RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness® Platform 11.4.0.1

Contact Information

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

Trademarks

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 11.4.0.0. Read this document before deploying or upgrading to NetWitness Platform 11.4.0.1.

Reporting Engine

Output Action for Blank Reports: NetWitness Platform provides the analyst with the ability to exclude blank reports while processing the output actions. You can configure this setting in the Reporting Engine service configuration view using Enable Output Actions for Reports with No Results option. For more details, see Reporting Engine General Tab.

Fixed Issues

This section lists issues fixed since the last major release.

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

Tracking Number	Description
SACE-12827/ ASOC-87857	Not able to extract the email attachment if the Content-disposition header is in upper case.
SACE-12387/ ASOC-87236	Unable to extract files from an SMB2 session due to the recent changes in the SMB2 protocol.

Investigation Fixes

Tracking Number	Description
SACE-11659/ ASOC-88050	When investigating an offline Archiver collection, it does not display metadata with events but displays only the events count.
SACE-11706/ ASOC-88025	Event export fails when investigating for a custom time frame and profile with no prequery.
SACE-12803/ ASOC-87643	Unable to export logs in the Investigate view when the user language setting is not English or French.
ASOC-87633	When the NOT operator is used in Event view Free-Form Mode without parenthesis, as in `NOT medium = 1` vs `NOT(medium = 1)`, the free-form query fails.
ASOC-87549	Packets are not rendered properly and the expected data is not displayed in the Events view packet reconstruction.
ASOC-87516	The packet reconstruction being viewed does not have data loaded after leaving the Events view for the Hosts, Files, or Entities view, and then returns to the Events view using the Events option in the Investigate submenu.
ASOC-87378	After upgrading to Version 11.4, there may be issues in the Navigate view and Legacy Events view because the column groups, meta groups, or profile groups permission is disabled for custom user roles.

Reporting Engine Fixes

Tracking Number	Description
SACE-12723	NetWitness Platform Recovery Tool does not clean up the old backup reporting-engine-home.tar.gz files.

Log Collection Fixes

Tracking Number	Description
ASOC-87953	Windows Legacy Collector (WLC) certificate renewal script packaged as part of 11.4 and located at /var/netwitness/root-ca- update/wlc/ does not run.

Context Hub Fixes

Tracking Number	Description
SACE-11272/ ASOC-84841	When STIX data is converted to CSV format, some of the STIX fields are not available in the CSV file.
ASOC-87937	Connection for Threat Insights (Live Connect) and File Reputation data source fails as the password gets saved as blank.

Health and Wellness Fixes

Tracking Number	Description
SACE-10378/ ASOC-74763	PSU shows incorrect status on the Health & Wellness view, when one PSU fails on the S5 Hybrid.

Malware Analysis Fixes

Tracking Number	Description
SACE-12834	When forwarding the syslog from Malware, the Source IP and Destination IP is not available in the forwarded events though it is available in the reports.

Tracking Number	Description
SACE-10302/ ASOC-88023	AV tab in Admin > Services > Malware > Config, does not display AV Vendor results.

ESA (Event Stream Analysis) Fixes

Tracking Number	Description
ASOC-87859	Some ESA Rule Deployments migrated from versions before 11.3 can cause ESA Rule Deployment issues during the 11.4 upgrade.

Build Numbers

The following table lists the build numbers for the components of NetWitness Platform 11.4.0.1.

Component	Version Number
NetWitness Platform Audit Plugins	11.4.0.1-4559.5
NetWitness Platform Appliance	11.4.0.1-10610.5
NetWitness Platform Archiver	11.4.0.1-10610.5
NetWitness Platform Broker	11.4.0.1-10610.5
NetWitness Platform Concentrator	11.4.0.1-10610.5
NetWitness Platform Config Management	11.4.0.1-2002030604.5
NetWitness Platform Config Server	11.4.0.1-200204231459.5
NetWitness Platform Console	11.4.0.1-10610.5
NetWitness Platform Content Server	11.4.0.1-200203010820.5
NetWitness Platform ContextHub Server	11.4.0.1-200203011811.5
NetWitness Platform Correlation Server	11.4.0.1-200123112452.5
NetWitness Platform Decoder	11.4.0.1-10610.5
NetWitness Platform Deployment Upgrade	11.4.0.1-2001271917.5
NetWitness Platform Integration Server	11.4.0.1-200206031328.5
NetWitness Platform Investigate Server	11.4.0.1-200131092039.5
NetWitness Platform Legacy Web Server	11.4.0.1-200210114322.5
NetWitness Platform License Server	11.4.0.1-200207025255.5
NetWitness Platform Log Decoder	11.4.0.1-10610.5
NetWitness Platform Log Player	11.4.0.1-10610.5
NetWitness Platform Malware Analytics Server	11.4.0.1-200123131723.5

NetWitness Platform Metrics Server	11.4.0.1-200122010852.5
NetWitness Platform Reporting Engine Server	11.4.0.1-5838.5
NetWitness Platform Respond Server	11.4.0.1-200203011845.5
NetWitness Platform Root CA Update	11.4.0.1-2001221338.5
NetWitness Platform SDK	11.4.0.1-10610.5
NetWitness Platform Source Server	11.4.0.1-200203011154.5
NetWitness Platform User Interface	11.4.0.1-200203070828.5
NetWitness Platform Workbench	11.4.0.1-10610.5
NetWitness Platform SA Tools	11.4.0.1-2002041822.5
NetWitness Platform SMS Runtime	11.4.0.1-4559.5
NetWitness Platform SMS Server	11.4.0.1-4559.5

Upgrade Instructions

You need to read the information and follow these procedures for upgrading NetWitness Platform version 11.4.0.1.

The following upgrade paths are supported for NetWitness Platform 11.4.0.1:

- NetWitness Platform 11.2.x.x to 11.4.0.1
- NetWitness Platform 11.3.x.x to 11.4.0.1
- NetWitness Platform 11.4.0.0 to 11.4.0.1

- To upgrade from NetWitness Platform 11.2.x.x or 11.3.x.x to 11.4.0.1, you must download files for the 11.4.0.0 release and the 11.4.0.1 patch release.
- To upgrade from NetWitness Platform 11.4.0.0 to 11.4.0.1, you only need to download files for the 11.4.0.1 patch release.

You can upgrade 11.4.0.1 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 upgrading from 11.2.x.x to 11.4.0.1, see the "Upgrade Considerations for ESA Rule Deployments" section in the Upgrade Overview in the *Upgrade Guide for RSA NetWitness Platform 11.4.0.0*.

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

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

Upgrade Preparation Tasks

There are no required upgrade preparation tasks if you are upgrading to 11.4.0.1. However, if you are upgrading from 11.3.x.x to 11.4.0.1, the Event Stream Analysis (ESA) upgrade preparation task in the *Upgrade Guide for RSA NetWitness Platform 11.4.0.0* can be completed, but it is optional for 11.4.0.1.

Upgrade Tasks

Task 1: Download the 11.4.0.1 Patch

Download the RSA NetWitness Platform 11.4.0.1 Upgrade Pack file, which contain all the NetWitness Platform 11.4.0.1 upgrade files, from the RSA Link

https://community.rsa.com/community/products/netwitness/114/downloads to a local directory.
`netwitness-11.4.0.1.zip`

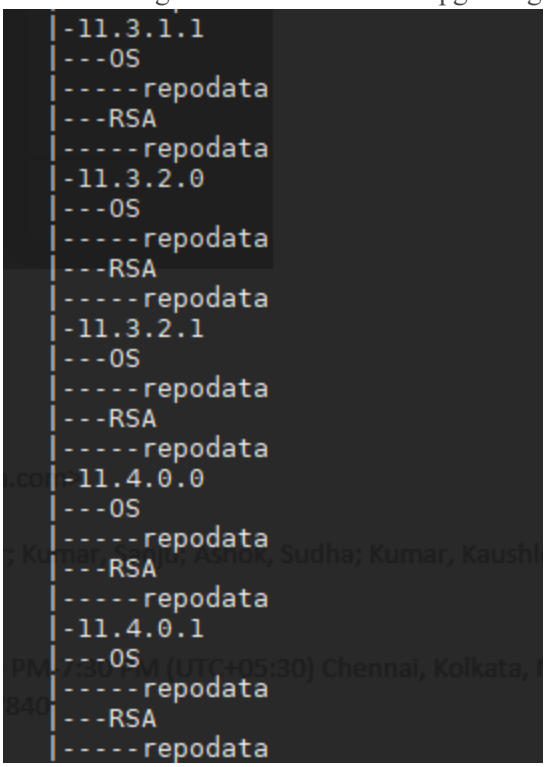
Upgrading from	Download and Stage file
11.2.x.x	`netwitness-11.4.0.0.zip` and `netwitness-11.4.0.1.zip`
11.3.x.x	`netwitness-11.4.0.0.zip` and `netwitness-11.4.0.1.zip`
11.4.0.0	`netwitness-11.4.0.1.zip`

Task 2: Upgrade External Repository

Note: Perform the below steps only if you are using an external repository for 11.4.0.1.

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-11.4.0.1.zip`.
   The following is the structure after upgrading the external repository:



Task 3: Disable Decoder Services

Before upgrading to 11.4.0.1, 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:

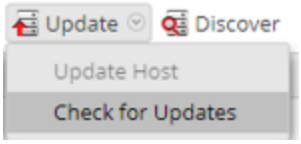
1. The "Automatically download information about new upgrades every day" option is checked and is applied in **ADMIN** > **System** > **Upgrades**.
2. Go to **ADMIN** > **Hosts** > **Update** > **Check for Updates** to check for upgrades. The Host page displays the **Update Available** status.
3. 11.4.0.1 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 **11.4.0.1** 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 11.4.0.1, 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 11.4.0.1 Upgrade Pack file, which contain all the NetWitness Platform 11.4.0.1 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 11.4.0.1, download `netwitness-11.4.0.0.zip` and `netwitness-11.4.0.1.zip`.
- If you are upgrading from 11.4.0.0 to 11.4.0.1, download `netwitness-11.4.0.1.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 11.4.0.1**, you must stage 11.4.0.0 and 11.4.0.1. Log into the `/root` directory of the Admin NetWitness Server and create the following directories:
  `/tmp/upgrade/11.4.0.0`
  `/tmp/upgrade/11.4.0.1`
  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-11.4.0.1.zip -d /tmp/upgrade/11.4.0.1
  ```
- **If you are upgrading from 11.4.0.0 to 11.4.0.1**, you only need to stage 11.4.0.1. Log into the `/root` directory of the Admin NetWitness Server and create the following directory:
  `/tmp/upgrade/11.4.0.1`
  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/11.4.0.1` directory:
  ```
  unzip netwitness-11.4.0.1.zip -d /tmp/upgrade/11.4.0.1
  ```

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 11.4.0.1 --stage-dir /tmp/upgrade
   ```
2. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.0.1
   ```
3. When the component host upgrade is successful, reboot the host from NetWitness UI.
4. Repeat steps 4 and 5 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 Contacting Customer Care.

External Repo Instructions for CLI Upgrade

Note: The external repo should have separate directories for 11.4.0.0 and 11.4.0.1, as described in Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface .

1. Stage 11.4.0.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.4.0.1` and extract the zip package.
   ```
   unzip netwitness-11.4.0.1.zip -d /tmp/upgrade/11.4.0.1
   ```
   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 11.4.0.1 --stage-dir /tmp/upgrade
   ```
3. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.0.1
   ```
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 Contacting Customer Care.

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.

Note: The offline User Interface method is only available if you are upgrading a host from 11.3.1.0 or later to 11.4.0.1. 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 .

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 (except 11.4.0.0) to 11.4.0.1, download the `netwitness-11.4.0.0.zip` and `netwitness-11.4.0.1.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.4.0.0 to 11.4.0.1, download the `netwitness-11.4.0.1.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 (except 11.4.0.0) to 11.4.0.1, copy `netwitness-11.4.0.1.zip` and `netwitness-11.4.0.1.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-11.4.0.1.zip /var/lib/netwitness/common/update-stage/
   ```
3. If you are upgrading from 11.4.0.0 to 11.4.0.1, copy `netwitness-11.4.0.1.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:

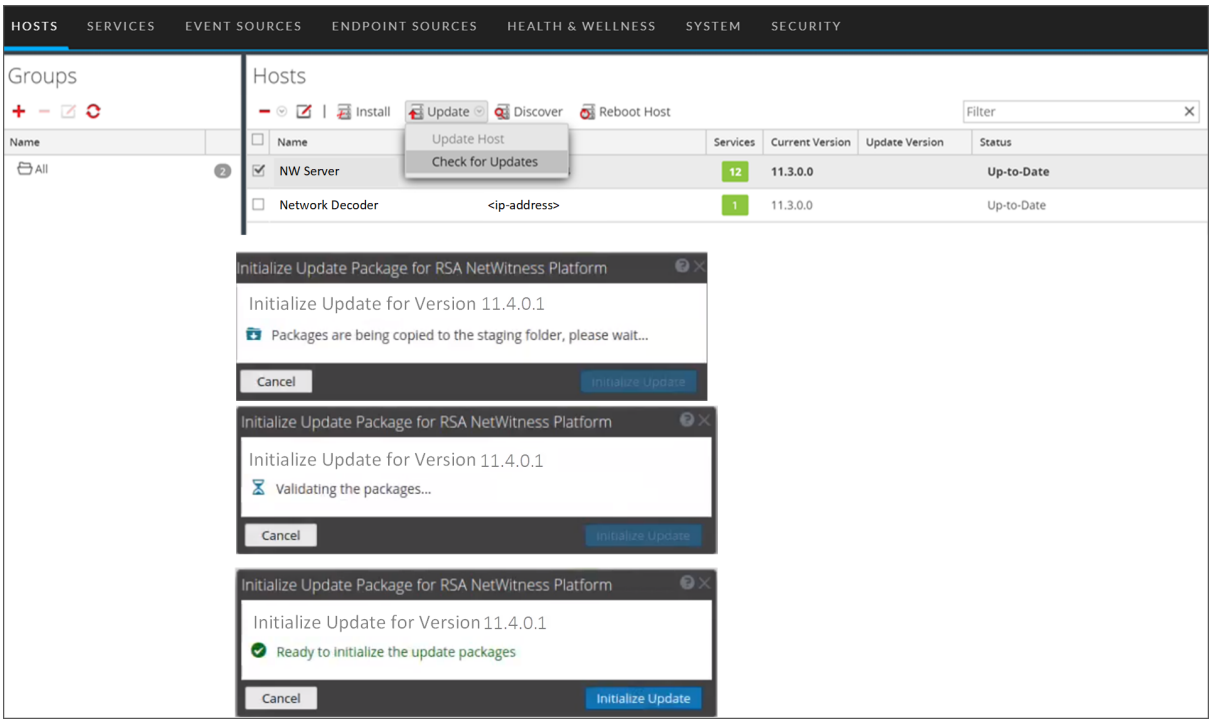
   ```
   sudo cp /tmp/netwitness-11.4.0.1.zip /var/lib/netwitness/common/update-stage/
   ```

   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.

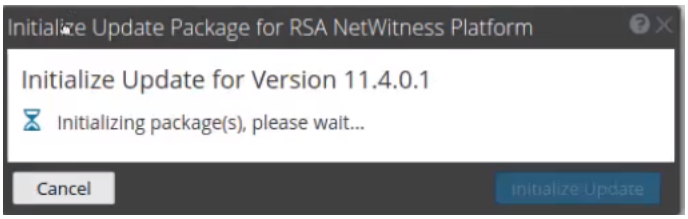


"Ready to initialize packages" is displayed if:

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

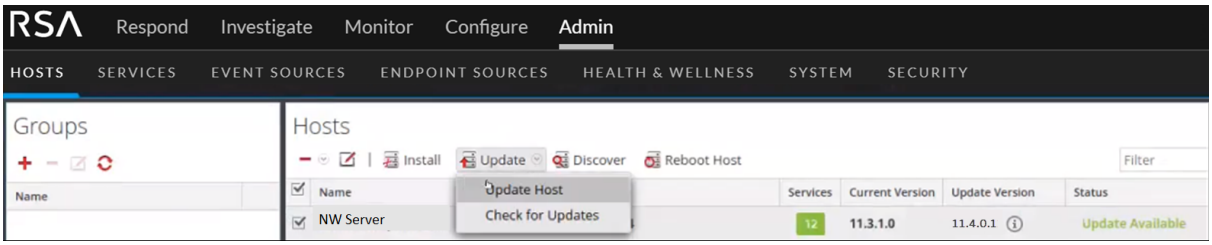
Refer to Troubleshooting Version Installations and upgrades for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

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.

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 11.4.0.0

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

Post Upgrade Tasks for Customers Upgrading From 11.4.0.0

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 11.4.0.1, 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 11.4.0.1, 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 11.2.x.x or 11.3.x.x

Perform all the post upgrade tasks mentioned in *Upgrade Guide for RSA NetWitness Platform 11.4.0.0*.

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.

Support Information

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

- See documentation for all aspects of NetWitness Platform here:
  RSA NetWitness Platform Online Documentation
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here:
  Welcome to RSA Link
- If you need further information, contact Customer Care.

If you contact Customer Care, you should be at your computer. Be prepared to give 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**.
Phone	1-800-995-5095, option 3
International Contacts	How to contact RSA Customer Support
Community	RSA Customer Support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Contacting Customer Care

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

- See 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
- If you need further information, contact Customer Care.

If you contact Customer Care, you should be at your computer. Be prepared to give 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** from the list at the bottom of the browser.
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.