RSA NETWITNESS® SUITE

Release Notes

for Version 11.0.0.3

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 11.0.0.3. Read this document before deploying or updating RSA NetWitness Suite 11.0.0.3.

Build Numbers

The following table lists the build numbers for various components of RSA NetWitness Suite 11.0.0.3.

Component	Version Number
Netwitness Suite Web Server	11.0.0.3-180316060323.5
Netwitness Suite Decoder	11.0.0.3-8746.5
Netwitness Suite Concentrator	11.0.0.3-8746.5
Netwitness Suite Broker	11.0.0.3-8746.5
Netwitness Suite Log Decoder	11.0.0.3-8746.5
Netwitness Suite Log Collector	11.0.0.3-14602.5
Netwitness Suite Archiver (Workbench)	11.0.0.3-8746.5
Netwitness Suite Event Stream Analysis	11.0.0.3-413.g85aac8b.5

Fixed Issues

This section lists issues fixed since the last major release.

Security Fixes

Tracking Number	Description
ASOC-48910	Openjdk Security Update https://access.redhat.com/errata/RHSA-2018:0095
ASOC-48093	Kernel Security Update https://access.redhat.com/errata/RHSA-2018:0007
ASOC-46054	Samba Security Update https://access.redhat.com/errata/RHSA-2017:3260
ASOC-46046	Curl Security Update https://access.redhat.com/errata/RHSA-2017:3263
ASOC-43723	Tcpdump Security Update https://access.redhat.com/errata/RHSA-2017:1871

Server Fixes

Tracking Number	Description
SACE-8477	Login Banner tab is missing on Netwitness 11.0 UI (Admin > Security > Tab).
ASOC-44650	Even if the update is successful using the Command Line Interface, a message displays the message "Update path not supported."

Respond Fixes

Tracking Number	Description
SACE-8822	After upgrading to 11.0.0.2, the Respond Server service is disabled.

Core Fixes

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

Tracking Number	Description
SACE-8469	Errors due to default table-map.xml settings while deploying feed to Log Decoder.

Update Instructions

You need to read the information and follow these procedures for updating RSA NetWitness Suite from version 11.0.0.0 to version 11.0.0.3.

The following update paths are supported for RSA NetWitness Suite 11.0.0.3:

- RSA NetWitness Suite 11.0.0.0 to 11.0.0.3
- RSA NetWitness Suite 11.0.0.1 to 11.0.0.3
- RSA NetWitness Suite 11.0.0.2 to 11.0.0.3

You can update 11.0.0.3 patch using the Command Line Interface (CLI) to apply the patch.

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

Update Tasks

Note: If you are updating from 11.0.0.0, you must also download the NetWitness Suite 11.0.0.1 and 11.0.0.2 update files (netwitness-11.0.0.1.zip and netwitness-11.0.0.2.zip) and set them up in the staging folder along with the 11.0.0.3 files, as described below.

Prerequisites

Make sure that:

- You have 11.0.0.0 RPMs installed on the NW Server. You can verify this by checking the `/var/netwitness/common/repo/` for an 11.0.0.0 directory with .rpm files inside of its directory structure. If this directory does not exist, contact Customer Support. For information, see Contacting Customer Care.
- You have downloaded the following file, which contain all the NetWitness Suite 11.0.0.3 update files, from RSA Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:
  `netwitness-11.0.0.3.zip`

Procedure

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

Note: If you are updating from version 11.0.0.0, perform step 1 to create a `/tmp/upgrade/11.0.0.1` and `/tmp/upgrade/11.0.0.2` directory for the 11.0.0.1 and 11.0.0.2 files, in addition to creating a `/tmp/upgrade/11.0.0.3` directory for the 11.0.0.3 files.

1. Stage 11.0.0.3 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.0.0.3` and extract the zip package.

   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 on the NetWitness Server, using the following command:
   `upgrade-cli-client --init --version 11.0.0.3 --stage-dir /tmp/upgrade`
3. Update NetWitness Server, using the following command:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.0.0.3`
4. When the component host update is successful, restart the host.
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

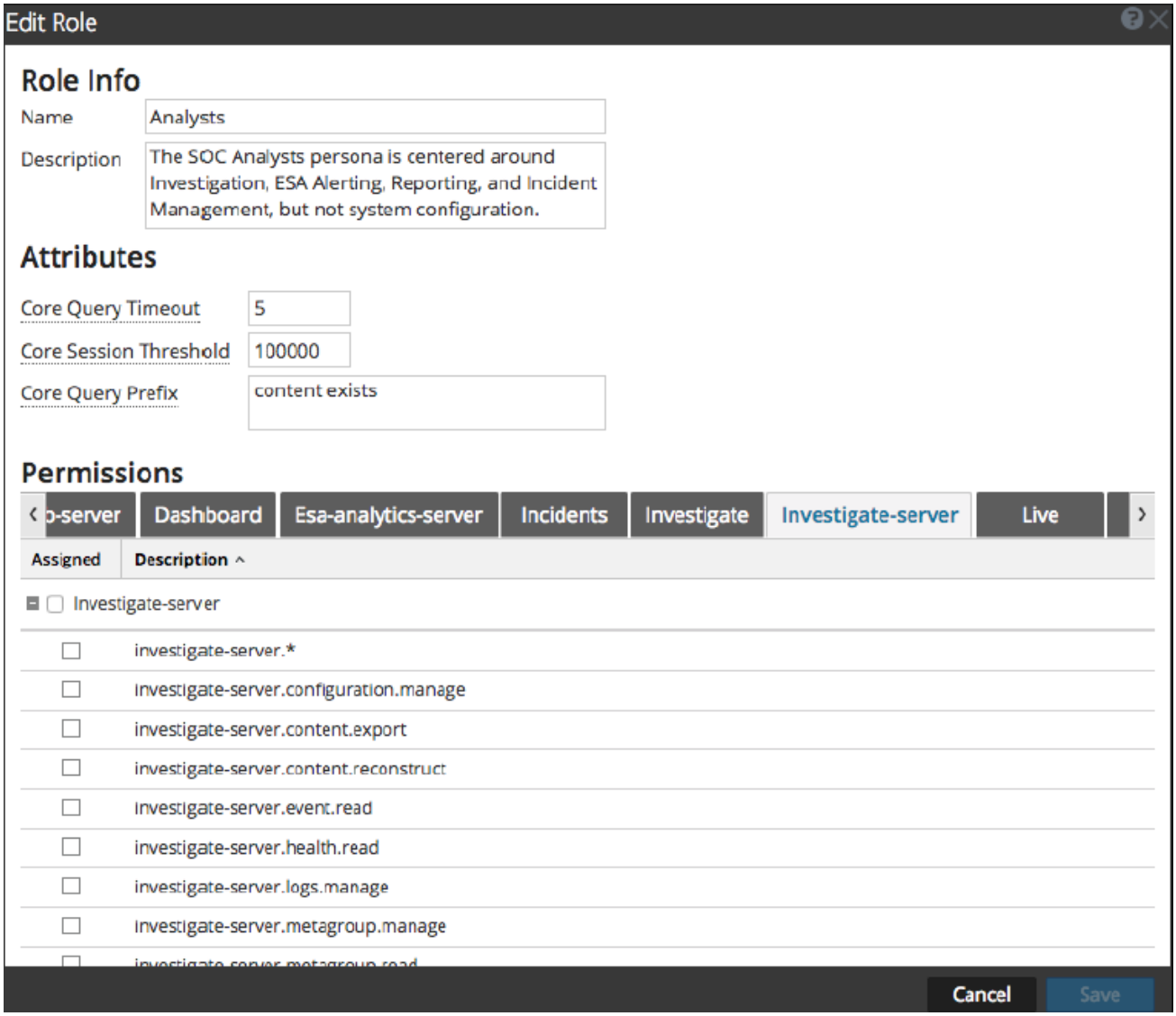
(Optional, for 11.0.0.0 to 11.0.0.3 updates) Task 1: Reset Event Analysis Access with Role Attributes

As the new Investigate Event Analysis does not enforce user and role attributes, you must lock down access to the Event Analysis workflow so users cannot bypass permission attributes:

1. Go to **ADMIN** > **Security**.
2. Select **Roles** tab.
3. Select a role and click  .

4. Select the **Investigate-server** tab.
5. Clear the **investigate-server*** checkbox.

Note: By default, this checkbox is selected on update.



The following three access permissions have been added to allow further access control to the Event Analysis.

- **investigate-server.event.read** provides access to meta, meta panel, and events list in Event Analysis.
- **investigate-server.content.export** provides access to downloads of files, PCAPs, logs, or endpoint events in Event Analysis.

- **investigate-server.content.reconstruct** provides access to packet analysis, text analysis, and file analysis views in Event Analysis.

  - If you are not using user or role attributes, select all the three permissions to provide normal access.

  - If you are using user or role attributes to restrict access to what users can view and want to limit all access to the Event Analysis, make sure these three and **investigate-server.*** permissions are not selected for each role the user is in.

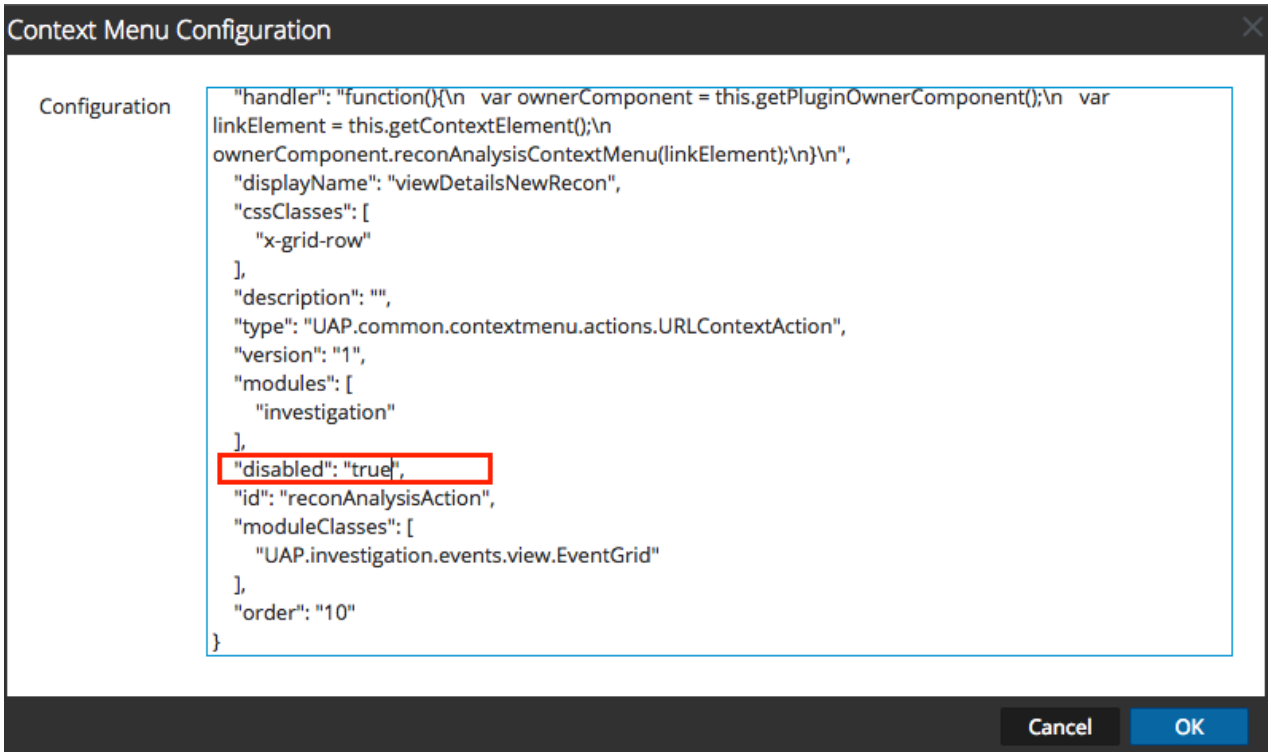
Note: By default, the new permissions are not selected for all roles. These permissions will not be applied even if selected unless the investigate-server.* permission is disabled.

6. Click **Save**.

To lock down access to the Context Menu Action on Event Analysis, which is enabled by default, do the following:

1. Navigate to **ADMIN** > **System.**
2. Select **Context Menu Actions** from the left panel.
3. Select **Event Analysis**, and click  .

   The Context Menu Configuration dialog is displayed.



4. Edit the disabled parameter and set it to "True".
5. Click **OK**.

Task 2: (Conditional) For Automated Threat Detection - Change "Group By" from “Domain for Suspected C&C" to “Domain”.

If you used Automated Threat Detection in 10.6.4.x, you must complete the following steps to change **Group By** from **Domain for Suspected C&C** back to **Domain**.

1. Log in to NetWitness Suite 11.0.0.3
2. Click **CONFIGURE** > **Incident Rules** > **Aggregation Rule**.
3. Select the **Suspected Command & Control Communication by Domain** rule, and double-click to open it.
4. Change the **Group By** condition to **Domain**.

For more information, see the *NetWitness Suite Automated Threat Detection Guide*. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

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 11.0.0.3 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/.

Log Collector

The vsftpd service has been changed to support only TLSv1.2

Tracking Number: ASOC-42497, ASOC-44863

Problem: For compliance reasons, the vsftpd service configuration on Log Collector and Virtual Log Collector nodes has been changed to support only TLSv1.2 and high encryption ciphers. TLSv1.0, 3DES and NULL encryption will no longer be accepted by default. This will break uploading of log files by FTPS protocol from event sources that do not support higher encryption.

Workaround: Use the following procedures to restore collection.

If you have event sources requiring TLSv1.0, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_tlsv1=NO` to `ssl_tlsv1=YES`
2. Restart **vsftpd** service by running this command:

   systemctl restart vsftpd

If you have event sources requiring 3DES and/or NULL encryption, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_ciphers=HIGH:-3DES:-aNULL` to `ssl_ciphers=HIGH`
2. Restart **vsftpd** service by running this command:

   systemctl restart vsftpd

Core Services

After updating the Packet Decoder to 11.0.0.3 ,in some cases required 10g drivers are not loaded into the kernel .

Tracking Number: ASOC-51212

Problem: Even if the update is successful on packet decoder, capture start may fail due to drivers unavailable in some cases.

Workaround: Perform the following steps to load 10g drivers into the Kernel.

1. Verify that Packet Decoder is reporting the following error “No suitable PF_RING ixgbe driver installed” in `/var/log/message`.
2. Verify that kernel is upgraded successfully and diaplays the following version “3.10.0-693.11.6.el7"
3. Verify that “dkms status” command is not displaying any drivers with above mentioned kernel version.

   Note: If “dkms status” is showing ixgbe-zc and pfring drivers with the latest kernel, do not run the next steps.

4. Run the below commands to upgrade the pfring and ixgbe packages.
   - `yum reinstall ixgbe`
   - `yum reinstall pfring`
5. Reboot the Packet Decoder appliance after the upgrade and verify that the capture is able to start.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Suite 11.0.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0.0.0 Upgrade Instructions	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0.0.0 Upgrade Checklist	https://community.rsa.com/community/products/netwitness/110
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
Email	nwsupport@rsa.com
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	22-March	Final Draft