



# Upgrade Guide

for RSA NetWitness Platform 11.3.1.1



## 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

For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>.

## License Agreement

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

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

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

## Third-Party Licenses

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

## 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.

September 2019

# Contents

---

<b>Upgrade Overview .....</b>	<b>6</b>
Upgrade Considerations for ESA Rule Deployments .....	7
<b>Pre-Upgrade Tasks .....</b>	<b>8</b>
Task 1. Stop Data Capture and Aggregation .....	8
Task 2. (Conditional) Back Up Customized Respond Service Normalization Scripts .....	9
Task 3. Record Any String Array Type Meta Keys on the Event Stream Analysis Service .....	10
<b>Upgrade Tasks .....</b>	<b>12</b>
Task 1. (Conditional - Offline Methods Only) Download the 11.3.1.1 Patch .....	12
Task 2. (Conditional - CLI Offline Method Only) Upgrade External Repository .....	12
Task 3. Upgrade the Service Pack .....	12
Online Method (Connectivity to Live Services) .....	13
Offline Method (No connectivity to Live Services) .....	14
<b>Post Upgrade Tasks .....</b>	<b>17</b>
<b>Post Upgrade Tasks for Customers Upgrading From 11.3.x.x .....</b>	<b>17</b>
General .....	17
Task 1. Start Data Capture and Aggregation .....	17
Event Stream Analysis .....	18
Task 2 - (Conditional) Update Memory Required for Virtual ESA Host only .....	18
Task 3. Verify the ESA Rule Deployments .....	19
Task 4 - (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules .....	20
Task 5 - (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules .....	21
ESA Troubleshooting information .....	22
Respond .....	22
Task 6. (Conditional) Restore any Respond Service Custom Keys in the Aggregation Rule Schema ....	22
Task 7. Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts .....	22
Task 8. Update Default Incident Rule Group By Value .....	23
Task 9. (Conditional) Add Respond Notification Settings Permissions .....	23
<b>Post Upgrade Tasks for Customers Upgrading From 11.1.x.x or 11.2.x.x .....</b>	<b>24</b>

General .....	24
Task 1. Start Data Capture and Aggregation .....	24
Task 2. Set Up Context Menu Actions User Permissions .....	25
Task 3. Add "Manage Jobs" Permission to Roles Missing this Permission .....	27
Task 4. Upgrade Hive Version .....	29
Task 5. (Conditional) Reissue Certificates for Your Hosts .....	29
Task 6. Modify the Analyst Role investigate-server Permissions .....	29
Task 7. (Conditional) Reconfigure PAM RADIUS Authentication .....	30
Task 8. (Conditional) If NetWitness Platform Has No Web Access, Upload Response .bin File Again (License Server) .....	31
Event Stream Analysis .....	31
Task 9 - (Conditional) Update Memory Required for Virtual ESA Host only .....	31
Task 10 - Verify the String Array Type Meta Keys on the ESA Correlation Service and Next Steps ....	32
Task 11 (Conditional) Update RSA Live ESA Rules with Meta Type Changes from String to Array ....	33
Task 12 Verify the ESA Rule Deployments .....	34
Task 13 - (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules .....	35
Task 14 - (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules .....	36
ESA Troubleshooting Information .....	37
Example ESA Correlation Server Warning Message for Missing Meta Keys .....	38
Respond .....	38
Task 15. (Conditional) Restore any Respond Service Custom Keys in the Aggregation Rule Schema ...	38
Task 16. Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts .....	38
Task 17. upgrade Default Incident Rule Group By Value .....	39
Task 18. (Conditional) Add Respond Notification Settings Permissions .....	40
Decoder and Log Decoder .....	40
Task 19. (Conditional - for 11.1.x.x upgrade paths, Not in 11.2.x.x or later) Enable Metadata for GeoIP2 Parser .....	40
NetWitness Endpoint .....	41
Task 20. Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed .....	41
NetWitness UEBA .....	41
Task 21. (Conditional) Enable Endpoint Data Sources .....	41
Task 22. Enable UEBA Indicator Forwarder .....	41
Task 23. Upgrade Broker or Concentrator UUID .....	42

Task 24. Upgrade Airflow Configuration .....	42
Task 25. Restart Airflow Scheduler Service .....	42
<b>Enabling New Features .....</b>	<b>43</b>
New Support for Relay Server in NetWitness Endpoint .....	43
Expanded Detection of Encrypted Channels .....	43
Data Retention for Risk Scores .....	43
Configurable Event Analysis View Event Limit .....	43
Configurable Clearing of the Reconstruction Cache the Event Analysis View to Save Disk Space .....	44
<b>Product Documentation .....</b>	<b>45</b>
Feedback on Product Documentation .....	45
<b>Appendix A. Offline Method (No connectivity to Live Services). Upgrade Using the Command Line Interface .....</b>	<b>46</b>
External Repo Instructions for CLI Upgrade .....	47

# Upgrade Overview

---

This document provides instructions to upgrade RSA NetWitness® Platform. Read this document before deploying or upgrading to RSA NetWitness® Platform 11.3.1.1. If you have questions or have any issues with this upgrade, contact Customer Support for assistance (<https://community.rsa.com/docs/DOC-1294>).

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

The following upgrade paths are supported for RSA NetWitness® Platform 11.3.1.1:

**Note:** If your current hosts are on 10.6.x.x, you must first upgrade to 11.3.0.2, and then upgrade to 11.3.1.1. For information about upgrading to 11.3.0.2, see the "Installation & Upgrade Guides" section on RSA Link to find information about the types of systems you need to upgrade. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

- RSA NetWitness® Platform 11.1.0.0 to 11.3.1.1
- RSA NetWitness® Platform 11.1.0.1 to 11.3.1.1
- RSA NetWitness® Platform 11.1.0.2 to 11.3.1.1
- RSA NetWitness® Platform 11.1.0.3 to 11.3.1.1
- RSA NetWitness® Platform 11.2.0.0 to 11.3.1.1
- RSA NetWitness® Platform 11.2.0.1 to 11.3.1.1
- RSA NetWitness® Platform 11.2.1.0 to 11.3.1.1
- RSA NetWitness® Platform 11.2.1.1 to 11.3.1.1
- RSA NetWitness® Platform 11.2.1.2 to 11.3.1.1
- RSA NetWitness® Platform 11.3.0.0 to 11.3.1.1
- RSA NetWitness® Platform 11.3.0.1 to 11.3.1.1
- RSA NetWitness® Platform 11.3.0.2 to 11.3.1.1
- RSA NetWitness® Platform 11.3.1.0 to 11.3.1.1

For more information about this release, see the *Release Notes for RSA NetWitness Platform 11.3.1.1* on the NetWitness Platform documentation page on RSA Link. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

You can upgrade to the 11.3.1.1 service pack using one of the following options:

- If the NW Server host has internet connectivity to Live Services, the NetWitness Platform User Interface can be used to apply the patch.

- If the NW Server host does not have internet connectivity to Live Services, the Command Line Interface (CLI) can be used to apply the patch.

## Upgrade Considerations for ESA Rule Deployments

This section applies to upgrades from 11.1.x.x and 11.2.x.x to 11.3.1.1.

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

After you upgrade to 11.3.1.1, migrated ESA rule deployments have the following changes.

1. If an ESA rule deployment contains two services before you upgrade to 11.3.1.1, the deployment splits into two deployments. You can only have one ESA Correlation service in an ESA rule deployment in version 11.3.1.1.
2. If an ESA service has multiple ESA rule deployments before you upgrade to 11.3.1.1, they are combined into one deployment in version 11.3.1.1.

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

# Pre-Upgrade Tasks

## Task 1. Stop Data Capture and Aggregation

You must stop data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

### Stop Network Capture



These steps are for Decoders.

1. Log in to NetWitness Platform and go to **ADMIN > Services**.  
The Services view is displayed.
2. Select each **Decoder** service.

The screenshot shows the NetWitness Platform Admin interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the SERVICES sub-tab is selected. Below the navigation bar, there is a toolbar with buttons for Change Service, SIT-DEC1 - Decoder, System, Upload Packet Capture File, Stop Capture, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into four sections: Decoder Service Information, Appliance Service Information, Decoder User Information, and Host User Information. The Decoder Service Information section shows details for SIT-DEC1 (Decoder), including Name, Version, Memory Usage (414 MB), CPU (51%), Running Since (2016-Nov-15 10:12:07), Uptime (3 days 4 hours 25 minutes), and Current Time (2016-Nov-18 14:37:07). The Appliance Service Information section shows details for SIT-DEC1 (Host), including Name, Version, Memory Usage (24876 KB), CPU (52%), Running Since (2016-Nov-15 10:12:04), Uptime (3 days 4 hours 25 minutes 4 seconds), and Current Time (2016-Nov-18 14:37:08). The Decoder User Information and Host User Information sections are currently empty.

Decoder Service Information		Appliance Service Information	
Name	SIT-DEC1 (Decoder)	Name	SIT-DEC1 (Host)
Version		Version	
Memory Usage	414 MB (2.57% of 16081 MB)	Memory Usage	24876 KB (0.15% of 16081 MB)
CPU	51%	CPU	52%
Running Since	2016-Nov-15 10:12:07	Running Since	2016-Nov-15 10:12:04
Uptime	3 days 4 hours 25 minutes	Uptime	3 days 4 hours 25 minutes 4 seconds
Current Time	2016-Nov-18 14:37:07	Current Time	2016-Nov-18 14:37:08

Decoder User Information		Host User Information	

3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Stop Capture**.

### Stop Log Capture

These steps are for Log Decoders.



1. Log in to NetWitness Platform and 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  **Stop Capture**.

### Stop Aggregation

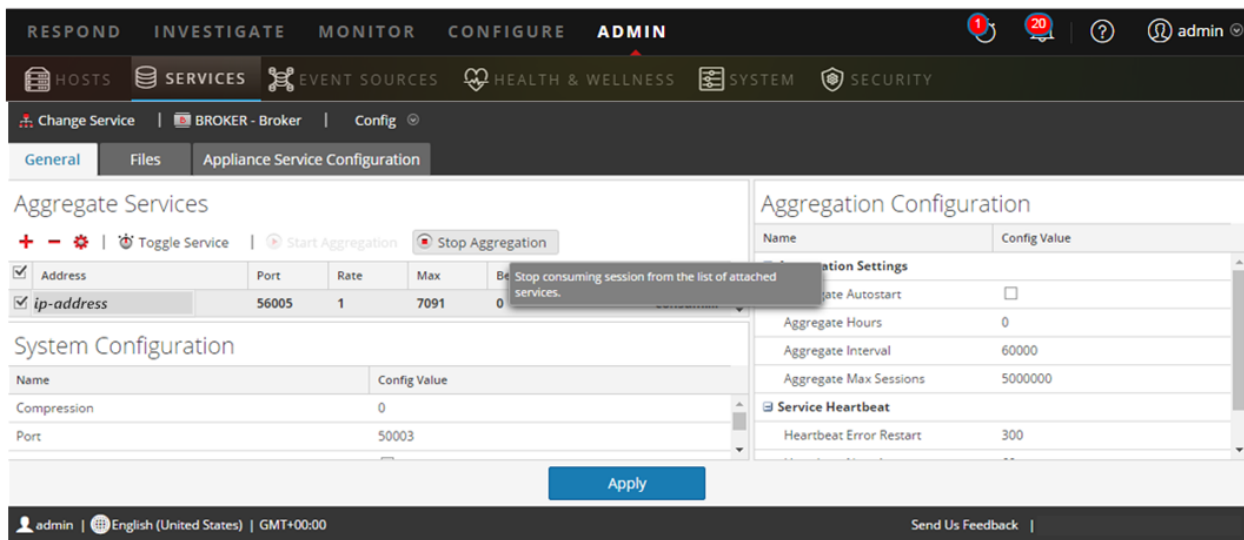
These steps are for Brokers, Concentrators, and Archivers.

1. Log in to NetWitness Platform and go to **ADMIN > Services**.

2. Select the **Broker**, **Concentrator**, or **Archiver** service.

3. Under  (actions), select **View > Config**.

4. The **General** tab is displayed.



5. Under **Aggregated Services** click  **Stop Aggregation**.

## Task 2. (Conditional) Back Up Customized Respond Service Normalization Scripts

Respond service normalization scripts are stored in the `/var/lib/netwitness/respond-server/scripts` directory. Back them up before you upgrade to 11.3.1.1 so you can restore your customizations in 11.3.1.1 as described in the [Respond](#) Post Upgrade Tasks.

1. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
2. Back up the following files:
 

```
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 only)
normalize_wtd_alerts.js
utils.js
```
3. If you customized any of the above scripts, copy the customizations so that you can restore them in 11.3.1.1.

### Task 3. Record Any String Array Type Meta Keys on the Event Stream Analysis Service

**Note:** If you are upgrading directly from 11.1.x.x or 11.2.x.x, you must perform this task.

To record any string array type meta keys in the `ArrayFieldNames` parameter on the Event Stream Analysis service:

1. Log into NetWitness Platform and go to **ADMIN > Services**.
2. Select the Event Stream Analysis service and click (actions) > **View > Explore**.
3. In the **Explore** view node list, select **Workflow > Source > netgenAggregationSource**.
4. In the **ArrayFieldNames** list, make a note of the string array type meta keys listed so you can verify that they are on the ESA Correlation service after the upgrade.

These are the default string array types from versions 11.1.x.x to 11.2.x.x:

- `action`
- `alias_host`
- `alias_ip`
- `alias_ipv6`
- `analysis_file`
- `analysis_service`
- `analysis_session`

- boc,email
- eoc
- inv\_category
- inv\_context
- ioc
- netname
- username

## Upgrade Tasks

---

Perform the following tasks to upgrade to 11.3.1.1:

- [Task 1. \(Conditional - Offline Methods Only\) Download the 11.3.1.1 Patch](#)
- [Task 2. \(Conditional - CLI Offline Method Only\) Upgrade External Repository](#)
- [Task 3. Upgrade the Service Pack](#)

There are two methods you can use to upgrade the service pack:

- [Online Method \(Connectivity to Live Services\)](#)
- [Offline Method \(No connectivity to Live Services\)](#)

### Task 1. (Conditional - Offline Methods Only) Download the 11.3.1.1 Patch

Download the file below, which contains all the NetWitness Platform 11.3.1.1 upgrade files, from RSA Link (<https://community.rsa.com/>) >NetWitness Platform > RSA NetWitness Logs and Network Downloads to a local directory: netwitness-11.3.1.1.zip

For more information, see [Offline Methods \(No Connectivity to Live Services\)](#).

### Task 2. (Conditional - CLI Offline Method Only) Upgrade External Repository

**Note:** Perform this step only if you are using an external repository for 11.3.1.1.

Upgrade the external repository with the latest upgrade content for NetWitness Platform 11.3.1.1 by downloading the following file: netwitness-11.3.1.1.zip.

For more information, see [Appendix A. Offline Method \(No connectivity to Live Services\). Upgrade Using the Command Line Interface](#).

### Task 3. Upgrade the Service Pack

You can choose one of the following upgrade methods based on your internet connectivity:

- [Online Method \(Connectivity to Live Services\)](#)
- [Offline Methods \(No Connectivity to Live Services\)](#)

## Online Method (Connectivity to Live Services)

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

**Note:** If the NW Server host does not have access to Live Services, use [Offline Method \(No connectivity to Live Services\)](#).

### Prerequisites

Make sure that:

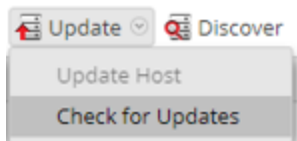
1. The **Automatically download information about new upgrades every day** option is checked and is applied in **ADMIN > System > Updates**.
2. Go to **ADMIN > Hosts > Update > Check for Updates** to check for upgrades. The Host view displays the **Update Available** status.
3. 11.3.1.1 is available in the **Update Version** column.


**Note:** If you have custom certs, move any custom certs from `/etc/pki/nw/trust/import/` directory to `/root/cert`. Follow these steps to move the certs:

1. `mkdir /root/cert`
2. `mv /etc/pki/nw/trust/import/* /root/cert`

### 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 **11.3.1.1** from the **Update Version** column. If you:
  - Want to view a dialog with the major features in the update and information on the updates, click the information icon (  ) to the right of the update 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 update at the same time only after upgrading 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.

## Offline Method (No connectivity to Live Services)

If your version of NetWitness Platform has no connection to the Internet and you want to upgrade to 11.3.1.1:

- **From the User Interface**, follow these instructions.

**Caution:** The offline User Interface method is only available if you are upgrading a host from 11.3.1.0 or later to 11.3.1.1. If you are upgrading a host on an earlier version, you must use the Offline Command Line Interface method.

- **From the Command Line Interface**, follow the instructions in [Appendix A. Offline Method \(No connectivity to Live Services\). Upgrade Using the Command Line Interface](#).

The following rules apply when you apply version updates:

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

**Note:** Alternatively, you can upgrade using the Command Line Interface if you have no connectivity to Live Services. Refer to [Appendix A. Offline Method \(No connectivity to Live Services\). Upgrade Using the Command Line Interface](#) for instructions.

### Task 1. Populate Staging Folder (/var/lib/netwitness/common/update-stage/) with Version Updates

1. Download the `netwitness-11.3.1.1.zip` update package from RSA Link to a local directory.
2. SSH to the NW Server host.

- Copy `netwitness-11.3.1.1.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder. For example:  

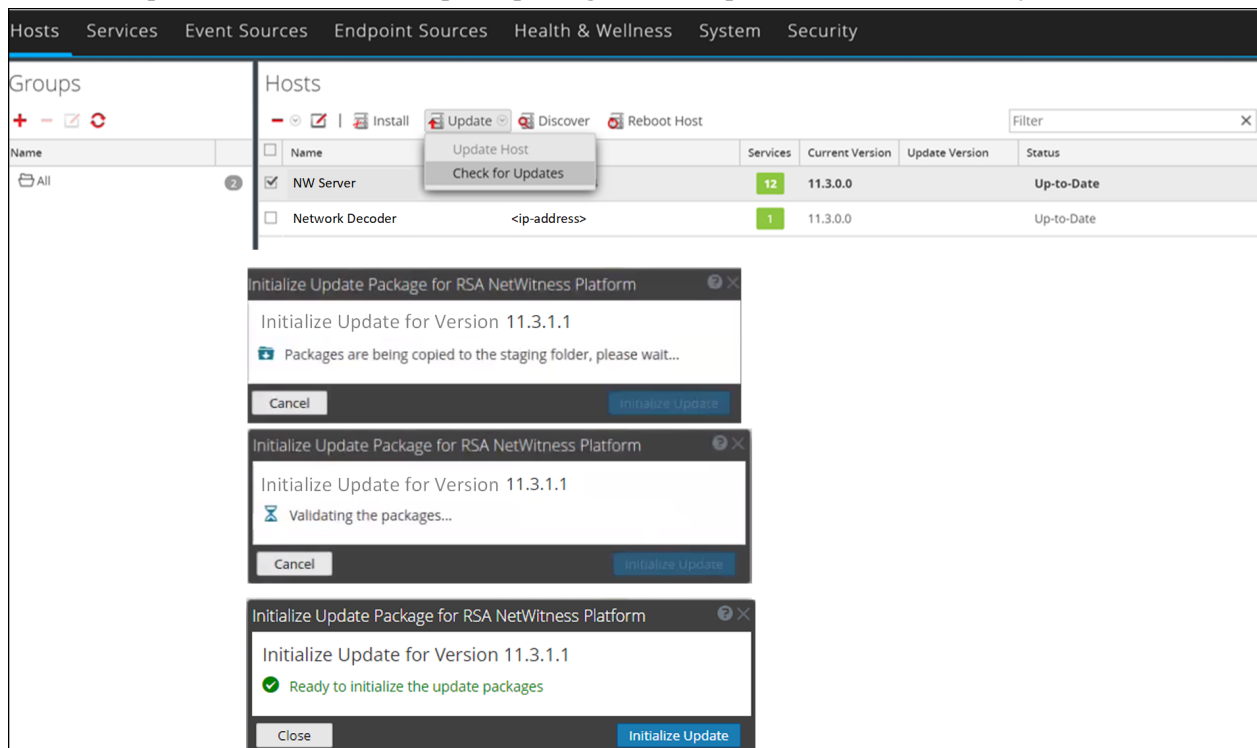
```
sudo cp /tmp/netwitness-11.3.1.1.zip /var/lib/netwitness/common/update-stage/
```

**Note:** NetWitness Platform unzips the file automatically.

## Task 2. Apply Updates from the Staging Area to Each Host

**Caution:** You must update the NW Server host before updating any Non-NW Server host.

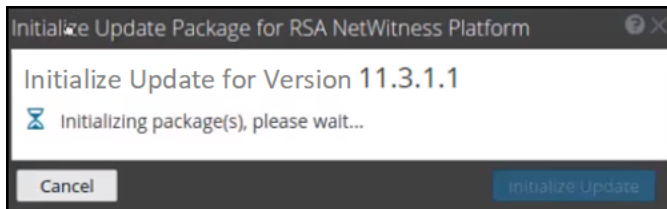
- Log in to NetWitness Platform.
- Go to **ADMIN > HOSTS**.
- Check for updates and wait for the update packages to be copied, validated, and ready to be initialized.



"Ready to initialize packages" is displayed if:

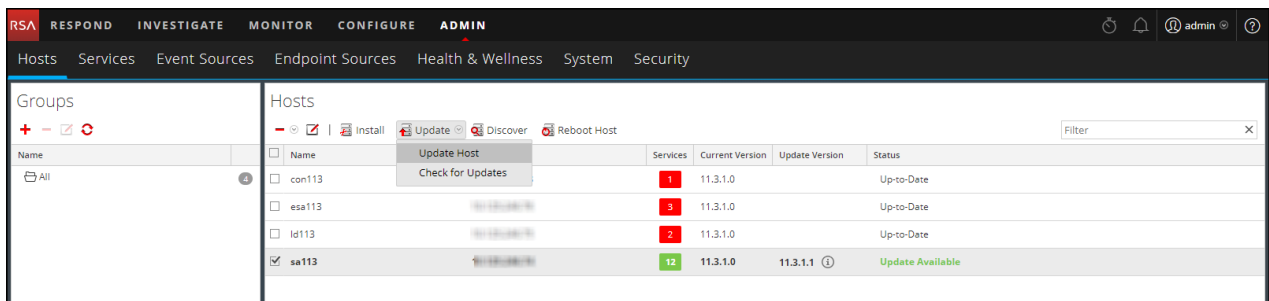
- NetWitness Platform can access the update package.
- The package is complete and has no errors.

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)," displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.

4. Click **Initialize Update**.

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 update of the host.

5. Click **Update > Update Hosts** from the toolbar.6. Click **Begin Update** from the **Update Available** dialog.

After the host is updated, it prompts you to reboot the host.

7. Click **Reboot** from the toolbar.



# Post Upgrade Tasks

---

After you have upgraded to 11.3.1.1, you can take advantage of the new features described in [Enabling New Features](#). This topic is divided into two sections, based on the version that you are upgrading from:

- [Post Upgrade Tasks for Customers Upgrading From 11.3.x.x](#)
- [Post Upgrade Tasks for Customers Upgrading From 11.1.x.x or 11.2.x.x](#)

## Post Upgrade Tasks for Customers Upgrading From 11.3.x.x

---

Perform all the tasks in this section if you are upgrading from 11.3.x.x to 11.3.1.1.

- [General](#)
- [Event Stream Analysis](#)
- [Respond](#)

### General

These tasks apply to all NetWitness Platform 11.3.1.1 customers.

**Note:** If you are trying to add an additional component host during the upgrade process, you might see this error "Failure: repodata/repomd.xml from bootstrap-rsa-11-3-0-2: [Errno 256] No more mirrors to try" or "Failed to get services for this appliance" during RSA NetWitness Platform Enablement . Refer to this KB article for more information: <https://community.rsa.com/docs/DOC-107255>.

### Task 1. Start Data Capture and Aggregation

After upgrading to 11.3.1.1, you must restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

#### Start Network Capture

1. In the **NetWitness Platform** menu, select **ADMIN > Services**.  
The Services view is displayed.

2. Select each **Decoder** service.

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

4. In the toolbar, click  .

#### Start Log Capture

1. In the **NetWitness Platform** menu, select **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 Aggregation

1. In the **NetWitness Platform** menu, select **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  .

**Note:** When you are upgrade from 11.3.0.0, 11.3.0.1, 11.3.1.0, or 11.3.0.2 to 11.3.1.1, make sure the Hive version is compatible with Warehouse. For more information, see [Task 4. Upgrade Hive Version](#)

## Event Stream Analysis

### Task 2 - (Conditional) Update Memory Required for Virtual ESA Host only

You must update the **Xmx** memory setting from **164G** to eighty percent of the total host memory to prevent the Correlation Server failing to start and re-spawning. For example, if

- 180 Gigabytes is eighty percent of your memory, specify `-Xmx180G`.
  - 500 Megabytes is eighty percent of your memory, specify `-Xmx500M`.
1. SSH to the ESA host and log in with your ESA host credentials.
  2. Open the **correlation-server.conf** file in edit mode.
 

```
vi /etc/netwitness/correlation-server/correlation-server.conf
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx164G -
javaagent:/var/lib/netwitness/esper-enterprise/esper-7.1.0.jar"
```
  3. Modify the Xmx parameter.
 



```
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -<eighty-
percent-of-total-memory> -javaagent:/var/lib/netwitness/esper-
enterprise/esper-7.1.0.jar"
```
  4. Save and exit the **correlation-server.conf** file.
  5. Restart the Correlation service.
 

```
systemctl restart rsa-nw-correlation-server
```

### Task 3. Verify the ESA Rule Deployments

Check the status of the ESA rule deployments. For each deployment, do the following:

1. Go to **CONFIGURE > ESA Rules > Rules** tab. In the Options panel on the left, select an ESA rule deployment.
2. Make sure that the ESA Correlation service has a status of “Deployed”.
3. Make sure that the Data Source status shows a green circle.
4. Make sure that the status of the ESA Rules shows “Deployed”.

If the ESA rule status shows “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 tool tip without going to the error log. (The ESA Correlation Service log files are located at `/var/log/netwitness/correlation-server/correlation-server.log`)

See the [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.




## Task 4 - (Conditional) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules

**Note:** This task is only for upgrades from 11.3.0.0, 11.3.0.1 and 11.3.1.

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 11.3.1.1, 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 5 - \(Conditional\) 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 5 - (Conditional) Adjust Custom ESA Rule Builder and ESA Advanced Rules

**Note:** This task is only for upgrades from 11.3.0.0, 11.3.0.1 and 11.3.1.

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](#).

## Respond

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

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. Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts

Respond service normalization scripts are in the `/var/lib/netwitness/respond-server/scripts` directory in 11.3.1.1. You must replace the old versions.

Before the update to 11.3.1.1, you backed up the following files from the `/var/lib/netwitness/respond-server/scripts` directory.

```
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 only)
normalize_wtd_alerts.js
utils.js
```

Complete the following procedure to get the latest version of the normalization scripts.

1. After backing up the files listed above, delete the `/var/lib/netwitness/respond-server/scripts` directory and its contents.
2. Restart the Respond server.  

```
systemctl restart rsa-nw-respond-server
```
3. (Conditional ) Edit the new files to include any customizations from the 11.x scripts that were backed up.

**Note:** The following files changed with the 11.3.0.0 release:

```
normalize_alerts.js
aggregation_rule_schema.json
```

## Task 8. Update Default Incident Rule Group By Value

The **High Risk Alerts: NetWitness Endpoint** default incident rule now uses Host Name as the Group By value. If you have NetWitness Endpoint, you can use this rule. Change the Group By value of the default NetWitness Endpoint rule to "Host Name."

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules** and click on the rule that you want to update in the **Name** column. The **Incident Rule Details** view is displayed.
2. In the **GROUP BY** field, select the new Group By value from the drop-down list.
3. Click **Save** to update the rule.

To aggregate NetWitness Endpoint alerts based on the File Hash, complete the following steps to clone the default NetWitness Endpoint incident rule and change the Group By value.

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules**. The **Incident Rules List** view is displayed.
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**. You will receive a message that you successfully cloned the selected rule.
3. Change the Name of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint File hash.
4. In the **GROUP BY** field, remove the previous Group By value and add **File MD5 Hash**. It is important that File MD5 Hash is the only Group By value listed.
5. Click **Save** to create the rule.

For detailed information, see the *Respond Configuration Guide for NetWitness Platform 11.3*.

## Task 9. (Conditional) Add Respond Notification Settings Permissions

**Note:** If you already configured these permissions in 11.1 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. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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*.

## Post Upgrade Tasks for Customers Upgrading From 11.1.x.x or 11.2.x.x

---

Perform all the tasks in this section if you are upgrading from 11.1.x.x or 11.2.x.x to 11.3.1.1.

- [General](#)
- [Event Stream Analysis](#)
- [Respond](#)
- [Decoder and Log Decoder](#)
- [NetWitness UEBA](#)

### General

**Note:** If you are trying to add an additional component host during the upgrade process, you might see this error "Failure: repodata/repomd.xml from bootstrap-rsa-11-3-0-2: [Errno 256] No more mirrors to try" or "Failed to get services for this appliance" during RSA NetWitness Platform Enablement . Refer to the KB article for more information: <https://community.rsa.com/docs/DOC-107255>.

### Task 1. Start Data Capture and Aggregation


After upgrading to 11.3.1.1, you must restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

#### Start Network Capture


1. In the **NetWitness Platform** menu, select **ADMIN > Services**.  
The Services view is displayed.
2. Select each **Decoder** service.



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


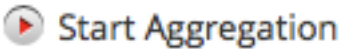
4. In the toolbar, click  .

### Start Log Capture

1. In the **NetWitness Platform** menu, select **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 Aggregation

1. In the **NetWitness Platform** menu, select **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  .

## 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, select **ADMIN > Security > Roles**.

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



(Edit).

The screenshot displays the RSA NetWitness Platform Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, a sub-navigation bar shows various system components like Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The main content area is titled 'Roles' and contains a table of user roles. The 'Data\_Privacy\_Officers' role is selected and highlighted with a red box. The table has columns for Name, Description, and Permissions. The 'Data\_Privacy\_Officers' role has the description 'The persona of Data Privacy ...' and permissions including 'View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.\*, Define Rule, Dashle...'. The bottom of the screen shows the RSA NetWitness Platform logo and version 11.x.0.0.

Name	Description	Permissions
Administrators	The System Administrators per...	*
Respond_Administrator	The persona of Respond Admi...	Dashlet Access - Unified RSA First Watch Dashlet, correlation-server.engine.manage, integration-server.notification...
<input checked="" type="checkbox"/> Data_Privacy_Officers	The persona of Data Privacy ...	View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.*, Define Rule, Dashle...
SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export List, con...
Operators	The System Operators Persona...	Dashlet Access - Unified RSA First Watch Dashlet, correlation-server.engine.manage, integration-server.notification...
Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, View and Manage Incidents, contexthub-server.list...
Analysts	The SOC Analysts persona is ce...	View and Manage Incidents, Export List, contexthub-server.listentries.manage, Define Rule, endpoint-server.agent...
UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

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

**Edit Role**

**Attributes**

Core Query Timeout: 5

Core Session Threshold: 100000

Core Query Prefix:

**Permissions**

< \* Admin-server **Administration** Alerting Config-server Content-serv >

Assigned	Description ^
<input checked="" type="checkbox"/>	Manage Logs
<input type="checkbox"/>	Manage Notifications
<input checked="" type="checkbox"/>	Manage Plugins
<input type="checkbox"/>	Manage Predicates
<input type="checkbox"/>	Manage Reconstruction
<input checked="" type="checkbox"/>	Manage Security
<input checked="" type="checkbox"/>	Manage Services
<input checked="" type="checkbox"/>	Manage System Settings
<input type="checkbox"/>	Modify ESA Settings
<input type="checkbox"/>	Modify Event Sources
<input type="checkbox"/>	Modify Hosts

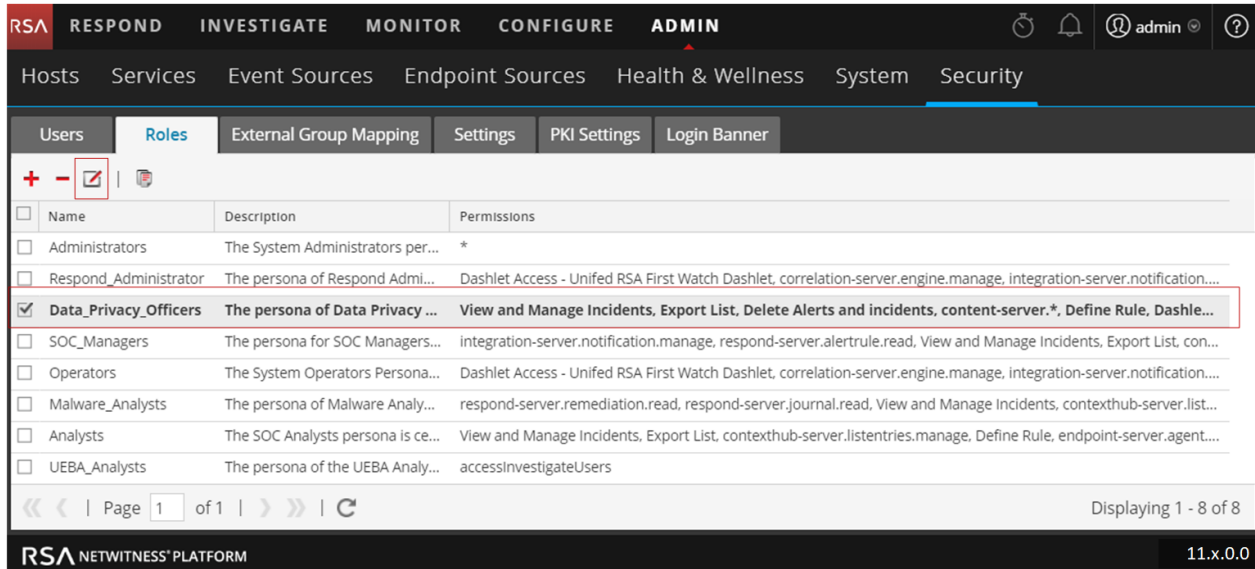
4. Complete steps 1 through 3 for the **Analysts** and **SOC Managers** roles in addition to **Data Privacy Officers**.

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

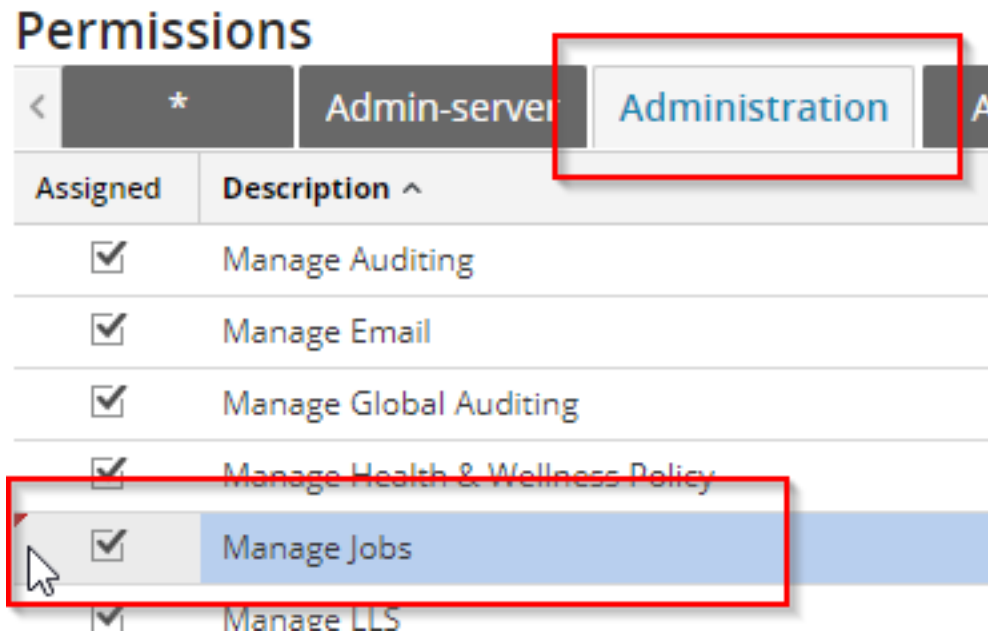
Add the 'Manage Jobs' Administration permission to the following roles:

- SOC\_Managers
- Operators
- Data\_Privacy\_Officers

1. In the **NetWitness Platform** menu, select **ADMIN > Security** and click **Roles**.
2. Select the role you need to upgrade (that is, **SOC\_Managers**, **Operators**, or **Data\_Privacy\_Officers**) and click .



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



4. Complete steps 1 through 3 inclusive for all three roles (**SOC\_Managers**, **Operators**, and **Data\_Privacy\_Officers**).

## Task 4. Upgrade Hive Version

If you are upgrading from 11.1.x.x, 11.2.1.0, or 11.2.1.1 to 11.3.1.1, you must install the Hive version that is compatible with Warehouse. To install the latest Hive version, run the following commands on the NW Server host and restart the Reporting Engine service.

1. To install Hive version 0.12, run the following command:

```
rpm -ivh rsa-nw-hive-jdbc-0.12.0-1.x86_64.rpm
```

2. To Install Hive version 1.0, run the following command:

```
rpm -ivh rsa-nw-hive-jdbc-1.0.0-1.x86_64
```

## Task 5. (Conditional) Reissue Certificates for Your Hosts

In 11.3.0.0, RSA introduced a `cert-reissue` command line command and its arguments to reissue host certificates. After you upgrade all your hosts to 11.3.1.1, you should reissue certificates for all of them as soon as possible to avoid having them expire. If the certificates expire, this places your NetWitness deployment in a bad security state. Refer to the *RSA NetWitness® Platform Security Configuration Guide* for instructions on how to use the `cert-reissue` command.


**Note:** Regardless of the version that you are upgrading from, RSA recommends that you rerun the `cert-reissue` process every two years to prevent the certificates from expiring.

## Task 6. Modify the Analyst Role `investigate-server` Permissions

The default permissions for the **SOC Managers**, **Malware Analysts**, and **Analysts** roles are fixed in 11.3 so that these roles have specific permissions required to view and work in 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, you must upgrade the default permissions to match the 11.3.x.x 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. Check the user role checkbox (for example, **Analysts**) and click  (Edit icon).

- b. Under **Permissions**, click the **Investigate-server** tab.
- c. Make sure that the following permissions are not checked.
  - `investigate-server.*`
  - `investigate-server.predicate.manage`
- d. Check the following permissions.
  - `investigate-server.content.export`
  - `investigate-server.content.reconstruct`
  - `investigate-server.event.read`
  - `investigate-server.metagroup.read`
  - `investigate-server.predicate.read`
- e. Click **Save**.

## Task 7. (Conditional) Reconfigure PAM RADIUS Authentication

If you configured PAM RADIUS authentication in 11.x.x.x using the `pam_radius` package, you must reconfigure it in 11.3.1.1 using the `pam_radius_auth` package.

You must run the following commands on the NW Server host.

**Note:** If you have configured `pam_radius` in 11.x.x.x, perform the below steps to uninstall the existing version, or 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 the write permission to `/etc/raddb/server` files using 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 8. (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 11.3.1.1, 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 *RSA NetWitness Platform Licensing Management Guide for Version 11.3* for instructions. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## Event Stream Analysis

### Task 9 - (Conditional) Update Memory Required for Virtual ESA Host only

You must update the **Xmx** memory setting from **164G** to eighty percent of the total host memory to prevent the Correlation Server failing to start and re-spawning. For example, if

- 180 Gigabytes is eighty percent of your memory, specify `-Xmx180G`.
- 500 Megabytes is eighty percent of your memory, specify `-Xmx500M`.

1. SSH to the ESA host and log in with your ESA host credentials.

2. Open the **correlation-server.conf** file in edit mode.

```
vi /etc/netwitness/correlation-server/correlation-server.conf
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx164G -
javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-7.1.0.jar"
```

3. Modify the Xmx parameter.



```
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -<eighty-
percent-of-total-memory> -javaagent:/var/lib/netwitness/esper-
enterprise/esperee-utilagent-7.1.0.jar"
```

4. Save and exit the **correlation-server.conf** file.

5. Restart the Correlation service.

```
systemctl restart rsa-nw-correlation-server
```

## Task 10 - Verify the String Array Type Meta Keys on the ESA Correlation Service and Next Steps

1. Verify that your existing string array meta keys migrated to 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**.
  - c. Verify that the previously recorded **ArrayFieldNames** values are the same as in the **multi-valued** parameter. The **multi-valued** parameter shows the string array meta keys currently used for your ESA rules.
2. Your ESA rules continue to work, but if you are using Live, UEBA, or Endpoint rules, follow the [Task 13 - \(Conditional\) Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules](#) procedure.

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 11.3.1.1, 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 11.3.1.1 from versions prior to 11.3.1.1, 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.



To use the latest Endpoint, UEBA, and Live content rules, you must update the **multi-valued** parameter 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. To do this, follow the [Task 13 - \(Conditional\) 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 11 (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 11.3.1.1.

Rule #	Rule Name	Array Type Meta Keys in 11.3.x
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 11.3.1.1:
    - 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 11.3.1.1, 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 12 Verify the ESA Rule Deployments

After you upgrade to 11.3.1.1, 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 the ESA rule status shows “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*.

### Task 13 - (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 11.3.1.1 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 14 - \(Conditional\) 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 14 - (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:

```
@RSAAAlert
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:

```
@RSAAAlert
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

**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 11.3.1.1, 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 11.3.1.1 and 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 11.3.1.1 and 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 11.3.1.1:

```
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 11.3.1.1:

```
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*.

**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*.

## 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 13 - \(Conditional\) 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
```

## Respond

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

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. Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts

Respond service normalization scripts are in the `/var/lib/netwitness/respond-server/scripts` directory in 11.3.1.1. You must replace the old versions.

Before the upgrade to 11.3.1.1, you backed up the following files from the `/var/lib/netwitness/respond-server/scripts` directory.

```
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 only)
normalize_wtd_alerts.js
utils.js
```

Complete the following procedure to get the latest version of the normalization scripts.

1. After backing up the files listed above, delete the `/var/lib/netwitness/respond-server/scripts` directory and its contents.
2. Restart the Respond server.  

```
systemctl restart rsa-nw-respond-server
```
3. (Conditional ) Edit the new files to include any customizations from the 11.x scripts that were backed up.

**Note:** The following files changed with the 11.3.0.0 release:

```
normalize_alerts.js
aggregation_rule_schema.json
```

## Task 17. upgrade Default Incident Rule Group By Value

The **High Risk Alerts: NetWitness Endpoint** default incident rule now uses Host Name as the Group By value. If you have NetWitness Endpoint, you can use this rule. Change the Group By value of the default NetWitness Endpoint rule to "Host Name."

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules** and click on the rule that you want to upgrade in the **Name** column. The **Incident Rule Details** view is displayed.
2. In the **GROUP BY** field, select the new Group By value from the drop-down list.
3. Click **Save** to upgrade the rule.

To aggregate NetWitness Endpoint alerts based on the File Hash, complete the following steps to clone the default NetWitness Endpoint incident rule and change the Group By value.

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules**. The **Incident Rules List** view is displayed.
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**. You will receive a message that you successfully cloned the selected rule.

3. Change the Name of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint File hash.
4. In the **GROUP BY** field, remove the previous Group By value and add **File MD5 Hash**. It is important that File MD5 Hash is the only Group By value listed.
5. Click **Save** to create the rule.

For detailed information, see the *Respond Configuration Guide for NetWitness Platform 11.3*.

## Task 18. (Conditional) Add Respond Notification Settings Permissions

**Note:** If you already configured these permissions in 11.1 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 upgraded.

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 NetWitness Platform Logs & Network 11.x documents.

## Decoder and Log Decoder

### Task 19. (Conditional - for 11.1.x.x upgrade paths, Not in 11.2.x.x or later) Enable Metadata for GeoIP2 Parser

By default, the GeoIP2 parser generates less metadata than the GeoIP parser did. After upgrading to 11.3.1.1, if you require any of the additional metadata, you must enable them (once only) for each Decoder. This can also be altered post-upgrade. Keep in mind that the `isp` and `org` meta fields usually produce an equivalent value to `domain`.

To enable metadata:

1. Go to **ADMIN > Services**.
2. In the **Administration services** view, select a Log Decoder service or a Decoder service.
3. Click the settings icon () and select **View > Config**. The Parsers Configuration panel is displayed, from which you can select **GeoIP2** to enable the desired metadata.

For more information about GeoIP2 parsers, see the "GeoIP2 and GeoIP Parsers" topic in the *Decoder and Log Decoder Configuration Guide*.



## NetWitness Endpoint

### Task 20. 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.

1. 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 NetWitness Platform Logs & Network 11.x documents.

## NetWitness UEBA

### Task 21. (Conditional) Enable Endpoint Data Sources

If NetWitness Endpoint Server is configured in NetWitness Platform 11.3.1.1, you can enable the Endpoint data sources such as Process and Registry to generate alerts in UEBA.

To enable Endpoint data sources:

```
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"}]}'
```

### Task 22. Enable UEBA Indicator Forwarder

If the NetWitness Respond server is configured in NetWitness Platform 11.3.1.1, 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:

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

## Task 23. Upgrade Broker or Concentrator UUID

In UEBA, after you upgrade to NetWitness Platform 11.3.1.1, the Broker or Concentrator UUID changes . You must upgrade the NetWitness Platform core services, and upgrade the Broker or Concentrator UUID in UEBA.

To upgrade the Broker or Concentrator UUID, on the UEBA host:

```
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
```

## Task 24. Upgrade Airflow Configuration

After you upgrade to NetWitness Platform 11.3.1.1, you must upgrade Airflow configurations. Perform the following:

1. To access Airflow, go to `https://<UEBA_host>/admin/`, and then enter user name and password.

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

You may see some tasks in red in the full flow DAG due to mismatching tasks between NetWitness Platform 11.2 and the NetWitness Platform 11.3.1.1.

2. Click (Trigger Dag) on `presidio_upgrade_dag_from_11.2.0.0_to_11.3.0.1` DAG .

This pauses the full flow DAG and runs `reset_presidio` DAG to:

- Create a new full flow DAG where the start date is 27 days ago.
- Remove the old full flow DAG.
- Start the new full flow DAG.

3. Once the upgrade DAG is successful, the `presidio_upgrade` DAG task is marked in green with one task in the **Recent Tasks** Column as shown below.

## Task 25. Restart Airflow Scheduler Service

You must restart the Airflow scheduler service after the `presidio_upgrade` DAG operation is successful.

**Note:** A `presidio_upgrade` DAG with a **dark green circle** in the **resent tasks** column indicates that `presidio_upgrade` DAG is successful.

To restart the airflow scheduler service, run:

```
systemctl restart airflow-scheduler
```

## Enabling New Features

---

This section describes how to enable new features in 11.3.1. For a complete list of new features in this release, see the *Release Notes for RSA NetWitness Platform 11.3.1.1*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

### New Support for Relay Server in NetWitness Endpoint

After you have upgraded to 11.3.1.1, the Relay Server (referred to as RAR in RSA NetWitness Endpoint) is now available, and extends NetWitness Platform's visibility into endpoints outside the corporate network. For more information, see the "NetWitness Endpoint" topic of the "What's New" section in the *Release Notes for RSA NetWitness Platform 11.3.1.1*, and the *NetWitness Endpoint Configuration Guide for RSA NetWitness Platform*.

### Expanded Detection of Encrypted Channels

To help you identify encrypted channels, the Network Decoder can produce the JA3 value of TLS clients and the JA3S value of TLS servers that are observed in a Network session. The values that are produced conform to the values generated by the open source JA3 tools (<https://github.com/salesforce/ja3>). For information about how to set this up, see "JA3 and JA3S TLS Fingerprints" in the *Decoder and Log Decoder Configuration Guide for RSA NetWitness Platform*.

### Data Retention for Risk Scores

In NetWitness Endpoint, analysts can retain risk score data for a specified amount of time before it is deleted. Data retention for risk scores is enabled by default, with the retention period configured for 30 days, to free up the disk space periodically. However, the amount of time risk score data is retained is configurable. For information about how to configure data retention, see the *NetWitness Respond Configuration Guide for RSA NetWitness Platform*.

### Configurable Event Analysis View Event Limit

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

## **Configurable Clearing of the Reconstruction Cache the Event Analysis View to Save Disk Space**

Any Event Analysis view reconstruction cache older than 24 hours is automatically cleared every 24 hours at 3 A.M. to avoid filling up disk space and to clear data from the Investigate user interface. The administrator can change the interval to an interval greater than 24 hours. For additional information, see "Configure the Reconstruction Cache Clearing Interval for the Event Analysis View" in the *System Configuration Guide for RSA NetWitness Platform*.

# Product Documentation

---

The following documentation is provided with this release.

Document	Location
RSA NetWitness® Platform 11.3 Online Documentation	<a href="https://community.rsa.com/community/products/netwitness/documentation">https://community.rsa.com/community/products/netwitness/documentation</a>
RSA NetWitness® Hardware Setup Guides	<a href="https://community.rsa.com/community/products/netwitness/hardware-setup-guides">https://community.rsa.com/community/products/netwitness/hardware-setup-guides</a>
RSA Content for RSA NetWitness® Platform	<a href="https://community.rsa.com/community/products/netwitness/rsa-content">https://community.rsa.com/community/products/netwitness/rsa-content</a>

## Feedback on Product Documentation

You can send an email to [sahelpfeedback@emc.com](mailto:sahelpfeedback@emc.com) to provide feedback on RSA NetWitness® Platform documentation.

## Appendix A. Offline Method (No connectivity to Live Services). Upgrade Using the 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 11.1.x.x, 11.2.x.x, 11.3.0.0, 11.3.0.1, 11.3.1.0 or 11.3.0.2 release, download `netwitness-11.3.1.1.zip`.

### Procedure

You need to 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. **If you are upgrading from 11.1.x.x, 11.2.x.x, 11.3.0.0, 11.3.0.1, 11.3.1.0 or 11.3.0.2 to 11.3.1.1**, you must stage 11.3.1.1. Log into the `/root` directory of the NW Server and create the following directories:  
`/tmp/upgrade/11.3.1.1`  
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-11.3.1.1.zip -d /tmp/upgrade/11.3.1.1`

**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.

3. Initialize the upgrade, using the following command:  
`upgrade-cli-client --init --version 11.3.1.1 --stage-dir /tmp/upgrade`
4. Upgrade the NW Server host, using the following command:  
`upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.3.1.1`
5. When the component host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
6. 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 upgrading a host to a new version, contact Customer Support ([Contacting Customer Care](#)).

## External Repo Instructions for CLI Upgrade

**Note:** The external repo should have separate directories for 11.3.0.0 and 11.3.1.1, as described in [Appendix A. Offline Method \(No connectivity to Live Services\). Upgrade Using the Command Line Interface](#).

1. Stage 11.3.1.1 by creating a directory on the NW Server host at `/tmp/upgrade/11.3.1.1` and extract the zip package.

```
unzip netwitness-11.3.1.1.zip -d /tmp/upgrade/11.3.1.1
```

**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 11.3.1.1 --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
11.3.1.1
```

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 upgrading a host to a new version, contact Customer Support ([Contacting Customer Care](#)).