RSA NETWITNESS® SUITE

Release Notes

for Version 11.1.0.1

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

Introduction

This document lists enhancements and fixes in RSA NetWitness Suite 11.1.0.1. Read this document before deploying or updating RSA NetWitness Suite 11.1.0.1.

- Build Numbers
- What's New
- Update Instructions
- Fixed Issues
- Known Issues
- Product Documentation
- Contacting Customer Care
- Revision History

Build Numbers

The following table lists the build numbers for various components of RSA NetWitness Suite 11.1.0.1.

Component	Version Number
Netwitness Suite Web Server	11.1.0.1-180413052407
Netwitness Suite Decoder	11.1.0.1-9043
Netwitness Suite Concentrator	11.1.0.1-9043
Netwitness Suite Broker	11.1.0.1-9043
Netwitness Suite Log Decoder	11.1.0.1-9043
Netwitness Suite Archiver (Workbench)	11.1.0.1-9043
Netwitness Suite Event Stream Analysis Server	11.1.0.1-436
Netwitness Suite Appliance	11.1.0.1-9043
Netwitness Suite Archiver	11.1.0.1-9043
Netwitness Suite Cloud Gateway Server	11.1.0.1-180413152801
Netwitness Suite Concentrator	11.1.0.1-9043
Netwitness Suite Console	11.1.0.1-9043
Netwitness Suite Endpoint Agents	11.1.0.1-1804190837
Netwitness Suite Endpoint Server	11.1.0.1-180419015718
Netwitness Suite Investigate Server	11.1.0.1-180417084126
Netwitness Suite Legacy Web Server	11.1.0.1-180413052407
Netwitness Suite Log Player	11.1.0.1-9043
Netwitness Suite Orchestration Server	11.1.0.1-180323104408
Netwitness Suite Respond Server	11.1.0.1-180322090443
Netwitness Suite SDK	11.1.0.1-9043

What’s New

The RSA NetWitness Suite 11.1.0.1 patch release provides fixes to 11.1.0.0. This document describes the enhancements and fixes included in this release.

Endpoint Insights

Endpoint Meta Mapping. APIs are introduced to view the default endpoint meta mapping or modify the endpoint meta mapping; `get-default, get-custom, set-custom`. For more information on these APIs, see the *Endpoint Insights Configuration Guide*.

NetWitness Investigate

Sorted Service List in the Event Analysis View. Services are sorted alphabetically in the Event Analysis view service drop-down menu.

Operator indicator when building a query in Event Analysis. When analysts are adding filters to a query in the Event Analysis view, the auto-complete drop-down list of operators has a stopwatch indicator to mark operations that take more time to execute. For more information on these features, see the *NetWitness Investigate User Guide*.

Update Instructions

You need to read the information and follow these procedures for updating RSA NetWitness Suite version 11.1.0.1.

The following update paths are supported for RSA NetWitness Suite 11.1.0.1:

- RSA NetWitness Suite 11.1.0.0 to 11.1.0.1

For update paths supported for 11.1.0.0, see the *Update Guide for Version 11.0.x to 11.1*.

You can update 11.1.0.1 patch using one of the following options:

- If the NetWitness Server has internet connectivity to Live Services, the NetWitness Suite 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

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

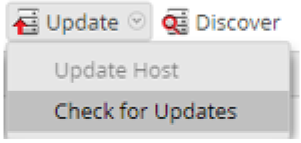
Make sure that:

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. 11.1.0.1 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 update in your Local Update Repository for the selected host.
5. Select **11.1.0.1** 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 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 11.1.0.1, 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 file, which contain all the NetWitness Suite 11.1.0.1 update files, from RSA Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:
  `netwitness-11.1.0.1.zip`

Procedure

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

> **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 11.1.0.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.1.0.1` and extract the zip package.
   ```
   unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1
   ```
   > **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 update, using the following command:
   ```
   upgrade-cli-client --init --version 11.1.0.1 --stage-dir /tmp/upgrade
   ```
3. Update Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
   11.1.0.1
   ```
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).

Note: To Enable Respond Server, you need update ESA Primary and restart the Respond server.

External Repo Instructions for CLI Update

Note: External repo which is to be setup should have 11.1.0.1 repo set under the same directory as 11.1.0.0.

1. Stage 11.1.0.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.1.0.1` and extract the zip package.

   ```
   unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1
   ```

   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 update, using the following command:

   ```
   upgrade-cli-client --init --version 11.1.0.1 --stage-dir /tmp/upgrade
   ```

3. Update Netwitness Server, using the following command:

   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
   11.1.0.1
   ```

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).

Note: To Enable Respond Server, you need update ESA Primary and restart the Respond server.

Post-Update Tasks

Task 1 (Optional) - Move the custom certs

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

Task 2 (Conditional) - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.1.x.x using the `pam_radius` package, you must reconfigure it in 11.1.0.1 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, excute 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 3 - Restart the Respond Server

Restart the Respond server:

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

Fixed Issues

This section lists issues fixed since the last major release.

Server Fixes

Tracking Number	Description
ASOC-50835	Integration-server service is missing on the UI after update.

Investigate Fixes

Tracking Number	Description
ASOC-50771	If you go to Event Analysis by way of the Events view, either by clicking the Event Analysis link or by right-clicking one of the events, the right-click options on meta values do not work.
ASOC-49854	The service keeps loading infinitely.
ASOC-51011	RSA Endpoint Analysis, RSA Outbound SSL/TLS, and RSA Outbound HTTP column groups and meta groups are not created after upgrading from 10.6.5 to 11.x.
ASOC-48710	Getting an "unexpected error has occurred" message when access removed or rolled out sessions.
ASOC-50924	Pivot to Event Analysis from Endpoint is supported only for IPv4.
ASOC-50712	Cannot add meta entities to a custom column group in the Events view with the Optimize Investigation Page Loads option disabled.

Endpoint Insights Fixes

Tracking Number	Description
ASOC-49846	No option to disable log collection in Windows agent.

ASOC-49957	A warning message was being written in logs (/var/log/messages). This message has now been removed.
ASOC-50782	In 11.1.0.1, the package names for the Linux installer have changed from: • nwe-agent.rpm to nwe-agent.i686.rpm for Linux 32-bit. • nwe-agent(64-bit).rpm to nwe-agent.x86_64.rpm for Linux 64-bit.
ASOC-50162	Endpoint meta integration is updated so the mappings for the meta keys align better with metadata generated from logs and packets.

Telemetry Fixes

Tracking Number	Description
ASOC-50740	Telemetry JSON updated with Account Attribution details at Service levels like Decoder, Log Decoder and Malware.

Respond Fixes

Tracking Number	Description
ASOC-51133	Respond does not handle notification related load gracefully and is crashing.

Context Hub Fixes

Tracking Number	Description
ASOC-51110	ESA rule with a CH List was getting disabled on System Restart.
ASOC-51069	ESA rule associated with a large context-hub list fails to get deployed.

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 11.1.0.0 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/.

Upgrade

The following known issues occur during upgrade from 11.1.0.x :

Endpoint Incidents are not being created

Tracking Number: ASOC-51480

Problem: Endpoint events with a source IP are working fine, but Endpoint events with a detector IP are not being aggregated by the Endpoint incident rule and do not create incidents. In NetWitness Suite 11.1, the GroupBy field of the “High Risk Alerts: NetWitness Endpoint” incident rule was changed from “Risk Score” to “Source IP Address.”.

Workaround: For upgrades from 10.6.x to 11.1:

1. Go to **CONFIGURE** > **Incident Rules**. The Incident Rules List view is displayed.
2. Click the link in the **Name** field of **High Risk Alerts: NetWitness Endpoint** incident rule to edit it.
3. Change the **GroupBy** field value to **Risk Score**.

For fresh installs:

1. Go to **CONFIGURE** > **Incident Rules**. The Incident Rules List view is displayed.
2. Click the link in the **Name** field of **High Risk Alerts: NetWitness Endpoint** incident rule to edit it.
3. Change the **GroupBy** field value to **Risk Score** or any other GroupBy field value.

Duplicate Alerts in Respond

Tracking Number: ASOC-50994

Problem: Duplicate Alerts in Respond are observed from certain sources like Reporting Engine.

Workaround: Follow these steps to delete obsolete federated exchanges that would cause duplicate alerts in Respond:

1. Login to https://<adminServerIP>:15671/ Rabbitmq cluster with the following credentials.

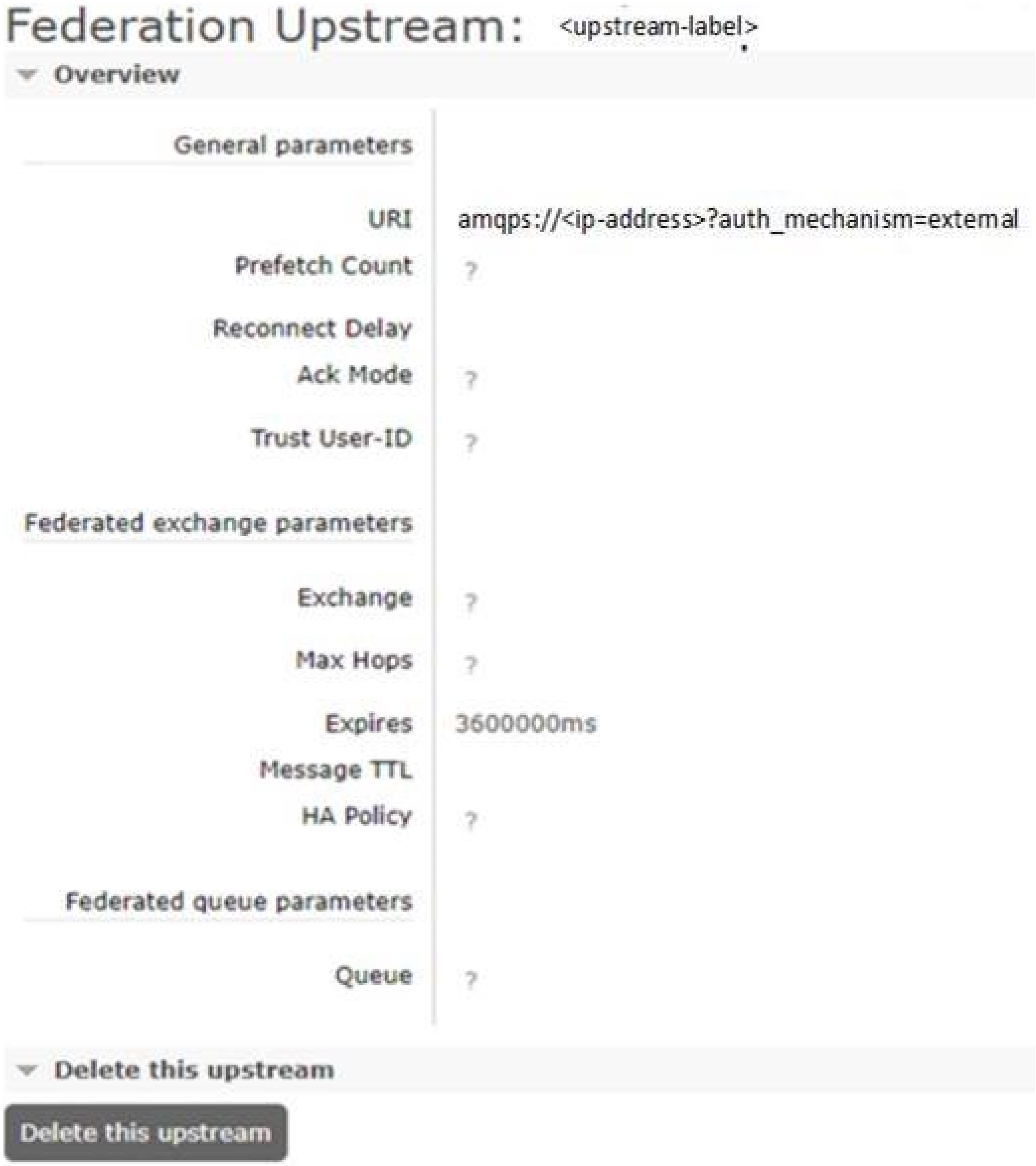
username: deploy_admin

password: <deployment-password-used-during-NW-Server-host-11.x-setup>

2. Go to **Admin** > **Federation Upstream**.
3. Select the URI with **NW Server host IP address** to it. The **Federation Upstream** view is .displayed.
4. Make sure the URI is similar to the following value

```
amqps : // <adminServerIP>?auth_mechanism=external
```

5. Click **Delete the Upstream** to delete the URI.



Federation Upstream: <upstream-label>

Overview

General parameters

URI amqps://<ip-address>?auth_mechanism=external

Prefetch Count ?

Reconnect Delay

Ack Mode ?

Trust User-ID ?

Federated exchange parameters

Exchange ?

Max Hops ?

Expires 3600000ms

Message TTL

HA Policy ?

Federated queue parameters

Queue ?

Delete this upstream

Endpoint Insights

After agent update, the agent version is not reflected in the UI

Tracking Number: ASOC-52761

Problem: When you update the agent version from 11.1 to 11.1.0.1, the agent version shows 11.1 in the Hosts view.

Workaround: In the **Investigate** > **Hosts** view, select the host on which you installed the latest version of the agent, and click **Start Scan**. The agent version is updated to 11.1.0.1.

Not able to forward logs on 6514, when only TLS 1.2 is enabled in Log Decoder

Tracking Number: ASOC-52761

Problem: In Log Decoder if you have `/sys/config/ssl.context.options` set to `SSL_OP_NO_SSLv2,SSL_OP_NO_SSLv3,SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1` and allow only TLS1.2 to accept logs, then log forwarding is not working when forwarded to 6514 from agents deployed in Windows 7 SP1 and Windows 2008.

Workaround: Refer to the article on how to enable TLS 1.2: https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Suite 11.1.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Upgrade Instructions	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Upgrade Checklist	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Contacting Customer Care

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

RSA SecurCare	https://knowledge.rsasecurity.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/docs/DOC-1294
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 Suite product or application you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
0.1	17-April	RTO Draft