RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness® Platform 11.5.2

Contact Information

RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

January 2021

Contents

What's New

The RSA NetWitness® Platform 11.5.2 release provides new features and enhancements for every role in the Security Operation Center.

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.5.2.0:

- RSA NetWitness® Platform 11.3.x.x to 11.5.2.0*
- RSA NetWitness® Platform 11.4.x.x to 11.5.2.0
- RSA NetWitness® Platform 11.5.x.x to 11.5.2.0

* If you are upgrading from 11.3.0.0, or 11.3.0.1, you must upgrade to 11.3.1.1 before you can upgrade to 11.5.2.0.

If you are upgrading from NetWitness Platform version (10.6.6.x) or (11.2.x.x or below), you must upgrade to 11.3.0.2 before you can upgrade to 11.5.2.0. For more information, see the guides that apply to your environment.

For more information on upgrading to 11.5.2.0, see *Upgrade Guide for RSA NetWitness Platform 11.5.2*.

Enhancements

The following sections are a complete list and description of enhancements to specific capabilities:

- Licensing
- Endpoint Investigation
- Investigation - SIEM and Network Detection & Response
- Broker, Concentrator, Decoder and Log Decoder Services

To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents. Product Documentation has links to the documentation for this release.

Licensing

Enhanced License Status

If your deployment is in a breach state, you can bring the state back to normal by keeping the usage in a compliant state for 7 consecutive days.

Endpoint Investigation

Extended Windows Agent Support for Windows 10 version 20H2

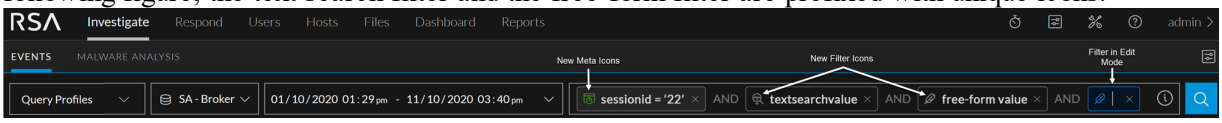
Extended agent support for Windows 10 version 20H2 (32 and 64-bit). For more information, see the *NetWitness Endpoint Agent Installation Guide*.

Investigation - SIEM and Network Detection & Response

Enhanced Query Builder UI

The following UI enhancements make the query bar more responsive and user friendly. These enhancements provide a visual aid that helps analysts to utilize filters more efficiently.

- A filter awaiting input is highlighted with a blue color border. You can click **X** to delete the filter in the edit mode.
- An invalid filter is highlighted with a red color border.
- Guided filters display the associated new meta key icons.
- Filters display unique icons that help analysts to distinguish among them. For example, in the following figure, the text search filter and the free-form filter are prefixed with unique icons.



For more information on how to use filters and query bar, see the "Filter Results in the Events View" topic in the *NetWitness Investigate User Guide*.

Broker, Concentrator, Decoder and Log Decoder Services

Network Virtualization Enhancements

To further support enterprises that use network virtualization to segment their networks, the Decoder automatically performs decapsulation of the Virtual Extensible LAN (VXLAN) protocol. There is no configuration required to enable this functionality. When Decoder ingests network traffic available on UDP-4789, it analyzes the traffic for VXLAN and parses the decapsulated Ethernet frames.

Fixed Issues

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the RSA NetWitness® Platform Known Issues list on RSA Link: https://community.rsa.com/community/products/netwitness/documentation/known-issues

Security Fixes

Tracking Number	Description
ASOC-104032	CentOS 7 dbus security update - https://access.redhat.com/errata/RHSA-2020:2894
ASOC-104030	CentOS 7 grub2 security and bug fix update - https://access.redhat.com/errata/RHSA-2020:3217
ASOC-104029	CentOS 7 java-11-openjdk security update - https://access.redhat.com/errata/RHSA-2020:2969
ASOC-104035	rsa-nw-legacy-web-server issue reported for Cross Site Scripting - https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
ASOC-104034	Reflected xss present in the malware service - https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
ASOC-104033	Stored xss present in reporting module - https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Administration Fixes

Tracking Number	Description
SACE-14665/ ASOC-104534	PKI Authentication based status in Admin > Security > PKI Settings did not clearly mention how to add configure Server CA Certificate in the trust store.

Core Services (Broker, Concentrator, Decoder, Archiver) Fixes

Tracking Number	Description
SACE-14578	After enabling packetdb compression on Packet Decoder, higher sessions per file were observed.
ASOC-105703 / SACE-14609	Due to access packet consumption for a Decoder the license usage shows exceeded limit of packets.

Server Fixes

Tracking Number	Description
SACE-14462/ ASOC-104534	After upgrading to NetWitness Platform 11.5 recurring feeds failed. This is because "Upload as CSV File Feed" was removed from 11.5 but it was being referenced during XML file upload.
ASOC-105189	During rescheduling of job the feed def xml and feed config file are not restored and hence the feed to failed when redeployed.
ASOC-105152 / SACE-14792	While running the script `/usr/bin/nw-manage` with `--check-hosts-status`, nodes containing space in the displayName are not getting parsed correctly.

Content Server Fixes

Tracking Number	Description
ASOC-105441	Content Management System server request queued due to high volume Content sever requests.

Reporting Engine Fixes

Tracking Number	Description
ASOC-105593 / SACE-14612 / SACE-14400	Unexpected alerts are getting triggered due to a Reporting Engine rule that was grouped to an incident by an incident rule.

Log Collector Fixes

Tracking Number	Description
ASOC-105276	Log Collector IPs are replaced by Host IDs when editing shovel which was created after setting up push configuration on the remote Log Collector.

Health and Wellness Fixes

Tracking Number	Description
ASOC-101652/ ASOC-105264	If an AD group is configured with an Administrator role in NetWitness Platform and you log in as an AD user (associated with the AD group), the New Health and Wellness dashboard is not displayed when you pivot to Dashboards.

UEBA Fixes

Tracking Number	Description
ASOC-104867/ SACE-14380	On the Investigate > Entities > Alerts view, when you export alerts to a CSV file, only 25 alerts are exported.

Endpoint Fixes

Tracking Number	Description
ASOC-104219/ SACE-14786	Too many FILELESS_SCRIPT reported by Windows Agent causing increased file collection.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.x Master Table of Contents	https://community.rsa.com/docs/DOC-81328
RSA NetWitness Platform 11.5 Product Documentation	https://community.rsa.com/community/products/netwitness/115
RSA NetWitness Platform 11.5.2 Upgrade Guide	https://community.rsa.com/docs/DOC-115381

Feedback on Product Documentation

You can send an email to sahelpfeedback@rsa.com to provide feedback on RSA NetWitness Platform documentation.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness Platform:

- See the documentation for all aspects of NetWitness Platform here: https://community.rsa.com/community/products/netwitness/documentation
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here: https://community.rsa.com/welcome
- See the RSA NetWitness® Platform Knowledge Base: https://community.rsa.com/community/products/netwitness/knowledge-base
- See Troubleshooting the RSA NetWitness® Platform: https://community.rsa.com/community/products/netwitness/documentation/troubleshooting
- See also RSA NetWitness® Platform Blog Posts.
- If you need further assistance, contact RSA Support.

Contact RSA Support

If you contact RSA Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the RSA NetWitness Platform product or application you are using.
- The type of hardware you are using.

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

RSA Link	https://community.rsa.com In the main menu, click **My Cases**.
International Contacts (How to Contact RSA Support)	https://community.rsa.com/docs/DOC-1294
Community	https://community.rsa.com/community/support

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.5.2.0.

Component	Version Number
NetWitness Platform Admin Server	11.5.2.0-201201172554.5
NetWitness Platform Appliance	11.5.2.0-11409.5
NetWitness Platform Archiver	11.5.2.0-11409.5
NetWitness Platform Bootstrap	11.5.2.0-2011101930.5
NetWitness Platform Broker	11.5.2.0-11409.5
NetWitness Platform Cloud Link Server	11.5.2.0-201207234103.5
NetWitness Platform Component Descriptor	11.5.2.0-2012080554.5
NetWitness Platform Concentrator	11.5.2.0-11409.5
NetWitness Platform Config Management	11.5.2.0-2011201642.5
NetWitness Platform Config Server	11.5.2.0-201130122010.5
NetWitness Platform Console	11.5.2.0-11409.5
NetWitness Platform Content Server	11.5.2.0-201204005920.5
NetWitness Platform ContextHub Server	11.5.2.0-201028035226.5
NetWitness Platform Correlation Server	11.5.2.0-201111032415.5
NetWitness Platform Decoder	11.5.2.0-11409.5
NetWitness Platform Decoder Content	11.5.2.0-11409.5
NetWitness Platform Deployment Upgrade	11.5.2.0-2011201644.5
NetWitness Platform Endpoint Agents	11.5.2.0-2012021858.5
NetWitness Platform Endpoint Broker Server	11.5.2.0-201207111933.5
NetWitness Platform Endpoint Server	11.5.2.0-201207112813.5

NetWitness Platform Integration Server	11.5.2.0-201130123026.5
NetWitness Platform Investigate Server	11.5.2.0-201201174253.5
NetWitness Platform Legacy Web Server	11.5.2.0-201125141221.5
NetWitness Platform License Server	11.5.2.0-201202033739.5
NetWitness Platform Log Decoder	11.5.2.0-11409.5
NetWitness Platform Log Player	11.5.2.0-11409.5
NetWitness Platform Malware Analytics Server	11.5.2.0-201016052001.5
NetWitness Platform Metrics Server	11.5.2.0-201130074428.5
NetWitness Platform Node Infra Server	11.5.2.0-201130121407.5
NetWitness Platform Orchestration CLI	11.5.2.0-2010261539.5
NetWitness Platform Orchestration Server	11.5.2.0-201130121431.5
NetWitness Platform Relay Server	11.5.2.0-201207111838.5
NetWitness Platform Respond Server	11.5.2.0-201130124343.5
NetWitness Platform Root CA Update	11.5.2.0-2010201839.5
NetWitness Platform Security Server	11.5.2.0-201130121431.5
NetWitness Platform Shell	11.5.2.0-201123145432.5
NetWitness Platform Source Server	11.5.2.0-201207114039.5
NetWitness Platform User Interface	11.5.2.0-201204152723.5
NetWitness Platform Workbench	11.5.2.0-11409.5
NetWitness Platform SA Tools	11.5.2.0-2011201855.5
NetWitness Platform SMS Server	11.5.2.0-4636.5

Revision History

Date	Description
January 2021	Release to Operations