



Upgrade Guide

for RSA NetWitness® Platform 11.5.1



Contact Information

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

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

December 2020

Contents

Upgrade Overview	6
Upgrade Paths	6
Running in Mixed Mode	6
Upgrade Considerations for ESA Hosts	6
Upgrade Considerations for ESA Analytics	7
Upgrade Considerations for STIX Custom Feeds	7
Change to Column Groups in the Events View	7
Upgrade or install Windows Legacy Collection	7
Feedback on Product Documentation	7
Getting Help with NetWitness Platform	8
Self-Help Resources	8
Contact RSA Support	8
Upgrade Preparation Tasks	9
Task 1. (Conditional) Upgrade External Repository	9
Task 2. (Optional) Remove Legacy Package Repositories	9
Task 3. (Optional) Ensure that Any Respond Normalization Script Customizations Are in the Custom Files	9
Upgrade Tasks	11
Upgrade Options	11
Option 1: User Interface Method with Connectivity to the Internet	12
Option 2: User Interface with No Connectivity to the Internet	13
Task 1. Populate Staging Folder (/var/lib/netwitness/common/update-stage/) with Version Upgrade Files	13
Task 2. Apply Upgrades from the Staging Area to Each Host	14
Upgrading from 11.3.1.0 or later except 11.4.0.0, 11.4.0.1	15
Upgrading from 11.4.0.0 or 11.4.0.1	15
Option 3: Command Line Interface (CLI) with No Connectivity to the Internet	16
Post Upgrade Tasks	17
Post Upgrade Tasks for Customers Upgrading from version 11.5.x.x	18
User Entity Behavior Analytics	18
Task 1- Update UEBA Configurations	18
Task 2- Update the User Entity Behavior Analytics Incident Rule Priority Thresholds, Grouping Options, and Title	20
Post Upgrade Tasks for Customers Upgrading From 11.3.x.x or 11.4.x.x	22
General	22
(Conditional) Configure NAT-Based IP Addresses	22

(Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts	22
Review Contents of /etc/hosts.user for Obsolete Host Entries	23
Reconfigure DNS Servers	23
Make Sure Services Have Restarted and Are Capturing and Aggregating Data	23
Event Stream Analysis (ESA)	24
New Health and Wellness	25
Deploy the New Health and Wellness Content from Live	25
(Optional) Update UUID of New Health and Wellness Host to Update Service Configuration Documents	25
(Optional) Uninstall New Health and Wellness	26
Investigate	30
(Conditional - For Custom Roles Only) Adjust investigate-server Permissions for Custom User Roles	30
Respond	31
(Conditional) Restore Any Respond Service Custom Keys in the Aggregation Rule Schema	31
(Conditional) Restore any Customized Respond Service Normalization Scripts	31
Update the User Entity Behavior Analytics Incident Rule Priority Thresholds, Grouping Options, and Title	33
Reference Log Decoder	34
Windows Log Collector	34
Update the Windows Log Collector UUID	34
Context Hub	34
Disable the UCF configuration	34
Update UEBA Configurations	35
Endpoint Upgrade Tasks	38
Install the 11.5 or Later Relay Server	38
Upgrade Endpoint Agents	38
Start Using New Features	39
Investigation - SIEM and Network Detection & Response	39
User Entity Behavior Analytics	40
Incident Response	40
Endpoint Investigation	40
Endpoint Configuration	40
Broker, Concentrator, Decoder and Log Decoder Services	40
Administration and Configuration	40
Log Collection	40
Logstash Integration	40
Licensing	40

Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface	41
External Repo Instructions for CLI upgrade	42
Appendix B. Troubleshooting Version Installations and Upgrades	44
deploy_admin User Password Has Expired Error	45
Downloading Error	46
Error Deploying Version <version-number> Missing Update Packages	47
Upgrade Failed Error	47
External Repo Update Error	49
Host Installation Failed Error	49
Host Update Failed Error	50
Missing Update Packages Error	51
OpenSSL 1.1.x	52
Patch Update to Non-NW Server Error	52
Reboot Host After Update from Command Line Error	53
Reporting Engine Restarts After Upgrade	53
Log Collector Service (nwlogcollector)	55
NW Server	56
Orchestration	57
Reporting Engine Service	57
Event Stream Analysis	57
ESA Troubleshooting Information	58
ESA Rules are Not Creating Alerts	58
Endpoint, UEBA, and Live Content Rules are Not Working	59
Example ESA Correlation Server Warning Message for Missing Meta Keys	60

Upgrade Overview

RSA NetWitness® Platform 11.5.1.0 provides enhancements and fixes for all products in NetWitness Platform. The instructions in this guide apply to both physical and virtual hosts (including AWS, Azure Public Cloud, and Google Cloud Platform) unless stated to the contrary.

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.5.1.0:

- RSA NetWitness® Platform 11.3.x.x to 11.5.1.0 *
- RSA NetWitness® Platform 11.4.x.x to 11.5.1.0
- RSA NetWitness® Platform 11.5.0.0 to 11.5.1.0
- RSA NetWitness® Platform 11.5.0.1 to 11.5.1.0

* If you are upgrading from 11.3.0.0, or 11.3.0.1, you must upgrade to 11.3.1.1 before you can upgrade to 11.5.1.0.

If you are upgrading from NetWitness Platform version (10.6.6.x) or (11.2.x.x or below), you must upgrade to 11.3.0.2 before you can upgrade to 11.5.1.0. For more information, see the [guides](#) that apply to your environment.

For upgrading from 11.3.0.0, or 11.3.0.1, see the [Upgrade Guide for RSA NetWitness Platform 11.3.1.1](#). This guide applies to both physical and virtual hosts (including AWS and Azure Public Cloud).

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.

Note: If you are running Endpoint Log Hybrid in mixed mode, make sure Endpoint Broker is on the same version as one of the Endpoint Servers.

Upgrade Considerations for ESA Hosts

Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later.

IMPORTANT: The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

Upgrade Considerations for ESA Analytics

The Event Stream Analytics Server (ESA Analytics) service is not supported or available in NetWitness Platform version 11.5 and later. The Whois Lookup Configuration and ESA Analytics Mapping panels



are no longer in the user interface ((Admin) > System).

Note: Event Stream Analysis (ESA) is not end of life. ESA Correlation rules and the ESA Correlation service are supported. ESA Analytics, which is used for Automated Threat Detection, is different from ESA Correlation Rules and is EOL. In its place, you can use ESA Correlation as it offers more functional capabilities and better performance.

Upgrade Considerations for STIX Custom Feeds

The custom feeds created before version 11.5 are processed automatically. On upgrade, the data sources created for ADHOC, REST and TAXII server and the feeds are pulled automatically. See "Create a STIX Custom Feed" in the *RSA NetWitness Platform Live Service Management Guide* and "Configure STIX as a Data Source" in the *RSA NetWitness Platform Context Hub Configuration Guide* for further information.

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.

If you are upgrading from version 11.4.0.0 or later, after you upgrade to 11.5.1.0, 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.

Upgrade or install Windows Legacy Collection

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.

Feedback on Product Documentation

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

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness Platform:

- See the documentation for all aspects of NetWitness Platform here:
<https://community.rsa.com/community/products/netwitness/documentation>
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here:
<https://community.rsa.com/welcome>
- See the RSA NetWitness® Platform Knowledge Base:
<https://community.rsa.com/community/products/netwitness/knowledge-base>
- See Troubleshooting the RSA NetWitness® Platform:
<https://community.rsa.com/community/products/netwitness/documentation/troubleshooting>
- See also [RSA NetWitness® Platform Blog Posts](#).
- If you need further assistance, contact RSA Support.

Contact RSA Support

If you contact RSA Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the RSA NetWitness Platform product or application you are using.
- The type of hardware you are using.

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

RSA Link	https://community.rsa.com In the main menu, click My Cases .
International Contacts (How to Contact RSA Support)	https://community.rsa.com/docs/DOC-1294
Community	https://community.rsa.com/community/support

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Platform 11.5.1.0.

Task 1. (Conditional) Upgrade External Repository

Note: Perform the below steps only if you are using an external repository for 11.5.1.

To upgrade the external repository which is an externally managed server:

Upgrade the external repository with the latest upgrade content for the RSA `netwitness-11.5.1.0.zip`.

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the *11.5 Upgrade Guide for RSA NetWitness Platform*. The following instructions assume that you already have an external repository set up. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

Task 2. (Optional) Remove Legacy Package Repositories

Perform this task to free up space by removing unused repositories from previous releases from your system.

1. Determine the version of the oldest NetWitness Platform host in your environment by reviewing the host list in the Admin user interface, or by running the following command on the NW Server:
`upgrade-cli-client --list`
2. You can safely remove all legacy package repository folders located at `/var/netwitness/common/repo/<version>` on the NW Server for all versions prior the baseline major release version of the oldest active host in the environment.
 - If the oldest host version is 11.4.x.x (for example, 11.4.1.0), you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, and 11.3.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.4.0.0.**
 - If the oldest host version is 11.3.x.x, you can safely remove 11.0.x.x, 11.1.x.x, and 11.2.x.x repository folders. However, do not remove repository versions greater than or equal to 11.3.0.0.

Task 3. (Optional) Ensure that Any Respond Normalization Script Customizations Are in the Custom Files

Note: This task applies to upgrades from NetWitness Platform version 11.4.x.x to 11.5.1.0.

For upgrades from 11.4.x.x to 11.5.x.x, there are no backups of the normalization script files since customizations are added to separate `custom_normalize` script files. These script files are in the `/var/lib/netwitness/respond-server/scripts` directory. If you have any customizations, add them to the normalization files with the `custom` prefix.

Upgrade Tasks

Important Notes - Read the following First

- **Synchronize Time on Component Hosts with NW Server Host**

Before upgrading your 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*.
- Perform the following steps on each host:
 - a. SSH to a component host.
 - b. Run the following commands.

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

- **Mixed Mode Unsupported for ESA Hosts**

Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

- **Endpoint Hybrid Systems Not Supported**

For RSA NetWitness Endpoint customers only, Endpoint Hybrid is not supported in 11.3.0.0 and later releases.

If you have deployed an Endpoint Hybrid host in 11.2.x.x and did not install an Endpoint Log Hybrid host in 11.3.x.x or 11.4.x.x, you must install an Endpoint Log Hybrid host in 11.5.x.x. See the *Physical Host Installation Guide for RSA NetWitness Platform* or the *Virtual Host Installation Guide for RSA NetWitness Platform* for instructions on how to install an 11.5.x.x Endpoint Log Hybrid on a physical host.

- **Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 11.5 or Later**

After upgrading the primary NW Server (including the Respond Server service), the Respond Server service is not automatically re-enabled until after the Primary ESA host is also upgraded to 11.5 or later. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Upgrade Options

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

- [Option 1: User Interface Method with Connectivity to the Internet](#)
- [Option 2: User Interface with No Connectivity to the Internet](#) (available for upgrades from 11.3.1 or later)
- [Option 3: Command Line Interface \(CLI\) with No Connectivity to the Internet](#)

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



- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.
- The NW Server, ESA primary, ESA secondary, and Analyst UI hosts must all be on the same NetWitness Platform version.

Option 1: User Interface Method with Connectivity to the Internet


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

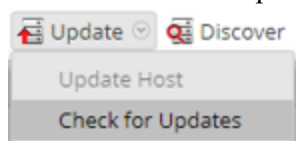
Prerequisites

Make sure that:


1. The **Automatically download information about new upgrades every day** option is selected and is applied in  (Admin) > System > Updates.
2. Updates are available. Go to  (Admin) > Hosts > Update > Check for Updates to check for updates. The Host view displays the **Update Available** status.
3. 11.5.1.0 is available in the **Update Version** column.

Procedure

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



4. **Update Available** is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.
5. Select **11.5.1.0** from the **Update Version** column. If you:

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

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

Option 2: User Interface with No Connectivity to the Internet

Caution: The offline User Interface method is only available if you are upgrading a host from version 11.3.1.0 or later, except for 11.4.0.0 and 11.4.0.1 (please see the caution below regarding offline UI method for 11.4.0.0 and 11.4.0.1). If you are upgrading a host on an earlier version, you must use the [Upgrade Tasks](#) method. After you complete Step 5 in [Task 2. Apply Upgrades from the Staging Area to Each Host](#), go to [Upgrading from 11.3.1.0 or later except 11.4.0.0, 11.4.0.1](#).

Caution: If you are upgrading a host from 11.4.0.0 or 11.4.0.1 to 11.5.1.0 using the offline User Interface method, in Step 5 of [Task 2. Apply Upgrades from the Staging Area to Each Host](#), the upgrade will fail with the message **Download error**. You can still complete the upgrade successfully by following the steps in [Upgrading from 11.4.0.0 or 11.4.0.1](#). This issue has been fixed in 11.4.1.0 and later.

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

1. Download the upgrade package from RSA Link (<https://community.rsa.com/>) > Downloads > NetWitness Platform > Version 11.5 to a local directory:
 - If you are upgrading from 11.3.x.x or 11.4.x.x, download `netwitness-11.5.0.0.zip` and `netwitness-11.5.1.0.zip`
 - If you are upgrading from 11.5.x.x, download `netwitness-11.5.1.0.zip`
2. SSH to the NW Server host.
3. Copy `netwitness-11.5.1.0.zip` (and `netwitness-11.5.0.0.zip` if upgrading from 11.3.x.x or 11.4.x.x) from the local directory to the `/var/lib/netwitness/common/update-stage/`

staging folder.

Example, if you are upgrading from 11.5.x.x to 11.5.1.0

```
sudo cp /tmp/netwitness-11.5.1.0.zip /var/lib/netwitness/common/update-stage/
```

Example, if you are upgrading from 11.3.x.x or 11.4.x.x to 11.5.1.0


```
sudo cp /tmp/netwitness-11.5.1.0.zip /var/lib/netwitness/common/updatestage/
```

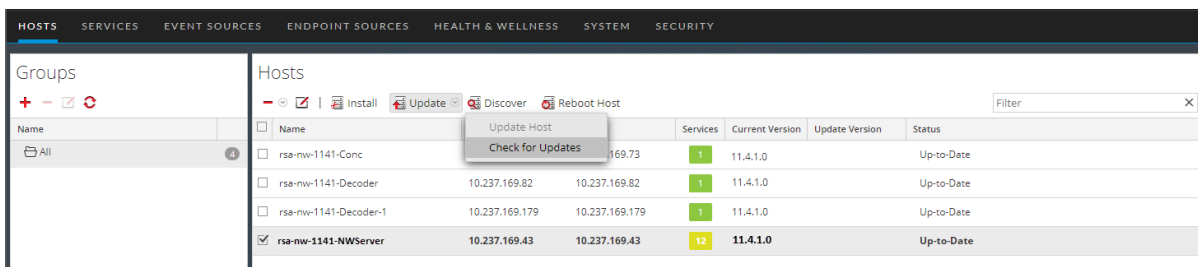
```
sudo cp /tmp/netwitness-11.5.0.0.zip /var/lib/netwitness/common/updatestage/
```

Note: NetWitness Platform unzips the file automatically.

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

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

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



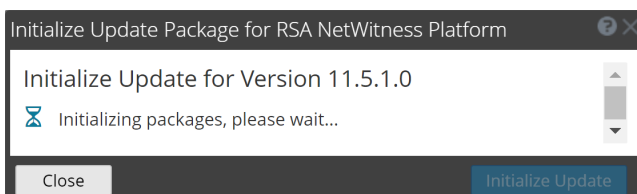
Name	IP Address	Services	Current Version	Update Version	Status
rsa-nw-1141-Conc	10.237.169.73	1	11.4.1.0		Up-to-Date
rsa-nw-1141-Decoder	10.237.169.82	1	11.4.1.0		Up-to-Date
rsa-nw-1141-Decoder-1	10.237.169.179	1	11.4.1.0		Up-to-Date
rsa-nw-1141-NWServer	10.237.169.43	12	11.4.1.0		Up-to-Date

"Ready to initialize packages" is displayed if:

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

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

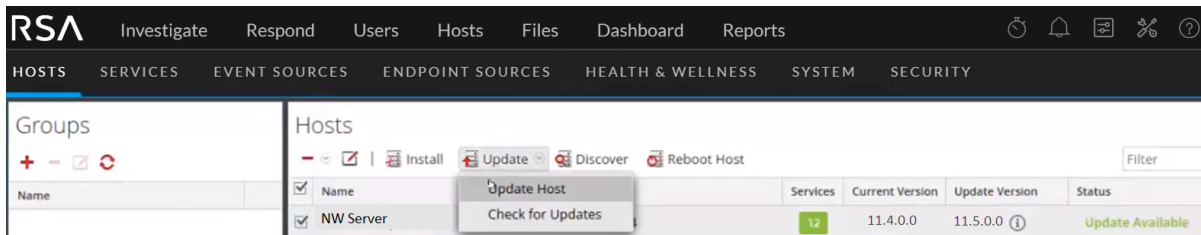
4. Click **Initialize Update**.



It takes some time to initialize the packages because the files are large and need to be unzipped. The time varies depending on how the host is configured.

After the initialization is successful, the **Status** column displays **Update Available** and you complete the rest of the steps in this procedure to finish the upgrade of the host.

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



Upgrading from 11.3.1.0 or later except 11.4.0.0, 11.4.0.1

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

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

Upgrading from 11.4.0.0 or 11.4.0.1

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

1. In the Command Line Interface (CLI):
 - a. SSH to NW Server.
 - b. Run the following command:


```
upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.5.1.0
```
2. After the NW Server is successfully updated, log in to the NW Server user interface and go to **(Admin) > Hosts**, where you are prompted to reboot the host.
3. Click **Reboot Host** from the toolbar.

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

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

Option 3: Command Line Interface (CLI) with No Connectivity to the Internet

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

Post Upgrade Tasks

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

- [Post Upgrade Tasks for Customers Upgrading from version 11.5.x.x](#)
- [Post Upgrade Tasks for Customers Upgrading From 11.3.x.x or 11.4.x.x](#)

Post Upgrade Tasks for Customers Upgrading from version 11.5.x.x

Complete the tasks that apply to the hosts in your environment.

User Entity Behavior Analytics

Task 1- Update UEBA Configurations

Perform the following steps after upgrading the UEBA to version 11.5.1.0.

IMPORTANT: In order to complete an upgrade process, every UEBA upgrade needs to be followed by upgrade steps.
In case of gradual upgrade, follow the instruction of each upgrade's guide before continuing to the next upgrade.

Note: The Modeled Behaviors functionality is added to UEBA in 11.5.1. For any reason if you need to disable this functionality for your organization, see "Enable or Disable the Modeled Behaviors for Users" topic in the *NetWitness UEBA Configuration Guide*.

1. (For Virtual Machines Only) Update the airflow parallelism on VM.
If the UEBA system is running on VM, update the airflow parallelism to be 64 by running the following command as root from the UEBA host.

```
sed -i "s|parallelism = 256|parallelism = 64|g" /var/netwitness/presidio/airflow/airflow.cfg
```
2. Update the UEBA configuration using the following command as root from the UEBA machine.

```
python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_server_config.py
```
3. (Optional) Update the UEBA processing schemas:

Note: Adding a UEBA schema does not require to re-run the UEBA system if it was upgraded from version 11.5.0.

To add a new UEBA schema, run the following command from the UEBA host.

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

where <SCHEMA> string is the schema that you can replace from the following list:

AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY, and TLS.


4. Run the airflow upgrade DAG.

Pool	Slots	Used Slots	Queued Slots
retention_spring_boot_jar_pool	8	0	0
default_pool	256	0	0
spring_boot_jar_pool	22	20	0

Task 2- Update the User Entity Behavior Analytics Incident Rule Priority Thresholds, Grouping Options, and Title

In NetWitness 11.5.1, the Entity Behavior Analytics incident rule default priority threshold ranges are now consistent with the severity ranges in NetWitness UEBA. The rule also captures user entity behavior grouped by both UEBA Classifier Id and UEBA Entity Name. The incident name created by the rule uses the UEBA Entity Name.

It is important to update the User Entity Behavior Analytics incident rule priority thresholds for matched incidents, grouping options, and incident title to the 11.5.1 default values.


1. Go to  (**Configure**) > **Incident Rules** and in the Incident Rules list, double-click the **User Entity Behavior Analytics** incident rule.
2. In the **Grouping Options – Group By** field, add **UEBA Entity Name**. You should have both UEBA Classifier Id and UEBA Entity Name.

ACTION* CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT
 Group into an Incident Suppress the Alert

GROUPING OPTIONS

GROUP BY*

TIME WINDOW 1 Hours

Advanced Grouping Options
 Choose grouping behavior if incoming alert does not contain the "Group By" field 

Group all alerts missing "Group By" fields into a single incident over the time window.
 (This may result in incidents with alerts that do not belong together)

Do not group alerts.
 (Alerts will still be generated, but will not be aggregated into incidents automatically)

INCIDENT OPTIONS

TITLE*

3. In the **Incident Options – Title** field, change `${groupByValue1}` to `${groupByValue2}: ${ruleName} for ${groupByValue2}`
4. In the **Incident Options – Priority** section, update the **Critical**, **High**, **Medium**, and **Low** priority thresholds to the default values.

Priority Threshold	Default Value
Critical	98

Priority Threshold	Default Value
High	93
Medium	85
Low	1

For example, with the Critical priority now set to 98, incidents with a risk score of 98 or higher are assigned a Critical priority for this rule.

The screenshot shows a configuration window titled "PRIORITY" with the instruction "Use the following to set the priority for the incident". There are three radio button options: "Average of Risk Score across all of the Alerts" (selected), "Highest Risk Score available across all of the Alerts", and "Number of Alerts in the time window". To the right, a list of priority levels is shown with corresponding colored bars and input fields: Critical (red) with value 98, High (orange) with value 93, Medium (yellow) with value 85, and Low (green) with value 1. A red rectangular box highlights the Critical, High, and Medium priority settings.

5. Click **Save**.

Post Upgrade Tasks for Customers Upgrading From 11.3.x.x or 11.4.x.x

Complete the tasks that apply to the hosts in your environment.

- [General](#)
- [Event Stream Analysis \(ESA\)](#)
- [New Health and Wellness](#)
- [Investigate](#)
- [Respond](#)
- [Reference Log Decoder](#)
- [Windows Log Collector](#)
- [Context Hub](#)
- [User Entity Behavior Analytics](#)

General

(Conditional) Configure NAT-Based IP Addresses

If you have a host, such as a VLC, that requires a NAT-based IP address in order to connect to the NW Server host, you must update the host configuration with the following steps.

1. Log in to the host that requires the use of NAT IP addresses, using the console or SSH.
2. Run the following command:
`nw-manage --enable-nat-usage`
3. To set the NAT address for the NW Server:
 - a. Log into the NW Server using the console or SSH.
 - b. Run the following command:
`nw-manage -update-host --host-id <UUID of NW Server> --ipv4-public <NAT IP of NW Server>`

Note: You can find the UUID and view the current NAT IP address of the host by running `nw-manage --list-hosts`.

(Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts

The Warm-Standby server must be upgraded to 11.5 or later before completing the following steps.

1. Log in to the NW Server using the console or SSH.
2. Run the following command:

```
nw-manage --add-nws-secondary-ip --ipv4 <ip address of Warm/Standby Server>
```

Note: If the Warm-Standby server requires a NAT-based IP address (IPv4-public) for any host to access it during failover, the NAT IP address must also be registered by running the following command: `nw-manage --add-nws-secondary-ip --ipv4 <NAT-based IP address of Warm Standby Server>`

3. Verify the correct Warm Standby host IP address value by running the following command:

```
nw-manage --get-nws-secondary-ip
```

Review Contents of `/etc/hosts.user` for Obsolete Host Entries

After upgrading the NW Server host or a component host, review the contents of the `/etc/hosts.user` file for any obsolete host entries. The `/etc/hosts.user` file contains system and user-generated entries that are not managed by NetWitness Platform. However, entries from `/etc/hosts.user` are merged with NetWitness Platform-generated host mappings to create and update `/etc/hosts`. To avoid conflicts with NetWitness Platform-generated mappings, and to avoid generating connectivity errors resulting from an IP address change, RSA recommends that you remove any entries in `/etc/hosts.user` that include a non-loopback IP address of a NetWitness Platform host.

After updating `/etc/hosts.user`, you must refresh the system by running the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

Reconfigure DNS Servers

By default, a component host upgraded from 11.4 or earlier is configured with the same system DNS server as the NW Server. If this component host requires a different system DNS address, see "Change Host Network Configuration" in the *System Maintenance Guide* for instructions.




Make Sure Services Have Restarted and Are Capturing and Aggregating Data

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




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

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver




Start Network Capture

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

Start Log Capture

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

Start Aggregation

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

Event Stream Analysis (ESA)

Note: Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

There are no required post-upgrade tasks for ESA. For ESA troubleshooting, see [ESA Troubleshooting Information](#).

If you want to add support for Endpoint, UEBA, and Live content rules, you must update the `multi-valued` and `single-valued` parameter meta keys on the ESA Correlation service to include all the required meta keys. It is not necessary to make these adjustments during the upgrade; you can make the adjustments later at a convenient time. For detailed information and instructions, see "Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys" in the *ESA Configuration Guide*.



New Health and Wellness

Note: New Health and Wellness in 11.5.x.x replaces Next GEN Health and Wellness (BETA) in 11.4.x.x.

Deploy the New Health and Wellness Content from Live

After you upgrade from version 11.4.x.x to 11.5.1.0, New Health and Wellness content is not updated. To use the latest (default) content, you must deploy the content through NetWitness Live Services.

Note: RSA recommends you to take a copy of 11.4.x.x Health and Wellness content before you deploy the content from NetWitness Live Services, as it overwrites the existing content.

1. Log in to NetWitness Platform UI.
2. Click  (CONFIGURE) > LIVE CONTENT.
3. In the **Search Criteria** panel, select the **Resource Types** as:
 - Health and Wellness Dashboards
 - Health and Wellness Monitors
4. Click **Search**.
5. In the **Matching Resources** view, select the checkbox to the left of the resources that you want to deploy.
6. In the **Matching Resources** toolbar, click  **Deploy**.
7. In the **Deployment Wizard** > **Resources** tab, click **Next**.
8. In the **Services** tab, select the Metrics Server service.
9. Click **Next**.
10. Click **Deploy**.
The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.
11. Click **Close**.

(Optional) Update UUID of New Health and Wellness Host to Update Service Configuration Documents

If you have configured services for New Health and Wellness from `nw-shell` using `set-config` API and upgrade NetWitness Platform version from 11.4.x.x to 11.5.1.0, you must update IP with UUID for a host on which New Health and Wellness is installed.

1. SSH to Admin Server.
2. Check the UUID of a host on which New Health and Wellness is installed using the command:

```
orchestration-cli-client --list-hosts
```

This lists NetWitness Platform hosts along with the respective UUIDs. Make a note of the UUID of host on which New Health and Wellness is installed.

3. Identify the services on which set-config is invoked using the command:

```
mongo localhost/metrics-server -u deploy_admin -p <deployment_password> --
authenticationDatabase admin --eval 'db.metric_config.find({ "createdBy": {
  $ne: "system" }})'
```

This will list the configuration documents of the services on which set-config is invoked.

Note: If no service documents are listed which means no services are configured before the upgrade, so you can ignore the remaining steps.

4. In the configuration file, update the service document “host” field by replacing IP with the UUID of the host on which New Health and Wellness is installed.

For example, update the host IP with UUID as below:

```
"host" : "e086511c-121c-4e66-95a3-e87e27b12acb"
```

5. Log in to nw-shell using the command:

```
nw-shell
```

6. Connect to metrics-server service using the command:

```
connect --service metrics-server
```

7. Enter the log in command:

```
login
```

8. Enter the admin username and password.

9. Go to /rsa/metrics/elastic/set-config and invoke configuration files using the command:

```
invoke --file /<absolute_path_of_service_config_file>
```

(Optional) Uninstall New Health and Wellness

To uninstall New Health and Wellness, perform the following:

1. Take a backup of NetWitness Server host. For more information, see “Disaster Recovery (Back Up and Restore)” topic in the *NetWitness Recovery Tool User Guide*.

```
nw-recovery-tool --export --dump-dir /some/folder --category AdminServer --
category Search
```

Note: If New Health and Wellness is not installed on NetWitness Server, you must take a backup of the host on which New Health and Wellness is installed.

2. Make sure that the installation or upgrades are not in progress and stop the orchestration server on NetWitness Server host:

```
systemctl stop rsa-nw-orchestration-server
```

3. Remove the New Health and Wellness service category (“Search”) from the host:

- a. SSH to Admin server
- b. Fetch host details where New Health and Wellness is installed using the following command:


```
mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
password> --authenticationDatabase admin --eval 'db.host.find({
"installedServices": /.?Search.*/i })'
```

Sample output

```
{ "_id" : "56f2a90b-1f03-d09a-fb71-42c2a93958a8", "hostname" :
"10.10.10.11", "ipv4" : "10.10.10.11", "ipv4Public" : "", "displayName"
: "adminserver", "version" : { "major" : 11, "minor" : 5, "servicePack"
: 0, "patch" : 0, "snapshot" : false, "rawVersion" : "11.5.1.0" },
"lastFailedRefreshAttempt" : NumberLong(0), "refreshAttemptDelayFactor"
: 0, "thirdParty" : false, "installedServices" : [ "Search",
"AdminServer" ], "meta" : { "node-zero" : true }, "_class" :
"com.rsa.asoc.orchestration.host.HostEntity" }
```

- c. Remove the "Search" from the installedServices.

IMPORTANT: Do not remove any other category names.

- d. Replace <LIST-OF-CATEGORIES-EXCEPT-SEARCH> with a comma-delimited AND double-quoted list of all the existing installed services found earlier EXCEPT "Search":


```
mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
password> --authenticationDatabase admin --eval 'db.host.update({ "_id"
: "<hw-node-uuid>" },{$set: {"installedServices" : [ <LIST-OF-
CATEGORIES-EXCEPT-SEARCH> ]}})'
```

Example

```
mongo localhost/orchestration-server -u deploy_admin -p netwitness --
authenticationDatabase admin --eval 'db.host.update({ "_id" : "56f2a90b-
1f03-d09a-fb71-42c2a93958a8" },{$set: {"installedServices" : [
"AdminServer" ]}})'
```

Sample output

```
MongoDB shell version v4.0.19

connecting to: mongod://localhost:27017/orchestration-
server?authSource=admin&gssapiServiceName=mongod

Implicit session: session { "id" : UUID("04e32380-347e-4b7d-a63e-
a094536d7242") }

MongoDB server version: 4.0.19

WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
```

- e. Make sure that the "Search" category is removed in the updated host record in the installedServices :

```
mongo localhost/orchestration-server -u deploy_admin -p <deploy_admin-
password> --authenticationDatabase admin --eval 'db.host.find({ "_id" :
"<hw-node-uuid>" })'
```

Example

```
mongo localhost/orchestration-server -u deploy_admin -p netwitness --
authenticationDatabase admin --eval 'db.host.find({ "_id" : "56f2a90b-
1f03-d09a-fb71-42c2a93958a8" })'
```

Note: Any inconsistencies can result in unrecoverable errors.

Sample output

```
{ "_id" : "56f2a90b-1f03-d09a-fb71-42c2a93958a8", "hostname" :
"10.10.10.11", "ipv4" : "10.10.10.11", "ipv4Public" : "", "displayName" :
"adminserver", "version" : { "major" : 11, "minor" : 5, "servicePack" : 0,
"patch" : 0, "snapshot" : false, "rawVersion" : "11.5.1.0" },
"lastFailedRefreshAttempt" : NumberLong(0), "refreshAttemptDelayFactor" :
0, "thirdParty" : false, "installedServices" : [ "AdminServer" ], "meta" :
{ "node-zero" : true }, "_class" :
"com.rsa.asoc.orchestration.host.HostEntity" }
```

4. Stop the New Health and Wellness services:

```
systemctl stop rsa-nw-metrics-server elasticsearch opendistro-performance-
analyzer kibana
```

5. Disable the New Health and Wellness services:

```
systemctl disable rsa-nw-metrics-server elasticsearch opendistro-performance-
analyzer kibana
```

6. Uninstall the New Health and Wellness packages using the command:

```
yum erase -y rsa-nw-metrics-server opendistroforelasticsearch
opendistroforelasticsearch-kibana
```

Note: `rsa-nw-shell` (installed with metrics server) is a shared package and should not be removed.

7. Remove the configuration folders or files:

- `/etc/netwitness/metrics-server`
- `/etc/netwitness/platform/elasticsearch`
- `/etc/netwitness/platform/nodeinfo/metrics-server`
- `/etc/netwitness/platform/nodeinfo/elasticsearch-open-distro`
- `/etc/netwitness/platform/nodeinfo/kibana-open-distro`
- `/etc/systemd/system/rsa-nw-metrics-server.service.d`
- `/etc/systemd/system/elasticsearch.service.d`
- `/etc/pki/nw/service/bootstrap/metrics-server.completed`
- `/etc/pki/nw/service/rsa-nw-metrics-server-cert.pem`
- `/etc/pki/nw/service/rsa-nw-metrics-server.chain`
- `/etc/pki/nw/elastic`
- `/etc/pki/nw/kibana`
- `/var/log/netwitness/metrics-server`
- `/var/log/kibana`
- `/etc/collectd.d/rsa-metrics-server.conf`
- `/etc/logrotate.d/kibana`
- `/etc/elasticsearch`

- /etc/kibana
- /var/lib/elasticsearch
- /var/lib/kibana
- /var/netwitness/elasticsearch

8. Start the orchestration Server on NetWitness Server:
`systemctl start rsa-nw-orchestration-server`

9. Unregister the New Health and Wellness from the `installedService`:

- a. Find the service IDs for `metrics-server`, `elasticsearch-open-distro`, and `kibana-open-distro`

Note: Make sure you look for service IDs for the correct host; do not unregister elastic or kibana on an UEBA host.

```
orchestration-cli-client --list-services | grep <hw-node-IP-address>
```

Sample output

```
ID=50082d04-320c-4ce2-8379-00f38ae2d1df, NAME=metrics-server,  
HOST=192.168.1.2:7018, TLS=true
```

```
ID=530ff46a-8793-4e8e-be9c-742193d1705a, NAME=elasticsearch-open-distro,  
HOST=192.168.1.2:9200, TLS=true
```

```
ID=4bad6ea8-e3a4-46ab-a342-34356bea65bb, NAME=kibana-open-distro,  
HOST=192.168.1.2:5601, TLS=true
```

```
... (other services) ...
```

- b. Remove the service IDs returned above for `metrics-server`, `elasticsearch-open-distro`, and `kibana-open-distro` (associated with New Health new Wellness host):

```
orchestration-cli-client --remove-service --id <metrics-server-service-id>
```

```
orchestration-cli-client --remove-service --id <elasticsearch-open-distro-service-id>
```

```
orchestration-cli-client --remove-service --id <kibana-open-distro-service-id>
```

- c. Verify if the services are removed:

```
orchestration-cli-client --list-services | grep <hw-node-IP-address>
```

10. On all hosts, except for UEBA, stop and disable `metricbeat`:

```
systemctl stop metricbeat
```

```
systemctl disable metricbeat
```

Note: For NetWitness Platform without UEBA, you can stop and disable `metricbeat` on all hosts through salt:

```
salt '*' cmd.run 'systemctl stop metricbeat && systemctl disable metricbeat'
```

11. (Optional) - If you are not reinstalling New Health and Wellness (on same or other hosts), you can also remove `metricbeat` package and configuration:

- a. Package to uninstall:
metricbeat
 - b. Service configurations to uninstall:
 - /etc/metricbeat
 - /var/log/metricbeat
 - mongo account
 - systemd configuration
12. Refresh the New Health and Wellness host:
nw-manage --refresh-host --host-key <node-ip>
Make sure that the New Health and Wellness service is not installed or running and metricbeat service is not active on the New Health and Wellness host.
13. If you are not reinstalling New Health and Wellness on another host, you must refresh UI hosts (NetWitness Server host and Analyst UI) to update NGNIX:
nw-manage --refresh-host --host-key <node-ip>

Note: After uninstalling New Health and Wellness, if you want to install New Health and Wellness again, see "New Health and Wellness" in the *Deployment Guide*.

Investigate



(Conditional - For Custom Roles Only) Adjust investigate-server

Permissions for Custom User Roles

If you are upgrading from a version prior to 11.5, after upgrading to version 11.5 or later, the built-in user roles for analysts (and others) using Investigate have the `investigate-server.event.filter` permission enabled, but the upgrade process does not enable the permission for custom user roles. Users who are assigned a custom user role that does not have this permission enabled cannot see the Filter Events panel, a new panel in 11.5.x.x where they can drill into metadata.

Note: When upgrading from Version 11.3.x.x or earlier, the built-in user roles for analysts using Investigate have three additional permissions added in Version 11.4 enabled, but the upgrade process does not enable the permissions for custom user roles. Users who are assigned a custom user role that does not have these permissions cannot see the Navigate view and Legacy Events view in the Investigate menu. The three permissions that need to be enabled for custom user roles are: `investigate-server.columngroup.read`, `investigate-server.metagroup.read`, and `investigate-server.profile.read`

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 four permissions are enabled:
`investigate-server.event.filter`
`investigate-server.columngroup.read`
`investigate-server.metagroup.read`
`investigate-server.profile.read`
4. Click **Save** to save your changes. When analysts with the custom user role log in to the NetWitness Platform, the changes are in effect.

Respond

The Primary ESA server must be upgraded to 11.5.1.0 or later before you can complete these tasks.

Note: After upgrading the primary NW Server (including the Respond Server service), the Respond Server service is not automatically re-enabled until after the Primary ESA host is also upgraded to 11.5.1.0. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

(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>`

(Conditional) Restore any Customized Respond Service Normalization Scripts

Note: If you did not manually customize any alert normalization scripts, you can skip this task. This procedure applies to upgrades from 11.3.x to 11.5.1.0. (For upgrades from 11.4.x to 11.5.1.0, there are no backups of the normalization script files since customizations are in separate `custom_normalize` script files, which are not overwritten during the upgrade.)

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

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

```

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

```

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

```

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

```

For Example, the `custom_normalize_core_alerts.js` is the normalization script for ESA to add any custom logic. This java script file has a function 'normalizeAlert' with the parameters `headers`, `rawAlert`, and `normalizedAlert`. The variable 'normalized' is an immutable copy object, which has an embedded object of a 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.

```

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);
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;
};


```

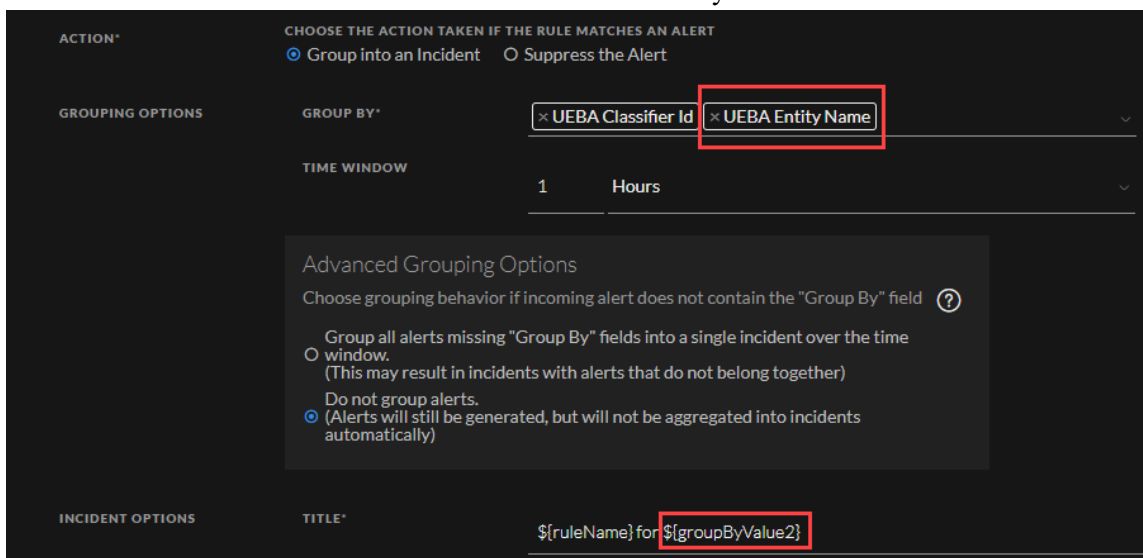
You can also look at the built-in Respond normalization script files for reference, such as `normalize_alerts.js`. For more information, see "Configure Custom Respond Server Alert Normalization" in the *NetWitness Respond Configuration Guide*.

Update the User Entity Behavior Analytics Incident Rule Priority Thresholds, Grouping Options, and Title

In NetWitness 11.5.1, the Entity Behavior Analytics incident rule default priority threshold ranges are now consistent with the severity ranges in NetWitness UEBA. The rule also captures user entity behavior grouped by both UEBA Classifier Id and UEBA Entity Name. The incident name created by the rule uses the UEBA Entity Name.

It is important to update the User Entity Behavior Analytics incident rule priority thresholds for matched incidents, grouping options, and incident title to the 11.5.1 default values.

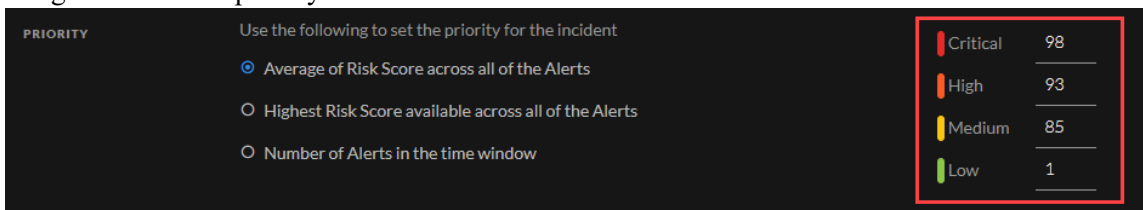
1. Go to  (Configure) > Incident Rules and in the Incident Rules list, double-click the **User Entity Behavior Analytics** incident rule.
2. In the **Grouping Options – Group By** field, add **UEBA Entity Name**. You should have both UEBA Classifier Id and UEBA Entity Name.



3. In the **Incident Options – Title** field, change `${groupByValue1}` to `${groupByValue2}: $ {ruleName} for $ {groupByValue2}`
4. In the **Incident Options – Priority** section, update the **Critical, High, Medium, and Low** priority thresholds to the default values.

Priority Threshold	Default Value
Critical	98
High	93
Medium	85
Low	1

For example, with the Critical priority now set to 98, incidents with a risk score of 98 or higher are assigned a Critical priority for this rule.



5. Click **Save**.

Reference Log Decoder

For full functionality, make sure your reference Log Decoder is at 11.5 or later. If you never set up a reference Log Decoder, there is no need to take action. For details, see the *Log Parser Customization Guide*.

Windows Log Collector

Update the Windows Log Collector UUID

After upgrading to 11.5 or later, for each Windows Log Collector configured in your environment, run the following command on the NW Server:

```
wlc-cli-client --update-to-uuid --host <WLC host address>
```

Context Hub

Disable the UCF configuration

Disable the UCF (Unified Collection Framework) configuration to stop sending events to NetWitness Platform. Do the following steps.

1. On the UCF host, stop the UCF services (SA SecOps Watchdog, RSA Unified Collector Framework). For more information, see "Manage Unified Collector Framework" topic in *Archer Integration Guide for RSA NetWitness Platform*.

2. Create a backup of the `collector-config.properties` file which is in the following location.
`C:\Program Files\RSA\SA IM integration service\config`
3. In the `collector-config.properties` file, comment the lines that starts with `"archer.ArcherPull.baseUrl = xxx"` by adding `#` character before the line.
For example,

```
#archer.ArcherPull.baseUrl = xxx  
#archer.ArcherPull.instance = xxx  
#archer.ArcherPull.userName = xxx  
#archer.ArcherPull.password = xxx  
#archer.ArcherPull.readWrite = xxx  
#archer.ArcherPull.moduleId.dataBreach = xxx  
#archer.ArcherPull.moduleId.incident = xxx
```
4. Also delete the value `"ArcherPull"` in all the lines. For example, for the line `"archer.configured.endpoints = ArcherPull,ArcherPush"`, delete `"ArcherPull"` but retain the other values. `"archer.configured.endpoints = ArcherPush"`
5. Start the UCF services (SA SecOps Watchdog, RSA Unified Collector Framework). For more information, see "Manage Unified Collector Framework" topic in *Archer Integration Guide for RSA NetWitness Platform*.

Update UEBA Configurations

IMPORTANT: In order to complete an upgrade process, every UEBA upgrade needs to be followed by upgrade steps.
In case of gradual upgrade, follow the instruction of each upgrade's guide before continuing to the next upgrade.

IMPORTANT: The UEBA system requires a re-run in the following cases:
(a) When removing a UEBA schema.
(b) When the UEBA is upgraded from 11.3.x or from a lower version.
The UEBA system does not require a re-run in case of upgrading from 11.4.x or higher version (even in case of adding a schema).

Note: The Modeled Behaviors functionality is added to UEBA in 11.5.1. For any reason if you need to disable this functionality for your organization, see "Enable or Disable the Modeled Behaviors for Users" topic in the *NetWitness UEBA Configuration Guide*.

1. (For Virtual Machines Only) Update the airflow parallelism on VM.
If the UEBA system is running on VM, update the airflow parallelism to be 64 by running the following command as root from the UEBA host.

```
sed -i "s|parallelism = 256|parallelism = 64|g"  
/var/netwitness/presidio/airflow/airflow.cfg
```
2. Update the UEBA configuration using the following command as root from the UEBA machine.

```
python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-  
packages/presidio_workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_  
server_config.py
```

3. (Optional) Update the UEBA processing schemas:

- **In case of upgrade from 11.4.x or higher versions:**

To add a new UEBA schema, run the following command from the UEBA host.

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

where <SCHEMA> string is the schema that you can replace from the following list:

AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY, and TLS.

- **In case of upgrade from 11.3.x or lower versions:**

Upgrade from version 11.3.x or lower requires re-run of the UEBA system.

RSA recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

Use the `reset_presidio.py` script to update the UEBA system, by running the following commands from the UEBA host:

```
source /etc/sysconfig/airflow
source $AIRFLOW_VENV/bin/activate

OWB_ALLOW_NON_FIPS=on python
/var/netwitness/presidio/airflow/venv/lib/python2.7/site-
packages/presidio_workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_
presidio.py --help
```

For more information about the script, see "reset-presidio script" section in the *NetWitness UEBA Configuration Guide*.

4. Run the airflow upgrade DAG.

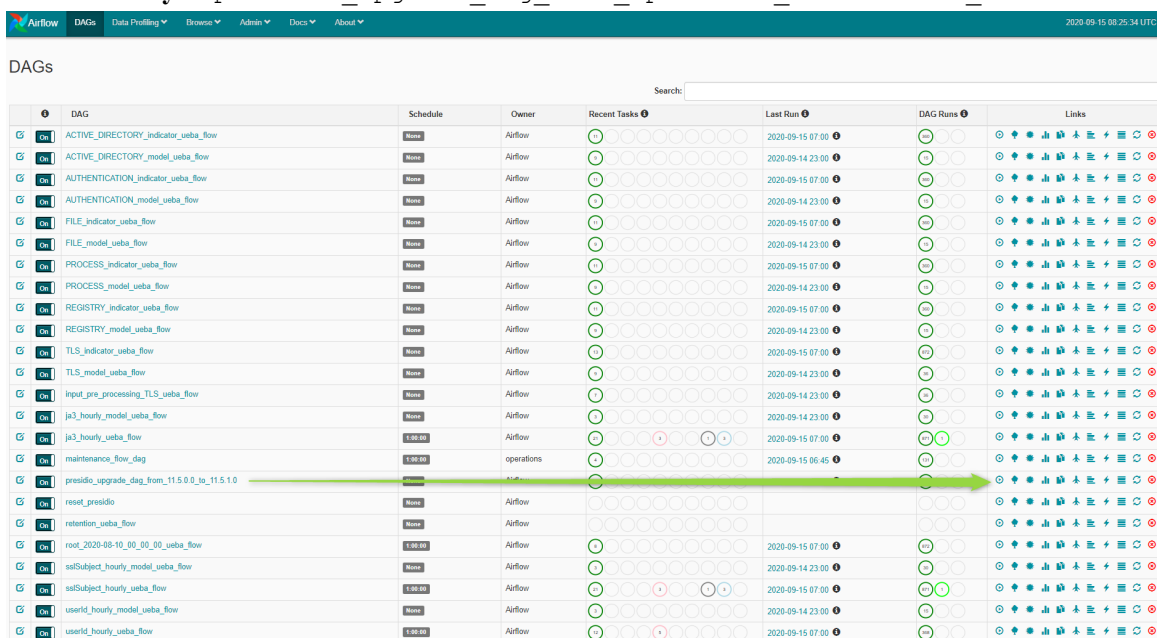
Note: An error message may appear at the top of the Airflow home page until the post upgrade process is complete.

- a. Go to Airflow main page <https://<UEBA-host-name>/admin> and enter the credentials.

User: admin

Password: The environment deploy admin password.

- b. Click the **Play** in `presidio_upgrade_dag_from_<previous_version> to_11.5.1.0`.

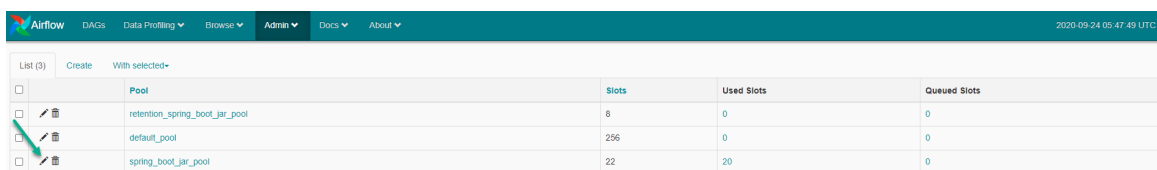


Note: A light green circle will appear next to the upgrade DAG row during the upgrade. If the upgrade process is completed successfully the light green circle changes to green. If the upgrade process fails, the light green circle changes to red.

5. Set the appropriate Boot Jar Pools according to the setup.
 - **Physical Appliance:** Update the `spring_boot_jar_pool` slot value be 18.
 - **Virtual Appliance:** Update the `spring_boot_jar_pool` slot values to 22.

To update the number of Spring Boot Jar Pools:

- a. Go to the Airflow main page `https://<UEBA_host>/admin` and enter the credentials.
 - User:** admin
 - Password:** The environment deploy admin password.
- b. Click the **Admin > Pools**.
- c. Edit the `spring_boot_jar_pool` and update the slots amount.



Endpoint Upgrade Tasks

Install the 11.5 or Later Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 11.5 or later by downloading the Relay Server installer from the upgraded Endpoint Server. For more information see "(Optional) Installing and Configuring Relay Server" section in the *Endpoint Configuration Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.
2. Restart the Endpoint Server using the command:

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

Upgrade Endpoint Agents

See "Upgrade Agents" in the *Endpoint Agent Installation Guide for NetWitness Platform 11.5* for instructions on how to upgrade agents.

Start Using New Features

There are many exciting new features that you can enable after you have upgraded to 11.5.1.0. The following is a list of the new features for each area of NetWitness Platform. For a detailed description of the new features in this release, see the *Release Notes for RSA NetWitness Platform 11.5.1.0*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

- [Investigation - SIEM and Network Detection & Response](#)
- [User Entity Behavior Analytics](#)
- [Incident Response](#)
- [Endpoint Investigation](#)
- [Endpoint Configuration](#)
- [Broker, Concentrator, Decoder and Log Decoder Services](#)
- [Administration and Configuration](#)
- [Log Collection](#)
- [Logstash Integration](#)
- [Licensing](#)

To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents: <https://community.rsa.com/docs/DOC-81328>.

Investigation - SIEM and Network Detection & Response

- JSON Viewer for Logs
- Investigation Using the Event Time
- Manual Column Width Adjustments Automatically Apply
- Option to Add Multiple Filters Prior to Query
- New Icons for Meta Keys
- Optimized Loading of Springboard Panels
- Expanded Network Visibility with Endpoint Data Enrichment
- Improved Meta Group Usage while Filtering Events
- Performance Improvements while Filtering Events
- Option to Download Files from Multiple Events
- Enhanced Events Query Experience
- User Experience Improvements while Filtering Events

User Entity Behavior Analytics

- Introduction of Modeled Behaviors for Users

Incident Response

- Improved the User Entity Behavior Analytics Incident Rule

Endpoint Investigation

- Extended Linux Agent Support with SUSE

Endpoint Configuration

- Added Option to Select CPU Utilization for Manual Scans

Broker, Concentrator, Decoder and Log Decoder Services

- Expanded Selective Network Data Collection
- N-gram Free-text Search Enabled by Default

Administration and Configuration

- RAID Configuration for PowerVault and DACs

Log Collection

- Enhanced JSON Mapping (BETA)

Logstash Integration

- NetWitness Export Connector

Licensing

- Enhanced License Details

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

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

Prerequisites

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

- If you are upgrading from an 11.3.x.x or 11.4.x.x release to 11.5.1.0, download:
`netwitness-11.5.0.0.zip`
`netwitness-11.5.1.0.zip`
- If you are upgrading from an 11.5.0.x release to 11.5.1.0 release, download:
`netwitness-11.5.1.0.zip`
- If you are using external repository, you can update the external repository with the latest upgrade content. For more information, see [External Repo Instructions for CLI upgrade](#).

Procedure

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

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

1. Stage the 11.5.1.0 files to prepare them for the upgrade.
 - **If you are upgrading from 11.3.x.x or 11.4.x.x**, you must stage 11.5.0.0 and 11.5.1.0. Log into the NW Server as `root` and create the following directories:
`/tmp/upgrade/11.5.0.0`
`/tmp/upgrade/11.5.1.0`
and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:
`unzip netwitness-11.5.0.0.zip -d /tmp/upgrade/11.5.0.0`
`unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0`
 - **If you are upgrading from 11.5.0.0 to 11.5.1.0**, you only need to stage 11.5.1.0. Log into the NW Server as `root` and create the following directory:
`/tmp/upgrade/11.5.1.0`
and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:
`unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0`

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

2. Initialize the upgrade, using the following command:
`upgrade-cli-client --init --version 11.5.1.0 --stage-dir /tmp/upgrade`
3. Upgrade the NW Server host, using the following command:
`upgrade-cli-client --upgrade --host-<id/name/addr> <ID / display name / (hostname/ IP address)> --version 11.5.1.0`
4. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
5. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being upgraded.

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

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

External Repo Instructions for CLI upgrade

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the *11.5 Upgrade Guide for RSA NetWitness Platform*. The following instructions assume that you already have an external repository set up. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

1. Stage the 11.5.1.0 files to prepare them for the upgrade:
 - **If you are upgrading from 11.3.x.x or 11.4.x.x**, you must stage 11.5.0.0 and 11.5.1.0. Log into the NW Server as `root` and create the following directories:
`/tmp/upgrade/11.5.0.0`
`/tmp/upgrade/11.5.1.0`
 and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:
`unzip netwitness-11.5.0.0.zip -d /tmp/upgrade/11.5.0.0`
`unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0`
 - **If you are upgrading from 11.5.0.x to 11.5.1.0**, you only need to stage 11.5.1.0. Log into the NW Server as `root` and create the following directory:
`/tmp/upgrade/11.5.1.0`
 and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:
`unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0`

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

2. Initialize the upgrade, using the following command:
`upgrade-cli-client --init --version 11.5.1.0 --stage-dir /tmp/upgrade`
3. Upgrade the NW Server host using the following command:
`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.5.1.0`
4. When the NW Server host upgrade is successful, reboot the host from NetWitness UI.
5. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being upgraded.

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

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

Appendix B. Troubleshooting Version Installations and Upgrades

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

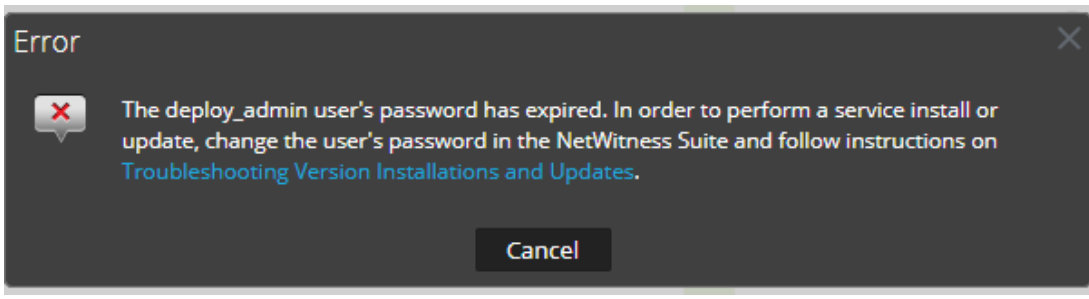
Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

- [deploy_admin Password Expired Error](#)
- [Downloading Error](#)
- [Error Deploying Version <version-number> Missing Update Packages](#)
- [Upgrade Failed Error](#)
- [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](#)

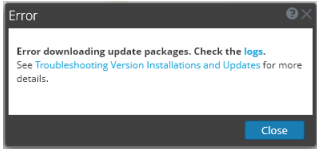
Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

- [Log Collector Service](#)
- [NW Server](#)
- [Orchestration](#)
- [Reporting Engine](#)
- [Event Stream Analysis](#)

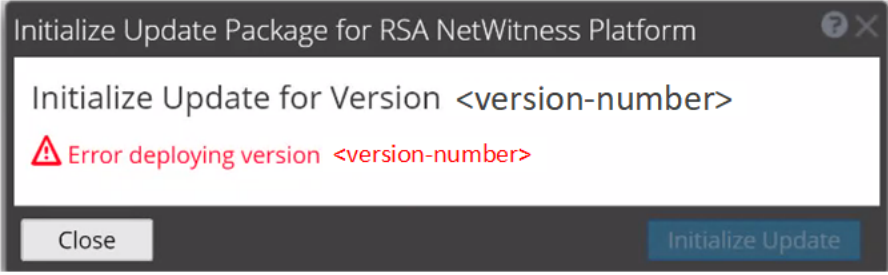
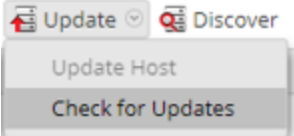
deploy_admin User Password Has Expired Error

Error Message	
Cause	The <code>deploy_admin</code> user password has expired.
Solution	<p>Reset your <code>deploy_admin</code> password.</p> <ol style="list-style-type: none">1. On the NW Server host only, run the following command. <pre>nw-manage --update-deploy-admin-pw</pre>Please enter the new <code>deploy_admin</code> account password: <new-deploy-admin-password> Please confirm the new <code>deploy_admin</code> account password: <new-deploy-admin-password>2. Review the output of the <code>nw-manage --update-deploy-admin-pw</code> command to verify the <code>deploy_admin</code> password was successfully updated on all hosts. If an NW host is down or fails for any reason as displayed by the output of the <code>nw-manage --update-deploy-admin-pw</code> command, run <code>nw-manage --sync-deploy-admin-pw --host-key <host-identifier></code> to synchronize the password between the NW Server and the host that failed once the communication failure is resolved.3. On the host that failed installation or orchestration, run the <code>nwsetup-tui</code> 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	<ol style="list-style-type: none">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 <i>Upgrade Guide for NetWitness Platform 11.5</i>. 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	<p>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.</p>
Solution	<ol style="list-style-type: none"> 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.

Upgrade Failed Error

Error Message	<p>While updating/installing a device to version 11.2 or above, the following error can occur and be found in <code>/var/log/netwitness/config-management/chef-solo.log</code>:</p> <pre> [2019-04-16T20:55:32+00:00] ERROR: Running exception handlers [2019-04-16T20:55:32+00:00] ERROR: Exception handlers complete [2019-04-16T20:55:32+00:00] FATAL: Stacktrace dumped to /var/lib/netwitness/config-management/cache/chef-stacktrace.out [2019-04-16T20:55:32+00:00] FATAL: Please provide the contents of the stacktrace.out file if you file a bug report [2019-04-16T20:55:32+00:00] ERROR: ruby_block[resolve ips] (nw-dns-client::config line 69) had an error: Resolv::ResolvError: no address for 889e5752-6ae3-4286-33f4ccbc [2019-04-16T20:55:32+00:00] FATAL: Chef::Exceptions::ChildConvergeError: Chef run process exited unsuccessfully (exit code 1) </pre>
----------------------	---

Cause	<p>The reason can be because the target host is unable to communicate to the Admin Server on port 53 as it is attempting to use the dnsmasq service on the Admin Server to resolve, in this case, 889e5752-6ae3-4286-a944-c182 33f4ccbc. This is the salt minion id of the admin server. You can see this by running "cat /etc/salt/minion" on the Admin Server to compare. Example output:</p> <pre>[root@S5-NWAdmin ~]# cat /etc/salt/minion master: localhost hash_type: sha256 log_level: info id: 889e5752-6ae3-4286-a944-c18233f4ccbc</pre>
Solution	<p>If possible, configure any firewalls between the target host and the Admin Server host to be able to communicate on port 53. If this is not possible, the workaround is to include the minion id in the /etc/host file on the component hosts and starting in the 11.4 release, modify the chef recipe not to overwrite this workaround.</p>
Workaround	<p>Refer to Install/Upgrade fails in RSA NetWitness Platform because Resolv::ResolvError: no address for a particular host KB Article.</p>

Error Message	<p>Received an error in the error log similar to the following when trying to update to version 11.5.1 :</p> <pre>FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt</pre>
Cause	<p>Custom builds/rpms installed for certain components installed on hosts, such as in the case of installing Hotfixes.</p>
Solution	<p>To resolve the issue, follow the below steps.</p> <ol style="list-style-type: none"> 1. SSH to Admin Server. 2. Locate the component descriptor file by running the following command. <pre>cd /etc/netwitness/component-descriptor/</pre> 3. Open the component descriptor file by running the following command. <pre>vi nw-component-descriptor.json</pre> 4. Search for “packages” section for the component you have custom build/rpm. For example, below shown is the package details for “concentrator” host that has custom build/rpm. <pre>"concentrator": { "cookbook_name": "rsa-concentrator", "service_names": ["rsa-nw-concentrator"], "family": "launch", "default_port": xxxx, "description": "Concentrator", "packages": [{ "name": "rsa-nw-concentrator", "version" : "11.5.1.0-2003001075220.5.cecf24b.e.17.centos" }, },</pre> 5. Delete the complete version details including (,) character in the packages section. For

example, it should look like as shown below after you delete the version details.

```
"packages": [{
  "name": "rsa-nw-concentrator"
},
```

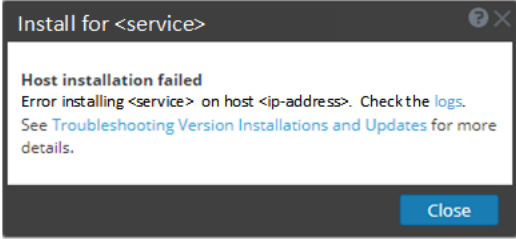
Note: You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.

6. Run the upgrade process again.

External Repo Update Error

Error Message	Received an error similar to the following error when trying to update to a new version from the : <pre>.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 ""</pre>
Cause	There is an error the path you specified.
Solution	Make sure that: <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 1. Try to install the service again. Often this is all you need to do. 2. If you still cannot install the service: <ol style="list-style-type: none"> a. Monitor the following logs on NW Server as it progresses (for example, submit the <code>tail -f</code> command string from the command line'): <pre>/var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log</pre>

```

/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

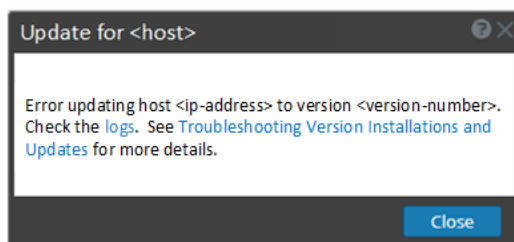
```

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	Initialize Update for Version xx.x.x.x Missing the following update package(s) Download Packages from RSA Link
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	<ol style="list-style-type: none"> 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 the missing packages from the staging folder. The Initialize Update Package for RSA NetWitness Platform dialog is displayed telling you that it is ready to initialize the update packages.

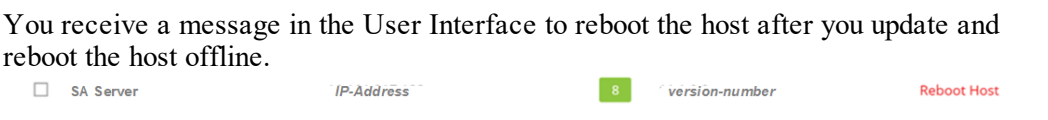
OpenSSL 1.1.x

Error Message	<p>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:</p> <pre>\$ ssh root@10.1.2.3 ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect</pre>
Problem	<p>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:</p> <pre>\$ rpm -q openssl openssl-1.1.1-8.el8.x86_64</pre>
Solution	<p>Specify the compatible cipher list on the command line. For example:</p> <pre>\$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3</pre> <p>I've read & consent to terms in IS user agreement.</p> <pre>root@10.1.2.3's password: Last login: Mon Oct 21 19:03:23 2019</pre>

Patch Update to Non-NW Server Error

Error Message	<p>The <code>/var/log/netwitness/orchestration-server/orchestration-server.log</code> has an error similar to the following error:</p> <pre>API Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported</pre>
Problem	<p>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 11.5.0.0, the only update path for the non-NW Server hosts is the same version (that is, 11.5.0.0). 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.x.x) you will get this error.</p>
Solution	<p>You have two options:</p> <ul style="list-style-type: none"> • Update the non-NW Server host to 11.5.0.0, 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 11.5 from versions of 11.x, such as 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	<p>To resolve the issue, do the following:</p> <ol style="list-style-type: none"> Check which database files are corrupted: <ul style="list-style-type: none"> Navigate to the file located at <code>/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log</code> and check the following blocks: <ul style="list-style-type: none"> If the live charts db file is corrupted, the following logs are displayed: <pre>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!</pre> If the alert status db file is corrupted, the following logs are displayed: <pre>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'</pre>

- 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]
```

- To resolve the live charts database file corruption, perform the following steps:
 - Stop the Reporting Engine service.
 - Move the `livechart.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` folder to a temporary location.
 - 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:

- Stop the Reporting Engine service.
- 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.
- Restart the Reporting Engine service.

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

Problem	After you upgrade to version 11.5, the Reporting Engine service does not restart.
Cause	<p>The Reporting Engine service may not start due to any of the following reasons.</p> <ul style="list-style-type: none"> - workspace.xml not updated. - Time is not converted properly in livechart h2 database. - JCR (Jackrabbit repository) is corrupted with primary key violation.
Solution	<p>To resolve the issue, run the Reporting Engine Migration Recovery tool (<code>rsa-nw-re-migration-recovery.sh</code>) on the Admin Server where the Reporting Engine service is installed.</p> <p>Note: You can find the Reporting Engine Migration Recovery tool in the below location. <code>/opt/rsa/soc/reporting-engine-11.5.0.0-<Tag>/nwtools</code></p> <ol style="list-style-type: none"> SSH to Admin Server. Untar the RE (Reporting Engine) tool, run the following command. <pre>tar -xvf rsa-nw-re-recovery-tool-bundle.tar</pre> (Optional) If you want to untar the RE tool file in some other directory, you can create a directory and untar the RE tool. Run the following commands. <pre>mkdir <NAME OF THE DIRECTORY> tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY></pre>

4. Run the script, run the following command.

```
./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh
```

For more information, see the Knowledge Base article **Reporting Engine Migration Recovery Tool**.

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	<code><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.</code>
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 <i>Log Collection Configuration Guide</i> .

Error Message	<code><timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
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 <i>Log Collection Configuration Guide</i> .

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 <i>Log Collection Configuration Guide</i> .

Error Message	Decoder tries to start capture events but fails. <pre>Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.</pre>
Solution	To resolve the issue, do the following steps, <ol style="list-style-type: none"> 1. SSH to the Decoder host. 2. Run the following commands. <pre>yum reinstall pfring* systemctl restart nwdecoder</pre>

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 <code>sa.log</code> . Syslog Configuration migration failed. Restart jetty service to fix this issue
Cause	NW Server Global Audit setup migration failed to migrate from 11.3.x.x. to 11.5.0.0.
Solution	<ol style="list-style-type: none"> 1. SSH to the NW Server. 2. Submit the following command. <pre>orchestration-cli-client --update-admin-node</pre>

Orchestration

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

Problem	<ol style="list-style-type: none"> 1. Tried to upgrade a non-NW Server host and it failed. 2. Retried the upgrade for this host and it failed again.
Cause	<p>You will see the following message in the <code>orchestration-server.log</code>. <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p> <p>Salt minion may have been upgraded and never restarted on failed non-NW Server host</p>
Solution	<ol style="list-style-type: none"> 1. SSH to the non-NW Server host that failed to upgrade. 2. Submit the following commands. <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> 3. Retry the upgrade of the non-NW Server host.



Reporting Engine Service

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

Error Message	<pre><timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB >] is less than the required space [<required-GB>]</pre>
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 <i>Reporting Engine Configuration Guide</i> for instructions on how to free up disk space.

Event Stream Analysis

Problem	After upgrading to version 11.5, the ESA correlation server does not aggregate events from the configured data sources.
Error Message	<pre>Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)</pre>
Solution	To resolve the issue, do the following steps. In the NetWitness Platform user interface,

1. Go to  (**Configure**) > **ESA Rules**.
ESA Rules panel is displayed with **Rules** tab open.
2. In the Rules tab options panel, under Deployments, select a deployment.
3. In the **Data Sources** section, select the data source and click  in the toolbar.
4. In the **Edit Service** dialog, type the password for that data source.
5. Click the **Test Connection** button to make sure that it can communicate with the ESA service and then click **OK**.


Note: Do the above procedure for all the configured data sources.

6. After you finish making changes to the deployment, click **Deploy Now** to redeploy the ESA rule deployment.

ESA Troubleshooting Information


ESA Rules are Not Creating Alerts

If you are not seeing any alerts, 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.

The screenshot displays the 'ESA - ESA Correlation' configuration page. It is divided into several sections:

- Engine Stats:** Shows Esper Version 8.2.0, Time 2019-12-11T22:18:06, Events Offered 11406057584, Offered Rate 62,222 per second / 335,898 max, and Status Active.
- Rule Stats:** Shows 99 Rules Enabled and 1 Rule Disabled.
- Alert Stats:** Shows 0 Notifications and 0 Message Bus.
- Deployed Rule Stats:** A table listing rules with columns for Enable, Name, Rule Type, Trial Rule, Last Detected, Events Matched, and Memory Usage. The first rule, 'No Log Traffic Detected from Device in Given Time...', is highlighted in red.

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`.

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

Endpoint, UEBA, and Live Content Rules are Not Working

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

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

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

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

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

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

To update your meta keys, see "Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules" in the *ESA Configuration Guide*.

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

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

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

Example ESA Correlation Server Warning Message for Missing Meta

Keys

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