RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness® Platform 11.4.1.3

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

September 2020

Contents

Introduction

This document lists the fixes made to improve NetWitness Platform 11.4.1.0. Read this document before deploying or upgrading to NetWitness Platform 11.4.1.3.

Fixed Issues

This section lists issues fixed since the last major release.

Administration Fixes

Tracking Number	Description
SACE13731/ ASOC-101327	Single Sign On (SSO) connection does not work for NetWitness Platform 11.4.0.1.

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

Tracking Number	Description
SACE-13985	Index customizations for Retention Log Hybrid service not reflecting on updating entities from Index definition files on Decoder.
SACE-13977	Packet pool depletion due to either large HTTP sessions or newly installed feeds like ThreatStreamIP.
SACE-13812/ ASOC-100351	No alarms triggered from ESM test policy even after disabling automatic monitoring and restarting rabbit-mq, collectd and rsa-sms.
SACE-14051	Issue with deployment of Non-IP feeds with IPv6 values (non CIDR) on Decoders or Log Decoders. The first entry on the feed fails to load.
SACE-13928	When you upgrade to 11.4.x version except 11.4.1.3, the calculation of the bytes filtered by Apprule has an issue.
SACE-14408	SSL Pakcet decryption fails on Investigator Thick Client version 11.4.0.0.781 as the pem file (Key file) is not recognized in the Investigator logs.
SACE-13706/ ASOC-102996	Issue with transferring logs from Log Decoder to external devices as the connection between Log Decoder and destination Server could not be established.

Health and Wellness Fixes

Tracking Number	Description
SACE-13666/ ASOC-101606	For Hybrids, few statistics on the Health and Wellness are not showing the historical representation of the graph. However, numbers are displayed after hovering the mouse over the white space.

Investigate Fixes

Tracking Number	Description
SACE-13914/ SACE-13887/ ASOC-101707	PCAP export fails as the system was cross linking the credentials of two accounts.
SACE-14314/ ASOC-102261	Right most column in the Events View is partially visible/ truncated due to incorrect width calculation in NetWitness. After adjusting the size of the columns, the original size gets automatically restored if a column is added or removed.

Malware Analysis Fixes

Tracking Number	Description
SACE-14144/ ASOC-101767	A mismatch between the directory name and MD5 hash value for the files ending with "-" extension in 11.3.2 Malware Analysis. The actual file name was missing under spectrum/repository/files folder.
SACE-13682	Malware Analysis appliance license displays as unlicensed on the UI.

Context Hub Fixes

Tracking Number	Description
ASOC-101486	During the alerts data prefetch process, once the mongo doc size limit exception is hit for any alert entity, processing of other alerts data is skipped, resulting in loss of contextual data from other alerts.

Endpoint Fixes

Tracking Number	Description
SACE-13963/ ASOC-101948	The assigned VPN IP address is not displayed from Endpoint Agents deployed on Mac-OS.
SACE-13300/ ASOC-101948	High CPU use by Endpoint agents during scanning.
SACE-13721/ ASOC-101948	Unable to identify the process running from drive letter "Z" on Investigate > Hosts > Processes view.
SACE-13670/ ASOC-101948	Agent is unable to retrieve a policy due to an error in evaluating IPv4/IPv6 addresses of the host.
SACE-13294/ ASOC-101948	After installing NetWitness Endpoint Advanced agent, issue with launching of Windows Pseudo Console apps until you run it as an administrator.
SACE-13584/ ASOC-101948	BSOD occurred after the installation of NetWitness Endpoint agent on Windows Server 2008-R2.
SACE-13476/ ASOC-101948	NWE Agent Service crash observed in CentOS-8/RHEL-8.x due to RPM verify.
SACE-13763/ ASOC-101948	NWEAgent Service crashes when enumerating network interfaces on RHEL-8.x.
ASOC-87703/ ASOC-101948	Agent enhancement to hash the file to avoid reopening file in user mode. This eliminates any interference of NetWitness agent during third party software updates and installations.

ESA Fixes

Tracking Number	Description
SACE-14293/ ASOC-103904	ESA is giving error and not generating alerts after upgrading to 11.4.1.1. Also, it starts generating older events.
ASOC-103988/ SACE-12773	Subqueries with isOneOfIgnoreCase or isNotOneOfIgnoreCase helper functions are not evaluated.

Upgrade Instructions

You need to read the information and follow these procedures for upgrading NetWitness Platform version 11.4.1.3.

The following upgrade paths are supported for NetWitness Platform 11.4.1.3:

- NetWitness Platform 11.3.x.x to 11.4.1.3
- NetWitness Platform 11.4.0.x to 11.4.1.3
- NetWitness Platform 11.4.1.0 to 11.4.1.3
- NetWitness Platform 11.4.1.1 to 11.4.1.3
- NetWitness Platform 11.4.1.2 to 11.4.1.3

To upgrade from NetWitness Platform 11.3.x.x to 11.4.1.3, you must download files for the 11.4.0.0 base pack, 11.4.1.0 service pack, 11.4.1.1 patch, 11.4.1.2 patch, and the 11.4.1.3 patch release.

To upgrade from NetWitness Platform 11.4.0.x to 11.4.1.3, you must download files for the 11.4.1.0 service pack, 11.4.1.1 patch, 11.4.1.2 patch, and the 11.4.1.3 patch release.

To upgrade from NetWitness Platform 11.4.1.0 to 11.4.1.3, you only need to download files for the 11.4.1.1 patch, 11.4.1.2 patch, and 11.4.1.3 patch release.

To upgrade from NetWitness Platform 11.4.1.1 to 11.4.1.3, you only need to download files for the 11.4.1.2 patch and 11.4.1.3 patch release.

To upgrade from NetWitness Platform 11.4.1.2 to 11.4.1.3, you only need to download files for the 11.4.1.3 patch release.

You can upgrade 11.4.1.3 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.

Getting Help with NetWitness Platform

Self-Help Resources

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

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

Contact RSA Support

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

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

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

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

Upgrade 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.

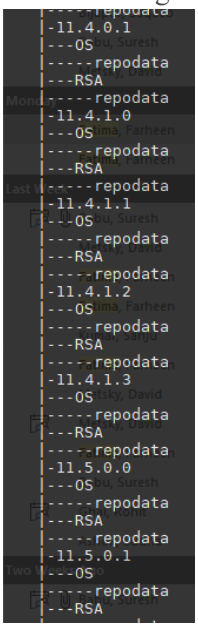
```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ntpd
```

Task 1: Upgrade External Repository

Note: Perform the below steps only if you are using an external repository for 11.4.1.3.

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-11.4.1.3.zip`.
   The following is the structure after upgrading the external repository:



Task 2: Disable Decoder Services

Before upgrading to 11.4.1.3, 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 3: Upgrade the Patch

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

- Option 1: Online Method (Connectivity to Live Services): Upgrade Using NetWitness Platform User Interface .
- Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface .
- Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface

Upgrade Options

Option 1: Online Method (Connectivity to Live Services): Upgrade Using NetWitness Platform 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 Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface . or use Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface

Prerequisites

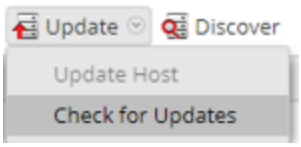
Make sure that:

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. 11.4.1.3 is available under "Update Version" column.

Note: If you have custom certifictes, move any custom certificates from `/etc/pki/nw/trust/import/` directory to `/root/cert`. Follow these steps to move the certificates:
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 **11.4.1.3** 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.

Note: Not all components have been changed for 11.4.1.3, 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.

Option 2: 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 Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface

Download the 11.4.1.3 Patch

Download the RSA NetWitness Platform 11.4.1.3 Upgrade Pack file, which contain all the NetWitness Platform 11.4.1.3 upgrade files, from the RSA Link https://community.rsa.com/community/products/netwitness/114/downloads to a local directory.
`netwitness-11.4.1.3.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`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`
11.4.0.x	`netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`

Upgrading from	Download and Stage file
11.4.1.0	`netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`
11.4.1.1	`netwitness-11.4.1.2.zip` and `netwitness-11.4.1.3.zip`
11.4.1.2	`netwitness-11.4.1.3.zip`

Note: If you are using external repository, you can upgrade the external repository with the latest upgrade content. For more information see, Task 1: 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 11.3.x.x to 11.4.1.3**, you must stage 11.4.0.0, 11.4.1.0, 11.4.1.1, 11.4.1.2, and 11.4.1.3. 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
  /tmp/upgrade/11.4.1.3
  ```

  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
  unzip netwitness-11.4.1.3.zip -d /tmp/upgrade/11.4.1.3
  ```

- **If you are upgrading from 11.4.0.x to 11.4.1.3**, you must stage 11.4.1.0, 11.4.1.1, 11.4.1.2, and 11.4.1.3. 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
  /tmp/upgrade/11.4.1.3
  ```

  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
  unzip netwitness-11.4.1.3.zip -d /tmp/upgrade/11.4.1.3
  ```

- **If you are upgrading from 11.4.1.0 to 11.4.1.3**, you only need to stage 11.4.1.1, 11.4.1.2, and 11.4.1.3. 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`
  `/tmp/upgrade/11.4.1.3`
  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-11.4.1.1.zip -d /tmp/upgrade/11.4.1.1
  unzip netwitness-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
  unzip netwitness-11.4.1.3-zip -d /tmp/upgrade/11.4.1.3
  ```
- **If you are upgrading from 11.4.1.1 to 11.4.1.3**, you only need to stage 11.4.1.2 and 11.4.1.3. Log into the `/root` directory of the Admin NetWitness Server and create the following directory:
  `/tmp/upgrade/11.4.1.2`
  `/tmp/upgrade/11.4.1.3`
  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-11.4.1.2.zip -d /tmp/upgrade/11.4.1.2
  unzip netwitness-11.4.1.3.zip -d /tmp/upgrade/11.4.1.3
  ```
- **If you are upgrading from 11.4.1.2 to 11.4.1.3**, you only need to stage 11.4.1.3. Log into the `/root` to the directory of the Admin NetWitness Server and create the following directory:
  `/tmp/upgrade/11.4.1.3`
  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 directory:
  ```
  unzip netwitness-11.4.1.3.zip -d /tmp/upgrade/11.4.1.3
  ```

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 11.4.1.3 --stage-dir /tmp/upgrade
   ```
2. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.3
   ```
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, 11.4.1.2, and 11.4.1.3, as described in Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface .

1. Stage 11.4.1.3 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.4.1.3` and extract the zip package.
   ```
   unzip netwitness-11.4.1.3.zip -d /tmp/upgrade/11.4.1.3
   ```
   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 11.4.1.3--stage-dir /tmp/upgrade
   ```
3. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.3
   ```
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.

Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface

Follow the instructions in Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface.

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 11.3.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 11.4.1.3, 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 certificates

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

Task 3 - Enable Decoder Services

After you upgrade to 11.4.1.3, 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 11.3.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*.

Build Numbers

The following table lists the build numbers for the components of NetWitness Platform 11.4.1.3.

Component	Version Number
NetWitness Platform Warehouse Connector	11.4.1.3 - 2005. 5
RSA Audit Plugins	11.4.1.3 - 4599.5
RSA Audit RT	11.4.1.3 - 4599.5
RSA Collectd	11.4.1.3 - 4599.5
RSA Collectd Sms	11.4.1.3 - 4599.5
NetWitness Platform Admin Server	11.4.1.3 - 200818060805.5
NetWitness Platform Appliance	11.4.1.3 - 10671.5
NetWitness Platform Archiver	11.4.1.3 - 10671.5
NetWitness Platform Broker	11.4.1.3 - 10671.5
NetWitness Platform Component Descriptor	11.4.1.3 - 2010061008.5
NetWitness Platform Concentrator	11.4.1.3 - 10671.5
NetWitness Platform Console	11.4.1.3 - 10671.5
NetWitness Platform Context Hub Server	11.4.1.3 - 200907051522.5
NetWitness Platform Correlation Server	11.4.1.3 - 201005171531.5
NetWitness Platform Decoder	11.4.1.3 - 10671.5
NetWitness Platform Decoder Content	11.4.1.3 - 10671.5
NetWitness Platform Deployment Upgrade	11.4.1.3 - 2009070410.5
NetWitness Platform Endpoint Agents	11.4.1.3 - 2009102136.5
NetWitness Platform Endpoint Broker Server	11.4.1.3 - 200827095959.5
NetWitness Platform Endpoint Server	11.4.1.3 - 200827094016.5

NetWitness Platform Legacy Web Server	11.4.1.3 - 200930170256.5
NetWitness Platform License Server	11.4.1.3 - 200818060849.5
NetWitness Platform Log Decoder	11.4.1.3 - 10671.5
NetWitness Platform Log Player	11.4.1.3 - 10671.5
NetWitness Platform Malware Analytics Server	11.4.1.3 - 200904041632.5
NetWitness Platform Relay Server	11.4.1.3 - 200827100415.5
NetWitness Platform SDK	11.4.1.3 - 10660.5
NetWitness Platform User Interface	11.4.1.3 - 201001043756.5
NetWitness Platform Work Bench	11.4.1.3 - 10671.5
RSA Sms Runtime-RT	11.4.1.3 - 4599.5
RSA Sms Server	11.4.1.3 - 4599.5

Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform 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, 11.4.1.1, or 11.4.1.2 to 11.4.1.3. If you are upgrading a host on an earlier version, you must use the Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface method. After you complete Step 5 in Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface, go to Upgrading from 11.3.1.x, 11.3.2.x, 11.4.1.x to 11.4.1.3.

Caution: If you are upgrading a host from 11.4.0.0 or 11.4.0.1 to 11.4.1.3 using the offline User Interface method, in Step 5 of Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User 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 11.4.1.3 .

Download the 11.4.1.3 Patch

Download the RSA NetWitness Platform 11.4.1.3 Upgrade Pack file, which contain all the NetWitness Platform 11.4.1.3 upgrade files, from the RSA Link https://community.rsa.com/community/products/netwitness/114/downloads to a local directory. `netwitness-11.4.1.3.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`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`
11.4.0.x	`netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`
11.4.1.0	`netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip`
11.4.1.1	`netwitness-11.4.1.2.zip` and `netwitness-11.4.1.3.zip`
11.4.1.2	`netwitness-11.4.1.3.zip`

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 11.4.1.3, download the `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.0.x to 11.4.1.3, download the `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.1.0 to 11.4.1.3, download the `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.1.1 to 11.4.1.3, download the `netwitness-11.4.1.2.zip` and `netwitness-11.4.1.3.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.1.2 to 11.4.1.3, download the `netwitness-11.4.1.3.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 11.4.1.3, copy `netwitness-11.4.0.0.zip`, `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.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/

   sudo cp /tmp/netwitness-11.4.1.3.zip /var/lib/netwitness/common/update-stage/
   ```

3. If you are upgrading from 11.4.0.x or later to 11.4.1.3, copy `netwitness-11.4.1.0.zip`, `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.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/

   sudo cp /tmp/netwitness-11.4.1.3.zip /var/lib/netwitness/common/update-stage/
   ```

4. If you are upgrading from 11.4.1.0 to 11.4.1.3, copy `netwitness-11.4.1.1.zip`, `netwitness-11.4.1.2.zip`, and `netwitness-11.4.1.3.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/
   ```

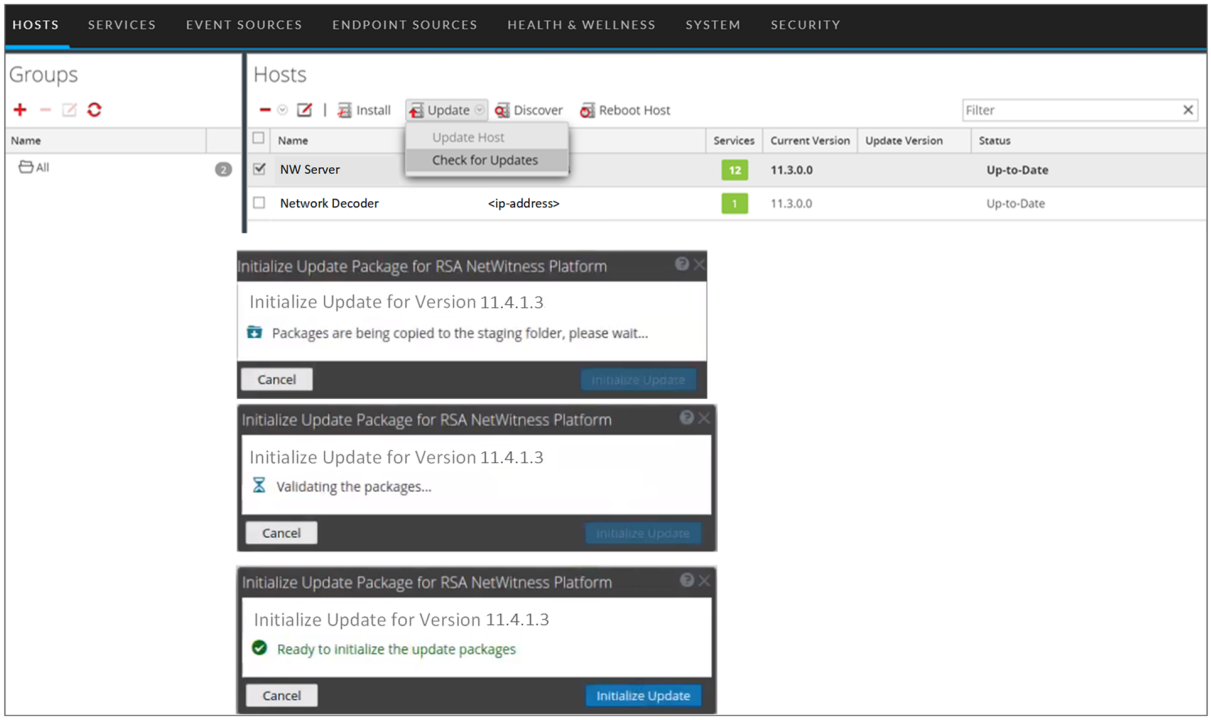
```
sudo cp /tmp/netwitness-11.4.1.2.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.4.1.3.zip /var/lib/netwitness/common/update-stage/
```

5. If you are upgrading from 11.4.1.1 to 11.4.1.3, copy `netwitness-11.4.1.2.zip` and `netwitness-11.4.1.3.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/
sudo cp /tmp/netwitness-11.4.1.3.zip /var/lib/netwitness/common/update-stage/
```
6. If you are upgrading from 11.4.1.2 to 11.4.1.3, copy `netwitness-11.4.1.3.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
```
sudo cp /tmp/netwitness-11.4.1.3.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.

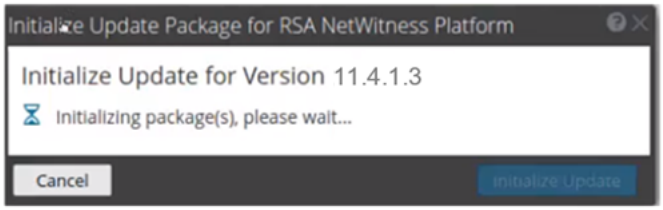


"Ready to initialize packages" is displayed if:

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

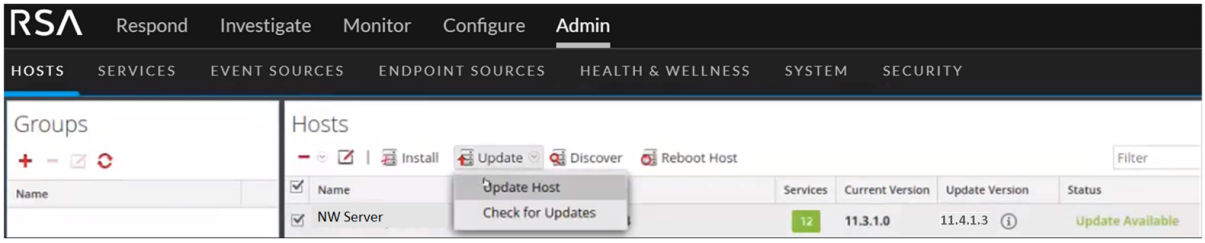
Refer to Troubleshooting Version Installations and upgrades for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

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.x, 11.3.2.x, 11.4.1.x to 11.4.1.3

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 11.4.1.3

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 11.4.1.3
```

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.