RSA NETWITNESS® PLATFORM

Update Guide

for Version 11.2.1.0

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase 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 www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

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

Contents

Update Guide

This document lists the instructions to upgrade NetWitness Platform. Read this document before deploying or updating NetWitness Platform 11.2.1.0

Update Instructions

You need to read the information and follow these procedures for updating NetWitness Platform version 11.2.1.0.

The following update paths are supported for NetWitness Platform 11.2.1.0:

- RSA NetWitness® Platform 11.1.0.0 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.1 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.2 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.3 to 11.2.1.0
- RSA NetWitness® Platform 11.2.0.0 to 11.2.1.0
- RSA NetWitness® Platform 11.2.0.1 to 11.2.1.0

For update paths supported for 11.2.0.0, see the *Update Guide for Version 11.0.x.x or 11.1.x.x to 11.2*.

You can update 11.2.1.0 service pack 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) can be used to apply the patch.

Update Tasks

Task 1: Disable Decoder Services

Before updating to 11.2.1.0, you must disable Capture AutoStart on Network Decoder and Network Hybrid Services.

To disable 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, deselect the **Capture Autostart** field and click **Apply**.

Task 2: Update the Service Pack

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

Online Method (Connectivity to Live Services): Update 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): Update using the Command Line Interface.

Prerequisites

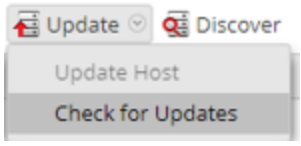
Make sure that:

1. The "Automatically download information about new updates every day" option is checked and is applied in **ADMIN** > **System** > **Updates** .
2. Go to **ADMIN** > **Hosts** > **Update** > **Check for Updates** to check for updates. The Host page displays the **Update Available** status.
3. 11.2.1.0 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 update in your Local Update Repository for the selected host.

5. Select **11.2.1.0** from the **Update Version** column. If you:
   - Want to view a dialog with the major features in the update and information on the updates, 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 updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show Update Available. By default, only supported updates for the selected host are displayed.
6. Click **Update** > **Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click the **Reboot Host**.
9. Repeat steps 6 to 8 for other hosts.

Note: You can select multiple hosts to update at the same time only after updating and rebooting the NetWitness Admin server. All ESA, Endpoint Insights, and Malware Analysis hosts should be updated to the same version as that of NetWitness Admin Server.

Note: Not all components have been changed for 11.2.1.0, so after you perform the update steps, it is normal to see some components with different version numbers. For a list of the components that were updated for this release, see Build Numbers.

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

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

Prerequisites

Make sure that:

- You have downloaded the following file, which contain all the NetWitness Platform 11.2.1.0 update files, from RSA Link (https://community.rsa.com/) > **NetWitness Platform** > **RSA NetWitness Logs and Network** > **Downloads** > RSA Dowloads to a local directory:
  `netwitness-11.2.1.0.zip`

Procedure

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

Note: If you are updating from 11.1.0.x to 11.2.1.0, you must download the NetWitness Platform 11.2.0.0 files netwitness-11.2.0.0.zip and set them up in the staging folder along with the 11.2.1.0 files.

Note: If you copy paste the commands from PDF to Linux SSH terminal, the characters don't work. It is recommended to type the commands.

1. Stage 11.2.1.0 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.2.1.0` and extract the zip package.
   ```
   unzip netwitness-11.2.1.0.zip -d /tmp/upgrade/11.2.1.0
   ```
   Note: If you copied the .zip file to the created staging directory to unzip, make sure that you delete the initial .zip file that you copied to the staging location after you extract it.
2. Initialize the update, using the following command:
   ```
   upgrade-cli-client --init --version 11.2.1.0 --stage-dir /tmp/upgrade
   ```
3. Update Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.1.0
   ```
4. When the component host update 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 updated.

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 update process:
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support (Contacting Customer Care).

External Repo Instructions for CLI Update

Note: External repo which is to be setup should have 11.2.1.0 repo set under the same directory as 11.2.0.0.

1. Stage 11.2.1.0 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.2.1.0` and extract the zip package.
   ```
   unzip netwitness-11.2.1.0.zip -d /tmp/upgrade/11.2.1.0
   ```

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

2. Initialize the update, using the following command:
   `upgrade-cli-client --init --version 11.2.1.0 --stage-dir /tmp/upgrade`
3. Update Netwitness Server, using the following command:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.1.0`
4. When the component host update 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 updated.

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 update process:
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support (Contacting Customer Care).

Post-Update Tasks

Task 1 - Update Hive version

After you update to 11.2.1.0, you need to update 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.

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 (Conditional) - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.2.x.x using the `pam_radius` package, you must reconfigure it in 11.2.1.0 using the `pam_radius_auth` package.

You need to execute the below commands on NW Server on which the Admin server resides.

Note: If you have configured `pam_radius` in 11.x.x.x, perform the below steps to uninstall the existing version, or you can proceed with Step 2.

Step 1: Verify the existing page and uninstall the existing `pam_radius`

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Step 2: To install the `pam_radius_auth` package, execute the following command

```
yum install pam_radius_auth
```

Step 3: Edit the RADIUS configuration file, `/etc/raddb/server` as follows and add the configurations for radius server:

```
# server[:port] shared_secret timeout (s)
server secret 3
```

For example - 111.222.33.44 secret 1

Step 4: Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

```
auth sufficient pam_radius_auth.so
```

Step 5: Provide the write permission to `/etc/raddb/server` files using below command

```
chown netwitness:netwitness /etc/raddb/server
```

Step 6: To copy the `pam_radius_auth` library, execute the following command

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Step 7: Restart the jetty server after making the changes to `pam_radius_auth` configurations, excute the following command.

```
systemctl restart jetty
```

Task 4 - Restart the Respond Server

Restart the Respond server:

```
systemctl restart rsa-nw-respond-server
```

Task 5 - Update the 10G driver Location

You must update the 10G driver in the correct location in the current kernel.

Step 1: If you are using 10G decoder, run the below commands after 11.2.1.0 upgrade and reboot the decoder appliance. Click **Y** when you are prompted to overwrite.

- cp /var/lib/dkms/ixgbe-zc/5.3.7.14/$(uname -r)/x86_64/module/ixgbe_zc.ko.xz /lib/modules/$(uname -r)/extra/
- cp /var/lib/dkms/i40e-zc/2.4.6.14/$(uname -r)/x86_64/module/i40e_zc.ko.xz /lib/modules/$(uname -r)/extra/
- `cp /var/lib/dkms/pfring/6.5.0.14/$(uname -r)/x86_64/module/pf_ring.ko.xz /lib/modules/$(uname -r)/extra/`

Step 2: If you have disabled the **Capture Autostart** field as mentioned in the Task 1: Disable Decoder Services, you must re-enable the **Capture AutoStart** on the 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**.

Product Documentation

The following documentation is provided with this release.

Document	Location
NetWitness Platform 11.2.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/112
NetWitness Platform 11.2.1.0 Release Notes	https://community.rsa.com/docs/DOC-100349

Feedback on Product Documentation

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

Contacting Customer Care

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

RSA Link	https://community.rsa.com/
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/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.

Preparing to Contact Customer Care

When 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.

Revision History

Revision	Date	Description
0.1	09-Jan-19	Final Draft