RSA NETWITNESS® PLATFORM

Upgrade Guide

for RSA NetWitness® Platform 11.4

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

September 2020

Contents

Upgrade Overview

RSA NetWitness® Platform 11.4.0.0 provides enhancements and fixes for all products in the Platform. The components of the platform are: The NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, Security sever, and Source server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Broker, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Health & Wellness Beta, Log Collector, Log Decoder, Log Hybrid, Log Hybrid Retention, Malware Analysis, Network Decoder, Network Hybrid, Reporting Engine, UEBA, and Warehouse Connector.

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

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

Upgrade Path

The following upgrade paths are supported for NetWitness Platform 11.4.0.0:

- RSA NetWitness® Platform 11.2.x.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.0.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.1.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.2.x to 11.4.0.0

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

The following matrix shows all the supported upgrade paths.

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

Running in Mixed Mode

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

Upgrade Considerations for ESA Rule Deployments

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

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

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

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

Change to Column Groups in the Events View

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

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

Feedback on Product Documentation

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

Contacting Customer Care

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

RSA Link	https://community.rsa.com/
Phone	1-800-995-5095, option 3

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

Upgrade or Install Windows Legacy Collection

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

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

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

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Platform 11.4.

Event Stream Analysis (ESA)

Task 1 - Delete ESA Rule Deployments that do not contain an ESA Correlation service

Note: This Event Stream Analysis (ESA) task is for upgrades to 11.4 from 11.3.x.x.

Unused ESA rule deployments left over from the migration from the 10.6 or 11.2 legacy Event Stream Analysis service, which do not contain an ESA Correlation service, cause ESA rule deployments to not deploy after upgrading to NetWitness Platform 11.4.

Before you upgrade to 11.4, delete ESA rule deployments that do not contain an ESA Correlation service. The remaining ESA rule deployments should have been deployed at least once with the ESA Correlation service.

To delete an ESA rule deployment,

1. Go to **Configure > ESA Rules > Rules** tab.
2. In the options panel to the left under **Deployments**, select the deployment that you want to remove.
3. Select  **> Delete**.
4. Click **Yes** to confirm the delete.

Upgrade Tasks

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

Note: After upgrading the primary NW server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Note: If you are using S4s devices that use SD cards, SSH to NW Server and run the following command before starting the upgrade process.

```
manage-stig-controls --disable-control-groups 7 --host-id <node uuid>
```

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

```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ntpd
```

Use one of the following methods to apply version updates (for example, 11.4.0.0) to a host.

- Online Method - Connected to RSA Live
- Offline Method from Hosts View
- Offline Method using Command Line Interface

Online Method (Connected to RSA Live)

Use this method if NetWitness Platform has an RSA Live Update Repo Connection (Web Access).

Task 1. Populate Local Repo or Set Up an External Repo

When you set up your NW Server, you select the Local Repository (Repo) or an External Repository (Repo). The Hosts view retrieves version updates from the repo you selected.

If you select the Local Repo, you do not need to set it up, but you must make sure that it is populated with the latest version updates. See Appendix A. Populate Local Repo for instructions on how to populate it with a version update.

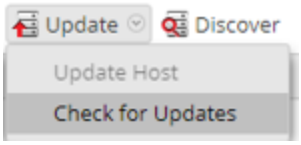
Note: If you selected an External Repo, you must set it up. For more information on how for instructions on how to populate it with a version update see Appendix B. Set Up External Repo.

Task 2. Apply Updates from the Hosts View to Each Host

The Hosts view displays the software version updates available in your Local Update Repository, and you choose and apply the updates you want from the Host view.

This procedure tells you how to update a host to a new version of NetWitness Platform.

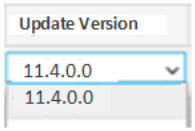
1. Log in to NetWitness Platform.
2. Go to **Admin** > **Hosts**.
3. (Conditional) Check for the latest updates.



4. Select a host or hosts.

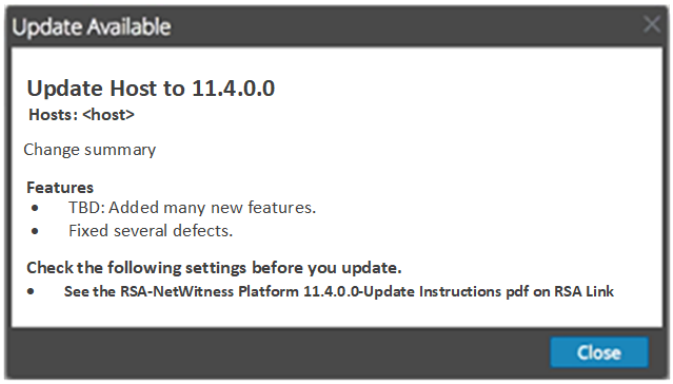
   You must update the NW Server to the latest version first. You can update the other hosts in any sequence you prefer, but RSA recommends that you follow the guidelines in Running in Mixed Mode.
   `Update Available` is displayed in the Status column of the Hosts list view if you have an version update in your Local Update Repository for the selected hosts.

5. Select the version you want to apply from the **Update Version** column.



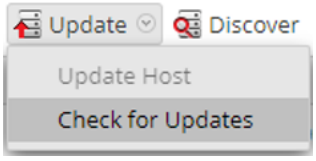
   If you:

   - Want to update more than one host to that version, after you update the NW Server host, select the checkbox to the left of the hosts. Only currently supported update versions are listed.
   - Want to view a dialog with the major features in the update, click the ⓘ to the right of the update version number. The following is an example of this dialog.

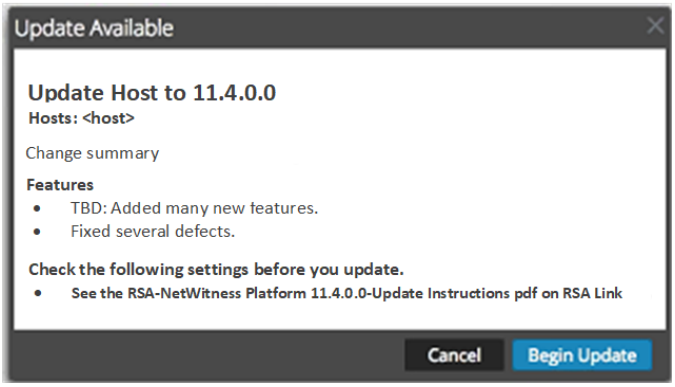


- Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message `New updates are available` is displayed, and the Status column updates automatically to show `Update Available`. By default, only supported updates for the selected host are displayed.

6. Click **Update > Update Host** from the toolbar.



A dialog is displayed with information about the selected update. Click **Begin Update**.



The Status column tells you what is happening in each of the following stages of the update:

- Stage 1 - **Downloading update packages** - downloads the repository artifacts to the NW Server applicable to the services on the host you chose.
- Stage 2 - **Configuring update packages** - configures update files in to correct format.
- Stage 3 - **Update in progress** - updates host to the new version.

7. When you see `Update in progress`, refresh the browser.

   This may display the NetWitness Log In screen from which you log in again and navigate back to the Host view.

   After the host is updated, NetWitness Platform prompts you to **Reboot Host**.

8. Click **Reboot Host** from the toolbar.

NetWitness Platformshows the status as `Rebooting...` until the host comes back online and the Status shows `Up-to-Date`. Contact Customer Care if the host does not come back online.

Note: If you have the Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) enabled, opening core services can take approximately 5 to 10 minutes. This delay is caused by the generation of new certificates.

Offline Method from Hosts View

Use this method if NetWitness Platform does not have an RSA Live Update Repo Connection (No Web Access) and you want to apply updates from the **Admin** > **Hosts** view.

Note: The offline User Interface method is only available if you are upgrading a host from 11.3.1.0 or later to 11.4.0.0. If you are upgrading a host on an earlier version, you must use the Offline Method described in Offline Method Using Command Line Interface .

Follow these instructions to apply version updates from the User Interface without a NetWitness Platform connection to the Internet (for example, no Live connection). The follow 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.

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

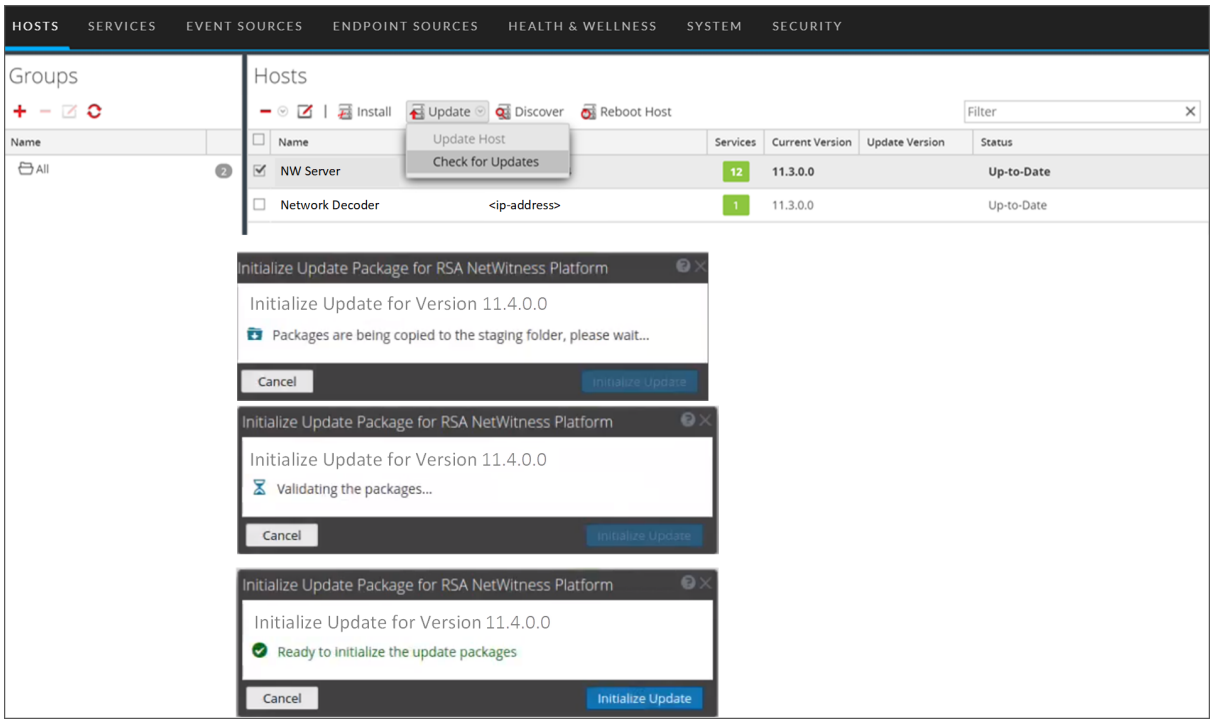
1. Download `.zip` update package for the version you want (for example, `netwitness-11.4.0.0.zip`) from RSA Link to a local directory.
2. SSH to the NW Server host.
3. Copy update package you want from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder. For example:
   ```
   sudo cp /tmp/netwitness-<version-number>.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.

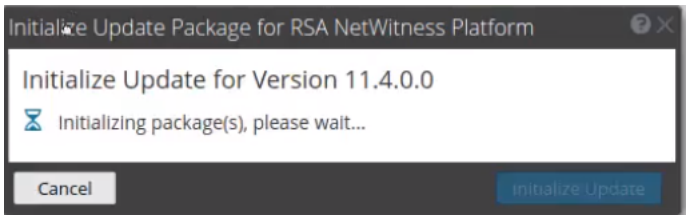


`Ready to initialize the update packages` is displayed if:

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

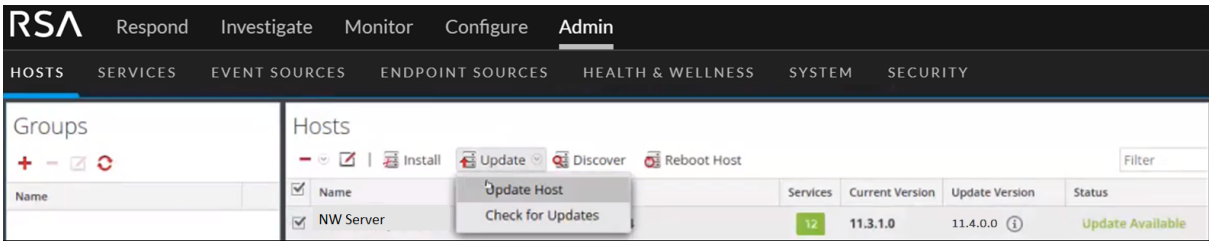
Refer to Appendix C. Troubleshooting Version Installations and Upgrades for instructions on how to troubleshoot errors (for example, `Error deploying version <version-number>` and `Missing the following update package(s)`, displayed in the Initiate Update Package for RSA NetWitness Platform dialog.

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.

Offline Method Using Command Line Interface

Use this method if NetWitness Platform does not have an RSA Live Update Repo Connection (No Web Access) and you want to apply updates using the Command Line Interface.

If your RSA NetWitness Platform deployment does not have Web access, complete the following procedure to apply a version update.

1. Download the `.zip` update package for the version you want (for example, `netwitness-11.4.0.0.zip`) from RSA Link to the `/root` directory.
2. SSH to the NW Server host.
3. Make a `/tmp/upgrade/<version>` staging directory for the version you want (for example, `/tmp/upgrade/11.4.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.4.0.0
   ```
4. Copy the `.zip` update package to the `/root` directory).

   Note: 1.) Make sure that you copy the `netwitness-11.4.0.0.zip` file to a directory path other than the staging directory path (for example, the `/root` directory). 2.) Make sure that you extract the rpm files to the staging directory path (for example, `/tmp/upgrade/11.4.0.0` directory).

5. Unzip the package into the staging directory you created (for example, `/tmp/upgrade/11.4.0.0`).
   ```
   unzip /root/netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0
   ```
6. Initialize the update on the NW Server.
   ```
   upgrade-cli-client --init --version 11.4.0.0 --stage-dir /tmp/upgrade/
   ```
7. Apply the update to the NW Server.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.4.0.0
   ```
8. Log in to NetWitness Platform, go to **Admin** > **Hosts**, and reboot the NW Server host in the Host view.
9. For each component host:

   a. Apply the update to each component host:
      ```
      upgrade-cli-client --upgrade --host-addr <component-host IP address> --
      ```

```
version 11.4.0.0
```

The update is complete when the polling is completed.

b. Log in to NetWitness Platform, go to **Admin** > **Hosts**, and reboot the component host in the Host view.

You can verify the version applied to the host with the following command.

```
upgrade-cli-client --list
```

Note: 1.) If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates.
2.) If you have Unity storage, check the PowerPath status and verify the it can see the Unity device.
3.) If you get the error illustrated in the following example, the update installs correctly and no action is required. If you encounter additional errors during the update, contact Customer Support

```
2019-01-28 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)
```

Post Upgrade Tasks

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

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

After you have upgraded to 11.4, refer to the *Post Install Instructions* in the 11.4 Installation Guides so you can take advantage of the new features introduced in 11.4. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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 11.4.

General

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

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

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

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

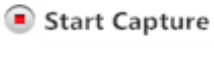
Start Network Capture

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

.

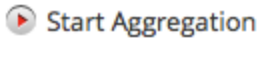
Start Log Capture

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

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

.

Start Aggregation

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

.

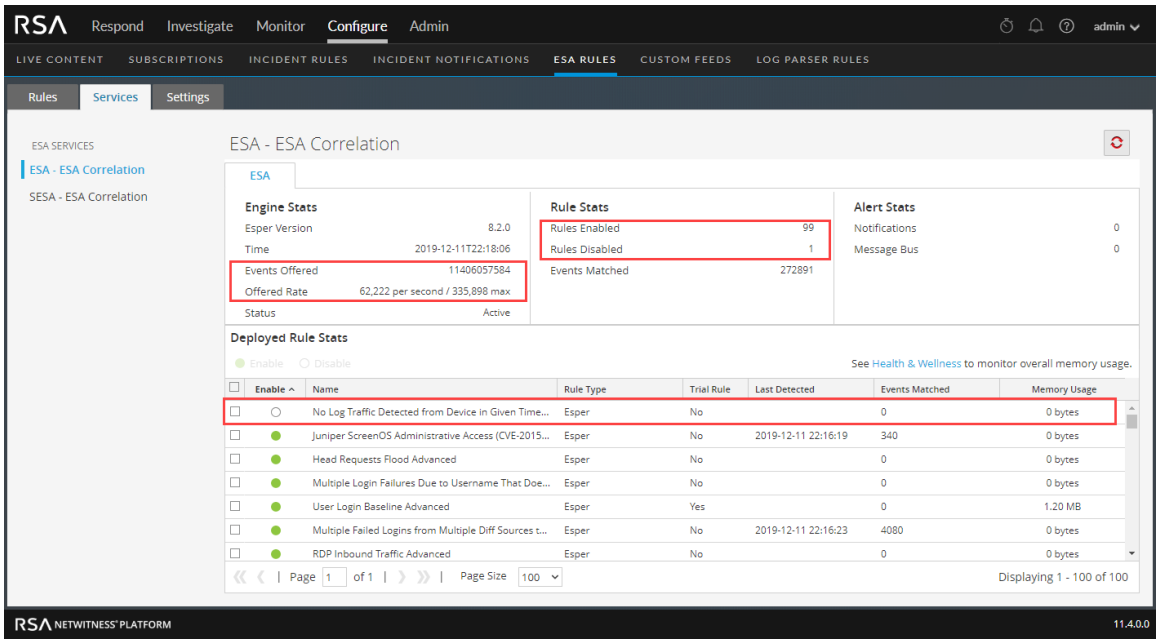
Event Stream Analysis

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

Task 2. Verify the Status of the ESA Rule Deployments

Check the status of the ESA rule deployments.

1. Go to **Configure** > **ESA Rules** > **Services** tab.
   The Services view is displayed, which shows the status of your ESA services and deployments.
2. In the options panel on the left, select an ESA service.
3. For each service listed, look at the deployment tabs in the panel on the right. Each tab represents a separate ESA rule deployment.
4. For each ESA rule deployment:
   a. In the **Engine Stats** section, look at the **Events Offered** and the **Offered Rate**. They confirm that the data is being aggregated and analyzed properly. If you see 0 for Events Offered, nothing is coming in for the deployment.
   b. In the **Rule Stats** section, look at the **Rules Enabled** and **Rules Disabled**. If there are any disabled rules, look in the **Deployed Rule Stats** section below to view the details of the disabled rules. Disabled rules show a white circle. Enabled rules show a green circle.



5. If you notice any disabled rules that should be enabled:
   a. Go to **Configure** > **ESA Rules** > **Rules** tab and redeploy the ESA rule deployments that contain disabled rules.
   b. Go back to the **Services** tab and check to see if the rules are still disabled. If the rules are still disabled, check the ESA Correlation service log files, which are located at `/var/log/netwitness/correlation-server/correlation-server.log`.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ESA Troubleshooting information

For more information, see ESA Troubleshooting Information.

Investigate

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

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

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

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

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

To enable the permissions for a user role:

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

Respond

The Primary ESA server must be upgraded to 11.4 before you can complete these tasks.

Note: After upgrading the primary NW server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  // Add custom logic below
  var custom_events;

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

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

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

  }

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

  return normalized;
}
```

Task 8. (Conditional) Add Respond Notification Settings Permissions

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

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

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

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

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

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

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

Perform all the tasks in this section if you are upgrading from 11.2.x.x to 11.4.

General

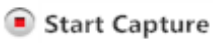
Task 1. Make Sure Services Have Restarted and Are Capturing and Aggregating Data

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

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

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Start Network Capture

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

.

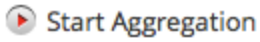
Start Log Capture

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

2. Select each **Log Decoder** service.
3. Under  (actions), select **View** > **System**.
4. In the toolbar, click 

.

Start Aggregation

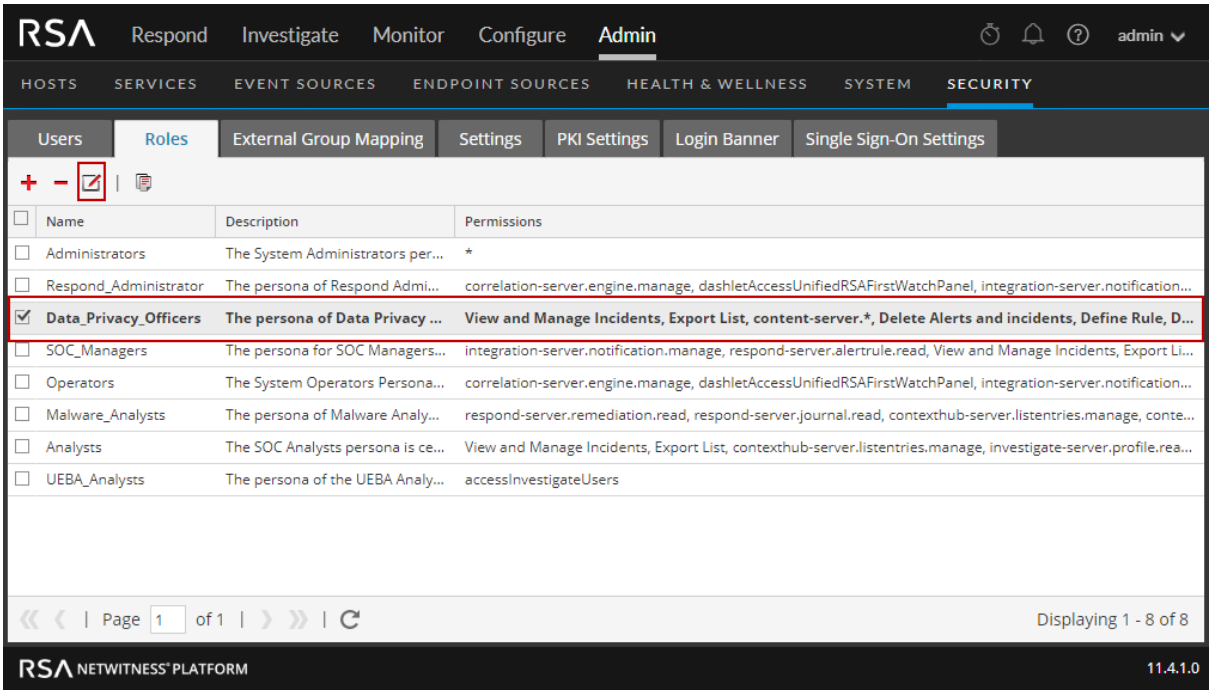
1. In the NetWitness Platform menu, go to **Admin** > **Services**.
   The Services view is displayed.
2. For each **Concentrator**, **Broker**, and **Archiver** service:
   a. Select the service.
   b. Under  (actions), select **View** > **Config**.
   c. In the toolbar, click 

.

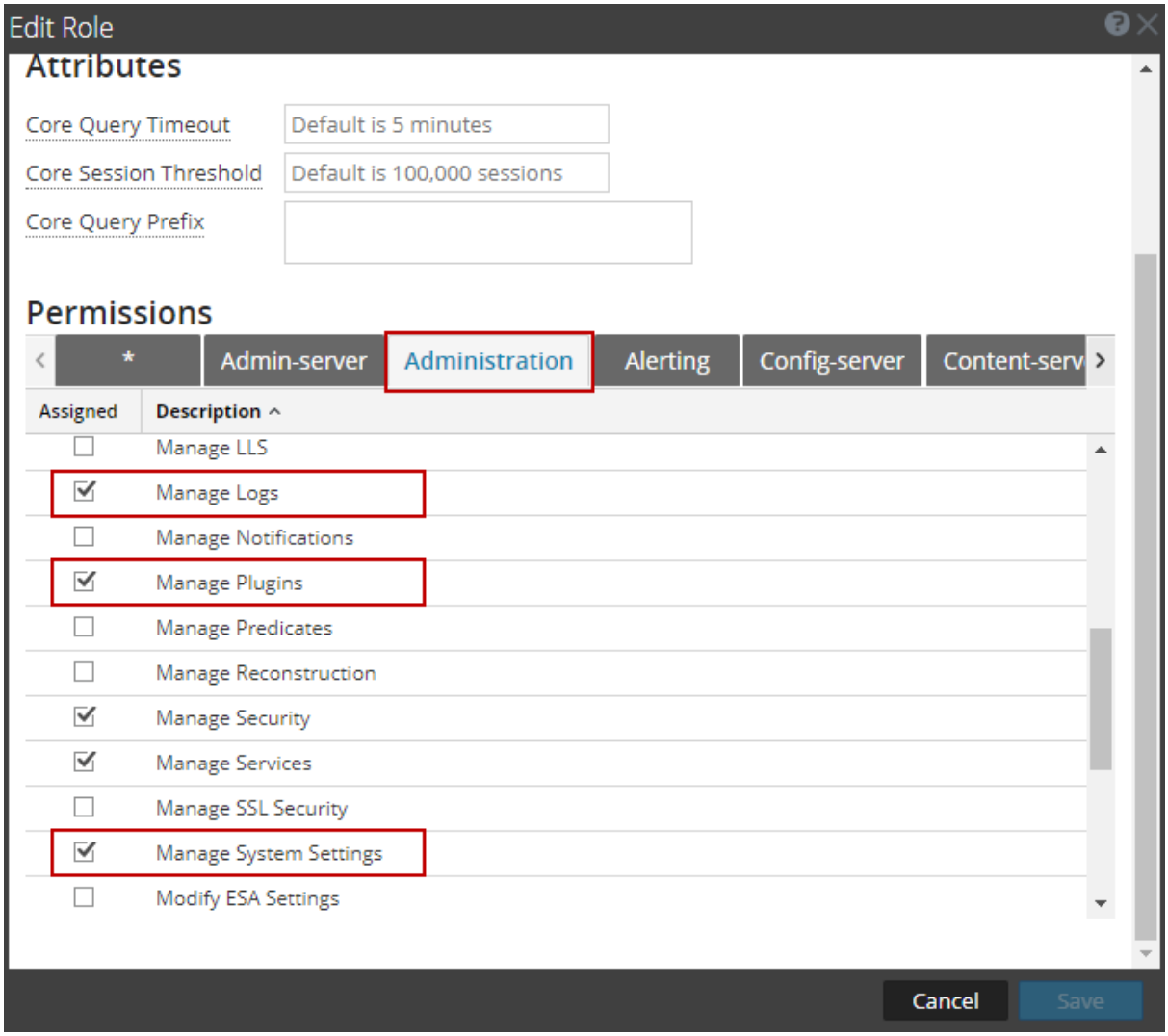
Task 2. Set Up Context Menu Actions User Permissions

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

1. In the **NetWitness Platform** menu, go to **Admin** > **Security** > **Roles**.
2. Double-click on the user role (for example, **Data Privacy Officers**), or click to select the role and click  (Edit).



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



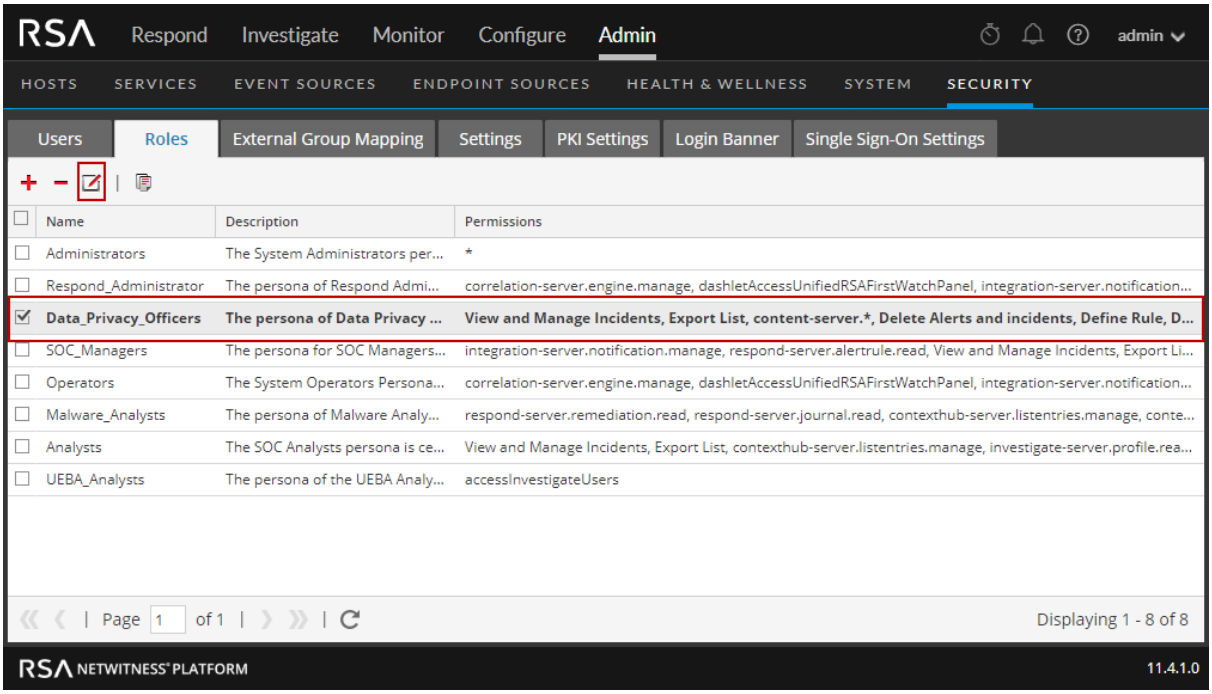
4. Complete steps 1 through 3 for the **Analysts** and **SOC Managers** roles in addition to **Data Privacy Officers**.

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

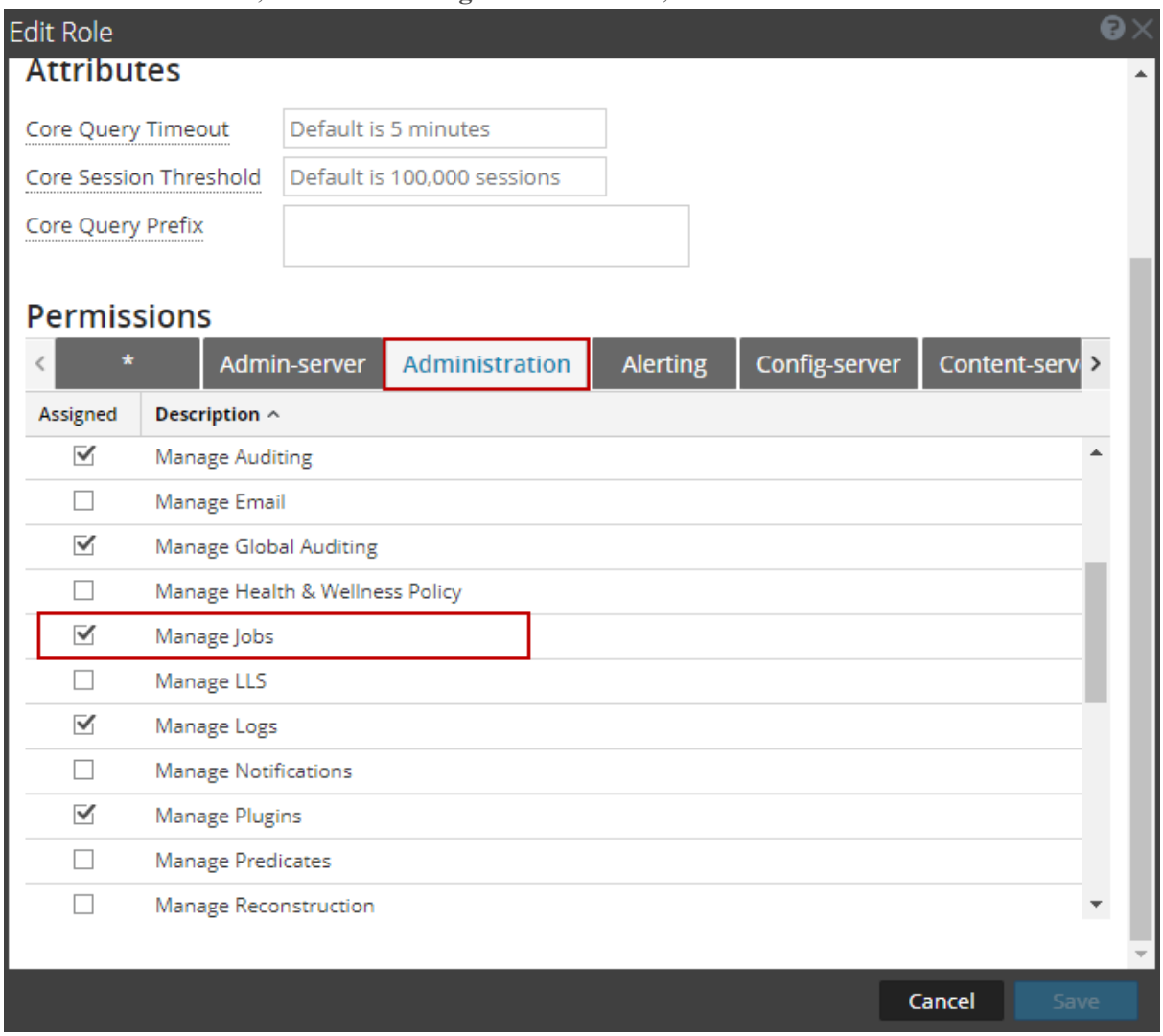
Add the 'Manage Jobs' Administration permission to the following roles:

- SOC_Managers
- Operators
- Data_Privacy_Officers

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



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. (Conditional) Reissue Certificates for Your Hosts

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

The validity for NetWitness Platform certificates are as follows:

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

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

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

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

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

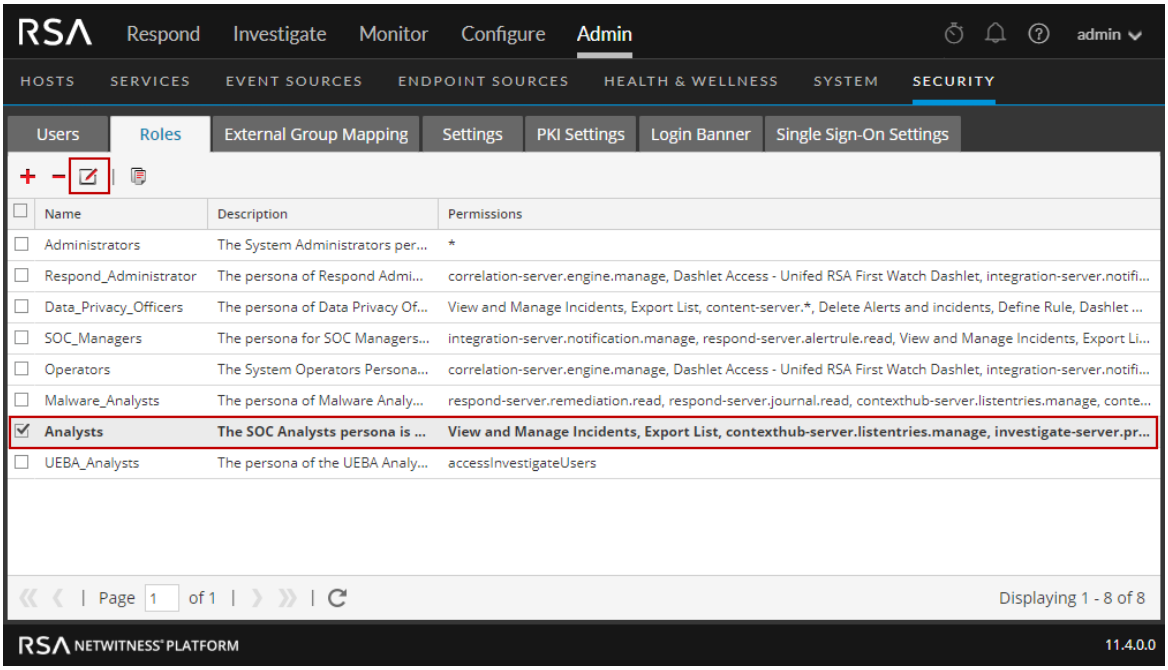
Task 5. Modify the Analyst Role `investigate-server` Permissions

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

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

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

1. Go to **Admin** > **Security** > **Roles**.
2. Complete the following steps for **SOC Managers**, **Malware Analysts**, and **Analysts** roles.
   a. Check the user role checkbox (for example, **Analysts**) and click (Edit icon).



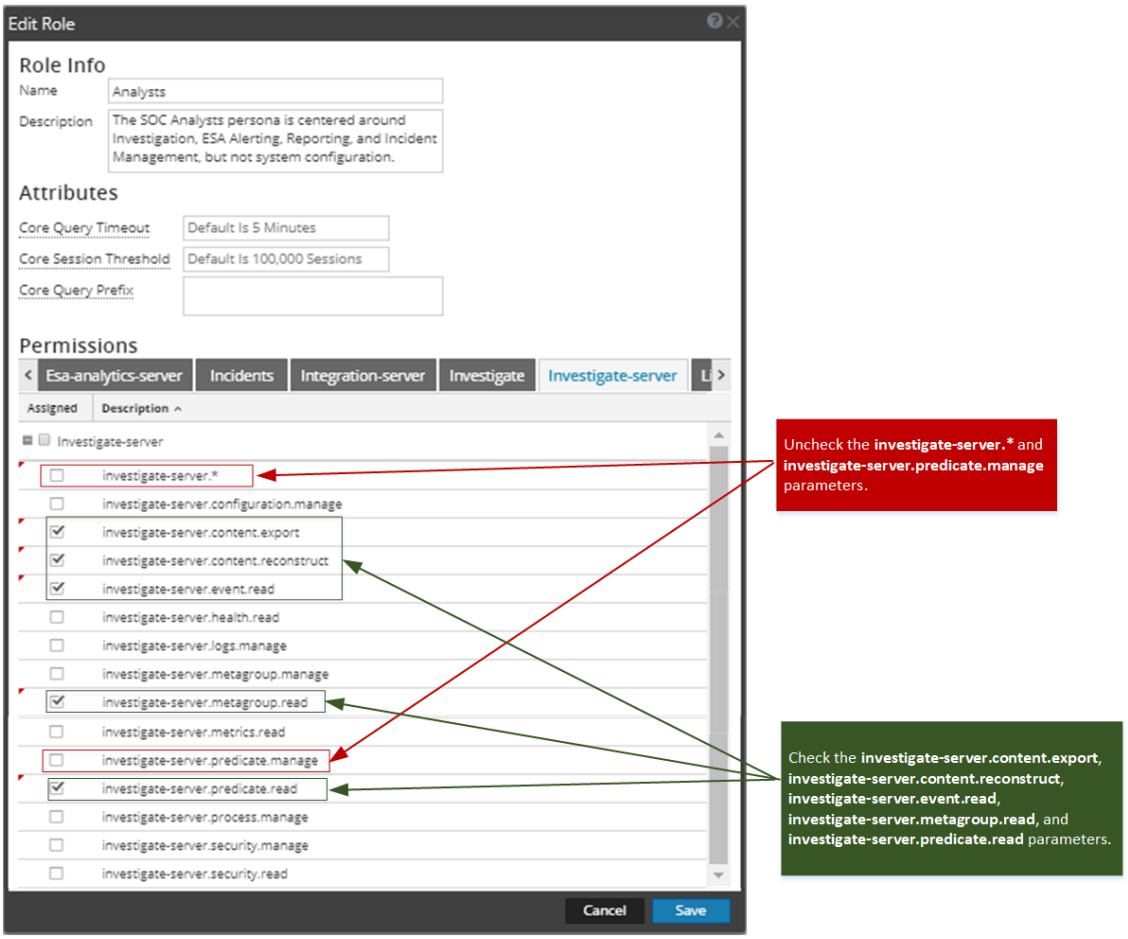
b. Under **Permissions**, click the **Investigate-server** tab.

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 6. (Conditional) Reconfigure PAM RADIUS Authentication

If you configured PAM RADIUS authentication in 11.2.x.x using the `pam_radius` package, you must reconfigure it in 11.4 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 11.2.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 7. (Conditional) If NetWitness Platform Has No Web Access, Upload Response .bin File Again (License Server)

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

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

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

Event Stream Analysis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Task 11. Verify the ESA Rule Deployments

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

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

For a detailed example, see the *ESA Configuration Guide*. For Deployment information, see "ESA Rule Deployment Steps" in the *Alerting with ESA Correlation Rules User Guide*. For troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.

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

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

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

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

1. After an upgrade to 11.4, 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 11.4, NetWitness Platform does not modify existing rules for the Ignore Case option. If an existing Rule Builder rule has the Ignore Case option selected for a meta key that no longer has the option available, an error occurs if you try to edit the statement and try to save it again without clearing the checkbox.

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

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

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

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

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

```
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
```

Investigate

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

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

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

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

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

To enable the permissions for a user role:

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

Respond

The Primary ESA server must be upgraded to 11.4 before you can complete these tasks.

Note: After upgrading the primary NW server (including the Respond Server service), the Respond Server service will not be re-enabled until after the Primary ESA host is also upgraded to 11.4. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

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

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

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

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

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

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

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

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

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

appropriate meta keys with values from the '`rawAlert.events`' object. Below is the sample code.

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

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

  // Add custom logic below
  var custom_events;

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

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

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

  }

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

  return normalized;
}
```

Task 17. (Conditional) Add Respond Notification Settings Permissions

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

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

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

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

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

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

Decoder and Log Decoder

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

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

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

Endpoint Installation Tasks

Install the 11.4 Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 11.4 by downloading the Relay Server installer from the upgraded Endpoint Server. For more information see "(Optional) Installing and Configuring Relay Server" section in the *Endpoint Configuration Guide*.
2. Restart the Endpoint Server using the command:

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

Upgrade Endpoint Agents

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

NetWitness UEBA Installation Tasks

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

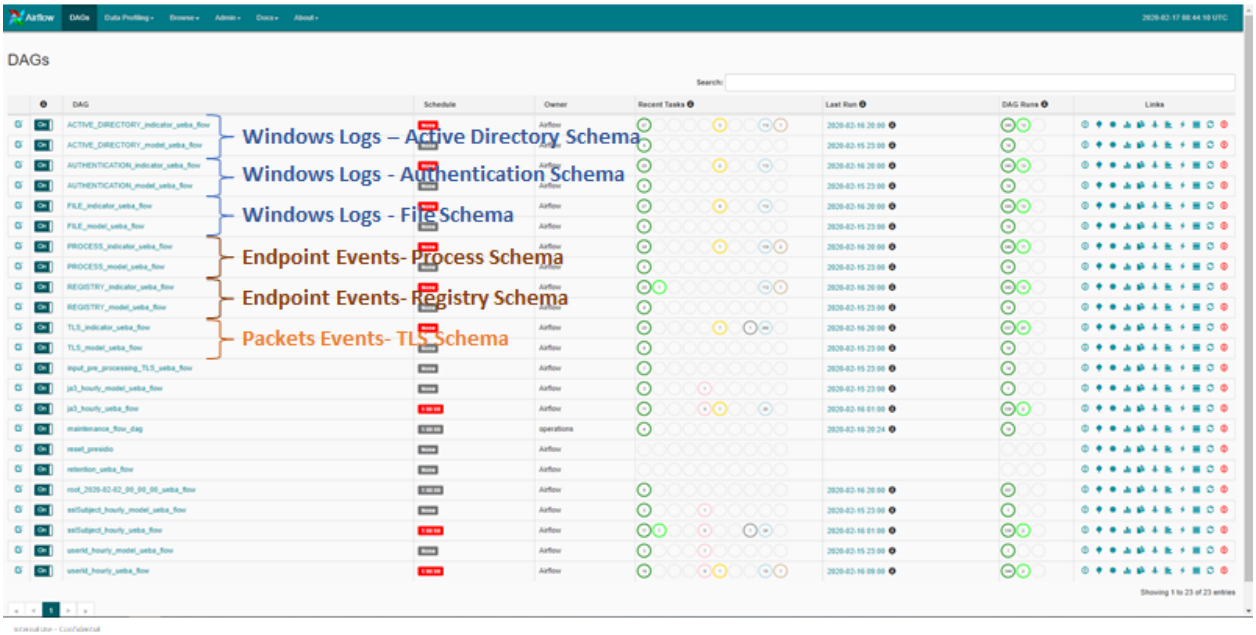
(Optional) Add Packets Schema

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

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

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

To see the schemas that are processed by the UEBA, access the airflow main page (`https://<ueba_host>/admin`). You can see each processed schema appears on this page.



To change schema or data source, run the following script before you run the upgrade DAG.

```
/opt/rsa/saTools/bin/ueba-server-config
```

To see the data sources that are processed by the UEBA, run the following command on the UEBA server to get the NetWitness Platform data source.

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

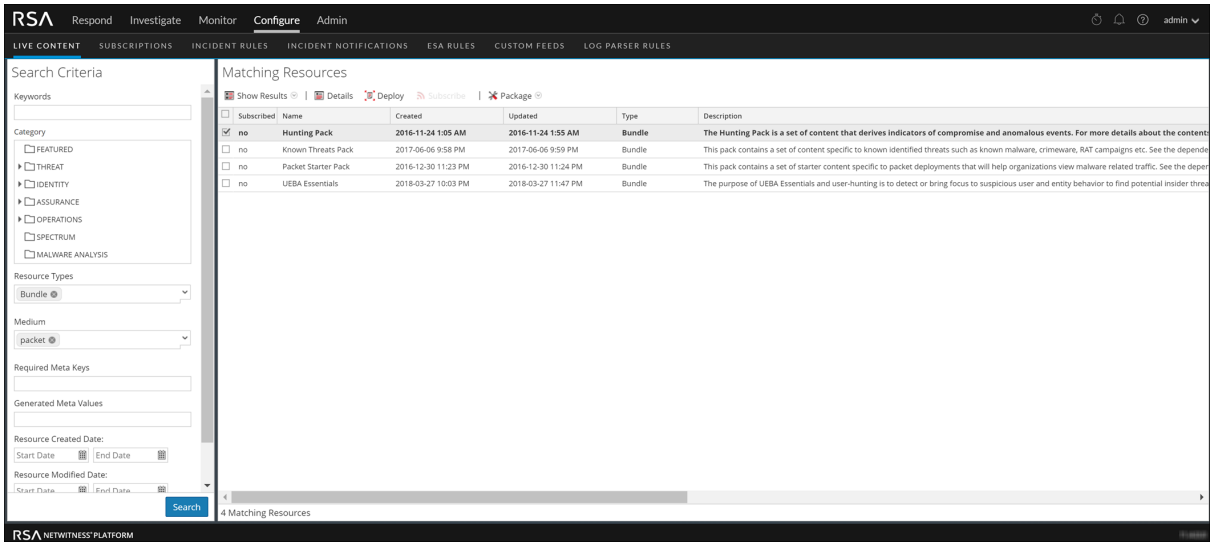
You can also use the following command to get the NetWitness Platform data source.

```
curl http://localhost:8888/application-presidio-default.properties | grep 'dataPulling.source'
```

Add the Hunting Pack

In NetWitness Platform, add the hunting pack or verify it it's available:

1. Log in to NetWitness Platform
2. Go to **ADMIN** and select **Admin Server**
3. Click  and select **Configure** > **Live Content**



.

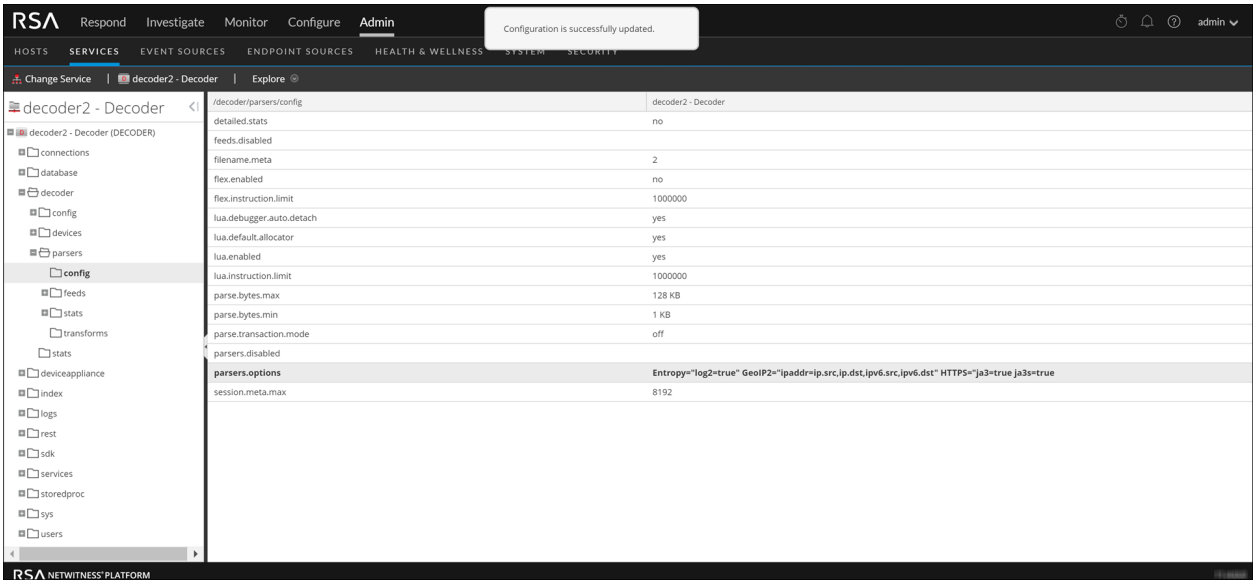
4. In the Search criteria, select the following:
   a. **Bundle** under Resources Type.
   b. **Packet** under Medium.
5. Click **Search**.
   A list of matching resources is displayed.
6. Select **Hunting Pack** from the list and click **Deploy**.
   The hunting pack is added.

Add JA3 and JA3s

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

To add JA3 and Ja3s:

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



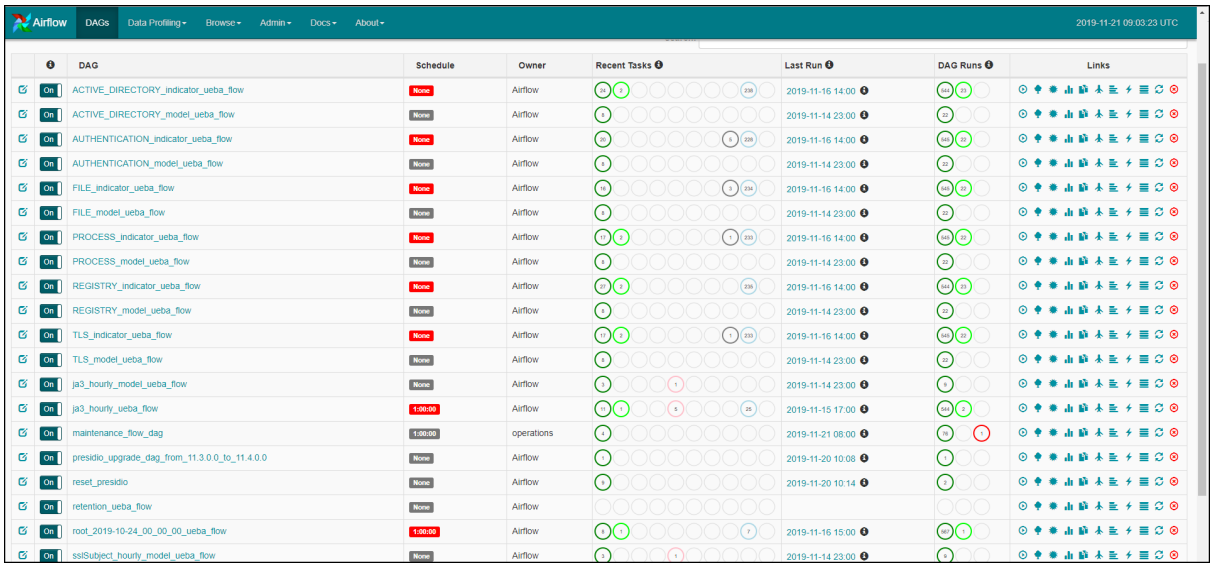
Update Airflow Configuration

After you upgrade to NetWitness Platform 11.4, make sure you update the Airflow Configurations.
To update the Airflow Configurations:

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

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

   Note: The mismatched tasks between NetWitness Platform 11.3 and NetWitness Platform 11.4 in the full flow DAG can be marked in red.



2. Click  on `presidio_upgrade_dag_from_11.3.0.0_to_11.4.0.0 DAG` to pause the full flow DAG to:

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

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

Note: If you are upgrading from 11.2.x.x, perform the steps in Steps for Upgrading UEBA from 11.2.x.x now, and then restart the Airflow Schedule service as described below.

Restart Airflow Scheduler Service

After the `presidio_upgrade DAG` operation is successful, you must restart the Airflow scheduler service.

Note: When the `presidio_upgrade DAG` is successful, the DAG is indicated with a dark green circle under the **Recent Tasks**.

To restart the airflow scheduler service, run the following command on the UEBA server:

```
systemctl restart airflow-scheduler
```

Steps for Upgrading UEBA from 11.2.x.x

(Optional) Enable UEBA Indicator Forwarder

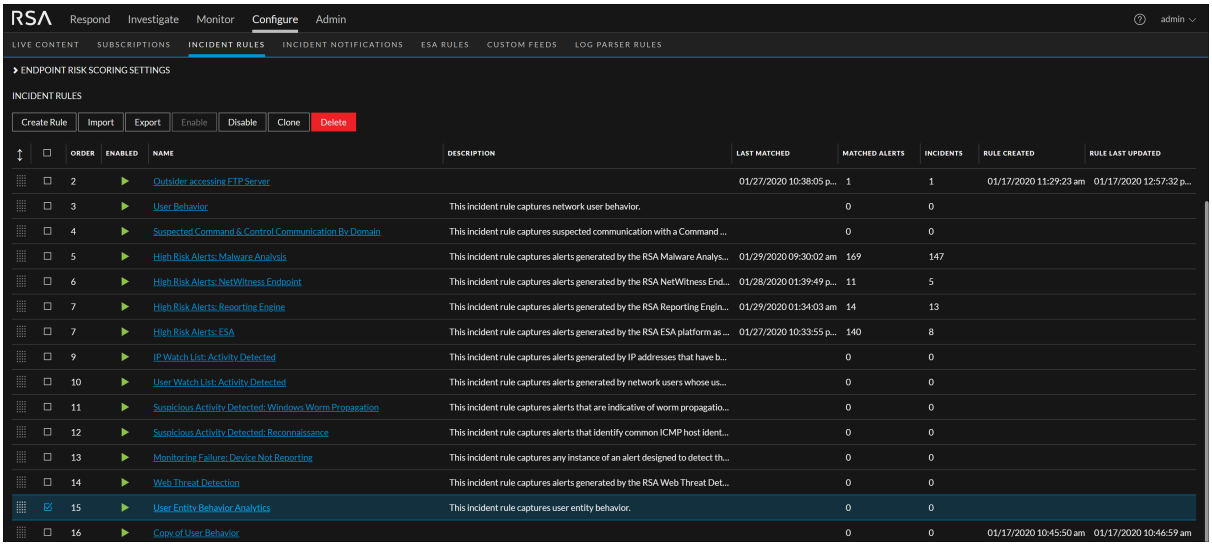
If NetWitness Respond server is configured in NetWitness Platform 11.4, you can transfer the NetWitness UEBA indicators to the NetWitness Respond server and to the correlation server to create an Incidents.

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}]}'
```

To view the incidents in Respond, please follow the below steps.

1. Log in to NetWitness Platform.
2. Go to **Configure** > **INCIDENT RULES**
3. Select the **User Entity Behavior Analytics** rule checkbox.



(Optional) Enable Endpoint Data Sources

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

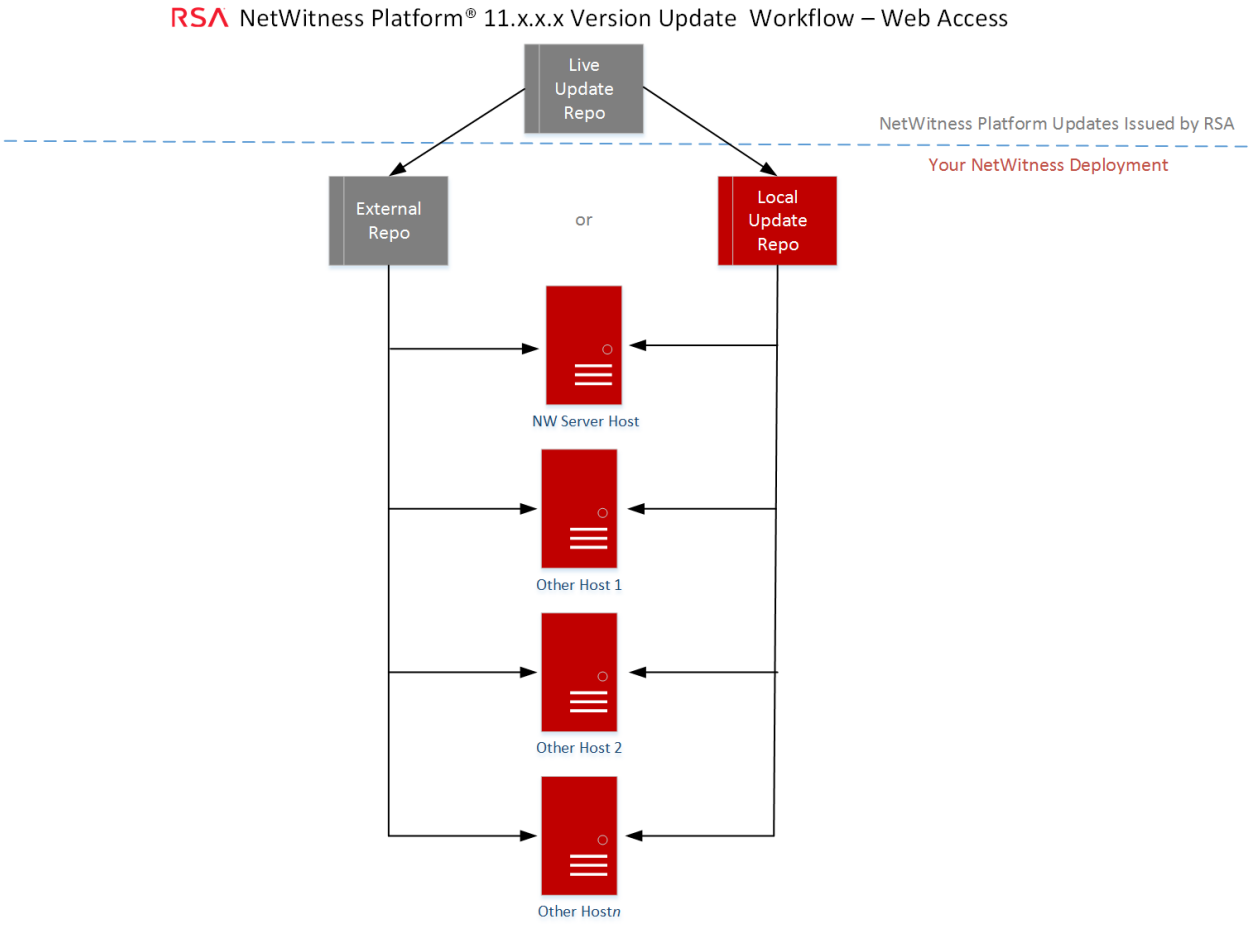
To enable Endpoint data sources, run the following commands on the UEBA server :

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

Appendix A. Populate Local Repo

NetWitness Platform sends version updates to the Local Update Repository from the Live Update Repository. Access to the Live Update Repository requires and uses the Live Account credentials configured under **ADMIN > System > Live Services**. In addition, you must check the **Automatically download information about new updates every day** checkbox under **ADMIN > System > Updates** to populate the Local Repo daily.

The following diagram illustrates how you obtain version updates if your NetWitness Platform deployment has web access.



Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 7 system packages and the RSA Production packages. This download of over 6.5 GB of data takes an indeterminate amount of time depending on your NW Server Internet connection and the traffic of the RSA repository. It is not mandatory to use the Live update repository. Alternatively you can use an external Repo.

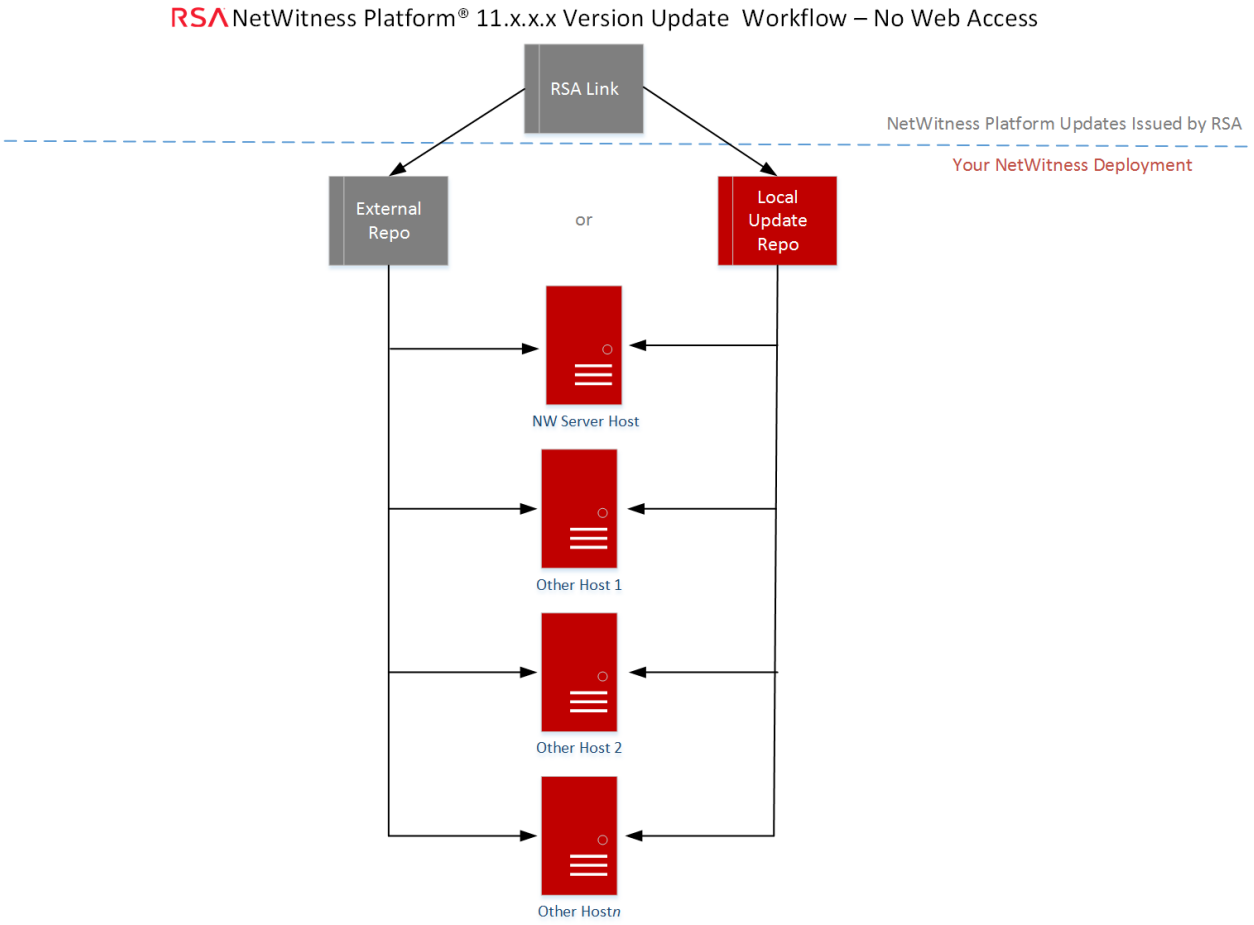
To connect to the Live Update Repository, go to Admin > System, select **Live Services** in the options panel and make sure that credentials are configured (Connection light should be green). If it is not green, click **Sign In** and connect.

Note: If you need to use proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. For more information see "Configure Proxy for NetWitness Platform" in the *System Configuration Guide*.

If your NetWitness Platform deployment does not have Web Access, you can use one of the following procedures to apply version updates to hosts.

- Apply Version Update from Hosts View without RSA Live Update Repo Connection (No Web Access)
- Apply Updates from the Command Line (No Web Access)

The following diagram illustrates how you obtain version updates if your NetWitness Platform deployment does not have web access.



Appendix B. Set Up External Repo

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step if you have an external repo and you want to override it.
   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
        The instructions are in the Offline Method Using Command Line Interface.
2. Set up the external repo.
   a. Log in to the web server host.
   b. Create directory to host the NW repository (`netwitness-11.4.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, /var/netwitness is the web-root, run the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. Create the 11.4.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0`
   d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.4.0.0`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA`
   e. Unzip the `netwitness-11.4.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0` directory.
      `unzip netwitness-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0`

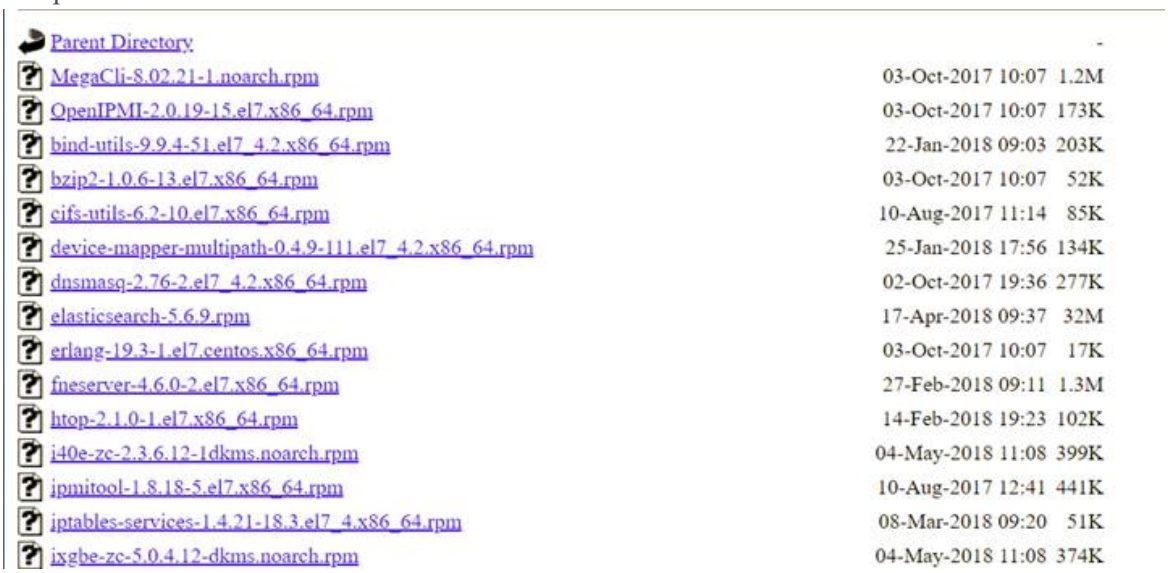
Unzipping `netwitness-11.4.0.0.zip` results in two zip files (`OS-11.4.0.0.zip` and `RSA-11.4.0.0.zip`) and some other files.

f. Unzip the:
`OS-11.4.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0/OS` directory.
`unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS`
The following example illustrates how the Operating System (OS) file structure appears after you unzip the file.

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

g. Unzip the:
`RSA-11.4.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA` directory.
`unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA`
The following example illustrates how the RSA version update file structure appears after you

unzip the file.



Parent Directory		-
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K
fneserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K

h. (Conditional - For Azure) Follow these steps for Azure update.

   i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS/other`

   ii. `unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS/other`

   iii. `cd /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS`

   iv. `createrepo`

i. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.4.0.0 Setup program (`nwsetup-tui`) prompt.

Appendix C. Troubleshooting Version Installations and Upgrades

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

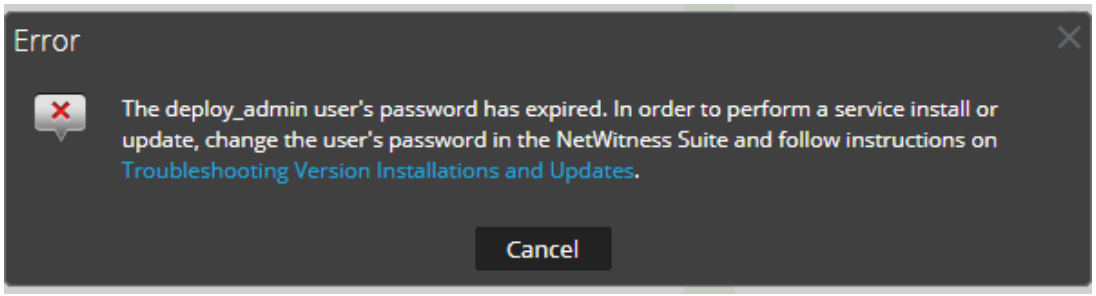
Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

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

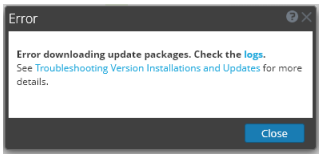
Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

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

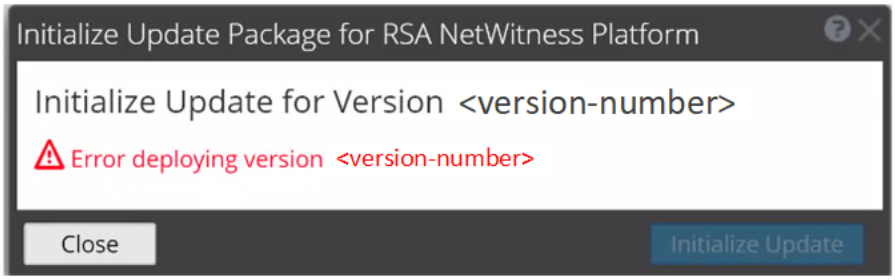
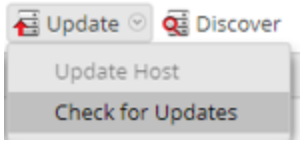
deploy_admin User Password Has Expired Error

Error Message	
Cause	The `deploy_admin` user password has expired.
Solution	Reset your `deploy_admin` password password. 1. On all component hosts (not including the NW Server host), run the following command. `/opt/rsa/saTools/bin/set-deploy-admin-password` 2. After all the component hosts have been updated, run this command on the NW Server host. `/opt/rsa/saTools/bin/set-deploy-admin-password` 3. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

Downloading Error

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

Error Deploying Version <version-number> Missing Update Packages

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

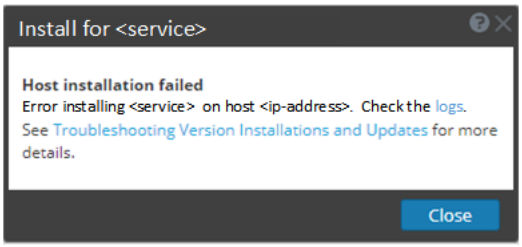
External Repo Update Error

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

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

Host Installation Failed Error

Error Message



Problem

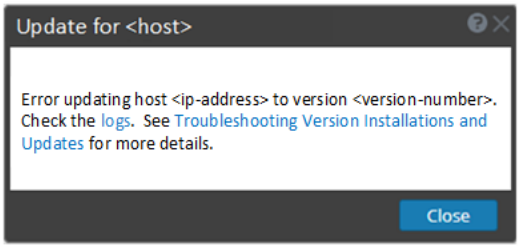
When you select a host and click **Install** the install service process fails.

Solution

1. Try to install the service again.
   Often this is all you need to do.
2. If you still cannot install the service:
   a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):
   `/var/netwitness/uax/logs/sa.log`
   `/var/log/netwitness/orchestration-server/orchestration-server.log`
   `/var/log/netwitness/deployment-upgrade/chef-solo.log`
   `/var/log/netwitness/config-management/chef-solo.log`
   `/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
   The error appears in one or more of these logs.
   b. Try to resolve the issue and reinstall the service.
   - Cause 1 - Entered the wrong `deploy_admin` password in the nwsetup-tui.
     Solution - Reset your `deploy_admin` password password.
     1. On the NW Server host and all other hosts on 11.x, run the following command.
        `/opt/rsa/saTools/bin/set-deploy-admin-password`
     2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.
   - Cause 2 -The `deploy_admin` password has expired.
     Solution - Reset your `deploy_admin` password password.
     1. On the NW Server host and all other hosts on 11.x, run the following command.
        `/opt/rsa/saTools/bin/set-deploy-admin-password`
     2. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

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

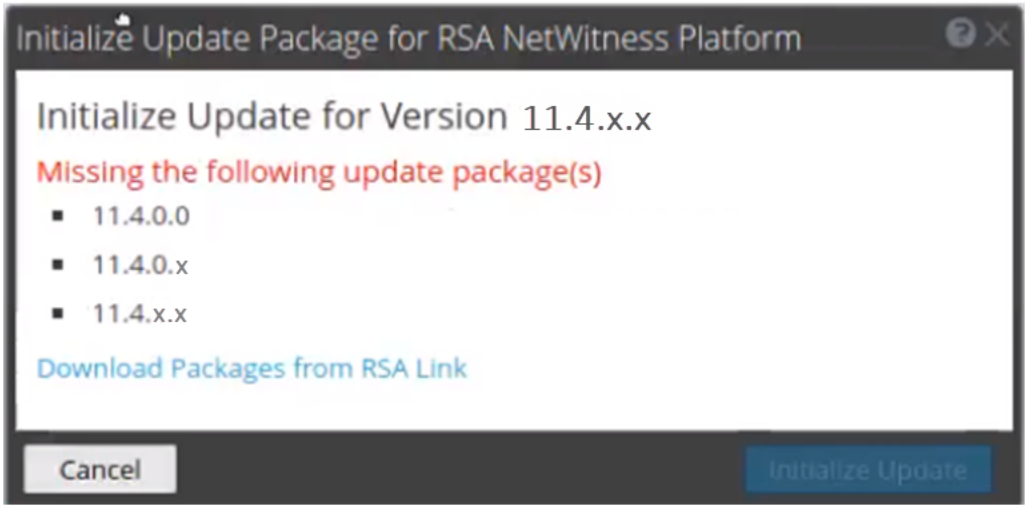
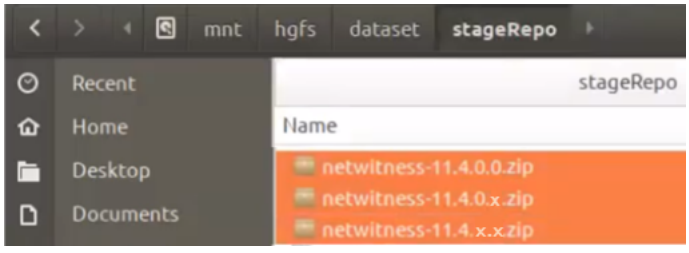
Host Update Failed Error

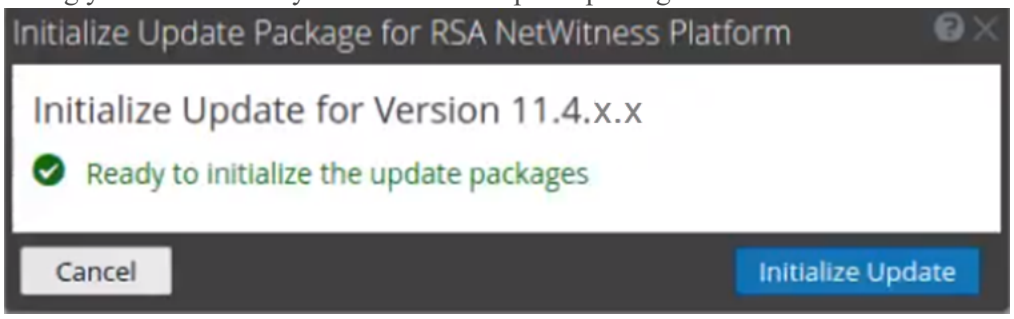
Error Message	
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.

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

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

Missing Update Packages Error

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

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

OpenSSL 1.1.x

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

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

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

Patch Update to Non-NW Server Error

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

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

Reboot Host After Update from Command Line Error

Error Message	You receive a message in the User Interface to reboot the host after you update and reboot the host offline. 
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Reporting Engine Restarts After Upgrade

Problem	In some cases, after you upgrade to 11.4 from versions of 11.x, such as 11.2 or 11.3, the Reporting Engine service attempts to restart continuously without success.
Cause	The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.
Solution	To resolve the issue, do the following: 1. Check which database files are corrupted: Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks: • If the live charts db file is corrupted, the following logs are displayed: Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • If the alert status db file is corrupted, the following logs are displayed:

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

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

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

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

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

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

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

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

   a. Stop the Reporting Engine service.

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

   c. Restart the Reporting Engine service.

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

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

   a. Stop the Reporting Engine service.

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

   c. Restart the Reporting Engine service.

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

Log Collector Service (`nwlogcollector`)

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

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

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

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

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

NW Server

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

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

Orchestration

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

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

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

Reporting Engine Service

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

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