RSA NETWITNESS® SUITE

Release Notes

for Version 11.0.0.2

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

This document lists enhancements and fixes in RSA NetWitness Suite 11.0.0.2. Read this document before deploying or updating RSA NetWitness Suite 11.0.0.2.

If you encounter any issues during the update, contact Customer Support (Contacting Customer Care).

Build Numbers

The following table lists the build numbers for the components of RSA NetWitness Suite that were updated for 11.0.0.2.

Component	Version Number
Netwitness Suite Web Server	11.0.0.2-171207105055
Netwitness Suite Admin Server	11.0.0.2-171204093128
Netwitness Suite Log Collector	11.0.0.2-14600
Netwitness Suite Respond	11.0.0.2-171117075816

If you are updating to 11.0.0.2 from 11.0.0.0, the following components must be included. For more information, see Update Instructions.

Component	Version Number
Netwitness Suite Investigate Server	11.0.0.1-171018143329
Netwitness Suite Security Server	11.0.0.1-171023132845

What's New

The RSA NetWitness Suite 11.0.0.2 patch release provides additional security controls and fixes to 11.0.0.0 and 11.0.0.1. This document describes the security controls and fixes included in this release.

Fixed Issues

This section lists issues fixed since the last major release.

Security

Tracking Number	Description
ASOC-38281	RabbitMQ HTTP Management Console update from 3.6.5 to 3.6.12.
ASOC-41849	Samba Security Update https://access.redhat.com/errata/RHSA-2017:2790
ASOC-42355	nss Security Update https://access.redhat.com/errata/RHSA-2017:2832
ASOC-43717	Java-1.8.0-openjdk Security Update https://access.redhat.com/errata/RHSA-2017:2998
ASOC-43889	wget Security Update https://access.redhat.com/errata/RHSA-2017:3075

Log Decoder

Tracking Number	Description
ASOC-42542	Warehouse Connector is not displayed in the UI after installation.

User Interface

Tracking Number	Description
ASOC-43321	New users created in 11.0.0.2 (after the patch has been applied) should be sent to the Dashboard page after logging into NetWitness Suite.

Update Instructions

You need to read the information and follow these procedures for updating RSA NetWitness Suite from version 11.0.0.0 or 11.0.0.1 to version 11.0.0.2.

The following update paths are supported for RSA NetWitness Suite 11.0.0.2:

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

You can update 11.0.0.2 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 update files (`netwitness-11.0.0.1.zip`) and set them up in the staging folder along with the 11.0.0.2 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 11.0.0.2 update files, from RSA Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:
  `netwitness-11.0.0.2.zip`

Procedure

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

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

1. Stage 11.0.0.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.0.0.2` 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 11.0.0.2 --stage-dir /tmp/upgrade`
3. Update NetWitness Server, using the following command:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.0.0.2`
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

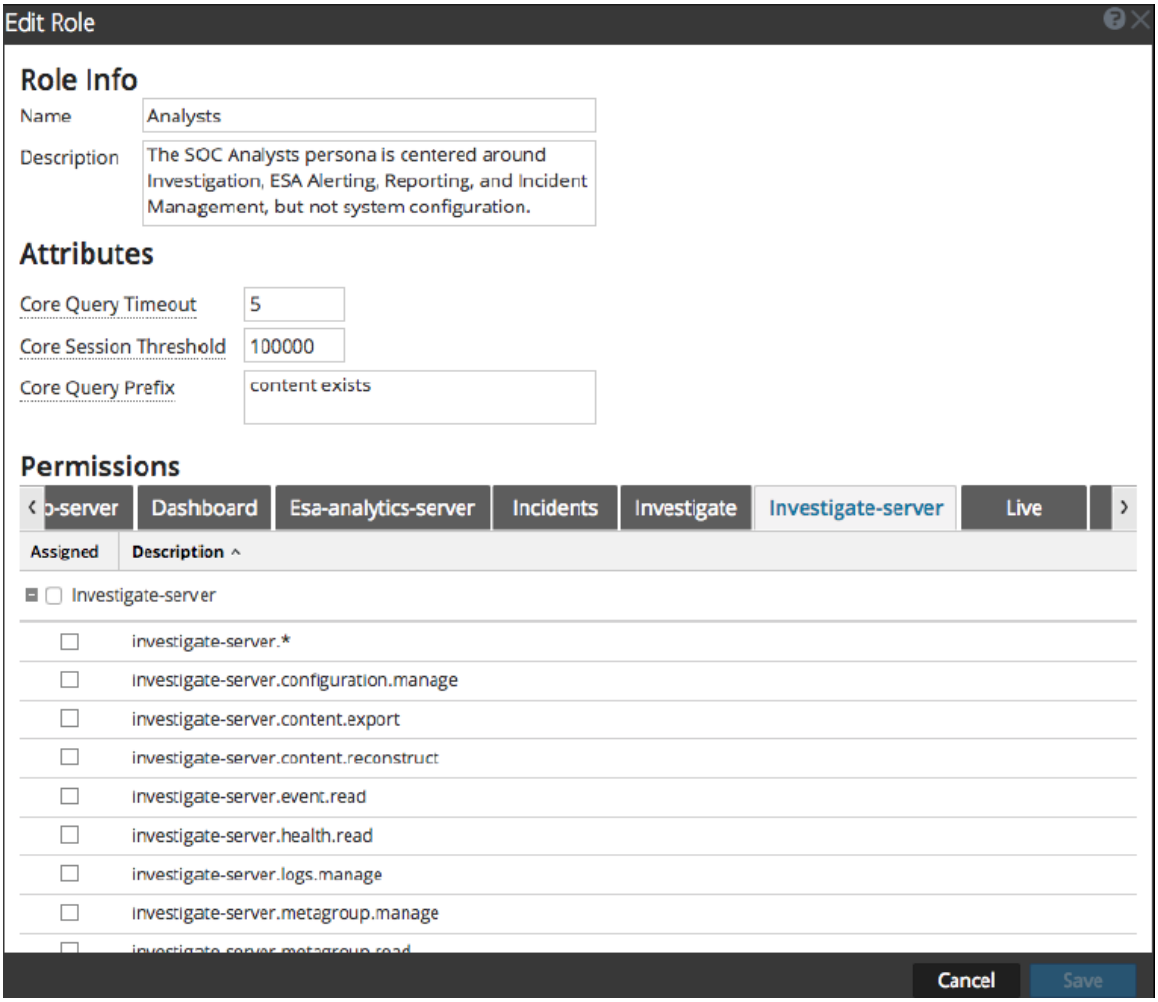
(Optional, for 11.0.0.0 to 11.0.0.2 updates) Task 1: Reset Event Analysis Access with Role Attributes

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 11.0.0.2
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.

Upgrade

The following known issues occur during upgrade from 11.0.0.0 or 11.0.0.1:

After updating to 11.0.0.2 using the Command Line Interface, the message "Update path not supported" is displayed in the host UI .

Tracking Number: ASOC-44650

Problem: Even if the update is successful using the Command Line Interface, a message displays the message "Update path not supported."

Workaround: Delete the `repo.manifest` file from `/var/netwitness/srv/www/rsa/updates/manifest` and restart the Jetty server.

The following known issues occur during the upgrade from 10.6.x to 11.0.0.0:

After upgrade from 10.6.4.x to 11.0.0.0, offline licenses are not retained.

Tracking Number: ASOC-41757

Problem: Even if you upload a new response bin file from Download Central, offline licenses still don't work. Though old files are restored in `/var/lib/fneserver`, the licenses still remain deactivated.

Workaround: Perform the following steps to restore the licenses:

1. Generate a new response bin file from Download Central.
2. Log in to Netwitness Server 11.0.0.0 (AdminServer).
3. Move ra* files (3 files) out of `/var/lib/fneserver/`
4. Log in to RSA NetWitness 11.0.0.0 UI with admin user credentials and navigate to Admin > System >Licensing Overview tab.
5. Under Licensing actions, click Refresh licenses.
6. Now, upload the response file received from Download Central under Admin > System > Licensing > Settings Tab > Upload Response.

Note: Upgrade using Online mode (RSA Netwitness Suite 11.0.0.0 connected to the Internet) works successfully and all licenses are restored after upgrade to 11.0.0.0

User Attributes are absent.

Tracking Number: ASOC-42374

Problem:When you upgrade to 11.0, the user attributes (query prefix, session timeout, and query threshold) available in SA 10.6.x are absent. The same attributes are available at the role level for use.

Workaround: If user attributes were used to restrict user access, apply patch Netwitness Suite 11.0.0.1 patch. Refer to the *Netwitness Suite 11.0.0.1 Release Notes*.

After you upgrade to 11.0.0.0, new event sources cannot be added in a mix mode deployment.

Tracking Number: ASOC-41867

Problem:After you upgrade to 11.0.0.0 and connect to 10.6.4 Log Collectors, test connections fail on the Edit UI. This is because the UI converts the collection Start Date value (int) into string date format "1970-01-01 00:00:00". You will continue to collect events from the existing event source but will not be able to add a new event source. However, in case of Bulk test connection, all values are directly fetched from REST interface and "Test connection" is successfully passed.

Workaround: Use the REST interface to add a new event source in a mix mode.

FIPS is disabled by default for the Log Collector Service

Tracking Number: ASOC-41841

Problem: FIPS is disabled by default for the Log Collector service, even if FIPS was enabled in 10.6.4.

> **Note:** Even if FIPS is enabled in 10.6.4, it becomes disabled post-migration

Workaround: To enable FIPS on the Log collector service, perform the following steps:

1. Stop the Log Collector service.
2. Open the `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` file.
3. Change the value of the following variable to **off** as described here:

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```
   to
   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```
4. Reload the system daemon by running `systemctl daemon-reload` command.
5. Restart the Log Collector service.
6. Set the FIPS mode for the Log Collector service on the UI:

   > **Note:** This step is not required in case of upgrade, if FIPS was enabled on 10.6.4.

   a. Go to ADMIN > Services.

   b. Select the Log Collector service and go to View > Config.

c. In SSL FIPS Mode, select the checkbox under Config Value and click **Apply**.

Note: To enable Log Decoder and Packet Decoder, in `/sys/config` set `ssl.fips` to ON and restart the service.

The investigation links are disabled for static charts

Tracking Number: ASOC-42136

Problem: The investigation link is disabled for the static chart (the result of the report is in chart format) which has the datasource as NetWitness Suite-Broker (This service is available by default).

Workaround: There are two workarounds for this issue:

- The rules that have the result in static chart can be viewed in Tabular format and the investigation works as expected.
- Or you can perform the following steps to fix the issue:
  1. Delete and add the NetWitness Suite-Broker again as the datasource to Reporting Engine with the same name.
  2. If the reports with static chart are scheduled reports, then in the next run, the investigation link will work as expected.
  3. If the report is an Adhoc report then, then re-run the report for getting the investigation links.

Warehouse Connector is not installed on Decoders

Problem: The Warehouse Connector is not installed on the Decoders by default.

Workaround: If, after an upgrade there is a need to re-establish a Warehouse connection, a utility is provided to reinstall the service. The utility is deployed during the bootstrap phase. To install Warehouse Connector, you must run the following command and specify the host by ID (--host-id), name (--host-name), or address (--host-addr). The latest available version will be installed by default unless a specific version is specified with --version. To install the Warehouse Connector on a host, run the following command on the Admin server:

[root]warehouse-installer --host-id <*uuid of the host*>

Details about the command:

Location: /usr/bin

Utility Name: warehouse-installer

Usage:

[root@nw11pds5 bin]# warehouse-installer --help

Warehouse Connector Installer

warehouse-installer [options]

Install options:

--host-id <id> Specify host to install (by ID)

--host-name <name> Specify host to install (by name)

--host-addr <address> Specify host to install (by address)

--version <#.#.#.#> Install version (defaults to latest)

General options:

-v, --verbose Enable verbose output

Meta keys for investigation and hunting added to default Concentrator index file.

Tracking Number: ASOC-22338, ASOC-22895, ASOC-19406

Problem: If you have added the following meta keys as custom to your index-concentrator-custom.xml file, they may be removed post-upgrade and are present now a standard meta keys within the index-concentrator.xml file. The meta keys are: direction, netname, ioc, eoc, boc, analysis.file, analysis.session, analysis.service, inv.category, inv.context.

Workaround: Remove the listed keys from the index-concentrator-custom.xml file.

Duplicate dashboards for threat indicators.

Tracking Number: ASOC-41701

Problem: The dashboard, Threat–Indicators, was updated to report against new Hunting meta keys and renamed to Threat–Malware Indicators. On upgrade, both will appear in the UI instead of the old being replaced.

Workaround: Enable the Threat–Malware Indicators report charts and dashboard and disable the old Threat–Indicators dashboard.

On upgrade, the Health and Wellness custom policies for Context Hub Server are not available.

Tracking Number: ASOC-41826

Problem: When you upgrade to Netwitness Suite 11.0.0.0, the Health and Wellness custom policies configured for Context Hub server will not be available.

Workaround: You must define these custom policies in 11.0.0.0

On upgrade to 11.0, collections created from a 10.4 Workbench display blank Date Range and Date Created values

Tracking Number: ASOC-9035

Problem: Any collections created from a 10.4 Workbench displays blank Date Range and Date Created values after upgrading to 11.0.0.0.

Workaround: None.

On upgrade, the Geo-map dashlet cannot be created using a pre-configured (OOTB) chart.

Tracking Number: ASOC-41896

Problem: When you upgrade to Netwitness Suite 11.0.0.0, the Geo-map dashlet cannot be created using a pre-configured (OOTB) chart. This happens if a custom dashboard uses a Geo-map dashlet, which is created using a pre-configured (OOTB) chart.

Workaround: The data source must be manually updated for that OOTB chart that is required to be used in the dashlet with Geo-map. Or, create a new chart using the same pre-configured (OOTB) rule and use the new chart in the dashlet with Geo-map.

Warehouse Connector Service shows SSL FIPS is disabled.

Tracking Number: ASOC-41930

Problem: When you upgrade from 10.6.x non-FIPS setup to 11.0.0.0, though the Warehouse Connector service is running on FIPS the UI shows SSL FIPS is disabled.

Workaround: Check the SSL FIPS on the Config page (UI) and restart the Warehouse Connector service.

Context Hub

OutOfMemoryError in the Context Hub service

Tracking Number: ASOC-41664

Problem: The Context Hub service runs into OutOfMemoryError and becomes unresponsive, if a large number of TAXII feeds are configured to fetch data.

Workaround: Restart the Context Hub service and make sure that the time range you select to fetch TAXII feeds from the TAXII server is not more than 6 months. If the issue persist even after updating the time range, see the Troubleshooting topic in the *Live Services Management Guide*.

The Pivot to Investigate option on the Respond view does not navigate to the correct link.

Tracking Number: ASOC-40944

Problem: Everytime you stop and restart the RabbitMQ server, the Pivot to Investigate option available on the respond screen, is not visible. And the context panel for Pivot to Investigate reopens the same page.

Workaround:Restart the jetty service on the Netwitness Server, login to the Netwitness Server Host and enter the service jetty restart command.

Increasing the limit settings for Alerts and Incidents leads to lookup error.

Tracking Number: ASOC-40246

Problem: By default, the limit settings to view number of Alerts and Incidents is set to 50. If the limit is increased and you view the lookup error then it is due to large number of Incidents and Alerts. This happens due to an internal database restriction.

Workaround:To limit and view Alerts and Incidents to 50.

Single-column and multi-column lists added from the Data Source tab are not supported for Add to a list and Remove from list.

Tracking Number: ASOC-37998

Problem: When you do a lookup on a specific context meta in the Investigation or Events or Respond view, the list names displayed are the ones which have matching values.

When you right-click on specific meta and select the Add or Remove list option, the single-column and multi-column list names added from the data source tab will not be displayed. It will only display the lists added from the UI using the List tab.

Workaround: You need to manually add the values which were added from the Data Source tab to the specific CSV file. So that, next time when the scheduler runs, the values from the updated CSV file will be available in the specific lists.

Empty list imported

Tracking Number: ASOC-34187

Problem: When you import a list with missing quotes such as “172.16.0.0, the list is saved without any data. This is because of the Apache bug (CSV-141), does not parse the CSV file with incorrect format.

Workaround: Import a list with correct quotes. For example, “172.16.0.0”, “host.mycompany.com” and so on.

SSL handshake with RSA Archer certificate fails while adding it as a data source

Tracking Number: ASOC-32654

Problem: When you try to add RSA Archer as a data source using valid credentials, the test connection fails (ARCHER-37085). This happens when the 'Trust all Certificates' option is unchecked and you try to upload an RSA Archer trust certificate.

Workaround: Select the ‘Trust All Certificates’ checkbox and do not upload a certificate.

General Platform Issues

NetWitness Suite User Interface may become unresponsive

Tracking Number: SACE-7751

Problem: The NetWitness Suite UI may become unresponsive when the system is trying to read large volume Live Connect logs.

Workaround: This issue can be temporarily resolved by restarting jettysrv.

Issue with meta export

Tracking Number: SACE-8116

Problem: Although the export works, if there are more than one meta value in a session, the current capability will only export one of the meta values. For example, if you have a session with 100 alias.host meta values, only one value is exported.

Workaround: None.

User selects to extract meta, but no data is downloaded

Tracking Number: ASOC-35600

Problem: If you select to export meta for an event, the export file is downloaded and saved with specified file name, but there is no data contained in the downloaded file.

Workaround: None.

Empty popup dialog is returned in NW UI for invalid STIX file

Tracking Number: ASOC-36138

Problem: If you try to upload an invalid STIX file, an error message should be displayed but instead an empty popup dialog is returned.

Workaround: None.

Log export always exports in Log format

Tracking Number: ASOC-38270

Problem: In the Investigation UI, if you select to Extract Log(s) from the NetWitness Server, the log will always be exported in "Log" format.

Workaround: None.

General Application Issues

NetWitness Suite UI classic pages fail to load when the system is under heavy usage

Tracking Number: ASOC-41999

Problem: NetWitness Suite UI classic pages will fail to load when the system is under heavy usage with "`OutOfMemoryError: Metaspace`" error.

Workaround: Change "`-XX:MaxMetaspaceSize=256m`" to "`-XX:MaxMetaspaceSize=512m`" in `/etc/default/jetty` file on Admin Node. After the changes are saved restart the jetty service (`systemctl restart jetty`).

Entitlements

Metered license does not flip back to an in compliance immediately when there are no services attached to that Metered license

Tracking Number: ASOC-9078

Problem: As an example, if there is a Metered license available for a Log Decoder and you have one Log Decoder listed under it, the following conditions may occur:

- You are over your entitled usage and marked as out of compliance.
- You decide to move the Log Decoder into an available service-based license.
- Your Metered license has no service under it.
- Your Metered license flips back to an in-compliance state after seven days.

Workaround: None.

Aggregate usage report gets generated whenever one service is attached to a license and "All" is selected while exporting usage stats

Tracking Number: ASOC-10079

Problem: For any license type (All/Metered/Service-based), the aggregate PDF/CSV file should get generated only when there is more than one service listed under any license type.

Workaround: None.

Respond

When upgrading, the Aggregation rule for C2 alerts Group By condition is incorrect

Tracking Number: ASOC-41934

Problem: When upgrading 11.0.0.0, the C2 aggregation rule used by Automated Threat Detection has a different Group By condition value.

Workaround: After upgrading to 11.0.0.0, edit the “Suspected Command & Control Communication By Domain” aggregation rule and change the Group By condition to “Domain.” (To do this, go to CONFIGURE > Incident Rules > Aggregation Rules and double-click the Suspected Command & Control Communication Rule to edit it.) This will aggregate the alerts and incidents will be created for “Suspected C&C”.

Unable to Create an Incident using 1000 alerts

Tracking Number: ASOC-41855

Problem: When you try to manually create an incident with more than 400 alerts selected in the Alerts List view, you may experience problems.

Workaround: Do not select more than 400 alerts when you create an incident.

Respond Administrator cannot query Investigate or view Live dashlets in the Dashboard

Tracking Number: ASOC-40749

Problem: The Respond_Administrator role does not have permission to query Investigate. This is necessary so that the Respond Administrator can pivot to Investigate or create incidents from events. The Respond_Administrator Role also does not have the Live: Access Live Module permission, which is required to view Live dashlets in the dashboard.

Workaround:

1. Manually create the Respond_Administrator role on the Core services. To do this, go to ADMIN > Services, select a Core service, and then in the Actions drop-down list, select View > Security > Roles Tab. Click + to add the Respond_Administrator role. Add the following permissions to the Respond_Administrator role:

- sdk.content
- sdk.meta

- sdk.packets
- storedproc.execute

Replicate the Respond_Administrator role to other Core services that may be used by the users.

2. In the ADMIN > Security > Role tab, add the Live: Access Live Module permission to the Respond_Administrator role.

When the metered or service based license is mapped, the licensed days and the start date are incorrectly displayed.

Tracking Number: ASOC-26334

Problem: When the metered or service based license is mapped, the licensed days and the start date are incorrectly displayed on the user interface (UI). This occurs due to an issue with the licensing system and if/when a new license is mapped. However, the correct data (licensed days and the start date) is reflected in the UI after few days.

Workaround: None.

Malware event File name with Korean characters is not shown properly in the Respond view

Tracking Number: ASOC-40159

Problem: If there are Korean characters in an alert that is received from Malware Analysis they will not be displayed correctly in the Respond view.

Workaround: None.

Unable to query domain in source/destination.device.geolocation

Tracking Number: ASOC-39938

Problem: Geo-location that comes from ESA Correlation Rules is not available in the Incident Details view Related Indicators panel. (To access the Related Indicators panel, Go to RESPOND > Incidents and in the Incidents List, click the ID or NAME link of the incident. In the Incident Details view toolbar, click the Journal, Task, and Related icon. The Journal is displayed on the right. Click the RELATED tab.)

Workaround: None. This is a new functionality, so it is just data that is not searchable.

Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is not valid in NetWitness Suite 11.0.0.0

Tracking Number: ASOC-41891

Problem: NetWitness Suite 11.0.0.0 will only work with NetWitness SecOps Manager 1.3.1.2. However, the Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is navigating to the legacy Security Analytics Incident Management page, which is not valid in NetWitness Suite 11.0.0.0.

Workaround: None.

Incidents and Tasks are still available when RSA NetWitness SecOps Manager integration is enabled

Tracking Number: ASOC-39886

Problem: After enabling NetWitness SecOps Manager integration in the Respond Server service, all incidents are managed in NetWitness SecOps Manager. In previous versions, when SecOps was enabled, incidents and remediation tasks were hidden. In NetWitness Suite 11.0.0.0, users are still able to access incidents and tasks in the Respond view (RESPOND > Incidents and RESPOND > Tasks). They are also not prevented from creating incidents in NetWitness Suite. If they create incidents from the Respond Alert List view (RESPOND > Alerts) or from Investigate, those incidents will not go to NetWitness SecOps Manager.

Workaround: If you enabled SecOps Manager integration in the Respond Server service, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Also, do not create incidents from the Respond Alerts List view or from Investigate.

For migrated incidents, the event count always shows as 0 in the Overview panel

Tracking Number: ASOC-38026

Problem: In the Incidents Overview panel Catalysts field, the number of events for migrated incidents always shows as 0 (zero). This is expected behavior in NetWitness Suite 11.0.0.0 (To access the Overview panel, go to Respond > Incidents. If you click an incident in the Incidents List, the Overview panel appears to the right. If you click a link in the ID or NAME field in the Incidents List, the Incident Details view opens with the Overview panel on the left.)

Workaround: None.

Unable to Pivot to Investigate on all username, filename, and domain values when multiple values are present.

Tracking Number: ASOC-37997

Problem: If username fields contain commas that do not represent delimiters between values, you may not be able to pivot to Investigate on certain meta if there is more than one value in the field.

Workaround: You can query or pivot on other data, or manually investigate the meta. You can still access the meta through Investigate.

In memory table enrichment info is not displayed for ESA alerts

Tracking Number: ASOC-37533

Problem: You cannot view custom enrichments for ESA Correlation Rules in the Respond Alerts view.

Workaround: None.

DOMAIN and HOST metas do not display correctly in the Respond view

Tracking Number: ASOC-37232

Problem: Domain and Host metas may be incorrectly labeled in the Respond Incidents Details view when alias.host contains different types of data. The Domain field behavior is inconsistent and it may be populated with hostnames.

Workaround: None. Multiple types of information will continue to exist in the Domain field.

After upgrade, unable to filter incidents using the Assignee field

Tracking Number: ASOC-36973

Problem: After upgrading incidents from 10.6.x to 11.0.0.0, Analysts are not able to filter the migrated incidents using the Assignee field (RESPOND > Incidents - Filter panel).

Workaround: None.

Respond - Create Incidents from Alerts in the Respond Alert List view

Tracking Number: ASOC-35811

Problem: When you manually create an incident from alerts in the Respond Alert List view (RESPOND > Alerts) in 11.0.0.0, you just have the minimum functionality to create an incident from alerts. You can only provide a name for the incident and the priority defaults to Low. When manually creating an incident, you do not have additional options, such as adding a Priority, Assignee, or Category.

Workaround: You can update additional fields by manually editing the incident after you create it, such as changing the priority from Low to High. However, you cannot add a category to an incident.

Whitelist Domains while closing Incidents as False Positive

Tracking Number: ASOC-25135

Problem: In 10.6.x, if a Suspected C&C Incident was marked as "Closed - False Positive" , an entry was made to the "Whitelisted Domains" list from context hub. There should be a similar functionality in the Respond view.

Workaround: Analysts can manually add domains to a whitelist in the Respond view. The *NetWitness Respond User Guide* provides procedures.

Integration Settings for SecOps Manager should be exposed in the User Interface

Tracking Number: ASOC-25127

Problem: The Integration settings for sending all incidents to RSA NetWitness SecOps Manager should be exposed in the user interface.

Workaround: The user interface for partial RSA NetWitness SecOps Manager integration was removed in 11.0.0.0. Administrators can complete the integration from the Explorer view for the Respond Server service.

Incidents are not flagged when a user manually adds alerts to an existing incident.

Tracking Number: ASOC-16640

Problem: Investigation values are not highlighted when alerts in Respond have manually been added to an incident. Alerts that are dynamically added to an incident will get highlighted.

Workaround: None.

Log Collector

DPO Role missing on Log Collector

Tracking Number: ASOC-7937

Problem: The new Data Privacy Officer role does not exist on the Log Collector.

Workaround: None.

Checkpoint collection not working with error "peer ended the session"

Tracking Number: ASOC-8351

Problem: The checkpoint collection is not working and the logs show the error: **peer ended the session**

Workaround: To resolve this issue:

1. Make a backup and then remove the checkpoint position file (**/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_Security.xml**).
2. Restart the service to regenerate the file.
3. (Optional) If the **Max Idle Time Poll** is set to 0, set it to 5.

Throttle Remote Collector to Local Collector Bandwidth Error

Tracking Number: ASOC-16717

Problem: Bandwidth throttling configuration changes to control the rate that the Remote Collector sends event data to a Local Collector do not persist after a reboot.

The `set-shoveltransfer-limit.sh` script is used to set the bandwidth throttle for event data transferred from a remote collector to local collector. The script uses both iptables rules and linux kernel traffic shaping filters to control the upload bandwidth used by the RabbitMQ port on transfers to an upstream collector. The script works correctly when executed, but fails to persist the traffic shaping filter values once the appliance is rebooted.

Workaround: Add the script execution to the `/etc/rc.local` on the remote collector, as shown in the following example:
`"/opt/netwitness/bin/set-shovel-transfer-limit.sh -s -r 4096kbit"`

Investigation

Custom meta keys are not being displayed.

Tracking Number: SACE-8549

Problem: Custom meta keys are not being displayed.

Workaround: Create a custom meta group that contains the custom meta keys. The custom meta keys will then be displayed.

User and Role attributes (query prefix) is not applicable to Investigate Event Analysis.

Tracking Number: ASOC-42735

Problem: The user and role attributes, most importantly the query prefix, do not apply to the new Investigate Event Analysis. Any user can modify the URL in browser to access data that should be restricted from viewing even when query prefix is applied.

Workaround: Apply the Netwitness Suite 11.0.0.1 patch. Refer to the *Netwitness Suite 11.0.0.1 Release Notes*.

In a mixed mode environment, an Analyst with insufficient permissions can download PCAPs and logs from a 10.6.x service in the Investigate > Event Analysis View, but not files or payloads.

Tracking Number: ASOC-41697, ASOC-41698

Problem: Role-Based Access Control (RBAC) on the 11.0.0.0 NW Server is not applied uniformly to downloads when investigating 10.6.x services. If the sdk.packets setting has not been disabled, Analysts with SDK Meta and roles permission in place to restrict viewing and reconstructing event content can download the PCAP and log of an event that has content restrictions. Other types of downloads appear to download, then generate errors due to insufficient permissions, and the data is still protected.

Workaround: Disable the sdk.packets setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during phased upgrade. When the upgrade of all services is complete, the RBAC experience will be consistent across all services. See the "Upgrade Tasks" section in the *Physical Host Upgrade Guide* for details.

In a mixed mode environment the Event Reconstruction View > File View displays the word "terminated" instead of the list of files.

Tracking Number: ASOC-41703

Problem: The first time an admin user reconstructs an event of service=other and .raw file, the word "terminated" may be displayed in the Event Reconstruction view instead of the .raw file.

Workaround: Go to another event in the Events view and come back to this event, or clear the services cache to see the proper result. Alternatively, the admin user can view the file in the Event Analysis View. The issue occurs only during upgrade while in mixed mode, so the best workaround is to finish upgrading connected services to NW 11.0.0.0. See the "Upgrade Tasks" section in the *Physical Host Upgrade Guide* for details.

In a mixed mode network and in an all 11.0.0.0 network, an analyst with content restrictions appears to be able to download restricted content, but is unable to unzip the downloaded file archive due to the zip file not having the restricted content.

Tracking Number: ASOC-41698, ASOC-41696

Problem: When a user who does not have permissions to the content downloads files, the content restriction applied using RBAC is upheld, but the user experience is not consistent with the user experience for other types of downloads with insufficient permissions. This is seen in an all 11.0.0.0 environment and a mixed mode 11.0.0.0/10.6x. environment. An analyst whose permissions restrict viewing content in the Event Reconstruction View can download restricted content on connected 10.6.x services. The analyst can export restricted files as Zip or GZip, and the Job Queue shows a successful download. However, the file is downloaded as Zip or tar format, and the archive fails to unzip, instead creating a copy as 'cpgz'.

Workaround: None. When the upgrade of all services is complete, the RBAC experience will be consistent across all services. See the "Upgrade Tasks" section in the Physical Host Upgrade Guide for details.

Right-click action in the Log View does not launch Event Reconstruction or Event Analysis when you click on a Logs column that wraps to more than one row.

Tracking Number: ASOC-37989

Problem: In the Log View of an event, the right-click action to launch Event Reconstruction or Event Analysis is not available when the Logs column in the Log View wraps to more then one row.

Workaround: Analysts can right click in another column that is not word wrapped on same event row.

In Event Analysis, the Rendered Packets message is not displayed for events with a small payload but large number of packets.

Tracking Number: ASOC-37348

Problem: When an event has more that 2500 packets, a message should be displayed at the bottom of the results to show the count of rendered packets. This message is not displayed for events with 2500 or more packets and a very small payload because the entire payload can be displayed in the view.

Workaround: None.

PCAP and payload download issues in Event Analysis view in a Mixed Mode Environment

Tracking Number: ASOC-37309

Problem: The Event Analysis workflow requires all services to be running 11.0.0.0. If the NW Server, Broker, and Concentrator are running 11.0.0.0, and the Decoders are running 10.6.x, the admin user will not be able to download files, logs, PCAPs, and payloads.

Workaround: Download files from Event Reconstruction.

When viewing a file archive in the Event Analysis - File Analysis panel, the individual filenames in the archive are not displayed.

Tracking Number: ASOC-35607

Problem: You can see the archive, but not the filenames contained in the archive.

Workaround: View the event in Investigate Event Reconstruction view files to see the individual filenames.

Parallel Coordinate visualization is not displaying special characters correctly

Tracking Number: ASOC-9346

Problem: When configuring meta key content type as one of the meta for the axis, if the meta value contains any special characters, the values do not display correctly.

Workaround: None.

Workbench

Tracking Number: ASOC-6859

Problem: An empty collection is seen in the Collections tab if the workbench service stops or restarts during restoration process

Workaround: None.

Data range is not displayed for collection if workbench service or Jettysrv is restarted while restoration is in process

Tracking Number: ASOC-6822

Problem: The date range is not displayed for a collection if the workbench service or Jettysrv is restarted while the restoration is in process.

Workaround: None.

Live

The status of STIX feed progress bar is incomplete.

Tracking Number: ASOC-40642

Problem: Sometimes, the status of the progress bar for some of the STIX feeds are incomplete even if the feeds are successfully pushed to the Decoder(s).

Workaround: None.

Malware Analysis

Users with Analyst role are not able to run the on-demand malware scan

Tracking Number: ASOC-5425

Problem: A user who has the Analyst role has access to the Investigation and Malware Analysis modules. But when the user tries to run the on-demand Malware Analysis scan from the Investigation screen, it fails with an invalid username error. The job gets submitted but fails because of the credentials.

Workaround: None.

If the Core device is not configured with IP address, the View Network Session option is disabled for Malware Analysis events

Tracking Number: ASOC-5571

Problem: Due to the new service ID and changes to the ASG, Malware Analysis is not showing the View Network Session option from the Malware Event Summary. It looks like the device ID is coming as null.

Workaround: None.

Event Stream Analysis

Deployment (called Synchronization in 10.4 and earlier) fails if you deploy this rule from RSA Live: No Log Traffic detected from device in given time frame

Tracking Number: SAENG-5888

Problem: Deployment, formerly called synchronization, fails for rule "No Log Traffic detected from device in given time frame" deployed from Live. This issue is not observed if you deploy the rules from Live on a 10.4 setup and do the synchronization. The issue is observed if you update your system from a pre-10.4 where the rules are deployed from Live with incorrect Module IDs.

Workaround: Delete the rules with incorrect Module ID's and redeploy them from Live.

Case-sensitive sorting is not working properly in ESA All Rules grid

Tracking Number: SAENG-3605

Problem: When rule names begin with lower and upper case letters, the sort does not work properly in the Rule Name column of ESA All Rules grid. For example, "Rule 1" is not followed by "rule 2" when you sort by name.

Workaround: None.

Cannot set ESA compression level as in other appliances

Tracking Number: ASOC-26481

Problem: Administrators cannot set the compression level in ESA like they can with other appliances, even using the Explorer view.

Workaround: Delete the Concentrator source from ESA and add it again so that the compression level changes are reflected:

1. Remove the Concentrator data source from ESA. (Go to ADMIN > Services, select the Event Stream Analysis service, and from the actions menu select View > Config. On the Config view Data Sources tab, remove the Concentrator data source.)
2. Set compression level in ESA. (Go to the Explore view, and in the node list, navigate to Workflow/Source/nextgenAggregationSource and set the CompressionLevel.)

3. Add the Concentrator Data Source again to ESA. (Return to the Config view Data Sources tab and add the Concentrator data source.)

Event Stream Analysis service becomes unresponsive when using Query-based aggregation for automated threat detection for Logs

Tracking Number: ASOC-25174

Problem: Event Stream Analysis may become unresponsive due to heavy resource usage, and the configuration for the wrapper may need to be adjusted.

Workaround: You may need to change the ping time settings in the `wrapper.conf` file. Perform the following:

1. Go to **Administration > Services > Event Stream Analysis> Explorer** and navigate to the `/opt/rsa/esa/conf/` folder.
2. Change the settings to the following values:
   `wrapper.ping.timeout=300`
3. Add the following lines at the end of the file:
   `wrapper.restart.delay=40`
   `wrapper.ping.timeout.action=RESTART`
4. Restart the Event Stream Analysis service.

ESA Displays Warning For Array Operators

Tracking number: ASOC-14157

Problem: When writing an advanced rule, array operators, such as anyOf, fails. For example:

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

results in an error similar to the following:

```
Logger name: com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class java.util.Vector
```

Workaround: To do a fuzzy comparison, first convert the array to a string. For example:

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

> **Note:** If you used array operators in EPL developed in versions 10.5, 10.5.0.1, and 10.6, you will need to modify the EPL to use the above workaround.

Forwarding rule name is not updated when advanced rule name changes

Tracking number: ASOC-9585

Problem: For a cross-site deployment, when you change the name of an advanced rule, the forwarding rule does not change along with the name change for the advanced rule. This can result in an orphaned rule which can continue to forward events.

Workaround: To rename a cross-site advance rule, create a new rule and delete the old one.

Deployment fails if the server that hosts an external database goes down

Tracking Number: ASOC-9011

Problem: You configure a database connection to use the database as an enrichment source for a rule. A reference to the data base is deployed on every ESA, even if the ESA does not deploy any rules that use the database. If the server that hosts the database goes down, any new deployment will fail.

Workaround: Restart the server that hosts the database.

Trial rules configuration: Out-of-Bound Values are Capped

Tracking Number: ASOC-6633

Problem: When configuring parameters for trial rules, you can configure the following values:

- **MemoryCheckPeriod**: Defines the polling interval to check the ESA memory consumption.
- **MemoryThresholdForTrialRules**: Defines the threshold value; when reached, all trial rules will be disabled.

  If you configure these parameters with out-of-bound values, the values are capped to the system's minimum or maximum values rather than the values defined in the parameters.

Workaround: None.

Reporting Engine

Some compliance reports cannot be deployed from Live

Tracking Number: SAENG-1334

Problem: If the dependencies of certain compliance reports in Live are not deployed prior to the reports themselves, deployment of those fails.

Workaround: Retry the deployment. If the problem persists, try to deploy the rule or list dependencies first and then deploy the reports.

Some Reporting Alerts can fail or be delayed if the RabbitMQ connection is blocked

Tracking Number: SAENG-5329

Problem: If the **Forward Alerts to Respond** option is enabled and RabbitMQ connections to the Respond Server are blocked, some of the Reporting Engine threads can be blocked.

Workaround: Disable the **Forward Alerts to Respond** option until the RabbitMQ broker in the NetWitness Suite server at the Respond, has started and can accept the connections.

Updates to connection parameters on the Service page do not reflect on the Reporting Data sources

Tracking Number: ASOC-8149

Problem: If there are any changes or updates to service names, ports or parameters on the service page, they are not propagated to the corresponding data sources added in the Reporting Engine.

Workaround: Add data sources with modified service and use them. Additionally, if the names of the existing services are modified, the corresponding schedules must be updated in Reporting.

Cannot Navigate to Investigation from the NWDB reports if the connection parameters on the Service page are updated

Tracking Number: ASOC-8575

Problem: The Investigation link for the meta values of the executed reports is not displayed on the NWDB results page.

Workaround: None. To be fixed in the future release.

Updates to connection parameters on the Service page do not reflect on the Reporting Data sources

Tracking Number: ASOC-8149

Problem: If there are any changes or updates to service names, ports or parameters on the service page, they are not propagated to the corresponding data sources added in the Reporting Engine.

Workaround: Add data sources with modified service and use them. Additionally, if the names of the existing services are modified, the corresponding schedules must be updated in Reporting.

Reporting

Categories meta for incident collection is not supported.

Tracking Number: ASOC-40851

Problem: When using the Categories meta for incident collection, the results rendered are in an incorrect format. Hence this meta is not supported and you cannot use the categories meta in either select clause or where clause. Also, it is not available in the list of metas for selection in the Rule Builder page.

Workaround: None.

When querying on the Respond DB, empty rows are displayed.

Tracking Number: ASOC-37846

Problem: When querying on the Respond DB, and if the data is not available for the requested columns, then empty rows are displayed on the UI.

Workaround: None.

Chart with totals displays incorrect data.

Tracking Number: ASOC-37958

Problem: Chart with totals displays incorrect data when total numbers of values are higher than the chart limit. For example, if the number values that are retrieved is 16, the number of values that get displayed on the chart may be only the first 10.

Workaround: None.

Hide and Investigate options are not supported in Google Chrome and Mozilla Firefox browsers on Windows 10 operating system.

Tracking Number: ASOC-37590

Problem: If you are using Chrome or Firefox browsers on a Windows 10 operating system, and click on a chart data point, the hide and investigate options are not displayed. However, these options are available using the Internet Explorer browser.

Workaround: Disable the touch feature on Chrome and Firefox browsers. To disable this option in Chrome use the following procedure:

1. Navigate to - chrome://flags/ on Chrome or Firefox Browser.
2. Select the "Disable" option for "Touch Events API" flag.
3. Relaunch the browser.

To disable this option in Firefox, use the following procedure:

1. Navigate to - "about:config".
2. Click on "I accept the risk".
3. Search for the "Preference Name" - "dom.w3c_touch_events.enabled".
4. Update the "Value" column to 0.
5. Relaunch the browser.

Test Rule results with large data are not displayed in Internet Explorer 10

Tracking Number: SAENG-3926

Problem: When you click the **Test Rule** multiple times in quick succession, results with large input data may not displayed in Internet Explorer 10.

Workaround: If this issue occurs, try one of the following steps:

- Close the Test Rule window on Internet Explorer 10 and run the test again.
- Use other browsers like Chrome or Mozilla Firefox to test the rule execution.

Dynamic Lists cannot be added when editing a report schedule from the View All Schedules page

Tracking Number: SAENG-5837

Problem: You cannot add a dynamic list from the Edit option on the 'View All Schedules' page to an existing schedule.

Workaround: Edit the schedule from the Report Schedule page to add a dynamic list.

Administration

Configuration audit event captured by NetWitness Suite lacks context of which service was changed

Tracking Number: ASOC-8889

Problem: The NetWitness Suite server does not capture the applicable target service for configuration changes in audit events.

Workaround: None.

Excessive audit logs are logged when accessing NetWitness Suite UI pages/ importing/ exporting/ login/ logout`

Tracking Number: ASOC-8916

Problem: NetWitness Suite creates an excessive amount of audit logs when NetWitness Suite users log on, log out, import, export, and access pages from the NetWitness Suite user interface.

Workaround: None.

Audit Logs: SA_SERVER is not capturing the value for queryString

Tracking Number: ASOC-8994

Problem: When changing file contents of a NetWitness Suite service, the NetWitness Suite server audit logs do not indicate which file the user changed.

Workaround: None.

Password expiry email lacks source information

Tracking Number: ASOC-9187

Problem: The password expiry email sent by the NetWitness Suite server does not mention the name or URL of the NetWitness Suite server that sent the email. If there are multiple NetWitness Suite servers, you may not know where to go to update your password.

Workaround: None.

Audit logs do not report the page (name) accessed when user tries to access NetWitness Suite pages where the user does not have permissions

Tracking Number: ASOC-9323

Problem: When a user tries to access NetWitness Suite user interface pages without the necessary permissions, the audit logs do not capture the page names accessed by the user.

Workaround: None.

Event Source Management

Renaming the Log Collector or Log Decoder hostname is not reflected in Event Source Manage View

Tracking Number: ASOC-9235

Problem: On the **Administration > Host** page, if you edit the Log Collector or Log Decoder appliance "name," then the change will not be reflected on the **Administration > Event Sources > Manage** page in the Log Collector or Log Decoder columns.

Workaround: Once you update a name from the Host page perform the following steps:

1. SSH to the NetWitness Suite appliance.
2. Restart the SMS service by running this command: service rsa-sms restart.
3. On the NetWitness Suite UI, wait for the **Event Source Manage** page to come back up, then delete the event sources with the old Log Collector or Log Decoder names.

If you are collecting events from deleted event sources, then they are automatically added back to the Event Source Manage page with the new Log Collector or Log Decoder name.

Core Services

The SSL FIPS Mode checkbox in the Services Config view should be disabled for Brokers, Concentrators, and Archivers, because changing the checkbox value does not turn off FIPS enforcement for the service.

Tracking Number: ASOC-41902

Problem: In 11.0.0.0 the Broker, Concentrator, and Archiver are always FIPS enforced and the administrator does not have the option to toggle between between FIPS and Non-FIPS. The admin can use the SSL FIPS Mode checkbox to toggle FIPS mode on and off on a Log Decoder, Packet Decoder, or Log Collector.

Workaround: None.

Broker System roles do not show the custom meta keys defined in Concentrator

Tracking Number: ASOC-6749

Problem: If any custom meta keys are defined, the same meta keys should show up in the Broker, too. But the Broker system roles are not showing the custom meta.

Workaround: You can copy the Concentrator Language file and the custom index file (if it exists) to the Broker to add the SDK meta key roles to the system roles.

Custom Feed configuration- Advanced Option XML file invalid error for multi metacallback.

Tracking Number: ASOC-40867

Problem: Netwitness Suite does not support uploading feeds for the xmls where there are more than one callback.

Workaround: The Adhoc Feed can be uploaded using NwConsole, or using the REST URL of the decoder directly. This is not applicable for Recurring Feed.

Ability to Create Source and Destination IP-Based Feeds Using CIDR or Range

Tracking Number: SATCE-628

Problem: When creating a source and destination based feed on a Log Decoder, it only populates the source meta key. You cannot use a range-based or CIDR feed. You must list every single IP address.

Workaround: Create two different feeds using IP addresses and you can use CIDR in these feeds.

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
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.