RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness Platform 11.2.1.1

Contents

Release Notes

This document lists the fixes in NetWitness Platform 11.2.1.1. Read this document before deploying or updating NetWitness Platform 11.2.1.1

Fixed Issues

This document lists issues fixed in NetWitness Platform 11.2.1.1.

Security Fixes

Tracking Number	Description
ASOC-65311	CVE-2019-3724, Authorization Bypass Vulnerability. https://nvd.nist.gov/vuln/detail/CVE-2019-3724?cpeVersion=2.2
ASOC-72910	CVE-2019-3725, Command Injection Vulnerability. https://nvd.nist.gov/vuln/detail/CVE-2019-3725?cpeVersion=2.2

Server Fixes

Tracking Number	Description
SACE-10387	When you save a query on the Dashboard, the query with single quotes is displayed in encoded HTML format.
SACE-10907	When you log out from **INVESTIGATE** > **Navigate** view, the UI does not redirect to the login page.

Reporting Fixes

Tracking Number	Description
SACE-10099	When you execute a rule using the line graph format, the dates are not in order.
SACE-9696	In the Use Rule dialog box, the Reports folder list is not displayed when you navigate from Reports to Alerts or Charts option.

Investigate Fixes

Tracking Number	Description
SACE-10879/SACE-10870	On **INVESTIGATE** > **Navigate** view, an error is displayed or different query is executed when you drill down using a query created in 10.6.6.
SACE-10402	When you select an event on **INVESTIGATE** > **Event Analysis** view, the BASE64 FORMAT displays incorrect characters.
SACE-9822	PCAPs and logs cannot be download on the Event Analysis view if the user name contains backslash (\).

Core Fixes

Core Services include Broker, Concentrator, Decoder, and Log Decoder.

Tracking Number	Description
SACE-10719	Decoder service crashes when `parser.options` is modified with `HTTPS-S="cert.sha1=true"`
SACE-10689	An error is displayed when Log Decoder uses `syslogtimestampscan` parser, due to which the `/var/log` storage partition is consumed.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.2.1.1.

Component	Version Number
NetWitness Platform Decoder	11.2.1.1-9491.5
NetWitness Platform Concentrator	11.2.1.1-9491.5
NetWitness Platform Context hub Server	11.2.1.1-190314005200.5
NetWitness Platform Broker	11.2.1.1-9491.5
NetWitness Platform Log Decoder	11.2.1.1-9491.5

NetWitness Platform Archiver (Workbench)	11.2.1.1-9491.5
NetWitness Platform Event Stream Analysis Server	11.2.1.1-88.5
NetWitness Platform Appliance	11.2.1.1-9491.5
NetWitness Platform Archiver	11.2.1.1-9491.5
NetWitness Platform Console	11.2.1.1-9491.5
NetWitness Platform Malware Analytics Server	11.2.1.1-190315144219.5
NetWitness Platform Legacy Web Server	11.2.1.1-190315142835.5
NetWitness Platform Log Player	11.2.1.1-9491.5
NetWitness Platform SDK	11.2.1.1-9491.5
NetWitness Platform Legacy Windows Collector	11.2.1.1-14701.5

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

> **Note:** The known issues from the previous releases of 11.2.0.0 may be fixed in the service packs. Refer to the respective service pack or patch release notes that are available on RSA Link: https://community.rsa.com/.

Update

NetWitness Hosts displays the status as rebooting

Tracking Number: ASOC-70992

Problem: After you update to 11.2.1.1, multiple NetWitness Hosts on **ADMIN** > **Hosts** view displays the status as rebooting even after the Hosts are updated.

Workaround:

- Log in to NW Admin server and run the following command to update MongoDB.

```
mongo admin -u deploy_admin -p <Replace_With_Deploy_admin_passwrod>
> use sa
> db.appliance_update.updateMany(
```

```
{ "status": "REBOOTING" }
,{$set:
{ "status" : "REBOOTED"}
} )
```

- Refresh the NetWitness UI.

Update Instructions

You need to read the information and follow these procedures for updating NetWitness Platform version 11.2.1.1.

The following update paths are supported for NetWitness Platform 11.2.1.1:

- 11.1.x.x to 11.2.1.1

- 11.2.x.x to 11.2.1.1

To update NetWitness Platform to 11.2.1.1 from either of these versions, you must have files for 11.2.0.0 (base release), 11.2.1.0 (service pack release) and 11.2.1.1 (patch release).

Note: Even if you are updating from an 11.2.x.x release, it is possible that the 11.2.0.0 base repository files could have been removed. These files must be on your system for the upgrade to be successful.

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 to the 11.2.1.1 patch release 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 11.2.1.1, 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 Patch

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. 11.2.1.1 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.
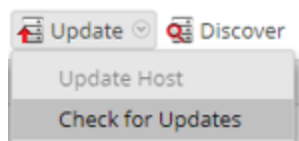
4. Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.

5. Select **11.2.1.1** 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 NW Admin Server or NetWitness Admin Server.

> **Note:** Not all components have been changed for 11.2.1.1, 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 files, which contain all the NetWitness Platform 11.2.1.1 update files, from RSA Link (https://community.rsa.com/) > NetWitness Platform > RSA NetWitness Logs and Network > Downloads > RSA Downloads to a local directory:

- If you are updating from an 11.1.x.x. or an 11.2.x.x release, download `netwitness-11.2.0.0.zip`, `netwitness-11.2.1.0.zip` and `netwitness-11.2.1.1.zip`.

- If you are updating from 11.2.1.0, download `netwitness-11.2.1.1.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.x.x or 11.2.x.x to 11.2.1.1, you must download the NetWitness Platform 11.2.0.0 files `netwitness-11.2.0.0.zip` and NetWitness Platform 11.2.1.0 files `netwitness-11.2.1.0.zip`, and set them up in the staging folder, in addition to the 11.2.1.1 files.

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

1. Before you stage 11.2.1.1, you must stage the required previous releases by creating the following directories on the NetWitness Server and copying the package zip files to these directories:
   ```
   /tmp/upgrade/11.2.0.0
   /tmp/upgrade/11.2.1.0
   ```
   and then extract the zip packages for those releases:
   ```
   unzip netwitness-11.2.0.0.zip -d /tmp/upgrade/11.2.0.0
   unzip netwitness-11.2.1.0.zip -d /tmp/upgrade/11.2.1.0
   ```

2. Stage 11.2.1.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.2.1.1` and extract the zip package.
   ```
   unzip netwitness-11.2.1.1.zip -d /tmp/upgrade/11.2.1.1
   ```

   > **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.

3. Initialize the update, using the following command:
   ```
   upgrade-cli-client --init --version 11.2.1.1 --stage-dir /tmp/upgrade
   ```

4. Update Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.1.1
   ```

5. When the component host update is successful, reboot the host from NetWitness UI.

6. Repeat steps 3 through 5 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 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 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 patch 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 11.2.1.1 repo set under the same directory as 11.2.0.0.

1. Stage 11.2.1.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.2.1.1` and extract the zip package.
   ```
   unzip netwitness-11.2.1.1.zip -d /tmp/upgrade/11.2.1.1
   ```

   > **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 update, using the following command:
   ```
   upgrade-cli-client --init --version 11.2.1.1 --stage-dir /tmp/upgrade
   ```

3. Update Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
   11.2.1.1
   ```

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 patch 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 11.2.1.1, 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 11.2.1.1 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, execute 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 11.2.1.1 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 enable the **Capture AutoStart** again 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
RSA NetWitness Platform 11.3.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/112

Feedback on Product Documentation

You can send an email to sahelpfeedback@emc.com to provide feedback on RSA 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	20-March	Final Draft