RSA NetWitness

Version 11.7.1

Upgrade Guide

NETWITNESS

Contact Information

NetWitness Community at https://community.netwitness.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 NetWitness Community. 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.

January 2023

Contents

Upgrade Overview

NetWitness 11.7.1.0 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 11.7.1.0:

- NetWitness 11.5.3.2 to 11.7.1.0
- NetWitness 11.5.3.3 to 11.7.1.0
- NetWitness 11.6.0.0 to 11.7.1.0
- NetWitness 11.6.1.0 to 11.7.1.0
- NetWitness 11.6.1.1 to 11.7.1.0
- NetWitness 11.6.1.2 to 11.7.1.0
- NetWitness 11.6.1.3 to 11.7.1.0
- NetWitness 11.7.0.0 to 11.7.1.0
- NetWitness 11.7.0.1 to 11.7.1.0
- NetWitness 11.7.0.2 to 11.7.1.0

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 version 11.6 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 STIX Custom Feeds

The custom feeds created before version 11.6 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.

Upgrade or install Windows Legacy Collection

Refer to the Windows Legacy Collection Guide for RSA NetWitness 11.x.

> **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 nwdocsfeedback@rsa.com to provide feedback on NetWitness 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:

- See the documentation for all aspects of NetWitness here:
  https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation

- Use the **Search** and **Ask it** fields in NetWitness Community to find specific information here:
  https://community.netwitness.com/

- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base

- See Troubleshooting section in the Guides.

- See also RSA NetWitness® Platform Blog Posts.

- If you need further assistance, contact RSA NetWitness Support.

Contact RSA NetWitness Support

If you contact RSA NetWitness 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.

NetWitness Community	https://community.netwitness.com/
	In the main menu, click **Support** > **Case Portal** > **View My Cases**.
International Contacts (How to Contact RSA NetWitness Support) Community	https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897 https://community.netwitness.com/t5/support/ct-p/support

Pre Upgrade Checks

You must run the pre-upgrade checks before you upgrade to NetWitness 11.7.1 to identify any issues that may result in upgrade failure.

To run the pre-upgrade checks, perform the following:

1. Log in to Admin console.

2. Run the following command:
   `nw-precheck-tool upgrade-checklist`

   The pre-upgrade checks verifies the following:

   - **(Component Hosts) Node X Service Status** - Verifies the status of services (Active or In Active) on all the Node X.

   - **(Component Hosts) Node X Certificates Check** - Checks the certificate expiry, missing, corrupted, and issuer mismatch in all categories of Node X.

   - **CPU-Memory Info** - Provides CPU and Memory details along with the real-time available memory.

   - **(Admin Server) Node 0 File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness` and `root` on Node 0.

   - **(Component Hosts) Node X File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness` and `root` for ESA Primary, Endpoint Log Hybrid, and UEBA services on Node X.

   - **Mongo File (ESAPrimary)** - Checks the ESA Primary node in the system and verifies the permission mode of mongo file.

   - **Orchestration Server Normal Mode** - Checks if the orchestration service is running in normal or safe mode.

   - **(Admin Server) Node 0 Init status** - Checks if there are any issues that might fail init process.

   - **(Admin Server) Node 0 closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node 0.

   - **(Component Hosts) Node X closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node X.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness 11.7.1.0.

Task 1. (Conditional) Upgrade External Repository

> **Note:** Perform the below steps only if you are using an external repository for 11.7.1.0

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

Upgrade the external repository with the latest upgrade content for the RSA `netwitness-11.7.1.0.zip`.

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the 11.7.0.0 *Upgrade Guide for RSA NetWitness Platform*. The following instructions assume that you already have an external repository set up. Go to the NetWitness Documents - All Versions 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 11.6.x.x (for example, 11.6.1.0), you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, and 11.4.x.x, and 11.5.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.7.0.0.**

   - If the oldest host version is 11.7.x.x, you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, 11.4.x.x, 11.5.x.x, and 11.6.x.x repository folders. However, do not remove repository versions greater than or equal to 11.7.0.0.

Task 3. Uninstall the Security Analytics l10n language pack

Before upgrading to 11.6.x.x or 11.7.x.x versions from 11.5.x.x, you must uninstall the Security Analytics l10n language pack.

Upgrade Task

Upgrade the systems in your environment in the following order:

1. NW Server hosts

2. Analyst UI hosts

3. ESA Primary hosts

4. ESA Secondary hosts

5. The rest of your component hosts

> **Note:** NW Server, Analyst UI, and ESA Primary and Secondary hosts must all be upgraded on the same day. The rest of your component hosts can be upgraded on the same day or later.

For information about all the host types in NetWitness, see the *Host and Services Getting Started Guide for RSA NetWitness Platform 11.x*. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

Important Notes - Read This 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 ndpd
     ```

Mixed Mode Unsupported for ESA Hosts

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

Respond Server Service Not Enabled Until NW Server and Primary

ESA Host Upgraded to same version

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 same version. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Deploy_Admin Password Guidelines

In NetWitness Platform version 11.6 or Later, deployment account password (only on node-zero) must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.

If `deploy_admin` password is changed on Primary NW Server, it must be changed in the Warm Standby Server if it exists.

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

- 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. 11.7.1.0 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.
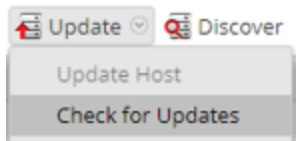
4. Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.

5. Select **11.7.1.0** 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

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

1. Make sure that you have downloaded the following file from NetWitness Community (https://community.netwitness.com/) > **Products > NetWitness Platform** > **Downloads** to a local directory:

   - If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.1.0, 11.6.1.1, 11.6.1.2 or 11.6.1.3, download `netwitness-11.7.0.0.zip` and `netwitness-11.7.1.0.zip`

   - If you are upgrading from 11.7.0.0, 11.7.0.1 or 11.7.0.2, download `netwitness-11.7.1.0.zip`

2. SSH to the NW Server host.

3. Copy `netwitness-11.7.1.0.zip` (and `netwitness-11.7.0.0.zip` if upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.1.0, 11.6.1.1, 11.6.1.2 or 11.6.1.3) from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.
   For example:
   sudo cp /tmp/netwitness-11.7.1.0.zip /var/lib/netwitness/common/update-stage/
   If you are logged as a root user you can ignore sudo in the command, for example,
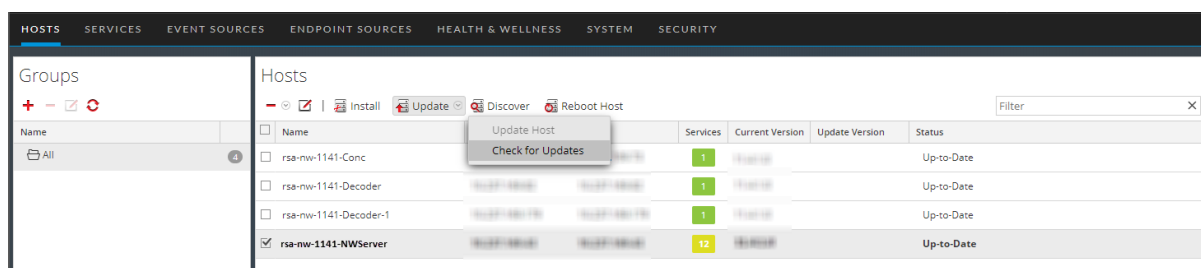
   cp /tmp/netwitness-11.7.1.0.zip /var/lib/netwitness/common/update-stage/

   Note: NetWitness Platform unzips the file automatically.

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

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

1. Log in to NetWitness.

2. Go to ⚒ (**Admin**) **> Hosts**.

3. Check for updates and wait for the upgrade packages to be copied, validated, and ready to be initialized.

"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.
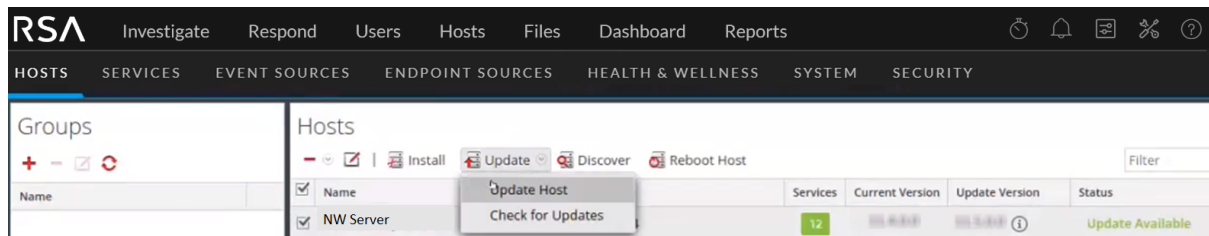
6. Click **Begin Update** from the Update Available dialog.
After the host is upgraded, it prompts you to reboot the host.

7. 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 11.7.x.x](#)
- [Post Upgrade Tasks for Customers Upgrading From 11.5.3.2 or 11.6.x.x](#)

Post Upgrade Tasks for Customers Upgrading from version 11.7.x.x

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

- General
- Platform
- Event Stream Analysis (ESA)
- 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>
```

Jetty Configuration

For Jetty Configuration and related information, see **Manage Custom Host Entries** topic in the *System Maintenance Guide*.

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

Platform

Enable Service Topology

To view the **Service Topology** Tab, you must ensure this feature is enabled under **Admin Server** > **Explorer** > **Feature**> **service-topology-feature**.

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*

Show Updates to an ESA Rule Deployment

You can view changes to an ESA rule deployment, such as adding or removing rules. When there is a change to a deployment, the update icon () appears next to the name of the deployment in the Rules tab options panel.

1. Go to (**Configure**) > **ESA Rules**.The Rules tab is displayed.

2. In the options panel, under **Deployments** click **Show Updates** on the far right.

3. Click **Deploy Now**.

If you are unable to deploy the ESA rule, see Known Issues for the workaround.

Respond

The Primary ESA server must be upgraded to 11.7.1.0 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 11.7.1.0. 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>`

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. 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*.

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.baseUri = xxx`" by adding # character before the line.
   For example,
   `#archer.ArcherPull.baseUri = 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*.

User Entity Behavior Analytics

> **IMPORTANT:** Before the upgrade, if you encountered and resolved the task failure issues, then after the upgrade, you must replace the `authentication.json` file before you run the post-upgrade tasks. The task failure issues in Airflow and their solutions are described in the 'Troubleshooting' topic of the *UEBA Configuration Guide*.

> **IMPORTANT:** Every UEBA deployment when upgraded requires additional steps to complete the upgrade process. When you upgrade from 11.6.x to 11.6.x.x, you must follow UEBA instructions in the Upgrade Guide for 11.6.x.x, before you upgrade to 11.7.x.

> **Note:** When you upgrade to 11.7.1.0 from 11.6.x.x, you don't need to rerun the UEBA system for the last 28 days, if you don't update the current processing schemas. When you upgrade to 11.7.1.0 from a version prior to 11.6.x, the UEBA system runs a rerun automatically.

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 from the UEBA machine.

   ```
   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/resources/rerun_ueba_server_config.py
   ```

3. (Optional) Update the UEBA processing schema, if needed:

   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.

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

4. Run the airflow upgrade DAG.

   - Go to Airflow main page `https://<UEBA-host-name>/admin`

   - Enter the admin username and password.

- Click the **Play** in `presidio_upgrade_dag_from_<previous_version> to_11.7.1.0.`

> **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" slots:

   - **Physical Appliance**: Update the `spring_boot_jar_pool` slot value be 18.

   - **Virtual Appliance**: Update the `spring_boot_jar_pool` slot value to 22.
     To update the **Spring Boot Jar Pools** slots, go to the Airflow main page, tap the **Admin** tab at the top bar and tap **Pools**.

   a. To access the Airflow UI, go to `https://<UEBA_host>/admin` and enter the credentials.
      User: admin
      Password: The environment deploy admin password.

   b. Click on the pencil mark of the Pools to update the slot values.

6. Edit the `spring_boot_jar_pool` and update the slots amount to 22.

Post Upgrade Tasks for Customers Upgrading From 11.5.3.2 or 11.6.x.x

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

- General
- Event Stream Analysis (ESA)
- New Health and Wellness
- Respond
- Reference Log Decoder
- Windows Log Collector
- Context Hub
- Update UEBA Configurations

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 Log Capture

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

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

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

4. In the toolbar, click

Start Aggregation

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

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

   a. Select the service.

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

   c. In the toolbar, click

Event Stream Analysis (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*

Show Updates to an ESA Rule Deployment

You can view changes to an ESA rule deployment, such as adding or removing rules. When there is a change to a deployment, the update icon () appears next to the name of the deployment in the Rules tab options panel.

1. Go to (**Configure**) > **ESA Rules**.The Rules tab is displayed.

2. In the options panel, under **Deployments** click **Show Updates** on the far right.

3. Click **Deploy Now**.

If you are unable to deploy the ESA rule, see Known Issues for the workaround.

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 11.5.3.2 to 11.7.1.0, 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 .

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 11.5.3.2 to 11.7.1.0, you must update IP with UUID for a host on which New Health and Wellness is installed.

This is an example of service configuration file with the file path `/root/example_config.json`

```
{
"service" : "concentrator",
"serviceId" : "6c552cde-4153-4e1b-a0a0-c74e8756cce1",
"enabled" : true,
"username" : "nwservice",
"password" : "4f809baabcbe7ed663c10e4cf786ce24",
"port" : 9200,
"secure" : true,
"host" : "196.168.0.1",
"verifyHostname" : false,
"conversionUnit" : "SECONDS",
"interval" : "60 SECONDS",
"exclusion" : [ ],
"inclusion" : [
"/concentrator/**",
"/database/**",
"/sdk/**",
"/sys/**"
]
}
```

To update UUID of a host:

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 API 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 API is invoked.

Sample output
```
{ "_id" : ObjectId("5f83f44b913a613985072396"), "port" : 0, "secure" :
true, "family" : "NEXTGEN", "service" : "concentrator", "enabled" : true,
"interval" : { "duration" : NumberLong(120), "unit" : "SECONDS" },
"inclusion" : [ "/concentrator/**", "/database/**", "/sdk/**", "/sys/**" ],
"exclusion" : [ "/concentrator/config/recovery/**",
"/concentrator/config/rules/**", "/concentrator/devices/**",
"/sdk/stats/queries/**", "/sys/config/scheduler/**" ], "forceDisabled" :
false, "createdBy" : "admin", "createdOn" : NumberLong("1602483359444"),
"lastModifiedBy" : "system", "lastModifiedOn" : NumberLong
("1604382316156"), "_class" :
"com.rsa.asoc.metrics.config.ElasticConfigUpdateEntity" }
```

> **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, "`host`" : "`196.168.0.1`" will become "`host`" : "`e28665d5-1c2c-dbe3-1b9e-4767271ce805`"

> **Note:** If you do not know the file used for configuration (For example, `/root/example_config.json`). You can create a new file containing the configuration of the service.
> To create new configuration file:
> 1) List all the services using the following command:
> `orchestration-cli-client --list-services`
> **Result**
> Service-ID of the service is displayed. For example,
> `2020-12-01 10:11:30.195 INFO 11535 --- [ main]`
> `c.r.n.i.o.c.OrchestrationApplication : Service: ID=60a97481-1568-4da1-b91a-`
> `e0f0b38836d4, NAME=concentrator, HOST=196.168.0.1:56005, TLS=true`
> 2) To get the current configuration of the same service run the following commands:
> a) SSH to Admin Server
> b) Log in to `nw-shell`
> c) Run the following command:
> `connect --service metrics-server`
> d) Navigate to the below location:
> `/rsa/metrics/elastic/get-config`
> e) Run the following command:
> `invoke <service_id> [example: invoke 60a97481-1568-4da1-b91a-e0f0b38836d4]`
> Result:
> `example_config.json`
> `{`
> `"service" : "concentrator",`
> `"serviceId" : "6c552cde-4153-4e1b-a0a0-c74e8756cce1",`
> `"enabled" : true,`
> `"username" : "nwservice",`
> `"password" : "4f809baabcbe7ed663c10e4cf786ce24",`
> `"port" : 9200,`
> `"secure" : true,`

```
"host" : "196.168.0.1",
"verifyHostname" : false,
"conversionUnit" : "SECONDS",
"interval" : "60 SECONDS",
"exclusion" : [ ],
"inclusion" : [
 "/concentrator/**",
 "/database/**",
 "/sdk/**",
 "/sys/**"
]
}
```
3) Copy the Configuration file above (For example, `/root/example2_config.json`) and save it in a file (For example, `/root/example2_config.json`).

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>
   ```
   For example, `invoke --file /root/example2_config.json`

Respond

The Primary ESA server must be upgraded to 11.7.1.0 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 11.7.1.0. 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>`

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. 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*.

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.baseUri = xxx`" by adding # character before the line.
   For example,
   `#archer.ArcherPull.baseUri = 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*.

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 11.5.2. 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 schema, using the following script:
   ```
   python
   /var/netwitness/presidio/airflow/venv/lib/python2.7/sitepackages/presidio_
   workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_presidio.pys
   ```

   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.

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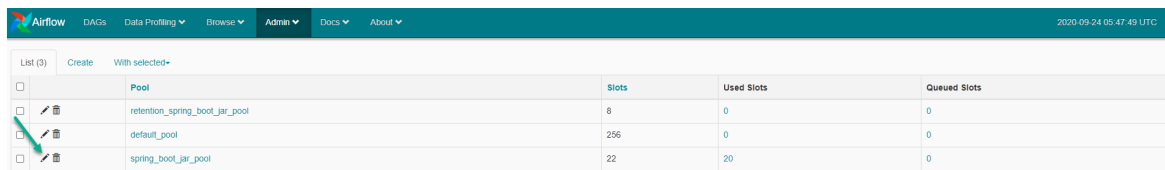
a. Go to Airflow main page `https://<UEBA-host-name>/admin` and enter the credentials. **User**: admin

   Password: The environment deploy admin password.

b. Click the **Play** in `presidio_upgrade_dag_from_<previous_version> to_11.7.1.0`.

> **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 value 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 11.7 or Later Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 11.7 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 NetWitness Documents - All Versions 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.x* 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 11.7.1.0. The following is a list of the new features for each area of NetWitness. For a detailed description of the new features in this release, see the *Release Notes for RSA NetWitness Platform 11.7.1.0*. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

The following sections are a complete list and description of enhancements to specific capabilities:

- Upgrade
- Investigation - SIEM and Network Traffic Analysis
- Endpoint Investigation
- Concentrator, Decoder, and Log Decoder Services
- Event Stream Analysis (ESA)
- Platform

Upgrade

- Pre-stage the upgrade repo to minimize downtime
- Support for Additional Pre-Upgrade Check Utility

Investigation - SIEM and Network Traffic Analysis

- Investigation Enhancements

Endpoint Investigation

- Capabilities for Detecting Ransomware That Use the Registry
- Endpoint Agent Support for macOS Monterey and Windows 11
- Support for Offline or Standalone Scans on Air-gapped Windows Hosts
- Support for Full System Scan
- Redesigned Alerts Tab for Optimized Navigation

Concentrator, Decoder, and Log Decoder Services

- Centralized Configuration Management Enhancements
- Enhanced Network Decoder to Support Load Balancing Deployments

Event Stream Analysis (ESA)

- Enhanced Performance when Retaining Incident Network Data Artifacts

Configuration Updates

- Feed Case Sensitivity

- NetWitness Topology Feature

Platform

- Backup and Restore CLI Improvements

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

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

Prerequisites

Make sure that you have downloaded the following file from NetWitness Community (https://community.netwitness.com/) > **Products > NetWitness Platform** > **Downloads** to a local directory:

- If you are upgrading from an 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.1.0, 11.6.1.1, 11.6.1.2 or 11.6.1.3 release to 11.7.1.0 release, download:
  ```
  netwitness-11.7.0.0.zip
  netwitness-11.7.1.0.zip
  ```

- If you are upgrading from an 11.7.0.0, 11.7.0.1 or 11.7.0.2 release to 11.7.1.0 release, download:
  ```
  netwitness-11.7.1.0.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 11.7.1.0 files to prepare them for the upgrade.

   - **If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.1.0, 11.6.1.1, 11.6.1.2 or 11.6.1.3**, you must stage 11.7.0.0, 11.7.1.0. Log into the NW Server as `root` and create the following directories:
     ```
     /tmp/upgrade/11.7.0.0
     /tmp/upgrade/11.7.1.0
     ```
     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-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0
     unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0
     ```

   - **If you are upgrading from 11.7.0.0, 11.7.0.1 or 11.7.0.2**, you only need to stage 11.7.1.0. Log into the NW Server as `root` and create the following directory:

     - **Option 1 (Manual)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:
       ```
       /tmp/upgrade/11.7.1.0
       ```
       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-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0
       ```

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.

- ○ **Option 2 (Automated)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:

  `/tmp/upgrade` and `/root/NW`

  and then copy the NetWitness 11.7.1.0 package zip files to the `/root/NW` directory of the NetWitness Server.

  After this, run the below command to extract, validate, and initialize the 11.7.1.0 zip files:

  `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.1.0`

  Here, `<download file path>` is the location where you need to copy the `netwitness-11.7.1.0.zip` if it is downloaded to the local directory earlier.

  For Example: `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path /root/NW --version 11.7.1.0`

  Once the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed** is displayed in the console of the admin server, only then the initialization process will begin.

> **Note:** If you do not receive the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed**, run the command `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.1.0` again to stage 11.7.1.0.

> **IMPORTANT:** After staging 11.7.1.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.7.1.0 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the step 2 Initialize the upgrade and proceed with the further steps in it.

2. Initialize the upgrade using the following command:
   `upgrade-cli-client --init --version 11.7.1.0 --stage-dir /tmp/upgrade`

3. Upgrade the NW Server host, using the following command:
   `upgrade-cli-client --upgrade --host-key <ID / display name / (hostname/ IP address)> --version 11.7.1.0`

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

5. (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 4 on the Warm Standby Server host.

6. 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.

External Repo Instructions for CLI upgrade

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the *11.7 Upgrade Guide for RSA NetWitness Platform*. The following instructions assume that you already have an external repository set up. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

1. Stage the 11.7.1.0 files to prepare them for the upgrade:

    - **If you are upgrading from 11.5.3.2, 11.6.0.0, 11.6.1.0, 11.6.1.1, or 11.6.1.2**, you must stage 11.7.0.0, 11.7.1.0. Log into the NW Server as `root` and create the following directories:

      `/tmp/upgrade/11.7.0.0`

      `/tmp/upgrade/11.7.1.0`

      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-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0`

      `unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0`

    - **If you are upgrading from 11.7.0.0 to 11.7.1.0**, you only need to stage 11.7.1.0. Log into the NW Server as `root` and create the following directory:

        ○ **Option 1 (Manual)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:

          `/tmp/upgrade/11.7.1.0`

          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-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0`

          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.

        ○ **Option 2 (Automated)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:

          `/tmp/upgrade` and `/root/NW`

          and then copy the NetWitness 11.7.1.0 package zip files to the `/root/NW` directory of the NetWitness Server.

          After this, run the below command to extract, validate, and initialize the 11.7.1.0 zip files:

          `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.1.0`

          Here, `<download file path>` is the location where you need to copy the `netwitness-11.7.1.0.zip` if it is downloaded to the local directory earlier.

          For Example: `[root@SA ~]# upgrade-cli-client --init --stage-dir`

```
/tmp/upgrade --download-path /root/NW --version 11.7.1.0
```
Once the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed** is displayed in the console of the admin server, only then the initialization process will begin.

> **Note:** If you do not receive the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed**, run the command `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.1.0` again to stage 11.7.1.0.

> **IMPORTANT:** After staging 11.7.1.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.7.1.0 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the step 2 Initialize the upgrade and proceed with the further steps in it.

2. Initialize the upgrade, using the following command:
```
upgrade-cli-client --init --version 11.7.1.0 --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 11.7.1.0
```

4. When the NW Server host upgrade is successful, reboot the host from NetWitness UI.

5. (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 4 on the Warm Standby Server host.

6. 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.

Appendix B. Set Up External Repo

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

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

1. (Conditional) Complete this step if you have an external repo and you want to override it.

   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.

     a. Create the `/etc/netwitness/platform/repobase` file.

        `vi /etc/netwitness/platform/repobase`

     b. Edit the `repobase` file so that the only information in the file is the following URL.

        `https://nw-node-zero/nwrpmrepo`

     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.

   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.

     a. Create the `/etc/netwitness/platform/repobase` file.

        `vi /etc/netwitness/platform/repobase`

     b. Edit the `repobase` file so that the only information in the file is the following URL.

        `https://<webserver-ip>/<alias-for-repo>`

     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool. The instructions are in [Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface](#) .

2. Set up the external repo.

   a. Log in to the web server host.

   b. Create directory to host the NW repository (`netwitness-11.7.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, /var/netwitness is the web-root, run the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`

   c. Create the 11.7.1.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.5.0.0`

   d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.5.0.0`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.5.0.0/OS`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.5.0.0/RSA`

   e. Unzip the `netwitness-11.5.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.5.0.0` directory.
      `unzip netwitness-11.5.0.0.zip -d /var/netwitness/<your-zip-file-`

`repo>/11.5.0.0`

Unzipping `netwitness-11.5.0.0.zip` results in two zip files (`OS-11.5.0.0.zip` and `RSA-11.5.0.0.zip`) and some other files.

f. Unzip the:

`OS-11.5.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.5.0.0/OS` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.5.0.0/OS-11.5.0.0.zip -d
/var/netwitness/<your-zip-file-repo>/11.5.0.0/OS
```

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

g. Unzip the:

`RSA-11.5.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.5.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.5.0.0/RSA-11.5.0.0.zip -d
/var/netwitness/<your-zip-file-repo>/11.5.0.0/RSA
```

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

   i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.5.0.0/OS/other`

   ii. `unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.5.0.0/OS/other`

   iii. `cd /var/netwitness/<your-zip-file-repo>/11.5.0.0/OS`

   iv. `createrepo`

i. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.5.0.0 Setup program (`nwsetup-tui`) prompt.

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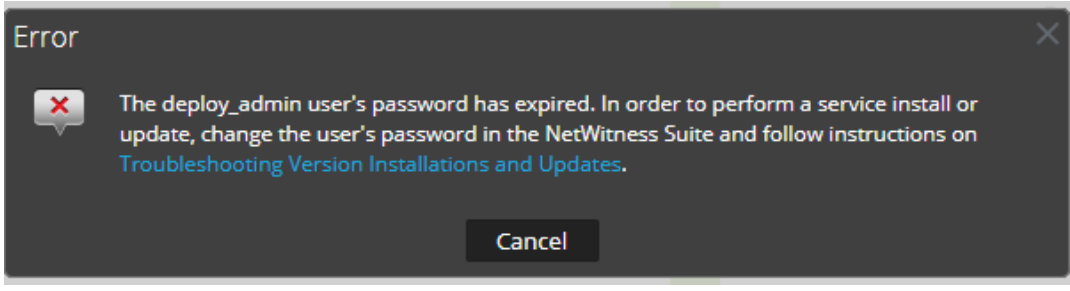
Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

- deploy_admin Password Expired Error
- Downloading Error
- Error Deploying Version <version-number> Missing Update Packages
- Upgrade Failed Error
- External Repo Update Error
- Host 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
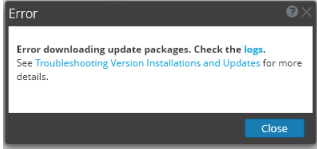
Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

- Log Collector Service
- NW Server
- Orchestration
- Reporting Engine
- Event Stream Analysis
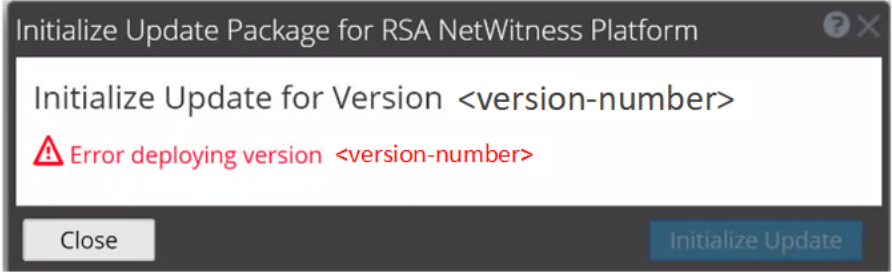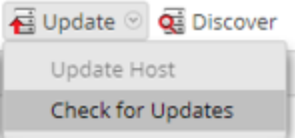
deploy_admin User Password Has Expired Error

Error Message	Error ✕ ❌ The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on Troubleshooting Version Installations and Updates. Cancel
Cause	The `deploy_admin` user password has expired.

Solution	Reset your `deploy_admin` password password.
	
	1. On the NW Server host only, run the following command.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	
	2. Review the output of the `nw-manage --update-deploy-admin-pw` command to verify the `deploy_admin` 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 `nw-manage --update-deploy-admin-pw` command, run `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` 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 `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt.

Downloading Error

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

Error Message	If you are upgrading from NetWitness Platform 11.x.x.x to 11.6.x.x or later, offline UI upgrade fails with the Download error message.

Solution	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 <version number>`
	For example:
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	
	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.

Error Deploying Version <version-number> Missing Update Packages

Error Message	Initialize Update Package for RSA NetWitness Platform ❓✖ Initialize Update for Version <version-number> ⚠ Error deploying version <version-number> Close ___ Initialize Update
Problem	Error deploying version <version-number> is displayed in the **Initialize Update Package for RSA NetWitness Platform** dialog after you click on **Initialize Update** if the update package is corrupted.
Solution	1. Click **Close** to close the dialog. 2. Remove the version folder from staging folder. 3. Make sure that the salt-master service is running. 4. Recopy the update package zip file to the staging folder. 5. In the Hosts view toolbar, select Check for Updates again. 📧 Update ⊙ 📧 Discover Update Host Check for Updates 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	While updating/installing a device to version 11.2 or above, the following error can occur and be found in /var/log/netwitness/config-management/chef-solo.log:
	
	`.......`
	`[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)`

Cause	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: ``` [root@S5-NWAdmin ~]# cat /etc/salt/minion master: localhost hash_type: sha256 log_level: info id: 889e5752-6ae3-4286-a944-c18233f4ccbc ```
Solution	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.
Workaround	Refer to Install/Upgrade fails in RSA NetWitness Platform because Resolv::ResolvError: no address for a particular host KB Article.

Error Message	Received an error in the error log similar to the following when trying to update to version 11.6 or later: ``` 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 ```
Cause	Custom builds/rpms installed for certain components installed on hosts, such as in the case of installing Hotfixes.

Solution	To resolve the issue, follow the below steps.
	
	1. SSH to Admin Server.
	
	2. Locate the component descriptor file by running the following command.
	`cd /etc/netwitness/component-descriptor/`
	
	3. Open the component descriptor file by running the following command.
	`vi nw-component-descriptor. json`
	
	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.
	`"concentrator": {`
	`"cookbook_name": "rsa-concentrator",`
	`"service_names": ["rsa-nw-concentrator"],`
	`"family": "launch",`
	`"default_port": xxxx, "description": "Concentrator",`
	`"packages"``:[{ "name": "rsa-nw-concentrator",`
	`"version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"`
	`},`
	
	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"
 },
```
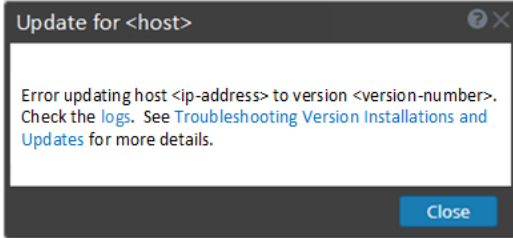
> **Note:** You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.

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 : `.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
Cause	There is an error the path you specified.
Solution	Make sure that: • the URL does exist on the NW Server host. • you used the correct path and remove any spaces from it.

Host Update Failed Error

Error Message	**Update for <host>** ⊘ ✕ Error updating host <ip-address> to version <version-number>. Check the logs. See Troubleshooting Version Installations and Updates for more details. **Close**
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.
Solution	1. Try to apply the version update to the host again. Often this is all you need to do. 2. If you still cannot apply the new version update: 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.

3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support.

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	1. Click Download Packages from NetWitness Community in the **Initialize Update Package for RSA NetWitness Platform** dialog. The NetWitness Community 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	The following example illustrates an ssh error that can occur when the ssh client is run from a host with OpenSSL 1.1.x installed: `$ ssh root@10.1.2.3` **ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect**

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

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

```
Last login: Mon Oct 21 19:03:23 2019
```

Patch Update to Non-NW Server Error

Error Message	The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error: **API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported**
Problem	After you update the NW Server host to a version, you must update all non-NW Server hosts to the same version. For example, if you update the NW Server from 11.4.0.0 to 11.6.0.0 or later, the only update path for the non-NW Server hosts is the same version (that is, 11.6.0.0). 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.
Solution	You have two options: • Update the non-NW Server host to 11.6.0.0 or later, or • Do not update the non-NW Server host (keep it at its current version)

Reboot Host After Update from Command Line Error

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

Reporting Engine Restarts After Upgrade

Problem	In some cases, after you upgrade to 11.6 or later from versions of 11.x, such as 11.4, the Reporting Engine service attempts to restart continuously without success.
Cause	The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.

Solution	To resolve the issue, do the following:
	1. Check which database files are corrupted:
	   Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks:
	   • If the live charts db file is corrupted, the following logs are displayed:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    a. Stop the Reporting Engine service.

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

    c. Restart the Reporting Engine service.

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

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

    a. Stop the Reporting Engine service.

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

    c. Restart the Reporting Engine service.

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

Problem	After you upgrade to version 11.6 or later, the Reporting Engine service does not restart.
Cause	The Reporting Engine service may not start due to any of the following reasons. - workspace.xml not updated. - Time is not converted properly in livechart h2 database. - JCR (Jackrabbit repository) is corrupted with primary key violation.

Solution	To resolve the issue, run the Reporting Engine Migration Recovery tool (`rsa-nw-re-migration-recovery.sh`) on the Admin Server where the Reporting Engine service is installed.
	
	Note: You can find the Reporting Engine Migration Recovery tool in the below location.
	`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`
	For example:
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	
	1. SSH to Admin Server.
	
	2. Untar the RE (Reporting Engine) tool, run the following command.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	
	3. (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.
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	
	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 installation logs posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Error Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

Error	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`

Message	
Cause	The Log Collector Lockbox is not configured after the update.
Solution	If you use a Log Collector Lockbox, log in to NetWitness and configure the Lockbox as described in the "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*.

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

Error Message	Decoder tries to start capture events but fails. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`

Solution	To resolve the issue, do the following steps,
	
	1. SSH to the Decoder host.
	
	2. Run the following commands.
	`yum reinstall pfring*`
	`systemctl restart nwdecoder`

NW Server

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

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 11.4.x.x or 11.5.x.x. to 11.6.0.0 or later.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Orchestration

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

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

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

Reporting Engine Service

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

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

Event Stream Analysis

Problem	After upgrading to version 11.6 or later, the ESA correlation server does not aggregate events from the configured data sources.
Error Message	`Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)`
Solution	To resolve the issue, do the following steps. In the NetWitness 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 deploymIent.

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

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

   a. Go to ![icon] **(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 NetWitness Documents - All Versions 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 NetWitness Documents - All Versions 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
```