RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness Platform 11.3.2

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

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

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

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

December 2019

Contents

Introduction

The NetWitness Platform 11.3.2.0 release provides new features and enhancements for every role in the Security Operation Center. These are a few examples: usability improvements to the layout and labeling of the Respond and Incidents List views, improved native network parsers to identify HTTP/2 sessions, update to CentOS 7.6 to take advantage of the latest security updates and improvements, improved endpoint visibility into remote console events, and support for WinRM in User and Entity Behavior Analytics. These sections provide the complete list of enhancements to specific capabilities:

Incident Response

Key Incident Information and Workflow Actions are More Readily Accessible in the Respond View

Key information and actions in the Respond view are now more readily available, such as where to add notes, create tasks, and find related indicators.

Usability improvements to the Respond view layout and labeling provide the following benefits:

- Enables analysts to work more quickly and efficiently to resolve incidents.
- Reduces the amount of analyst training required.
- Reduces time to value.

Incidents List View Improvements

To access the Incidents List view, go to Respond > Incidents.

- Clicking on a row automatically selects the checkbox so that you can take actions on that row, such as changing the priority, status, or assignee. This reduces clicks and improves consistency with other tables in NetWitness Platform.

Incident Details View Improvements

To access the Incident Details view, go to Respond > Incidents and in the Incident List view, click the link in the ID or Name column for that incident.

- Journal and Tasks are more visible and easier to locate.
  - The Journal is open by default on the right-side panel.
  - The labeled 'Journal & Tasks' button enables easy access to notes and tasks without the need for training.
- The Related Indicators are now located on the left-side panel near the incident Indicators, where they are frequently used.
- The Indicators panel is now open by default when an analyst opens a new incident since it provides the analyst more valuable information than the Overview panel.
- In the nodal graph, you can now see file hash nodes for User and Entity Behavior Analytics (UEBA) events.

For more information, see the *NetWitness Respond User Guide*.

Core Services (Broker, Concentrator, Decoder, Archiver)

Network Parsers Identify and Tag HTTP/2 Sessions

NetWitness Platform native network parsers have been improved to identify HTTP/2 sessions and correctly tag them with the `service=80` meta type. Currently, HTTP/2 support is limited to identification only.

Community ID Support

The Network Decoder generates Community ID flow hash values that are compatible with the Community ID specification defined by https://github.com/corelight/community-id-spec.

Administration

Upgrade to CentOS 7.6 Version

RSA upgraded the Operating System (OS) version for NetWitness Platform from CentOS 7.4 to CentOS 7.6. This upgrade was required to keep current with the latest security updates and improvements in CentOS 7.6.

Endpoint Investigation

Visibility into Remote Console Events

Analysts can obtain complete visibility into commands remotely executed by an attacker on a compromised host using the reverse shell technique. The Windows agent has a new capability to capture and report commands passed to the `cmd.exe`, `powershell.exe` process instances using anonymous pipes. Analysts can view these console events with the context as `console.remote` in the Investigate > Navigate and Event Analysis views. For more information, see the *NetWitness Endpoint User Guide*.

Support for REST APIs

To enhance Security Orchestration Automation and Response capability and to integrate with other applications, NetWitness Platform provides a set of REST APIs for hosts and files. For more information, see the *NetWitness Platform API User Guide*.

User and Entity Behavior Analytics

Additional Data Source Support

NetWitness UEBA supports the WinRM (Windows Remote Management) data source, which enables data collection from NetWitness Endpoint agents. This enables the analyst to collect endpoint logs from remote systems and perform analytics to discover, investigate, and monitor risky behaviors across all users and entities in the network environment.

Note: You can collect NetWitness Endpoint agent data only if you are not already collecting data from NIC snare parsers.

Event Stream Analysis

RSA made key performance improvements for ESA Correlation rule deployments:

- Improved analysis performance (EPS) when there are a large number of data sources.
- Improved aggregation speed, especially for data sources that suffer from high latency.
- Position Tracking for data sources now records every minute, reducing risk in error scenarios.
- Rules now deploy faster with better completion progress feedback.
- Improved resiliency and error handling during ESA rule deployment when data sources are slow or down.

Log Collection

Plugin Transform Parameter <includeNullValueParameters> does not Replace Null Tokens to Empty String

RSA has added a parameter to the Transform XML File. This file is used for creating and configuring plugins. The new parameter is `includeEmptyValueParameters`. If you set this parameter to **true**, empty parameters, as well as empty lists, are included in the output of the transform. If set to **false**, which is the default, parsing excludes empty parameters in the output of the transform.

Additionally, the existing parameter `includeNullValueParameters` has been updated to behave as expected. Previously this parameter was incorrectly including or excluding empty value parameters and doing nothing for `null` valued parameters. This parameter now, if set to **true**, includes null tokens items in the output of the transform. If set to **false**, which is the default, parsing excludes null value parameters in the output of the transform.

Warehouse Connector

Aggregate Metadata and Raw Logs for a Log Session into an AVRO File

NetWitness Platform aggregates raw logs and metadata from Log Decoder into a single AVRO file for faster access and easy analysis. The new parameter is `export.logAndsession.avro.enabled`. If set to **yes**, the raw logs and metadata are stored in a file named `sessions-withlogs-*.avro` under sessions directory. If set to **no**, which is the default, they are stored in two separate folders under sessions and logs. For more information, see the *Warehouse Connector Configuration Guide*.

Fixed Issues

This section lists issues fixed since the last major release.

Security

Tracking Number	Description
ASOC-81624	CentOS 7 kernel Security Update - https://access.redhat.com/errata/RHSA-2019:1873
ASOC-79205	CentOS 7 bind Secuirty Update - https://access.redhat.com/errata/RHSA-2019:1294
ASOC-81177	CentOS 7 java-1.8.0-openjdk Security Update - https://access.redhat.com/errata/RHSA-2019:1815
ASOC-81622	CentOS 7 libssh2 Security Update - https://access.redhat.com/errata/RHSA-2019:1884
ASOC-73237	CentOS 7 systemd Security Update - https://access.redhat.com/errata/RHSA-2019:0368
ASOC-79835	CentOS 7 python Security Update - https://access.redhat.com/errata/RHSA-2019:1587
ASOC-77410	CentOS7 python-jinja2 Security Update - https://access.redhat.com/errata/RHSA-2019:1022
ASOC-74485	CentOS 7 openssl Security Update - https://access.redhat.com/errata/RHSA-2019:0483
ASOC-69299	CentOS 7 jasper Security Update - https://access.redhat.com/errata/RHSA-2018:3253
ASOC-69298	CentOS 7 setup Security Update - https://access.redhat.com/errata/RHSA-2018:3249

Tracking Number	Description
ASOC-69292	CentOS 7 glibc Security Update - https://access.redhat.com/errata/RHSA-2018:3092
ASOC-69290	CentOS 7 krb5 Security Update - https://access.redhat.com/errata/RHSA-2018:3071
ASOC-68943	CentOS 7 wget Security Update - https://access.redhat.com/errata/RHSA-2018:3052
ASOC-68887	CentOS 7 binutils Security Update - https://access.redhat.com/errata/RHSA-2018:3032
ASOC-65195	CentOS 7 nss Security Update - https://access.redhat.com/errata/RHSA-2018:2768
ASOC-81623	CentOS 7 curl Security Update - https://access.redhat.com/errata/RHSA-2019:1880
ASOC-81621	CentOS 7 httpd Security Update - https://access.redhat.com/errata/RHSA-2019:1898
ASOC-80161	CentOS 7 vim Security Updated - https://access.redhat.com/errata/RHSA-2019:1619
ASOC-78364	CentOS 7 wget Security Update - https://access.redhat.com/errata/RHSA-2019:1228
ASOC-73832	CentOS 7 polkit Security Update - https://access.redhat.com/errata/RHSA-2019:0230
ASOC-70077	CentOS 7 samba Security Update - https://access.redhat.com/errata/RHSA-2018:3056

Upgrade

Tracking Number	Description
ASOC-79110	After you upgrade to 11.3.1, the default CEF and Human readable format, audit templates are not updated.

NetWitness Endpoint

Tracking Number	Description
ASOC-82880	Registry Monitor may cause Blue Screen Error on 32-bit agents.
ASOC-82891	In the policy, the Windows Log Setting, Send Test Log is not working.

Core Services (Broker, Concentrator, Decoder, Archiver)

Tracking Number	Description
SACE-12285	Log Decoder is not receiving data over UDP.
SACE-12068	The Physical Drives and Logical Drives for all core appliances is missing in the Service Stats view.

Investigation

Tracking Number	Description
SACE-11752	Unable to download file for external account from the Event Analysis view.
SACE-11365	When a Broker is connected to any offline Concentrator, the timeline will not render results in the Investigation.
SACE-12126	“Score” custom meta key is not displaying correct results.

Administration

Tracking Number	Description
SACE-12189	After upgrade, unable to export all the existing application rules from the Decoder due to huge size.

Event Stream Analysis

Tracking Number	Description
SACE-11827	When you export ESA rules from the NetWitness Platform UI, you are unable to import due to the Endpoint bundle file in it.
SACE-11857	If you have an ESA rule in more than one ESA rule deployment and that rule has notifications, if you delete the rule from one deployment, then the notifications in the other deployments break and you have to redeploy the other deployments.
SACE-12089	When redeploying ESA rules, aggregation would sometimes resume from data sources at the wrong position in time.
SACE-12182	Adjusted the timestamp format in notifications to match previous NetWitness Platform versions for compatibility.
ASOC-82076	If a Concentrator is added to the available data sources for ESA rule deployments and then the host is removed from the NetWitness server, you can still see that host in the available data sources list.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.3.2.0.

Component	Version Number
NetWitness Platform Decoder	11.3.2.0-9916.5
NetWitness Platform Concentrator	11.3.2.0-9916.5
NetWitness Platform Broker	11.3.2.0-9916.5
NetWitness Platform Log Decoder	11.3.2.0-9916.5
NetWitness Platform Archiver (Work-bench)	11.3.2.0-9916.5
NetWitness Platform ESA Analytics Server	11.3.2.0-190911141733.5
NetWitness Platform Correlation Server	11.3.2.0-191107173904.5
NetWitness Platform Appliance	11.3.2.0-9916.5
NetWitness Platform Archiver	11.3.2.0-9916.5
NetWitness Platform Cloud Gateway Server	11.3.1.0-190310223630.5
NetWitness Platform Console	11.3.2.0-9916.5
NetWitness Platform Endpoint Agents	11.3.2.0-1910142004.5
NetWitness Platform Endpoint Broker Server	11.3.2.0-190807043944.5
NetWitness Platform Endpoint Server	11.3.2.0-191009045426.5
NetWitness Platform Endpoint RAR Server	11.3.2.0-190807044150.5

NetWitness Platform Malware Analytics Server	11.3.2.0-191111132647.5
NetWitness Platform Legacy Web Server	11.3.2.0-191111132522.5
NetWitness Platform Orchestration Server	11.3.2.0-191009045712.5
NetWitness Platform Respond Server	11.3.2.0-191009045541.5
NetWitness Platform Security Server	11.3.2.0-191009045628.5

Update Notes

The following update paths are supported for NetWitness Platform 11.3.2.0:

- NetWitness Platform 11.1.0.0 to 11.3.2.0
- NetWitness Platform 11.1.0.1 to 11.3.2.0
- NetWitness Platform 11.1.0.2 to 11.3.2.0
- NetWitness Platform 11.1.0.3 to 11.3.2.0
- NetWitness Platform 11.2.0.0 to 11.3.2.0
- NetWitness Platform 11.2.0.1 to 11.3.2.0
- NetWitness Platform 11.2.1.0 to 11.3.2.0
- NetWitness Platform 11.2.1.1 to 11.3.2.0
- NetWitness Platform 11.2.1.2 to 11.3.2.0
- NetWitness Platform 11.3.0.0 to 11.3.2.0
- NetWitness Platform 11.3.0.1 to 11.3.2.0
- NetWitness Platform 11.3.0.2 to 11.3.2.0
- NetWitness Platform 11.3.1.0 to 11.3.2.0
- NetWitness Platform 11.3.1.1 to 11.3.2.0

For more information on updating to 11.3.2.0, see the *Update Guide for RSA NetWitness Platform 11.3.2.0* on RSA Link. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Product Documentation

The following documentation is provided with this release.

Document	Location
NetWitness Platform 11.3.2.0 Product Documentation	https://community.rsa.com/community/products/netwitness/113
NetWitness Platform Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Known Issues

Issues that remain unresolved in this release are documented here: https://community.rsa.com/community/products/netwitness/documentation/known-issues. Wherever a workaround is available, it is noted or referenced in detail.

Feedback on Product Documentation

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

Contacting Customer Support

If you have questions, or you have any issues with this update, contact Customer Support for assistance (https://community.rsa.com/docs/DOC-1294).