RSA NETWITNESS® PLATFORM

Upgrade Guide

for RSA NetWitness Platform 11.3.2.0

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

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.

December 2019

Contents

Upgrade Overview

This document provides instructions to upgrade RSA NetWitness® Platform to the latest service pack. Read this document before deploying or updating to NetWitness Platform 11.3.2.0. 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 NetWitness Platform 11.3.2.0:

Note: If your current hosts are on 10.6.x.x or 11.0.x.x, you must first upgrade to 11.3.0.2, and then upgrade to 11.3.2.0. For information about upgrading to 11.3.0.2, see the "Installation & Upgrade Guides" section on the NetWitness Platform documentation page 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.

- NetWitness Platform 11.1.0.0 to 11.3.2.0
- NetWitness Platform 11.1.0.1 to 11.3.2.0
- NetWitness Platform 11.1.0.2 to 11.3.2.0
- NetWitness Platform 11.1.0.3 to 11.3.2.0
- NetWitness Platform 11.2.0.0 to 11.3.2.0
- NetWitness Platform 11.2.0.1 to 11.3.2.0
- NetWitness Platform 11.2.1.0 to 11.3.2.0
- NetWitness Platform 11.2.1.1 to 11.3.2.0
- NetWitness Platform 11.2.1.2 to 11.3.2.0
- NetWitness Platform 11.3.0.0 to 11.3.2.0
- NetWitness Platform 11.3.0.1 to 11.3.2.0
- NetWitness Platform 11.3.0.2 to 11.3.2.0
- NetWitness Platform 11.3.1.0 to 11.3.2.0
- NetWitness Platform 11.3.1.1 to 11.3.2.0

For more information about this release, see the *Release Notes for RSA NetWitness Platform 11.3.2* 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 11.3.2.0 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 service pack.
- If the NW Server host does not have internet connectivity to Live Services, the Command Line Interface (CLI) can be used to apply the service pack.

Feedback on Product Documentation

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

Upgrade Considerations for ESA Rule Deployments

This section applies to upgrades from 11.2.x.x or earlier directly to 11.3.2.0.

Caution: In NetWitness Platform 11.3.0.2 and later, the ESA Correlation service contains data source changes that require changes to migrated ESA rule deployments. The 11.3.0.2 ESA Correlation service replaces the Event Stream Analysis service in earlier versions.

After you upgrade to 11.3.2.0, migrated ESA rule deployments have the following changes.

1. If an ESA rule deployment contains two services before you upgrade to 11.3.2.0, the deployment splits into two deployments. You can only have one ESA Correlation service in an ESA rule deployment in version 11.3.2.0.
2. If an ESA service has multiple ESA rule deployments before you upgrade to 11.3.2.0, they are combined into one deployment in version 11.3.2.0.

You can still access your old deployments. For a detailed example, see the *ESA Configuration Guide for RSA NetWitness Platform 11.3*.

Pre-Upgrade Tasks

Task 1. (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 11.3.2.0 so you can restore your customizations in 11.3.2.0 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 11.3.2.0.

Task 2. 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 (ESA Correlation service Explore view (correlation > stream > multi-valued).

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 11.3.2.0:

- Task 1. (Conditional - Offline Methods Only) Download the 11.3.2.0 Service Pack
- Task 2. (Conditional - CLI Offline Method Only) Upgrade the 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 Methods (No Connectivity to Live Services)

Task 1. (Conditional - Offline Methods Only) Download the 11.3.2.0 Service Pack

If you are upgrading from 11.1.x.x, 11.2.x.x or 11.3.x.x to 11.3.2.0, you must download the following file from RSA Link (https://community.rsa.com/) > Downloads > NetWitness Platform > Version 11.3:
`netwitness-11.3.2.0.zip`

For more information, see Offline Methods (No Connectivity to Live Services).

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

Note: Perform this step only if you are using an external repository for 11.3.2.0.

Upgrade the external repository with the latest upgrade content for NetWitness Platform 11.3.2.0 by downloading the following file, if you are upgrading from 11.1.x.x, 11.2.x.x or 11.3.x.x to 11.3.2.0:
`netwitness-11.3.2.0.zip`

For more information, see Appendix A. Offline Method (No Connectivity to Live Services) - 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 Methods (No Connectivity to Live Services) .

Prerequisites

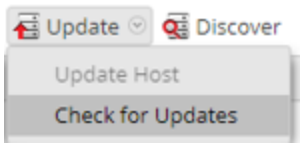
Make sure that:

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. 11.3.2.0 is available in the **Update Version** column.

Note: If you have custom certs, move them from the `/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 **11.3.2.0** 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.

Offline Methods (No Connectivity to Live Services)

If your version of NetWitness Platform has no connection to the Internet and you want to upgrade to 11.3.2.0:

- **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 11.3.2.0. 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) - 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 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 toAppendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface for instructions.

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

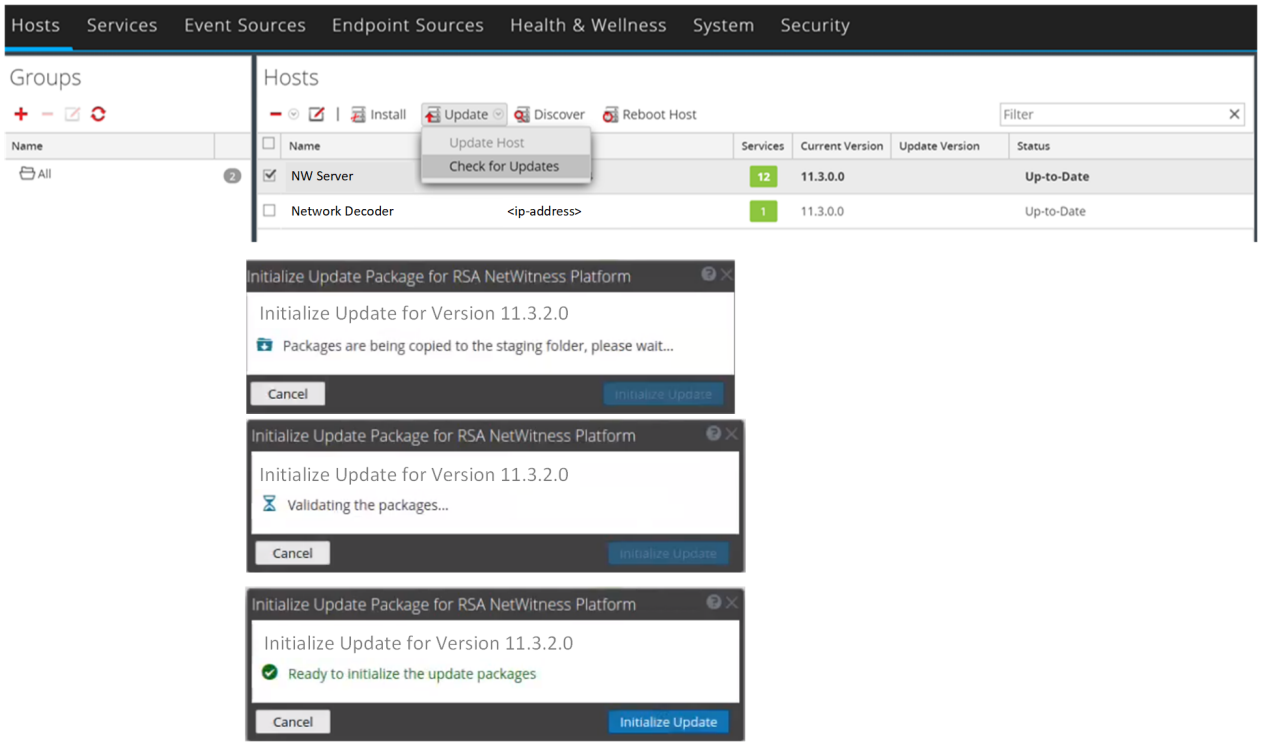
1. Download the `netwitness-11.3.2.0.zip` update package from RSA Link to a local directory.
2. SSH to the NW Server host.
3. Copy `netwitness-11.3.2.0.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder. For example:
   `sudo cp /tmp/netwitness-11.3.2.0.zip /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.

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

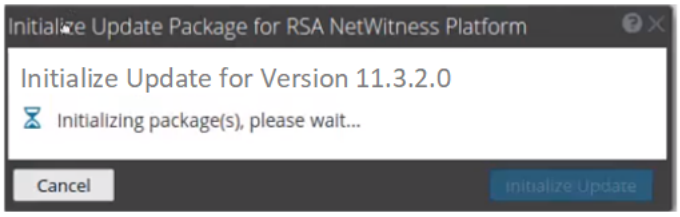


"Ready to initialize packages" is displayed if:

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

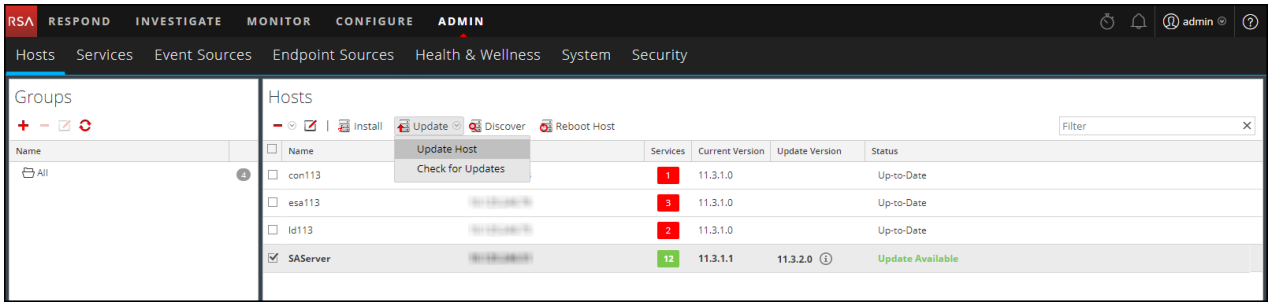
4. Click **Initialize Update**.



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

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 11.3.2.0.

- General
- Event Stream Analysis
- Respond

General

These tasks apply to all NetWitness Platform 11.3.2.0 customers.

Task 1. Start Data Capture and Aggregation

After upgrading to 11.3.2.0, 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 

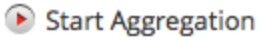
.

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 11.3.0.2 or 11.3.1.1 to 11.3.2.0, make sure the Hive version is compatible with Warehouse. For more information, see Task 4. Upgrade Hive Version

Event Stream Analysis

Task 2. 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 3. (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 11.3.0.2 and 11.3.1.1.

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 11.3.2.0, 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: This task is only for upgrades from 11.3.0.2 and 11.3.1.1.

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 5. (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 6. 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 11.3.2.0. You must replace the old versions.

Before the update to 11.3.2.0, 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 7. 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 8. (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** > **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. 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 11.3.2.0.

General

Task 1. Start Data Capture and Aggregation

After upgrading to 11.3.2.0, you must restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Start Network Capture

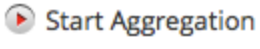
1. In the **NetWitness Platform** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. Select each **Decoder** service.

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

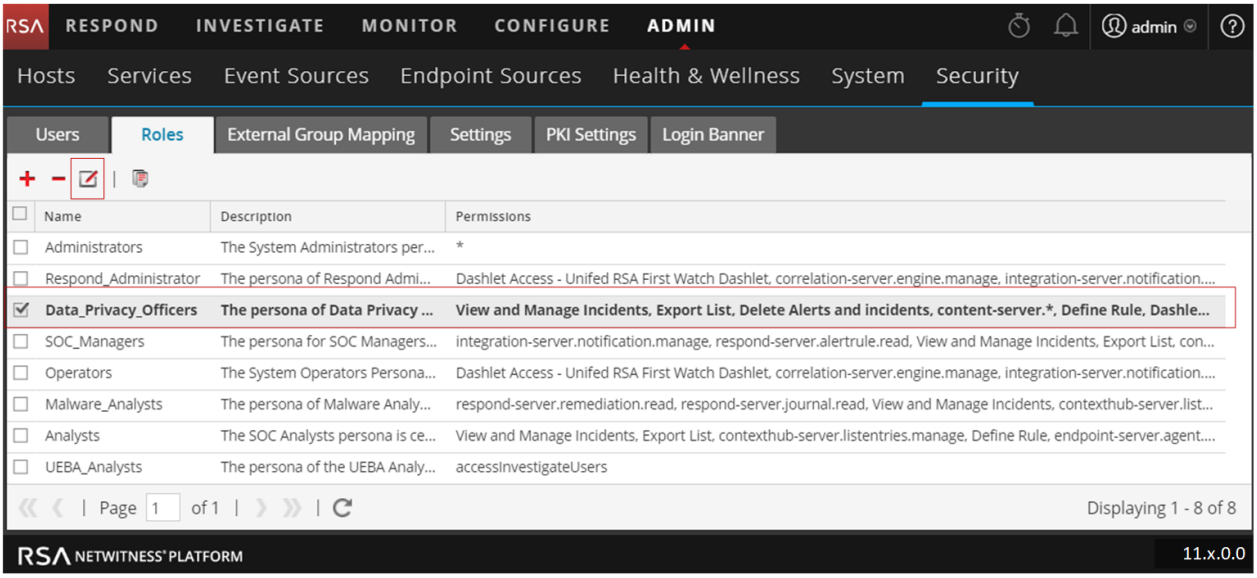
1. In the **NetWitness Platform** menu, select **ADMIN** > **Services**.
   The Services view is displayed.
2. For each Concentrator, Broker, and Archiver service:
   a. Select the service.
   b. Under  (actions), select **View** > **Config**.
   c. In the toolbar, click  .

Task 2. Set Up Context Menu Actions User Permissions

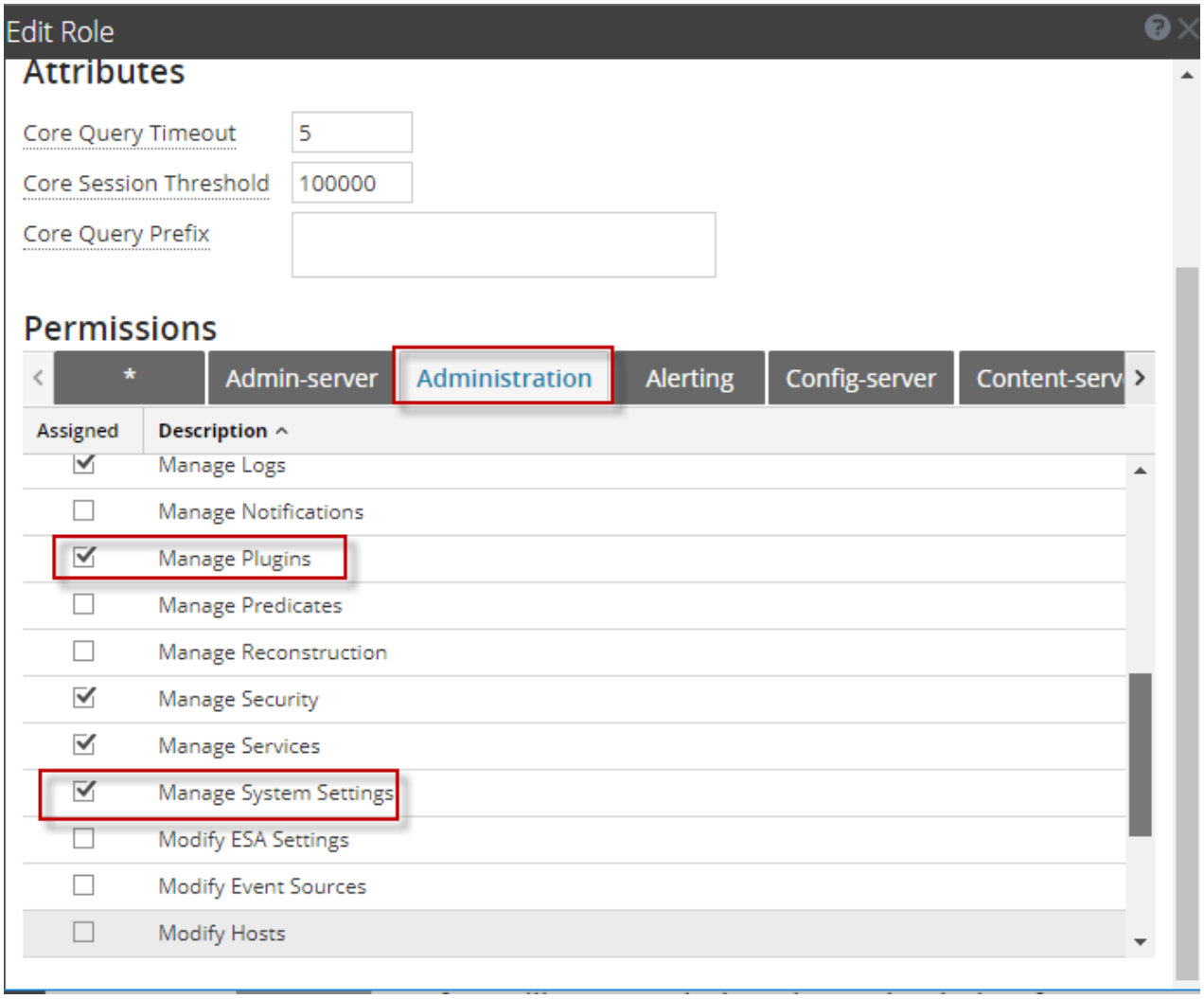
Complete the following steps for **Analysts**, **SOC Managers**, **Data Privacy Officers** roles to set up their Context Menu Actions. You must complete these steps for the **Analysts**, **SOC Managers**, and **Data Privacy Officers** roles.

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).



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



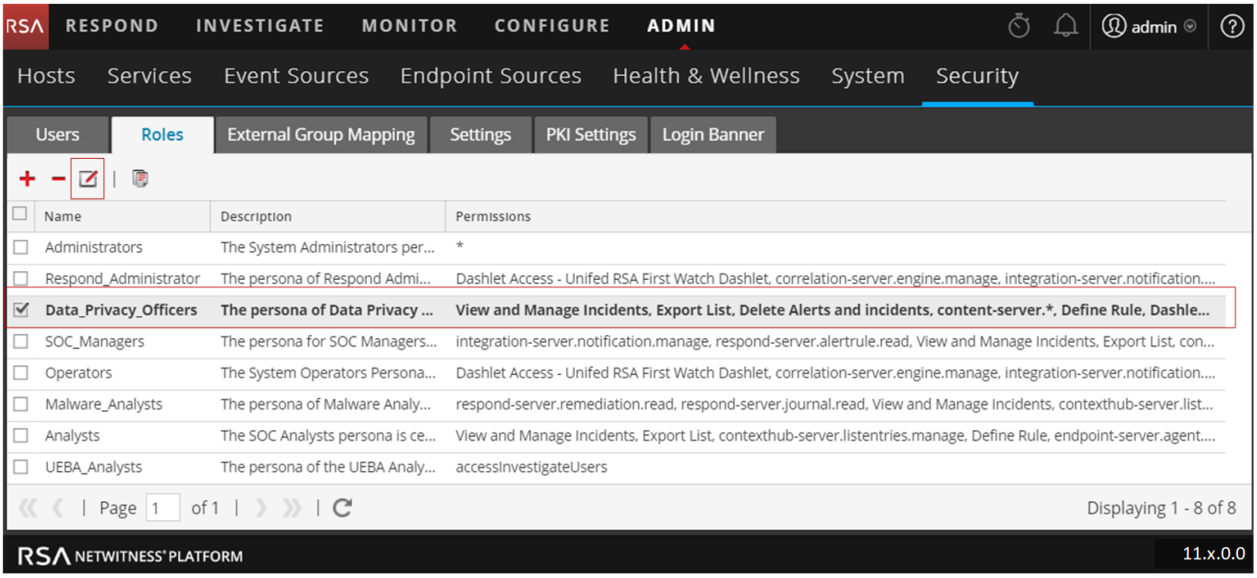
4. Complete steps 1 through 3 for the **Analysts** and **SOC Managers** roles in addition to **Data Privacy Officers**.

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

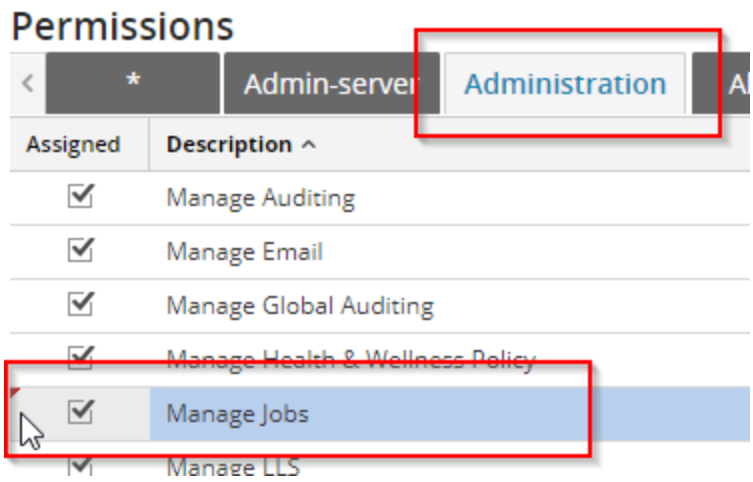
Add the 'Manage Jobs' Administration permission to the following roles:

- 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

Note: If you already configured these permissions in 11.2.1 or later, you can skip this task.

When you upgrade to 11.3.2.0, 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 11.3.2.0, 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.

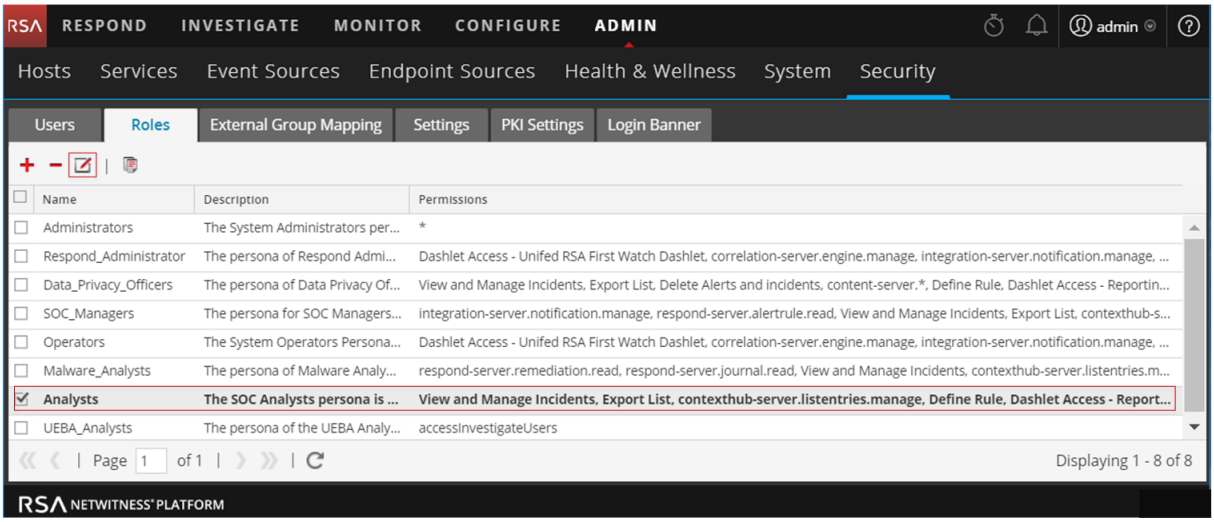
Task 6. Modify the Analyst Role `investigate-server` Permissions

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.

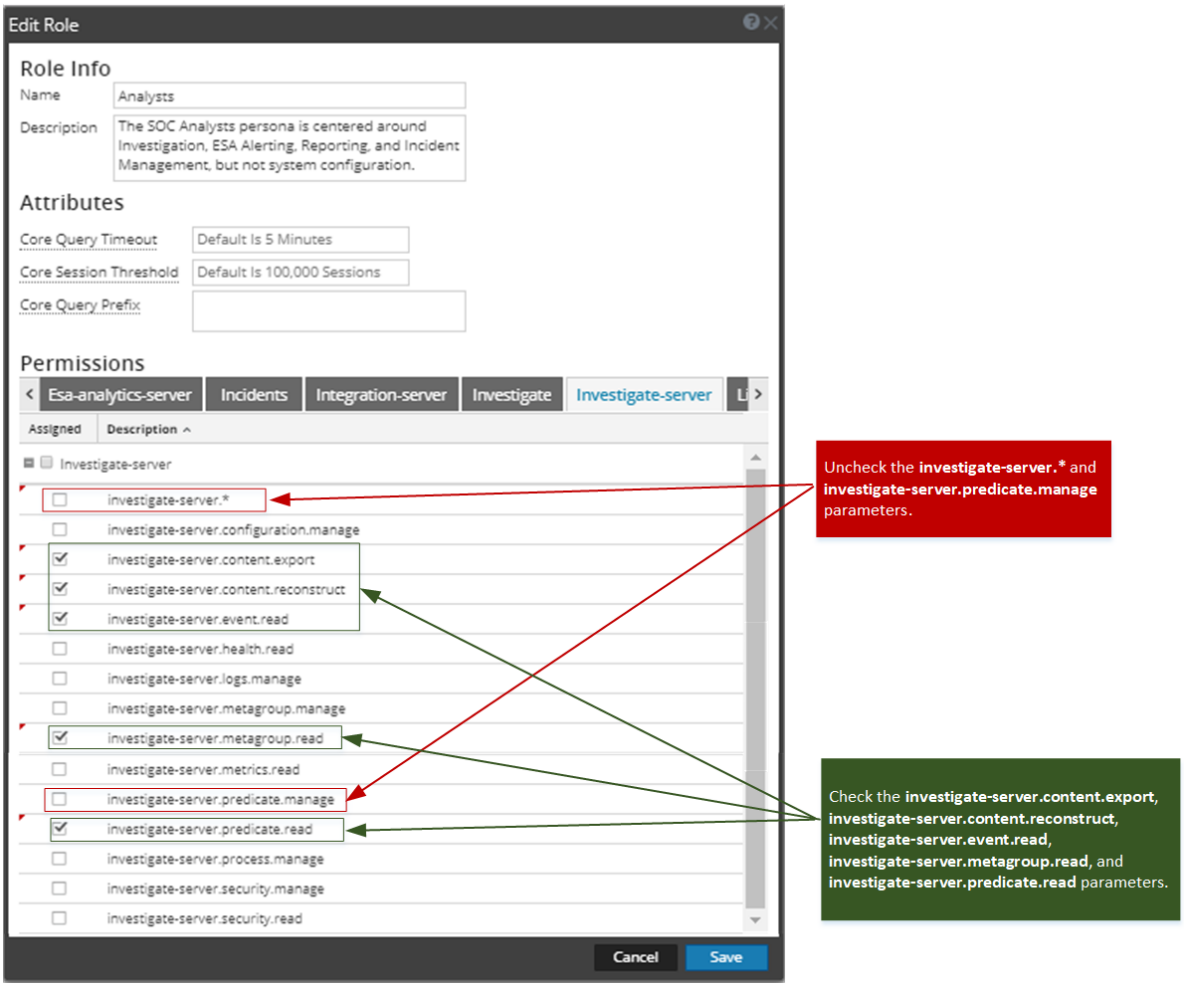
As a result, you must upgrade the default permissions to match the 11.3.x.x default permissions, as described in the following procedure.

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 11.3.2.0 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 11.3.2.0, 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. 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 12. (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 11.3.2.0, 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 11.3.2.0 from versions prior to 11.3.2.0, 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 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 11.3.2.0.

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 11.3.2.0:
     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 11.3.2.0, 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 11.3.2.0, 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 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 11.3.2.0 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*.
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*.

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 11.3.2.0, 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 11.3.2.0 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 11.3.2.0 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 11.3.2.0:

```
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 11.3.2.0:

```
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 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
```

Respond

Task 14. (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 15. 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 11.3.2.0. You must replace the old versions.

Before the upgrade to 11.3.2.0, 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 16. 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 17. (Conditional) Add Respond Notification Settings Permissions

Note: If you have 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 18. (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 11.3.2.0, 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 19. 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 20. (Conditional) Enable Endpoint Data Sources

If NetWitness Endpoint Server is configured in NetWitness Platform 11.3.2.0, 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 21. Enable UEBA Indicator Forwarder

If the NetWitness Respond server is configured in NetWitness Platform 11.3.2.0, 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":tru
e}]}'
```

Task 22. Upgrade Broker or Concentrator UUID

In UEBA, after you upgrade to NetWitness Platform 11.3.2.0, 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
```

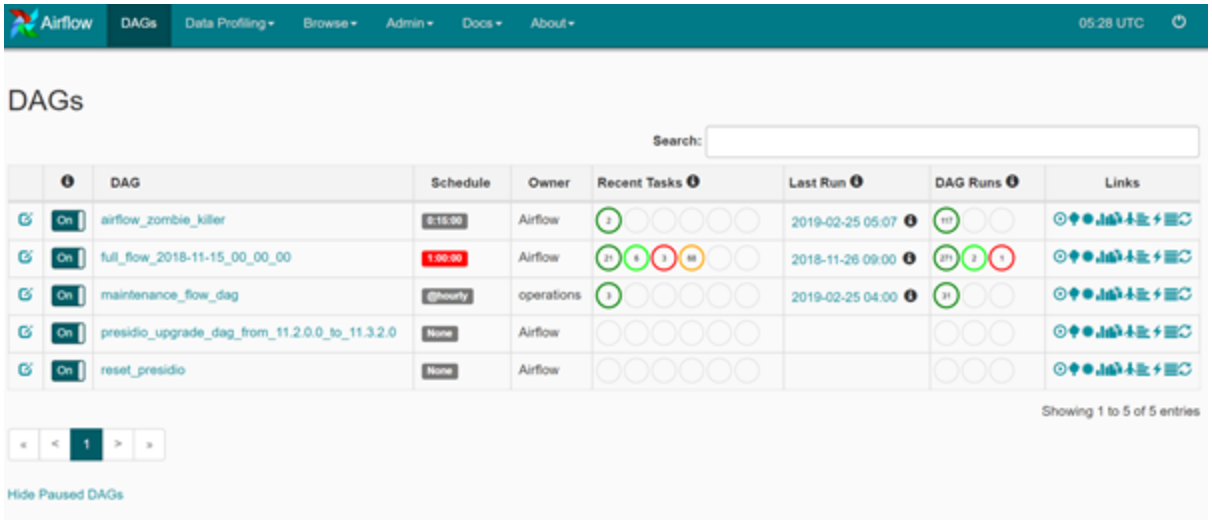
Task 23. Upgrade Airflow Configuration

After you upgrade to NetWitness Platform 11.3.2.0, you must upgrade Airflow configurations. Perform the following:

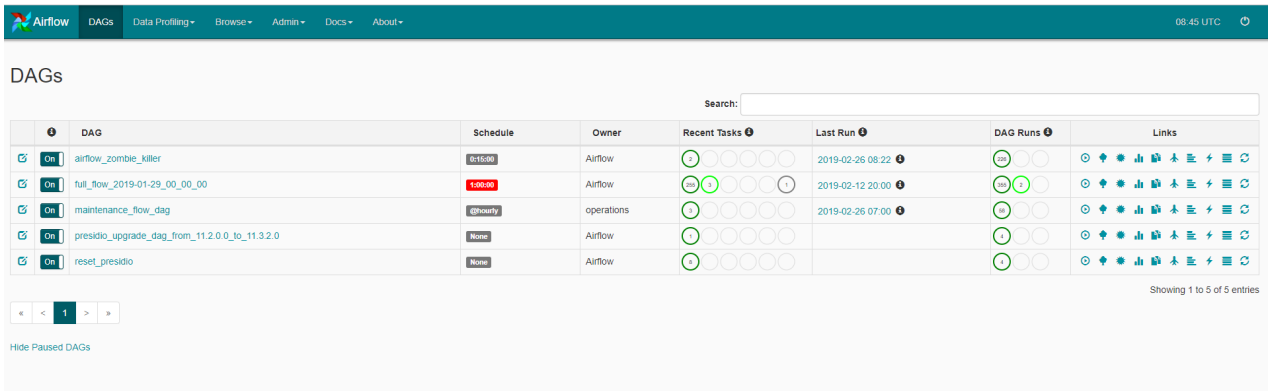
1. To access Airflow, go to `https://<UEBA_host>/admin/`, and the enter user name and password.

   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 11.3.2.0.



2. Click  (Trigger Dag) on `presidio_upgrade_dag_from_11.2.0.0_to_11.3.2.0 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 24. 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
```

Product Documentation

The following documentation is provided with this release.

Document	Location
NetWitness Platform 11.3.2.0 Online Documentation, including Release Notes	https://community.rsa.com/community/products/netwitness/113
NetWitness Platform Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Feedback on Product Documentation

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

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 file 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 11.1.x.x, 11.2.x.x or 11.3.x.x to 11.3.2.0 release, download:
  `netwitness-11.3.2.0.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 updating from 11.1.x.x, 11.2.x.x or 11.3.x.x to 11.3.2.0** , you only need to stage 11.3.2.0. Log into the `/root` directory of the NW Server and create the following directory:
   `/tmp/upgrade/11.3.2.0`
   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 directories using the following commands:
   `unzip netwitness-11.3.2.0.zip -d /tmp/upgrade/11.3.2.0`

   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 11.3.2.0 --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 11.3.2.0`
4. When the component 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

Note: The external repo should have separate directories for 11.3.0.0 and 11.3.2.0, as described in Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface.

1. Stage 11.3.2.0 by creating a directory on the NW Server host at `/tmp/upgrade/11.3.2.0` and extract the zip package.

   ```
   unzip netwitness-11.3.2.0.zip -d /tmp/upgrade/11.3.2.0
   ```

   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 11.3.2.0 --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
   11.3.2.0
   ```

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).