RSA NETWITNESS® SUITE

Release Notes

for Version 11.1.0.2

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 7

Build Numbers 8

Update Instructions 9

Update Tasks 9

Offline Method (No connectivity to Live Services): Update using the Command Line Interface 9

Prerequisites 9

Procedure 9

External Repo Instructions for CLI Update 10

Post-Update Tasks 11

Task 1 (Optional) - Move the custom certs 11

Task 2 - Restart the Respond Server 12

Fixed Issues 13

Server Fixes 13

Known Issues 14

Investigation 14

Log Decoder 15

Product Documentation 17

Contacting Customer Care 18

Preparing to Contact Customer Care 18

Revision History 19

Introduction

This document lists the fixes in RSA NetWitness Suite 11.1.0.2. Read this document before deploying or updating RSA NetWitness Suite 11.1.0.2.

- Build Numbers
- Update Instructions
- Fixed Issues
- Product Documentation
- Contacting Customer Care
- Revision History

Build Numbers

The following table lists the build numbers for various components of RSA NetWitness Suite 11.1.0.2.

Component	Version Number
Netwitness Suite Web Server	11.1.0.2-180627122312.5
Netwitness Suite Decoder	11.1.0.2-9051.5
Netwitness Suite Concentrator	11.1.0.2-9051.5
Netwitness Suite Broker	11.1.0.2-9051.5
Netwitness Suite Log Decoder	11.1.0.2-9051.5
Netwitness Suite Archiver (Workbench)	11.1.0.2-9051.5
Netwitness Suite Event Stream Analysis Server	11.1.0.2-7.5.g811f4fb.el7
Netwitness Suite Appliance	11.1.0.2-9051.5
Netwitness Suite Archiver	11.1.0.2-9051.5
Netwitness Suite Console	11.1.0.2-9051.5.
Netwitness Suite Integration Server	11.1.0.2-180627081332.5
Netwitness Suite Legacy Web Server	11.1.0.2-180627081332.5
Netwitness Suite Log Player	11.1.0.2-9051.5
Netwitness Suite Reporting Engine Server	11.1.0.2-5722.5
Netwitness Suite SDK	11.1.0.2-9051.5

Update Instructions

You need to read the information and follow these procedures for updating RSA NetWitness Suite version 11.1.0.2.

The following update paths are supported for RSA NetWitness Suite 11.1.0.2:

- RSA NetWitness Suite 11.1.0.0 to 11.1.0.2
- RSA NetWitness Suite 11.1.0.1 to 11.1.0.2

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

You can update 11.1.0.2 patch using the Command Line Interface:

Note: The Live Update method using the UI is not available for this release.

Update Tasks

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

Note: If you are updating from 11.1.0.0, you must also download the NetWitness Suite 11.1.0.1 files (netwitness-11.1.0.1.zip) and set them up in the staging folder along with the 11.1.0.2 files, as described below.

Prerequisites

Make sure that:

- You have downloaded the following file, which contain all the NetWitness Suite 11.1.0.2 update files, from RSA Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:
  `netwitness-11.1.0.2.zip`

Procedure

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

Note: If you are updating from version 11.1.0.0, perform step 1 to create a `/tmp/upgrade/11.1.0.1` directory for the 11.0.0.1 files, in addition to creating a `/tmp/upgrade/11.1.0.2` directory for the 11.1.0.2 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 11.1.0.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.1.0.2` and extract the zip package.
   ```
   unzip netwitness-11.1.0.2.zip -d /tmp/upgrade/11.1.0.2
   ```
   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 11.1.0.2 --stage-dir /tmp/upgrade
   ```
3. Update Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.2
   ```
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 11.1.0.2 repo set under the same directory as 11.1.0.0.

1. Stage 11.1.0.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.1.0.2` and extract the zip package.
   ```
   unzip netwitness-11.1.0.2.zip -d /tmp/upgrade/11.1.0.2
   ```

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 11.1.0.2 --stage-dir /tmp/upgrade`
3. Update Netwitness Server, using the following command:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.2`
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.

If you configured PAM Radius authentication in 11.1.x.x using the `pam_radius` package, you must reconfigure it in 11.1.0.2 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.

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 2 - Restart the Respond Server

Restart the Respond server:

```
service rsa-nw-respond-server restart
```

Fixed Issues

This section lists issues fixed since the last major release.

Server Fixes

Tracking Number	Description
SACE-7348	On the Decoder configuration Feeds and Parsers tabs, if you sort by ascending or descending order, the list is not sorted.
SACE-8090	Older jobs such as PCAP, Logs, and Packets are not automatically removed.
SACE-8966	Unable to export PCAP files due to an error "Out of Memory" is displayed.

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/.

Investigation

Unable to export logs from Events View for Log Decoder.

Tracking Number: ASOC-59145

Problem: After you update the Admin Server to 11.1.0.2, and you export the logs for the Log Decoder, the exported file is empty even though the logs are available in the Log Decoder.

Note: The below mentioned workaround is not required if you do not have a specific reason to export logs from Log Decoder. You can continue to investigate and export logs from Log Decoder through Concentrator by applying the filters `did=<decode_id>`.

Workaround: You must index the medium meta if you want to export logs for the Log Decoder. The following steps indexes the new events and you can export these events.

1. Update the custom index config file `index-logdecoder-custom.xml`

```
<key description="Medium" level="IndexValues" name="medium"
format="UInt8" valueMax="100" defaultAction="Hidden">
<aliases>
<alias format="$alias" value="1">Ethernet</alias>
<alias format="$alias" value="2">Tokenring</alias>
<alias format="$alias" value="3">FDDI</alias>
<alias format="$alias" value="4">HDLC</alias>
<alias format="$alias" value="5">NetWitness</alias>
<alias format="$alias" value="6">802.11</alias>
<alias format="$alias" value="7">802.11 Radio</alias>
<alias format="$alias" value="8">802.11 AVS</alias>
<alias format="$alias" value="9">802.11 PPI</alias>
<alias format="$alias" value="10">802.11 PRISM</alias>
<alias format="$alias" value="11">802.11 Management</alias>
```

```
<alias format="$alias" value="12">802.11 Control</alias>
<alias format="$alias" value="13">DLT Raw</alias>
<alias format="$alias" value="32">Logs</alias>
<alias format="$alias" value="33">Correlation</alias>
<alias format="$alias" value="34">Relationship</alias>
</aliases>
</key>
```

2. Restart the Log Decoder.

   If the Log Decoder is not restarted, you need to wait until the next index-save.

Log Decoder

Log Decoder service crashes when ESM Discovery auto mapping is enabled.

Tracking Number: SACE-9550

Problem: Log Decoder service crashes on `ipdevice` mapping updates from automated ESM discovery functionality on the Admin Server

Workaround: Disable ESM automated `ipdevice` mapping updates and entries on Node 0.

1. Login as root:

   `/opt/rsa/sms/bin/automap -off`

2. Check if the feature is disabled using command:
   `/opt/rsa/sms/bin/automap -?`

   Verify the automatic mapping is disabled "INFO com.rsa.smc.esm.core.jmx.tools.JmxAutomaticMapping".

3. Remove the existing automated mapping settings on Log Decoder. The Automated mappings are identified with an entry `soft=true`.

   a. Select the Log Decoder service.

   b. In the Actions coloum, select **View** > **Explore**.

   c. In the node, select decoder/parsers.

   d. Right click on the **parser** node and click **properties.**

   e. Select **ipdevice command**from the dropdown and enter `op=describe` in the Parameters and click Send.

      The list of mappings updated by ESM discovery with `soft=true` setting are displayed.

```
<addressmap-schema>
<DeviceEntry ipv4="1.1.1.1" device="foo"
lastUpdated="1528487466" soft="true"/>
<DeviceEntry ipv4="2.2.2.2" lastUpdated="1528489179"
soft="true">
<DeviceSubEntry lcid="lcid" device="bar"/>
</DeviceEntry>
</addressmap-schema>
```

In the ipdevice command , give the parameters `op=remove entries="<device ip1>=<device-name1> <device ip2>=<device-name2>"` and click Send. This will remove the device mappings.

For Example: `op=remove entries="1.1.1.1=foo 2.2.2.2=bar"`

Note: If there are soft mappings then you need to remove all select ipdevice command, give the parameters `op=remove entries=*` and click send. This will remove all mappings.

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 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 Suite product or application you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
0.1	09-July	Final Draft