RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness Platform 11.3.1.1

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.

October 2019

Contents

Introduction

This document lists enhancements and fixes in NetWitness Platform 11.3.1.1. Read this document before deploying or updating to NetWitness Platform 11.3.1.1.

Note: NetWitness Platform 11.3.1.1 replaces the NetWitness Platform 11.3.1 release. This release contains all the features of 11.3.1 and 11.3.0.2 (significant improvements to Event Stream Analysis (ESA)).

Note: If you are on 11.1.x.x, 11.2.x.x or 11.3.x.x, you must upgrade to 11.3.1.1. For information about the upgrade paths, see Upgrade Notes.

These sections provide the complete list of enhancements in this release:

Core Services (Broker, Concentrator, Decoder, Archiver)

Save Interval for Core Service Indexes Has Been Reduced to Improve Memory Consumption

The default save interval for Core service indexes has been reduced from 600 million to 200 million when it is set to `auto`. This allows large indexes to be saved more frequently, which reduces the index slice size and consequently reduces memory consumption in the index.

Expanded Detection of Encrypted Channels

To help you identify encrypted channels, the Network Decoder can produce the JA3 value of TLS clients and the JA3S value of TLS servers that are observed in a network session. The values that are produced conform to the values generated by the open source JA3 tools (https://github.com/salesforce/ja3). For more information, see "JA3 and JA3S TLS Fingerprints" in the *Decoder and Log Decoder Configuration Guide for RSA NetWitness Platform*.

Administration

Centralized Audit Logging

NetWitness Platform collects audit logs from all services and aggregates the logs into a single file in a centralized location for faster access and easy analysis. Standard filters determine and control the logs that must be aggregated. For more information, see "Centralized Audit Logging" in the *System Configuration Guide for RSA NetWitness Platform*.

Improved Audit Logging Text

Audit logging is improved to provide further granularity on the action taken, or the recipient of the action when that context is necessary. Audit logging descriptions for users logging on and off hosts have been improved in audit logs. You can view audit logs in the NetWitness Platform User Interface (select a log service and then View > Logs) or in the REST API (select `/logs` and then `/logs/download`, and then choose a time frame and the type of logs to be audited). For more information, see "Configure Global Audit Logging" in the *System Configuration Guide for RSA NetWitness Platform*, and the *RESTful API User Guide for RSA NetWitness Platform*.

Apply Version Updates from the User Interface without Direct Internet Access

After you update NetWitness Platform to 11.3.1.1, you can apply future version updates from the Hosts view in the User Interface (UI) without a NetWitness Platform connection to the Internet (for example, no Live connection). For detailed instructions on how to do this, refer to “Apply Update from Hosts View without RSA Live Update Repo Connection (No Web Access)" in the *Hosts and Services Getting Started Guide for RSA NetWitness Platform*.

DISA STIG Support

In 11.3.1.1, RSA added support for Audit Rules in the DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide) Control Group. For more information, see the "DISA STIG" topic in the *System Maintenance Guide for RSA NetWitness Platform*.

Health and Wellness

Monitor Lockbox Status for Warehouse Connector

A new Health & Wellness statistic for Warehouse Connector is added to indicate the status of its Lockbox. In addition, an out-of-the-box rule is added so that a Health & Wellness alarm is raised when the Lockbox does not exist or cannot be opened.

Monitor Risk Process Improved for Host and Files

This applies to customers who are using NetWitness Endpoint. New statistics and policies are added in Health & Wellness to monitor the health of Risk scores for hosts and files.

Monitor Health of Relay Servers

This applies to customers who are using NetWitness Endpoint. New statistics are added in Health & Wellness to monitor the health of relay servers.

Monitor System Resources for Virtual Log Collectors

A new statistic and policy are added in Health & Wellness to monitor the virtual system resource status for Virtual Log Collector configurations. The new out-of-the-box rule provides an indication of a VLC system that may be under-resourced for the current load.

Monitor Message Broker System Resources for Virtual Log Collectors

A new statistic and policy are added in Health & Wellness to monitor the message broker status for Virtual Log Collector configurations. The new out-of-the-box rule provides an indication of a when the message broker system's resources are near capacity, which indicates the VLC may be under-resourced for the current load.

Monitor Message Broker Queues for Log Collectors

A new policy is added in Health & Wellness to monitor when the message broker queue status reaches more than 50k messages for 10 minutes. The new out-of-the-box rule provides an indication of when there is a potential problem with the connection or processing of the upstream VLC or Log Decoder system, so that it can be remedied before system resources are affected.

Improved Message Broker Logging

Improved log rotation management and reduced the amount of information logged for the message broker to reduce disk usage.

Improved Message Broker Resource Management

Improved the H&W message broker system resource limits to match the system's available resources to reduce disk usage and memory resource issues.

Event Stream Analysis

Introduced a New Improved ESA Correlation Service for ESA Correlation Rules

The ESA Correlation service replaces the Event Stream Analysis service found in previous NetWitness Platform versions. Like the Event Stream Analysis service, the ESA Correlation service installs on the ESA Primary and ESA Secondary host types.

There are two ESA services that can run on an ESA host:

- ESA Correlation (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

The Context Hub server service, which provides enrichment lookup capability in the Respond and Investigate views, runs only on an ESA Primary host.

Support for Different Data Sources for Your ESA Correlation Rules

Instead of adding data sources, such as Concentrators, to the entire service, you can specify different data sources for each ESA rule deployment. For example, you may want to use Concentrators with HTTP packet data in one deployment and Concentrators with HTTP log data in another deployment. For more information, see the *Alerting with ESA Correlation Rules User Guide*.

For upgrade considerations for ESA rule deployments, see the applicable upgrade and update instructions as well as the *ESA Configuration Guide*.

The ESA Correlation Service Preserves Previous Versions of Multi-Value and Single Value Meta Keys Used in ESA Rules

The ESA Correlation service preserves the multi-valued and single-valued meta keys used in your existing ESA rules during an upgrade or update to the latest NetWitness Platform version. These meta keys are in the **multi-valued** and **single-valued** parameter fields in the ESA Correlation service. These parameters contain the current meta keys used for your ESA rules.

Required meta keys for the latest NetWitness Platform version are in the **default-multi-valued** and **default-single-valued** parameter fields in the ESA Correlation service. If the meta keys used for your ESA rules are different from the required meta keys, your ESA rules continue to work, but you should update your ESA rules to use the required meta keys as soon as possible to ensure that your rules continue to deploy properly. As you adjust your ESA rules, adjust the **multi-valued** and **single-valued** parameters to include the required meta keys.

To access these parameters, go to ADMIN > Services, and in the Services view, select an ESA Correlation service and then select  > View > Explore. In the Explore view node list for an ESA Correlation service, select **correlation > stream**.

To use the latest Endpoint, UEBA, and Live content rules, you must update the **multi-valued** parameter on the ESA Correlation service to include all of the meta keys in the **default-multi-valued** field. You must also update the **single-valued** parameter field to include all of the meta keys in the **default-single-valued** field.

Caution: Any changes that you make to the **multi-valued** parameter may cause an error when you deploy your existing rules. You can update the **multi-valued** parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

The New ESA Correlation Service Supports Endpoint and UEBA Content

To support Endpoint and UEBA content as well as changes to ESA rules from Live, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service.

The following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform:

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file ,
analysis.service , analysis.session , boc , browserprint , cert.thumbprint ,
checksum , checksum.all , checksum.dst , checksum.src , client.all , content ,
context , context.all , context.dst , context.src , dir.path , dir.path.dst ,
dir.path.src , directory , directory.all , directory.dst , directory.src , email
, email.dst , email.src , eoc , feed.category , feed.desc , feed.name , file.cat
, file.cat.dst , file.cat.src , filename.dst , filename.src , filter , function ,
host.all , host.dst , host.orig , host.src , host.state , inv.category ,
inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param , param.dst ,
param.src , registry.key , registry.value , risk , risk.info , risk.suspicious ,
risk.warning , threat.category , threat.desc , threat.source , user.agent ,
username
```

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform:

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

When upgrading to NetWitness Platform, some ESA rules from Live and ESA advanced rules must be updated to use array syntax and redeployed. You also need to adjust any custom rules to use array syntax as required. For more information, see the Event Stream Analysis (ESA) tasks in the upgrade or update instructions. To change the string type meta keys to string array type meta keys, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*.

ESA Automatically Adjusts the ESA Rule Statement Operator if an ESA Rule References a Meta Key that Changed from String to String Array

When you update ESA Rule Builder rules from string to string array, you also need to ensure that you are using a string array operator. ESA now automatically adjusts the operator in the rule statement when there is a change from string to string array.

Note: Advanced EPL rules may become disabled and are not automatically updated so they must be fixed manually.

View Error Messages for Disabled ESA Rules in the NetWitness Platform User Interface

Administrators can check the status of ESA Rules in the ESA Rules section of the ESA rule deployment (go to CONFIGURE > ESA Rules > Rules tab, select a deployment in the options panel on the left, and go to the ESA Rules section). If a disabled rule has an error message, it now shows in the Status field. Hover over the rule to view the error message tooltip without going to the error log. For more information, see the *Alerting with ESA Correlation Rules User Guide for RSA NetWitness Platform*.

To Avoid Unnecessary Processing Overhead, the Ignore Case Option is Not Available for Meta Keys that are Not Real Strings

To avoid unnecessary processing overhead, the Ignore Case option has been removed from the ESA Rule Builder - Build a Statement dialog for meta keys that do not contain text data values. The Ignore Case option allows meta values being compared to match regardless of case differences existing between the two values (for example, "JOHN SMITH" matches "John Smith" if Ignore Case is in effect). Adding Ignore Case on meta keys that do not contain alphabetic values causes additional processing to occur for no added benefit. For example, using Ignore Case on IP Addresses (for example, `ip_src` and `ip_dst`) provides no value and causes a slowdown in processing. Only meta keys listed as Text fields in the NetWitness Core database index files will continue to have the Ignore Case option available.

Likewise, when using the advanced EPL Rules with ESA, care should be taken to only add the case-insensitive `toLowerCase()` function on meta keys as needed. The `toLowerCase()` function can cause significant performance decreases. Consider checking the Investigate Events view or the Event Analysis view to see the actual character case for meta fields and avoid unnecessary usage of the function.

Note: During an upgrade or update, NetWitness Platform does not modify existing rules, advanced EPL rules, or content rules for the Ignore Case option. If an existing Rule Builder rule has the Ignore Case option selected for a meta key that no longer has the option available, an error occurs if you try to edit the statement and try to save it again without clearing the checkbox. When you edit your ESA rule in the rule builder and change a condition in the Build a Statement dialog, reselect the key to update the operator according to the type of meta. Reselecting the key also clears and removes the checkbox for a meta key that no longer has the Ignore Case option available.

Introduced Special Case-Insensitive Meta Keys to Optimize ESA Rule Deployments

You can optimize your rule performance by identifying the string and string array meta keys used most often in your environment. Instead of using the `toLowerCase()` function with the original meta key in your advanced ESA rules, you can replace the meta key throughout the rule with `<meta.key>_lower`. You can also use the special case-insensitive meta keys in your Rule Builder rules. For example, you can configure ESA Correlation to use `filename_lower` (which is case insensitive) instead of using the original filename meta key. In your rule, replace filename with `filename_lower`. To set up the special case-insensitive meta keys, see “Configure Character Case for Advanced ESA Rules” in the *ESA Configuration Guide*.

Note: String and string array are the only data types supported for the ESA Correlation service **lowercase** parameter.

Support for Adjusting the Compression Level for Concentrators on ESA

When you set up an ESA rule deployment and configure a Concentrator to use as a data source, you have the option to set the data compression level for the Concentrator on ESA. For more information, see the *Alerting with ESA Correlation Rules User Guide*.

Enable or Disable Forwarding Individual ESA Rule Alerts to the Respond View

You can turn alerts on or off for individual ESA rules. For more information, see the *ESA Configuration Guide*.

ESPER Version Upgraded from Version 5.3 to 7.1

Upgraded ESPER to the latest 7.1 release.

Endpoint Investigation

RSA NetWitness Relay Enables Offline Reporting of NetWitness Endpoint Protected Hosts

Relay Servers (referred to as RAR in prior versions of RSA NetWitness Endpoint) extend NetWitness Platform's visibility into endpoints while connected outside the corporate network. By configuring a relay in either the cloud or DMZ, any NetWitness Endpoint protected hosts can connect to the Relay Server to send updates on host activity and receive any time-sensitive response actions. For more information, see the *NetWitness Endpoint Configuration Guide for RSA NetWitness Platform*.

Data Retention for Risk Scores

Analysts can retain risk score data for a specified amount of time before it is deleted. Data retention for risk scores is enabled by default, with the retention period configured for 30 days, to free up the disk space periodically. However, the amount of time risk score data is retained is configurable. For more information, see the *NetWitness Respond Configuration Guide for RSA NetWitness Platform*.

Network Data and Log Investigation

Configurable Event Analysis View Event Limit in the ADMIN > System > Investigation Panel

To optimize performance in Event Analysis, administrators can configure the default number of events loaded in the Events panel and then configure a lower limit for different user roles. For details, see "Configure Event Analysis View Settings" in the *System Configuration Guide for RSA NetWitness Platform*.

Result Messaging Provides Clarity on the Reason that Events Were Not Found in Investigate

To eliminate the potential for analysts to interpret false negative results as accurate, messaging in the Event Analysis view differentiates between no matches in the data set and other reasons for no data being found. The lack of events returned may be due to a meta key that is not recognized or data that is not indexed.

Configurable Clearing of the Reconstruction Cache in the Event Analysis View to Save Disk Space

Any Event Analysis view reconstruction cache older than 24 hours is automatically cleared every 24 hours at 3 a.m. to avoid filling up disk space and to clear data from the Investigate user interface. The administrator can change the interval to an interval greater than 24 hours. For additional information, see "Configure the Reconstruction Cache Clearing Interval for the Event Analysis View" in the *System Configuration Guide for RSA NetWitness Platform*.

Incident Response

Simplified Update Process for Incident Rule Schema

Instead of backing up the `aggregation_rule_schema` file manually before it is overwritten during an update, NetWitness Platform now automatically creates a backup file before refreshing the `aggregation_rule_schema` file. Any prior customizations can be copied from the automatic backup file to the new schema file.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.x, you can modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file. The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format: `aggregation_rule_schema.json.bak-<time of the backup>`.

User and Entity Behavior Analytics

Support for Linux as a Data Source

NetWitness UEBA now supports RedHat Linux as a data source.

Support for Failed Authentication of Network Logons

NetWitness UEBA supports alerts for failed authentication of network logons (Type 3) taken from Windows event 4625.

Increased Scale of Support for Customers with Large Numbers of Endpoint and Log Events

NetWitness UEBA has increased its scale of support for customers with large numbers of users (for example, 100,000 users) who generate large quantities of log and endpoint events.

Fixed Issues

This topic is divided into two sections, based on the version:

Issues fixed in 11.3.1.1

This section lists issues fixed in NetWitness Platform 11.3.1.1.

Event Stream Analysis (ESA)

Tracking Number	Description
ASOC-82658 SACE-11759	When you deploy ESA rules, sometimes an error occurs that shows that the rules are disabled in the user interface (CONFIGURE > ESA Rules> Rules tab Deployment panel) when the ESA rule deployment is actually successful.
ASOC-82802	The maximum memory for the ESA Correlation server has been changed to 164 GB.
ASOC-82346	Unable to delete an endpoint bundle from an ESA deployment.
ASOC-82106	Converting arrays `toLowerCase` for use in `GROUP BY` or `PARTITION BY` function in Esper/ESA causes partitioning to malfunction.
ASOC-82105	Health & Wellness shows that ESA Correlation is Unhealthy after a notification failure and does not resolve itself over time.
ASOC-82103	ESA rules with Context Hub lists get disabled during upgrade when there are duplicate Context Hub data sources.
ASOC-82102	If the rules memory threshold is set to 60%, it needs tuning to avoid false Health & Wellness alerts.

Investigate

Tracking Number	Description
SACE-11800	If a `max.unique.values`.parameter is used for a single query on a Broker or Concentrator, an error is returned.
SACE-11226	In the Events view, when you select a metadata, you are not able to drill-down to view the details.
ASOC-81394	In the Navigate view, when you type a query such as `ip.src exists`, the query changes to a different query.
ASOC-80919	Meta values for the <span.code>Directory<span.code> meta key are truncated, if it contains multiple forward slash (/) characters.
ASOC-80278	In the Event Analysis view, Guided Mode, you cannot specify a query filter with CIDR notation for an IP address as it is not supported.

ASOC-80275	When you click on View Files in the Reconstruction view, you cannot download a file with special Korean characters in the file name. The following error message is displayed: `Unable to create temporary file, <filename with Korean characters>_temp_<nnnnnn>.tmp`.
ASOC-80263	When you Pivot to Investigate from the dashboard using an IP address, an invalid query is created and an error message is displayed.

Core Services (Broker, Concentrator, Decoder, Archiver)

Tracking Number	Description
SACE-11945	After upgrading from 11.2.1.1 to 11.3.1, Investigate searches from the Broker service are not working intemittenly.
SACE-11571	NetWitness appliance service crashes with SIGABRT during service monitoring on the Log Decoder.
ASOC-80266	CEF parser removes backslash (\) character.

Admin

Tracking Number	Description
ASOC-80280	On the Event Source Monitoring tab, if you sort by ascending or descending order, the Idle time column is not sorted.
ASOC-80270	Unable to log in to the Active Directory using UserPrincipalName.

Reporting Engine

Tracking Number	Description
SACE-11892	SFTP output action is not working properly.
SACE-11980 SACE-11491	Reports for the Respond server are not generating any results.
ASOC-81404	When multiple rules are applied in a single report and exported to PDF, data in the PDF is overlapped.

NetWitness Endpoint

Tracking Number	Description
ASOC-80796	Endpoint agent is not able to send Windows events when Event IDs more than 23 are configured in the log filter.
ASOC-80629	Linux agent crashes during a scan when it encounters a particular ELF file with no sections
ASOC-80227	"Unsigned Reserved Name" rule is not tracking events correctly.

Archiver

Tracking Number	Description
SACE-11837 SACE-12018	Retention rule does not filters logs in Archiver collection properly.
SACE-10744	Unable to push `index-archiver-custom.xml` from one Archiver to other Archiver services.

Upgrade

Tracking Number	Description
SACE-11954	After upgrading NetWitness Server to 11.3.1.0, the reports are failing due to `std::bad_alloc` error in the Reporting Engine.
SACE-11951 SACE-11895	After upgrading to 11.3.0.1, Brokers failed to retrieve meta keys, which prevented visualization to load in Investigate. This affected second level and top level Brokers.

Server

Tracking Number	Description
SACE-11362 SACE-11864	User credentials sometimes gets exchanged while performing a query on Investigate View.

ASOC-79876	When the Event Source Manage groups have the Idle time condition defined, alarms are not generated.

Issues fixed in 11.3.1

This section lists issues that were fixed in 11.3.1 release.

Security

Tracking Number	Description
ASOC-75957	Python Security Update https://access.redhat.com/errata/RHSA-2019:0710.

ESA

Tracking Number	Description
SACE-11668 ASOC-79640	Disabled rules were re-enabled after deployment and ESA Correlation service restart.
ASOC-83241	Sample Enrichment ESA rules are being disabled on 11.3.0.2 due to `src_ip` meta key error

Respond

Tracking Number	Description
ASOC-73743	Deleting an alert in Respond is not updating the High-Risk User List in Threat Aware Authentication.
ASOC-72759	Respond statistics reset after update. This is fixed for updates from 11.3 to 11.3.x, but is still an issue for updates from 11.2.x to 11.3.x.
ASOC-60463	Proper message is not displayed when Event Analysis is not loading in a mixed-mode environment.

Investigate

Tracking Number	Description
ASOC-73894	In Print Mode, raw meta key and descriptive names are missing.
ASOC-73826	In the Event Analysis view, the query console does not replace the information icon with an error icon when a service is offline.
ASOC-73224	When retrieval of events for a query is in progress in the Event Analysis view, events that are already displayed disappear if the query takes more than 5 minutes to finish.
ASOC-60464	The error message displayed when a download from the user interface times out needs clarification.

NetWitness Endpoint

Tracking Number	Description
ASOC-73120 ASOC-74872	Issues with the Powershell console events in Windows 10 1809 have been fixed in 11.3.1.

Core Services (Broker, Concentrator, Decoder, Archiver)

Tracking Number	Description
ASOC-75007	Previously, if the Log Decoder was sent bad data that appeared to consist of a certain number of bytes, but the message contained fewer bytes, the Log Decoder waited indefinitely for data that never arrived. The number of bytes allowed for length-prefixed transmissions is now limited to address this issue.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.3.1.1.

Component	Version Number
NetWitness Platform Decoder	11.3.1.1-9848.5
NetWitness Platform Concentrator	11.3.1.1-9848.5
NetWitness Platform Broker	11.3.1.1-9848.5
NetWitness Platform Log Decoder	11.3.1.1-9848.5
NetWitness Platform Archiver (Workbench)	11.3.1.1-9848.5
NetWitness Platform Appliance	11.3.1.1-9848.5
NetWitness Platform Console	11.3.1.1-9848.5
NetWitness Platform Endpoint Agents	11.3.1.1-1907311741.5
NetWitness Platform Log Player	11.3.1.1-9848.5
NetWitness Platform Respond Server	11.3.1.1-190809035730.5
NetWitness Platform SDK	11.3.1.1-9848.5

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.

Upgrade Notes

The following upgrade paths are supported for NetWitness Platform 11.3.1.1:

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

For more information on upgrading to 11.3.1.1, see the *Upgrade Guide for RSA NetWitness Platform 11.3.1.1* 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 Online Documentation	https://community.rsa.com/community/products/netwitness/113

Feedback on Product Documentation

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

Contact Customer Care

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