RSA NETWITNESS® PLATFORM

# Release Notes

for RSA NetWitness® Platform 11.4.1.2

## Contact Information

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

## Trademarks

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

## License Agreement



## Third-Party Licenses

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

## Note on Encryption Technologies

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

## Distribution

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

July 2020

# Contents

# What's New

This document lists the enhancements and fixes made to improve NetWitness Platform 11.4.1.0. Read this document before deploying or upgrading to NetWitness Platform 11.4.1.2.

## Warehouse Connector

### Option to view the Schema used in Warehouse Connector

Analyst can view the latest schema that is used in the Warehouse Connector for writing in AVRO files. A new option is available in the Explorer View to view the schema. For more information, see "View Current Schema" section in Warehouse Connector - Manage a Stream topic.

# Fixed Issues

This section lists issues fixed since the last major release.

## Core Services (Broker, Concentrator, Decoder, Archiver) Fixes

| Tracking Number | Description |
|---|---|
| SACE-13409 | In some cases, when rebooting the Decoder or Decoder Hybrids, the Decoder service hangs during restart and becomes unresponsive. |
| SACE-13291 | Log Decoder service crashes while querying using msearch on raw logs. |
| SACE-13363/ ASOC-94282 | Log Decoder service crashes continuously while validating the payload due to the unknown header field in custom parser. |
| SACE-12301/ ASOC-94403 | Virtual Log Collector (VLC) is running with high CPU memory utilization. |

## Administrator Fixes

| Tracking Number | Description |
|---|---|
| SACE-13181/ ASOC-96329 | In Admin > Health and Wellness tab, the Admin Server status displays as unhealthy due to the memory spike. |
| SACE-13757/ ASOC-97713 | When querying for SDK timeline or SDK values call, the user interface does not display any information when the maximum query memory limit is reached. |

## Event Stream Analysis (ESA) Fixes

| Tracking Number | Description |
|---|---|
| SACE-13453/ ASOC-97454 | In the Configure > ESA Rules > Rules tab, the data source is visible in the Available Services dialog of the same deployment even after it is added as a data source to use with ESA correlation deployment from the Available Services dialog. |

## Warehouse Connector Fixes

| Tracking Number | Description |
|---|---|
| SACE-12864 | Unable to connect to the destination when the Warehouse Connector uses SFTP passphrase. |

## Log Collection Fixes

| Tracking Number | Description |
|---|---|
| SACE-12750 | When the syslog event source is changed to syslog over SSL from Logstash, Log Collection service crashes. |
| SACE-12098 | Improved TCP (Transmission Control Protocol) Syslog performance. |

## UEBA Fixes

| Tracking Number | Description |
|---|---|
| ASOC-92627 | The UEBA Object Name pivot link in the Investigate > Entities view is populated with an incorrect meta key. Due to this issue, no matching events are displayed when pivoting to the Events view because the query includes the `obj.name` meta key. |
| ASOC-92943 | When querying the event.time meta key from the Entities view to the Events view, it results in a query with invalid event time. |

# Build Numbers

The following table lists the build numbers for the components of NetWitness Platform 11.4.1.2.

| Component | Version Number |
|---|---|
| NetWitness Platform Warehouse Connector | 11.4.1.2-2002.5 |
| NetWitness Platform Admin Server | 11.4.1.2-200623024222.5 |
| NetWitness Platform Appliance | 11.4.1.2-10647.5 |
| NetWitness Platform Archiver | 11.4.1.2-10647.5 |
| NetWitness Platform Broker | 11.4.1.2-10647.5 |
| NetWitness Platform Component Descriptor | 11.4.1.2-2006230729.5 |
| NetWitness Platform Concentrator | 11.4.1.2-10647.5 |
| NetWitness Platform Config Management | 11.4.1.2-2006091015.5 |
| NetWitness Platform Console | 11.4.1.2-10647.5 |
| NetWitness Platform Decoder | 11.4.1.2-10647.5 |
| NetWitness Platform Decoder Content | 11.4.1.2-10647.5 |
| NetWitness Platform Deployment Upgrade | 11.4.1.2-2005220343.5 |
| NetWitness Platform Legacy Web Server | 11.4.1.2-200609101541.5 |
| NetWitness Platform Log Collector | 11.4.1.2-14861.5 |
| NetWitness Platform Log Collector Perl | 11.4.1.2-14861.5 |
| NetWitness Platform Log Collector Tools | 11.4.1.2-14861.5 |
| NetWitness Platform Log Decoder | 11.4.1.2-10647.5 |
| NetWitness Platform Log Player | 11.4.1.2-10647.5 |
| NetWitness Platform SDK | 11.4.1.2-10647.5 |
| NetWitness Platform User Interface | 11.4.1.2-200616180209.5 |

| | |
|---|---|
| NetWitness Platform Work Bench | 11.4.1.2-10647.5 |
| NetWitness Platform Legacy Windows Collector | 11.4.1.2-14861.5 |

# Upgrade Instructions

You need to read the information and follow these procedures for upgrading NetWitness Platform version 11.4.1.2.

The following upgrade paths are supported for NetWitness Platform 11.4.1.2:

- NetWitness Platform 11.2.x.x to 11.4.1.2
- NetWitness Platform 11.3.x.x to 11.4.1.2
- NetWitness Platform 11.4.0.x to 11.4.1.2
- NetWitness Platform 11.4.1.0 to 11.4.1.2
- NetWitness Platform 11.4.1.1 to 11.4.1.2

To upgrade from NetWitness Platform 11.2.x.x or 11.3.x.x to 11.4.1.2, you must download files for the 11.4.0.0 base pack, 11.4.1.0 service pack, 11.4.1.1 patch and the 11.4.1.2 patch release.

To upgrade from NetWitness Platform 11.4.0.x to 11.4.1.2, you must download files for the 11.4.1.0 service pack, 11.4.1.1 patch and the 11.4.1.2 patch release.

To upgrade from NetWitness Platform 11.4.1.0 to 11.4.1.2, you only need to download files for the 11.4.1.1 patch and 11.4.1.2 patch release.

To upgrade from NetWitness Platform 11.4.1.1 to 11.4.1.2, you only need to download files for the 11.4.1.2 patch release.

You can upgrade 11.4.1.2 patch using one of the following options:

- If the NetWitness Server has internet connectivity to Live Services, the NetWitness Platform User Interface can be used to apply the patch.
- If the NetWitness Server does not have internet connectivity to Live Services, the Command Line Interface (CLI) or the NetWitness Platform User Interface can be used to apply the patch.

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

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

## Running in Mixed Mode

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

## Upgrade Considerations for ESA Rule Deployments

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

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

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

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

## Change to Column Groups in the Events View

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

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

## Upgrade Tasks

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

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

### Task 1: Download the 11.4.1.2 Patch

Download the RSA NetWitness Platform 11.4.1.2 Upgrade Pack file, which contain all the NetWitness Platform 11.4.1.2 upgrade files, from the RSA Link https://community.rsa.com/community/products/netwitness/114/downloads to a local directory.
`netwitness-11.4.1.2.zip`

| Upgrading from | Download and Stage file |
|---|---|
| 11.2.x.x | `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`,and `netwitness-11.4.1.2.zip` |

| Upgrading from | Download and Stage file |
|---|---|
| 11.3.x.x | `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` |
| 11.4.0.x | `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` |
| 11.4.1.0 | `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` |
| 11.4.1.1 | `netwitness-11.4.1.2.zip` |

## Task 2: Upgrade External Repository

**Note:** Perform the below steps only if you are using an external repository for 11.4.1.2.

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

1. Upgrade the external repository with the latest upgrade content for the RSA `netwitness-11.4.1.2.zip`.
   The following is the structure after upgrading the external repository:

## Task 3: Disable Decoder Services

Before upgrading to 11.4.1.2, you must disable Capture AutoStart on Network Decoder and Network Hybrid Services.

**To disable Capture Autostart:**

1. Go to **ADMIN** > **Services**.
   The Administration Services view is displayed.
2. Select a Network Decoder or Network Hybrid service and select  > **View** > **Config**.
   The services config view for the selected Network Decoder or Network Hybrid is displayed.
3. In the **Decoder Configuration** panel, deselect the **Capture Autostart** and click **Apply**.

## Task 4: Upgrade the Patch

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

## Online Method (Connectivity to Live Services): Upgrade Using NetWitness User Interface

You can use this method if the NetWitness Server is connected to Live Services and can obtain the package.

**Note:** If the NetWitness Server does not have access to Live Services, use Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface . or use Offline Method (No connectivity to Live Services): Upgrade using the NetWitness User Interface

## Prerequisites

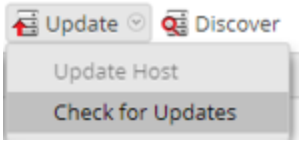
Make sure that:

1. The “Automatically download information about new upgrades every day” option is checked and is applied in **ADMIN** > **System** > **Upgrades**.
2. Go to **ADMIN** > **Hosts** > **Update** > **Check for Updates** to check for upgrades. The Host page displays the **Update Available** status.
3. 11.4.1.2 is available under “Update Version” column.

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

## Procedure

1. Go to **ADMIN** > **Hosts**.
2. Select the NetWitness Server (nw-server) host.
3. Check for the latest updates.




4. Update Available is displayed in the **Status** column if you have a version upgrade in your Local Update Repository for the selected host.
5. Select **11.4.1.2** from the **Update Version** column.
   If you:
   - Want to view a dialog with the major features in the upgrade and information on the upgrades click the information icon ( ⓘ ) to the right of the update version number.
   - Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available upgrades. If an upgrade is available, the message "New updates are available" is displayed and the **Status** column upgrades automatically to show Update Available. By default, only supported upgrades for the selected host are displayed.
6. Click **Update** > **Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click the **Reboot Host** when prompted.
9. Repeat steps 6 to 8 for other hosts.

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

**Note:** Not all components have been changed for 11.4.1.2, so after you perform the upgrade steps, it is normal to see some components with different version numbers. For a list of the components that were upgraded for this release, see Build Numbers.

## Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface

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

**Note:** Alternatively, you can upgrade using the Offline Method (No connectivity to Live Services): Upgrade using the NetWitness User Interface.

## Prerequisites

Make sure that you have downloaded the RSA NetWitness Platform 11.4.1.2 Upgrade Pack file, which contain all the NetWitness Platform 11.4.1.2 upgrade files, from the RSA Link https://community.rsa.com/community/products/netwitness/114/downloads to a local directory.

- If you are upgrading from an 11.2.x.x or 11.3.x.x to 11.4.1.2, download `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip`.
- If you are upgrading from an 11.4.0.x to 11.4.1.2, download `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip`.
- If you are upgrading from 11.4.1.0 to 11.4.1.2, download`netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip`.
- If you are upgrading from 11.4.1.1 to 11.4.1.2, download `netwitness-11.4.1.2.zip`.
- If you are using external repository, you can upgrade the external repository with the latest upgrade content. For more information see, Task 2: Upgrade External Repository.

## Procedure

You need to perform the upgrade steps for NW Admin servers and for component servers.

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

- **If you are upgrading from 11.2.x.x or 11.3.x.x to 11.4.1.2**, you must stage 11.4.0.0, 11.4.1.0, 11.4.1.1, and 11.4.1.2. Log into the `/root` directory of the Admin NetWitness Server and create the following directories:

  ```
  /tmp/upgrade/11.4.0.0
  /tmp/upgrade/11.4.1.0
  /tmp/upgrade/11.4.1.1
  /tmp/upgrade/11.4.1.2
  ```

  and then copy the package zip files to the `/root` directory of the Admin server and extract the package files from `/root` to the appropriate directories:

  ```
  unzip netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0
  unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
  unzip netwitness-11.4.1.1.zip -d /tmp/upgrade/11.4.1.1
  unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
  ```

- **If you are upgrading from 11.4.0.x to 11.4.1.2**, you must stage 11.4.1.0, 11.4.1.1, and 11.4.1.2. Log into the `/root` directory of the Admin NetWitness Server and create the following directories:

  ```
  /tmp/upgrade/11.4.1.0
  /tmp/upgrade/11.4.1.1
  /tmp/upgrade/11.4.1.2
  ```

  and then copy the package zip files to the `/root` directory of the Admin server and extract the package files from `/root` to the appropriate directories:

  ```
  unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0
  ```

```
unzip netwitness-11.4.1.1.zip -d /tmp/upgrade/11.4.1.1
unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
```

- **If you are upgrading from 11.4.1.0 to 11.4.1.2**, you only need to stage 11.4.1.1, and 11.4.1.2. Log into the `/root` directory of the Admin NetWitness Server and create the following directory:
  `/tmp/upgrade/11.4.1.1`
  `/tmp/upgrade/11.4.1.2`
  and then copy the package zip files to the `/root` directory of the Admin server and extract the package files from `/root` to the `/tmp/upgrade/11.4.1.2` directory:
  ```
  unzip netwitness-11.4.1.1.zip -d /tmp/upgrade/11.4.1.1
  unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
  ```
- **If you are upgrading from 11.4.1.1 to 11.4.1.2**, you only need to stage 11.4.1.2. Log into the `/root` directory of the Admin NetWitness Server and create the following directory:
  `/tmp/upgrade/11.4.1.2`
  and then copy the package zip files to the `/root` directory of the Admin server and extract the package files from `/root` to the `/tmp/upgrade/11.4.1.2` directory:
  ```
  unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
  ```

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

1. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.4.1.2 --stage-dir /tmp/upgrade
   ```
2. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.2
   ```
3. When the component host upgrade is successful, reboot the host from NetWitness UI.
4. Repeat steps 2 and 3 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 NetWitness Server. 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 patch will install correctly. No action is required. If you encounter additional errors when upgrading a host to a new version, contact Getting Help with NetWitness Platform.

## External Repo Instructions for CLI Upgrade

**Note:** The external repo should have separate directories for 11.4.0.0, 11.4.1.0, 11.4.1.1 and 11.4.1.2, as described in Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface .

1. Stage 11.4.1.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.4.1.2` and extract the zip package.
   ```
   unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
   ```
   **Note:** If you copied the .zip file to the created staging directory to unzip, make sure that you delete the initial .zip file that you copied to the staging location after you extract it.
2. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.4.1.2 --stage-dir /tmp/upgrade
   ```
3. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.2
   ```
4. When the component host upgrade is successful, reboot the host from NetWitness UI.
5. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being upgraded.

**Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on NetWitness Server. 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 patch will install correctly. No action is required. If you encounter additional errors when upgrading a host to a new version, contact Getting Help with NetWitness Platform.

## Offline Method (No connectivity to Live Services): Upgrade using the NetWitness User Interface

The following rules apply when you apply version upgrades:

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

**Caution:** The offline User Interface method is only available if you are upgrading a host from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1, 11.4.1.0, or 11.4.1.1 to 11.4.1.2. If you are upgrading a host on an earlier version, you must use the Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface method. After you complete Step 5 in Offline Method (No connectivity to Live Services): Upgrade using the NetWitness User Interface, go to Upgrading from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1, 11.4.1.0, or 11.4.1.1 to 11.4.1.2.

**Caution:** If you are upgrading a host from 11.4.0.0 or 11.4.0.1 to 11.4.1.2 using the offline User Interface method, in Step 5 of Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface , the upgrade will fail with the message Download error. You can still complete the upgrade successfully by following the steps in Upgrading from 11.4.0.0 or 11.4.0.1 to 11.4.1.2 .

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

- If you are upgrading from 11.3.1.0 or later to 11.4.1.2, download the `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.0.x to 11.4.1.2, download the `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.1.0 to 11.4.1.2, download the `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.1.1 to 11.4.1.2, download the `netwitness-11.4.1.2.zip` upgrade package from RSA Link to a local directory.

1. SSH to the NW Server host.
2. If you are upgrading from 11.3.1.0 or later to 11.4.1.2, copy `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.

   ```
   sudo cp /tmp/netwitness-11.4.0.0.zip /var/lib/netwitness/common/update-stage/
   sudo cp /tmp/netwitness-11.4.1.0.zip /var/lib/netwitness/common/update-stage/
   sudo cp /tmp/netwitness-11.4.1.1.zip /var/lib/netwitness/common/update-stage/
   sudo cp /tmp/netwitness-11.4.1.2.zip /var/lib/netwitness/common/update-stage/
   ```

3. If you are upgrading from 11.4.0.x or later to 11.4.1.2, copy `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, and `netwitness-11.4.1.2.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.

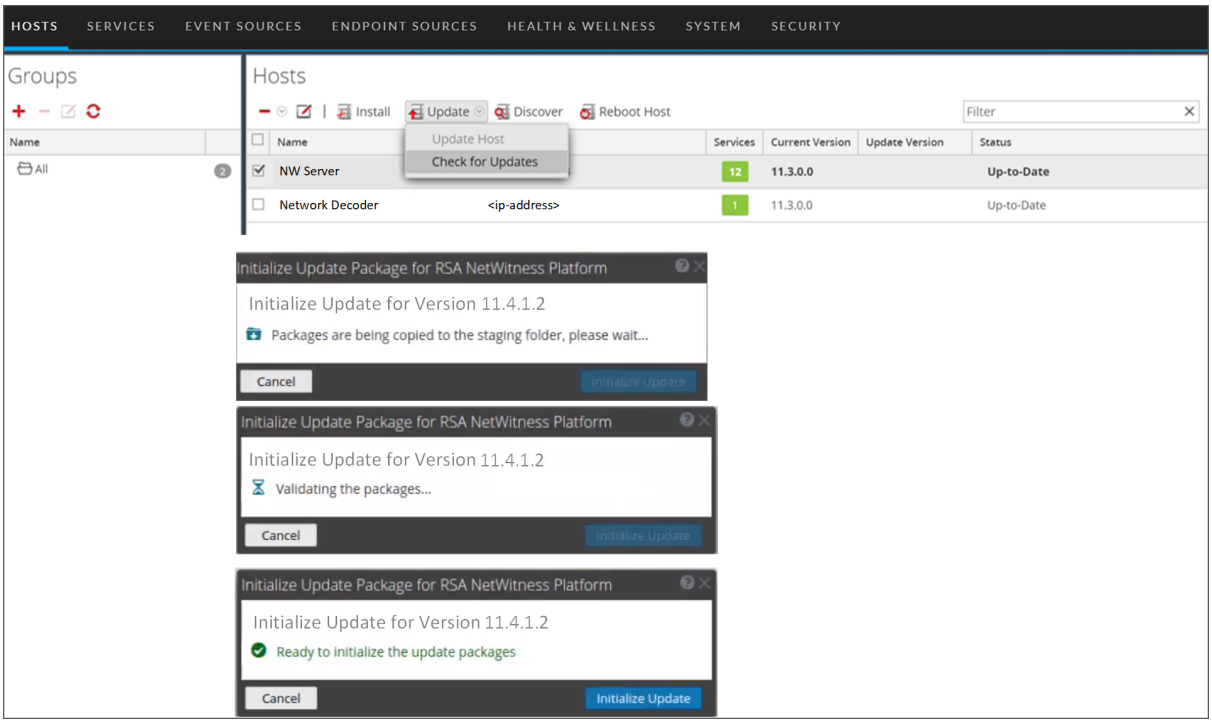
   ```
   sudo cp /tmp/netwitness-11.4.1.0.zip /var/lib/netwitness/common/update-stage/
   sudo cp /tmp/netwitness-11.4.1.1.zip /var/lib/netwitness/common/update-stage/
   sudo cp /tmp/netwitness-11.4.1.2.zip /var/lib/netwitness/common/update-stage/
   ```

4. If you are upgrading from 11.4.1.0 to 11.4.1.2, copy `netwitness-11.4.1.1.zip` and `netwitness-11.4.1.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
```
sudo cp /tmp/netwitness-11.4.1.1.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.4.1.2.zip /var/lib/netwitness/common/update-stage/
```
5. If you are upgrading from 11.4.1.1 to 11.4.1.2, copy `netwitness-11.4.1.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
```
sudo cp /tmp/netwitness-11.4.1.2.zip /var/lib/netwitness/common/update-stage/
```
NetWitness Platform unzips the file automatically.

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

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

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

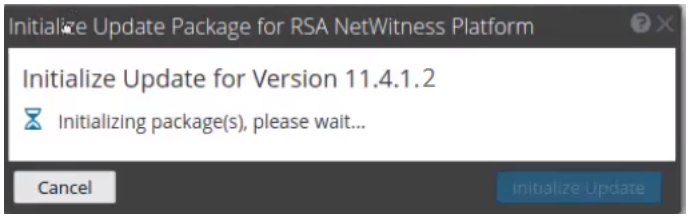



"Ready to initialize packages" is displayed if:

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

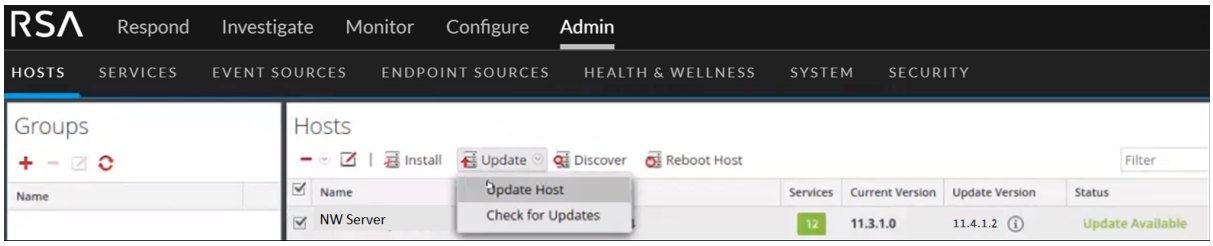
Refer to Troubleshooting Version Installations and upgrades for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

4. Click **Initialize Update**.




It takes some time to initialize the packages because the files are large and need to be unzipped. After the initialization is successful, the **Status** column displays Update Available and you complete the rest of the steps in this procedure to finish the update of the host.

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




6. Click **Begin Update** from the **Update Available** dialog.

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

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

## Upgrading from 11.3.1.0, 11.3.1.1, 11.3.2.0, 11.3.2.1, 11.4.1.0, or 11.4.1.1 to 11.4.1.2

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

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

## Upgrading from 11.4.0.0 or 11.4.0.1 to 11.4.1.2

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

1. In the Command Line Interface (CLI):
   a. SSH to NW Server.
   b. Run the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.2
   ```

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.

# Post-Upgrade Tasks

This topic is divided into two sections, based on the version that you are upgrading from:

Post Upgrade Tasks for Customers Upgrading from version 11.4.1.x

Post Upgrade Tasks for Customers Upgrading from version 11.2.x.x or 11.3.x.x or 11.4.0.x

# Post Upgrade Tasks for Customers Upgrading from version 11.4.1.x

## Task 1 - Upgrade HIVE version

**Note:** If you already installed customized HIVE RPMs in 11.2.1 or later, you can skip this task

After you upgrade to 11.4.1.2, you need to upgrade the HIVE version that is compatible with Warehouse. To install the latest HIVE version, run the following commands on the NetWitness admin server and restart the Reporting Engine service. Download the latest HIVE RPMs from https://community.rsa.com/docs/DOC-109473.

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

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

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

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

## Task 2 (Optional) - Move the custom certs

Move the custom certs from external directory to `/etc/pki/nw/trust/import` directory.

## Task 3 - Enable Decoder Services

After you upgrade to 11.4.1.2, you must enable Capture AutoStart on Network Decoder and Network Hybrid Services.

**To enable the Capture Autostart field:**

1. Go to **ADMIN** > **Services**.
   The Administration Services view is displayed.
2. Select a Network Decoder or Network Hybrid service and select  > **View** > **Config**.
   The services Config view for the selected Network Decoder or Network Hybrid is displayed.
3. In the **Decoder Configuration** panel, select the **Capture Autostart** field and click **Apply**.

# Post Upgrade Tasks for Customers Upgrading from version 11.2.x.x or 11.3.x.x or 11.4.0.x

Perform all the post upgrade tasks mentioned in *Upgrade Guide for RSA NetWitness Platform 11.4.1.0*.

# Product Documentation

The following documentation is provided with this release.

| Document | Location |
|---|---|
| NetWitness Platform 11.4 Product Documentation | RSA NetWitness Platform 11.4 Product Documentation |
| NetWitness Platform Hardware Setup Guides | RSA NetWitness Hardware Setup Guides |
| RSA Content for NetWitness Platform | RSA Content for the RSA NetWitness® Platform |

## Known Issues

Issues that remain unresolved in this release are documented here: RSA NetWitness Platform Known Issues. Wherever a workaround is available, it is noted or referenced in detail.

## Feedback on Product Documentation

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

# Getting Help with NetWitness Platform

## Self-Help Resources

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

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

## Contact RSA Support

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

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

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

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