



Release Notes

for RSA NetWitness Platform 11.2.1.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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 Dell, 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 Dell.

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.

August 2019

Contents

Introduction	5
Fixed Issues	5
Server Fixes	5
Investigate Fixes	5
Core Fixes	6
Admin Fixes	6
Windows Collector Fixes	7
Archiver Fixes	7
Upgrade Fixes	7
Build Numbers	7
Known Issues	8
Update Instructions	8
Update Tasks	9
Task 1: Disable Decoder Services	9
Task 2: Update the Patch	9
Online Method (Connectivity to Live Services): Update Using NetWitness User Interface	9
Prerequisites	10
Procedure	10
Offline Method (No connectivity to Live Services): Update using the Command Line Interface	11
Prerequisites	11
Procedure	11
External Repo Instructions for CLI Update	13
Post-Update Tasks	14
Post Update Tasks if you are Updating From 11.1.x.x	14
Task 1 - Update HIVE version	14
Task 2 (Optional) - Move the custom certs	14
Task 3 (Conditional) - Reconfigure PAM Radius Authentication	14
Task 4 - Restart the Respond Server	15
Post Update Tasks if you are Updating From 11.2.x.x	15
Task 1 - Update HIVE version	15
Task 2 - Restart the Respond Server	16

Product Documentation	16
Feedback on Product Documentation	16
Contacting Customer Care	16
Preparing to Contact Customer Care	17
Revision History	17

Introduction

This document lists the fixes in NetWitness Platform 11.2.1.2. Read this document before deploying or updating NetWitness Platform 11.2.1.2.

Fixed Issues

This section lists issues fixed in NetWitness Platform 11.2.1.2.

Server Fixes

Tracking Number	Description
SACE-10917	Line breaks are not displayed in the Login banner.
ASOC-67123	When the Event Source Manage groups have the Idle time condition defined, alarms are not generated.

Investigate Fixes

Tracking Number	Description
SACE-9738	In the Respond > Alerts view, when you click the Pivot to Investigate option for an IP address, no results are displayed on the Navigate view because the <code>orig_ip</code> meta is given without quotes and the query fails.
SACE-10668	You cannot query using IP address in the Event Analysis view as it is not supported.
SACE-10148	When you query for a session in the File view, Unable to create temporary file /tmp/..... error message is displayed and you will not be able to download the file.
SACE-10734	Meta value with escape sequence is truncated.
SACE-11436	ThreatExpert Search link is broken on the Investigation External Lookup.
ASOC-73008	When you Pivot to Investigate from the dashboard using an IP address, an error message is displayed due to an improper query.

Core Fixes

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

Tracking Number	Description
SACE-10351	Custom index file is not updated when it is pushed from one server to the other.
SACE-11260	Log Decoder service crashes with VALUEMAP and REGEX custom parsers.
ASOC-69957	GeoIP parser meta formats are not consistent across Decoder language and Maxmind database.
ASOC-73054	When you search any string using msearch, it displays an unexpected error.
ASOC-73238	CEF parser removes backslash (\) character.
ASOC-75006	Syslog Octet counting protocol logic stops Log Decoder.
ASOC-78912	NetWitness appliance service crashes with SIGABRT during service monitoring on the Log Decoder.

Admin Fixes

Tracking Number	Description
SACE-10992	Recurring custom feed is not updating Decoders when you select a Decoder Group List.
SACE-10682	On the Event Source Monitoring tab, if you sort by ascending or descending order, the Idle time column is not sorted.
SACE-11478	Unable to edit core attributes of an Active Directory user.
ASOC-79402	When you change the value of the Schedule Recurrence for the Respond data-source in the ContextHub configuration, it is not saved.
ASOC-76477	Unable to log in to the Active Directory using UserPrincipalName.

Windows Collector Fixes

Tracking Number	Description
ASOC-75636	Windows Legacy Collector pulls limited logs from certain event sources.

Archiver Fixes

Tracking Number	Description
SACE-10744	Unable to push <code>index-archiver-custom.xml</code> from one Archiver to other Archiver services.
SACE-10835	In the Archiver configuration, when you try to include any meta on the Meta Include tab, the default meta key word gets added automatically. If you remove this meta selection and click Apply , the <code>word</code> meta is not removed.
ASOC-75691	Unable to view <code>event.time</code> and <code>event.user</code> meta in the Archiver > View > Config > General tab.

Upgrade Fixes

Tracking Number	Description
ASOC-78279	After updating to 11.2.1.1, Reporting Engine restarts multiple times.
ASOC-78205	After updating to 11.2.1, Broker service on Malware appliance crashes.
ASOC-75542	After updating to 11.2, Active Directory user authentication fails intermittently.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.2.1.2.

Component	Version Number
NetWitness Platform Decoder	11.2.1.2-9503.5

NetWitness Platform Concentrator	11.2.1.2-9503.5
NetWitness Platform Broker	11.2.1.2-9503.5
NetWitness Platform Log Decoder	11.2.1.2-9503.5
NetWitness Platform Archiver (Workbench)	11.2.1.2-9503.5
NetWitness Platform Event Stream Analysis Server	11.2.1.2-91.5
NetWitness Platform Appliance	11.2.1.2-9503.5
NetWitness Platform Console	11.2.1.2-9503.5
NetWitness Platform Legacy Web Server	11.2.1.2-190716063058.5
NetWitness Platform Log Player	11.2.1.2-9503.5
NetWitness Platform SDK	11.2.1.2-9503.5
NetWitness Platform Legacy Windows Collector	11.2.1.2-14704.5
NetWitness Platform Reporting Engine	11.2.1.2-5807.5
NetWitness Platform Security Server	11.2.1.2-190710013259.5
NetWitness Platform SMS Server	11.2.1.2-4484.5

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 Instructions

You need to read the information and follow these procedures for updating NetWitness Platform version 11.2.1.2.

The following update paths are supported for NetWitness Platform 11.2.1.2:

- 11.1.x.x to 11.2.1.2
- 11.2.x.x to 11.2.1.2

To update NetWitness Platform to 11.2.1.2 from either of these versions, you must have files for 11.2.0.0 (base release), 11.2.1.0 (service pack release), 11.2.1.1 (patch release), and 11.2.1.2 (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 update 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 11.2.1.2 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 11.2.1.2, 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:

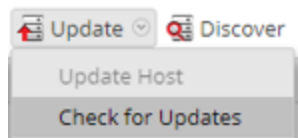
1. The “Automatically download information about new updates every day” option is checked and is applied in **ADMIN > System > Updates**.
2. Go to **ADMIN > Hosts > Update > Check for Updates** to check for updates. The Host page displays the **Update Available** status.
3. 11.2.1.2 is available under **Update Version** column.


Note: If you have custom certs, do the following to move custom certs from /etc/pki/nw/trust/import/ directory to /root/cert:

- 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 **11.2.1.2** 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 are changed for 11.2.1.2, 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 11.2.1.2 update files, from RSA Link (<https://community.rsa.com/>) > NetWitness Platform > RSA NetWitness Logs and Network > Downloads > RSA Downloads to a local directory: `netwitness-11.2.1.2.zip`.

Updating from	Download and Stage File
11.1.x.x	<code>netwitness-11.2.0.0.zip</code> , <code>netwitness-11.2.1.0.zip</code> , <code>netwitness-11.2.1.1.zip</code> , and <code>netwitness-11.2.1.2.zip</code>
11.2.0.0 or 11.2.0.1	<code>netwitness-11.2.1.0.zip</code> , <code>netwitness-11.2.1.1.zip</code> and <code>netwitness-11.2.1.2.zip</code>
11.2.1.0	<code>netwitness-11.2.1.1.zip</code> , and <code>netwitness-11.2.1.2.zip</code>
11.2.1.1	<code>netwitness-11.2.1.2.zip</code>

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 to 11.2.1.2, 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 11.2.1.2 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. **If you are updating from 11.1.x.x**, 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. For more information on packages, see [Prerequisites](#):

```
/tmp/upgrade/11.2.0.0
```

```
/tmp/upgrade/11.2.1.0
```

```
/tmp/upgrade/11.2.1.1
```

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
```

```
unzip netwitness-11.2.1.1.zip -d /tmp/upgrade/11.2.1.1
```

2. **If you are updating from 11.2.x.x**, 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. For more information on packages, see [Prerequisites](#):

```
/tmp/upgrade/11.2.1.0
```

```
/tmp/upgrade/11.2.1.1
```

and then extract the zip packages for those releases:

```
unzip netwitness-11.2.1.0.zip -d /tmp/upgrade/11.2.1.0
```

```
unzip netwitness-11.2.1.1.zip -d /tmp/upgrade/11.2.1.1
```

3. Stage 11.2.1.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.2.1.2` and extract the zip package.

```
unzip netwitness-11.2.1.2.zip -d /tmp/upgrade/11.2.1.2
```

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

4. Initialize the update, using the following command:

```
upgrade-cli-client --init --version 11.2.1.2 --stage-dir /tmp/upgrade
```

5. Update Netwitness Server, using the following command:

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.1.2
```

6. When the component host update is successful, reboot the host from the NetWitness UI.
7. 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, the patch will install correctly.:

```
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)
```

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 11.2.1.2 repo set under the same directory as 11.2.0.0.

1. Stage 11.2.1.2 by creating a directory on the NetWitness Server at /tmp/upgrade/11.2.1.2 and extract the zip package.

```
unzip netwitness-11.2.1.2.zip -d /tmp/upgrade/11.2.1.2
```

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

2. Initialize the update using the following command:

```
upgrade-cli-client --init --version 11.2.1.2 --stage-dir /tmp/upgrade
```

3. Update Netwitness Server using the following command:

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
11.2.1.2
```

4. When the component host update is successful, reboot the host from the 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, the patch will install correctly. :

```
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)
```

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

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

- [Post Update Tasks if you are Updating From 11.1.x.x](#)
- [Post Update Tasks if you are Updating From 11.2.x.x](#)

Post Update Tasks if you are Updating From 11.1.x.x

Perform all the tasks in this section if you are updating from 11.1.x.x.

Task 1 - Update HIVE version

If you are updating from 11.1.x.x, you must install 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 the `/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 11.2.1.2 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.

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

```
rpm -qi |grep pam_radius  
yum erase pam_radius
```
2. To install the `pam_radius_auth` package, execute the following command:

```
yum install pam_radius_auth
```

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

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
```

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

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

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

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

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
```

Post Update Tasks if you are Updating From 11.2.x.x

Perform all the tasks in this section if you are updating from 11.2.x.x.

Task 1 - Update HIVE version

If you are updating from 11.2.0.0, 11.2.0.1 to 11.2.1.2, you must install 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 - Restart the Respond Server

Restart the Respond server:

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

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Platform 11.2.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/112
RSA Content for RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

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
1.0	30-July	Final Draft