code> password was changed on NW Server host but not changed on non-NW Server hosts.
Complete the following step to resolve Cause 2.
<ul>
<li>On all non-NW Server hosts on 11.x , run the following command using the matching <code>deploy_admin</code> password from NW Server host.
<code>/opt/rsa/saTools/bin/set-deploy-admin-password</code></li>
</ul></li>
</ul>
3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (https://community.rsa.com/docs/DOC-1294).
</td></tr>
</table>

Missing Update Packages Error

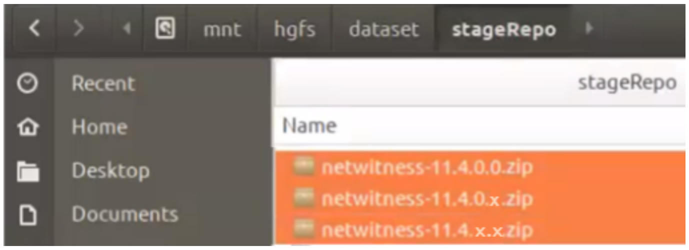
<table>
<tr><td><b>Error Message</b></td><td>

Initialize Update Package for RSA NetWitness Platform

Initialize Update for Version 11.4.x.x

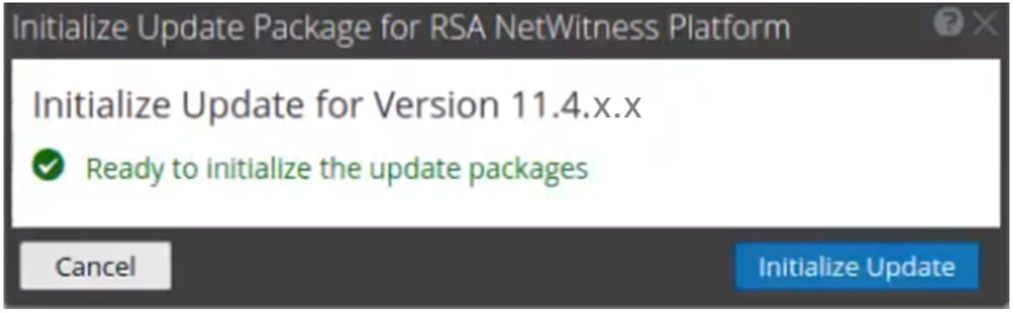
Missing the following update package(s)

- 11.4.0.0
- 11.4.0.x
- 11.4.x.x

Download Packages from RSA Link

</td></tr>
<tr><td><b>Problem</b></td><td>
Missing the following update package(s) is displayed in the <b>Initialize Update Package for RSA NetWitness Platform</b> dialog when you are updating a host from the <b>Hosts</b> view offline and there are packages missing in the staging folder.
</td></tr>
<tr><td><b>Solution</b></td><td>
1. Click Download Packages from RSA Link in the <b>Initialize Update Package for RSA NetWitness Platform</b> dialog.
The RSA Link page that contains the update files for the selected version is displayed.
2. Select missing packages from staging folder (for example, <b>11.4.0.0</b>, <b>11.4.0.x</b>, and <b>11.4.x.x</b>).


</td></tr>
</table>

	The **Initialize Update Package for RSA NetWitness Platform** dialog is displayed telling you that it is ready to initialize the update packages.  Initialize Update Package for RSA NetWitness Platform Initialize Update for Version 11.4.x.x Ready to initialize the update packages

OpenSSL 1.1.x

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

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

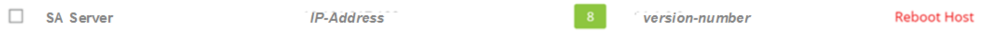
Solution	Specify the compatible cipher list on the command line. For example:
	`$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3`
	`I've read & consent to terms in IS user agreement.`
	`root@10.1.2.3's password:`
	`Last login: Mon Oct 21 19:03:23 2019`

Patch Update to Non-NW Server Error

Error Message	The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error: **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
Problem	After you update the NW Server host to a version, you must update all non-NW Server hosts to the same version. For example, if you update the NW Server from 11.4.0.0 to 11.4.x.x , the only update path for the non-NW Server hosts is the same version (that is, 11.4.x.x). If you try to update any non-NW Server host to a different version (for example, from 11.4.0.0 to an 11.4.0.x) you will get this error.
Solution	You have two options:

	- Update the non-NW Server host to 11.4.x.x, or - Do not update the non-NW Server host (keep it at its current version)

Reboot Host After Update from Command Line Error

Error Message	You receive a message in the User Interface to reboot the host after you update and reboot the host offline.  □ SA Server IP-Address 8 version-number Reboot Host
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Reporting Engine Restarts After Upgrade

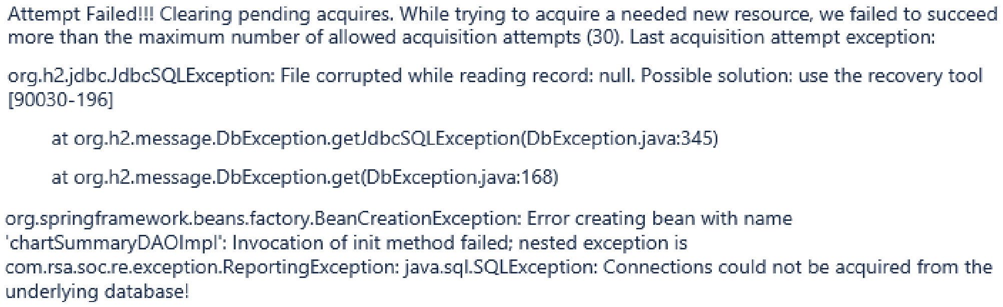
<table>
<tr><td><b>Problem</b></td><td>In some cases, after you upgrade to 11.4 from versions of 11.x, such as 11.2 or 11.3, the Reporting Engine service attempts to restart continuously without success.</td></tr>
<tr><td><b>Cause</b></td><td>The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.</td></tr>
<tr><td><b>Solution</b></td><td>

To resolve the issue, do the following:

1. Check which database files are corrupted:

   Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks:

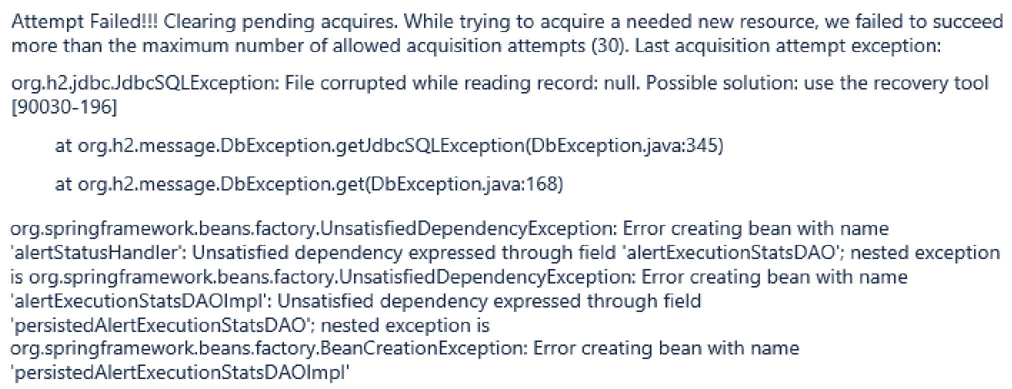
   - If the live charts db file is corrupted, the following logs are displayed:

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

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

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

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

     org.springframework.beans.factory.BeanCreationException: Error creating bean with name
     'chartSummaryDAOImpl': Invocation of init method failed; nested exception is
     com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the
     underlying database!
     ```

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

</td></tr>
</table>



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

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

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

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

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

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

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

2. To resolve the live charts database file corruption, perform the following steps:

   a. Stop the Reporting Engine service.

   b. Move the `livechart.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` folder to a temporary location.

   c. Restart the Reporting Engine service.

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

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

   a. Stop the Reporting Engine service.

   b. Replace the corrupted db file with the latest `alertstatusmanager.mv.db` or `reportstatusmanager.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/archives` folder.

   c. Restart the Reporting Engine service.

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

Log Collector Service (`nwlogcollector`)

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

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because`

	`the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Platform and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

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

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

NW Server

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

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 11.2.x.x or 11.3.x.x. to 11.4.0.0.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Orchestration

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

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

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

Reporting Engine Service

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

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